Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Selected Cyberattacks, 2012-2021

November 22, 2021

Congressional Research Service
https://crsreports.congress.gov
R46974

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46974

November 22, 2021

Chris Jaikaran
Analyst in Cybersecurity Policy

Cybersecurity: Selected Cyberattacks, 2012-2021

Many Members of Congress have raised concerns over the frequency, types, and impacts of cyber incidents during hearings, speeches, and in legislation. Cyber incidents affect nearly every national entity, from federal and state government agencies to private companies and individuals. One course of action to stymie attacks has been to investigate who the adversaries are that conduct cyberattacks, what types of activities they conduct online, and how the U.S. government can identify them. To assist with Congress's understanding of cyberattacks, this report describes attribution in cyberspace, confidence of attribution, and common types of cyberattack. Listed in this report are two categories of cyberattacks by foreign adversaries against entities in the United States: 23 cyberattack campaigns that the federal government has attributed to actors operating on behalf of other nation-states, and 30 cyberattacks the government has attributed to criminal actors seeking personal gain.

In investigating cyber incidents, the U.S. government attempts to unmask those behind the incident and attribute it as an attack. Attributing cyberattacks is difficult, but not impossible. Officials seek to develop a comprehensive understanding of the cyber incident not just from the victim, but also by corroborating that information with other government and private sector evidence to make a claim of attribution. While a process exists to repeatedly and consistently develop a claim of attribution and a confidence level in it, adversaries take steps to complicate these efforts by obfuscating and removing any trace of their activity, and using new infrastructure to make it difficult to track attack campaigns.

Nation-states are some of the most sophisticated actors that conduct cyberattacks. The Director of National Intelligence is required annually to deliver to Congress an assessment from the intelligence community on worldwide threats. Recent assessments have highlighted cyberspace as an area of strategic concern, with Russia, China, Iran, and North Korea as the leading threat actors. Attacks from these countries include spying on government agencies by accessing agency computers, stealing sensitive information from public and private sector entities in the United States, stealing intellectual property, and destroying or potentially destroying computer equipment.

Cyber criminals are less resourced than nation-state actors and are less likely to employ novel and cutting-edge techniques in campaigns, yet their attacks are often highly effective. Most criminals are financially motivated and use cyberspace as a medium for conducting profit-bearing schemes. However, gaining money is not a requirement for illicit activity. Cyberattacks against victims in the United States from actors located abroad include compromising computers to create and maintain botnets, business email compromise schemes, hack and release campaigns, and ransomware attacks.

Contents

Tables

Contacts

Introduction

The frequency, type, and impact of cyber incidents against and in the United States continues to grow.[1] In an effort to address this challenge, policymakers are considering a variety of solutions, such as denying opportunities for successful attacks by improving defenses and deterring adversaries from engaging in disruptive activities in cyberspace. As Congress considers options for deterrence, knowledge of known adversaries, the types of activities they conduct online, and how they are identified by the U.S. government may inform the debate. With this information, policymakers may gain a greater understanding of the risks that the nation and specific sectors face.

This report describes selected cyberattacks against entities in the United States which were discovered or ended within the past 10 years (even if the activity was observed earlier) and includes information on claims of attribution in cyberspace, confidence of attribution, and common types of cyberattack. Listed in this report are two categories of cyberattacks: 23 cyberattack campaigns that the government has attributed to actors operating on behalf of a nation-state, and 30 cyberattacks the government has attributed to criminal actors seeking personal gain.

Attribution

Attributing a cyberattack is difficult, but not impossible. Government investigators seek to develop a comprehensive understanding of cyber incidents from not just the victim but also by corroborating information in order to make claims of attribution.

First, investigators look at the attributes of the event itself, such as the *tradecraft* employed by the adversary (i.e., techniques, tactics, and procedures used to carry out the attack), any *malware* used (i.e., the type of the software that exploited a vulnerability for access), and the features of the attack (e.g., logging key stokes or encrypting data). Then investigators seek to discover the *infrastructure* used to carry out the attack (e.g., the command and control servers communicating with the malware). They will combine this information with government and industry analysis on an attacker's *intent* (e.g., reasons for targeting a particular victim) and information from external sources (e.g., cybersecurity firm reports, think tank analysis, and news media).[2] In analyzing this information, investigators will seek to minimize human error, substantiate hypotheses among various sources, and entertain competing theories of attribution. Finally, investigators typically provide their assessment and a confidence level.

- *High confidence* reflects an assessment that investigators believe beyond a reasonable doubt and without a viable alternative that the attributed party is responsible for the attack.
- *Moderate confidence* means that investigators believe that the evidence is clear and convincing, but alternatives are possible.
- *Low confidence* is used when evidence points to a particular actor, but there are significant information gaps.[3]

[1] Statista, *U.S. Companies and Cyber Crime*, 2021, https://www.statista.com/study/12881/smb-and-cyber-crime-in-the-united-states-statista-dossier/.

[2] Office of the Director of National Intelligence, *A Guide to Cyber Attribution*, report, September 14, 2018, at https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

[3] Ibid.

Developing a claim of attribution remains difficult despite having a process to determine attribution and a system for articulating confidence in a claim. For example, sophisticated actors continue to develop and deploy novel techniques and establish new infrastructure for different attacks, which may make it difficult to track known activity from one attack to another. Additionally, they will seek to obfuscate their activity as legitimate and remove records of their actions on a network.

Claims of attribution appear in a variety of sources. The authoritativeness of these sources exist on a spectrum. At the highest level of authority are *primary* sources, followed by *secondary* sources, *supposed* sources, and, finally, *conjecture* being the least authoritative. With regards to cyberattack attribution:

- **Primary** sources include statements by a U.S. government entity. A court finding that a party was guilty of committing the attack—usually by violating the Computer Fraud and Abuse Act[4] or the Economic Espionage Act[5]—is the most authoritative. A grand jury indictment is slightly less authoritative. An official statement by a government official (e.g., a press briefing by the National Security Advisor) providing attribution to a party is the least authoritative of the primary sources. Evidence of why a primary source believes a party is responsible for an attack is usually included in public documentation along with the claim and can be further examined (e.g., an unsealed indictment).
- **Secondary** sources include claims by non-governmental entities. These attributions frequently come from a cybersecurity firm releasing research on an adversary or attack campaign. These claims usually include research into the tradecraft, malware, infrastructure, and intent of a campaign or attack. Secondary sources usually include evidence to support their claims. However, private entities usually do not have access to classified government information (e.g., signals intelligence), which can further corroborate a claim of attribution. Cybersecurity firms have generally avoided attributing attacks to nation-states. Instead, a firm will attribute an attack to an actor set that the firm is tracking. These actor sets are sometimes referred to as an Advanced Persistent Threat (APT) or by a codename used for that company's research.
- **Supposed** sources are predominantly composed of statements reported by mainstream news media. These statements are frequently attributed to unidentified government officials and corroborated with other primary or secondary sources. However, these statements cannot otherwise be independently examined.
- **Conjecture** includes claims by victims that a certain party is responsible for an attack, or claims on social media platforms of attribution. These statements rarely include evidence or provide analysis.

[4] 18 U.S.C. §1030. For more information on the Computer Fraud and Abuse Act, see CRS Report R46536, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, by Peter G. Berris.

[5] 18 U.S.C. §§1831-1832. For more information on the Economic Espionage Act, see CRS Report R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, by Charles Doyle.

Common Cyberattack Terms

"Cyberattack" is a broad term for a variety of malicious actions against information and communications technologies. Below are a selection of common cyberattacks (in alphabetical order).

Botnet: A portmanteau of "robot" and "network" which refers to a collection of computers for which control has been seized by one or more unauthorized parties. Once an unauthorized party controls an individual computer, they may then connect it to other computers in their control to create a pool of computing resources (e.g., network bandwidth or processing power). Botnets are used to further illicit activity online, such as distributing malware and surreptitiously mining cryptocurrencies.

Business Email Compromise: A scam in which an attacker creates an email address (usually of a high ranking official in an organization) and alters the identifying information of that email to make it appear to come from the organization (e.g., changing the name associated with the email address). Typically, scammers then email members of that organization with urgent needs for funds to be transferred. These are sometimes under the guise of paying past due invoices. However, the invoices are fraudulent and the accounts where the funds are to be transferred belong to the scammers.

Denial of Service (DOS) or **Distributed Denial of Service (DDOS):** A DOS attack inhibits an authorized user's ability to access a resource (e.g., a website) by overwhelming that resource with unauthorized requests (e.g., more requests to load a webpage than it was built to support). DDOS attacks are more common and use many hosts to attack a single resource (e.g., a network of malware-infected computers—a botnet—sending junk web traffic to a single service provider).

Hack and Leak: An attack in which an unauthorized party gains access to a sensitive data store and exfiltrates (steals) the data. Once the sensitive data is in their control, the attacker either releases the data in an effort to expose or embarrass the victim or contacts the victim and demands a ransom in order to not release the data.

Phishing: An attack which attempts to gain access to a system by tricking authorized users into engaging with malicious computer code. Frequently, this attack is carried out by combining an email which uses social-engineering (i.e., an attempt to manipulate someone into revealing information or taking some action) with a malicious web link or attachment. When the web link is clicked or attachment opened, the device downloads and executes malware.

Malware: A portmanteau of "malicious" and "software" which refers to software and firmware intentionally added to an information technology (IT) product and designed to cause harm to the IT product or its data. There are many ways malware can be added to a product, such as from an inserted USB drive or downloaded from the internet. Data may be harmed by making it no longer private (i.e., compromising its confidentiality), manipulating it (i.e., compromising its integrity), or deleting it (i.e., compromising its availability).

Malvertising: A portmanteau of "malicious" and "advertising." This attack uses online advertising networks to spread malware and compromise computer systems. Malvertisers buy ad-space and inject malware into those ads in an effort to easily spread it online. When a user visits a website, they may be presented with the ad and download the malicious code via a legitimate advertising network. If the code downloads and successfully executes, then the computer succumbs to malware. Generally, neither the website delivering the ad nor the advertising networks are aware of the malicious code being delivered.

Man-in-the-Middle (MitM): An attack where a malicious actor seeks to insert itself between two computers in an effort to access the communications between those computers, usually in an effort to eavesdrop between the users of those computers (either directly, or by intercepting encryption keys so that encrypted text may be decrypted).

Ransomware: A portmanteau of "ransom" and "malware." Ransomware attacks seek to deny users access to data and IT systems by encrypting files and systems—thus, locking out users. Perpetrators usually extort victims for payment, typically in cryptocurrency, to decrypt the system. Recently, such attacks have been coupled with data breaches in which perpetrators also steal data from their victims. In addition to locking the computer systems, the perpetrators typically notify victims that they have copies of their data and will release sensitive information unless a ransom is paid, potentially extorting them twice. A triple extortion may occur if the perpetrators contact a company's clients to tell them about the attack in an effort to pressure the victim to pay the ransom or risk harming their future business prospects.

Supply Chain Attack: An attack in which an adversary inserts an unauthorized physical or software component into a product in order to surreptitiously access data or manipulate a system. These attacks can occur during any phase of a product lifecycle (e.g., development, shipping, or updating).[6]

Zero-Day: An attack that exploits a previously unknown vulnerability in an IT product. This type of attack is particularly dangerous because until it is noticed, there is usually no defense against it. This attack is sometimes written as "0-Day" and sometimes pronounced "oh-day."

These attacks may be used alone or in conjunction to conduct a variety of computer network operations (CNO), such as computer network exploitation (CNE) for the purposes of espionage or computer network attack (CNA) to disrupt a targeted victim.

Methodology

To develop the list of attacks, CRS considered only primary sources (explained further in the "Attribution" section). CRS searched for public statements on U.S. government websites belonging to the Department of Defense (DOD), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Office of the Director of National Intelligence (ODNI), and the Cybersecurity and Infrastructure Security Agency (CISA). Search terms (e.g., "cyber" and "state-sponsored") and topic filters (e.g., "national security" and "cybersecurity") were used to refine search results.

The results reflect the cybersecurity and legal communities' broad public understanding of responsible parties, but should not be considered comprehensive. DOJ's website only publishes press releases from 2009 onward, limiting the number of available press releases and indictments available for the search. There may be additional indictments that are not publicized but unsealed and available in court proceeding databases. Those documents are not searchable and accessible via the public internet, and are therefore not included in these results. Additionally, government officials may attribute a particular campaign to a nation-state actor or criminal group, but have not made evidence or corroborating information available (e.g., a list of victims or naming a specific actor in country). Such instances are not included in this list.

Tables are organized by attack and campaign year. The country of origin and entity responsible for a particular attack or campaign are listed next to it, followed by a short description. Colloquial

[6] For more information, see CRS In Focus IF10920, *Cyber Supply Chain Risk Management: An Introduction*, by Chris Jaikaran.

country names and abbreviations for the perpetrating entity are used in the tables. Full names are provided in the table notes. Further information is available in the citation provided for each row. In some cases, many individual attacks were combined in a single indictment against actors working in a single campaign. Nation-state campaigns are identified by their Advanced Persistent Threat (APT) identifier, as those are commonly used monikers in the cybersecurity community.

Other inventories of cyberattacks have many more incidents.[7] These inventories use different methodologies which have different criteria for attribution confidence and include unidentified victims and victims outside the United States.

Nation-State Cyberattacks

The Director of National Intelligence is required annually to deliver to Congress an assessment from the intelligence community on worldwide threats.[8] Recent assessments have highlighted cyberspace as an area of strategic concern, with Russia,[9] China,[10] Iran,[11] and North Korea[12] as the leading threat actors.[13] **Table 1** lists 23 selected cyberattack campaigns against the United States attributed to nation-state actors operating on behalf of a country. These attacks include spying on government agencies by accessing agency computers, stealing sensitive information from public and private sector entities in the United States to undermine confidence in those entities, stealing intellectual property to bolster national companies, and destroying or potentially destroying computer equipment.

[7] For examples, see Center for Strategic and International Studies, "Significant Cyber Incidents," website, 2021, at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; and Council on Foreign Relations, "Cyber Operations Tracker," website, 2021, at https://www.cfr.org/cyber-operations/.

[8] 50 U.S.C. §3043b.

[9] For more information, see CRS In Focus IF11718, *Russian Cyber Units*, by Andrew S. Bowen. For technical information, see Cybersecurity and Infrastructure Security Agency, "Russia Cyber Threat Overview and Advisories," website, at https://us-cert.cisa.gov/russia.

[10] For more information, see CRS In Focus IF11284, *U.S.-China Trade Relations*, by Karen M. Sutter. For technical information, see Cybersecurity and Infrastructure Security Agency, "China Cyber Threat Overview and Advisories," website, at https://us-cert.cisa.gov/china.

[11] For more information, see CRS In Focus IF11406, *Iranian Offensive Cyberattack Capabilities*, by Catherine A. Theohary. For technical information, see Cybersecurity and Infrastructure Security Agency, "Iran Cyber Threat Overview and Advisories," website, at https://us-cert.cisa.gov/iran.

[12] For more information, see CRS Report R44912, *North Korean Cyber Capabilities: In Brief*, by Emma Chanlett-Avery et al. For technical information, see Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," website, at https://us-cert.cisa.gov/northkorea.

[13] For examples, see Avril Haines, *Annual Threat Assessment*, remarks as prepared, April 14, 2021, at https://www.dni.gov/files/documents/Newsroom/Testimonies/2021-04-14-ATA-Opening-Statement-FINAL.pdf; and James R. Clapper, *Worldwide Threat Assessment of the U.S. Intelligence Community*, statement for the record, February 25, 2016, at https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf.

Table 1. Selected Cyberattack Campaigns Attributed to Nation States

In Descending Order by Campaign Year: 2021-2012

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2021	Iran	N/A	N/A	Government-sponsored actors exploiting vulnerabilities in email and security appliances to gain access to U.S. critical infrastructure. Once they have access, they conduct follow on theft, encryption, ransomware and extortion operations.	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Australian Cyber Security Centre, and National Cyber Security Centre, "Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities," AA21-321A, November 17, 2021, at https://us-cert.cisa.gov/sites/default/files/publications/AA21-321A-Iranian%20Government-Sponsored%20APT%20Actors%20Exploiting%20Vulnerabilities_1.pdf.
2020-2021	China	MSS	Hafnium	Exploited previously unknown vulnerabilities in on-premise Microsoft Exchange servers to gain access to sensitive data.	The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," press release, July 19, 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.
2020-2021	Russia	SVR	SolarWinds	Conducted a supply-chain attack against a widely used software management company to gain access to government and private sector networks.	Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), press release, January 5, 2021, at https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.
2020	Iran	Kazemi and Kashian[a]	2020 U.S. Presidential Election Disinformation and Election Infrastructure Hacking	Hacked into state election websites and accessed voter information on over 100,000 citizens. Sent disinformation to politicians and the media claiming to be from voters. Intimidated voters online. Attempted to hack into a media company to spread further disinformation.	Department of Justice, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election" press release, November 18, 2021, at https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2020	Iran	MOIS & IRGC	APT-39	Stole data pertaining to national security, foreign policy intelligence, non-military nuclear information, aerospace data, human rights activist information, individual financial information and PII, and intellectual property, including unpublished scientific research.	Department of Justice, "Department of Justice and Partner Departments and Agencies Conduct Coordinated Actions to Disrupt and Deter Iranian Malicious Cyber Activities Targeting the United States and the Broader International Community," press release, September 17, 2020, at https://www.justice.gov/opa/pr/department-justice-and-partner-departments-and-agencies-conduct-coordinated-actions-disrupt.
2014-2020	China	MSS	APT-41	Targeted IT companies, telecommunications companies, academic institutions, NGOs, and pro-democracy activists to steal intellectual property; deployed ransomware; and used illegally accessed computers to mine cryptocurrency.	Department of Justice, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally," press release, September 16, 2020, at https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2014-2020	North Korea	RGB	APT-38	Destroyed computers of Sony Pictures Entertainment over the release of *The Interview*; compromised the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network to steal money from banks; created and deployed the WannaCry 2.0 ransomware; created malicious cryptocurrency wallets; compromised cryptocurrency companies to steal cryptocurrencies; and conducted spear phishing campaigns against defense contractors, energy companies, aerospace companies, technology companies, the U.S. Department of State, and the U.S. Department of Defense.	Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," press release, February 17, 2021, at https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.
2013-2020	Iran	Criminal group operating on behalf of the state	N/A	Targeted universities, think tanks, defense contractors, and aerospace companies to steal sensitive data.	Department of Justice, "Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East," press release, September 16, 2020, at https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states.
2009-2020	China	MSS	N/A	Targeted technology manufacturing, healthcare, energy, defense, business, educational, and gaming companies to steal intellectual property and confidential business information, including COVID-19 research.	Department of Justice, "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research," press release, July 21, 2020, at https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2015-2019	Iran	IRGC	APT-33	Conducted spear phishing attacks against satellite and aerospace company employees to gain access to company networks, steal identities, and use malware to steal intellectual property and sensitive data.	Department of Justice, "State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies," press release, September 17, 2020, at https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies.
2015-2018	Russia	GRU	Sandworm	Attacked the Ukrainian government and critical infrastructure (BlackEnergy); sought to interfere in the French national elections; conducted the NotPetya attacks against U.S.-based hospitals, shipping companies, and pharmaceutical companies; sought to undermine the PyeongChang Winter Olympics; spear phished investigators of the Novichok poisoning to gain sensitive data; and sought to compromise Georgian government entities.	Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, October 19, 2020, at https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2014-2018	Russia	GRU	N/A	Conducted disinformation operations. Hacked into computers belonging to the World Anti-Doping Agency (WADA), United States Anti-Doping Agency (USADA), Rio de Janeiro Olympic and Paralympic games, Fédération Internationale de Football Association (FIFA), Westinghouse Electric Company's (WEC), and the [Organization] for the Prohibition of Chemical Weapons (OPCW). Published stolen and altered information from these entities to retaliate for and delegitimize doping charges against Russia's sporting organizations.	Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018, at https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.
2013-2018	Iran	IRGC	Mabna Institute	Stole academic data and intellectual property from universities, companies, and government agencies.	Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," press release, March 23, 2018, at https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.
2011-2018	China	MSS	APT-40	Stole the intellectual property of companies dealing with submersibles, autonomous vehicles, chemicals, aircraft, genetics, transportation, and infectious disease research.	Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," press release, July 10, 2021, at https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2006-2018	China	MSS	APT-10	Targeted and stole intellectual property and confidential business information from transportation, technology, shipping, consulting, healthcare, and energy companies through cloud and managed service providers.	Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," press release, December 20, 2018, at https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.
2017	China	PLA	Equifax Hack	Theft of the PII of nearly 150 million Americans.	Department of Justice, "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," press release, February 10, 2020, at https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.
2016	Russia	GRU	DCLeaks and Guccifer 2.0	Targeted political campaigns, state boards of elections, state secretaries of state, and companies providing technology for elections to steal and leak their sensitive data.	Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," press release, July 13, 2018, at https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
2014-2016	Russia	FSB	Yahoo Breach	Breach of 500 million accounts and other webmail account compromises targeted journalists, government officials, cybersecurity company employees, financial services companies, and transportation companies to steal sensitive information.	Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," press release, March 15, 2017, at https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
2015	China	Fujie Wang, and others[b]	Anthem Hack	Stole massive amounts of PII held by the health insurance company Anthem Inc., as well as other companies.	Department of Justice, "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," press release, May 9, 2019, at https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.

Incident/ Campaign Year(s)	Attributed Country	Perpetrating Entity	Campaign, Incident, or Identifier	Description	Citation
2014-2015	Iran	IRGC	N/A	Targeted intelligence community (IC) employees as part of an intelligence campaign with fake accounts used to deploy malware.	Department of Justice, "Former U.S. Counterintelligence Agent Charged with Espionage on Behalf of Iran; Four Iranians Charged with a Cyber Campaign Targeting Her Former Colleagues," press release, February 13, 2019, at https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber.
2010-2015	China	MSS	N/A	Targeted aerospace companies to steal intellectual property related to turbofan engine technology.	Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," press release, October 30, 2018, at https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.
2006-2014	China	PLA	N/A	Hacked into computers of U.S. manufacturers in order to steal sensitive information to benefit Chinese state enterprises.	Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014, at https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
2011-2013	Iran	ITSecTeam & Mersad Company	N/A	Waged DDOS attacks against financial services companies, and hacked into networks of a municipal dam in Rye Brook, N.Y.	Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," press release, March 24, 2016, at https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

Source: CRS analysis.

Notes: Abbreviations used in the table include: Advanced Persistent Threat (APT); Democratic People's Republic of North Korea (North Korea); Distributed Denial of Service (DDOS); Federal Security Service (FSB); Islamic Republic of Iran (Iran); Islamic Revolutionary Guard Corps (IRGC); The People's Republic of China (China); Main Intelligence Directorate, Military (GRU); Intelligence Community (IC); Ministry of Intelligence and Security (MOIS); Ministry of State Security (MSS); People's Liberation Army (PLA); Personal Identifiable Information (PII); The Russian Federation (Russia); Reconnaissance General Bureau (RGB); and Russia's Foreign Intelligence Service (SVR).

a. Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian are the two Iranian nationals charged. The indictment claims that they work for an Iranian company now known as Emennet Pasargad. The company is known to have provided services to the Iranian government and the Guardian Council.

b. The indictment does not attribute this attack as being for the benefit of the state. However, government officials have since speculated that this was under the direction of the Chinese government—see, Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic

and National Security of the United States," remarks to the Hudson Institute as delivered, July 7, 2020, at https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

Foreign Criminal Cyberattacks

Most criminals are financially motivated and use cyberspace as a medium for conducting profit-bearing schemes. However, financial gain is not a requirement for illicit activity. Some malicious actors also victimize entities online without desires for payment, such as in hack and leak operations intended to embarrass the victim. **Table 2** lists a selection of 30 cyberattacks against victims in the United States from actors located abroad. The country of residence for the perpetrator is included for each cyberattack campaign to highlight the geographic diversity from where attacks originate. Some campaigns were part of criminal groups and others are conducted by individuals, as indicated for each entry in the table. The U.S. government has determined that these actors were not operating to benefit the state, but where acting for personal gain—thus distinguishing these attacks from those listed in **Table 1**. Criminal cyberattacks also originate from U.S. individuals but are not included in this table as those individuals may face both state and federal criminal charges, which the search methodology does not take into account. These attacks include the compromise of computers to create and maintain botnets, business email compromise schemes, hack and release campaigns, and ransomware attacks.

Table 2. Selected Criminal Cyberattacks

In Descending Order by Campaign Year: 2021-2012

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2021	Ukraine and Russia	Multiple	REvil ransomware and Kaseya attack	Hackers built and distributed the Sodinokibi and REvil ransomware attacks. They conducted a supply chain attack against an IT management company to distribute ransomware to new victims.	Department of Justice, "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," press release, November 8, 2021, at https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.
2019-2021	Switzerland	Single	Hack & Leak	Hacked into U.S. companies and posted sensitive data.	Department of Justice, "Swiss Hacker Indicted for Conspiracy, Wire Fraud, and Aggravated Identity Theft," press release, March 18, 2021, at https://www.justice.gov/usao-wdwa/pr/swiss-hacker-indicted-conspiracy-wire-fraud-and-aggravated-identity-theft.
2011-2021	Moldova	Multiple	Bugat Botnet	Targeted school districts, banks, and energy companies to wire funds illicitly.	Department of Justice, "Bugat Botnet Administrator Arrested and Malware Disabled," press release, October 13, 2015, at https://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled.
2016-2020	Iran	Multiple	N/A	Defaced websites by changing them to protest U.S. government policies and actions. Stole credit card information and distributed spam emails.	Department of Justice, "Two Alleged Hackers Charged with Defacing Websites Following Killing of Qasem Soleimani," press release, September 15, 2020, at https://www.justice.gov/opa/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani.
2016-2020	Ukraine	Multiple	N/A	Hacked into computers, stole user credentials, managed a botnet of hacked computers and sold access online.	Department of Justice, "Ukrainian Cyber Criminal Extradited For Decrypting The Credentials Of Thousands Of Computers Across The World And Selling Them On A Dark Web Website," press release, September 8, 2021, at https://www.justice.gov/usao-mdfl/pr/ukrainian-cyber-criminal-extradited-decrypting-credentials-thousands-computers-across.

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2015-2020	Latvia	Multiple	Trickbot	Targeted hospitals, schools, utilities, and governments to steal financial information.	Department of Justice, "Latvian National Charged for Alleged Role in Transnational Cybercrime Organization," press release, June 4, 2021, at https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization.
2019	Nigeria	Multiple	Hushpuppi	Conducted business email compromise and money laundering campaigns.	Department of Justice, "Six Indicted in International Scheme to Defraud Qatari School Founder and Then Launder over $1 Million in Illicit Proceeds," press release, July 29, 2021, at https://www.justice.gov/usao-cdca/pr/six-indicted-international-scheme-defraud-qatari-school-founder-and-then-launder-over-1.
2013-2019	Romania, Bulgaria, U.S.A.	Multiple	Fraud	Sold non-existent goods online and attacked credentials for web services.	Department of Justice, "United States and International Law Enforcement Dismantle Online Organized Crime Ring Operating out of Romania that Victimized Thousands of U.S. Residents," press release, February 7, 2019, at https://www.justice.gov/opa/pr/united-states-and-international-law-enforcement-dismantle-online-organized-crime-ring.
2015-2018	Ukraine	Multiple	Fin7	Targeted retailers and point-of-sale terminals to steal credit card information.	Department of Justice, "Three Members of Notorious International Cybercrime Group "Fin7" in Custody for Role in Attacking over 100 U.S. companies," press release, August 1, 2018, at https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100.
2015-2018	Iran	Multiple	SamSam Ransomware	Conducted ransomware attacks against state and city government agencies, hospitals, and other victims.	Department of Justice, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," press release, November 28, 2018, at https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.
2013-2018	Ukraine	Single	Malvertising campaign	Delivered online advertisements embedded with malware.	Department of Justice, "International 'Malvertiser' Extradited from the Netherlands to Face Hacking Charges in New Jersey," press release, May 3, 2019, at https://www.justice.gov/opa/pr/international-malvertiser-extradited-netherlands-face-hacking-charges-new-jersey.

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2007-2018	Romania	Single	N/A	Targeted customers of the Better Business Bureau, the Internal Revenue Service, the U.S. Tax Court, the National Payroll Records Center, and others with phishing and fraudulent online auctions.	Department of Justice, "Leader of International Cyber Fraud Ring Returned to United States to Face Federal Racketeering Charges," press release, October 9, 2018, at https://www.justice.gov/opa/pr/leader-international-cyber-fraud-ring-returned-united-states-face-federal-racketeering.
2017	Romania	Multiple	Ransomware	Targeted Metropolitan Police Department surveillance cameras and compromised those devices to distribute ransomware.	Department of Justice, "Two Romanian Suspects Charged with Hacking of Metropolitan Police Department Surveillance Cameras in Connection with Ransomware Scheme," press release, December 28 2017, at https://www.justice.gov/usao-dc/pr/two-romanian-suspects-charged-hacking-metropolitan-police-department-surveillance-cameras.
2017	Turkey	Single	WireX Botnet	Used the WireX Botnet in a DDOS attack against a hospitality company.	Department of Justice, "Federal Indictment in Chicago Charges Turkish National with Directing Cyber Attack on Multinational Hospitality Company," press release, September 29, 2021, at https://www.justice.gov/usao-ndil/pr/federal-indictment-chicago-charges-turkish-national-directing-cyber-attack.
2016-2017	United Kingdom	Single	Dark Overlord	Breached the network of a business in St. Louis, MO, stole sensitive data, and threatened to release it unless a ransom was paid.	Department of Justice, "Member of 'The Dark Overlord' Hacking Group Extradited from United Kingdom to Face Charges in St. Louis," press release, December 18, 2019, at https://www.justice.gov/opa/pr/member-dark-overlord-hacking-group-extradited-united-kingdom-face-charges-st-louis.
2014-2017	Cyprus	Single	N/A	Hacked into a company's data store, stole sensitive information, then extorted the company for a fee to not release information. With persistent access, charged clients to remove unfavorable information from the company's records.	Department of Justice, "Two Alleged Criminals – A Hezbollah Associated Narco-Money Launderer and a Computer Hacker – Extradited from Cyprus to the United States," press release, July 18, 2020, at https://www.justice.gov/opa/pr/two-alleged-criminals-hezbollah-associated-narco-money-launderer-and-computer-hacker.

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2014-2017	Russia, Ukraine, and Kazakhstan	Multiple	MethBot	Built a botnet and maintained infrastructure to operate a malvertising campaign.	Department of Justice, "Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud," press release, November 27, 2018, at https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing.
2011-2017	China	Multiple	Economic Espionage	Targeted firms working on satellite, energy, technology, transportation, and economic analysis to steal credentials and access sensitive data.	Department of Justice, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," press release, November 27, 2017, at https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.
2010-2017	Russia	Single	Kelihos Botnet	Stole PII and credentials, distributed spam and malware, engaged in pump-and-dump stock schemes.	Department of Justice, "Russian National Indicted with Multiple Offenses in Connection with Kelihos Botnet," press release, April 21, 2017, at https://www.justice.gov/opa/pr/russian-national-indicted-multiple-offenses-connection-kelihos-botnet.
2010-2017	Russia	Multiple	InFraud Organization	Targeted financial institutions, merchants, and individuals to steal credit cards, PII, identities and engage in other crimes.	Department of Justice, "Russian National Pleads Guilty for Role in Transnational Cybercrime Organization Responsible for More Than $568 Million in Losses," press release, June 26, 2020, at https://www.justice.gov/opa/pr/russian-national-pleads-guilty-role-transnational-cybercrime-organization-responsible-more.
2015-2016	Russia, Georgia, Ukraine, Moldova, and Bulgaria	Multiple	GozNym Malware	Stole banking information from a paving company, law firms, churches, companies providing services to disabled individuals, medical equipment distributers, casinos, and furniture stores.	Department of Justice, "GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation," press release, May 16, 2019, at https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled.

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2007-2016	Romania	Multiple	Botnet	Developed malware that spread to more than 60,000 computers, creating a botnet used to mine cryptocurrency, send spam email, and steal credentials and financial information.	Department of Justice, "Three Romanian Nationals Indicted in $4 Million Cyber Fraud Scheme That Infected at Least 60,000 Computers and Sent 11 Million Malicious Emails," press release, December 16, 2016, at https://www.justice.gov/opa/pr/three-romanian-nationals-indicted-4-million-cyber-fraud-scheme-infected-least-60000-computers.
2016	Ukraine	Multiple	SEC EDGAR Compromise	Infiltrated the SEC EDGAR filing system to glean non-public company information in order to trade in company stock based on private information.	Department of Justice, "Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission," press release, January 15, 2019, at https://www.justice.gov/opa/pr/two-ukrainian-nationals-indicted-computer-hacking-and-securities-fraud-scheme-targeting-us.
2015	Kosovo	Single	Kosova Hacker's Security	Targeted PII of U.S. service members and government employees.	Department of Justice, "ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges," press release, October 15, 2015, at https://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges.
2007-2015	Ukraine	Single	Money Laundering	Spammed victims, maintained infrastructure to perpetuate cybercrimes, and stole money from company bank accounts.	Department of Justice, "Ukrainian National Extradited from Poland to Face Charges Related to $10 Million Cyber Money Laundering Operation," press release, December 23, 2015, at https://www.justice.gov/opa/pr/ukrainian-national-extradited-poland-face-charges-related-10-million-cyber-money-laundering.
2012-2014	Romania	Single	Guccifer	Hacked the personal email and social media accounts of high profile individuals and released sensitive information.	Department of Justice, "Romanian National "Guccifer" Extradited to Face Hacking Charges," press release, April 1, 2016, at https://www.justice.gov/opa/pr/romanian-national-guccifer-extradited-face-hacking-charges.
2010-2012	Ukraine/Italy	Single	Zeus Malware	Targeted banks and banking information for financial theft.	Department of Justice, "Ukrainian Citizen Sentenced to 41 Months in Prison for Using Army of 13,000 Infected Computers to Loot Log-In Credentials, Payment Card Data," press release, February 16, 2017, at https://www.justice.gov/usao-nj/pr/ukrainian-citizen-sentenced-41-months-prison-using-army-13000-infected-computers-loot-log.

Incident/ Campaign Year(s)	Perpetrator Country of Residence	Single or Multiple Perpetrators	Campaign, Incident, or Identifier	Description	Citation
2009-2012	China	Single	N/A	Targeted U.S. defense contractors to steal sensitive military transport design data and send the data to China.	Department of Justice, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," press release, March 23, 2016, at https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive.
2003-2012	Russia	Multiple	N/A	Theft of credit card information from payment processors, financial institutions, and retailers.	Department of Justice, "Russian National Admits Role in Largest Known Data Breach Conspiracy Ever Prosecuted," press release, September 15, 2015, at https://www.justice.gov/opa/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-prosecuted.
2012	Iran/Turkey	Single	N/A	Stole intellectual property from a Vermont-based defense contractor and engineering firm.	Department of Justice, "Man Pleads Guilty to Facilitating Computer Hacking of Vermont Company," press release, December 2, 2015, at https://www.justice.gov/opa/pr/man-pleads-guilty-facilitating-computer-hacking-vermont-company.

Source: CRS analysis.

Notes: Abbreviations and colloquialisms used in this table: the Republic of Bulgaria (Bulgaria); the People's Republic of China (China); the Republic of Cyprus (Cyprus); the Electronic Data Gathering, Analysis, and Retrieval system (EDGAR); the Federal Republic of Nigeria (Nigeria); the Islamic Republic of Iran (Iran); the Italian Republic (Italy); the Republic of Kazakhstan (Kazakhstan); the Republic of Kosovo (Kosovo); the Republic of Moldova (Moldova); personally identifiable information (PII); the Russian Federation (Russia); the U.S. Securities and Exchange Commission (SEC); the Swiss Confederation (Switzerland); the Republic of Turkey (Turkey); the United States of America (U.S.A.); and the United Kingdom of Great Britain and Northern Ireland (United Kingdom).

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Acknowledgments

Jared Nagel, Information Research Specialist with CRS, provided research support in identifying cyberattacks.

Disclaimer