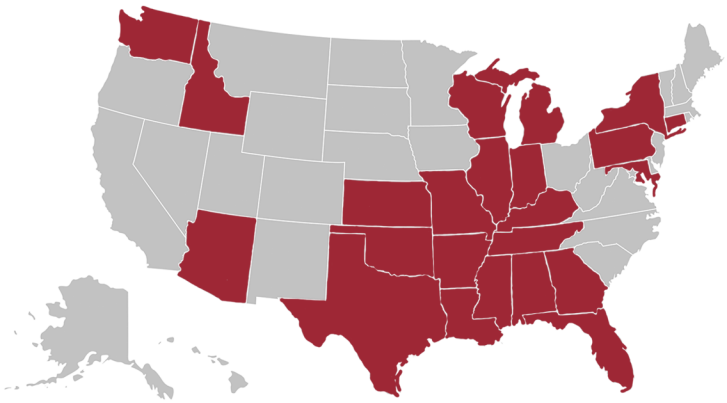
CYBER THREAT SNAPSHOT

MALIGN NATION-STATES AND OPPORTUNISTIC CRIMINAL NETWORKS:
A PERSISTENT CYBER THREAT IN AMERICA

NATIONWIDE IMPACTS OF ASCENSION HEALTHCARE HACKS



LOCATIONS OF ASCENSION HEALTH MINISTRIES AND AFFILIATES

IN MAY 2024, A THREAT ACTOR EXPLOITED KNOWN VULNERABILITIES USING A PHISHING ATTEMPT, IMPACTING IT NETWORKS IN **ALL 142 ASCENSION HOSPITALS IN THE UNITED STATES**.

STARTLING STATISTICS:

- THE AVERAGE COST OF A DATA BREACH IN THE U.S. AMOUNTS TO **$9.36 MILLION**, ALMOST DOUBLE THAT OF THE GLOBAL AVERAGE.
- RANSOMWARE ATTACKS **ROSE 74%** FROM 2022 TO 2023.
- CYBERATTACKS ON CRITICAL INFRASTRUCTURE GLOBALLY **INCREASED 30%** IN 2023.
- **1 IN 10 CYBER INTRUSIONS** IN 2023 WERE DUE TO CREDENTIALS ACCESS.
- **ONE IN THREE AMERICANS** WERE AFFECTED BY HEALTHCARE DATA BREACHES LAST YEAR.
- GOVERNMENT AGENCIES WERE THE **THIRD-MOST TARGETED** SECTOR FOR RANSOMWARE ATTACKS IN 2023.
- THERE ARE ROUGHLY **500,000 VACANT CYBERSECURITY JOBS** IN THE UNITED STATES.

NOTABLE RECENT ATTRIBUTABLE THREAT ACTOR ACTIVITY:

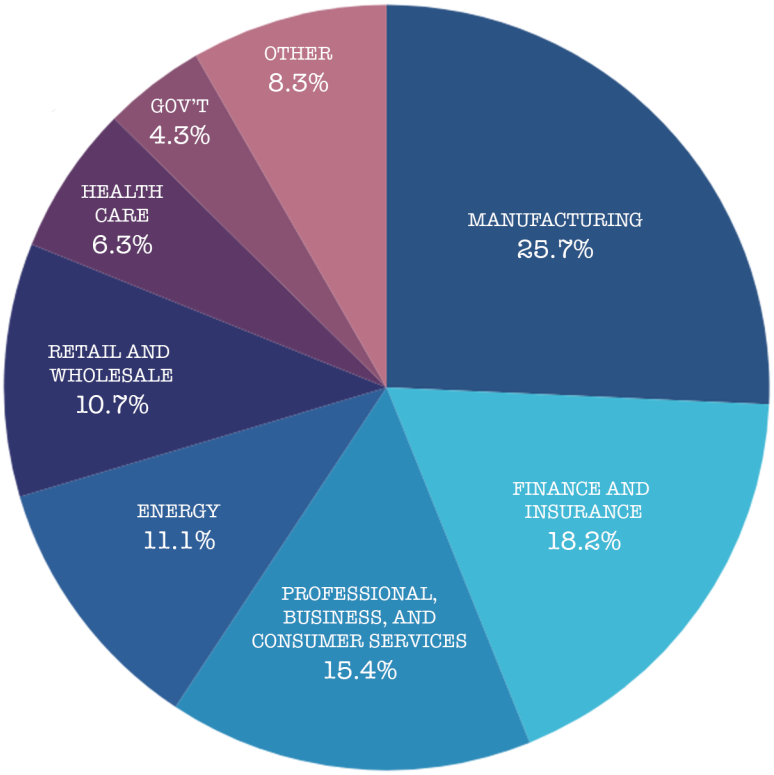
SALT TYPHOON: DISCOVERED IN 2024, THREAT ACTORS ASSOCIATED WITH THE PEOPLE'S REPUBLIC OF CHINA (PRC) REPORTEDLY INFILTRATED BACKDOORS IN MAJOR INTERNET SERVICE PROVIDERS.

ISLAMIC REVOLUTIONARY GUARD CORPS: DISCOVERED IN 2024, IRANIAN-BACKED HACKERS HAVE INFILTRATED THE CAMPAIGN NETWORKS OF THE TRUMP CAMPAIGN USING SPEAR-PHISHING.

VOLT TYPHOON: DISCOVERED IN 2023 AND ACTIVITIES CONFIRMED IN 2024, PRC STATE-SPONSORED HACKERS COMPROMISED U.S. CRITICAL INFRASTRUCTURE FOR AT LEAST FIVE YEARS, INCLUDING THE TRANSPORTATION, TELECOMMUNICATIONS, AND ENERGY SECTORS.

STORM-0558: DISCOVERED IN 2023, THE PRC-AFFILIATED INTRUSION SUCCESSFULLY COMPROMISED 22 ENTERPRISE ORGANIZATIONS AND OVER 500 INDIVIDUALS GLOBALLY THROUGH MICROSOFT EXCHANGE ACCOUNTS, INCLUDING FEDERAL GOVERNMENT ACCOUNTS.

GLOBAL CYBER INTRUSIONS BY SECTOR IN 2023:



SOURCE: IBM X-FORCE THREAT INTELLIGENCE INDEX 2024

TOP KEY DEVELOPMENTS:

2024

- **OCTOBER 2024: Salt Typhoon—**A threat actor associated with the PRC, Salt Typhoon, reportedly infiltrated backdoors in major internet service providers such as Verizon and AT&T to conduct espionage on law enforcement's wiretapping requests and potentially exfiltrate data.[1] This intrusion included accessing the phones of presidential candidates for surveillance purposes. The intrusion is still being investigated by authorities, but reports indicate phone call data and the locations of certain customers were potentially accessed, as well as call audio. There is no information available yet on how many calls were accessed, if so. [2]
- **OCTOBER 2024: American Water Works**—The networks of one of the country's major water utilities were breached by an unidentified cyber threat actor, forcing the company to shut down the online customer portal and billing services for days in an attempt to protect customer data.[3] The operational technology involved in water treatment operations was reportedly unaffected in the attack. The company provides services to more than 14 million Americans, including 18 military installations. Actor attribution has not been made, although nation-state actors such as China, Iran, and Russia have been known to target the sector.[4]
- **SEPTEMBER 2024: Flax Typhoon—**PRC-affiliated actors Flax Typhoon burrowed into "Internet of Things" consumer products such as cameras and network-connected storage devices to conduct espionage on strategic organizations in Taiwan, as well as organizations on U.S. soil through the telecommunications sector, media companies, and higher education institutions.[5] The Federal Bureau of Investigation (FBI) successfully took down the botnet associated with Flax Typhoon in September.[6]
- **SEPTEMBER 2024: Islamic Revolutionary Guard Corps—**Iran-backed hackers infiltrated the campaign networks of the Trump campaign through a high-level staffer's email using spear-phishing, and targeted government officials, lobbyists, think tanks, journalists, and Biden and Harris campaigns. [7] The Department of Justice (DOJ) indicted three Iranian nationals in the 'hack-and-leak' operation in September according to Microsoft,[8] the Iranian-backed group Peach Sandstorm was discovered in August to have used malware to target U.S. critical infrastructure,[9] including the energy sector and satellites.[10]
- **JUNE 2024: CDK Global—**A software firm serving 15,000 car dealerships in the United States was the target of a ransomware attack.[11] This attack forced thousands of dealers across the country to conduct transactions and other crucial administrative tasks manually. The company reportedly paid a $25 million ransom to bring the systems back online, although that is not confirmed by CDK Global.[12]
- **MAY 2024**: **Ticketmaster—**The cybercriminal group ShinyHunters—which claimed responsibility—allegedly hacked Ticketmaster through its customer sales portal.[13] The website tried to shut down quickly, but more than 40 million accounts had their data leaked onto a dark web forum used for further hacking attempts. Leaked data included contact information, biographical information, and payment data.[14]
- **MAY 2024: Ascension Hospitals—**A threat actor exploited known vulnerabilities after an employee downloaded malware from a phishing attempt,[15] impacting IT networks at all 142 Ascension hospitals in the United States and removing access to patient data in a ransomware

attack.[16] The outages impacted patient care, led to rerouted ambulances, and delayed emergency services at numerous locations.[17]

- **APRIL 2024: AT&T—**AT&T notified the public that the private call and text data of millions of its cellular customers,[18] as well as some customers' locations at the time of use,[19] was breached and released on the dark web due to an intrusion into the third-party cloud storage provider, Snowflake.[20] Federal agencies were potentially among the customers at the time, including agencies in the Department of Homeland Security (DHS).[21]
- **FEBRUARY 2024: UnitedHealth—**The UnitedHealth insurance company ransomware attack, allegedly by the threat actor BlackCat,[22] was the largest in the country and impacted 100 million people.[23] The intrusion was through a subsidiary payment processor, Change Healthcare. The company says the actor was potentially sponsored by a nation-state.[24] In Congressional testimony, United Health admitted they were not using multifactor authentication.[25] UnitedHealth paid $22 million in ransom to restore access to customer data, but the full impact has cost the company upwards of $872 million.[26]
- **FEBRUARY 2024: LockBit—**The DOJ and the United Kingdom disrupted a variant of the LockBit ransomware group in 2024, which had targeted 2,000 victims and extorted $120 million in ransom payments across the globe since 2020.[27] Their targets included organizations and individuals working in the manufacturing and semiconductor industries. LockBit works as 'ransomware-as-a-service,' allowing new users to personalize the process and target through which they encrypt and steal data.[28]
- **JANUARY 2024: CISA—**A threat actor presumed to be sophisticated targeted the Cybersecurity and Infrastructure Security Agency (CISA) through zero-day vulnerabilities discovered in Ivanti Connect Secure virtual private network (VPN) for espionage.[29]

2023

- **DECEMBER 2023: National Public Data—**A third-party bad actor is believed to have leaked the private data of almost three billion records involving the personal information of roughly 170 million people.[30] This potentially included Social Security numbers, credit information, addresses, and date of birth for individuals.[31]
- **DECEMBER 2024: Water Facilities—**An Iranian-linked hacking group, Cyber Av3ngers, infiltrated Israeli software used in U.S. water and wastewater facilities in the wake of the October 7 Hamas terrorist attacks.[32] For example, the group accessed a component that regulates water pressure at a water authority in Pennsylvania, forcing the facility to utilize manual controls.[33] In February 2024, the Treasury Department sanctioned IRGC-affiliated cyber actors involved in these operations.[34]
- **AUGUST 2023: HiatusRAT—**A suspected PRC-linked threat actor used HiatusRAT malware to target a U.S. military procurement system and Taiwan-based organizations. The threat gained access via pre-built malware samples which were then hosted on virtual private servers (VPSs). It is suspected the threat actor may have been gathering publicly available information about military requirements or searching for associated organizations.[35]
- **AUGUST 2023: Dollar Tree—**Nearly two million DollarTree and Family Dollar employees were impacted by a third-party breach of the service provider Zeroed-In Technologies. Names, dates of birth, and Social Security numbers were stolen in the attack.[36]
- **JULY 2023: Storm-0558—**The PRC-affiliated intrusion successfully compromised 22

enterprise organizations and over 500 individuals globally through Microsoft Exchange accounts, including the accounts of high-level U.S. officials, due to what the Cyber Safety Review Board described as "a cascade of security failures" by Microsoft. The actor gained access through a stolen account authentication key.[37]

- **JUNE 2023: MOVEit—**Russian ransomware group CLoP took advantage of a vulnerability in the MOVEit file transfer tool by infecting internet-facing web applications with a web shell,[38] which was then used to steal data from MOVEit Transfer databases.[39] Through the breach, hackers accessed 632,000 email addresses at the DOJ and the U.S. Department of Defense (DoD). The Oregon Department of Transportation was also a part of the hack with an estimated 3.5 million Oregon residents' personal information exposed in the breach.[40]
- **MAY 2023: Volt Typhoon—**Although first discovered in May 2023, Americans learned in 2024 that PRC state-sponsored hackers, code-named Volt Typhoon,[41] compromised U.S. critical infrastructure for surveillance and pre-positioning purposes for at least five years before being detected.[42] The intrusions used a technique called "living off the land," rather than malware, and included numerous sectors, including transportation, telecommunications, and energy.[43] A botnet used by the threat actor on U.S. soil was shut down by the DOJ in December 2023.[44]
- **MARCH 2023: Telerik Exploitation—**CISA announced that from November 2022-January 2023, multiple cyber threat actors exploited a vulnerability in an unnamed federal agency's Microsoft Internet Information Services (IIS) server to install malware, specifically in a user interface tool known as Telerik. One of the hacking groups is a state-backed and Vietnam-linked credit card skimming actor called XE Group.[45]
- **JANUARY 2023: T-Mobile—**A threat actor exploited a vulnerability in a T-Mobile "Application Programming Interface," or API,[46] to access basic customer data, including the names, billing addresses, emails, and phone numbers of up to 37 million individuals.[47]

2022

- **DECEMBER 2022: COVID Relief Funds—**China-linked hacking group, APT41, were publicly acknowledged by the U.S. Secret Service to have stolen at least $20 million in U.S. COVID-19 relief benefits since mid-2020 in over a dozen states.[48] The Secret Service did not reveal how this cyberattack was conducted, but it follows a pattern of the targeting of state government information technology by nation-state actors.[49]
- **NOVEMBER 2022: Rim Jong Hyok—**A North Korean national, Rim Jong Hyok, was indicted for targeting 17 hospitals and healthcare facilities across 11 U.S. states using Maui ransomware.[50] Data from these infiltrations enabled the North Korean military intelligence agency's Andariel Unit, of which Rim is an alleged member, to hack two U.S. Air Force bases. Rim faces charges for conspiracy to commit computer hacking and money laundering through China-based facilitators.[51]
- **SEPTEMBER 2022: Uber—**An unnamed 18-year-old hacker gained access to Uber's secure data via social engineering, posing as a corporate information technology worker, and compromising the entire company.[52] The hacker, who gained access to Uber's Google Suite and Amazon Web Services, was arrested and taken into custody.[53]
- **JULY 2022: Marriott—** An unnamed threat actor reportedly stole 20 gigabytes of sensitive data in a ransomware attack on the Marriott International Hotel chain. The threat actor gained

access to an associate's computer through social engineering tactics, which typically involve the bad actor pretending to be a known person or legitimate entity. Data stolen in the hack included classified business data and payment information within the BWI Airport Marriott in Baltimore, Maryland.[54]

- **JULY 2022: Nelnet Servicing—**Personal user information including names, home addresses, email addresses, phone numbers, and Social Security numbers for over 2.5 million student loan account holders with web portal provider Nelnet Servicing was exposed in a data breach. The hacker had access to the data between June-July 2022.[55]
- **MAY 2022: APT 41—**Reporting indicates that APT 41, which Mandiant assesses is a Chinese state-sponsored group,[56] extracted hundreds of gigabytes of intellectual property in a years-long industrial espionage theft.[57] This included blueprints of materials and sensitive formulas from multinational defense, manufacturing, energy, and pharmaceutical companies in North America, Europe, and East Asia.[58]
- **March 2022: Ronin Network—**The network experienced one of the largest attacks on the financial sector when a North Korean advanced persistent threat (APT) called Lazarus Group exploited a "bridge" in a blockchain game allowing for the transfer of crypto assets.[59] The group stole roughly $620 million worth of Ethereum.[60] Additionally, the event involved a 39-year-old American crypto expert who was then sentenced to five years in prison after helping North Korea with the intrusion.[61]
- **MARCH 2022: Shields Health Care Group—**An unauthorized party gained access to Shields Health Care Group's computer system, stealing sensitive data including medical record information, full names, Social Security numbers, and dates of birth of two million individuals.[62] Shields did not find evidence that this data breach, which impacted 56 facilities, was used to commit identity theft or fraud.[63]
- **JANUARY 2022: Bernalillo County Ransomware Attack—**On January 5, local officials in Bernalillo County, New Mexico, suffered a ransomware attack that took computer systems offline, closed government buildings, and forced emergency services to use "backup contingencies."[64] The attack even disabled security cameras and automatic door locks at an Albuquerque area jail. County officials quickly approved $2 million to recover from the attack.[65]
- **JANUARY 2022: News Corp Breach—**Suspected Chinese government-backed hackers, according to cybersecurity firm Mandiant, breached emails and documents of employees of News Corp, one of the most prominent media companies in the world.[66] Journalists for multiple publications including the *Wall Street Journal* and *New York Post* had data stolen in the attack.[67]

2021

- **NOVEMBER 2021: Log4J Vulnerability—**Log4J, a library of open source software for developers, was victim of a massive cyberattack. The vulnerability used in this attack became known as Log4Shell.[68] Many different versions of these source codes had vulnerabilities that hackers used to gain access to any system that used these source codes. Log4J is foundational to the software supply chain, and experts expect that vulnerabilities will continue to be found as a result of Log4Shell.[69]

- **JULY 2021: Kaseya—**The IT solutions company Kaseya was targeted with a ransomware attack by the Russian threat actor REvil,[70] which functions as "ransomware-as-a-service,"[71] impacting over 1,500 of Kaseya's client companies. The hack was carried out with fake software update files distributed to different parts of the company. The actor demanded a $70 million ransom to remove its encryption on the company's data.[72] In October 2021, the associated threat actor was later "forced offline" by the FBI, the Secret Service, and U.S. Cyber Command in conjunction with international partners.[73]
- **JULY 2021: WooCommerce—**A popular eCommerce payment platform found several vulnerabilities in its systems due to the work of a "white-hat" researcher.[74] Numerous attacks occurred on websites that utilized a WooCommerce plugin for WordPress, leading to the leak of private consumer data that potentially exposed websites using the plugin.[75]
- **JUNE 2021: Steamship Authority of Massachusetts—**As the summer travel season began, a cyberattack impacted the Steamship Authority when ransomware disrupted the ferry system and other maritime transportation systems.[76] This attack remains one of the most devastating against logistical and transportation systems. The logistics, ticket sales, and other online information was manipulated and leaked.[77]
- **MAY 2021: Brenntag Chemical Distribution—**Hackers targeted Brenntag's North American division and reportedly stole 150 gigabytes of data.[78] Although the hackers demanded a roughly $7.5 million ransom,[79] the company reportedly paid $4.4 million to continue operations.[80]
- **MAY 2021: JBS Meatpacking—**The ransomware attack against the Brazilian-based meat packing company JBS, the world's largest meat packer, is one of the worst to impact the food industry.[81] The hackers exploited the company's systems to hold large amounts of data for a ransom of $11 million. The company was forced to halt production temporarily before addressing the attack, impacting every JBS plant in America.[82]
- **MAY 2021: Colonial Pipeline—**A hacking group and "ransomware-as-a-service" group known as DarkSide attacked Colonial Pipeline's IT systems,[83] accessing just one password due to a lack of multifactor authentication in an older VPN.[84] The company, which provides fuel to large parts of the country, was forced to halt business operations, causing serious disruptions in consumer access to fuel and an increase in price.[85] Around 100 gigabytes of the company's data was held for a ransom of 75 bitcoin,[86] or about $5 million.[87] In June 2021, the DOJ seized $2.3 million worth of bitcoin from the threat actor.[88]
- **MARCH 2021: Facebook—**More than 500 million Facebook accounts from more than 100 countries were compromised, and private data from the hack was released on a hacking forum.[89]
- **March 2021: CNA:** The prominent insurance firm fell victim to a cyberattack when the threat actor gained access to over 15,000 devices both internally and those owned by clients. The data was held for ransom using a software called Phoenix CryptoLocker.[90]
- **JANUARY 2021: Microsoft—**A state-sponsored group based in China, as attributed by Microsoft, found numerous zero-day vulnerabilities in Microsoft's servers.[91] This intrusion allowed access to at least 30,000 of Exchange servers who had not applied necessary patches, and tens of thousands of organizations around the world reported attacks and incidents as a result.[92] It is believed that these attacks were used for espionage and potentially artificial intelligence.[93]

Notes

1. Ellen Nakashima and Josh Dawsey, “Chinese hackers said to have collected audio of American calls,” *The Washington Post*, updated October 27, 2024, https://www.washingtonpost.com/national-security/2024/10/27/chinese-hackers-cellphones-trump/.

2. Jessica Lyons, “Feds investigate China’s Salt Typhoon amid campaign phone hacks,” The Register, October 28, 2024, https://www.theregister.com/2024/10/28/feds_investigate_chinas_salt_typhoon/.

3. Kate Gibson, “Water supplier American Water Works says systems hacked,” CBS News, October 8, 2024, https://www.cbsnews.com/news/security-hack-breach-american-water-works/.

4. Sean Michael Kerner, “The American Water cyberattack: Explaining how it happened,” TechTarget, October 18, 2024, www.techtarget.com/whatis/feature/The-American-Water-cyberattack-Explaining-how-it-happend.

5. Sam Sabin, “Chinese hacking ‘typhoons’ threaten U.S. infrastructure,” Axios, September 20, 2024, https://www.axios.com/2024/09/20/china-critical-infrastructure-cyberattacks.

6. Cate Burgan, “Wray: FBI Takes Down Chinese ‘Flax Typhoon’ Hacker Botnet,” MeriTalk, September 18, 2024, https://www.meritalk.com/articles/wray-fbi-takes-down-chinese-flax-typhoon-hacker-botnet/.

7. Federal Bureau of Investigation, *U.S. Cyber Command, Cyber National Mission Force, the Department of the Treasury, and National Cyber Security Centre*, government advisory, September 2024, https://www.ic3.gov/CSA/2024/240927.pdf.

8. U.S. Department of Justice, “Three IRGC Cyber Actors Indicted for ‘Hack-and-Leak’ Operation Designed to Influence the 2024 U.S. Presidential Election,” press release, September 27, 2024, https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us.

9. Tim Starks, “Iranian hackers ‘tickle’ targets in US, UAE with custom tool, Microsoft says,” CyberScoop, August 28, 2024, https://cyberscoop.com/iranian-hackers-tickle-targets-in-us-uae-with-custom-tool-microsoft-says/.

10. Ibid.

11. Ananta Agarwal, “Why a hack at CDK Global is casting a shadow on US auto sales,” Reuters, July 1, 2024, https://www.reuters.com/technology/cybersecurity/why-hack-cdk-global-is-casting-shadow-us-auto-sales-2024-07-01.

12. Sean Lyngaas, “How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom,” CNN Business, July 11, 2024, https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html.

13. “Hacking group claims it breached Ticketmaster and stole data for 560 million customers,” CBS News, May 30, 2024, https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/.

14. Framework Security, “Ticketmaster Breach: A Deep Dive into the May 2024 Cyberattack and the History of the Alleged Hackers,” June 28, 2024,

https://www.frameworksec.com/post/ticketmaster-breach-a-deep-dive-into-the-may-2024-cyberattack-and-the-history-of-the-alleged-hackers.

15. Emily Olsen, "Ascension says cyberattack may have compromised protected health data," Cybersecurity Dive, June 14, 2024, https://www.cybersecuritydive.com/news/ascension-cyberattack-health-data-exposed/718978/.

16. Steve Alder, "Ascension Ransomware Attack Hurts Financial Recovery," *The HIPAA Journal*, September 20, 2024, https://www.hipaajournal.com/ascension-cyberattack-024.

17. Olivia Aldridge, "How the Ascension cyberattack is disrupting care at hospitals," NPR, May 23, 2024, https://www.npr.org/sections/shots-health-news/2024/05/23/1253011397/how-the-ascension-cyberattack-is-disrupting-care-at-hospitals.

18. AT&T, "AT&T Addresses Illegal Download of Customer Data," press release, July 12, 2024, https://about.att.com/story/2024/addressing-illegal-download.html.

19. Ryan Gallagher, "AT&T Hack Undermines US National Security, Experts Say," Bloomberg News, July 12, 2024, https://www.bloomberg.com/news/articles/2024-07-12/at-t-hack-undermines-us-national-security-experts-say.

20. David DiMolfetta, "Dozens of federal agencies' call data potentially exposed in AT&T breach," NextGov/FCW, July 12, 2024, https://www.nextgov.com/cybersecurity/2024/07/dozens-federal-agencies-call-data-potentially-exposed-t-breach/398005/.

21. Ibid.

22. Ashley Capoot, "Ransomware group Blackcat is behind cyberattack on UnitedHealth division, company says," CNBC, updated February 29, 2024, https://www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html.

23. Noah Barsky, "UnitedHealth Paid Hackers $22 Million, Fixes Will Soon Cost Billions," *Forbes*, updated June 7, 2024, https://www.forbes.com/sites/noahbarsky/2024/04/30/unitedhealths-16-billion-tally-grossly-understates-cyberattackcost/.

24. Darius Tahir, "Hacking at UnitedHealth unit cripples a swath of the U.S. health system: What to know," CBS News, February 29, 2024, https://www.cbsnews.com/news/unitedhealth-cyberattack-cloud-based-network-cybersecurity/.

25. House Energy and Commerce Committee, "What We Learned: Change Healthcare Cyber Attack," press release, May 3, 2024, https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

26. Khristopher J. Brooks, "UnitedHealth says Change Healthcare cyberattack cost it $872 million," CBS News, updated April 18, 2024, https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-hack-ransomware/.

27. U.S. Department of Justice, "U.S. and U.K. Disrupt LockBit Ransomware Variant," press release, February 20, 2024, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

28. Ibid.

29. U.S. Cybersecurity and Infrastructure Agency (CISA), *Cybersecurity Advisory: Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways*, government advisory, February 29, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b.

30. "Security Incident," National Public Data, n.d., last accessed October 30, 2024, https://nationalpublicdata.com/Breach.html.

31. "National Public Data breach: what you need to know," Microsoft Support, n.d., last accessed October 30, 2024, https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know.

32. Juliana Kim, "Iran-linked cyberattacks threaten equipment used in U.S. water systems and factories," NPR, updated December 2, 2023, https://www.npr.org/2023/12/02/1216735250/iran-linked-cyberattacks-israeli-equipment-water-plants.

33. Christian Vasquez and AJ Vicens, "Pennsylvania water facility hit by Iran-linked hackers," CyberScoop, November 28, 2023, https://cyberscoop.com/pennsylvania-water-facility-hack-iran/.

34. U.S. Department of the Treasury, "Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure," press release, February 2, 2024, https://home.treasury.gov/news/press-releases/jy2072.

35. Black Lotus Labs, "No Rest For The Wicked: HiatusRAT Takes Little Time Off In A Return To Action," Lumen Blog, August 17, 2023, https://blog.lumen.com/hiatusrat-takes-little-time-off-in-a-return-to-action/.

36. Alicia Hope, "Dollar Tree Third-Party Data Breach Exposes Sensitive Data of Nearly 2 Million Employees," *CPO Magazine*, December 8, 2023, https://www.cpomagazine.com/cyber-security/dollar-tree-third-party-data-breach-exposes-sensitive-data-of-nearly-2-million-employees/.

37. U.S. Department of Homeland Security, "Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023," press release, April 2, 2024, https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer.

38. U.S. Cybersecurity and Infrastructure Agency, *Cybersecurity Advisory: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, government advisory, June 7, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

39. Ari Natter, "Hackers Accessed 632,000 Email Addresses at US Justice, Defense Departments," Bloomberg News, October 30, 2023, https://www.bloomberg.com/news/articles/2023-10-30/hackers-accessed-632-000-email-addresses-at-defense-doj.

40. "MOVEit Data Breach," Oregon Driver and Motor Vehicle Services, the State of Oregon, last accessed October 30, 2024, https://www.oregon.gov/odot/dmv/pages/data_breach.aspx.

41. U.S. Cybersecurity and Infrastructure Agency, *Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, government advisory, May 24, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

42. U.S. Cybersecurity and Infrastructure Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, government advisory, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

43. U.S. Cybersecurity and Infrastructure Agency, *Risk and Vulnerability Assessments*, government advisory, September 13, 2024, https://www.cisa.gov/resources-tools/resources/risk-and-vulnerability-assessments.

44. U.S. Department of Justice, "US Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," press release, January 31, 2024, https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critica.

45. U.S. Cybersecurity and Infrastructure Agency, *Cybersecurity Advisory: Threat Actors Exploit Progress Telerik Vulnerabilities in Multiple U.S. Government IIS Servers*, government advisory, June 15, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a.

46. T-Mobile. "T-Mobile Informing Impacted Customers about Unauthorized Activity," press release, January 19, 2023, https://www.t-mobile.com/news/business/customer-information.

47. Jess Weatherbed, "T-Mobile discloses its second data breach so far this year," The Verge, May 2, 2023, https://www.theverge.com/2023/5/2/23707894/tmobile-data-breach-april-personal-data-pin-hack-security.

48. "Significant Cyber Incidents," Center for Strategic and International Studies, 2024 https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

49. Sarah Fitzpatrick and Kit Ramgopal, "Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says," NBC News, December 2, 2022, https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636.

50. Nick Ingram, Michael Goldberg, and Heather Hollingsworth, "North Korean charged in cyberattacks on US hospitals, NASA and military bases," *Associated Press*, July 25, 2024, https://apnews.com/article/north-korea-hacker-military-intelligence-hospitals-b3153dc0ad16652a80a9263856d63444.

51. U.S. Department of Justice, North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers, press release, July 25, 2024, https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

52. Lindsay Shachnow, "Uber Users: What You Need to Know about Last Month's Data Breach," *Boston University Today*, October 11, 2022, https://www.bu.edu/articles/2022/what-you-need-to-know-about-uber-data-breach/.

53. Kate Conger and Kevin Roose, "Uber Investigating Breach of Its Computer Systems," *The New York Times,* September 15, 2022, https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html.

54. Matt Kapko, "Latest Marriott breach shows a human error pattern," Cybersecurity Dive, July 7, 2022, https://www.cybersecuritydive.com/news/marriott-breach-human-error-pattern/626751/.

55. “Student Loan Breach Exposes 2.5M Records,” Marshall University, Institute for Cyber Security, August 31, 2022, https://www.marshall.edu/cyber/2022/08/31/student-loan-breach-exposes-2-5m-records/.

56. Mandiant, “APT41, A dual Espionage and Cyber Crime Operation,” report, 2022, https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf.

57. Nicole Sganga, “Chinese hackers took trillions in intellectual property from about 30 multinational companies,” CBS News, May 4, 2022, https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinationalcompanies/.

58. Ravie Lakeshmanan, “Chinese Hackers Caught Stealing Intellectual Property from Multinational Companies,” The Hacker News, May 4, 2022, https://thehackernews.com/2022/05/chinese-hackers-caught-stealing.html.

59. Derek Anderson, “North Korean Lazarus Group allegedly behind Ronin Bridge hack,” CoinTelegraph, April 14, 2022, https://cointelegraph.com/news/north-korean-lazarus-group-allegedly-behind-ronin-bridge-hack.

60. Federal Bureau of Investigation, “FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People’s Republic of Korea,” press release, April 14, 2022, https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea.

61. Ryan Browne, “U.S. Officials Link North Korean Hackers to $615 million Cryptocurrency Heist,” CNBC News, April 15, 2022, https://www.cnbc.com/2022/04/15/ronin-hack-north-korea-linked-to-615-million-crypto-heist-us-says.html.

62. Console and Associates, “Shields Health Care Group, Inc. Announces Data Breach,” JD Supra Legal News, July 25, 2022, https://www.jdsupra.com/legalnews/shields-health-care-group-inc-announces-8019546/.

63. Marc Fortier, “2 Million Impacted by Data Breach at Massachusetts Health Care Organization,” NBC Boston News, June 8, 2022, https://www.nbcboston.com/news/local/massachusetts-health-care-group-investigating-data-security-breach/.

64. Benjamin Freed, “New Mexico county ‘first’ local-government ransomware victim of 2022,” State Scoop News Group, January 5, 2022, https://statescoop.com/bernalillo-county-new-mexico-first-ransomware-2022/.

65. Bernalillo County, “County Commission Approves Ransomware Recovery Funds,” press release, https://www.bernco.gov/blog/2022/01/25/county-commission-approves-ransomware-recovery-funds/.

66. Caitlin Cimpanu, “News Corp breached by suspected Chinese hackers,” The Record News, February 3, 2022, https://therecord.media/news-corp-breached-by-suspected-chinese-hackers.

67. Kevin Collier, “News Corp. says Wall Street Journal, New York Post were targeted by hackers,” NBC News, February 4, 2022, https://www.nbcnews.com/tech/security/news-corp-says-wall-street-journal-new-york-post-targeted-hackers-rcna14.880.

68. IBM, “What is the Log4j vulnerability,” report, November 2021, https://www.ibm.com/topics/log4j.

69. Ibid.

70. Caitlin Cimpanu, “REvil gang asks for $70 million to decrypt systems locked in Kaseya attack,” The Record News, July 4, 2021, https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack.

71. Simon Chandler, “REvil Ransomware Gang Offers $1 Million As Part Of Recruitment Drive,” *Forbes*, October 6, 2020, https://www.forbes.com/sites/simonchandler/2020/10/06/revil-ransomware-gang-offers-1-million-as-part-of-recruitment-drive/.

72. Cimpanu, “REvil gang.”

73. Joseph Menn and Christopher Bing, “Governments turn tables on ransomware gang REvil by pushing it offline,” Reuters, October 21, 2021, https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

74. Beau Lebens, “Critical Vulnerability Detected in WooCommerce on July 13, 2021 – What You Need to Know,” *Woo Commerce*, July 15, 2021, https://woocommerce.com/posts/critical-vulnerability-detected-july-2021/.

75. Ibid.

76. Amanda Macias, “Ransomware attack hits ferry service to Cape Cod, Nantucket and Martha’s Vineyard,” CNBC News, June 2, 2021, https://www.cnbc.com/2021/06/02/ransomware-attack-hits-ferry-to-cape-cod-nantucket-marthas-vineyard.html.

77. Ibid.

78. Lawrence Abrams, “Chemical distributor pays $4.4 million to DarkSide ransomware,” Bleeping Computer, May 13, 2021, https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/.

79. Ibid.

80. Matt Steib, “What’s Driving the Surge in Ransomware Attacks,” *New York Magazine*, September 7, 2021, https://nymag.com/intelligencer/article/ransomware-attacks-2021.html.

81. Touro University Illinois, “The 10 Biggest Ransomware Attacks of 2021,” Touro University News, November 12, 2021, https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.

82. Aishwarya Nair and Chris Reese, “Meatpacker JBS says it paid equivalent of $11 million in ransomware attack,” Reuters, June 10, 2021, https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/.

83. Touro University, “10 Biggest Ransomware.”

84. Stephanie Kelly and Jessica Resnick-ault, “One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators,” Reuters, June 8, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack2021-06-08/.

85. Ibid.

86. Scott Neuman, “What We Know About The Ransomware Attack On A Critical U.S. Pipeline,” NPR, May 10, 2021, https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline.

87. Michael D. Shear, Nicole Perlroth, and Clifford Krauss, “Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers,” *The New York Times*, June 7, 2021, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.

88. U.S. Department of Justice, “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” press release, June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionistsdarkside.

89. Emma Bowman, “After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users,” NPR, April 9, 2021, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notifyusers.

90. Touro University, “10 Biggest Ransomware.”

91. Microsoft, “HAFNIUM targeting Exchange Servers with 0-day exploits,” Microsoft Threat Intelligence, report, March 2, 2021, https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

92. Cynthia Brumfield, “Why the Microsoft Exchange Server attack isn’t going away soon,” *CSO Magazine*, March 10, 2021, https://www.csoonline.com/article/570463/why-the-microsoft-exchange-server-attack-isn-t-going-away-soon.html.

93. Dina Temple-Raston, “China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying,” NPR, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.