

Photo: Adobe Stock

Significant Cyber Incidents

This timeline records significant cyber incidents since 2006. We focus on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

Download the Full Incidents List <https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_cyber_events.pdf>

Below is a summary of incidents from over the last year. For the full list, click the download link above.

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 exploiting IT supply chains.

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

February 2020. More than 10 countries accused Russia of being behind a series of cyber attacks against Georgia in 2019 that took thousands of websites for private, state, and media institutions offline

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 issue

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.

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.

TECHNOLOGY POLICY PROGRAM<<http://csis.org/programs/technology-policy-program>>

Cybersecurity and Governance <<http://csis.org/programs/technology-policy-program/cybersecurity-and-governance>>

Intelligence, Surveillance, and Privacy <<http://csis.org/programs/technology-policy-program/intelligence-surveillance-and-privacy>>

Significant Cyber Incidents <<http://csis.org/programs/technology-policy-program/significant-cyber-incidents>>

Technology and Innovation <<http://csis.org/programs/technology-policy-program/technology-and-innovation>>

Publicly Reported Iranian Cyber Actions in 2019 <<http://csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019>>

The Political Effect of the Internet <<http://csis.org/programs/technology-policy-program/political-effect-internet>>

Analysis <https://www.csis.org/analysis?&type=publication&field_categories_field_programs%5b1%5d=554&f%2525255b0%2525255d=field_categories%253afield_programs%3a554&f%2525255b1%2525255d=type%3apublication&=&type=publication&field_categories_field_programs%255b1%255d=554>

Occasional Paper Series <<http://csis.org/programs/technology-policy-program/occasional-paper-series>>

Podcasts <<http://csis.org/programs/technology-policy-program/podcasts>>

Blog <<http://csis.org/blogs/technology-policy-blog>>

Experts and Staff <<http://csis.org/programs/technology-policy-program/experts-and-staff>>

Subscribe to the Tech Update <<https://www.tfaforms.com/4693007>>

Survey of Chinese-linked Espionage in the United States Since 2000
<<http://csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000>>

 Find Additional Content <<http://csis.org/search?>

[f\[0\]=field_categories%253afield_programs%3a723](http://csis.org/search?f[0]=field_categories%253afield_programs%3a723)>

MEDIA QUERIES

Contact H. Andrew Schwartz

Chief Communications Officer

Tel: 202.775.3242


Contact Caleb Diamond
Media Relations Manager and Editorial Associate
Tel: 202.775.3173

RELATED

Cybersecurity <<http://csis.org/topics/cybersecurity-and-technology/cybersecurity>>, Cybersecurity and Governance <<http://csis.org/programs/technology-policy-program/cybersecurity-and-governance>>, Cybersecurity and Technology <<http://csis.org/topics/cybersecurity-and-technology>>, Significant Cyber Incidents <<http://csis.org/programs/technology-policy-program/significant-cyber-incidents>>, Technology Policy Program <<http://csis.org/programs/technology-policy-program>>

CONTACT CSIS

Email CSIS
Tel: 202.887.0200
Fax: 202.775.3199

 VISIT CSIS HEADQUARTERS
1616 Rhode Island Avenue, NW
Washington, DC 20036

MEDIA QUERIES

Contact H. Andrew Schwartz
Chief Communications Officer
Tel: 202.775.3242

Contact Caleb Diamond
Media Relations Manager and Editorial Associate
Tel: 202.775.3173

DAILY UPDATES

Sign up to receive *The Evening*, a daily brief on the news, events, and people shaping the world of international affairs.

SUBSCRIBE TO CSIS NEWSLETTERS <<http://csis.org/subscribe>>



FOLLOW CSIS

All content © 2020. All rights reserved.

Credits <<http://csis.org/credits>> | Privacy Policy <<http://csis.org/privacy-policy>> |
Reprint Permissions <<http://csis.org/reprint-permissions>>