Significant Cyber Incidents Since 2006

This timeline lists significant cyber incidents since 2006. We focus on state actions, espionage, and cyberattacks where losses are more than a million dollars. This is a living document. When we learn of a cyber incident, we add it to the tracker in chronological order. If you think we've missed something, please send an email to strategictech@csis.org.

October 2026: A suspected cyberattack targeting the State Bank of India (SBI), the country's largest lender, exposed 3,897 customer records on the dark web. The compromised information included customers' names, mobile numbers, dates of birth, gender, email and residential addresses, bank branch and customer identification numbers, and metadata associated with loan records. The bank identified the exposure after receiving alerts from its threat intelligence provider, India's Defense Cyber Agency, and CERT-In on October 16. SBI engaged an independent cybersecurity firm to investigate the source and extent of the breach and subsequently confirmed that affected customers had been individually notified.

October 2026: AI agents reportedly infiltrated the live systems of multiple Indian organizations, accessing confidential business records and personal information without authorization. According to India's Computer Emergency Response Team (CERT-In), the incidents involved both malicious use of AI-powered tools and AI agents exceeding their assigned operational tasks, allowing them to access sensitive data without being detected.

October 2026: A cyberattack targeting government contractor Senture disrupted the Federal Motor Carrier Safety Administration's (FMCSA) contact center, temporarily taking offline telephone support for commercial truck drivers and operators using the Department of Transportation's new Motus registration platform. The contractor's network domain and phone services were affected, forcing users to rely on alternative online ticketing and chat support. The disruption was first reported on October 6, and the Department of Transportation confirmed the incident. Officials stated that FMCSA data was not compromised.

October 2026: Suspected AI-assisted cyberattacks targeting 16 South Korean financial institutions exposed approximately 100,000 customer records, including names, contact details and resident registration numbers. Affected organizations included major banks, payment providers, and cryptocurrency businesses. South Korea's FSC and FSS launched investigations to identify the attack methods and determine whether the incidents were linked. The perpetrators remain unidentified.

October 2026: A new wave of cyberattacks affected Daishin Securities, Mirae Asset, and cryptocurrency exchange Bithumb. Daishin Securities confirmed that personal and financial information belonging to 38,490 customers was exposed, while Bithumb reported unauthorized access to employee information. Mirae Asset also identified unauthorized system access but reported no confirmed investor data exposure. South Korean authorities are investigating

potential links to earlier attacks on 16 financial institutions; no threat actor has been identified.

October 2026: Suspected cyberattacks on South Korea's Yoido Full Gospel and SaRang churches potentially compromised records of more than 850,000 congregants, including personal information, financial records and internal documents. Attackers reportedly exploited compromised credentials and application vulnerabilities to gain administrative access. Researchers also identified possible use of AI tools to automate vulnerability analysis and data extraction. Both churches have taken containment measures and notified authorities.

October 2026: A wave of cyberattacks targeting major Japanese companies and government institutions exposed personal information associated with millions of accounts. Ryohin Keikaku, the operator of Muji, reported that up to 27.26 million accounts may have been compromised, while restaurant chain Matsuya disclosed a breach affecting approximately 2.38 million users, exposing names and telephone numbers. All Nippon Airways (ANA) also reported the exposure of information belonging to approximately 37,800 passengers, including passport numbers, telephone numbers, and nationalities for a subset of affected individuals. Separately, Japan's Foreign Ministry reported a potential leak involving approximately 3,600 records, including names and email addresses.

October 2026: Hackers stole approximately $2.7 million from 737 Polymarket accounts after compromising a third-party website performance-monitoring provider, DebugBear, whose malicious JavaScript was embedded in Polymarket's international trading platform. The script exploited active user sessions to sell prediction-market positions and transfer funds without users' authorization, resulting in 985 unauthorized withdrawals within approximately one hour.

October 2026: Approximately 53,000 Cathay Pacific flight bookings were affected by unauthorized access to reservation data held by third-party travel technology provider Amadeus IT Group. The breach, which involved the use of compromised system-account login credentials, exposed booking references, passenger names, and flight details, while a smaller subset of records potentially included email addresses, phone numbers, travel document information, and frequent-flyer numbers. Cathay Pacific confirmed that its own systems and operations were unaffected and that there was no evidence of financial or payment information being accessed or exposed data being misused.

October 2026: A critical vulnerability (CVE-2026-101767, CVSS 9.8) affecting Oracle E-Business Suite was actively probed by attackers following the release of a security patch. The unauthenticated SQL injection flaw could allow remote attackers to execute arbitrary SQL and operating system commands, potentially gaining full control of affected systems and accessing sensitive financial, payroll, and human resources data. Exploratory exploitation attempts were detected against Oracle EBS honeypots on October 27. The vulnerability affects versions 12.2.3 through 12.2.15, with earlier unsupported versions also potentially exposed.

October 2026: LiteLLM's software release pipeline was compromised, resulting in the distribution of a malicious version (v1.107.0) through PyPI and Docker Hub. The compromised package contained malware designed to steal credentials, including API keys, cloud credentials, and database passwords, and enable remote code execution. The malicious PyPI package was available for approximately two hours, while affected Docker images remained accessible for

nearly three hours. LiteLLM removed the compromised releases and advised affected users to rotate exposed credentials. The attackers reportedly exploited stolen developer GitHub credentials to bypass security protections and publish malicious software through an attacker-controlled repository.

October 2026: Cyberattacks compromised refrigeration systems at least 350 French supermarkets, remotely forcing refrigerators and freezers into defrost mode and raising temperatures to 50°C (122°F), resulting in spoiled food, equipment damage, and losses estimated at tens of millions of euros. The attacks exploited internet-exposed Danfoss operational technology (OT) controllers, many running outdated or unsupported firmware.

October 2026: Indian digital trust company eMudhra announced its withdrawal from the global SSL/TLS certificate business after a security researcher discovered that the private keys associated with eight of its intermediate Certificate Authorities (CAs) were cryptographically weak and could be easily recovered. The flaw potentially allowed attackers to generate fraudulent certificates and impersonate legitimate websites and online services. Google, Mozilla, Apple, and Microsoft subsequently moved to distrust the affected certificates. eMudhra revoked all eight intermediate certificates and maintained that its infrastructure had not been compromised and no customer data had been breached.

October 2026: Multiple government agencies and public services across Europe temporarily took their websites and online platforms offline following the discovery of two critical vulnerabilities, dubbed "PHP2Shell," which could allow unauthenticated attackers to remotely execute code and gain control of affected servers. The vulnerabilities rated 9.2 out of 10 in severity, potentially exposed sensitive information, including passwords, authentication tokens, and access keys. Amazon Threat Intelligence detected exploitation attempts as early as October 17, four days before public disclosure, with subsequent attempts suggesting the involvement of multiple actors. Governments in the Netherlands, Finland, Denmark, and the UK restricted or suspended services as a precaution while emergency patches were deployed. No confirmed government compromise has been publicly attributed to the vulnerabilities.

October 2026: Hackers stole approximately $6.3 billion in cryptocurrency from Binance, the world's largest cryptocurrency exchange, in what is believed to be the largest crypto heist on record. The attackers reportedly exploited compromised internal systems to authorize unauthorized withdrawals across multiple blockchain networks. The attack was attributed to TraderTraitor, a North Korean state-sponsored hacking group. Binance suspended withdrawals and worked with law enforcement and industry partners to freeze and recover the stolen assets, pledging to cover customer losses.

October 2026: More than 40,000 Department of Homeland Security employee records were published online after an apparent breach, exposing names, contact information, job titles, and details tied to sensitive roles including surveillance, forensics, and undercover work. So far, no actor has been publicly linked to the attack.

September 2026: China-linked hackers impersonated an Anthropic employee and former U.S. officials in phishing campaigns targeting AI policy experts, seeking access to accounts that could

reveal insights on export controls and military AI.

September 2026: The UK's MI5 has accused China of using academic collaborations to obtain sensitive research, warning that more than 100 UK-based academics have unknowingly contributed to projects linked to China's Ministry of State Security in areas including AI, cybersecurity, and covert communications. China's embassy has rejected the allegations as baseless.

September 2026: The FBI is investigating claims that ShinyHunters breached its jobs portal and obtained sensitive information on FBI personnel and applicants. The group claims it stole 2–3 terabytes of data, though the full extent and source of the alleged breach remain unverified.

September 2026: Researchers at an AI nonprofit, Transluce, reported suspicious AI activity on Canadian government websites. AI agents attempted to access Library and Archives Canada, though they did not appear to be successful. While the source of the agents remains unconfirmed, researchers noted their behaviors as similar to OpenAI models.

September 2026: OpenAI agents violated explicit user guidelines when accessing websites for the Department of Education, the Securities Exchange Commission, and Commerce Department. No data was breached, however the agents reportedly used "gray area" tactics when exploring the websites. OpenAI discovered the activity while researchers were reviewing other incidents like the June hack on Australia's healthcare website.

September 2026: Air Traffic and Navigation Services (ATNS), a state-owned company based in South Africa, reportedly discovered ransomware-linked malware in its operational technology (OT) networks. ATNS is responsible for air traffic operations and weather control in 10% of the global airspace. Early investigations highlight data exfiltration to external IP addresses located in China.

September 2026: The Tokyo metro reported that an unauthorized third party had accessed the email addresses of up to 59,000 passengers subscribed to the Metpo loyalty program. Operators quickly contained the threat and identified a suspected point of access to prevent further occurrences.

September 2026: Novocure, an oncology company, reported unauthorized access that exposed internal records of over 1,400 patients in the United States. Data included patient ID numbers, contact information for healthcare providers the company works with, and employee job titles and phone numbers. Additional information was exposed for less than 50 other patients in the Western U.S. The company reports that all systems remain functional.

September 2026: Singapore telecommunications company SIMBA reported a data breach affecting 23,549 customers. Exposed information included customers' names, identity card numbers, dates of birth, mobile numbers, and email addresses. The company said it had contained and resolved the incident, was reviewing its security measures, and was notifying affected customers. Singapore's Personal Data Protection Commission is investigating the

breach.

September 2026: Data from a database reportedly containing 32.8 million Condé Nast user records was offered for sale for $15,000 on a Russian-language cybercrime forum. The dataset allegedly includes email addresses, names, postal addresses, gender, dates of birth, and phone numbers, but reportedly does not contain passwords, password hashes, usernames, or payment-card information. Researchers who reviewed a 5,000-record sample said the data appeared consistent with genuine Condé Nast account information collected between September and October 2025. Condé Nast has not publicly confirmed the breach or commented on the sale.

September 2026: Gyazo, an image-sharing service operated by Helpfeel, reported unauthorized access that exposed data associated with approximately 23.62 million user records. Exposed information varied by user and could include names, email addresses, user IDs, password hashes, device IDs, login session IDs, profile information, and authentication tokens. Attackers also accessed metadata for approximately 490 million images, including information that could potentially be used to construct image URLs, as well as a list of private images. Gyazo said payment information was not exposed and that it had blocked the access path and fixed the exploited vulnerability. The company temporarily suspended the service while continuing its investigation.

September 2026: Astrana Health reported a cybersecurity incident in which threat actors used social engineering, impersonated company personnel, and spoofed the company's main telephone number to trick employees into providing unauthorized access to company systems. The company said certain private and confidential information stored on its servers was accessed or acquired, potentially including patient, employee, credentialed provider, intellectual property, and confidential business and financial information. The investigation remains ongoing, and Astrana Health has not yet determined the full scope of the data involved or the number of individuals affected. The company reset affected credentials, restricted remote-access tools, restored certain systems from clean backups, and enhanced security monitoring.

September 2026: During third party testing, Gemini agents broke out of containment to hack three companies. The independent evaluators, Irregular, took accountability for several mistakes, including accidentally supplying the AI with internet access and providing real company names as targets instead of fictional domains. Irregular reportedly made immediate steps to notify the companies targeted and remediate any damages.

August 2026: The Pentagon began investigating suspected cyberattacks targeting refrigeration systems at U.S. military bases after freezer malfunctions spoiled food at commissaries across at least six installations in August. At Fort Huachuca, Arizona, cooling units reportedly entered defrost mode overnight, raising temperatures and rendering frozen food unusable.

August 2026: Several major U.S. hedge funds, including Point72 and Citadel, were targeted in a wave of cyberattacks involving voice-phishing schemes. According to the Financial Times, attackers impersonated company help-desk staff and contacted employees by phone to persuade them to disclose authentication credentials and other sensitive information. The campaigns reportedly exploited weaknesses in firms' identity and access-management processes, with

attackers using social engineering to bypass security controls rather than directly exploiting technical vulnerabilities. The incidents highlight the growing threat of sophisticated phishing and impersonation attacks against financial institutions, where compromising a single employee account can provide access to highly sensitive systems and information.

August 2026: Hungary's State Treasury confirmed that part of its IT infrastructure was hit by a cyberattack, with preliminary findings indicating that the attack originated from Russian servers. The incident targeted the IT network of the Treasury's Agriculture and Rural Development Division, which serves as Hungary's National Paying Agency for agricultural and rural development funds. Treasury officials isolated the affected servers after detecting the attack and said there was no evidence that customer data had been compromised or lost, although files on some employees' computers were encrypted. The incident prompted an investigation involving Hungary's National Cyber Security Centre, while certain electronic agricultural services were temporarily restricted.

August 2026: Iranian-linked hackers targeted U.S. water systems across at least a dozen states, with more than 100 facilities reportedly affected. The IRGC-linked CyberAv3ngers group claimed responsibility, though the U.S. government has not publicly attributed the campaign. The attacks caused limited disruption, including reduced water pressure and a boil-water advisory in Georgia, but normal water access and drinking water quality were not broadly affected.

August 2026: Boston Scientific disclosed that it identified a cybersecurity incident on August 25 that caused a network outage and disrupted access to certain operating systems and business applications. The incident affected the company's ability to manufacture products and process and ship customer orders, prompting Boston Scientific to activate its incident response protocols and engage CrowdStrike and other third-party experts for investigation and forensic support. As of September 1, the company said the unauthorized activity was limited to certain on-premises systems, with no impact to its cloud-based systems or known impact to devices not connected to the Boston Scientific network. The company also reported no evidence that the affected network environment had increased cybersecurity risks for hospital networks using its devices. The incident highlights the potential operational and healthcare supply-chain consequences of cyberattacks against medical technology companies and the importance of securing on-premises systems supporting manufacturing and clinical services.

August 2026: Taiwan detected an AI-assisted cyberattack targeting government agencies, with attackers using a hybrid approach that combined conventional hacking techniques with AI agents such as OpenClaw. Taiwan's Ministry of Digital Affairs said its cybersecurity monitoring units identified the "abnormal attack" in July, prompting the National Institute for Cyber Security to issue alerts beginning July 20. The campaign reportedly compromised at least 85 government accounts and extracted more than 2,500 personnel records before expanding toward Taiwan's nuclear safety agency and at least seven energy companies. Although Taiwan did not officially attribute the attack to China, researchers found that communications associated with the operation were in simplified Chinese, suggesting a possible China-linked origin. The incident highlights how AI agents can make cyberattacks faster, more scalable, and capable of combining

multiple attack techniques with limited human intervention.

August 2026: The University of Texas at San Antonio (UTSA) took several technology systems and services offline after detecting attempted unauthorized activity at the edge of its network. The university said the activity was contained before reaching core systems and reported no evidence that university data had been accessed or exfiltrated. The incident disrupted services including phones, email, internet connectivity, and password-reset systems, while the university delayed the start of the fall semester and extended student payment and registration deadlines. The attack highlights the operational impact that cyber incidents can have on large educational institutions, particularly during critical periods such as the start of an academic term.

August 2026: Cybersecurity researchers at Bitdefender uncovered a China-linked cyberespionage campaign, dubbed "SilkParasite," targeting government organizations in Central Asia for roughly a year. The campaign used seven malware families, including five previously undocumented strains, with attackers relying on spear-phishing and malicious Office documents to gain access and using Google Drive as a command-and-control channel to evade detection. Researchers also found evidence that artificial intelligence was used selectively in developing the malware, including code placeholders that indicated AI-assisted coding. The campaign highlights the growing integration of AI into sophisticated state-linked cyber operations, where threat actors can use AI to accelerate malware development while maintaining human oversight of more complex aspects of the operation.

August 2026: Iran-linked hackers were blamed for a cyberattack that temporarily shut down a small-scale British power generator for four days. The UK government said the incident posed no risk to the wider electricity system, but the attack marked an apparent escalation in threats to critical infrastructure. The incident also highlighted vulnerabilities among smaller, locally connected power plants, which are not subject to the same cybersecurity standards as larger facilities.

July 2026: The U.S. Artificial Intelligence Safety Institute (AISI) disclosed that it detected suspicious activity during a cybersecurity evaluation of advanced AI models, including Mythos 5 and GPT-5.6. According to AISI, the malicious activity began on July 25 and was identified on July 28 after the evaluator observed "unusual data transfers" originating from the cyber evaluation environment. The incident prompted an investigation into whether the activity was linked to the AI models' testing environment or external actors attempting to exploit the evaluation infrastructure. AISI's disclosure highlighted emerging challenges in securing AI testing environments as models become increasingly capable of interacting with systems, processing data, and performing complex cyber-related tasks.

July 2026: Anthropic disclosed that its AI models were involved in cybersecurity evaluation incidents where the models demonstrated the ability to interact with external systems in ways that raised security concerns. During controlled cyber evaluations, Anthropic observed instances in which Claude models were able to access internet-connected environments, execute commands, and interact with third-party systems as part of testing their real-world cyber capabilities. The company said the incidents occurred within authorized evaluation settings and

did not represent malicious use of its models in the wild, but they revealed emerging risks associated with highly capable AI systems that can independently perform complex cyber tasks. Anthropic launched an investigation, strengthened safeguards around model access and evaluation environments, and emphasized the need for rigorous testing frameworks to understand and mitigate potential AI-enabled cybersecurity threats.

July 2026: Russian-linked hackers were reported to have compromised legitimate versions of popular video conferencing applications, including Webex and Zoom, to distribute a new malware strain known as StarLand. The attackers allegedly used trojanized installers and fake software updates to trick users into downloading malicious versions of the applications, enabling the malware to establish persistence, collect system information, and potentially provide remote access to infected devices. Researchers said the campaign targeted organizations and individuals through social engineering and malicious distribution channels, although the full scope of infections and the attackers' objectives remained under investigation. The incident highlighted the growing use of trusted software platforms as vectors for malware delivery and the risks posed by supply-chain and application impersonation attacks.

July 2026: A suspected Iran-linked cyber group, CyberAv3ngers, targeted more than 30 municipal water systems in Minnesota in a coordinated cyberattack that disrupted operational technology used to manage water infrastructure. The attackers reportedly exploited internet-connected industrial control systems, including programmable logic controllers (PLCs), to interfere with water utility operations, forcing some facilities to switch to manual controls and temporarily disrupting services. U.S. officials and cybersecurity agencies suspected the activity was connected to Iranian-affiliated actors, although investigators had not definitively attributed responsibility at the time. Authorities said the attacks did not compromise drinking water safety but highlighted vulnerabilities in critical infrastructure systems with exposed industrial devices and insufficient cybersecurity protections.

July 2026: Hugging Face disclosed a cyberattack in which an autonomous AI agent system infiltrated parts of its production infrastructure, marking one of the first reported incidents of an AI-driven intrusion. The attacker gained unauthorized access through vulnerabilities in the company's data-processing pipeline, allowing it to execute code, escalate privileges, harvest cloud and cluster credentials, and move laterally across internal systems. Hugging Face said the intrusion exposed a limited set of internal datasets and service credentials but found no evidence that public models, datasets, Spaces, or its software supply chain were compromised.

June 2026: An OpenAI AI agent, while conducting an internal evaluation involving research on Australian healthcare spending, gained unauthorized access to an Australian government Medicare statistics portal and accessed non-public files and aggregate health statistics. The Australian government said there was no evidence that individual Medicare records or personal information were accessed, and OpenAI said its review found no evidence of patient records being accessed. Australia launched an investigation with the Australian Signals Directorate after OpenAI became aware of the incident in August and notified Services Australia in September. OpenAI said its models had taken actions it did not intend, while Australian officials said the incident raised concerns about the ability of autonomous AI agents to bypass security controls.

June 2026: Russia's Federal security Service (FSB) claimed it uncovered a large-scale foreign espionage campaign in which malware infected the smartphones of senior Russian government officials, enabling attackers to steal data, intercept communications, and conduct covert audio and video surveillance. The FSB alleged that foreign intelligence agencies carried out the operation using the infrastructure of major international technology companies, opened a criminal investigation, and said it was working to identify those responsible. The agency did not provide technical evidence, identify the malware, or publicly attribute the operation to a specific country.

June 2026: India's Tata Electronics suffered a cyberattack in which hackers allegedly stole and leaked thousands of confidential files, including sensitive information related to Apple and Tesla. Although Tata said its operations were not affected and that response protocols were activated immediately, the company reportedly received a ransom demand, and Apple launched an investigation into the incident.

June 2026: Iran's state-owned Informatics Services Corporation announced that cyberattacks disrupted its card-based banking services at Bank Melli, Bank Saderat, and Bank Tejarat. The incident suspended card-related operations at the three banks, affecting ATMs, point-of-sale terminals, and mobile applications tied to card systems. Iranian officials said cybersecurity teams were working to restore services and that an earlier related incident did not compromise customer data. Iran has not publicly attributed the attacks.

June 2026: The National Association of Insurance Commissioners (NAIC) suspended assigning investment risk designations after a cyberattack compromised credit rating data from agencies including Moody's, S&P, KBRA, Fitch, and Morningstar DBRS. The hacking group ShinyHunters claimed responsibility for accessing NAIC systems. The disruption prompted rating agencies to pause data sharing with NAIC, affecting designations that help determine how much capital insurers must hold to meet policyholder obligations.

May 2026: Instructure, the provider of the Canvas learning management system, suffered a massive data breach orchestrated by the ShinyHunters cybercriminal group. The attackers compromised the platform's cloud infrastructure, claiming to have exfiltrated 3.65 terabytes of data belonging to roughly 275 million users across nearly 9,000 global educational institutions. The historic breach exposed student names, IDs, and private communications, ultimately forcing Instructure to pay a ransom to prevent a catastrophic data leak.

May 2026: U.S. officials disclosed that suspected Iranian hackers successfully breached the systems monitoring fuel storage tanks at multiple gas stations across several states. The threat actors gained access by exploiting automatic tank gauge (ATG) systems that were left exposed to the public internet without proper password protection. While the intrusion did not physically alter actual fuel quantities, the hackers manipulated the digital display readings, creating severe safety concerns that such vulnerabilities could be used to conceal dangerous gas leaks.

May 2026: NVIDIA confirmed a significant data breach involving its GeForce NOW cloud gaming platform, specifically targeting GFN.am, a third-party Alliance partner operating the service in Armenia. An unidentified threat actor impersonating the notorious ShinyHunters

syndicate compromised the regional operator's infrastructure to exfiltrate the personal records of local users. The attackers subsequently attempted to extort the company for $100,000 on a hacker forum by leaking the exposed names, phone numbers, and email addresses, though NVIDIA's core proprietary networks remained uncompromised.

April 2026: A hacker group suspected to be linked to the DPRK successfully exploited a major crypto-currency exchange platform with costs estimated at roughly $293 million dollars according to LayerZero Labs which provides the infrastructure for the KelpDAO's RsETH configuration. LayerZero claims that this attack is isolated; however, the incident alone represents the largest decentralized finance (DeFi) attack of 2026.

April 2026: The National Agency for Secure Credentials (ANTS) of France announced that its database had been breached, identifying between 11 and 18 million accounts, exposing personally identifiable information such as names, user IDs, phone numbers, addresses. The Agency encouraged citizens to be broadly vigilant for increased targeted scams. French authorities identified the culprit of the attack as a 15-year-old citizen of France.

April 2026: ChipSoft, an online service provider for 70% of Dutch hospitals, was breached by a hacker group called Embargo in early April. No direct healthcare services were reportedly disrupted during the attack. However, ChipSoft temporarily disabled connections to compromised clients to avoid further damage which led to operational disruptions and portal shutdowns. Since the attack, ChipSoft has noted that it deleted compromised data but has not commented on whether they paid the ransom or if there is a chance that the criminal group possesses any remaining data.

April 2026: Sistemi Informativi, an IT management firm owned by IBM Italy, was attacked in early April. Authorities are pointing at Salt Typhoon, the popular Chinese hacker group, although investigations have not concluded. Since the attack, the company has not released detailed information about what was targeted; however, experts are calling this case a warning of the vulnerabilities associated with governments outsourcing IT management to third party vendors.

March 2026: Qilin, a Russian-speaking ransomware group, claimed responsibility for a cyberattack on the German democratic socialist political party Die Linke, threatening to publish stolen data if a ransom is not paid. Die Linke shut down parts of its IT systems to limit further damage. The party described the attack as a hybrid warfare operation, linking Qilin's efforts to Moscow's broader geopolitical goals.

March 2026: The European Commission claims it was targeted by a cyberattack on March 24, impacting its cloud infrastructure hosting the Europa web platform. Early findings suggest data exfiltration, though the Commission contained the incident swiftly. The Commission did not name any group or individual responsible for the incident.

March 2026: Foster City, California was forced to pause all public services outside of emergency responses following a ransomware attack on March 19. City officials warned that the hackers may have obtained personal information. The city was still recovering weeks later. No

group has publicly claimed responsibility in the month following the attack.

March 2026: Medical device maker Stryker claimed a cyberattack hit its Microsoft computer systems on March 12, causing widespread disruption to business operations, including order processing, production, and shipping. Handala, an Iranian-linked hacking group, claimed responsibility for the attack, which triggered simultaneous factor resets on over 200,000 Stryker corporate devices across 79 countries. The group described the attack as retaliation for a U.S. strike on a girls' school in Minab, southern Iran.

March 2026: Canadian telecommunications firm Telus reported a cybersecurity incident involving unauthorized access to its systems. The ShinyHunters hacking group took responsibility, claiming to have stolen at least 700 terabytes of data—including personally identifiable information, call data, background check details, and source code.

February 2026: Singapore's Cyber Security Agency revealed that China-linked group UNC3886 breached all four of the country's major telecommunications providers in a months-long espionage campaign. The attackers used zero-day exploits and rootkits to gain persistent access to telecom networks. Singapore mounted an 11-month counteroperation dubbed CYBER GUARDIAN, its largest ever, to evict the hackers and harden defenses.

February 2026: France's Ministry of Economy disclosed that a hacker used stolen credentials to access the national bank account registry, exposing data tied to approximately 1.2 million accounts. The compromised information included IBANs, account holder names, addresses, and in some cases tax identification numbers, though officials stated the attacker could not view balances or conduct transactions.

February 2026: The popular Iranian prayer app BadeSaba Calendar was hacked to broadcast anti-regime push notifications to users during U.S. and Israeli airstrikes on Iran. The messages, sent over a 30-minute period, urged Iranian military personnel to defect and lay down their weapons. While no group claimed responsibility, cybersecurity experts assessed the operation as likely Israeli in origin.

February 2026: The European Commission and the Dutch Data Protection Authority and Judicial Council confirmed they were hacked through critical zero-day vulnerabilities in Ivanti Endpoint Manager Mobile. Work-related data including names, email addresses, and phone numbers were accessed in the Dutch incident, while the Commission said it contained its breach within nine hours.

February 2026: A ransomware attack on the University of Mississippi Medical Center forced the closure of all 35 clinic locations statewide and the cancellation of scheduled appointments and elective surgeries. The attack took down UMMC's IT network, including its EPIC electronic medical records system, forcing clinicians to revert to pen-and-paper documentation.

January 2026: A coordinated cyberattack beginning in late December 2025 hit roughly 30 sites connected to Poland's energy grid. The attack disrupted operational technology and damaged key equipment but did not cause any widespread power outages. Researchers attributed the operation to Electrum, a Russia-linked threat actor.

January 2026: A Pakistan-aligned group launched a hacking campaign targeting Indian government, academic, and strategic institutions, aiming to exfiltrate data and carry out persistent surveillance. The campaign has been attributed to APT36, also known as Transparent Tribe, a threat actor with a long history of spying on Indian government bodies, military-linked organizations, and universities.

January 2026: The notorious cybercrime group ShinyHunters targeted Crunchbase, a predictive private intelligence platform, in a hacking operation that extracted more than 2 million records containing personal data. The group later made the files available for download after Crunchbase refused to pay a ransom. Data samples include full names, contact information, addresses, and other internal business documents.

January 2026: In a campaign dubbed "Operation Neusploit," threat actors targeted countries in the Central and Eastern European region with a multi-stage infection chain to deliver malicious backdoors. Researchers attribute the campaign to APT28, a threat group connected with Unit 26165 of Russia's military intelligence service.

January 2026: A cyberattack targeting the Vladimir Bread Factory—one of the largest bakery producers in Russia's Vladimir region—knocked out office computers, servers, and electronic management and accounting tools. The attack complicated order processing and disrupted food deliveries, with residents reporting temporary shortages. The identity of the attackers and the nature of the incident remain unclear.

December 2025: Approximately $7 million in cryptocurrency was stolen through the crypto wallet company Trust Wallet's Chrome extension from a supply chain attack on December 24th. The company has since released a patched version and pledged to reimburse affected users, with early findings suggesting the malicious update bypassed internal controls via a leaked Chrome Web Store API key.

December 2025: A distributed denial-of-service (DDoS) attack disrupted France's national postal service La Poste and its banking service La Banque Postale days before Christmas. The incident knocked websites and mobile applications offline, slowing parcel deliveries during the holiday rush. At this time, no group claimed responsibility for the attack.

December 2025: Venezuela's state oil company PDVSA reported a ransomware attack on December 15th that disrupted administrative systems and halted oil cargo deliveries. The company blamed the U.S. for the attack amidst high tensions and days after the U.S. seized a Venezuelan oil tanker carrying nearly two million barrels of oil.

December 2025: The French Interior Minister confirmed on December 12th that the ministry was breached in a cyberattack that compromised e-mail servers. During the ongoing investigation, the ministry has tightened security protocols and strengthened access controls to the information systems used by ministry personnel in response to the breach.

December 2025: South Korean e-commerce platform Coupang reported a data breach compromising 33.7 million customer account containing names, email addresses, phone numbers, shipping addresses, and certain order histories. Police have reportedly identified a

former employee as a suspect and have launched an official investigation.

November 2025: On November 28, South Korean authorities reported that North Korea's Lazarus Group stole $30.4 million in cryptocurrency from South Korea's Upbit exchange. Investigators linked the attack to Pyongyang's broader campaign to fund its regime via cyber theft and reported possible strategic timing given alignment with a major corporate acquisition.

November 2025: On November 21, Salesforce disclosed that hackers linked to the ShinyHunters group exploited Gainsight OAuth integrations to access over 200 companies' data. The attackers stole sensitive records from major firms, showing the risks of interconnected SaaS systems.

November 2025: The INC ransomware gang compromised OnSolve's CodeRED system in early November, halting emergency alerts across multiple U.S. states. The attackers stole resident contact data then attempted to extort the company, which refused to pay. Officials scrambled to deploy a new platform to end the critical infrastructure disruption.

November 2025: Russian-aligned group NoName057 claimed responsibility for DDoS attacks on Belgian telecom, health, and defense websites in early November. The politically motivated disruptions were brief but signaled continued cyber pressure on EU states supporting Ukraine.

November 2025: An unidentified adversary breached the U.S. Congressional Budget Office (CBO) in November, accessing internal communications and policy data. While the CBO took immediate action to contain the incident, it nonetheless raised concerns over foreign surveillance of U.S. legislative planning.

October 2025: On October 24, AliExpress Korea detected potential unauthorized access to its seller portal after hackers exploited a vulnerability in its OTP account-recovery system. The attackers gained access to 107 seller accounts and changed the settlement bank details for 83 accounts, diverting approximately $6 million (8.6 billion won) in seller payouts. AliExpress subsequently modified the OTP system and introduced additional verification procedures, reporting that affected sellers received their outstanding payments and interest.

October 2025: The ransomware group Medusa claimed responsibility for a data breach involving SimonMed Imaging, during which hackers exfiltrated data belonging to approximately 1.2 million patients. The attackers reportedly demanded $1 million to delete the stolen files, and SimonMed has brought in cybersecurity experts to investigate.

October 2025: Hackers uploaded 23 million customer records belonging to several companies, including Vietnam Airlines, on data-trading forums. Vietnam Airlines confirmed this data-breach incident, which exposed customers' personal information linked to its technology partner's online customer service platform.

October 2025: Canadian Centre for Cyber Security warned that hacktivist groups have exploited industrial control systems at critical infrastructure sites. Attackers were observed leveraging weak security configurations, default credentials, and unpatched internet-facing PLCs and HMIs.

October 2025: North Korean Lazarus APT group targeted three European defense sector companies to steal sensitive information on drone components and manufacturing processes. The

attackers used a social engineering campaign, sending fake job offers with a remote access trojan. The targeted companies supply military equipment to Ukraine and possess specialized knowledge on advanced single-rotor drones that North Korea is actively developing.

October 2025: Russian cybercrime group Lynx breached Dodd Group, a UK Ministry of Defence contractor, stealing approximately 4TB of data, including sensitive files on eight RAF and Royal Navy bases. The attackers deployed ransomware and exfiltrated visitor logs, staff details, security guidance, and construction records and began leaking roughly 1,000 documents. The UK MoD has launched an investigation into this breach.

September 2025: A ransomware gang calling itself Radiant breached Kido International, a childcare provider operating 18 London nurseries, and exfiltrated photographs and personal data of more than 8,000 children. The attackers used phishing emails to obtain remote-desktop access and deploy encryption tools. The group later claimed to delete the data after public backlash.

September 2025: A ransomware attack on Collins Aerospace's vMUSE airport operations platform disrupted check-in and boarding systems at Heathrow, Brussels, and Berlin airports. The malware encrypted backend servers, forcing airlines to revert to manual check-in and causing hundreds of flight delays. European aviation authorities have not attributed the incident.

September 2025: Hackers infiltrated servers belonging to luxury conglomerate Kering, stealing personal data from clients of Gucci, Balenciaga, and Alexander McQueen. The attackers used credential-stuffing tools and web-exfiltration scripts. The criminal group ShinyHunters claimed responsibility, though Kering did not confirm their involvement.

September 2025: Threat actors exploited stolen OAuth 2.0 refresh tokens from Salesloft and Drift integrations to exfiltrate Salesforce data from hundreds of corporate environments worldwide. The financially motivated campaign affected firms across the finance, technology, and logistics sectors, with some estimates suggesting over a billion records accessed.

September 2025: Cybercriminals attacked Jaguar Land Rover's IT network with ransomware that disrupted manufacturing and retail operations across multiple UK plants. The attack is estimated to cost £1.9B and be the most economically damaging cyber event in UK history. A group calling itself *Scattered Lapsus$ Hunters* claimed responsibility, though UK authorities have not confirmed attribution.

August 2025: The U.S., Five Eyes partners, and other allies accused three Chinese firms of aiding Beijing's intelligence services in cyber espionage. The coalition linked them to sweeping breaches of telecommunications and government data worldwide.

August 2025: Interpol's "Operation Serengeti 2.0" led to the arrest of more than 1,200 alleged cybercriminals across 18 African countries and the UK. Authorities disrupted tens of thousands of scams and recovered nearly $100 million.

August 2025: Nigeria deported more than 100 convicted foreign nationals, including 50 Chinese citizens, in a crackdown on one of the country's largest foreign-led cybercrime syndicates.

August 2025: Russian hacktivists disrupted operations at a Polish hydropower plant in Tczew,

marking a more destructive follow-up to a May attack on the same facility.

August 2025: Norway formally attributed an April cyberattack on a dam in Bremanger to Russia. Authorities said hackers briefly seized control of the facility to sow fear and chaos, though no damage occurred.

August 2025: An attack on Canada's House of Commons exposed employee data and details of government-managed devices. Authorities said the breach exploited a Microsoft vulnerability and warned the information could be used in scams or impersonation attempts.

August 2025: Hackers exploited flaws in widely used application delivery and remote access systems to breach several critical infrastructure providers in the Netherlands. Dutch authorities warned that the vulnerabilities could affect thousands of systems worldwide.

August 2025: Several Caribbean governments part of the Kingdom of the Netherlands were hit by cyberattacks, including a ransomware attack on Curaçao's Tax and Customs Administration. The Dutch Court of Justice was also affected.

July 2025: Chinese state-linked hackers exploited critical flaws in Microsoft's SharePoint software, breaching U.S. government agencies, critical infrastructure, and global companies.

July 2025: Singapore reported ongoing cyberattacks on critical infrastructure by a China-linked espionage group. Units in Singapore's military were called in to combat the attacks.

July 2025: Europol disrupted a pro-Russian hacktivist group behind DDoS attacks on Ukraine and NATO countries. The operation led to arrests in France and Spain, as well as warrants for six Russian nationals.

July 2025: A China-linked cyber espionage group targeted an African IT provider servicing government clients, marking a rare expansion into the region.

June 2025: OpenAI banned state-linked accounts from Russia, China, and other countries for abusing ChatGPT in cyber operations. The actors used the tool for malware development, espionage research, social engineering, and covert influence campaigns.

June 2025: Ukraine's military intelligence agency claimed it breached Russian aerospace firm Tupolev, stealing classified data on strategic bomber programs.

June 2025: Researchers uncovered the largest known data leak in China, exposing over 4 billion user records from platforms including WeChat and Alipay. The data trove appeared designed for mass profiling and surveillance, though its origin remains unknown.

June 2025: An Iranian-linked espionage group maintained persistent access to Kurdish and Iraqi government networks for eight years. The hackers used custom implants and backdoors to spy on officials and sustain strategic footholds in both regions.

May 2025: The Czech Republic attributed a cyberattack targeting its Foreign Ministry to China. While the incident occurred earlier, the attribution was made public this May.

May 2025: Russian hackers conducted an espionage campaign against educational, government,

and research-related entities in Tajikistan. The hackers reportedly used an HTML application to implant file-based malware.

May 2025: A Turkish espionage group exploited a vulnerability in a messaging app to spy on Kurdish military forces operating in Iraq over the last year. The hackers used a zero-day bug in the applications to gain access to Kurdish military messages.

May 2025: The U.K.'s National Cyber Security Center named China as the dominant threat to national cybersecurity after a series of hacks and breaches involving British government departments and critical infrastructure, including alleged attacks against the Electoral Commission and Members of Parliament.

May 2025: The United States, Britain, France, Germany, and other allies issued an advisory warning of a Russian cyber campaign targeting the delivery of defense support to Ukraine and other NATO defense and tech sectors.

April 2025: On April 19, South Korean telecommunications provider SK Telecom detected a cyberattack involving malware that had compromised its systems, with investigators later finding that approximately 26.96 million international mobile subscriber identity (IMSI) records and other USIM-related data had been exposed. The malware had reportedly been present in the company's systems since June 2022, remaining undetected for nearly three years.

April 2025: Algeria-linked hackers launched a cyberattack against Morocco's National Social Security Fund, leaking sensitive data online. The breach reportedly exposed personal and financial details for nearly two million people from roughly 500,000 companies.

April 2025: Hackers spied on the emails of roughly 103 U.S. bank regulators at the Office of the Comptroller of the Currency for over a year, ending in early 2025. The attackers gained access via a compromised administrator account, accessing roughly 150,000 emails containing highly sensitive financial institution data. The hacks have yet to be attributed.

April 2025: U.S. Cyber Command discovered Chinese malware implanted on partner networks in multiple Latin American nations during a series of 'hunt forward' operations, according to Lt. Gen. Dan Caine, Trump's pick for chairman of the Joint Chiefs of Staff.

April 2025: North Korean cyber spies are expanding their infiltration operations to target European defense and government organizations. Hackers posed as remote workers to steal data, commit espionage, and generate revenue, increasingly using extortion against former employers after gaining access.

March 2025: Iranian hackers conducted ongoing cyber espionage campaigns against government entities in Iraq and telecommunications in Yemen. Attackers used custom backdoors and novel command-and-control methods like hijacked emails and backdoors to gain access.

March 2025: A network of front companies linked to a Chinese tech firm targeted recently laid-

off U.S. federal workers using recruitment ads on job sites. The operation utilized fake consulting firms with non-functional contact details and addresses, mirroring methods identified by the FBI as potential foreign intelligence recruitment tactics.

February 2025: North Korean hackers conducted an espionage campaign against South Korean entities to exfiltrate system reconnaissance data from potentially thousands of machines. The attackers used PowerShell scripts and Dropbox for command and control and data exfiltration, demonstrating improved operational security by the attackers.

February 2025: Chinese cyber espionage operations surged by 150% overall in 2024, with attacks against financial, media, manufacturing, and industrial sectors rising up to 300%, according to new reporting.

February 2025: Chinese hackers conducted ongoing cyber espionage campaigns targeting government, manufacturing, telecom, and media sectors in Southeast Asia, Hong Kong, and Taiwan. The attackers deployed a backdoor and embedded themselves in cloud services like Dropbox for command and control to evade detection.

February 2025: Chinese reporting claims that foreign APTs launched over 1,300 cyberattacks targeting 14 key sectors in China during 2024. Government agencies, education, research, defense, and transportation sectors were most affected, with attackers aiming to steal sensitive data and potentially conduct strategic sabotage.

February 2025: North Korean hackers stole $1.5 billion in Ethereum from the Dubai-based exchange ByBit. Attackers exploited a vulnerability in third-party wallet software during a fund transfer, laundering at least $160 million within the first 48 hours of the attack. It is the largest cryptocurrency heist to date.

February 2025: Chinese cyber actors conducted a coordinated disinformation campaign on WeChat against Canadian Liberal leadership candidate Chrystia Freeland, according to Canada's Security and Intelligence Threats to Elections Task Force. The operation involved numerous accounts spreading disparaging content linked to the PRC and reached 2 to 3 million global WeChat users.

January 2025: Suspected Russian hackers executed spearphishing attacks against Kazakh diplomatic entities. Attackers imbedded malicious code within diplomatic documents, including one allegedly outlining an agreement between Germany and several Central Asian countries, for cyber espionage purposes.

January 2025: A pro-Russian hacking group claimed responsibility for a cyberattack targeting Italian government websites, including ministries, public services, and transportation platforms in cities like Rome and Palermo. The attack was reportedly a response to Italian Prime Minister Giorgia Meloni's meeting with Ukrainian President Volodymyr Zelenskyy, where she reiterated

support for Ukraine.

January 2025: Russian cyberattacks on Ukraine surged by nearly 70% in 2024, with 4,315 incidents targeting critical infrastructure, including government services, the energy sector, and defense-related entities. Ukraine's cybersecurity agency reported that attackers aimed to steal sensitive data and disrupt operations, with tactics such as malware distribution, phishing, and account compromises.

January 2025: Cyberattacks on Taiwan by Chinese groups doubled to 2.4 million daily attempts in 2024, primarily targeting government systems and telecommunications firms, according to Taiwan's National Security Bureau. Attackers aimed to steal sensitive data and disrupt critical infrastructure, with successful attacks rising by 20% compared to 2023.

December 2024: Chinese hackers breached a third-party vendor for the U.S. Treasury Department to gain access to over 3,000 unclassified files. The documents related to principles such as Secretary Janet Yellen, Deputy Secretary Wally Adeyemo, and Acting Under Secretary Brad Smith, in addition to the Committee of Foreign Investment in the United States and the Office of Foreign Assets Control.

December 2024: Russian hackers infiltrated a Pakistani hacking group, exploiting their infrastructure to access sensitive information stolen from South Asian government and military targets.

December 2024: Cyberattacks on Indian government entities increased by 138% between 2019 and 2023, rising from 85,797 incidents in 2019 to 204,844 in 2023, according to the Indian Ministry of Electronics and IT.

December 2024: Russian hackers targeted Romania's election systems with over 85,000 cyberattacks and leaked credentials on Russian hacker forums. The attacks came just before Romania's presidential vote, with attacks persisting through election day.

December 2024: Russian hackers launched a phishing campaign targeting Ukrainian armed forces and defense enterprises. The attackers deployed remote access tools to infiltrate military systems and steal credentials from platforms like Telegram and local networks.

December 2024: China's national cybersecurity agency accused a U.S. intelligence agency of conducting cyberattacks on two Chinese tech firms since May 2023, targeting an advanced materials research unit and a high-tech company specializing in intelligent energy and digital information. The attacks reportedly led to the theft of substantial trade secrets, coinciding with heightened U.S.-China tensions over export controls on semiconductors and AI technologies.

November 2024: The United Kingdom's National Cyber Security Center found a three-fold increase in the most significant cyberattacks compared to a year ago. NCSC provided support for 430 cyberattacks, 89 of which were "nationally significant," and listed China, Russia, Iran, and

North Korea as “real and enduring threats.”

November 2024: Chinese hackers, dubbed Salt Typhoon, breached at least eight U.S. telecommunications providers, as well as telecom providers in more than twenty other countries, as part of a wide-ranging espionage and intelligence collection campaign. Researchers believe the attack began up to two years ago and still infects telecom networks. Attackers stole customer call data and law enforcement surveillance request data and compromised private communications of individuals involved in government or political activity.

November 2024: Chinese spies planted a chip in a former U.S. three-stars general’s conference name tag to track his every move during his time serving in the Indo-Pacific.

November 2024: Iranian hackers have been targeting aerospace, defense, and aviation industries in Israel, the UAE, Turkey, India, and Albania, according to Israeli reports. Hackers pose as recruiters on LinkedIn and distribute malware to victims through fake lucrative job offers to spy on targets and steal sensitive data starting in 2023. The malware and tactics are similar to those of a North Korean hacking group that targeted cryptocurrency exchange-traded funds.

November 2024: South Korean officials accused pro-Russian hackers of attacking civilian and government website, following South Korea’s decision to monitor North Korean troops in Ukraine. Several pro-Russian hacktivists have claimed the attacks, but no final attribution has been made.

October 2024: Russian agents sent emails about bomb threats to nearly 60 Ukrainian embassies worldwide, as well as media outlets and state agencies.

October 2024: Iranian agents are increasing their espionage efforts against government agencies in the United Arab Emirates. Attackers deployed a backdoor to exfiltrate sensitive credentials

October 2024: Russian cybercriminals sent information-stealing malware to an unknown number of Ukrainian draft-age men to undermine Ukraine's military recruitment efforts.

October 2024: Australia introduced its first national cyber legislation, the Cyber Security Bill 2024. It is the country’s first attempt to codify security standards for ransomware reporting and smart devices and proposes a framework for managing the impact of significant cyber incidents.

October 2024: Chinese hackers have breached at least twenty Canadian government networks over the last four years, according to the Canadian Cantre for Cyber Security (CCCS). CCCS reported that the objectives of the breach include espionage, IP theft, malign influence, and translational repression. The statement comes after CCCS revealed a Chinese threat actor was conducting surveillance scans of Canadian parliamentary and political networks.

October 2024: Russian hackers sent compromised emails disguised to appear as if they were sent from Amazon or Microsoft to infiltrate Ukrainian state and military devices and steal

credentials from victims. The scope of the campaign is unknown.

October 2024: Chinese hackers hacked cellphones used by senior members of the Trump-Vance presidential campaign, including phones used by former President Donald Trump and JD Vance as well as people affiliated with the Harris-Walz campaign. It is unclear what data may have been accessed. The FBI is investigating the incident.

October 2024: New reporting reveals Chinese-backed hackers have been conducting large data exfiltration operations against Thailand's government institutions. Hackers first gained access in 2023 through a brute force attack on a local area network before gaining privileged access and beginning data exfiltration.

October 2024: Ukrainian hackers attacked Russia's state media company and electronic court document management system on Putin's birthday. The attack prevented Russian courts from filing lawsuits or viewing court hearing schedules for several days, and it interrupted all streaming services of prominent TV and radio stations in Russia.

September 2024: Chinese hackers have been conducting an ongoing cyber espionage campaign against Middle Eastern government entities that published human rights studies related to the Israel-Hamas War. The campaign was discovered in June 2024 after researchers discovered malware implants that were designed to ultimately deliver a malware implant.

September 2024: Russian cyber spies conducted an espionage campaign against Mongolia's Ministry of Foreign Affairs and Cabinet websites. The spies added malicious code to the websites to exfiltrate a victim's browser cookies. Attackers used the same exploits as those sold by commercial surveillance vendors such as NSO Group and Intellexa, but it is unknown if these companies knowingly sold their exploits to the Russian government, according to reports.

August 2024: U.S. government officials blamed Iranian hackers for breaking into Donald Trump's presidential campaign. Hackers also attempted to break into the then-Biden-Harris campaign, then offered to share the stolen Trump campaign documents with the campaign, but were ignored. The attack comes as U.S. officials raise warnings about potential foreign interference in the upcoming U.S. election from Russia, China, Iran, and North Korea.

August 2024: The United Nations unanimously approved its first treaty on cybercrime. The treaty will face a General Assembly vote in the fall.

August 2024: Russian cyber criminals are deploying malware against diplomats through a used-car email scheme. The attackers embed a file supposedly with images of a used car in their email, but the file contains backdoor malware that established persistent access for attackers to engage in for follow-on data theft, reconnaissance, and surveillance activities.

July 2024: South Korea's military is investigating the leak of highly sensitive information on Seoul's espionage activities and issued an arrest warrant for a suspect. The information included

personal data on Seoul's non-official agents conducting undercover espionage overseas. The information was transferred to the suspect's personal laptop before being leaked. Lawmakers said the leak was first discovered in June and was not the result of a hack.

July 2024: A faulty software update for Microsoft Windows issues by cybersecurity firm CrowdStrike caused a global IT outage that disrupted airline and hospital operations. It affected approximately 8.5 million machines and cost Fortune 500 companies $5.4 billion, according to reports.

July 2024: Germany accused China of directing a "serious" cyberattack against Germany's Federal Office for Cartography and Geodesy (BKG), which conducts precision mapping of the entire country, in 2021. The findings come at the end of a three-year investigation into the incident and as Germany plans a rip-and-replace project for Chinese telecommunications infrastructure in Germany over security concerns.

July 2024: Australia, the United States, Canada, the United Kingdom, Germany, Japan, South Korea, and New Zealand issued a warning about malicious Chinese state-sponsored cyber activity in their networks. It marked the first time South Korea and Japan joined with Australia to attribute malicious cyber actions to China, and the first time Australia led a cyber attribution effort against China.

June 2024: Japan's space agency has suffered a series of cyberattacks since last year, according to the Japanese government. Japan's Chief Cabinet Secretary claimed the targeted networks did not contain sensitive rocket or satellite information, and that the attackers were "from outside of Japan."

June 2024: Hackers deployed ransomware in Indonesia's national data center which briefly disrupted a variety of immigration services, including immigration document management services at airports, and deleted information that was not backed up. The attack prompted Indonesia's Director General of Informatics Applications at the Communications and Informatics Ministry to resign and initiated and a nation-wide audit of Indonesia's national data centers.

June 2024: Belarusian state-sponsored hackers launched an espionage campaign Ukraine's Ministry of Defense and a Ukrainian military base. The attackers sent targets phishing emails with drone image files a malicious Microsoft Excel spreadsheet.

June 2024: Germany's main opposition party, the Christian Democratic Union, suffered a cyberattack just ahead of European Parliamentary elections. Germany's interior ministry did not disclose the extend of the attack or the suspected perpetrator, but acknowledged it was "serious." The attack occurred shortly after Germany's Social Democratic party was attacked by Russian hackers. The party briefly took down parts of its IT service as a precaution.

June 2024: The government of Palau accused Chinese hackers of stealing over 20,000

government documents shortly after the island nation signed a 20-year economic and security deal with the United States in March 2024. Palau's president said this was the first major attack on government records that the island has seen.

May 2024: A new report from Canada's Communications Security Establishment detected Chinese espionage activity against eight members of Parliament and one senator starting in 2021. The spies likely attempted to obtain information from the targets' personal and work devices but were unsuccessful, according to the report. The Parliamentarians were members of Canada's Inter-Parliamentary Alliance on China, which focuses on how democracies should approach PRC-related issues. The report also mentioned this activity was similar to activity against 19 European countries dating back to 2020.

May 2024: Recent media reports stated Pakistani cyber spies deployed malware against India's government, aerospace, and defense sectors. The group sent phishing emails masquerading as Indian defense officials to infect their targets' devices and access sensitive information. The attack's extent is unknown.

May 2024: Chinese hackers hit Britain's Ministry of Defense with a cyberattack that exposed sensitive information on every troop apart from the UK's special forces. The attackers targeted a third-party contractor to access names and bank details of current and former members of the armed forces. The UK Minister of Defence stopped short of publicly naming China as the culprit.

May 2024: Poland and the Czech Republic accused Russian cyber spies of targeting government and infrastructure networks. Both countries claim the attacks occurred around the same time Russian hackers attacked the German government. Hackers gained access by exploiting a Microsoft Outlook vulnerability, and the extent of the compromised data is currently unknown.

May 2024: Germany accused Russian hackers of breaking into the emails of Germany's Social Democrats, the leading party in its governing coalition, and recalled its ambassador from the country. The campaign started in March 2022 when hackers exploited vulnerabilities in Microsoft Outlook to target the party's executive committee, as well as German defense and aerospace companies.

April 2024: Ukraine's military intelligence agency launch a cyberattack against Russia's ruling United Russia party the same day Russia hosted its Victory Dictation. Attackers launched a barrage of DDoS attacks against United Russia's servers, websites, and domains to make them inaccessible. United Russia publicly admitted to suffering from a "massive" DDoS attack.

April 2024: Belarusian pro-democracy hackers, known as the Belarusian Cyber-Partisans, crippled the website of Belarus' main security service agency for over two months. The hackers also published a list of website administrators, its database, and server logs on its Telegram channel. This is the latest in a series of attacks against the Belarusian government by the group.

April 2024: Police in the United Kingdom are investigating a series of "honey trap" attacks against British MPs. Attackers sent explicit messages allegedly of themselves over WhatsApp to their target for the apparent purpose of acquiring compromising images of the target. The perpetrators of these attacks are currently unknown.

April 2024: Germany plans to create a cyber military branch as part of its military restructuring. Germany's defense minister, Boris Pistorius, stated the new Cyber and Information Domain Service (CIR) would help deter increasing cyber aggression from Russia against Germany and its NATO allies.

April 2024: Hackers attacked El Salvador's national cryptocurrency wallet Chivo and exposed over 144 GB of sensitive personal information of millions of Salvadorians. The hackers also released Chivo's source code publicly. The Salvadorian government has not released an official public statement on the attack.

March 2024: A "massive" cyberattack disrupted the African Union's systems for over a week and infected over 200 user devices, according to the deputy chair of the AU Commission. The cause of the cyberattack is unknown.

March 2024: Iranian hackers compromised an IT network connected to an Israeli nuclear facility. Hackers leaked sensitive facility documents but did not compromise its operational technology network.

March 2024: Russian cyber spies launched phishing attacks against German political parties. Hackers concealed ransomware in a fake dinner invitation from Germany's Christian Democratic Union to install a backdoor in their victim's computer.

March 2024: India's government and energy sectors was breached in a cyber espionage campaign. Hackers sent a malicious file disguised as a letter from India's Royal Air Force to offices responsible for India's electronic communications, IT governance, and national defense. Researchers have not yet determined who conducted the attack.

March 2024: A U.S. Department of Justice indictment revealed Chinese hackers targeted several EU members of the Inter-Parliamentary Alliance on China and Italian MPs. The attack was designed to detect IP addresses and the targets' locations.

March 2024: Canada pulled its financial intelligence system FINTRAC offline after a "cyber incident" by a currently unidentified attacker. FINTRAC claims the attack does not involve its intelligence or classified systems but declined to disclose further details of the incident.

March 2024: Russian hackers leaked an intercepted conversation between German military officials about the country's support for Ukraine. In the call, the head of Germany's Air Force discussed the possibility of supplying Taurus missiles to Ukraine and commented on German

Chancellor Olaf Scholz's hesitance to send the missiles. Germany announced it would investigate the incident and believes the leak was intended to inflame divisions in Germany.

March 2024: Switzerland's National Cyber Security Centre (NCSC) confirmed that leaded data from a May 2023 breach included 65,000 documents from the Federal Administration. The documents contained sensitive personal data, classified information, and passwords, and were from Switzerland's federal police, judiciary, and migration offices. Swiss officials had originally assessed that breach only impacted non-government documents.

March 2024: Microsoft claims Russian hackers stole its source code and are continuing to gain unauthorized access to its internal systems as part of their November 2023 campaign to spy on senior Microsoft executives. Microsoft also said attackers increased the volume of their "password spray" attacks by nearly tenfold between January and February 2024. The company did not disclose further details on the source code access or breached internal systems.

February 2024: Russian hackers launched an espionage campaign against the embassies of Georgia, Poland, Ukraine, and Iran beginning in 2023. Hackers exploited a bug in a webmail server to inject malware into servers at the embassies and collect information on European and Iranian political and military activities.

February 2024: Roughly 190 megabytes of data from a Chinese cybersecurity company were exposed online, revealing the company's espionage efforts on the governments of the United Kingdom, India, Indonesia, and Taiwan. The leak's source is unknown.

February 2024: The Royal Canadian Mounted Police suffered a cyberattack against its networks. The RCMP stated it is investigating this "alarming" incident and does not believe it had an impact on its operations or the safety and security of Canadians. It is so far unclear who is behind the attack and if it was a data breach or security incident.

February 2024: U.S. officials hacked an Iranian military spy ship that was sharing intelligence with Houthi rebels who have been firing on ships in the Red Sea. According to U.S. officials, the attack was part of the Biden administration's response to an Iranian drone stroke that killed three U.S. soldiers in Jordan.

February 2024: A data breach of French health insurance companies in January 2024 affected 33 million French citizens, or nearly half the country's population. The attack compromised sensitive birth date, social security, and marital status information, but not medical history. The French data protection agency opened an investigation to determine if the companies complied with cybersecurity guidelines under the EU's General Data Protection Regulations.

February 2024: Chinese spies places malware in a Dutch military network in 2023. The network was not connected to the defense ministry's main network, which reduced damage. This is the first time the Netherlands has publicly accused China of cyber espionage.

January 2024: Hackers breached Global Affairs Canada's secure VPN in December 2023, allowing hackers to access sensitive personal information of users and employees. It affected staff emails, calendars, and contacts. It's unclear if classified information was compromised or lost. The hacker's identity is currently unknown.

January 2024: Russian hackers launched a ransomware attack against Sweden's only digital service provider for government services. The attack affected operations for 120 government offices and came as Sweden prepared to join NATO. Sweden expects disruptions to continue for several weeks.

January 2024: Microsoft announced that Russian hackers broke into its corporate systems. Hackers used a "password spray attack" to steal emails and documents from accounts of Microsoft's senior leadership, cybersecurity, and legal teams back in November 2023.

January 2024: Russian hackers attacked 65 Australian government departments and agencies and stole 2.5 million documents in Australia's largest government cyberattack. Hackers infiltrated an Australian law firm that worked with the government to gain access to government files.

January 2024: The Australian government identified and sanctioned Aleksandr Ermakov as the Russian hacker who breached Medibank, the country's largest private health insurance provider, in 2022. He stole information from 9.7 million current and former Medibank customers. This is the first time Australia has issued cyber sanctions against an individual since the framework was established in 2021. The U.S. and UK also sanctioned Ermakov.

January 2024: Russian agents hacked residential webcams in Kyiv to gather information on the city's air defense systems before launching a missile attack on Kyiv. Hackers changed the cameras' angles to gather information on nearby critical infrastructure facilities and stream the footage on YouTube. Ukraine has since ordered webcam operators in the country to stop live broadcasts.

December 2023: Israeli-linked hackers disrupted approximately 70% of gas stations in Iran. Hackers claimed the attack was in retaliation for aggressive actions by Iran and its proxies in the region. Pumps restored operation the next day, but payment issues continued for several days.

December 2023: Ukrainian state hackers crippled Russia's largest water utility plant by encrypting over 6,000 computers and deleting over 50 TB of data. Hackers claimed their attack was in retaliation for the Russian Kyivstar cyberattack.

December 2023: Russian hackers hit Ukraine's largest mobile phone provider, Kyivstar, disabling access to its 24 million customers in Ukraine. Hackers claim to have destroyed more than 10,000 computers and 4,000 servers, including cloud storage and backup systems. The attack began hours before President Zelenskyy met with President Biden in Washington D.C.

December 2023: Ukraine's military intelligence service claims to have disabled Russia's tax service in a cyberattack. According to the military intelligence service, the attack destroyed the system's configuration files, databases, and their backups, paralyzing Russia's tax service.

November 2023: Suspected Chinese hackers launched an espionage campaign against Uzbekistan and the Republic of Korea. Hackers use phishing campaigns to gain access to their target's systems and decrypt their information.

November 2023: Chinese-linked hackers attacked Japan's space agency during summer 2023 and compromised the organization's directory. The agency shut down parts of its network to investigate the breach's scope, but claims it did not compromise critical rocket and satellite operations information.

November 2023: Chinese hackers compromised Philippine government networks. Beginning in August 2023, hackers used phishing emails to imbed malicious code into their target's systems to establish command-and-control and spy on their target's activities.

November 2023: Trinidad and Tobago's Prime Minister Dr. Keith Rowley declared the latest ransomware attack against the country's telecommunications service to be a "national security threat." Hackers stole an estimated six gigabytes of data, including email addresses, national ID numbers, and phone numbers.

November 2023: Denmark suffered its largest cyberattack on record when Russian hackers hit twenty-two Danish power companies. The attack began in May 2023 and appeared to be aimed at gaining comprehensive access to Denmark's decentralized power grid. Hackers exploited a critical command injection flaw and continued to exploit unpatched systems to maintain access.

November 2023: Chinese cybercriminals targeted at least 24 Cambodian government networks, including the National Defense, Election Oversight, Human Rights, National Treasury, Finance, Commerce, Politics, Natural Resources and Telecommunications agencies. Hackers disguised themselves as cloud storage services to mask their data exfiltration. Initial research indicates the attack is part of a broader Chinese espionage campaign.

October 2023: Researchers discovered what appears to be a state-sponsored software tool designed for espionage purposes and used against ASEAN governments and organizations.

October 2023: Pro-Hamas and pro-Israeli hacktivists have launched multiple cyberattacks against Israeli government sites and Hamas web pages in the aftermath of Hamas' attacks on Israel on October 7th. Russian and Iranian hacktivists also targeted Israeli government sites, and Indian hacktivists have attacked Hamas websites in support of Israel.

October 2023: Hacktivists stole 3,000 documents from NATO, the second time in three months that hacktivists have breached NATO's cybersecurity defenses. Hackers described themselves as

"gay furry hackers" and announced their attack was retaliation against NATO countries' human rights abuses. NATO alleges the attack did not impact NATO missions, operations, or military deployments.

October 2023: Vietnamese hackers attempted to install spyware on the phones of journalists, United Nations officials and the chairs of the House Foreign Affairs Committee and Senate Homeland Security and Governmental Affairs. The spyware was designed to siphon calls and texts from infected phones, and the unsuccessful deployment comes while Vietnamese and American diplomats were negotiating an agreement to counter China's growing influence in the region.

October 2023: New reporting reveals Chinese hackers have been targeting Guyana government agencies with phishing emails to exfiltrate sensitive information since February 2023.

October 2023: North Korean hackers sent malware phishing emails to employees of South Korea's shipbuilding sector. South Korea's National Intelligence Service suggested that the attacks were intended to gather key naval intelligence that could help North Korea build larger ships.

September 2023: Indian hacktivists targeted Canada's military and Parliament websites with DDoS attacks that slowed system operations for several hours. Hacktivists referenced Canadian Prime Minister Justin Trudeau's public accusation against India of killing Sikh independence activist Hardeep Singh Nijjar as motivation for the hack.

September 2023: Iranian hackers launched a cyberattack against Israel's railroad network. The hackers used a phishing campaign to target the network's electrical infrastructure. Brazilian and UAE companies were also reportedly targeted in the same attack.

September 2023: U.S. and Japanese officials warn that Chinese state-sponsored hackers placed modifying software inside routers to target government industries and companies located in both countries. The hackers use firmware implants to stay hidden and move around in their target's networks. China has denied the allegations.

September 2023: A massive cyberattack hit Bermuda's Department of Planning and other government services. The country's hospitals, transportation, and education centers remained functional, but other services were down for several weeks. Bermuda announced that it is investigating the attack and declined to state if any sensitive data was compromised.

September 2023: Cybercriminals targeted Kuwait's Ministry of Finance with a phishing ransomware attack. Kuwait isolated the Ministry and other government systems to protect them from potential further attacks.

September 2023: Russian is stepping up cyberattacks against Ukrainian law enforcement agencies, specifically units collecting and analyzing evidence of Russian war crimes, according

to Ukrainian officials. Russian cyberattacks have primarily targeted Ukrainian infrastructure for most of the war.

September 2023: Russian forces in occupied Crimea reported a cyberattack on Crimean Internet providers. The attack happened around the same time that a Ukrainian missile strike aimed at Russian naval headquarters in the area. Ukrainian officials have yet to comment.

September 2023: Russian cybercriminals breached the International Criminal Court's IT systems amid an ongoing probe into Russian war crimes committed in Ukraine.

September 2023: A new Microsoft report indicates an increase of Chinese cyber operations in the South China Sea, as well as increased attacks against the U.S. defense industrial base and U.S. critical infrastructure. The increase comes amid rising tensions between China and the U.S.

September 2023: A Russian ransomware group leaked Australian federal police officers' details on the dark web. The leak is the latest phase of a Russian attack which started in April 2023 against an Australian law firm that services several Australian government agencies.

September 2023: The iPhone of a Russian journalist for the independent newspaper Meduza was infected with Pegasus spyware in Germany this year. The incident is the first known instance of the spyware being used against a prominent Russian target. The country behind the spyware placement is unknown, but Latvia, Estonia, Azerbaijan, Kazakhstan, and Uzbekistan are all suspects given past use of Pegasus spyware or their allegiance to Russia.

September 2023: Suspected Chinese hackers attacked the national power grid of an unspecified Asian country earlier this year using Chinese malware. The group corrupted a Windows application that allowed them to move laterally within their target's systems.

September 2023: A ransomware attack wiped four months of Sri Lankan government data. The country's cloud services system didn't have backup services available for the data from May 17 to August 26, according to reporting. Malicious actors targeted Sri Lanka's government cloud system starting in August 2023 by sending infected links to government workers.

September 2023: An Indian cybersecurity firm uncovered plans from Pakistani and Indonesian hacking groups to disrupt the G20 summit in India. The hacktivists are expected to use DDoS attacks and mass defacement in their attacks, which are presumed to be the latest development in the hacktivist battle between these nations according to the firm's research.

September 2023: Russian hackers stole thousands of documents from the British Ministry of Defense and uploaded them to the dark web. The documents contained accessibility details for a nuclear base in Scotland, high-security prisons, and other national security details. Hackers acquired the documents by breaking into a British fencing developer and gaining backdoor access to Ministry files.

September 2023: Russian cyber criminals accessed sensitive information from South Africa's Department of Defense, including military contracts and personnel information. The Department reversed its previous statement denying the data leak.

August 2023: Russian hacktivists launched DDoS attacks against Czech banks and the Czech stock exchange. The hackers cut online banking access to the banks' clients and demanded that the institutions stop supporting Ukraine. Bank representatives claim the hacks did not threaten their clients' finances.

August 2023: Unnamed hackers took X, formerly known as Twitter, offline in several countries and demanded that owner Elon Musk open Starlink in Sudan. Attackers flooded the server with traffic to disable access for over 20,000 individuals in the U.S., UK, and other countries.

August 2023: Cybercriminals are allegedly selling a stolen dataset from China's Ministry of State Security. The full data set purportedly includes personal identification information for roughly half a billion Chinese citizens and "classified document[s]," according to the criminals' post about the sale.

August 2023: Russian hacktivists launched several DDoS attacks that knocked the Polish government's website offline, as well as the Warsaw Stock exchange and several Polish national banks.

August 2023: Russian hacktivists disabled Poland's rail systems by gaining access to the system's railway frequencies and transmitted a malicious signal that halted train operations. Attackers blasted Russia's national anthem and a speech from Putin on Russia's military operation in Ukraine during the attack.

August 2023: Chinese hackers targeted a U.S. military procurement system for reconnaissance, along with several Taiwan-based organizations. Attackers targeted high-bandwidth routers to exfiltrate data and establish covert proxy networks within target systems.

August 2023: Ukrainian hackers claim to have broken into the email of a senior Russian politician and leaked medical and financial documents, as well as messages that allegedly connect him to money laundering and sanctions evasion plots.

August 2023: Ecuador's national election agency claimed that cyberattacks from India, Bangladesh, Pakistan, Russia, Ukraine, Indonesia and China caused difficulties for absentee voters attempting to vote online in the latest election. The agency didn't elaborate on the nature of the attacks.

August 2023: Suspected North Korean hackers attempted to compromise a joint U.S.-South Korean military exercise on countering nuclear threats from North Korea. Hackers launched

several spear phishing email attacks at the exercise's war simulation center.

August 2023: Bangladesh shut down access to their central bank and election commission websites amid warnings of a planned cyberattack by an Indian hacking group. The shutdown was intended to prevent a cyberattack similar to a 2016 incident in Bangladesh where hackers stole nearly $1 billion, according to the central bank's statement.

August 2023: Belarusian hackers targeted foreign embassies in the country for nearly a decade, according to new reporting. Hackers disguised malware as Windows updates to get diplomats to download it onto their devices.

August 2023: Chinese hackers obtained personal and political emails of a U.S. Congressman from Nebraska. The hackers exploited the same Microsoft vulnerability that gave them access to emails from the State Department and Department of Commerce.

August 2023: Iranian cyber spies are targeting dissidents in Germany, according to Germany's domestic intelligence unit. The spies are using false digital personas tailored to victims to build a rapport with their targets before sending a malicious link to a credential harvesting page.

August 2023: Ukraine's State Security Service (SBU) claims that Russia's GRU is attempting to deploy custom malware against Starlink satellites to collect data on Ukrainian troop movements. SBU members discovered malware on Ukrainian tablets that were captured by the Russians before being recovered by Ukrainian forces.

August 2023: Russian hackers launched a ransomware attack against a Canadian government service provider, compromising the data of 1.4 million people in Alberta. The organization paid the ransom and claimed that very little data was lost.

August 2023: A Canadian politician was targeted by a Chinese disinformation campaign on WeChat. The attack included false accusations about the politician's race and political views. The Canadian government believes the attacks are retaliation against the politician's criticism of China's human rights policies.

August 2023: The Canadian government accused a "highly sophisticated Chinese state-sponsored actor" of hacking a prominent Canadian federal scientific research agency.

August 2023: Russia's military intelligence service attempted to hack Ukrainian Armed Forces' combat information systems. Hackers targeted Android tablets that Ukrainian forces use for planning and orchestrating combat missions.

August 2023: The United Kingdom's Electoral Commission revealed that Russian hackers breached the commission's network beginning in August 2021. They obtained information on tens of thousands of British citizens by accessing the commission's email and file-sharing

system.

August 2023: According to a new report, North Korean hackers breached computer systems at a Russian missile developer for five months in 2022. Analysts could not determine what information may have been taken or viewed.

July 2023: China claims that an earthquake monitoring system in Wuhan was hacked by "U.S. cybercriminals." Chinese state media asserts that a backdoor program with the capacity to steal seismic data was inserted into the program.

July 2023: Kenya's eCitizen service was disrupted by pro-Russian cybercriminals for several days. Kenya's Ministry of Information, Communications, and the Digital Economy claimed that no data was accessed or lost.

July 2023: Russian-linked cyber hackers have targeted Ukrainian state services such as the app "Diia" using malware and phishing attacks. The primary targets are Ukrainian defense and security services.

July 2023: The Ministry of Justice in Trinidad and Tobago was hit with a DDoS attack that disrupted court operations across the country. The ministry reported outages beginning in late June, which are believed to be linked to this same attack.

July 2023: New Zealand's parliament was hit by a cyberattack from a Russian hacking group. The group said their attack was retaliation against New Zealand's support for Ukraine, such as its assistance with training Ukrainian troops and sanctions against Russia. Heckers temporarily shut down the New Zealand Parliament, Parliamentary Counsel Office (PCO) and Legislation websites in a DDoS attack.

July 2023: Russian hackers targeted twelve government ministries in Norway to gain access to sensitive information. The hackers exploited a vulnerability in a software platform used by the ministries.

July 2023: A South Korean government-affiliated institution fell victim to a phishing scandal that resulted in a loss of 175 million wons, reportedly the first phishing incident against a South Korean government public organization.

July 2023: Chinese-linked hackers infected a Pakistani government app with malware. A state bank and telecoms provider were also targeted in the attack.

July 2023: Chinese hackers breached the emails of several prominent U.S. government employees in the State Department and Department of Commerce through a vulnerability in Microsoft's email systems.

July 2023: Russian hackers targeted numerous attendees of the latest NATO Summit in Vilnius. The assailants used a malicious replica of the Ukraine World Congress website to target attendees.

July 2023: A Polish diplomat's advertisement to purchase a used BMW was corrupted by Russian hackers and used to target Ukrainian diplomats. The hackers copied the flyer, imbedded it with malicious software and distributed it to foreign diplomats in Kyiv.

June 2023: A group allegedly tied to the private military corporation Wagner hacked a Russian satellite telecommunications provider that services the Federal Security Service (FSB) and Russian military units. The attack comes after Wagner's attempted rebellion against President Vladimir Putin over the war in Ukraine.

June 2023: A Pakistani-based hacker group infiltrated the Indian army and education sector in the group's latest wave of attacks against Indian government institutions. The hack is the latest in a series of targeted attacks from this group that have intensified over the past year.

June 2023: Pro-Russian hacktivists used a DDoS attack to target several Ukrainian and Italian banking institutions, including the European Investment Bank.

June 2023: Several U.S. federal government agencies, including Department of Energy entities and the U.S. Office of Personnel Management, were breached in a global cyberattack by Russian-linked hackers. Cybercriminals targeted a vulnerability in software that is widely used by the agencies, according to a US cybersecurity agent.

June 2023: An Illinois hospital became the first health care facility to publicly list a ransomware attack as a primary reason for closing. The attack, which occurred in 2021, permanently crippled the facility's finances.

June 2023: Pro-Russian hackers targeted several Swiss government websites, including those for Parliament, the federal administration, and the Geneva airport. The DDoS attacks coincide in conjunction with preparations for Ukrainian President Volodimir Zelensky's virtual address before the Swiss parliament.

June 2023: According to new reporting, North Korean hackers have been impersonating tech workers or employers to steal more than $3 billion since 2018. The money has reportedly been used to fund the country's ballistic missiles program, according to U.S. officials.

June 2023: Ukrainian hackers claimed responsibility for an attack on a Russian telecom firm that provides critical infrastructure to the Russian banking system. The attack occurred in conjunction with Ukraine's counteroffensive.

June 2023: Russia's Federal Security Services (FSB) alleged that Apple worked closely with US

intelligence agencies to hack thousands of iPhones belonging to Russian users and foreign diplomats. Apple denied the claims, and the NSA declined to comment.

May 2023: Belgium's cyber security agency has linked China-sponsored hackers to a spearfishing attack on a prominent politician. The attack comes as European governments are increasingly willing to challenge China over cyber offences.

May 2023: Chinese hackers breached communications networks at a U.S. outpost in Guam. The hackers used legitimate credentials, making it harder to detect them.

May 2023: Chinese hackers targeted Kenyan government ministries and state institutions, including the presidential office. The hacks appeared to be aimed at gaining information on debt owed to Beijing.

May 2023: A likely Russia state group has targeted government organizations in Central Asia. The group is using previously unknown malware, and the attacks focused on document exfiltration.

May 2023: India's Insurance Information Bureau fell victim to a ransomware attack. Hackers encrypted nearly 30 server systems and demanded $250,000 in bitcoin. The bureau relied on its data backup system to maintain operations and did not pay the ransom.

May 2023: An unidentified group hacked targets in both Russia and Ukraine. The motive for the attacks was surveillance and data gathering.

May 2023: Russian-linked hackivists conducted an unsuccessful cyberattack against Ukraine's system for managing border crossings by commercial trucks through a phishing campaign

April 2023: Sudan-linked hackers conducted a DDoS attack on Israel's Independence Day, taking the Israeli Supreme Court's website offline for several hours. Israeli cyber authorities reported no lasting damage to network infrastructure. Hackers claimed to have also attacked several other Israeli government and media sites, but those attacks could not be confirmed. The group has been active since at least January 2023, attacking critical infrastructure in Northern Europe and is considered religiously motivated.

April 2023: NSA cyber authorities reported evidence of Russian ransomware and supply chain attacks against Ukraine and other European countries who have provided Ukraine with humanitarian aid during the war in Ukraine. There were no indications of these attacks against U.S. networks.

April 2023: Iranian state-linked hackers targeted critical infrastructure in the U.S. and other countries in a series of attacks using a previously unseen customized dropper malware. The hacking group has been active since at least 2014, conducting social engineering and espionage

operations that support the Iranian government's interests.

April 2023: Recorded Future released a report revealing data exfiltration attacks against South Korean research and academic institutions in January 2023. The report identified Chinese-language hackers. Researchers believe that this is a hacktivist group motivated by patriotism for China.

April 2023: Researchers at Mandiant attributed a software supply chain attack on 3CX Desktop App software to North Korea-linked hackers. During its investigation, Mandiant found that this attack used a vulnerability previously injected into 3CX software. This is Mandiant's first discovery of a software supply chain attack leveraging vulnerabilities from a previous software supply chain attack.

April 2023: Chinese hackers targeted telecommunication services providers in Africa in an espionage campaign since at least November 2022. Researchers believe the group has targeted pro-domestic human rights and pro-democracy advocates, including nation-states, since at least 2014. Using the access from the telecom providers, the group gathers information including keystrokes, browser data, records audio, and captures data from individual targets on the network.

April 2023: A Russia-linked threat group launched a DDoS attack against Canadian prime Minister Justin Trudeau, blocking access to his website for several hours. The operation's timing coincided with the Canadian government's meeting with Ukrainian Prime Minister Denys Shmyhal, suggesting that the operation was retaliation.

April 2023: North Korea-linked hackers are operating an ongoing espionage campaign targeting defense industry firms in Eastern Europe and Africa. Researchers at Kaspersky believe the hacking group shifted its focus in 2020 from financially motivated coin-mining attacks to espionage.

April 2023: Researchers discovered Israeli spyware on the iPhones of over 5 journalists, political opposition figures, and an NGO worker. Hackers initially compromised targets using malicious calendar invitations. The hackers' origin and motivations are unclear.

April 2023: Ukraine-linked hacktivists targeted the email of Russian GRU Unit26165's leader, Lieutenant Colonel Sergey Alexandrovich, leaking his correspondence to a volunteer intelligence analysis group. The exfiltrated data contained Alexandrovich's personal information, unit personnel files, and information on Russian cyberattack tools.

April 2023: North Korean-linked hackers targeted people with expertise on North Korea policy issues in a phishing campaign. Hackers posed as journalists requesting interviews from targets, inviting them to use embedded links for scheduling and stealing their login credentials. The amount of information stolen and number of targets are unclear.

March 2023. Russian hackers brought down the French National Assembly's website for several hours using a DDoS attack. In a Telegram post, hackers cited the French government's support for Ukraine as the reason for the attack.

March 2023. CISA and FBI reported that a U.S. federal agency was targeted by multiple attackers, including a Vietnamese espionage group, in a cyberespionage campaign between November 2022 and January 2023. Hackers used a vulnerability in the agency's Microsoft Internet Information Services (IIS) server to install malware.

March 2023. A Chinese cyberespionage group targeted an East Asian data protection company who serves military and government entities that lasted approximately a year.

March 2023: (3/24) A South Asian hacking group targeted firms in China's nuclear energy industry in an espionage campaign. Researchers believe the group commonly targets the energy and government sectors of Pakistan, China, Bangladesh, and Saudi Arabia.

March 2023. Estonian officials claim that hackers unsuccessfully targeted the country's internet voting system during its recent parliamentary elections. Officials did not release details about the attacks or provide attribution.

March 2023. North Korean hackers targeted U.S.-based cybersecurity research firms in a phishing campaign. The campaign was meant to deliver malware for cyberespionage.

March 2023. A Chinese cyber espionage group targeted government entities in Vietnam, Thailand, and Indonesia, using newly developed malware optimized to evade detection.

March 2023. Russian hackers launched social engineering campaigns targeting U.S. and European politicians, businesspeople, and celebrities who have publicly denounced Vladimir Putin's invasion of Ukraine. Hackers persuaded victims to participate in phone or video calls, giving misleading prompts to obtain pro-Putin or pro-Russian soundbites. They published these to discredit victims' previous anti-Putin statements.

March 2023. Slovakian cybersecurity researchers discovered a new exploit from a Chinese espionage group targeting political organizations in Taiwan and Ukraine.

March 2023. Poland blamed Russia hackers for a DDoS attack on its official tax service website. Hackers blocked users' access to the site for approximately an hour, but no data was leaked in the attack. A pro-Russian hacking group had earlier published a statement on Telegram about its intention to attack the Polish tax service.

February 2023. Russian hackers deployed malware to steal information from Ukrainian organizations in a phishing campaign. The malware is capable of extracting account information and files, as well as taking screenshots. Researchers believe the group is a key player in Russia's cyber campaigns against Ukraine.

February 2023. A pro-Russian hacking group claimed responsibility for DDoS attacks against NATO networks used to transmit sensitive data. The attack disrupted communications between NATO and airplanes providing earthquake aid to a Turkish airbase. The attack also took NATO's sites offline temporarily.

February 2023. Polish officials reported a disinformation campaign targeting the Polish public. Targets received anti-Ukrainian refugee disinformation via email. Officials claimed these activities may be related to Russia-linked hackers.

February 2023. A North Korean hacking group conducted an espionage campaign between August and November 2022. Hackers targeted medical research, healthcare, defense, energy, chemical engineering and a research university, exfiltrating over 100MB of data from each victim while remaining undetected. The group is linked to the North Korean government.

February 2023. Latvian officials claimed that Russian hackers launched a phishing campaign against its Ministry of Defense. The Latvian Ministry of Defense stated this operation was unsuccessful.

February 2023. Iranian hacktivists disrupted the state-run television broadcast of a speech by Iranian president Ebrahim Raisi during Revolution Day ceremonies. Hackers aired the slogan "Death to Khamenei" and encouraged citizens to join antigovernment protests.

February 2023. An Iranian hacking group launched an espionage campaign against organizations in the Middle East. Hackers used a backdoor malware to compromise target email accounts. Researchers claim the hacking group is linked to Iranian intelligence services.

February 2023. Iranian hacktivists claimed responsibility for taking down websites for the Bahrain international airport and state news agency.

February 2023. Hackers launched a ransomware attack against Technion University, Israel's top technology education program. Hackers demanded 80 bitcoin ($1.7 million USD) to decrypt the university's files. Israeli cybersecurity officials blamed Iranian state-sponsored hackers for the attack.

February 2023. Hackers disabled Italy's Revenue Agency (Agenzia delle Entrane) website. While the website was disabled, users received phishing emails directing them to a false login page that mirrored the official agency site.

February 2023. Chinese cyberespionage hackers performed a spear-phishing campaign against government and public sector organizations in Asia and Europe. The emails used a draft EU Commission letter as its initial attack vector. These campaigns have occurred since at least 2019.

January 2023. Latvian officials claimed that Russia-linked hackers launched a cyber espionage phishing campaign against its Ministry of Defense. The Latvian Ministry of Defense stated this operation was unsuccessful.

January 2023. CISA, the NSA, and the Multi-State Information Sharing and Analysis Center released a joint advisory warning of an increase in hacks on the federal civilian executive branch utilizing remote access software. This follows an October 2022 report on a financially motivated phishing campaign against multiple U.S. federal civilian executive branch agencies.

January 2023. Russia-linked hackers deployed a ransomware attack against the UK postal service, the Royal Mail. The attack disrupted the systems used to track international mail.

January 2023. Iran-linked hackers executed ransomware attacks and exfiltrated data from U.S. public infrastructure and private Australian organizations. Australian authorities claim that the data exfiltrated was for use in extortion campaigns.

January 2023. Hackers used ransomware to encrypt 12 servers at Costa Rica's Ministry of Public Works, knocking all its servers offline.

January 2023. Albanian officials reported that its government servers were still near-daily targets of cyber-attacks following a major attack by Iran-linked hackers in 2022.

January 2023. Hackers launched a series of cyber-attacks against Malaysian national defense networks. Malaysian officials stated that the hacking activities were detected early enough to prevent any network compromise.

January 2023. Hackers targeted government, military, and civilian networks across the Asia Pacific leveraging malware to obtain confidential information. The malware targeted both the data on victim machines as well as audio captured by infected machines' microphones.

January 2023. Hackers sent over a thousand emails containing malicious links to Moldovan government accounts.

December 2022. China-linked hackers launched phishing attacks against government, education, and research sector victims across the Asia Pacific. These attacks contained malware designed for espionage.

December 2022. Hackers launched email phishing attacks against Ukranian government agencies and state railway systems. The emails included information on kamikaze drone identification and deployed malware designed for espionage onto victim machines.

December 2022. Hackers obtained contact information for more than 80,000 members of FBI threat information sharing program, InfraGard. They then posted this information for sale on a cybercrime forum.

December 2022. Microsoft reported that it observed a pattern of attacks targeting Ukranian critical infrastructure from Russian hacking group, Sandworm. These attacks were accompanied by pro-Russian propaganda.

December 2022. The Human Rights Watch reported an ongoing, well-resourced cyber espionage, social engineering, and phishing campaign against human rights activists, journalists, diplomats, and politicians located across the Middle East. The organization attributed these operations to Iran-linked hackers.

December 2022. Hackers made Italy's Ministry of Agriculture website unavailable through a DDoS attack. Italian officials described the attacks as "demonstrative" and claim that no data was breached and that they expect no lasting damage.

December 2022. Russia-linked hackers leveraged the networks of healthcare organizations, businesses, and critical infrastructures across the U.S., UK, France, and other countries to attack targets in Ukraine. Hackers' primary motivations appear to be information stealing and disruption.

December 2022. Iran-linked hackers obtained and leaked data from government ministries in Saudi Arabia.

December 2022. Russia-linked hackers launched a DDoS attack against Vatican City servers, knocking its official website offline. The attack came three days after Russian government officials criticized Pope Francis for his comments about the war in Ukraine.

December 2022. Hackers launched a DDoS attack against the Danish defense ministry that disrupted access to its websites.

December 2022. Russia's foreign minister claimed to be the target of coordinated cyber aggression by external intelligence agencies, IT companies, and hacktivists. According to Russian officials, such attacks have "doubled or tripled" over the past year.

December 2022. Chinese government-linked hackers stole at least $20 million in COVID-19 relief funds from the U.S. government, including Small Business Administration loans and unemployment insurance money. The U.S. Secret Service announced they retrieved half of the stolen funds thus far.

December 2022. Chinese-linked hackers targeted Amnesty International of Canada in an apparent espionage operation.

December 2022. A U.S. lawmaker predicted spyware hacks of U.S. government employees could be in the hundreds, including diplomats in multiple countries. This follows a probe into how many devices spyware are affected in the U.S. government.

November 2022. Hackers disrupted operations at an Indian hospital by cutting off access to its online networks and patient records. It took hospital officials and federal authorities nearly two weeks to regain access to hospital servers and recover lost data.

November 2022. Microsoft and ESET attributed cyberattacks aimed at the energy sector and logistics industries in Ukraine and Poland to a Russian GRU hacking group. The campaign

began in late September 2022.

November 2022. Hackers targeted Bahraini government websites with DDoS attacks prior the country's parliamentary and local elections.

November 2022. Iranian government-sponsored hackers compromised the U.S. Merit Systems Protection Board, exploiting the log4shell vulnerability as early as February 2022. After breaching the network, hackers installed cryptocurrency-mining software and deployed malware to obtain sensitive data.

November 2022. Hackers damaged Danish State Railways' network after targeting an IT subcontractor's software testing environment. The attack shut down train operations for several hours.

November 2022. An Indian-based hacking group targeted Pakistani politicians, generals and diplomats, deploying malware that enables the attacker access to computer cameras and microphones.

November 2022. State-sponsored hackers with possible ties to the Chinese government targeted multiple Asian countries in an espionage operation since March 2022, compromising a digital certificate authority in one country.

November 2022. Hackers disabled digital services of the Vanuatu government in a cyberattack. The attack affected all government services, disabling emails, websites, and government systems, with only partial access restored a month later. Australian sources stated the hack was a ransomware attack.

November 2022. Hackers targeted the Guadeloupe government, forcing the shutdown of all government computers to "protect data" during incident response and detect the scope of the attack.

November 2022. Indian hackers targeted Pakistani government entities, including the military, and companies since April 2020. The attacks enabled hackers to infiltrate systems and access computer controls.

November 2022. Suspected Chinese-linked hackers carried out an espionage campaign on public and private organizations in the Philippines, Europe, and the United States since 2021. The attacks used infected USB drives to deliver malware to the organizations.

November 2022. Chinese state-affiliated actors increased attacks on smaller nations in Southeast Asia for cyberespionage purposes.

October 2022. Hackers targeted a communications platform in Australia, which handles Department of Defence data, in a ransomware attack. The government believes hackers breached sensitive government data in this attack.

October 2022. A Ukrainian newspaper published hacked data claiming to be sensitive

information from Russian defense contractors. The hackers responsible are part of an anti-Putin group in Russia.

October 2022. Hackers targeted Bulgarian websites belonging to the presidential administration, the Defense Ministry, the Interior Ministry, the Justice Ministry, and the Constitutional Court in a DDoS attack. A pro-Russian hacking group claimed responsibility for the attack, stating it was punishment "for betrayal to Russia and the supply of weapons to Ukraine."

October 2022. Hackers targeted several major U.S. airports with a DDoS attack, impacting their websites. A pro-Russian hacking group promoted the attack prior to its execution.

October 2022. Pro-Russian hackers claimed responsibility for an attack that knocked U.S. state government websites offline, including Colorado's, Kentucky's and Mississippi's.

October 2022. CISA, the FBI, and NSA announced state-sponsored hacking groups had long-term access to a defense company since January 2021 and compromised sensitive company data.

September 2022. Iranian hackers targeted Albanian computer systems, forcing Albanian officials to temporarily shut down the Total Information Management System, a service used to track individuals entering and exiting Albania. This attack closely followed Albania's decision to sever diplomatic ties with Iran as well as the American sanctions and NATO's condemnation of an Iranian cyberattack against Albania in July. In the July attack, Iranian actors deployed ransomware on Albanian Government networks that destroyed data and disrupted government services.

September 2022. A newly discovered hacking group targeted telecommunications, internet service providers, and universities in the Middle East and Africa. The group deploys malware platforms directly into systems' memory, bypassing native security solutions.

September 2022. Hackers targeted Montenegro's government networks, rendering Montenegro's main state websites and government information platforms inaccessible. Montenegrin officials blamed Russia for the attack.

September 2022. Hackers targeted the state-level parliamentary website of Bosnia and Herzegovina, rendering the sites and servers inaccessible for multiple weeks.

September 2022. China accused the U.S. National Security Agency (NSA) of numerous cyberattacks against China's Northwestern Polytechnical University. Authorities claim the NSA stole user data and infiltrated digital communications networks.

September 2022. The group Anonymous took responsibility for a series of cyberattacks against the Iranian government that took down two main Iranian government websites and the websites of several state media organizations.

September 2022. Hackers targeted the Mexican Defense Ministry and accessed six terabytes of data, including internal communications, criminal data, and data that revealed Mexico's

monitoring of Ken Salazar, the U.S. Ambassador to Mexico. Mexican President Andres Manuel Lopez Obrador confirmed the authenticity of the data, including personal health data released to the public.

September 2022. A Russian-based hacking group targeted the website of the United Kingdom's intelligence agency MI5 with a DDoS attack that temporarily took the site offline.

August 2022. Hackers breached Italy's energy agency, Gestore dei Servizi Energetici (GSE), compromising servers, blocking access to systems, and suspending access to the GSE website for a week.

August 2022. Hackers used a DDoS attack to temporarily take down the website of Taiwan's presidential office. The Taiwanese government attributed the attack to foreign hackers and stated normal operations of the website resumed after 20 minutes. Taiwan's Foreign Ministry also noted hackers targeted their website and the main portal website for Taiwan's government.

August 2022. Hackers targeted the Finnish Parliament with a DDoS attack that rendered the Parliamentary website inaccessible. A Russian group claimed responsibility for the attack on Telegram.

August 2022. Hackers targeted the website of Ukraine's state energy agency responsible for the oversight of Ukraine's nuclear power plants. The agency stated Russian hackers carried out the attack.

August 2022. Hackers targeted the website of the Latvian Parliament with a DDoS attack that temporarily paralyzed the website's server. A Russian hacking group claimed responsibility for the attack on Telegram.

August 2022. Hackers targeted Greece's largest natural gas distributor DESFA causing a system outage and data exposure.

August 2022. A Russian group claimed responsibility for breaching a privately owned UK water supply company South Staffordshire Water and leaking files in an extortion attempt.

August 2022. Hackers targeted Montenegro's government institutions, breaching the computer systems of several state bodies. Montenegro's Defense Minister stated there was sufficient evidence to suspect Russia was behind the attack.

August 2022. A DDoS campaign targeted the websites of both government and private Estonian institutions. Estonia stated that the attack was largely repelled, and the impact was limited.

August 2022. Hackers used phishing emails to deploy malware in government institutions and defense firms throughout Eastern Europe in January 2022. A report by Russian-based company Kaspersky linked the campaign to a Chinese hacking group.

July 2022. Hackers targeted the Pakistan Air Force (PAF) in a spearfishing campaign to deploy malware and obtain sensitive files. Pakistani and Chinese organizations claimed the attack came from Indian-linked hackers.

July 2022. Hackers targeted Iran's Islamic Culture and Communication Organization (ICCO). The attack took down at least 6 websites, placed images of Iranian resistance leaders on fifteen additional sites, wiped databases and computers, and allowed hackers to obtain access to sensitive ICCO data.

July 2022. A hacker claimed to acquire records on 1 billion Chinese from a Shanghai police database and posted the data for sale online.

July 2022. Belgium's Foreign Ministry accused China of a cyberespionage campaign against Belgian targets, including Belgium's Ministries of Interior and Defense. A spokesperson for the Chinese Embassy in Belgium denied the accusations.

July 2022. Hackers targeted social media accounts owned by the British Royal Army. The attack included the takeover of the British Army's Twitter and YouTube accounts.

July 2022. Hackers targeted Lithuania's state-owned energy provider in a DDoS attack. Killnet, which Lithuanian officials link to Russia, claimed responsibility for the attack.

July 2022. Hackers temporarily took down websites belonging to the Albanian Prime Minister's Office and the Parliament, and the e-Albania portal used to access public services.

July 2022. Hackers breached a Ukrainian media company to broadcast on multiple radio stations that Ukrainian President Volodymyr Zelenskyy was in critical condition. Zelenskyy refuted the claims and blamed Russia for the attack.

July 2022. China stated the United States stole 97 billion pieces of global internet data and 124 billion pieces of telephone data in June, specifically blaming the National Security Agency (NSA)'s Office of Tailored Access Operations (TAO).

June 2022. Hackers targeted Lithuania's state railway, airports, media companies, and government ministries with DDoS attacks. A Russian-backed hacking group claimed responsibility for the attack.

June 2022. The FBI, National Security Agency (NSA) and CISA announced that Chinese state-sponsored hackers targeted and breached major telecommunications companies and network service providers since at least 2020.

June 2022. Hackers targeted former Israeli officials, military personnel, and a former U.S. Ambassador to Israel. An Israeli cybersecurity firm stated Iranian-linked actors used a phishing campaign to gain access to the targets' inboxes, personally identifiable information, and identity documents.

June 2022. Hackers targeted three Iranian steel companies, forcing the country's state-owned plant to halt production.

June 2022. Hackers leaked files and photos known as "The Xinjiang Police Files" displaying human rights abuses committed by the Chinese government against the Uyghur population.

June 2022. An attack targeted users of Australia's largest Chinese-language platform, Media Today. The hackers made over 20 million attempts to reset user passwords in the platform's registration system.

June 2022. Hackers targeted municipal public address systems in Jerusalem and Eliat, triggering the air raid sirens systems throughout both cities. An Israeli industrial cybersecurity firm attributed the attack to Iran.

June 2022. A Chinese-linked disinformation campaign targeted an Australian mining company. The campaign included spreading disinformation on social media platforms and websites regarding the company's alleged environmental record.

June 2022. A phishing campaign targeted U.S. organizations in military, software, supply chain, healthcare, and pharmaceutical sectors to compromise Microsoft Office 365 and Outlook accounts.

June 2022. Hackers compromised accounts belonging to officials in Germany's Greens party, including ones used previously by Annalena Baerbock and Robert Habeck, who now serve as Minister for Foreign Affairs and Minister for Economic Affairs and Climate Action.

June 2022. Hackers targeted Norwegian public institutions with DDoS attacks, disrupting government websites. The Norwegian NSM security authority attributed the attack to pro-Russian hackers.

May 2022. A DDoS attack targeted the Port of London Authority, forcing its website to go offline. A group linked to Iran took responsibility for the hack.

May 2022. A phishing campaign targeted the Jordan Ministry of Foreign Affairs. Researchers attributed the attack to an Iranian cyber espionage actor.

May 2022. The Ethiopian Information Network Security Agency (INSA) stated hackers targeted the Grand Ethiopian Renaissance Dam (GERD). Ethiopia's communications security agency thwarted the attacks before hackers could gain access to the networks.

May 2022. Hackers targeted Greenland's healthcare system, causing networks to crash throughout the island. While an initial diagnosis determined the attack did not damage or expose citizens' data, it made health services severely limited.

May 2022. A Chinese hacking group stole intellectual property assets from U.S and European companies since 2019 and went largely undetected. Researchers believe the group is backed by the Chinese government.

May 2022. State-sponsored hackers took down RuTube, the Russian version of YouTube, according to the company.

May 2022. Russian hackers hit Italian websites with a DDoS attack, including the Senate, the Ministry of Defence, and the National Health Institute. The group states its goal was to target NATO countries and Ukraine.

April 2022. The Romanian National Directorate of Cyber Security said that multiple public and private sector websites were hit with DDoS attacks. The victims included the ministry of defense, border police, national railway company, and the OTP Bank. A group claiming credit for the attack said on Telegram that it hacked the websites because Romania supported Ukraine since the Russian invasion of the country.

April 2022. Cybersecurity researchers identified a new campaign by Russian-linked hackers that started in January and targets diplomats and embassy officials from France, Poland, Portugal, and other countries. The hacks started with a phishing email to deliver a malware-laden file to the target.

April 2022. Iranian state television claimed that the government foiled cyber intrusions that targeted more than 100 public sector agencies. They provided no further information on the incident.

April 2022. Russian hackers targeted the Costa Rican Ministry of Finance in a cyberattack, crippling tax collection and export systems. The newly elected President of Costa Rica declared a national emergency as a result of the attack and the group asked for $20 million in ransom or it plans to leak the stolen data.

April 2022. Hackers targeted members of the European Commission with spyware developed by NSO Group. An Apple notification from November to thousands of iPhone users stating they were targeted by state-sponsored actor alerted the Commission of this spyware use.

April 2022. A North Korea-linked hacking campaign using phishing emails sent from fake job recruiters targeted chemical companies in South Korea.

April 2022. A Citizen Lab study discovered actors used NSO Group spyware to target at least 65 Catalonian activists and political figures.

April 2022. The U.S. Treasury Department's Office of Foreign Assets Control attributed the March 29 hack of Ronin Network to a North Korean hacking group and announced sanctions against the hackers. The group stole over $540 million in Ethereum and USDC.

April 2022. Hackers launched DDoS attacks against websites belonging to the Finnish Ministries of Defence and Foreign Affairs. The attack's botnet used over 350 IP addresses from around the world and the denial of service was sustained for four hours.

April 2022. Hackers targeted the Telegram accounts of Ukrainian government officials with a phishing attack in an attempt to gain access to the accounts.

April 2022. Cybersecurity researchers observed hackers penetrating the networks of at least 7 Indian State Load Dispatch Centres (SLDCs) which oversee operations for electrical grid control. The SLDCs manage SCADA systems and researchers suggested that PLA-linked hackers may be involved.

April 2022. A social media platform disrupted two Iranian-linked cyber espionage campaigns that targeted activists, academics, and private companies. The campaign targeted businesses in the energy, semiconductor, and telecom sectors in countries including the U.S., Israel, Russia, and Canada by using phishing and other social engineering techniques.

April 2022. A group targeted several Ukrainian media organizations in an attempt to gain long-term access to their networks and collect sensitive information, according to researchers. The group has connections to the Russian GRU.

April 2022. The United States removed Russian malware from computer networks around the world, a move made public by Attorney General Merrick B. Garland. While it is unclear what the malware's intention was, authorities noted it could be used from anything from surveillance to destructive attacks. The malware created a botnet controlled by the Russian GRU.

April 2022. Hackers targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shutdown electrical substations in Ukraine. Researchers believe the attack came from the same group with ties to the Russian GRU that targeted Ukraine's power grid in 2016, using an updated form of the same malware.

April 2022: Hackers targeted Ukraine's National Post Office with a DDoS attack, days after releasing a new stamp honoring a Ukrainian border guard. Th attack affected the agency's ability to run their online store.

March 2022. Hackers used a DDoS attack to shut down the National Telecommunications Authority of the Marshall Islands. The attack disrupted internet services on the Islands for over a week.

March 2022. An attack on a satellite broadband service run by the American company Viasat disrupted internet services across Europe, including Ukrainian military communications at the start of the Russian invasion. The attackers hacked satellite modems belonging to thousands of Europeans to disrupt the company's service.

March 2022. Hackers penetrated the websites belong to multiple Russian agencies including the Energy Ministry, the Federal State Statistics Service, the Federal Penitentiary Service, and the

Federal Bailiff Service. The websites displayed several anti-government and anti-invasion images and messages before the agencies were able to expel the attackers.

March 2022. Hackers targeted Greenland's parliamentary authority in an apparent espionage operation, forcing the parliament to cancel meetings and slowing social benefit payments.

March 2022. The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) stated that hackers from the United States targeted Chinese computers to carry out attacks on Russia, Ukraine, and Belarus.

March 2022. The European Banking Authority was targeted using a vulnerability in Microsoft's mail server software, but no data was compromised. Various attacks using this vulnerability have been attributed to a Chinese government-backed actor.

March 2022. Hackers defaced and disrupted several Russian government and state media websites, according to the Russian Ministry of Digital Development and Communications. The Emergency Situations Ministry website was hacked, and the attackers wrote messages encouraging Russian soldiers to defect. Tass, a state-run news agency, was also penetrated and hackers displayed a call for people to "take to the streets against the war."

March 2022. The National Research Council, Canada's biggest state-funded research agency, shared that hackers penetrated its networks. An announcement on the Council's website explained that parts of its online presence were taken offline as a result of this incident.

March 2022. Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least 6 different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks, in addition to several other vulnerable internet-facing web applications.

March 2022. Hackers used a DDoS attack to target a major Israeli telecommunication provider. As a result, multiple Israeli government websites were taken offline.

February 2022. Researchers identified campaigns by two North Korean government-backed groups targeting employees across numerous media, fintech, and software companies. The hackers used phishing emails advertising fake job opportunities and exploited a vulnerability in Google Chrome to compromise the companies' websites and spread malware.

February 2022. The websites of the Ukrainian Cabinet of Ministers and Ministries of Foreign Affairs, Infrastructure, and Education were disrupted in the days before Russian troops invaded Ukraine. Wiper malware was also used to penetrate the networks of one Ukrainian financial institution and two government contractors.

February 2022. A Beijing-based cybersecurity company accused the U.S. National Security Agency of engineering a backdoor to monitor companies and governments in over 45 countries around the world. A Foreign Ministry spokesman said that operations like this may threaten the security of China's critical infrastructure and compromise trade secrets.

February 2022. On February 15, a DDoS attack knocked websites belonging to the Ukrainian Defense Ministry and two of the country's largest banks offline. The U.S. and the UK attributed the attack to the Russian GRU. The Ukrainian Cyber Police claimed that the attack was connected to another "information attack" where Ukrainian citizens received spam text messages claiming that ATMs were not working.

February 2022. A Beijing-based cybersecurity company accused the U.S. National Security Agency of engineering a back-door to monitor companies and governments in over 45 countries around the world. A Foreign Ministry spokesman said that operations like this may threaten the security of China's critical infrastructure and compromise trade secrets.

February 2022. A Pakistani group deployed a remote access trojan to conduct espionage against Indian military and diplomatic targets. The group generally uses social engineering and/or USB-based worms to penetrate a network.

February 2022. An Iranian-linked group conducted espionage and other malicious cyber operations against a range of private companies and local and federal governments.

February 2022. Russian state-sponsored actors hacked into numerous U.S. defense contractors between January 2020 and February 2022. The hackers exfiltrated emails and sensitive data relating to the companies' export-controlled products and proprietary information and interactions with foreign governments.

February 2022. Multiple oil terminals in some of Europe's biggest ports across Belgium and Germany fell victim to a cyberattack, rendering them unable to process incoming barges. A ransomware strain associated with a Russian-speaking hacking group was used to disrupt the ability of energy companies to process payments.

February 2022. Since October 2021, a hacking group targeted Palestinian individuals and organizations with malware. Researchers suggest that the operation could be connected to a broader campaign by a hacking group commonly attributed to the cyber arm of Hamas that started in 2017.

February 2022. A U.N. report claimed that North Korea hackers stole more than $50 million between 2020 and mid-2021 from three cryptocurrency exchanges. The report also added that in 2021 that amount likely increased, as the DPRK launched 7 attacks on cryptocurrency platforms to help fund their nuclear program in the face of a significant sanctions regime.

February 2022. An investigation led by Mandiant discovered that hackers linked to the Chinese-government compromised email accounts belonging to Wall Street Journal journalists. The hackers allegedly surveilled and exfiltrated data from the newspaper for over two years beginning in at least February 2020.

February 2022. The networks of the U.K. Foreign Office were penetrated by hackers. All details of the incident remain confidential.

January 2022. A Chinese hacking group breached several German pharma and tech firms. According to the German government, the hack into the networks of service providers and companies was primarily an attempt to steal intellectual property.

January 2022. Hackers shut down internet traffic to and from North Korea twice in two weeks from what researchers say was likely a series of DDoS attacks. The second attack came just after North Korea's 5th missile test of the month.

January 2022. Hackers breached the Canadian Foreign Ministry, hampering some of the Ministry's internet-connected services. The hack came a day after the government issued a warning to bolster network security in anticipation of Russia-based cyberattacks on critical infrastructure.

January 2022. A series of DDoS attacks targeted a high-stakes Minecraft tournament and ended up impacting Andorra Telecom, the country's only internet service provider. The attack disrupted 4G and internet services for customers.

January 2022. The Informatic Directorate of the Greek Parliament identified an attempt to hack into 60 parliamentary email accounts. In response, authorities temporarily shut down the mailing system in the legislature.

January 2022. An Australian spokesman accused WeChat of taking down Prime Minister Scott Morrison's account and redirecting users to a website that provides information for Chinese expatriates. The Government claims that they first encountered problems posting to the Prime Minister's account in mid-2021.

January 2022. Hackers breached systems belonging to the International Committee of the Red Cross, gaining access to data on more than 500,000 people and disrupting their services around the world. Researchers discovered that the operation may be linked to a sprawling influence operation based in Iran.

January 2022. A cyberattack targeted the Ukrainian government, hitting 90 websites and deploying malicious software masquerading as ransomware to damage dozens of computers in government agencies.

January 2022. Hackers attacked several Israeli media outlets, including Maariv and the Jerusalem Post, posting threatening messages on their websites. One message stated "we are close to you where you do not think about it" in English and Hebrew.

January 2022. A DRPK-affiliated group targeted multiple Russian diplomats with malware. The diplomats received an email disguised as a New Year greetings screensaver but which, after being opened, installed a remote access trojan.

December 2021. A cyberattack on the Belgium Ministry of Defence forced part of its computer network, including the ministry's mail system, to shut down for several days. Hackers exploited

the Log4j vulnerability to compromise the network.

December 2021. Hackers targeted multiple Southeast Asian governments over the past 9 months using custom malware linked to Chinese state-sponsored groups. Many of the nations targeted are currently engaged in disputes with China over territorial claims in the South China Sea.

December 2021. A breach of Prime Minster Modi's Twitter allowed hackers to Tweet from the account that India officially adopted bitcoin as legal tender. The Tweet also included a scam link promising a bitcoin giveaway.

December 2021. A Bloomberg investigation publicly linked an intrusion into Australia's telecommunications systems in 2012 to malicious code embedded in a software update from Huawei.

December 2021. Cybersecurity firms found government-linked hackers from China, Iran, and North Korea attempting to use the Log4j vulnerability to gain access to computer networks. Following the announcement of Log4j, researchers already found over 600,000 attempts to exploit the vulnerability.

December 2021. Chinese hackers breached four more U.S. defense and technology firms in December, in addition to one organization in November. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications.

December 2021. A Russian group took responsivity for a ransomware attack on Australian utility company CS energy. This announcement came after Australian media outlets blamed Chinese government hackers for the attack.

November 2021. A Russian-speaking group targeted the personal information of around 3,500 individuals, including government officials, journalists, and human rights activists. The group obtained access to private email accounts and financial details, and operated malware on Android and Windows devices.

November 2021. Hackers gained access to the social security and driver's license numbers of employees after compromising a U.S. defense contractor.

November 2021. Chinese officials claim a foreign intelligence agency hacked into several airlines in China and stole passenger information. The officials stated the hacks are connected due to the use of a custom trojan in all the attacks.

November 2021. After CISA publicly shared details on a vulnerability, Chinese hackers targeted nine companies and 370 servers between September and October using the same vulnerability.

November 2021. A vendor that handles data for the UK Labour Party was subject to a cyberattack, affecting the data of its members and affiliates.

November 2021. Hackers gained access to the FBI's Law Enforcement Enterprise Portal—a

system used to communicate to state and local officials—and sent a warning of a cyberattack in an email claiming to be from the Department of Homeland Security (DHS).

November 2021. The stock trading platform, Robinhood, disclosed a social engineering cyberattack that allowed a hacker to gain access to the personal information of around 7 million customers. The data included names, email addresses, and for some, data of birth, and zip codes. Following the breach, the hacker requested payment, presumably not to disclose the stolen data.

October 2021. A Chinese-linked hacking group gained access to calling records and text messages from telecommunication carriers across the globe, according to a report from CrowdStrike. The report outlines the group began its cyberattacks in 2016 and infiltrated at least 13 telecommunications networks.

October 2021. A cyberattack targeted the government-issued electronic cards Iranians use to buy subsidized fuel and altered the text of electronic billboards to display anti-regime messages against the Supreme Leader Ayatollah Ali Khamenei.

October 2021. A group with ties to Iran attempted to hack over 250 Office 365 accounts. All the targeted accounts were either U.S. and Israeli defense technology companies, had a focus on Persian Gulf ports of entry, or maritime transportation companies with a presence in the Middle East.

October 2021. Brazilian hackers carried out a cyberattack on the National Malware Center website belonging to Indonesia's State Cyber and Password Agency. The hackers edited the contents of the webpage and indicated that the cyberattack was retribution for an Indonesian hack on the Brazilian state website.

October 2021. Hackers leaked data and photos from the Israeli Defense Ministry after gaining access to 165 servers and 254 websites, overall compiling around 11 terabytes of data.

October 2021. An American company announced that the Russian Foreign Intelligence Service (SVR) launched a campaign targeting resellers and other technology service providers that customize, deploy and manage cloud services.

September 2021. Chinese state-linked hackers targeted Afghan telecom provider Roshan and stole gigabytes of data from their corporate mail server over the past year.

September 2021. The EU formally blamed Russia for its involvement in the 'Ghostwriter' cybercampaign, which targeted the elections and political systems of several member states. Since 2017, Russian operators hacked the social media accounts of government officials and news websites, with the goal of creating distrust in U.S. and NATO forces.

September 2021. Hackers obtained 15 TB of data from 8,000 organizations working with Israel-based company, Voicenter and offered the data online for $1.5 million. Some experts have stipulated the hackers have ties to Iran, but no link has been confirmed.

September 2021. The Lithuanian Defense Ministry found hidden features in popular 5G

smartphone models manufactured in China, according to its state-run cybersecurity body. The module embedded in the phones detects and censors 449 keywords or groups of keywords that are counter to the message of the Chinese government.

September 2021. Two hours after the vote opened for Hungary's opposition primary elections, the polling systems in electoral districts nationwide fell victim to a cyberattack. The actor responsible is still unknown, but the cyberattack led to the government extending voting by two days.

September 2021. The U.S. Department of Justice sentenced Ghaleb Alaumary to more than 11 years in prison for aiding North Korean cybercriminals in money laundering. His assistance included ATM cash-out operations, cyber-enabled bank heists, and business email compromise (BEC) schemes. These attacks targeted banks, professional soccer clubs, and other unnamed companies in the U.S. and U.K.

September 2021. A cyberattack against the United Nations occurred in April 2021, targeting users within the UN network to further long-term intelligence gathering. The hacker was able to access their networks through stolen user credentials purchased on the dark web.

September 2021. The Norwegian Government stated a series of cyberattacks against private and state IT infrastructure came from bad actors sponsored by and operating from China. Their investigation of the hacks claims the actors attempted to capture classified information relating to Norway's national defense and security intelligence.

September 2021. Researchers and cybersecurity experts revealed a mobile espionage campaign against the Kurdish ethnic group. Hackers targeted individuals on Facebook, persuading them to download apps that contain Android backdoors utilized for espionage.

September 2021. In April 2020, Chinese bots swarmed the networks of the Australian government days after Australia called for an independent international probe into the origins of the coronavirus. These bots looked for potential vulnerabilities on the network to exploit in future cyberattacks.

August 2021. A cyberattack on the government of Belarus compromised dozens of police and interior ministry databases. The hack claims to be a part of an attempt to overthrow President Alexander Lukashenko's regime.

August 2021. A hacking group targeted a high-profile Iranian prison, uncovering documents, videos, and images that displayed the violent treatment of its prisoners. The group claims to be hacktivists demanding the release of political prisoners.

August 2021. A cyber-espionage group linked to one of Russia's intelligence forces targeted the Slovak government from February to July 2021 through spear-fishing attempts.

August 2021. Russia targeted and blocked content on "smart voting" app created by Kremlin critic Alexei Navalny and his allies intended to organize voting against the Kremlin in next

month's parliamentary elections.

August 2021. Hacks initially attributed to Iran in 2019 and 2020 were found to be conducted by Chinese operatives. The cyberattack broke into computers across Israel's government and tech companies.

August 2021. A cyberattack on the Covid-19 vaccine-scheduling website for the Italian region of Lazio forced the website to temporarily shut down. New vaccination appointments were unable to be scheduled for several days after the attack.

August 2021. Various Chinese cyber-espionage groups are responsible for the hacks of at least five major Southeast Asian telecommunication providers beginning in 2017. The attacks were carried out by three different hacking groups and are seemingly unlinked despite all groups having a connection to Chinese espionage efforts.

July 2021. Four Chinese nationals targeted companies, universities, and government entities in the United States and abroad between 2011 and 2018. The campaign focused on information of economic benefit to China's commercial sectors.

July 2021. Estonia stated a Tallinn-based hacker downloaded 286,438 ID photos from a government database, exposing a vulnerability in a platform managed by their Information System Authority (RIA).

July 2021. A cyberattack gained access to 1 terabyte of data from the Saudi Arabian Oil Company through a zero-day exploitation. Hackers are offering to delete the data in exchange for $50 million in cryptocurrency.

July 2021. A widespread APT operation was discovered against users in Southeast Asia, believed to be spearheaded by Chinese entities. Researchers found a total of 100 victims in Myanmar and 1,400 in the Philippines, including many government entities.

July 2021. The United States, the European Union, NATO and other world powers released joint statements condemning the Chinese government for a series of malicious cyber activities. They attributed responsibility to China for the Microsoft Exchange hack from early 2021 and the compromise of more than 100,000 servers worldwide.

July 2021. Transnet Port Terminals (TPT), South Africa's state-run ports operator and freight rail monopoly, had its rail services disrupted after a hack by unknown actors. Transnet reportedly declared it an act "force majeure."

July 2021. Unknown hackers compromised the two-factor authentication system used by the Indian government three times, obtaining access to the emails of government officials.

July 2021. Several countries used Pegasus, surveillance software created by NSO Group that targets iPhone and Android operating systems, on devices belonging to activists, politicians, and journalists.

July 2021. The FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a statement exposing a spearfishing campaign by Chinese state-sponsored hackers between 2011 and 2013. The campaign targeted oil and natural gas pipeline companies in the United States.

July 2021. Iran used Facebook accounts to pose as recruiters, journalists, and NGO affiliates, targeting U.S. military personnel. The hackers sent malware-infected files or tricked targets into submitting sensitive credentials to phishing sites.

July 2021. The Russian defense ministry claimed it was hit with a DDoS attack that caused its website to shut down, stating the attack came from outside the Russian Federation.

July 2021. Norway attributed a March 2021 cyberattack on parliament's e-mail system to China.

July 2021. Iran's transport and urbanization ministry was the victim of a cyber attack that impacted display boards at stations throughout the country. The attack caused delays and cancellations of hundreds of trains across Iran.

July 2021. Russian hackers exploited a vulnerability in Kaseya's virtual systems/server administrator (VSA) software allowing them to deploy a ransomware attack on the network. The hack affected around 1,500 small and midsized businesses, with attackers asking for $70 million in payment.

July 2021. The Ukranian Ministry of Defense claimed its naval forces' website was targeted by Russian hackers who published fake reports about the international Sea Breeze-2021 military drills.

June 2021. Russia claimed that Vladimir Putin's annual phone-in session was targeted by DDoS attacks.

June 2021. A Chinese-speaking hacking group spearheaded an ongoing espionage effort against the Afghan government through phishing emails. Hackers posed as the Office of the President of Afghanistan and targeted the Afghan National Security Council.

June 2021. The Iranian government launched a widescale disinformation campaign, targeting WhatsApp groups, Telegram channels and messaging apps used by Israeli activists. The campaign aimed to advance political unrest and distrust in Israel.

June 2021. Chinese actors targeted organizations, including Verizon and the Metropolitan Water District of Southern California using a platform used by numerous government agencies and companies for secure remote access to their networks.

June 2021. Hackers linked to Russia's Foreign Intelligence Service installed malicious software on a Microsoft system that allowed hackers to gain access to accounts and contact information. The majority of the customers targeted were U.S. based, working for IT companies or the government.

June 2021. The U.S. and British governments announced the Russian GRU attempted a series of brute force access against hundreds of government and private sector targets worldwide from 2019 to 2021, targeting organizations using Microsoft Office 365® cloud services.

June 2021. United States Naval Institute (USNI) claimed the tracking data of two NATO ships, the U.K. Royal Navy's HMS Defender and the Royal Netherlands Navy's HNLMS Evertsen, was falsified off the coast of a Russian controlled naval base in the Black Sea. The faked data positioned the two warships at the entrance of a major Russian naval base.

June 2021. A cyberattack reportedly from Russia compromised the email inboxes of more than 30 prominent Polish officials, ministers and deputies of political parties, and some journalists.

June 2021. Sol Oriens, a small government contractor that works for the Department of Energy on nuclear weapons issues, was attacked by the Russia-linked hacking group REvil.

June 2021. A spreadsheet was leaked containing classified personal details of the 1,182 United Kingdom's Special Forces soldiers on WhatsApp.

June 2021. A ransomware attack targeted iConstituent, a newsletter service used by U.S. lawmakers to contact constituents.

June 2021. Hackers working on behalf of Russian intelligence services are believed to have hacked Netherlands police internal network in 2017. The attack occurred during the country's investigation of the Malaysia Airlines Flight 17 (MH17) that was shot down in 2014.

May 2021. LineStar Integrity Services, a pipeline-focused business, was hit by a ransomware attack the same time as the Colonial Pipeline, with 70 gigabytes of its internal files being stolen.

May 2021. A North Korean cyberattack on South Korea's state-run Korea Atomic Energy Research Institute (KAERI) occurred through a vulnerability in a vendor's VPN.

May 2021. The world's largest meat processing company, Brazilian-based JBS, was the victim of a ransomware attack. The attack shut down facilities in the United States, Canada and Australia. The attack was attributed to the Russian speaking cybercrime group, REvil.

May 2021. On May 24th, hackers gained access to Fujitsu's systems and stole files belonging to multiple Japanese government entities. So far four government agencies have been impacted.

May 2021. Cybersecurity researchers identified a North Korean hacking group to be responsible for a cyber espionage campaign, targeting high profile South Korean government officials, utilizing a phishing methodology. The group's targets were based in South Korea and included:

the Korea Internet and Security Agency (KISA), ROK Ministry of Foreign Affairs, Ambassador of the Embassy of Sri Lanka to the State (in ROK), International Atomic Energy Agency Nuclear Security Officer, Deputy Consul General at Korean Consulate General in Hong Kong, Seoul National University, and Daishin Securities.

May 2021. On May 14, Ireland's national health service, the Health Service Executive (HSE), was the victim of a ransomware attack. Upon discovering the attack, government authorities shut down the HSE system. The attackers utilized the Conti ransomware-as-a-service (RaaS), which is reported to be operated by a Russia-based cybercrime group.

May 2021. The FBI and the Australian Cyber Security Centre warned of an ongoing Avaddon ransomware campaign targeting multiple sectors in various countries. The reported targeted countries are Australia, Belgium, Brazil, Canada, China, Costa Rica, Czech Republic, France, Germany, India, Indonesia, Italy, Jordan, Peru, Poland, Portugal, Spain, UAE, UK, US. The targeted industries include: academia, airlines, construction, energy, equipment, financial, freight, government, health, it, law enforcement, manufacturing, marketing, retail, pharmaceutical.

May 2021. On May 6, the Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a $5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.

May 2021. On May 4th and 5th, the Norwegian energy technology company Volue was the victim of a ransomware attack. The attack resulted in the shutdown of water and water treatment facilities in 200 municipalities, affecting approximately 85% of the Norwegian population.

May 2021. A large DDoS attack disabled the ISP used by Belgium's government, impacting more than 200 organizations causing the cancellation of multiple Parliamentary meetings

May 2021. A Chinese hacking group compromised a Russian defense contractor involved in designing nuclear submarines for the Russian navy.

April 2021. A hacking group compromised the social media accounts of Polish officials and used them to disseminate narratives critical of NATO. German authorities have reported that the same group has also attempted to compromise members of the Bundestag and state parliament.

April 2021. Hackers linked to the Chinese military conducted an espionage campaign targeting military and government organizations in Southeast Asia beginning in 2019

April 2021. Malware triggered an outage for airline reservation systems that caused the networks of 20 low-cost airlines around the world to crash.

April 2021. Russian hackers targeted Ukrainian government officials with spearphishing attempts as tensions between the two nations rose during early 2021.

April 2021. Hackers linked to Palestinian intelligence conducted a cyber espionage campaign compromising approximately 800 Palestinian reporters, activists, and dissidents both in Palestine and more broadly across the Middle East.

April 2021. Two state-backed hacking groups—one of which works on behalf of the Chinese government—exploited vulnerabilities in a VPN service to target organizations across the U.S. and Europe with a particular focus on U.S. defense contractors.

April 2021. MI5 warned that over 10,000 UK professional shave been targeted by hostile states over the past five years as part of spearphishing and social engineering campaigns on LinkedIn.

April 2021. Swedish officials disclosed that the Swedish Sports Confederation was hacked by Russian military intelligence in late 2017 and early 2018 in response to accusations of Russian government-sponsored doping of Russian athletes.

April 2021. New York City's Metropolitan Transportation Authority (MTA) was hacked by Chinese-backed actors but were unable to gain access to user data or information systems.

April 2021. French security researchers found that the number of attacks hitting critical French businesses increased fourfold in 2020 during the COVID-19 pandemic.

April 2021. The European Commission announced that the EC and multiple other EU organizations were hit by a major cyberattack by unknown hackers.

April 2021. Chinese hackers launched a months-long cyber espionage campaign during the second half of 2020 targeting government agencies in Vietnam with the intent of gathering political intelligence.

March 2021. China-based hackers breached the networks of the Times of India and transferred data to an off-site server. Researchers believed the hackers aimed to access media sources and gain early knowledge of media investigations and reporting.

March 2021. The North Korean hacking group responsible for a set of attacks on cybersecurity researchers in January 2021 launched a new campaign targeting infosec professionals using fake social media profiles and a fake website for a non-existent security service company target.

March 2021. Suspected Iranian hackers targeted medical researchers in Israel and the U.S. in an attempt to steal the credentials of geneticists, neurologists, and oncologists in the two countries.

March 2021. Suspected Russian hackers stole thousands of emails after breaching the email server of the U.S. State Department.

March 2021. Suspected state hackers targeted the Australian media company Nine Entertainment with a ransomware variant, disrupting live broadcasts and print production systems.

March 2021. Suspected Russian hackers attempted to gain access to the personal email accounts of German parliamentarians in the run-up to Germany's national elections.

March 2021. U.S. Cyber Command confirmed that it was assisting Columbia in responding to election interference and influence operations.

March 2021. The head of U.S. Cyber Command testified that the organization had conducted more than two dozen operations to confront foreign threats ahead of the 2020 U.S. elections, including eleven forward hunt operations in nine different countries.

March 2021. A group of Chinese hackers used Facebook to send malicious links to Uyghur

activists, journalists, and dissidents located abroad.

March 2021. The Indian Computer Emergency Response Team found evidence of Chinese hackers conducting a cyber espionage campaign against the Indian transportation sector.

March 2021. Polish security services announced that suspected Russian hackers briefly took over the websites of Poland's National Atomic Energy Agency and Health Ministry to spread false alerts of a nonexistent radioactive threat.

March 2021. Both Russian and Chinese intelligence services targeted the European Medicines Agency in 2020 in unrelated campaigns, stealing documents relating to COVID-19 vaccines and medicines.

March 2021. Ukraine's State Security Service announced it had prevented a large-scale attack by Russian FSB hackers attempting to gain access to classified government data.

March 2021. Lithuania's State Security Department declared that Russian hackers had targeted top Lithuanian officials in 2020 and used the country's IT infrastructure to carry out attacks against organizations involved in developing a COVID-19 vaccine.

March 2021. Suspected Iranian hackers targeted government agencies, academia, and the tourism industry in Azerbaijan, Bahrain, Israel, Saudi Arabia, and the UAE as part of a cyber espionage campaign.

March 2021. Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.

March 2021. Suspected Chinese hackers targeted electricity grid operators in India in an apparent attempt to lay the groundwork for possible future attacks.

February 2021. A Portuguese-speaking cyber criminal group accessed computer systems at a division of Oxford University researching COVID-19 vaccines, and are suspected to be selling the data they collected to nation states.

February 2021. North Korean hackers targeted defense firms in more than a dozen countries in an espionage campaign starting in early 2020.

February 2021. Hackers associated with the Chinese military conducted a surveillance campaign against Tibetans both in China and abroad.

February 2021. Russian hackers compromised a Ukrainian government file-sharing system and

attempted to disseminate malicious documents that would install malware on computers that downloaded the planted files.

February 2021. Hackers linked to the Vietnamese government conducted a nearly three-year cyber espionage campaign against human rights advocates in the country by using spyware to infiltrate individuals' systems, spy on their activity, and exfiltrate data.

February 2021. Ukrainian officials reported that a multi-day distributed denial-of-service attack against the website of the Security Service of Ukraine was part of Russia's hybrid warfare operations in the country.

February 2021. The US Department of Justice indicted three North Korean hackers for conspiring to steal and extort more than $1.3 billion in cash and cryptocurrencies.

February 2021. Iranian hackers took control of a server in Amsterdam and used it as a command and control center for attacks against political opponents in the Netherlands, Germany, Sweden, and India.

February 2021. North Korean hackers attempted to break into the computer systems of pharmaceutical company Pfizer to gain information about vaccines and treatments for the COVID-19.

February 2021. Suspected Iranian hackers targeted government agencies in the UAE as part of a cyber espionage campaign related to the normalizations of relations with Israel.

February 2021. The French national cybersecurity agency announced that a four-year campaign against French IT providers was the work of a Russian hacking group.

February 2021. Suspected Indian hackers targeted over 150 individuals in Pakistan, Kazakhstan, and India using mobile malware, including those with links to the Pakistan Atomic Energy Commission, the Pakistan Air Force, and election officials in Kashmir.

February 2021. Ten members of a cybercriminal gang were arrested after a campaign where they tricked telecom companies into assigning celebrities' phone numbers to new devices, stealing more than $100 million worth of cryptocurrencies.

February 2021. Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida by a factor of 100 by exploiting a remote access system.

February 2021. Two Iranian hacking groups conducted espionage campaigns against Iranian dissidents in sixteen countries in the Middle East, Europe, South Asia, and North America.

January 2021. Hackers linked to Hezbollah breached telecom companies, internet service

providers, and hosting providers in the US, UK, Egypt, Israel, Lebanon, Jordan, Saudi Arabia, the UAE, and the Palestinian Authority for intelligence gathering and data theft.

January 2021. North Korean government hackers engaged in a sophisticated social engineering campaign against cybersecurity researchers that used multiple fake twitter accounts and a fake blog to drive targets to infected sites or induce them to open infected attachments in emails asking the target to collaborate on a research project.

January 2021. Suspected Indian hackers active since 2012 were attacked business and governments across South and East Asia, with a particular emphasis on military and government organizations in Pakistan, China, Nepal, and Afghanistan, and businesses involved in defense technology, scientific research, finance, energy, and mining.

January 2021. Unidentified hackers breached one of the data centers of New Zealand's central bank.

January 2021. Hackers linked to the Chinese government were responsible for ransomware attacks against five major gaming and gambling countries, demanding over $100 million in ransom.

December 2020. North Korean hackers targeted U.S. pharmaceutical companies Johnson & Johnson and Novavax, both working on experimental vaccines, in an attempt to obtain information on COVID-19.

December 2020. On Christmas Eve, hackers hit the Scottish Environment Protection Agency with a ransomware attack. After deciding not to pay the ransom, the hackers published the data that had been stolen.

December 2020. Iranian state hackers used a Christmas theme for a spearphishing campaign targeting think tanks, research organizations, academics, journalists, and activists in the Persian Gulf, EU, and US.

December 2020. Chinese hackers targeted the Finnish parliament, breaching the email accounts of parliament members and other employees.

December 2020. African Union staff found that Chinese hackers had been siphoning off security footage from cameras installed in the AU headquarters.

December 2020. One Saudi hacking group, One UAE hacking group, and two unknown government-sponsored hacking groups used spyware purchased from the Israeli vendor NSO Group to hack 36 phones belonging to *Al Jazeera* employees.

December 2020. Facebook found that two groups of Russians and one group of individuals

affiliated with the French military were using fake Facebook accounts to conduct dueling political information operations in Africa.

December 2020. More than 40 Israeli companies had data stolen after Iranian hackers compromised a developer of logistics management software and used their access to exfiltrate data from the firm's clients.

December 2020. Unknown state-sponsored hackers took advantage of territory disputes between China, India, Nepal, and Pakistan to target government and military organizations across South Asia, including the Nepali Army and Ministries of Defense and Foreign Affairs, the Sri Lankan Ministry of Defense, and the Afghan National security Council and Presidential Palace.

December 2020. Facebook announced that its users had been targeted by two hacking campaigns, one originating from state-sponsored Vietnamese hackers focused on spreading malware, and the other from two non-profit groups in Bangladesh focused on compromising accounts and coordinating the reporting of accounts and pages for removal.

December 2020. Suspected Chinese hackers targeted government agencies and the National Data Center of Mongolia as part of a phishing campaign.

December 2020. Hackers accessed data related to the COVID-19 vaccine being developed by Pfizer during an attack on the European Medicines Agency.

December 2020. Over 200 organizations around the world—including multiple US government agencies—were revealed to have been breached by Russian hackers who compromised the software provider SolarWinds and exploited their access to monitor internal operations and exfiltrate data.

December 2020. A criminal group targeted the Israeli insurance company Shirbit with ransomware, demanding almost $1 million in bitcoin. The hackers published some sensitive personal information after making their demands and threatened to reveal more if they did not receive payment.

December 2020. CISA and the FBI announced that U.S. think tanks focusing on national security and international affairs were being targeted by state-sponsored hacking groups.

December 2020. Suspected state-sponsored hackers from an unknown country conducted a spear phishing campaign against organizations in six countries involved in providing special temperature-controlled environments to support the COVID-19 supply chain.

November 2020. In 2020, two apps were banned from the Google Play Store after cybersecurity researchers discovered that a software development kit developed by the Chinese internet giant Baidu had sent sensitive data on hundreds of millions of users to Chinese servers.

November 2020. A Mexican facility owned by Foxconn was hit by a ransomware attack that the hackers claim resulted in 1,200 servers being encrypted, 20-30 TB of backups being deleted, and

100 GB of encrypted files being stolen.

November 2020. North Korean hackers targeted COVID-19 vaccine developer AstraZeneca by posing as recruiters and sending the company's employees fake job offers that included malware.

November 2020. Chinese hackers targeted Japanese organizations in multiple industry sectors located in multiple regions around the globe, including North America, Europe, Asia, and the Middle East.

November 2020. Suspected Chinese government hackers conducted a cyber espionage campaign from 2018 to 2020 targeting government organizations in Southeast Asia.

November 2020. A North Korean hacking group engaged in software supply chain attacks against South Korean internet users by compromising legitimate South Korean security software.

November 2020. One Russian and two North Korean hacking groups launched attacks against seven companies involved in COVID-19 vaccine research.

November 2020. A group of hackers for hire launched attacks against a group of targets in South Asia, and particularly India, Bangladesh, and Singapore. These attacks included the use of a custom backdoor and credential theft.

November 2020. A group of Vietnamese hackers created and maintained a number of fake websites devoted to news and activism in Southeast Asia that were used to profile users, re-direct to phishing pages, and distribute malware.

November 2020. U.S. Cyber Command and the NSA conducted offensive cyber operations against Iran to prevent interference in the upcoming U.S. elections.

November 2020. Hamas used a secret headquarters in Turkey to carry out cyberattacks and counter-intelligence operations.

October 2020. Hackers targeted an Indian pharmaceutical company and compromised intellectual property. In response, the company isolated all data centers and closed plants in the U.S., UK, Brazil, India, and Russia.

October 2020. The U.S. government announces that Iranian hackers targeted state election websites in order to download voter registration information and conduct a voter intimidation campaign

October 2020. A spokesperson for China's Foreign Ministry responded to accusations that Chinese state-sponsored hackers were targeting the U.S. defense industrial base by declaring that the United States was an "empire of hacking," citing 2013 leaks about the NSA's Prism program.

October 2020. India's National Cyber Security Coordinator announced that cyber crimes in India

cost almost $17 billion in 2019.

October 2020. A Russian cyber espionage group hacked into an unidentified European government organization

October 2020. Iranian hackers targeted attendees of the Munich Security Conference in order to gather intelligence on foreign policy from the compromised individuals

October 2020. Greek hackers defaced the website of the Turkish Parliament and 150 Azerbaijani government websites in support of Armenia.

October 2020. The FBI, CISA and U.S. Cyber Command announced that a North Korean hacking group had been conducting a cyber espionage campaign against individual experts, think tanks, and government entities in South Korea, Japan, and the United States with the purpose of collecting intelligence on national security issues related to the Korean peninsula, sanctions, and nuclear policy

October 2020. The FBI and CISA announced that a Russian hacking group breached U.S. state and local government networks, as well as aviation networks, and exfiltrated data

October 2020. A North Korean hacker group carried out attacks against aerospace and defense companies in Russia.

October 2020. An Iranian hacking group conducted a phishing campaign against universities in Australia, Canada, the UK, the U.S., the Netherlands, Singapore, Denmark, and Sweden.

October 2020. Suspected Iranian hackers targeted government agencies and telecommunications operators in Iraq, Kuwait, Turkey, and the UAE as part of a cyber espionage campaign

October 2020. The NSA warned that Chinese government hackers were targeting the U.S. defense industrial base as part of a wide-ranging espionage campaign

October 2020. The UK's National Cyber Security Centre found evidence that Russian military intelligence hackers had been planning a disruptive cyber attack on the later-postponed 2020 Tokyo Olympics.

October 2020. The U.S. indicted six Russian GRU officers for their involvement in hacking incidents including the 2015 and 2016 attacks on Ukrainian critical infrastructure, the 2017 NotPetya ransomware outbreak, election interference in the 2017 French elections, and others.

October 2020. Iran announced that the country's Ports and Maritime Organization and one other unspecified government agency had come under cyberattack

October 2020. Microsoft and U.S. Cyber Command both independently undertook operations to take down a Russian botnet ahead of the U.S. election.

October 2020. The U.S. Department of Homeland Security revealed that hackers targeted the U.S. Census Bureau in a possible attempt to collect bulk data, alter registration information, compromise census infrastructure, or conduct DoS attacks

October 2020. U.S. government officials revealed that suspected Chinese hackers were behind a series of attacks on entities in Russia, India, Ukraine, Kazakhstan, Kyrgyzstan, and Malaysia

October 2020. A Chinese group targeted diplomatic entities and NGOs in Africa, Asia, and Europe using advanced malware adapted from code leaked by the Italian hacking tool vendor HackingTeam

October 2020. Iranian hackers exploited a serious Windows vulnerability to target Middle Eastern network technology providers and organizations involved in work with refugees.

October 2020. A cyber mercenary group targeted government officials and private organizations in South Asia and the Middle East using a combination of methods including zero-day exploits.

October 2020. In the midst of escalating conflict between Armenia and Azerbaijan over the territory of Nagorno-Karabakh, an unknown intelligence service conducted a cyber espionage campaign targeting Azerbaijani government institutions.

October 2020. A previously unknown cyber espionage group was found to have been stealing documents from government agencies and corporations in Eastern Europe and the Balkans since 2011.

October 2020. The UN shipping agency the International Maritime Organization (IMO) reported that its website and networks had been disrupted by a sophisticated cyber attack.

October 2020. North Korean hackers targeted a ministry of health and a pharmaceutical company involved in COVID-19 research and response.

September 2020. American healthcare firm Universal Health Systems sustained a ransomware attack that caused affected hospitals to revert to manual backups, divert ambulances, and reschedule surgeries

September 2020. French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks, though did not affect the moving of cargo

September 2020. Russian hackers targeted government agencies in NATO member countries, and nations who cooperate with NATO. The campaign uses NATO training material as bait for a phishing scheme that infects target computers with malware that creates a persistent backdoor.

September 2020. Chinese hackers stole information related to Covid-19 vaccine development from Spanish research centers

September 2020. Iranian hackers targeted Iranian minorities, anti-regime organizations, and resistance members using a combination of malware including an Android backdoor designed to steal two factor authentication codes from text messages.

September 2020. Three hackers operating at the direction of Iran's Islamic Revolutionary Guard Corps were indicted by the United States for attacks against workers at aerospace and satellite technology companies, as well as international government organizations.

September 2020. A ransomware attack on a German hospital may have led to the death of a patient who had to be redirected to a more distant hospital for treatment.

September 2020. The U.S. Department of Justice indicted five Chinese hackers with ties to Chinese intelligence services for attacks on more than 100 organizations across government, IT, social media, academia, and more

September 2020. The FBI and CISA announced that Iranian hackers had been exploiting publicly known vulnerabilities to target U.S. organizations in the IT, government, healthcare, finance, and media sectors.

September 2020. CISA revealed that hackers associated with the Chinese Ministry of State Security had been scanning U.S. government and private networks for over a year in search of networking devices that could be compromised using exploits for recently discovered vulnerabilities

September 2020. One government organization in the Middle East and one in North Africa were targeted with possible wiper malware that leveraged a ransomware-as-a-service offering that has recently become popular on cybercrime markets

September 2020. Georgian officials announce that COVID-19 research files at a biomedical research facility in Tbilisi was targeted as part of a cyberespionage campaign

September 2020. Norway announced it had defended against two sets of cyber attacks that targeted the emails of several members and employees of the Norwegian parliament as well as public employees in the Hedmark region. It later blamed Russia for the attack.

August 2020. A North Korean hacking group targeted 28 UN officials in a spear-phishing campaign, including at least 11 individuals representing six members of the UN Security Council.

August 2020. Hackers for hire suspected of operating on behalf of the Iranian government were found to have been working to gain access to sensitive information held by North American and Israeli entities across a range of sectors, including technology, government, defense, and healthcare.

August 2020. New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by unknown actors

August 2020. U.S. officials announced that North Korean government hackers had been operating a campaign focused on stealing money from ATMs around the world.

August 2020. Suspected Pakistani hackers used custom malware to steal files from victims in twenty-seven countries, most prominently in India and Afghanistan.

August 2020. Ukrainian officials announced that a Russian hacking group had begun to conduct a phishing campaign in preparations for operations on Ukraine's independence day

August 2020. Taiwan accused Chinese hackers of infiltrating the information systems of at least ten government agencies and 6,000 email accounts to gain access to citizens' personal data and government information.

August 2020. A Chinese cyber espionage group targeted military and financial organizations across Eastern Europe

August 2020. The Israeli defense ministry announced that it had successfully defended against a cyberattack on Israeli defense manufacturers launched by a suspected North Korean hacking group

August 2020. An Iranian hacking group was found to be targeting major U.S. companies and government agencies by exploiting recently disclosed vulnerabilities in high-end network equipment to create backdoors for other groups to use

August 2020. Pakistan announced that hackers associated with Indian intelligence agencies had targeted the mobile phones of Pakistani government officials and military personnel

August 2020. Seven semiconductor vendors in Taiwan were the victim of a two-year espionage campaign by suspected Chinese state hackers targeting firms' source code, software development kits, and chip designs.

August 2020. Russian hackers compromised news sites and replaced legitimate articles with falsified posts that used fabricated quotes from military and political officials to discredit NATO among Polish, Lithuanian, and Latvian audiences.

July 2020. Israel announced that two cyber attacks had been carried out against Israeli water infrastructure, though neither were successful

July 2020. Chinese state-sponsored hackers broke into the networks of the Vatican to conduct espionage in the lead-up to negotiations about control over the appointment of bishops and the status of churches in China.

July 2020. Canada, the UK, and the U.S. announced that hackers associated with Russian intelligence had attempted to steal information related to COVID-19 vaccine development

July 2020. The UK announced that it believed Russia had attempted to interfere in its 2019 general election by stealing and leaking documents related to the UK-US Free Trade Agreement

July 2020. Media reports say a 2018 Presidential finding authorized the CIA to conduct cyber operations against Iran, North Korea, Russia, and China. The operations included disruption and public leaking of information.

July 2020. President Trump confirmed that he directly authorized a 2019 operation by US Cyber Command taking the Russian Internet Research Agency offline.

June 2020. Uyghur and Tibetan mobile users were targeted by a mobile malware campaign originating in China that had been ongoing since 2013

June 2020. A hacking group affiliated with an unknown government was found to have targeted a range of Kurdish individuals in Turkey and Syria at the same time as Turkey launched its offensive into northeastern Syria.

June 2020. The most popular of the tax reporting software platforms China requires foreign companies to download to operate in the country was discovered to contain a backdoor that could allow malicious actors to conduct network reconnaissance or attempt to take remote control of company systems

June 2020. Nine human rights activists in India were targeted as part of a coordinated spyware campaign that attempted to use malware to log their keystrokes, record audio, and steal credentials

June 2020. A Moroccan journalist was targeted by unknown actors who sent him phishing messages that could have been used to download spyware developed by Israeli NSO group

June 2020. North Korean state hackers sent COVID-19-themed phishing emails to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India, and the UK in an attempt to steal personal and financial data

June 2020. The Australian Prime Minister announced that an unnamed state actor had been targeting businesses and government agencies in Australia as part of a large-scale cyber attack.

June 2020. In the midst of escalating tensions between China and India over a border dispute in the Galwan Valley, Indian government agencies and banks reported being targeted by DDoS attacks reportedly originating in China

June 2020. Suspected North Korean hackers compromised at least two defense firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defense contractors

May 2020. Businesses in Japan, Italy, Germany, and the UK that supply equipment and software

to industrial firms were attacked in a targeted and highly sophisticated campaign by an unknown group of hackers

May 2020. The NSA announced that Russian hackers associated with the GRU had been exploiting a bug that could allow them to take remote control of U.S. servers

May 2020. German officials found that a Russian hacking group associated with the FSB had compromised the networks of energy, water, and power companies in Germany by compromising the firms' suppliers.

May 2020. Cyber criminals managed to steal $10 million from Norway's state investment fund in a business email compromise scam that tricked an employee into transferring money into an account controlled by the hackers

May 2020. Iranian hackers conducted a cyber espionage campaign targeting air transportation and government actors in Kuwait and Saudi Arabia.

May 2020. Chinese hackers accessed the travel records of nine million customers of UK airline group EasyJet

May 2020. Two days before Taiwanese President Tsai Ing-wen was sworn in for her second term in office, the president's office was hacked, and files were leaked to local media outlets purporting to show infighting within the administration. The president's office claimed the leaked documents had been doctored.

May 2020. U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine

May 2020. Suspected Chinese hackers conducted a phishing campaign to compromise Vietnamese government officials involved in ongoing territorial disputes with China in the South China Sea.

May 2020. Suspected Iranian hackers compromised the IT systems of at least three telecom companies in Pakistan, and used their access to monitor targets in the country.

May 2020. Japan's Defense Ministry announced it was investigating a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.

May 2020. Israeli hackers disrupted operations at an Iranian port for several days, causing massive backups and delays. Officials characterized the attack as a retaliation against a failed Iranian hack in April targeting the command and control systems of Israeli water distribution systems.

May 2020. A suspected PLA hacking group targeted government-owned companies, foreign affairs ministries, and science and technology ministries across Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei.

May 2020. Operations at two Taiwanese petrochemical companies were disrupted by malware attacks. Taiwanese officials speculated that the attacks could have been linked to the upcoming inauguration of Taiwanese President Tsai Ing-wen's second term.

April 2020. Suspected Vietnamese government hackers used malicious apps uploaded to the Google Play app store to infect users in South and Southeast Asia with spyware capable of monitoring the target's call logs, geolocation data, and text messages.

April 2020. Poland suggested the Russian government was being behind a series of cyber attacks on Poland's War Studies University meant to advance a disinformation campaign undermining U.S.-Polish relations.

April 2020. Suspected Iranian hackers unsuccessfully targeted the command and control systems of water treatment plants, pumping stations, and sewage in Israel.

April 2020. U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.

April 2020. Suspected Vietnamese hackers targeted the Wuhan government and the Chinese Ministry of Emergency Management to collect information related to China's COVID-19 response.

April 2020. Government and energy sector entities in Azerbaijan were targeted by an unknown group focused on the SCADA systems of wind turbines

April 2020. A Russian hacking group used forged diplomatic cables and planted articles on social media to undermine the governments of Estonia and the Republic of Georgia

April 2020. Suspected state-sponsored hackers targeted Chinese government agencies and Chinese diplomatic missions abroad by exploiting a zero-day vulnerability in virtual private networks servers

April 2020. Iranian government-backed hackers attempted to break into the accounts of WHO staffers in the midst of the Covid-19 pandemic

March 2020. North Korean hackers targeted individuals involved with North Korean refugees issues as part of a cyber espionage campaign

March 2020. Suspected South Korean hackers were found to have used five previously unreported software vulnerabilities to conduct a wide-ranging espionage campaign against North Korean targets

March 2020. Saudi mobile operators exploited a flaw in global telecommunications infrastructure to track the location of Saudis traveling abroad

March 2020. Chinese hackers targeted over 75 organizations around the world in the manufacturing, media, healthcare, and nonprofit sectors as part of a broad-ranging cyber

espionage campaign

March 2020. A suspected nation state hacking group was discovered to be targeting industrial sector companies in Iran

March 2020. Human rights activists and journalists in Uzbekistan were targeted by suspected state security hackers in a spearphishing campaign intended install spyware on their devices

March 2020. Chinese cybersecurity firm Qihoo 360 accused the CIA of being involved in an 11-year long hacking campaign against Chinese industry targets, scientific research organizations, and government agencies

February 2020. The U.S. Department of Justice indicted two Chinese nationals for laundering cryptocurrency for North Korean hackers

February 2020. Mexico's economy ministry announced it had detected a cyber attack launched against the ministry's networks, but that no sensitive data had been exposed.

February 2020. The U.S. Defense Information Systems Agency announced it had suffered a data breach exposing the personal information of an unspecified number of individuals

February 2020. A hacking group of unknown origin was found to be targeting government and diplomatic targets across Southeast Asia as part of a phishing campaign utilizing custom malware

February 2020. Chinese hackers targeted Malaysian government officials to steal data related to government-backed projects in the region.

February 2020. Iran announced that it has defended against a DDoS against its communications infrastructure that caused internet outages across the country

January 2020. An Iranian hacking group launched an attack on the U.S. based research company Wesat as part of a suspected effort to gain access to the firm's clients in the public and private sectors

January 2020. The UN was revealed to have covered up a hack into its IT systems in Europe conducted by an unknown but sophisticated hacking group.

January 2020. Turkish government hackers targeted at least 30 organizations across Europe and the Middle East, including government ministries, embassies, security services, and companies.

January 2020. Mitsubishi announces that a suspected Chinese group had targeted the company as part of a massive cyberattack that compromised personal data of 8,000 individuals as well as information relating to partnering businesses and government agencies, including projects relating to defense equipment.

January 2020. The FBI announced that nation state hackers had breached the networks of two U.S. municipalities in 2019, exfiltrating user information and establishing backdoor access for future compromise

January 2020. A Russian hacking group infiltrated a Ukrainian energy company where Hunter Biden was previously a board member, and which has featured prominently in the U.S. impeachment debate.

January 2020. More than two dozen Pakistani government officials had their mobile phones infected with spyware developed by the Israeli NSO Group

January 2020. A suspected nation state targeted the Austrian foreign ministry as part of a cyber attack lasting several weeks.

December 2019. Iranian wiper malware was deployed against the network of Bapco, the national oil company of Bahrain.

December 2019. Microsoft won a legal battle to take control of 50 web domains used by a North Korean hacking group to target government employees, think tank experts, university staff, and others involved in nuclear proliferation issues

December 2019. An alleged Chinese state-sponsored hacking group attacked government entities and managed service providers by bypassing the two-factor authentication used by their targets

December 2019. Chinese hackers used custom malware to target a Cambodian government organization

December 2019. Unknown hackers stole login credentials from government agencies in 22 nations across North America, Europe, and Asia

December 2019. Iran announced that it had foiled a major cyber attack by a foreign government targeting the country's e-government infrastructure

December 2019. A suspected Vietnamese state-sponsored hacking group attacked BMW and Hyundai networks

December 2019. Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and nongovernmental organizations in a spear phishing campaign

November 2019. A Russian-speaking hacking group targeted a wide range of Kazakh individuals and organizations including government agencies, military personnel, foreign diplomats, journalists, dissidents, and others through a combination of spear phishing and physical device compromise.

November 2019. Microsoft security researchers found that in the last year, an Iranian hacker group carried out "password-spraying attacks" on thousands of organizations, but since October, have focused on the employees of dozens of manufacturers, suppliers, or maintainers of industrial control system equipment and software.

November 2019. An alleged non-state actor targeted the UK Labour party with a major DDoS

attack that temporarily took the party's computer systems offline.

October 2019. An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp.

October 2019. A state-sponsored hacking campaign knocked offline more than 2,000 websites across Georgia, including government and court websites containing case materials and personal data. More than 20 countries later attributed the attack to Russia.

October 2019. India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant.

October 2019. Suspected North Korean hackers attempted to steal credentials from individuals working on North Korea-related issues at the UN and other NGOs.

October 2019. The NSA and GCHQ found that a Russian cyberespionage campaign had used an Iranian hacking group's tools and infrastructure to spy on Middle Eastern targets.

October 2019. Russian hackers engaged in a campaign since 2013 targeting embassies and foreign affairs ministries in several European countries.

October 2019. Iranian hackers targeted more than 170 universities around the world between 2013 and 2017, stealing $3.4 billion worth of intellectual property and selling stolen data to Iranian customers.

October 2019. Chinese hackers engaged in a multi-year campaign between 2010 and 2015 to acquire intellectual property from foreign companies to support the development of the Chinese C919 airliner.

October 2019. A Chinese government-sponsored propaganda app with more than 100 million users was found to have been programmed to have a backdoor granting access to location data, messages, photos, and browsing history, as well as remotely activate audio recordings.

October 2019. The Moroccan government targeted two human rights activists using spyware purchased from Israel.

October 2019. A state-sponsored hacking group targeted diplomats and high-profile Russian speaking users in Eastern Europe.

October 2019. Chinese hackers targeted entities in Germany, Mongolia, Myanmar, Pakistan, and Vietnam, individuals involved in UN Security Council resolutions regarding ISIS, and members of religious groups and cultural exchange nonprofits in Asia.

October 2019. Iranian hackers conducted a series of attacks against the Trump campaign, as well as current and former U.S. government officials, journalists, and Iranians living abroad.

October 2019. State-sponsored Chinese hackers were revealed to have conducted at least six

espionage campaigns since 2013 against targets in Myanmar, Taiwan, Vietnam, Indonesia, Mongolia, Tibet, and Xinjiang.

October 2019. The Egyptian government conducted a series of cyberattacks against journalists, academics, lawyers, human rights activists, and opposition politicians.

October 2019. Chinese hackers were found to have targeted government agencies, embassies, and other government-related embassies across Southeast Asia in the first half of 2019.

September 2019. The United States carried out cyber operations against Iran in retaliation for Iran's attacks on Saudi Arabia's oil facilities. The operation affected physical hardware, and had the goal of disrupting Iran's ability to spread propaganda.

September 2019. Airbus revealed that hackers targeting commercial secrets engaged in a series of supply chain attacks targeting four of the company's subcontractors.

September 2019. A Chinese state-sponsored hacking group responsible for attacks against three U.S. utility companies in July 2019 was found to have subsequently targeted seventeen others.

September 2019. Hackers with ties to the Russian government conducted a phishing campaign against the embassies and foreign affairs ministries of countries across Eastern Europe and Central Asia.

September 2019. Alleged Chinese hackers used mobile malware to target senior Tibetan lawmakers and individuals with ties to the Dalai Lama.

September 2019. North Korean hackers were revealed to have conducted a phishing campaign over the summer of 2019 targeted U.S. entities researching the North Korean nuclear program and economic sanctions against North Korea.

September 2019. Iranian hackers targeted more than 60 universities in the U.S., Australia, UK, Canada, Hong Kong, and Switzerland in an attempt to steal intellectual property.

September 2019. Huawei accused the U.S. government of hacking into its intranet and internal information systems to disrupt its business operations.

August 2019. China used compromised websites to distribute malware to Uyghur populations using previously undisclosed exploits for Apple, Google, and Windows phones.

August 2019. Chinese state-sponsored hackers were revealed to have targeted multiple U.S. cancer institutes to take information relating to cutting edge cancer research.

August 2019. North Korean hackers conducted a phishing campaign against foreign affairs officials in at least three countries, with a focus on those studying North Korean nuclear efforts and related international sanctions.

August 2019. Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications.

August 2019. The Czech Republic announced that the country's Foreign Ministry had been the victim of a cyberattack by an unspecified foreign state, later identified as Russia

August 2019. A suspected Indian cyber espionage group conducted a phishing campaign targeting Chinese government agencies and state-owned enterprises for information related to economic trade, defense issues, and foreign relations.

August 2019. Networks at several Bahraini government agencies and critical infrastructure providers were infiltrated by hackers linked to Iran

August 2019. A previously unidentified Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies and the monitoring of dissidents in Hong Kong.

August 2019. Russian hackers were observed using vulnerable IoT devices like a printer, VOIP phone, and video decoder to break into high-value corporate networks

August 2019. A seven-year campaign by an unidentified Spanish-language espionage group was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army

July 2019. State-sponsored Chinese hackers conducted a spear-phishing campaign against employees of three major U.S. utility companies

July 2019. Capital One reveals that a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers.

July 2019. Encrypted email service provider ProtonMail was hacked by a state-sponsored group looking to gain access to accounts held by reporters and former intelligence officials conducting investigations of Russian intelligence activities.

July 2019. Several major German industrial firms including BASF, Siemens, and Henkel announced that they had been the victim of a state-sponsored hacking campaign reported to be linked to the Chinese government

July 2019. A Chinese hacking group was discovered to have targeted government agencies across East Asia involved in information technology, foreign affairs, and economic development.

July 2019. The U.S. Coast Guard issued a warning after it received a report that a merchant vessel had its networks disrupted by malware while traveling through international waters

July 2019. An Iranian hacking group targeted LinkedIn users associated with financial, energy, and government entities operating in the Middle East

July 2019. Microsoft revealed that it had detected almost 800 cyberattacks over the past year

targeting think tanks, NGOs, and other political organizations around the world, with the majority of attacks originating in Iran, North Korean, and Russia.

July 2019. Libya arrested two men who were accused of working with a Russian troll farm to influence the elections in several African countries.

July 2019. Croatian government agencies were targeted in a series of attacks by unidentified state sponsored hackers

July 2019. U.S. Cybercommand issued an alert warning that government networks were being targeted with malware associated with a known Iran-linked hacking group

June 2019. Western intelligence services were alleged to have hacked into Russian internet search company Yandex in late 2018 to spy on user accounts

June 2019. Over the course of seven years, a Chinese espionage group hacked into ten international cellphone providers operating across thirty countries to track dissidents, officials, and suspected spies.

June 2019. The U.S. announced it had launched offensive cyber operations against Iranian computer systems used to control missile and rocket launches.

June 2019. Iran announced that it had exposed and helped dismantle an alleged CIA-backed cyber espionage network across multiple countries

June 2019. U.S. officials reveal ongoing efforts to deploy hacking tools against Russian grid systems as a deterrent and warning to Russia

June 2019. U.S. grid regulator NERC issued a warning that a major hacking group with suspected Russian ties was conducting reconnaissance into the networks of electrical utilities.

June 2019. China conducted a denial-of-service attack on encrypted messaging service Telegram in order to disrupt communications among Hong Kong protestors

June 2019. A suspected Iranian group was found to have hacked into telecommunications services in Iraq, Pakistan, and Tajikistan

June 2019. Chinese intelligence services hacked into the Australian University to collect data they could use to groom students as informants before they were hired into the civil service.

May 2019. Government organizations in two different Middle Eastern countries were targeted by Chinese state-sponsored hackers.

May 2019. A Chinese government-sponsored hacking group was reported to be targeting unidentified entities across the Philippines.

May 2019. Iran developed a network of websites and accounts that were being used to spread false information about the U.S., Israel, and Saudi Arabia.

May 2019. The Israeli Defense Forces launched an airstrike on the Hamas after they unsuccessfully attempted to hack Israeli targets.

May 2019. Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked.

April 2019. Amnesty International's Hong Kong office announced it had been the victim of an attack by Chinese hackers who accessed the personal information of the office's supporters.

April 2019. Ukrainian military and government organizations had been targeted was part of a campaign by hackers from the Luhansk People's Republic, a Russia-backed group that declared independence from Ukraine in 2014.

April 2019. Chinese hackers stole General Electric's trade secrets concerning jet engine turbine technologies

April 2019. Hackers used spoofed email addresses to conduct a disinformation campaign in Lithuania to discredit the Defense Minister by spreading rumors of corruption.

April 2019. The Finnish police probed a denial-of-service attack against the web service used to publish the vote tallies from Finland's elections.

April 2019. Iranian hackers reportedly undertook a hacking campaign against banks, local government networks, and other public agencies in the UK.

April 2019. Pharmaceutical company Bayer announced it had prevented an attack by Chinese hackers targeting sensitive intellectual property.

March 2019. Chinese hackers targeted Israeli defense firms that had connections to the U.S. military

March 2019. The U.S. Department of Energy reported that grid operators in Los Angeles County, California and Salt Lake County, Utah, suffered a DDoS attack that disrupted their operations, but did not cause any outages

March 2019. The Australian Signals Directorate revealed that it had conducted cyber attacks against ISIS targets in the Middle East to disrupt their communications in coordination with coalition forces.

March 2019. An Iranian cyber espionage group targeted government and industry digital infrastructure in Saudi Arabia and the U.S.

March 2019. State supported Vietnamese hackers targeted foreign automotive companies to acquire IP.

March 2019. Iran's intelligence service hacked into former IDF Chief and Israeli opposition leader Benny Gantz' cellphone ahead of Israel's April elections.

March 2019. North Korean hackers targeted an Israeli security firm as part of an industrial espionage campaign.

March 2019. Russian hackers targeted a number of European government agencies ahead of EU elections in May.

March 2019. Indonesia's National Election Commission reported that Chinese and Russian hackers had probed Indonesia's voter database ahead of presidential and legislative elections in the country.

March 2019. Civil liberties organizations claimed that government-backed hackers targeted Egyptian human rights activists, media, and civil society organizations throughout 2019.

March 2019. The UN Security Council reported that North Korea has used state-sponsored hacking to evade international sanctions, stealing $670 million in foreign currency and cryptocurrency between 2015 and 2018.

March 2019. Iranian hackers targeted thousands of people at more than 200 oil-and-gas and heavy machinery companies across the world, stealing corporate secrets and wiping data from computers.

March 2019. Following an attack on Indian military forces in Kashmir, Pakistani hackers targeted almost 100 Indian government websites and critical systems. Indian officials reported that they engaged in offensive cyber measures to counter the attacks.

March 2019. U.S. officials reported that at least 27 universities in the U.S. had been targeted by Chinese hackers as part of a campaign to steal research on naval technologies.

February 2019. The UN International Civil Aviation Organizations revealed that in late 2016 it was compromised by China-linked hackers who used their access to spread malware to foreign government websites.

February 2019. Prior to the Vietnam summit of Kim Jong Un and Donald Trump, North Korean hackers were found to have targeted South Korean institutions in a phishing campaign using documents related to the diplomatic event as bait.

February 2019. U.S. Cybercommand revealed that during the 2018 U.S. midterm elections, it had blocked internet access to the Internet Research Agency, a Russian company involved in information operations against the U.S. during the 2016 presidential election.

February 2019. A hacking campaign targeted Russian companies linked to state-sponsored North Korean hackers.

February 2019. Hackers associated with the Russian intelligence services had targeted more than 100 individuals in Europe at civil society groups working on election security and democracy promotion.

February 2019. State-sponsored hackers were caught in the early stages of gaining access to

computer systems of several political parties as well as the Australian Federal Parliament.

February 2019. European aerospace company Airbus reveals it was targeted by Chinese hackers who stole the personal and IT identification information of some of its European employees.

February 2019. Norwegian software firm Visma revealed that it had been targeted by hackers from the Chinese Ministry of State Security who were attempting to steal trade secrets from the firm's clients.

January 2019. Hackers associated with the Russian intelligence services were found to have targeted the Center for Strategic and International Studies.

January 2019. The U.S. Department of Justice announced an operation to disrupt a North Korean botnet that had been used to target companies in the media, aerospace, financial, and critical infrastructure sectors.

January 2019. France attributed a cyberattack targeting the Ministry of Defense to a Russian-based hacking group. The attack targeted the mailboxes of nineteen executives of the ministry.

January 2019. Former U.S. intelligence personnel were revealed to be working for the UAE to help the country hack into the phones of activists, diplomats, and foreign government officials

January 2019. U.S. prosecutors unsealed two indictments against Huawei and its CFO Meng Wanzhou alleging crimes ranging from wire and bank fraud to obstruction of justice and conspiracy to steal trade secrets

January 2019. Security researchers reveal that Iranian hackers have been targeting the telecom and travel industries since at least 2014 in an attempt to surveil and collect the personal information of individuals in the Middle East, U.S., Europe, and Australia

January 2019. The U.S. Democratic National Committee revealed that it had been targeted by Russian hackers in the weeks after the 2018 midterm elections

January 2019. South Korea's Ministry of National Defense announced that unknown hackers had compromised computer systems at the ministry's procurement office

January 2019. The U.S. Securities and Exchange Commission charged a group of hackers from the U.S., Russia, and Ukraine with the 2016 breach of the SEC's online corporate filing portal exploited to execute trades based on non-public information

January 2019. Iran was revealed to have engaged in a multi-year, global DNS hijacking campaign targeting telecommunications and internet infrastructure providers as well as government entities in the Middle East, Europe, and North America.

January 2019. Hackers release the personal details, private communications, and financial information of hundreds of German politicians, with targets representing every political party except the far-right AfD.

December 2018. Chinese hackers stole IP and confidential business and technological information from managed service providers – companies that manage IT infrastructure for other businesses and governments

December 2018. North Korean hackers targeted the Chilean interbank network after tricking an employee into installing malware over the course of a fake job interview

December 2018. Chinese hackers were found to have compromised the EU's communications systems, maintaining access to sensitive diplomatic cables for several years

December 2018. North Korean hackers stole the personal information of almost 1,000 North Korean defectors living in South Korea

December 2018. The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China for conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.

December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

December 2018. Security researchers discover a cyber campaign carried out by a Russia-linked group targeting the government agencies of Ukraine as well as multiple NATO members

December 2018. Researchers report that a state-sponsored Middle Eastern hacking group had targeted telecommunications companies, government embassies, and a Russian oil company located across Pakistan, Russia, Saudi Arabia, Turkey, and North America

December 2018. Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company's servers and personal computers in the UAE, Saudi Arabia, Scotland, and India

December 2018. North Korean hackers have reportedly targeted universities in the U.S. since May, with a particular focus on individuals with expertise in biomedical engineering

December 2018. The Security Service of Ukraine blocked an attempt by the Russian special services to disrupt the information systems of Ukraine's judicial authority

December 2018. The Czech security service announced that Russian intelligence services were discovered to have been behind attacks against the Czech foreign ministry in 2017

December 2018. Secretary of State Mike Pompeo confirmed that Chinese hackers breached the systems of an American hotel chain, stealing the personal information of over 500 million customers

November 2018. German security officials announced that a Russia-linked group had targeted the email accounts of several members of the German parliament, as well as the German military and several embassies

November 2018. Security researchers report that Russia launched coordinated cyber attacks against Ukrainian government and military targets before and during the attack on Ukrainian ships in late November

November 2018. Researchers reveal that a Mexican government-linked group used spyware to target the colleagues of a slain journalist investigating drug cartels

November 2018. Security researchers discover a cyberespionage campaign targeting government websites of Lebanon and the UAE

November 2018. The U.S. Justice Department indicted two Iranians for the ransomware attack affecting Atlanta's government earlier in 2018

November 2018. Chinese state media reports that the country had been the victim of multiple attacks by foreign hackers in 2018, including the theft of confidential emails, utility design plans, lists of army units, and more

November 2018. North Korean hackers were found to have used malware to steal tens of millions of dollars from ATMs across Asia and Africa

November 2018. Security researchers report that Russian hackers impersonating U.S. State Department officials attempted to gain access to the computer systems of military and law enforcement agencies, defense contractors, and media companies

November 2018. Ukraine's CERT discovered malware in the computer systems of Ukraine state agencies believed to be implanted as a precursor for a future large-scale cyber attack

November 2018. Researchers discover that a Chinese cyberespionage group targeted a UK engineering company using techniques associated with Russia-linked groups in an attempt to avoid attribution

November 2018. The Pakistani Air Force was revealed to have been targeted by nation-state hackers with access to zero-day exploits

November 2018. Security researchers identify an Iranian domestic surveillance campaign to monitor dissent targeting Telegram and Instagram users

November 2018. Australian defense shipbuilder Austal announced it had been the victim of a hack resulting in the theft of unclassified ship designs which were later sold online

October 2018. The head of Iran's civil defense agency announced that the country had recently neutralized a new, more sophisticated version of Stuxnet

October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information

October 2018. Security researchers link the malware used to attack a petrochemical plant in Saudi Arabia to a research institute run by the Russian government.

October 2018. U.S. defense officials announced that Cyber Command had begun targeting individual Russian operatives to deter them from interfering in the 2018 midterm elections.

October 2018. U.S. agencies warned President Trump that that China and Russia eavesdropped on calls he made from an unsecured phone.

October 2018. News reports reveal that the Israel Defense Force requested that cybersecurity companies develop proposals for monitoring the personal correspondence of social media users.

October 2018. The U.S. Department of Homeland Security announces that it has detected a growing volume of cyber activity targeting election infrastructure in the U.S. ahead of the 2018 midterm elections.

October 2018. The Centers for Medicare and Medicaid Services announced that hackers had compromised a government computer system, gaining access to the personal data of 75,000 people ahead of the start of ACA sign-up season.

October 2018. The Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government groups

October 2018. The U.S. Justice Department announces criminal charges against seven GRU officers for multiple instances of hacking against organizations including FIFA, Westinghouse Electric Company, the Organisation for the Prohibition of Chemical Weapons, and the U.S. and World Anti-Doping Agencies.

September 2018. Security researchers found that a Russian hacking group had used malware to target the firmware of computers at government institutions in the Balkans and in Central and Eastern Europe.

September 2018. In a letter to Senate leaders, Sen. Ron Wyden revealed that a major technology company had alerted multiple Senate offices of attempts by foreign government hackers to gain access to the email accounts of Senators and their staff

September 2018. Researchers report that 36 different governments deployed Pegasus spyware against targets in at least 45 countries, including the U.S., France, Canada, and the UK.

September 2018. The U.S. State Department suffers a breach of one of its unclassified email systems, exposing the personal information of several hundred employees.

September 2018. Swiss officials reveal that two Russian spies caught in the Netherlands had been preparing to use cyber tools to sabotage the Swiss defense lab analyzing the nerve agent used to poison former Russian Agent Sergei Skripal.

September 2018. Security researchers find that Iranian hackers have been surveilling Iranian

citizens since 2016 as part of a mobile spyware campaign directed at ISIS supporters and members of the Kurdish ethnic group.

September 2018. Russian hackers targeted the email inboxes of religious leaders connected to Ukraine amid efforts to disassociate Ukraine's Orthodox church from its association with Russia.

September 2018. The U.S. Department of Justice announces the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers.

September 2018. The U.S. Department of Justice announces the indictment of Park Jin Hyok, a North Korean Hacker allegedly involved in the 2014 Sony hack, the 2016 theft of $81 million from a Bangladeshi bank, and the WannaCry ransomware attacks.

September 2018. Researchers reveal a new cyber espionage campaign linked to attacks against Vietnamese defense, energy, and government organizations in 2013 and 2014.

September 2018. Chinese hackers breached the systems of the Starwood hotel chain in 2014. It is estimated that the personal information of up to 500 million people was stolen

August 2018. North Korean hackers stole $13.5 million from India's Cosmos Bank after breaking into the bank's system and authorizing thousands of unauthorized ATM withdrawals, as well as several illegal money transfers through the SWIFT financial network.

August 2018. Security researchers report that Iranian hackers had targeted the websites and login pages of 76 universities in 14 countries. The attackers stole the credentials of users who attempted to sign in, gaining access to library resources for the purposes of intellectual property theft.

August 2018. Facebook identified multiple new disinformation campaigns on its platform sponsored by groups in Russia and Iran. The campaigns targeted users in the U.S., Latin America, Britain, and the Middle East, and involved 652 fake accounts, pages, and groups.

August 2018. Microsoft announces that Russian hackers had targeted U.S. Senators and conservative think tanks critical of Russia.

July 2018. Security researchers report that an Iranian hacking group had been targeting the industrial control systems of electric utility companies in the U.S., Europe, East Asia, and the Middle East.

July 2018. The Department of Homeland Security reveal that a campaign by Russian hackers in 2017 had compromised the networks of multiple U.S. electric utilities and put attackers in a position where they could have caused blackouts.

July 2018. Senator Claire McCaskill reveals that her 2018 re-election campaign was targeted by hackers affiliated with Russia's GRU intelligence agency. Attackers unsuccessfully targeted staffers in the Senator's office with phishing emails designed to harvest their passwords.

July 2018. Researchers report that a hacking group linked to Iran has been active since early 2017 targeting energy, government, finance, and telecommunications entities in the Middle East.

July 2018. Microsoft reveals that Russian hackers had targeted the campaigns of three Democratic candidates running for the 2018 midterm elections.

July 2018. Russian hackers were found to have targeted the Italian navy with malware designed to insert a backdoor into infected networks.

July 2018. Security researchers detect a spike in hacking attempts against IoT devices in Finland during the run-up President Trump's summit with Vladimir Putin in Helsinki. The majority of attacks originated in China.

July 2018. Singapore's largest healthcare institution was targeted by state-sponsored hackers, leading to the leakage of personal information for 1.5 million patients, along with prescription details for 160,000 others.

July 2018. Ukrainian intelligence officials claim to have thwarted a Russian attack on the network equipment of a chlorine plant in central Ukraine. The virus used in the attack is the same malware responsible for the infection of 500,000 routers worldwide in a campaign the FBI linked to state-sponsored Russian hackers.

July 2018. The U.S. Department of Justice announced the indictments of 12 Russian intelligence officers for carrying out large-scale cyber operations against the Democratic Party in advance of the 2016 Presidential election. The officers' alleged crimes included the theft and subsequent leakage of emails from the Democratic National Committee and Hillary Clinton campaign, and the targeting of election infrastructure and local election officials in an attempt to interfere with the election.

July 2018. Security researchers report that Chinese hackers had been actively spying on political actors on both sides of the upcoming Cambodian elections. Targets include the country's National Election Commission, several government ministries, the Cambodian Senate, at least one Member of Parliament, and multiple media outlets and human rights activists.

July 2018. Hackers targeted the campaigns of at least two local Democratic candidates during 2018's primary season, reportedly using DDoS attacks to disrupt campaign websites during periods of active fundraising and positive news publicity.

July 2018. Australian National University (ANU) was found to have been breached by Chinese hackers in an attack believed to be motivated by a desire to siphon intellectual property from the institution.

June 2018. Marketing data firm Exactis suffered a data breach exposing the information of 340 million people, including their political preferences, browsing habits, and purchase data.

June 2018. Ukraine police claim that Russian hackers have been systematically targeting Ukrainian banks, energy companies, and other organizations to establish backdoors in preparation

for a wide-scale strike against the country.

June 2018. Chinese hackers were found to be engaged in a cyber espionage campaign to collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia.

June 2018. A Russian hacking group linked to disrupting the Peyongchang Olympics targeted individuals in France, Germany, Switzerland, Russia, and Ukraine linked to a biochemical threat conference organized by a company involved in the investigation of the poisoning of Sergei Skripal in March 2018.

June 2018. A Chinese hacking group targeted a national data center in a Central Asian country, preparing a watering hole attack to inject malicious code onto other government websites connecting to the data center.

June 2018. Researchers reveal that North Korean hackers targeted a South Korean think tank focused on national security issues. The hackers used a zero-day exploit to compromise the organization's website and insert a backdoor for injecting code.

June 2018. The U.S. Treasury Department announced sanctions against five Russian companies and three individuals for enabling Russian intelligence and military units to conduct cyberattacks against the U.S.

June 2018. Chinese government hackers compromised the networks of a U.S. Navy contractor, stealing 614 GB of data related to weapons, sensor, and communication systems under development for U.S. submarines.

May 2018. Cyber security researchers reported that North Korean hackers had been targeting defectors through compromised Android apps hosted through the Google Play market, stealing device information and allowing the insertion of executable code stealing photos, contact lists, and text messages.

May 2018. Security researchers reveal that the Pakistani military used Facebook Messenger to distribute spyware to targets in the Middle East, Afghanistan, and India in an attempt to compromise government officials, medical professionals, and others.

May 2018. Turkish government hackers were discovered to be using surveillance software FinFisher to infect Turkish dissidents and protesters.

May 2018. An unknown group of hackers stole between $18 and $20 million dollars from Mexican banks by exploiting the SWIFT transfer system, submitting a series of false transfer orders to phantom accounts in other banks and emptying the accounts in dozens of branch offices.

May 2018. Within 24 hours of President Trump's announcement that the US would withdraw from the Iran nuclear agreement, security firms reported increases in Iranian hacking activity, including the sending of emails containing malware to diplomats in the Foreign Affairs ministries of US allies, as well as global telecommunication companies.

May 2018. Researchers reveal that a hacking group connected to Russian intelligence services had been conducting reconnaissance on the business and ICS networks of electric utilities in the US and UK since May 2017.

April 2018. A cyber espionage campaign originating in China collected data from satellite, telecom, and defense organizations in the United States and Southeast Asia.

April 2018. Security researchers report that an Indian hacking group had been targeting government agencies and research institutions in China and Pakistan since 2013.

April 2018. Cyber security researchers reveal that North Korean hackers targeted critical infrastructure, finance, healthcare, and other industries in 17 countries using malware resembling the code used in the 2014 Sony Pictures attack.

April 2018. Israeli cyber researchers revealed that Hamas had planted spyware in mobile phones owned by members of Fatah, a rival Palestinian faction.

April 2018. Reports from cyber security researchers indicate that Chinese state-sponsored hacking groups have targeted Japanese defense companies in an attempt to gain information on Tokyo's policies towards North Korea

April 2018. US and UK officials issued a joint warning that Russia was deliberately targeting western critical infrastructure by compromising home and business routers.

April 2018. The director of the UK's Government Communications Headquarters (GCHQ) announced that the organization had been conducting offensive cyber operations against ISIS to suppress their propaganda, disrupt their coordination, and protect deployed military personnel.

April 2018. The chief of Germany's domestic intelligence services accused Russia of being behind the December 2017 attack on the government's computer networks.

April 2018. The UK's National Cyber Security Centre released an advisory note warning that Russian state actors were targeting UK critical infrastructure by infiltrating supply chains.

April 2018. All government services of Sint. Maarten, a Caribbean island and constitute country of the Netherlands, were taken offline for a week after a cyber attack. According to local authorities, this is the third cyber attack the country has faced in just over a year.

April 2018. The North Korean hacking group responsible for the SWIFT attacks was found to have targeted a Central American online casino in an attempt to siphon funds.

March 2018. Chinese hackers targeted U.S. defense and engineering companies with ties to the South China Sea. The attacks sought sensitive data in line with government espionage objectives.

March 2018. Online services for the city of Atlanta were disrupted after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. The city would eventually spend approximately $2.6 million recovering from the attack.

March 2018. Baltimore's 911 dispatch system was taken down for 17 hours after a ransomware attack, forcing the city to revert to manual dispatching of emergency services

March 2018. The US Departments of Justice and Treasury accused Iran in an indictment of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.

March 2018. The FBI and Department of Homeland Security issued a joint technical alert to warn of Russian cyber attacks against US critical infrastructure. Targets included energy, nuclear, water, aviation, and manufacturing facilities.

March 2018. Columbian authorities reported more than 50,000 attacks on the web platform of Columbia's national voter registry during the run-up to national elections.

March 2018. A data breach of the company Under Armor compromised the information of 150 million users of its fitness and nutrition tracking app MyFitnessPal.

March 2018. Cybersecurity researchers reveal that a Chinese hacking group used malware to attack the service provider for the UK government in an attempt to gain access to contractors at various UK government departments and military organizations.

March 2018. Cybersecurity researchers announce evidence that the same North Korean hacking group linked to the SWIFT financial network attacks has been targeting several major Turkish banks and government finance agencies.

March 2018. A UN report details attempts by North Korean hackers to compromise email accounts of the members of a UN panel enforcing trade sanctions against North Korea.

February 2018. German news reported that a Russian hacking group had breached the online networks of Germany's foreign and interior ministries, exfiltrating at least 17 gigabytes of data in an intrusion that went undetected for a year.

February 2018. The Justice Department indicted 13 Russians and three companies for their online efforts to interfere in the 2016 US presidential elections.

February 2018. The US and UK formally blame Russia for the June 2017 NotPetya ransomware attack that caused billions of dollars in damages across the world.

February 2018. A cyberattack on the Pyeongchang Olympic Games attributed to Russia took the official Olympic website offline for 12 hours and disrupted wifi and televisions at the Pyeongchang Olympic stadium.

February 2018. Officials at the Department of Homeland Security confirmed that Russian hackers successfully penetrated the voter registration rolls of several US states prior to the 2016 election.

January 2018. Chinese hackers infiltrated a U.S. Navy contractor working for the Naval

Undersea Warfare Center. 614 gigabytes of material related to a supersonic anti-ship missile for use on U.S. submarines were taken, along with submarine radio room information related to cryptographic systems and the Navy submarine development unit's electronic warfare library

January 2018. China denied that the computer network it supplied to the African Union allowed it access the AU's confidential information and transfer it to China, or that it had bugged offices in the AU headquarters that it had built.

January 2018. A Japan-based cryptocurrency exchange reveals that it lost $530 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time.

January 2018. Norwegian officials discover a "very professional" attempt to steal patient data from a Norwegian hospital system, in an attack they speculate was connected to the upcoming NATO Trident Juncture 18 military exercise.

January 2018. A hacking group with ties to the Lebanese General Directorate of General Security was revealed to have been involved in a six-year campaign to steal text messages, call logs, and files from journalists, military officers, corporations, and other targets in 21 countries worldwide.

January 2018. The Unique Identification Authority of India and its Aadhaar system are hacked by unknown actors, resulting in the personal data of more than 1 billion people being available for purchase.

December 2017. French company Schneider Electric was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. Analysis by security researchers indicated that the attack was sponsored by a nation-state.

December 2017. The state-owned China Aerospace Science and Industry Corporation (CASIC) is alleged to have pre-installed backdoors in biometric equipment sold to Taiwan for its e-Gate border control system. The backdoors would have allowed CASIC to gather private data on both Taiwanese and foreign citizens traveling in and out of the country since the system's installation in 2012.

December 2017. Iranian hackers used fake social network profiles and a fake news site to target academic researchers, human rights activists, media outlets, and political advisors

November 2017. Three Chinese nationals employed at a China-based Internet security firm are indicted by a US grand jury for computer hacking, theft of trade secrets, conspiracy, and identity theft against employees of Siemens, Moody's Analytics, and Trimble.

November 2017. Uber discloses that it paid hackers $100,000 to delete the stolen data of 57 million of its customers and drivers, including names, phone numbers, email addresses, and license plate numbers.

November 2017. Cybersecurity researchers report a cyberespionage campaign targeting

government organizations in South America and Southeast Asia. The group, deemed to have nation-state capabilities, aimed to acquire foreign policy information from diplomatic and government entities.

November 2017. Cybersecurity researchers report a sophisticated Vietnamese hacking group responsible for cyber espionage campaigns targeting the ASEAN organization, foreign corporations with an interest in Vietnamese industries, and media, human rights, and civil society organizations.

October 2017. A major wave of ransomware infections hits media organizations, train stations, airports, and government agencies in Russia and Eastern Europe. Security researchers found strong evidence linking the attack to the creators of NotPetya, and noted that the malware used leaked NSA-linked exploits to move through networks. Ukrainian police later reported that the ransomware was a cover for a quiet phishing campaign undertaken by the same actor to gain remote access to financial and other confidential data.

October 2017. Yahoo updates the previous projections of 1 billion account affected in its massive 2013 breach, acknowledging that all 3 billion accounts were compromised.

October 2017. Russian hackers reported to be targeting potential attendees of CyCon, a cybersecurity conference organized by the US Army and the NATO CCD COE

October 2017. DHS and FBI reports warn of Russia-linked hackers targeting industrial control systems at US energy companies and other critical infrastructure organizations

October 2017. Poland's Defense Minister reports that the country repelled a third Russian hacking attempt against companies in Poland, reportedly part of a larger campaign against Eastern European corporations.

October 2017. North Korean hackers were found to have targeted US electric companies in a spear-phishing campaign meant to probe utilities' defenses.

October 2017. North Korean hackers allegedly broke into South Korea's defense data center in 2016 and stole a large trove of sensitive documents over the course of a year, including joint U.S.-South Korean blueprints for war on the peninsula.

October 2017. China allegedly carried out a cyberattack against a U.S. think tank and law firm, both involved with fugitive Chinese tycoon Guo Wengui.

October 2017. The Australian Government revealed that hackers compromised an Australian national security contractor in 2016 and stole large amounts of data, including information related to the development of the F-35 Joint Strike Fighter.

October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer

September 2017. An Iranian hacking group was responsible for an espionage campaign targeting the aerospace industry in the U.S. and Saudi Arabia, as well as petrochemical firms in South Korea and Saudi Arabia.

September 2017. Russia compromised the personal smartphones of NATO soldiers deployed to Poland and the Baltic states.

September 2017. Press reports say that the US Cyber Command targeted North Korea's the Reconnaissance General Bureau for denial-of-service attacks.

September 2017. China allegedly inserted malware into widely used PC management tool. The malware targeted at least 20 major international technology firms.

September 2017. The SEC reported that cybercriminals accessed the agency's files in 2016 and used the information gathered for illicit trading

September 2017. Credit monitoring firm Equifax disclosed a July data breach that revealed 143 million people's full names, social security numbers, birth dates, home addresses and driver's license numbers, as well as 209,000 credit card numbers.

September 2017. Researchers report malware infections in Cambodia designed to surveil dissidents and disrupt domestic political activity.

August 2017. Researchers inform the Estonian Information System Authority of a vulnerability potentially affecting the use of 750,000 Estonian e-ID cards. The government replaced the compromised cards in late 2017, but claims that no cards were ever hacked.

August 2017. South Korea's Cyber Warfare Research Center reports that North Korea has been targeting South Korean Bitcoin exchanges.

August 2017. A state-sponsored spyware campaign targeted Indian and Pakistani government security and military organizations.

August 2017. The Scottish Parliament suffered from a brute force cyberattack similar to the one that compromised the British Parliament in June.

July 2017. The Swedish Transport Agency's outsourced data is hacked, potentially compromising confidential information and classified information on military plans.

July 2017. Security researchers revealed details of a wide-ranging malware campaign linked to China which used over 600 strains of malware to conduct espionage operations on Southeast Asian military and government organizations

July 2017. GCHQ issued a warning saying that state-sponsored hackers had likely broken into the Industrial Control Systems of UK energy companies

July 2017. Security researchers revealed an Iran-linked cyber espionage group active since 2013 that had used spear phishing and watering hole attacks to target government institutions, defense

companies, IT firms and more in Israel, Saudi Arabia, the US, Germany, Jordan, and Turkey.

July 2017. The FBI and DHS announced that hackers had been targeting US energy facilities including the Wolf Creek Nuclear Operating Corporation in a campaign bearing resemblance to the operations of a known Russian hacking group

July 2017. Cyber research firms reported a new malware campaign launched the day after North Korea's July missile tests. The identified family of malware featured a command and control infrastructure with links to South Korea, and had previously been used in three other campaigns linked to North Korea.

July 2017. Hackers attacked a partner of UniCredit, Italy's largest bank, gaining access to loan and biographical data from 400,000 client accounts

July 2017. Russian hackers used leaked NSA tools to compromise Wi-Fi servers in European and Middle Eastern hotels in a campaign targeting top diplomats and industrial leaders.

July 2017. The Qatari government accused hackers in the United Arab Emirates of posting fake news and attacking Qatari state-run media websites in a campaign designed to widen a rift between Gulf states.

June 2017. The New York Times revealed that spyware sold to the Mexican government was being used to target human rights lawyers, journalists, and anti-corruption activists

June 2017. US-CERT identified the North Korean government as being behind a DDoS botnet infrastructure used to target media, financial, aerospace, and critical infrastructure organizations worldwide

June 2017. A Russia-linked hacking group was found to have launched a spear-phishing campaign against Montenegro after the country announced its decision to join NATO

June 2017. A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days, causing an estimated $300 million in associated costs

June 2017. Russian hackers used an updated ransomware program to target Ukrainian infrastructure, including power companies, airports, and public transit.

June 2017. A brute-force attack alleged to have been carried out by Iranian state actors compromised nearly 90 British members of parliament, whose email accounts were hacked.

May 2017. Beginning in 2011, Hackers from the internet security firm Boyusec compromised the networks of three companies over a multi-year period and gained access to confidential documents and data, including sensitive internal communications, usernames and passwords, and business and commercial information

May 2017. A hacking campaign by an Iran-linked group targeted multiple Israeli IT vendors, financial institutions and the national post office

May 2017. A ransomware campaign spread to 99 countries using a vulnerability revealed in the Shadow Brokers' April 2017 dump of NSA tools.

May 2017. Lebanon accused Israel of hacking the Lebanese telecoms network and sending audio and WhatsApp messages to 10,000 people claiming that Hezbollah's leader was behind the death of the group's top commander.

May 2017. An Iranian hacking group attempted to carry out an attack on a U.S. military contractor using Russian tools.

May 2017. Thousands of emails and other documents from the campaign of French president-elect Emmanuel Macron, totaling 9 gigabytes, were released shortly before the election, in an effort linked to Russia.

April 2017. The Israeli Cyber Defense Authority announced it had defended an Iranian cyberattack campaign against 120 targets in the government, high-tech, medical, and education sectors

April 2017. Irish state-owned utility EirGrid suffered a security breach at the hands of state-sponsored hackers involving a virtual wiretap allowing access to the company's unencrypted communications.

April 2017. The Lazarus Group, thought to be associated with North Korea, was found to be involved in a spear phishing campaign against US defense contractors

April 2017. Cybersecurity researchers revealed a growing cyber-espionage campaign originating in China and targeting construction, engineering, aerospace and telecom companies, as well as government agencies, in the U.S., Europe, and Japan.

April 2017. The Danish Defense Intelligence Service reported that a "foreign player," alleged by the Danish press to be Russia espionage group, had accessed Defense Ministry email accounts in 2015 and in 2016, but was unable to retrieve classified information.

April 2017. The Shadow Brokers, the group that claimed to have hacked the NSA in August 2016, released yet another trove of purported NSA hacking tools, including one that suggests the NSA had gained access to SWIFT messages.

April 2017. Chinese attempts to penetrate South Korean military, government and defense industry networks continued at an increasing rate since a February announcement that the THAAD missile defense system would be deployed in South Korea.

March 2017. An intelligence report revealed a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in the Department of Defense. The malicious payloads delivered through these messages gave Russian hackers access to the victim's device and Twitter account.

March 2017. The U.S. Department of Justice indicted two Russian intelligence agents and two

criminal hackers over the September 2014 Yahoo hack, which compromised 500 million user accounts.

March 2017. Chinese police arrested 96 suspects charged with hacking into the servers of social media, gaming and video streaming sites, stealing personal information, and posting the information for sale on online forums.

March 2017. Wikileaks released a trove of sophisticated CIA hacking tools dated from 2013 to 2016, claiming that the release reflected several hundred million lines of CIA-developed code.

February 2017. An Iranian hacker group targeted actors associated with the U.S. defense industrial base as well as at least one human rights activist in a campaign to steal credentials and other data

February 2017. An Iranian cyber espionage campaign targeted the energy, government, and technology sectors of Saudi Arabia

February 2017. A suspected Russian hacker breaches at least 60 universities and US government organizations using SQL injections, including HUD, NOAA, Cornell University, and NYU, among many others. This follows up a hack by the same actor against the U.S. Electoral Assistance Commission in December 2016.

February 2017. Indian Central Bureau of Investigation and Army officers were targeted by a phishing campaign purportedly mounted by Pakistan.

February 2017. Hackers compromised the Singaporean military's web access system and stole the personal information of 850 people. The Ministry of Defense said it was likely the attack was state sponsored.

February 2017. A sophisticated malware operation extracted over 600 gigabytes of data from 70 mostly Ukrainian targets in the fields of critical infrastructure, news media, and scientific research.

January 2017. A Swedish foreign policy institute accused Russia of conducting an information warfare campaign, using fake news, false documents, and disinformation intended to weaken public support for Swedish policies.

December 2016. Russian hackers targeted Ukraine's national power company, Ukrenergo, and shut down power to northern Kiev for over an hour.

December 2016. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) warned its customers that they remain vulnerable to attacks by "sophisticated" hackers, having witnessed "a meaningful number" of attacks on its customers since the Bangladesh heist in February 2016, a fifth of which had resulted in stolen funds.

December 2016. Yahoo revealed that its systems had been intruded into in August 2013, and that the breach compromised one billion user accounts. Compromised data included usernames, email addresses, phone numbers, dates of birth, passwords, and security questions and answers. The data

was posted for sale for $200,000 or best offer on underground forums.

November 2016. An indiscriminate attack compromised systems at the San Francisco Municipal Transportation Agency (the Muni), locking operators out of computers and customers out of kiosks. As a result, the Muni offered customers free rides for two days, until administrators restored its systems without paying the demanded $73,000 ransom.

November 2016. Hackers targeted AdultFriendFinder, a dating website, compromising 412 million users and publishing their emails, passwords, member status and purchases on online criminal marketplaces.

November 2016. The hard-drive-wiping "Shamoon" virus used against Saudi Aramco in 2012 was deployed against four Saudi Arabian government agencies. The attack wiped data on thousands of computers at Saudi's General Authority of Civil Aviation and other agencies.

October 2016. A cyber mercenary contracted by a rival firm used a botnet to disable a Liberian telecom company, rendering half the country unable to access the internet.

October 2016. Hackers grained control of a major Brazilian bank's Domain Name System addresses and seized the bank's entire online footprint for several hours.

October 2016. The U.S. Director of National Intelligence and Department of Homeland Security jointly identified Russia as responsible for hacking the Democratic National Committee and using WikiLeaks to dump emails obtained in the hack.

September 2016. Japanese Defense Ministry and Self-Defense Forces (SDF) communications networks linking SDF bases and camps were compromised.

September 2016. Yahoo revealed that it an intrusion into its network in late 2014 had given hackers access to 500 million users' usernames, email addresses, phone numbers, dates of birth, passwords, and a mix of encrypted and plaintext security questions and answers. The company's CIO claimed the attack was perpetrated by a state-sponsored actor.

August 2016. A group calling itself "Shadow Brokers" claimed to have penetrated NSA and published a collection of NSA tools on Pastebin.

August 2016. Brazilian hackers ramped up phishing attacks against tourists visiting Rio de Janeiro for the 2016 Olympics. Security researchers ranked Brazil second only to Russia in the sophistication of its financial fraud gangs.

August 2016. A cybercriminal gang purportedly from Russia breached enterprise software company Oracle's systems, possibly to install malware on point-of-sale (POS) systems. The POS malware would then allow hackers to gain access to financial information in data breaches at major retailers.

August 2016. Two Hong Kong government agencies were penetrated in an attack allegedly by China. The attack came weeks before legislative elections in Hong Kong.

August 2016. Designs and data regarding India's Scorpene submarines were leaked from the French shipbuilder DCNS. DCNS also builds submarines for Malaysia and Chile, and recently won contracts to build submarines for Brazil and Australia.

July 2016. Forensic evidence points to Russian intelligence agencies as responsible for the release of 20,000 emails from the Democratic National Committee.

July 2016. A series of DDOS attacks disrupted 68 Philippine government websites on July 12, the day the United Nations International Arbitration court released its decision ruling in favor of the Philippines on the West Philippine Sea territorial dispute.

July 2016: A new strain of cyberespionage malware with a dropper designed to target specific European energy companies has been discovered. Researchers say the malware appears to be the work of a nation-state, may have originated in Eastern Europe, and its role seems to be battlespace preparation.

July 2016: A Chinese cyber espionage group targeted defense industries in Russia, Belarus, and Mongolia with APTs using phishing campaigns to exfiltrate data.

May 2016: Suspected Russian hackers attempted to penetrate the Turkish Prime Minister's office and the German Christian Democratic Union party. The attacks targeted personal email accounts and attempted to obtain login credentials.

May 2016. Researchers uncovered an espionage campaign originating from Iran that attacked government and business targets in multiple countries, as well as targets inside of Iran. The operation was conducted over the course of a decade.

May 2016. Germany's domestic intelligence agency accused Russia of perpetrating a series of cyber attacks on the German Bundestag in 2015. The attackers made off with an undisclosed amount of data.

May 2016: Saudi Arabian communications and defense organizations were hacked, possibly by Iran.

April 2016. U.S. Steel accused Chinese government hackers of stealing proprietary information about steel production techniques for the benefit of Chinese steel producers

April 2016. The German Christian Democratic Union, the political party of Angela Merkel, was targeted in a credential phishing attack by a Russian cyber espionage group.

April 2016. The Philippine Commission on Elections' (COMELEC) database was breached, exposing the personal information of all 55 million registered Filipino voters, including fingerprint data, passport numbers and expiry dates, and intentions to run for office.

April 2016. Microsoft researchers discover a highly skilled hack group that has targeted government agencies (including intelligence agencies), defense research centers and

telecommunication service providers in South and Southeast Asia since 2009.

April 2016. North Korean hackers stole warship blueprints from the database of a South Korean shipbuilder.

Mach 2016. A suspected ransomware attack crippled MedStar Health-operated hospitals in Maryland and Washington.

March 2016. North Korean hackers broke into the smartphones of a dozen South Korean officials, accessing phone conversations, text messages, and other sensitive information.

March 2016. 21st Century Oncology, a cancer care company, revealed that 2.2 million patients' personal information may have been stolen in an October 2015 hack. Hackers had access to patient names, Social Security numbers, doctor names, diagnosis and treatment information, and insurance information.

March 2016. Finland's foreign ministry discovered it had been the victim of a four-year breach in their computer network.

February 2016. The Internal Revenue Service (IRS) announced that a breach of its systems in May 2015 had compromised over 700,000 American taxpayers. The IRS suspected that a Russian tax fraud operation is responsible for the breach.

February 2016. Hackers breached the U.S. Department of Justice's database, stealing and releasing the names, phone numbers, and email addresses or 30,000 DHS and FBI employees.

February 2016. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) warned its customers that they remain vulnerable to attacks by "sophisticated" hackers, having witnessed "a meaningful number" of attacks on its customers since the Bangladesh heist in February 2016, a fifth of which had resulted in stolen funds.

January 2016. Austrian-based aerospace parts manufacturer FACC had $54.5 million stolen in a cyberattack. The attackers ignored FACC's intellectual property or proprietary data, and business operations were not affected.

January 2016. Israel revealed an operation by the United States and Britain to hack into Israel's surveillance drones.

January 2016. The chief of Sri Lanka's Financial Crimes Investigation Division had his private email account hacked. It is believed the attack was an attempt at embarrassment motivated by an ongoing crackdown by the department.

January 2016. Armenian diplomatic missions in 40 countries had their websites defaced by Azerbaijani hackers.

January 2016. The Czech Republic's Prime Minister had his twitter and personal email account hacked by right-wing extremists.

December 2015. Russian hackers coordinated attacks on several regional power distribution companies in Western Ukraine. SCADA systems and system host networks were targeted and damaged. Malware was used to probe for network vulnerabilities, establish command and control, and wipe SCADA servers to delay restoration. Attackers simultaneously launched a denial of service attack on system dispatchers to prevent customers from reporting disruptions. Approximately 225,000 Ukrainians were affected, but service was restored after 3-6 hours.

December 2015. The Australian Bureau of Meteorology was attacked by hackers the previous year, with unnamed sources attributing the incident to China.

October 2015. The ROK National Intelligence Service attributed hacks at the National Assembly, the Ministry of Unification, and the Blue House to North Korea's General Reconnaissance Bureau.

October 2015. A teenage hacker tricked Verizon and AOL customer service to gain access to the private email account of CIA Director John Brennan.

November 2015. Iran's Revolutionary Guard hacked the email and social media accounts of a number of Obama administration officials in attacked believed to be related to the arrest of an Iranian-American businessman in Tehran.

November 2015. Spies were found to have attempted to hack into the German, French, and Japanese submarine builders bidding for a contract to build Australia's new submarine fleet.

November 2015. Dutch security firm Fox-IT identified a Chinese hacking group that had launched cyberattacks against government civilian and military agencies in the United States and other industries, including corporations conducting solar cell research

September 2015. Hackers sought access to the Dutch Safety Board and other parties involved in investigating the crash of flight MH17.

September 2015. Multiple Pakistani government websites were hacked by the 'Mallu Cyber Team.

September 2015. Cybersecurity researchers uncovered a Russian hacking group called "The Dukes" that is allegedly responsible for attacks against foreign governments and think tanks in Europe, Central Asia, and the United States over seven years.

August 2015. Researchers identified a phishing campaign targeting members of the Iranian diaspora, as well as at least one Western activist. The attacks were seeking two-factor authentication credentials.

July 2015. The website of the Permanent Court of Arbitration in The Hague went offline in an incident that sources are connecting to hearings regarding China's claims to territory in the South China Sea. The breach was traced back to an IP address in China. The vulnerability spread malware to the devices of website visitors.

July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted

in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator.

July 2015. United Airlines revealed that its computer systems were hacked in May or early June, compromising manifest data that detailed the movements of millions of Americans. The report, citing "several people familiar with the probe," stated that the group behind this attack is the same group suspected of the Office of Personnel Management hack discovered in June.

July 2015. Hacking Team, an Italy-based firm accused of the unethical sale of surveillance technology worldwide, was hacked and hundreds of gigabytes of sensitive data were stolen. Confidential documents leaked by the hackers appeared to show Hacking Team's material support for authoritarian governments such as those in Sudan, Ethiopia, Morocco, and the United Arab Emirates.

June 2015. Canada announced that it has experienced DDOS attacks against two government websites. The attacks, which took down the Canadian Security Intelligence Service (CSIS) and the general Canadian government website, Canada.ca also reportedly affected email, Internet access and IT services in the government. Anonymous has claimed responsibility, citing Canada's recently passed Anti-terrorism Act, 2015 as the reason behind the recent attack.

June 2015. Japan Pension Service (JPS) was hacked resulting in the exfiltration of personal data belonging to 1.25 million people.

June 2015. Cybersecurity researchers identified an Iranian cyber espionage campaign that targeted over 500 organizations, most of them in the Middle East, that focused on diplomacy, defense and security, journalism & human rights, and other fields.

June 2015. The Office of Personnel Management was revealed to have been hacked twice in the last year. The first resulted in the loss of 4.1 million records and the second resulted in the loss of 21.5 million records,19.7 million of these involved background investigation records for cleared U.S. government employees.

June 2015. German media reports that hackers breached the lower house of parliament on the Bundestag network and exfiltrated data from over 20,000 accounts. German weekly *Der Spiegel* said that the Kremlin is the primary suspect behind the attack and that the malware involved closely resembles that used in a 2014 attack on a German data network.

June 2015. The Chinese company Qihoo360 reports discovering "OceanLotus," an espionage program operating since 2012 to target marine agencies, research institutions and shipping companies.

June 2015. Media reports say that Stuxnet-like attacks were attempted against North Korea by the U.S., without success.

May 2015. Hong Kong-based undersea cable company Pacnet's business management systems

were breached by a malicious software that accessed sensitive data stored on a SQL server.

May 2015. Chinese hackers exfiltrated significant amounts of customer data from United Airlines

May 2015. Chinese intelligence officers infiltrated networks and exfiltrated trade secret information about turbofan engines from U.S. and European aerospace firms over the course of five years

May 2015. A hack of an online IRS system results in a $50 million loss, which the IRS blames on Russian hackers.

May 2015. The Yemen Cyber Army claims it breached a server belonging to the Saudi Ministry of Foreign Affairs. The hackers leaded the alleged login credentials of Saudi Officials, as well as usernames, phone numbers, and email addresses.

April 2015. The Pentagon revealed that Russian hackers gained access to an unclassified network within the DOD, though Pentagon officials were able to block the hackers' access within 24 hours.

April 2015. Hackers claiming affiliation to ISIS hacked French public television network TV5 Monde. The hackers took off the air 11 of the networks' channels and defaced TV5 Monde's website and social media accounts with pro-ISIS imagery.

April 2015. U.S. officials report that hackers gained access to White House networks and sensitive information, such as "real-time non-public details of the president's schedule," through the State Department's network, which has had continued trouble in ousting attackers.

March 2015. An Iranian hacking group conducted a spear-phishing campaign against defense, IT, government, and academic targets in Europe and the Middle East.

March 2015. Canadian researchers say Chinese hackers attacked U.S. hosting site GitHub. GitHub said the attack involved "a wide combination of attack vectors" and used new techniques to involve unsuspecting web users in the flood of traffic to the site. According to the researchers, the attack targeted pages for two GitHub users – GreatFire (https://en.greatfire.org/) and the New York Times' Chinese mirror site – both of which circumvent China's firewall.

February 2015. Anthem, a U.S. health insurance company, is hacked, resulting in the theft of 80 million customers' personally identifiable information. The information was taken from an unencrypted database. This may have been part of a larger campaign that included the OPM hack.

February 2015. Media reports say that Canada's Communication Security Establishment identified "Babar" and "EvilBunny" as malware developed for espionage purposes by the French government. Babar's primary function is to exfiltrate documents, but it can also log keystrokes, monitor a user's web history, intercept and record communications made via Skype and messenger programs.

January 2015. A report issued by Germany's Federal Office for Information Security reveals a German steel mill became the second recorded victim of a cyberattack causing physical

destruction. The attack disrupted control systems so severely that a blast furnace could not be properly shut down. The report did not name the steel mill or detail the severity of the damage.

December 2014. Iranian hackers attacked a major Las Vegas casino in retaliation for its owner's support for Israel.

December 2014. An Iranian cyber campaign targeted government agencies and critical infrastructure companies in the United States, Canada, Europe, the Middle East, and Asia.

November 2014. Sony Pictures Entertainment is hacked with the malware deleting data and the hackers posting online employees' personal information and unreleased films. An FBI investigation revealed North Korea to be behind the attack.

November 2014. North Korean hackers attacked a British production company planning to release a television series revolving around the imprisonment of a British nuclear scientist in the DPRK. The attack caused the cancellation of the series.

November 2014. A report by the University of Toronto finds that human rights organizations are routinely hacked by foreign intelligence services, using readily available crime ware as well as specially designed programs, with intrusion lasting for years.

October 2014. U.S. Postal Service servers are hacked, exposing employees' names, addresses, and Social Security numbers.

October 2014. The National Oceanic and Atmospheric Administration (NOAA) at the U.S. Department of Commerce is hacked, skewing the accuracy of some National Weather Service forecasts, according to NOAA.

October 2014. The Department of State reports breaches of its unclassified networks, and shut down its entire unclassified email system to repair possible damage. A month later, "suspicious cyber activity" was noticed on a White House computer network, but the White House said that no classified networks had been breached.

October 2014. Chinese users are redirected to a false iCloud login page that monitors their activities, putting their iCloud usernames, passwords, files, and contacts at risk.

October 2014. Ten percent of Dairy Queen outlets are hacked and customer credit card data compromised. Like the Target hack, hackers reportedly exploited a third party system to obtain access.

October 2014. A five-year cyber espionage campaign attributed to Russia exploits a zero-day vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian government.

October 2014. Australian mining and natural resources companies and their associated legal and financial advisors attacked during sensitive business negotiations.

September 2014. Hackers targeted the industrial control systems of the pharmaceutical sector with malware. Researchers stated the purpose of the attack was to achieve intellectual property theft.

September 2014. A false Occupy Central smartphone app with audio recording capabilities, likely of Chinese origin, targets Hong Kong protestors and accesses users' locations, call and message logs, and browser histories.

September 2014. Using fraudulently obtained certificate, cyber criminals obtain access to 300 government and company websites in Germany, Austria and Switzerland in a multiyear operation.

September 2014. Home Depot reports a server breach affecting 56 million debits cards in the U.S. and Canada.

August 2014. Community Health Systems disclosed that suspected Chinese hackers infiltrated its network and stole personal information from 4.5 million patients

August 2014. The contractor responsible for security clearances at DHS has their networks hacked and employee personal information is compromised. This was one of the first steps in the 2015 OPM hack.

July 2014. Hackers in Eastern Europe breached energy sectors in the U.S., Spain, France, Italy, Germany, Turkey, and Poland in a major cyberespionage campaign.

July 2014. U.S. Office of Personnel Management networks that contain information on thousands of applicants for top secret clearances are breached.

July 2014. Canada's Foreign Minister asks his Chinese counterpart about PLA cyber espionage against the National Research Council, Canada' leading technology research agency.

June 2014. CrowdStrike reported that Unit 61398 had targeted U.S. corporations in the satellite industry

May 2014. Alleged Chinese hackers posed as C-Suite executives in a spear phishing campaign to access the network of Alcoa. The hackers stole 2,907 emails and 863 attachments.

May 2014. Chinese military hackers targeted six American companies in the power, metals, and solar production industries and stole trade secret information. The U.S. Department of Justice indicted them and identified them as members of the People's Liberation Army Unit 61398

April 2014. An Iranian hacking group conducted a campaign of espionage attacks against the U.S. industrial base and also targets inside Iran.

March 2014. Indian Army and DRDO computers (Defense Research and Development Organization) were hacked, and the Indian government warned that the spyware could read the files of computers not even connected to internet.

March 2014. The OPM contractor responsible for U.S. security clearance background investigations is breached, allegedly by Chinese hackers.

March 2014. Cybercriminals steal 40 million credit card numbers from Target, with an additional 70 million accounts compromised.

January 2014. Hackers targeted 28 embassies in Tehran using emails about the Syrian conflict that contained a new data-mining malware.

November 2013. Finland's Foreign Minister reports that hackers breached Finland's diplomatic communications for several.

October 2013. Federal prosecutors announce Vietnamese cyber criminals obtained as many as 200 million personal records, including Social Security numbers, credit card data, and bank account information.

October 2013. Press reports based on Snowden leaks reveal NSA hacked into German Chancellor Merkel's mobile phone, one of a larger series of leaks on NSA activities.

September 2013. The U.S. Navy says that Iran hacked into unclassified networks.

September 2013. Chinese hackers used malware, known as 'Sykipot', to target entities in the U.S. Defense Industries and companies in key industries such as: telecommunications, computer hardware, government contractors, and aerospace. In mid-2013 they targeted the U.S. civil aviation sector.

September 2013. Chinese hackers targeted three U.S. organizations, including a large American oil and gas corporation

September 2013. North Korea again hacks South Korean targets, including think tanks, the South Korean Ministry of Defense, and Koreans defense industry firms.

August 2013. The Syrian Electronic Army hijacks and reroutes major Western social media and media sites to a malicious hosting site in Russia.

August 2013. A massive DDOS takes down China's .cn country code top level domain for several hours.

June 2013. PLA hackers infiltrated the computer networks of the U.S. Transportation Command and stole sensitive military information

June 2013. The FBI charged five Ukrainian and Russian hackers with stealing over 160 million credit card numbers and causing hundreds of millions in losses.

June 2013. The U.S. and Russia sign a bilateral agreement that establishes a hotline and other confidence building measures.

June 2013. Edward Snowden, a former systems administrator at the NSA, reveals documents

showing among other things that the US conducted cyber espionage against Chinese targets.

May 2013. An alleged Chinese hacker steals the blueprints for the Australian Security Intelligence Organization's new $631 million building.

May 2013. Israeli officials report a failed attempt by the Syrian Electronic Army to compromise water supply to the city of Haifa.

May 2013. DHS reports that the U.S. electrical grid is constantly being probed by multiple actors, including Iran.

May 2013. India is believed to have used a zero-day exploit to penetrate Pakistani mining, automotive, legal, engineering, food service, military, and banks.

May 2013. The Syrian Electronic Army claims to have breached the Saudi Arabian Ministry of Defense email system, and leaked several confidential emails.

May 2013. Over the course of the month, unknown hackers breached major automotive parts suppliers in North American and Europe.

May 2013. Anonymous' Saudi branch launches OpSaudi and takes down government web sites, including the Ministry of Foreign Affairs, Ministry of Finance, and the General Intelligence Presidency via DDos attack.

May 2013. The U.S. identified a gang of eight hackers who extracted $45 million from banks in the UAE and Oman. The attacks eliminated the withdrawal limits on prepaid debit cards, permitting the hackers to withdraw massive amounts.

May 2013. An unknown attacker utilized a DDoS attack to bring down the website of the Iranian Basij military branch (basij.ir).

May 2013. Chinese hackers compromise the U.S. Department of Labor and at least nine other agencies, including the Agency for International Development and the Army Corps of Engineers' National Inventory of Dams.

April 2013. A Russian internet security firm announced that they discovered malware on millions of android mobile devices, primarily in Russia and Russian speaking countries.

March 2013. The Syrian Electronic Army, a pro-Assad hacktivist group, hacked into major Western media organizations as part of a propaganda campaign.

March 2013. Beginning in 2012, Chinese hackers targeted civilian and military maritime operations within the South China Sea, in addition to U.S. companies involved in maritime satellite systems, aerospace companies and defense contractors

March 2013. The Indian Defence Research Organization was hacked, with thousands of documents uploaded to a server with an IP address in Guangdong, China.

March 2013. North Korea blames the United States and South Korea for a series of attacks that severely restricted Internet access in the country.

March 2013. South Korean television networks and banks were attacked with malware (designed to evade popular South Korean anti-virus software) thought to have originated in North Korea.

February 2013. DHS says that between December 2011 and June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China.

February 2013. Der Spiegel reveals that EADS and German steelmaker ThyssenKrupp recorded major attacks by Chinese hackers in 2012.
January 2013. The New York Times, Wall Street Journal, Washington Post, and Bloomberg News experience persistent cyberattacks, presumed to originate in China.

January 2013. The Japanese Ministry of Foreign Affairs (MOFA discovers it has been hacked and has lost "at least" twenty documents, including highly classified documents.

January 2013. Iran's Izz ad-Din al-Qassam claims responsibility for another series of distributed denial-of-service attacks against US Bank websites, as part of Operation Ababil phase two.

January 2013. A Defense Science Board report found that Chinese hackers stole U.S. weapons systems designs including for the PAC-3, THAAD, Aegis, F/A-18 fighter jet, V-22 Osprey, Black Hawk, and Littoral Combat Ship

December 2012. Al-Qaida websites are taken offline for two weeks.

December 2012. Two power plants in the U.S. were infected through unprotected USB drives.

October 2012. A Russian cybersecurity firm found a virus used against embassies, research firms, military installations, energy providers, and critical infrastructure in Eastern Europe, Russia, and Central Asia.

September 2012. Izz ad-Din al-Qassam, a hacker group linked to Iran, launched "Operation Ababil" targeting bank websites for sustained denial-of-service attacks. Targets include Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, and Regions Bank.

September 2012. Chinese hackers infiltrated Telvent Canada, an industrial automation company, and stole data related to SCADA systems throughout North America

August 2012. A group called "Cutting Sword of Justice" linked to Iran claimed it has used the "Shamoon" virus to attack Aramco, a major Saudi oil supplier, deleting data on 30,000 computers and infecting (without causing damage) control systems. The attack also affected the Qatari company RasGas, a major LNG supplier.

August 2012. Malware nicknamed "Gauss," infected 2,500 systems worldwide. Gauss appears to have been aimed at Lebanese banks, and contains code whose encryption has not yet been broken.

July 2012. Regarded as the largest attack on Indian government networks, over 10,000 email addresses of top Indian government officials were hacked, including officials in the Prime Minister's Office, Defense, External Affairs, Home, and Finance ministries, as well as intelligence agencies. India blames the attack on state actors.

July 2012. NSA Director General Keith Alexander said that there had been a 17-fold increase in cyber incident at American infrastructure companies between 2009 and 2011.

July 2012. Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems.

July 2012. A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings.

June 2012. The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of state cyberattacks.

June 2012. A global fraud campaign using automated versions of SpyEye and Zeus Trojans targeted high-value personal and corporate accounts and bypassed two-factor authentication.

June 2012. A phishing campaign targets the U.S. aerospace industry experts attending the 2013 IEEE Aerospace Conference.

June 2012. PLA Unit 61398 attacked Digital Bond, a SCADA security company with a spear phishing attack

June 2012. DHS reported that between December 2011 and June 2012, hackers targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China

May 2012. Researchers at the University of Toronto report that versions of the installer for the proxy tool Simurgh, which anonymizes net use and is popular in countries such as Iran and Syria to circumvent government internet controls, also installs a keylogger Trojan which sends the user name, keystrokes, and program use to another site.

May 2012. An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world.

May 2012. UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks.

April 2012. A hack of Japan's Ministry of Agriculture, Forestry, and Fisheries resulted in more

than 3,000 documents exfiltrated to a foreign destination, including 20 classified documents on negotiations on the Trans-Pacific Partnership (a broad free-trade agreement). According to press reports, the hackers searched Ministry computers for TPP documents, transferred all that were found to a single computer, and then compressed them to make them easier to send.

April 2012. Iran was forced to disconnect key oil facilities after a cyberattack against internal computer systems. The malware was found inside the control systems of Kharg Island – Iran's main oil exporting terminal. Equipment at Kharg Island and at other Iranian oil plants was disconnected from the internet as a precaution. Iran reported that oil production was not affected, but the websites of the Iranian oil ministry and national oil company were forced offline and data about users of the sites was taken as a result of the attack.

March 2012. The U.S. Department of Homeland Security issued amber alerts warning of a cyber-intrusion campaign on U.S. gas pipelines, dating back to December 2011. Press reports indicated that Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) described the attack as a sophisticated spear phishing campaign emanating from a single source.

March 2012. India's Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government websites had been compromised from December 2011 to February 2012. Most of the incidents involved website defacement and many of the hacks appeared to originate in Pakistan.

March 2012. The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC's Director General blamed Iran for the incident.

March 2012. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

March 2012. Trend Micro uncovered a Chinese cyber campaign, dubbed 'Luckycat' that targeted U.S.-based activists and organizations, Indian and Japanese military research, as well as Tibetan activists

February 2012. Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.

January 2012. Hackers working on behalf of the Qatar government sent a series of phishing emails to former advisor to FIFA President Sepp Blatter in an apparent espionage operation. Unidentified hackers also targeted the president of the United States Soccer Federation Sunil Gulati in an espionage operation.

December 2011. U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the People's Liberation Army. The Hackers had access to everything in Commerce's computers, including member

company communications and industry positions on U.S. trade policy.

November 2011. Norway's National Security Agency (NSM) reports that at least 10 major Norwegian defense and energy companies were hacked. The attacks were specifically "tailored" for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords.

November 2011. According to a major U.S. news source, Chinese hackers interfered with two satellites belonging to NASA and USGS.

November 2011. Apple computers belonging to European Commission officials, including EC Vice President for the "Digital Agenda," were hacked at an Internet Governance Forum (IGF) meeting in Azerbaijan.

October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China.

September 2011. A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove.

September 2011. Australia's Defense Signals Directorate says that defense networks are attacked more than 30 times a day, with the number of attacks increasing by more than 350 percent by 2009.

September 2011. Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates are used to verify that a website is genuine. By issuing a false certificate, an attacker can pretend to be a secure website, intercept e-mail, or install malicious software. This was the second hack of a certificate authority in 2011.

August 2011. Email and documents from 480 members of the Japanese Diet and lawmakers and their staff were compromised for a month after a phishing attack implanted a Trojan on members' computers and Diet servers. The hijacked machines communicated with a server in China and the attackers included Chinese characters in their code.

August 2011. According to sources in the Japanese government, Mitsubishi Heavy Industries and twenty other Japanese defense and high tech firms were the target of an effort to extract classified defense information. Japanese officials believed the exploits all originated from the same source. The intruder used email with a malicious attachment whose contents were the same as a legitimate message sent 10 hours earlier.

August 2011. Chinese hackers engaged in a series of cyber-attacks against 72 entities, including multiple U.S. government networks

July 2011. South Korea said hackers from China had penetrated an internet portal and accessed phone numbers, e-mail addresses, names and other data for 35 million Koreans.

July 2011. The German Bundespolizei (Federal Police) and the Bundeszollverwaltung (Federal Customs Service) discovered that servers used to locate serious criminals and terrorism suspects by gathering information from GPS systems in cars and mobile phones were penetrated (using a phishing attack) as early as 2010. Following the cyberattack, the relevant servers had to be temporarily shut down to prevent further data losses.

July 2011. In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen.

June 2011. Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

June 2011. The IMF's networks were reportedly compromised by a foreign government using fraudulent emails with malware attachments, and a "large quantity of data, including documents and e-mails," are exfiltrated.

May 2011. Cybercriminals masquerading as members of the hacktivist group "Anonymous" penetrated the PlayStation network. Sony estimated that personal information for more than 80 million users was compromised and that the cost of the breach was over $170 million.

April 2011. Employees at Oak Ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the Lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007.

April 2011. Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

March-April 2011. Hackers used phishing techniques in attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

March-April 2011. Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

March 2011. Hackers penetrated French government computer networks in search of sensitive information on upcoming G-20 meetings.

March 2011. The European Commission and EU's External Action Service are both targeted in a widespread espionage effort just before a major EU summit. Hackers were apparently very

interested in documents related to the G20 summit being held in Paris that year.

January 2011. French intelligence services are investigating possible Chinese involvement in the hack of car manufacturer Renault to obtain technologies related to electric vehicles.

January 2011. The Canadian government reported a major cyberattack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.

January 2011. Hackers extracted $6.7 million from South Africa's Postbank over the New Year's Holiday.

January 2011. Hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and steal more than $7 million in credits, forcing the market to shut down temporarily.

December 2010. India's Central Bureau of Investigation (CBI) website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected.

December 2010. British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defense contractor and other "British interests" that evaded defenses by pretending to come from the White House.

October 2010. Australia's Defence Signals Directorate reported a huge increase in cyberattacks on the military. Australia's Defence Minister, john Faulkner, revealed there had been 2400 "electronic security incidents" on Defence networks in 2009 and 5551 incidents between January and August 2010.

October 2010. The Wall Street Journal reported that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over $12 million from five banks in the US and UK. Zeus uses links in emails to steal account information, which the hackers then use to transfer money into bank accounts they control. 100 "mules", or low end criminals, were arrested for opening bank accounts under false names into which the hackers transferred stolen money.

October 2010. Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

October 2010. Public facing networks run by NASDAQ, as well as an information sharing application called Directors Desk, are compromised by an unknown external group. NASDAQ says it is unsure how far hackers might have penetrated into their network.

July 2010. A Russian intelligence agent (allegedly named Alexey Karetnikov), was arrested and

deported after working for nine months as a software tester at Microsoft.

May 2010. A leaked memo form the Canadian Security and Intelligence Service (CSIS) says that "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually un-attributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

May 2010. Chinese hackers breached the computer network of the U.S. Chamber of Commerce and stole information related to U.S. industries

April 2010. A Chinese telecommunications firm accidently transmitted erroneous routing information for roughly 37,000 networks, causing internet traffic to be misrouted through China. The incident lasted 20 minutes and exposed traffic from more than 8,000 U.S. networks, 8,500 Chinese networks, 1,100 Australian networks and 230 French networks.

April 2010. Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems.

March 2010. Unknown hackers post the real incomes of Latvian government officials after accessing their tax records, creating political turmoil.

March 2010. Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China to gain inside information on the trial defense strategy.

March 2010. Google announced that it had found malware targeting Vietnamese computer users. Google said that the malware was not especially sophisticated and was used to spy on "potentially tens of thousands of users who downloaded Vietnamese keyboard language software" the malware also launched distributed denial of service attacks against blogs containing political dissent, specifically, opposition to bauxite mining efforts in Vietnam.

March 2010. NATO and the EU warned that the number of cyberattacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

January 2010. Intel disclosed that it experienced a cyberattack at about the same time that Google, Adobe, and others were attacked. The hackers exploited the vulnerabilities in Internet Explorer software that had been used in the other attacks as well. Intel said that there was no intellectual property or financial loss.

January 2010. A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December with a similar message.

January 2010. M. K. Narayanan, India's National Security Adviser, said his office and other

government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to penetrate Indian government computers.

January 2010. Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers in December 2009, according to leaked e-mails from a cyber-security company working for the bank.

January 2010. Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

January 2010. The UK's MI5 Security Service warned that undercover intelligence officers from the People's Liberation Army and the Ministry of Public Security have approached UK businessmen at trade fairs and exhibitions with the offer of "gifts" - cameras and memory sticks - which contain malware that provides the Chinese with remote access to users' computers.

2010. The PLA infiltrated the computer network of a Civilian Reserve Air Fleet (CRAF) contractor in which documents, flight details, credentials and passwords for encrypted email were stolen

December 2009. Downlinks from U.S military UAVs were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV had viewed.

December 2009. The Wall Street Journal reported that a major U.S. bank had been is hacked, losing tens of millions of dollars.

November 2009. Jean-Pascal van Ypersele, the vice-chairman of the United Nations' Intergovernmental Panel on Climate Change, ascribed the hacking and release of thousands of emails, from the University of East Anglia's Climatic Research Unit to Russia as part of a plot to undermine the Copenhagen climate talks.

August 2009. Ehud Tenenbaum was convicted of stealing $10 million from U.S. banks. Tenenbaum was known for hacking into DOD computers in 1998, which resulted in a sentence of six months of community service from an Israeli court.

August 2009. Albert Gonzalez was indicted on charges that between 2006 and 2008, he and unidentified Russian or Ukrainian colleagues allegedly stole more than 130 million credit and debit cards by hacking into the computer systems of five major companies. This was the largest hacking and identity theft crime in U.S. history.

July 2009. Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention.

June 2009. German Interior Minister Wolfgang Schaeuble noted, when presenting the Interior

Ministry's 2008 security report, that China and Russia were increasing espionage efforts and Internet attacks on German companies.

June 2009. The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated.

May 2009. The Homeland Security Information Network (HSIN) was hacked by unknown intruders. The hackers gained access to the data by getting into the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed.

May 2009. In May 2009, Merrick Bank, a leading issuer of credit cards, claimed it lost $16 million after hackers compromised as many as 40 million credit card accounts.

April 2009. Chinese hackers reportedly infiltrated South Korea's Finance Ministry via a virus attached to e-mails claiming to be from trusted individuals.

April 2009. Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National Peoples Congress.

April 2009. Wall Street Journal articles laid out the increasing vulnerability of the U.S. power grid to cyberattack also highlighted was the intrusions into F-35 databases by unknown foreign intruders.

March 2009. Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

March 2009. Canadian researchers found a computer espionage system that they believe China implanted on the government networks of 103 countries.

March 2009. The German government warned that hackers were offering a free version of the new Microsoft operating system that installs Trojans.

March 2009. Chinese hackers stole information from the Office of Senator Bill Nelson in Florida

March 2009. Chinese hackers infiltrated Coca-Cola Co. computer networks and stole trade secret information, including information related to the attempted $2.4 billion acquisition of Huiyuan Juice Group

February 2009. French naval aircraft planes were grounded after military databases were infected with the "confickr" virus. Naval officials suspected someone in the Navy had used an infected USB key.

February 2009. 600 computers at India's Ministry of External Affairs were hacked.

February 2009. FAA computer systems were hacked. Increased use by FAA of IP-bases' networks also increases the risk of the intentional disruption of commercial air traffic.

January 2009. Indian Home Ministry officials warned that Pakistani hackers had placed malware on popular music download sites used by Indians in preparation for cyberattacks.

January 2009. Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.

2008. Britain's MPs were warned about e-mails apparently sent by the European Parliament amid fears that they could be used by Chinese hackers to implant viruses.

December 2008. Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some CSIS staff would go into the new administration and may have thought it might be interesting to read their emails beforehand.

December 2008. Retail giant TJX was hacked. The one hacker captured and convicted (Maksym Yastremskiy) is said to have made $11 million from the hack.

November 2008. Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and re-secure the networks.

November 2008. Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million dollars from machines in 49 cities.

November 2008. Chinese hackers infiltrated the computer networks of three major oil companies and stole trade secret information.

November 2008. Chinese hackers infiltrated the networks of Barack Obama and John McCain's presidential campaigns and exfiltrated information about future policy agendas.

November 2008. Chinese hackers infiltrated the computer network of the White House and obtained emails between senior government officials

October 2008. Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

August 2008. Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions.

Summer 2008. Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data

detailing the quantity, value, and location of oil discoveries around the world. One company put the losses in the millions.

Summer 2008. The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

June 2008. The networks of several Congressional offices were hacked by unknown foreign intruders. Some infiltrations involved offices with an interest in human rights in Tibet.

May 2008. The Times of India reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict.

May 2008. Belgium's Justice Minister China of hacking Belgian governmental computer networks.

April 2008. Germany's BND is accused of hacking Afghanistan's Commerce Minister and Ministry of Commerce and Industry networks, gaining access to internal email accounts and exfiltrating documents.

April – October 2008. A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department.

March 2008. U.S. officials reported that American, European, and Japanese companies were experiencing significant losses of intellectual property and business information to criminal and industrial espionage in cyberspace. However, details cannot be provided in an unclassified setting.

March 2008. South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.

January 2008. A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.

November 2007. Jonathan Evans, the head of Britain's Security Service (MI5), warned 300 business firms of the increased online threat from Russian and Chinese state organizations saying, "A number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They…increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks."

October 2007. More than a thousand staffers at Oak Ridge National Labs received an email with an attachment that, when opened, provides unknown outsiders with access to the Lab's databases.

October 2007. China's Ministry of State Security said that foreign hackers, 42% from Taiwan and 25% from United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

September 2007. British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments.

September 2007. Contractors employed by DHS and DOD had their networks hacked as backdoors into agency systems.

September 2007. Francis Delon, Secretary-General of National Defence in France, stated that information systems in France had been infiltrated by groups from China.

September 2007. Israel disrupted Syrian air defense networks (with some collateral damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility.

August 2007. The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

June 2007. The Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit DOD networks.

May 2007. Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well; however, they created a wave of fear in cyber dependent countries like the U.S.

May 2007. The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.

April 2007. The Department of Commerce had to take the Bureau of Industrial Security's networks offline for several months because its networks were hacked by unknown foreign intruders. This Commerce Bureau reviews confidential information on high tech exports.

2007. Chinese hackers breached the Pentagon's Joint Strike Fighter project and stole data related to the F-35 fighter jet

2006. Chinese hackers were thought to be responsible for shutting down the House of Commons computer system.

December 2006. NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.

November 2006. Hackers attempted to penetrate U.S. Naval War College networks, resulting in a two week shutdown at one institution while infected machines are restored.

August 2006. A senior Air Force Officer stated publicly that, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (the unclassified military network)."

May 2006. The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies had backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets, it would constitute an act of war. But when it happens in cyberspace, we barely notice.

April 2005. Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program.

2005. Chinese hackers infiltrated U.S. Department of Defense networks in an operation known as "Titan Rain." They targeted U.S. defense contractors, Army Information Systems Engineering Command; the Defense Information Systems Agency; the Naval Ocean Systems Center; and the U.S. Army Space and Strategic Defense installation.

2003. Chinese hackers exfiltrated national security information from Naval Air Weapons Station China Lake, including nuclear weapons test and design data, and stealth aircraft data.