Nation-State-Sponsored Attacks: Not Your Grandfather's Cyber Attacks

By **Alan Charles Raul**, **Joan Loughnane**, **Stephen McInerney**, and **Laura Sorice**

It used to be that data breaches were all about cyber-crooks hacking computer systems to steal personal information, followed by an affected company sending regretful notification letters offering a year or two of complimentary credit monitoring. Not anymore. Now, state-sponsored attacks threaten to wreak havoc on companies' essential IT systems, Internet devices, software, and all manner of critical infrastructure in private sector hands. Just a few weeks ago, the Director of the Federal Bureau of Investigation (FBI) and the U.S. Attorney General described a recent takedown of a Russian government-sponsored botnet called Cyclops Blink before it was weaponized and caused damage. That case is one reflection of a wave of state-sponsored attacks that can transform routine "incident response" into more dramatic corporate cyber crises.

In this article, we detail a few observations about nation-state-sponsored attacks, including:

- State-sponsored attacks tend to be highly sophisticated—ranging from a sophisticated botnet used to launch DDoS attacks to supply chain compromises.

- Response to state-sponsored hacking routinely requires close coordination with multiple U.S. and foreign government agencies.

- State-sponsored threat actors often target companies that run outdated software that contains previously identified and publicized vulnerabilities.

- State-sponsored threat actors may be politically motivated and, as such, their goals for the attack are not always clear—and can change over time—unlike threat actors purely motivated by profit.

- While state-sponsored cyber-attacks pose exceptional risks, technical experts may recommend the same preventative measures to defend against a state-sponsored attack as any other type of cyber-attack.

Current State of Play. In March 2022, the White House issued a dramatic warning based on "evolving intelligence" about potential Russian cyberattacks on the United States in response to U.S.-imposed economic sanctions. The U.S. government observed Russia conducting "preparatory activities," including scanning websites and hunting for software vulnerabilities, and President Biden warned that "the Russian Government is exploring options for potential cyberattacks." Statement by President Biden on our Nation's Cybersecurity (March 21, 2022). He urged the private sector, especially those companies that operate critical infrastructure, to "harden your cyber defenses immediately by implementing the best practices we have developed together over the last year." Id.

These alarm bells are not new. Earlier this year, the U.S. government reported a significant rise in hacks perpetrated against private companies by nation-state-sponsored threat actors. See *Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information Technology*, Cybersecurity & Infrastructure Sec. Agency (Feb. 16, 2022).

In response, the Biden Administration has made cybersecurity defense a key agenda item. For example:

- On May 12, 2021, President Biden signed an Executive Order on Improving the Nation's Cybersecurity. Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021). This Order makes clear that amidst a mounting cybersecurity threat, the public and private sectors must work together to protect the American public.

- Two months later, on July 19, 2021, the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and FBI assessed that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. See *Alert (AA21-200B): Chinese State-Sponsored Cyber Operations: Observed TTPs*, Cybersecurity & Infrastructure Sec. Agency (July 19, 2021, revised Aug. 20, 2021).

- On Jan. 19, 2022, President Biden signed the National Security Memorandum, which implemented requirements from EO 14028 by setting out specific cyber requirements for government agencies and contractors, such as multifactor authentication, encryption, cloud technologies, and endpoint detection services. Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (Jan. 19, 2022).
- On Feb. 24, 2022, President Biden declared that the United States is "prepared to respond" to "Russia[n] … cyberattacks against our companies [or] our critical infrastructure." Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine (Feb. 24, 2022).
- In March 2022, Congress passed the Strengthening American Cybersecurity Act, which was signed by President Biden and will require critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. Strengthening American Cybersecurity Act of 2022, S. 3600, 117th Cong. (as passed by Senate, March 1, 2022).
- On April 6, 2022, the U.S. Department of Justice (DOJ) and FBI announced a court-authorized operation, conducted in March 2022, to disrupt a global botnet of thousands of infected network hardware devices under the control of a threat actor known as Sandworm, understood to be a Russian-sponsored threat actor. This operation proceeded under judicial order with significant public-private sector collaboration. Press Release No. 22-332, U.S. Dep't of Just., Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (April 6, 2022).

This full-court press by the Biden Administration has made one thing clear: Nation-state cyber attacks can be fiendishly sophisticated and not readily rebuffed. Even large companies that dedicate significant budgets and human resources to cybersecurity must evolve in their preparations to defend against such attacks. Lawyers must understand some of the exceptional attributes of nation-state-sponsored attacks in order to properly advise and guide clients experiencing such an attack, as these attacks can become dramatic corporate cyber crises.

Below we outline five unique attributes of a nation-state-sponsored attack. This is neither a technical guide nor an exhaustive list. This list instead is meant to serve as a primer to help lawyers understand some of the attributes of nation-state cyberattacks in order to better advise client a responding to such an attack and help them navigate a potentially high-profile corporate crisis.

State-sponsored attacks tend to be highly sophisticated—ranging from a sophisticated botnet used to launch DDoS attacks to supply chain compromises. Attacks perpetrated with the backing of foreign governments tend to be well-resourced and highly sophisticated, and are therefore able to levy significant damage against their victims.

Distributed denial-of-service (DDoS) attacks have long been a choice weapon to disrupt power grids or shut down access to servers and websites. DDoS attacks attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

At the end of 2021, DDoS attacks had grown more than 24%, while the total number of smart attacks (advanced, often targeted, DDoS attacks) had increased by 31% when compared to the same period in 2020. *DDoS attacks in Q3 grow by 24%, become more sophisticated*, Kaspersky (Nov. 8, 2021). These attacks may take advantage of home office routers, small businesses, and individual consumer-owned devices that may not employ the same level of security as large, sophisticated corporations.

In December 2020, Mandiant informed the public about an advanced cyberattack, which later became known as the SolarWinds attack. *Highly Evasive Attacker Leverages SolarWinds Supply Chain To Compromise Multiple Global Victims with SUNBURST Backdoor*, Mandiant (Dec. 13, 2020). NOBELIUM, a group of Russia-based hackers, gained access to multiple enterprises through software code, stolen passwords, compromised on-premises servers, and minted SAML (Security Assertions Markup Language) tokens. In this supply chain attack, hackers were allegedly able to access the SolarWinds code, infect the software with malicious code, and use the vendor's legitimate software updates to spread their malware to customer systems. Successful attacks gave NOBELIUM hackers high-level permissions on the downstream compromised systems. Vasu Jakkal, *How nation-state attackers like NOBELIUM are changing cybersecurity,* Microsoft Security (Sept. 28, 2021).

Microsoft's reporting highlights that enterprises have become a key focus for state-sponsored threat actors. In addition, threat actors now look to a company's vendors/third parties as a potential weak point in a company's defense perimeter (e.g., supply chain attacks). The September 2020 Microsoft Digital Defense Report indicated that in 2019 and 2020, 13,000 nation-state attack alerts were emailed to customers. Moreover, following a 78% increase in attacks on supply chain vendors between 2017 and 2020, 35% of all nation-state attacks are now targeted at enterprises.

The Russian government-sponsored organization known as Sandworm likewise tried to create large botnets—connecting large numbers of routers and network devices—to carry out DDoS attacks and cause real harm.

The 2018 VPNFilter attack was responsible for multiple large-scale attacks that targeted devices in Ukraine. New VPNFilter malware targets at least 500K networking devices worldwide, Talos (May 23, 2018). VPNFilter, a potentially destructive malware, infected over 500,000 devices in at least 54 countries.

More recently, on Feb. 23, 2022, CISA announced that it, together with the National Security Agency (NSA), FBI, and the United Kingdom's National Cyber Security Centre (NCSC), has identified that Sandworm is using a new malware, Cyclops Blink. Cyclops Blink appeared to be a replacement network for the VPNFilter malware. *Alert (AA220054A): New Sandworm Malware Cyclops Blink Replaces VPNFilter*, Cybersecurity & Infrastructure Sec. Agency (Feb. 23, 2022). Then, on April 6, 2022, Justice Department announced a successful court-authorized operation, conducted in March 2022, to disrupt Cyclops Blink and remove the malware from thousands of devices. Press Release No. 22-332, U.S. Dep't of Just., Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (April 6, 2022). The insidiousness and reiterative nature of these attacks could pose significant risk for small businesses, as well as B2B and B2C corporations that may sell or distribute devices to businesses and consumers.

Response to state-sponsored hacking routinely requires very close coordination with multiple U.S. and foreign government agencies. This is a critical difference from "your grandfather's cyber attack," when Companies sometimes conducted their investigation and response without government intervention (until notice is sent to state Attorneys General offices). To be sure, many companies submitted an IC3 Report to the FBI about the incident; but for "your grandfather's cyberattack," those Reports might not routinely lead to any substantial interaction with the FBI as part of the company's incident response.

Depending on the scope of a state-sponsored cyber-attack, companies should plan close coordination with domestic and foreign government agencies and law enforcement. These agencies may include the NSA, CISA, and the FBI. In particular, CISA's mission is to "lead[] the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." *About CISA*, Cybersecurity & Infrastructure Sec. Agency (last visited April 26, 2022). According to CISA's website: "CISA acts as the quarterback for the federal cybersecurity team, protecting and defending the home front—our federal civilian government networks—in close partnership with the Office of Management and Budget, which is responsible [for] federal cyber security overall…. CISA also coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensur[ing] that timely and actionable information is shared across federal and non-federal and private sector partners." Id.

Due to the geopolitical impacts of state-sponsored cyber-attacks, government agencies are important partners in the discovery, investigation, and remediation of these attacks.

Coordination between companies and intelligence agencies, as well as across the public sector, should be prioritized. While attorneys representing impacted companies may interface primarily with the Department of Justice (DOJ) and CISA, technical personnel will tend to work closely with FBI personnel; and both groups may work closely with agencies like the NCSC in non-U.S. jurisdictions. In these instances, it is increasingly important that the companies coordinate across internal teams that may interface with different regulators. In addition, coordination should occur among the DOJ, CISA, NCSC, and other public sector actors like the White House National Cybersecurity Director and the National Security Advisor. The NCSC, CISA, NSA, and FBI response to

Cyclops Blink is a prime example of this cross-agency coordination. In order to successfully identify and provide remediation to take down the botnet, these agencies worked closely and benefitted from the cooperation of the private sector. 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 (Jan. 5, 2021).

The fight against state-sponsored threat actors is an ongoing focus for the U.S. government. In March 2022, the Strengthening American Cybersecurity Act as passed by Congress and signed into law by President Biden. This law would require critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. Strengthening American Cybersecurity Act of 2022, S. 3600, 117th Cong. (as passed by Senate, March 1, 2022). The threat of state-sponsored cyberattacks has also sparked significant cross-border coordination. On Feb. 9, 2022, CISA, along with the FBI, NSA, Australian Cyber Security Centre (ACSC), and the NCSC issued a joint Cybersecurity Advisory outlining the growing international threat posed by ransomware in 2021. The advisory, titled "2021 Trends Show Increased Globalized Threat of Ransomware," outlines top trends seen across the United States, Australia, and the United Kingdom.

Less than one year prior, on July 28, 2021, CISA, ACSC, NCSC and the FBI released a joint Cybersecurity Advisory, highlighting the top Common Vulnerabilities and Exposures routinely exploited by cyber actors in 2020 and those vulnerabilities being widely exploited in mid-2021. The advisory highlighted the importance of patching vulnerabilities, specifically for VPNs and cloud-based networks. *Alert (AA21-209a): Top Routinely Exploited Vulnerabilities*, Cybersecurity & Infrastructure Sec. Agency (July 28, 2021).

State-sponsored threat actors tend to target companies that run outdated software that contain previously identified and publicized vulnerabilities. A study by the Ponemon Institute found that 57% of survey respondents who reported their companies had one or more data breaches in the past year say these breaches could have occurred because a patch was available for a known vulnerability but not applied. *Separating the Truths from the Myths in Cybersecurity*, Ponemon Institute (June 2018).

Leaving vulnerabilities unpatched continues to leave systems susceptible to acts of cyber warfare. In February 2022, the International Committee of the Red Cross (ICRC) reported a cyberattack that compromised the data of more than 515,000 "highly vulnerable" people and was likely the work of state-sponsored hackers. Carly Page, *Red Cross says 'state-sponsored' hackers exploited unpatched vulnerability*, TechCrunch (Feb. 16, 2022). ICRC confirmed that the hackers gained access to the ICRC's network by exploiting a known but unpatched critical-rated vulnerability. CISA published an advisory on the vulnerability in September 2021, giving the vulnerability a CVSS severity score of 9.8 out of 10.

A month prior, U.S. federal agencies warned in a joint Cybersecurity Advisory (*Alert (AA22-011A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, Cybersecurity & Infrastructure Sec. Agency (Jan. 11, 2022, revised March 1, 2022)) released by CISA, FBI, and NSA that keeping software updated and using industry-recommended antivirus programs are central to preventing state-sponsored cyber-attacks. The Advisory reminds organizations to update their software regularly, especially to patch vulnerabilities that are known to have been exploited. Organizations should promptly patch and harden any identified vulnerabilities and update their firmware. Moving forward, the agencies urge organizations to adopt a centralized patch management system and to use antivirus programs to scan IT network assets regularly for malware.

The fact that state-sponsored threat actors tend to focus on known vulnerabilities further emphasizes the importance of prompt patching as well as only disclosing newly identified vulnerabilities once a fix has been identified, consistent with the concept of "responsible disclosure." Alan Charles Raul and Steve McInerney, *A Software Primer for Attorneys After Cyber Executive Order*, Law360 (Nov. 22, 2021). Under this doctrine, for "zero day" vulnerabilities, software developers and ethical hackers only disclose the vulnerability once a patch or mitigation has been developed. Lou Ronnau, *Cisco's Process for Fixed Software Release and Vulnerability Disclosure*, Cisco (June 14, 2018). In contrast, the full disclosure model advocates for complete vulnerability disclosure immediately. Despite the varied approaches of private companies when it comes to disclosure, enterprises should pay close attention to disclosed vulnerabilities, whether or not a patch is available, to facilitate rapid remediation and monitoring for potential attack vectors.

State-sponsored threat actors may be politically motivated and, as such, their goals for the attack are not always clear—and can change over time—as compared to threat actors purely motivated by cyber-theft for money. This can lead to an unpredictable and challenging legal response.

In your grandfather's data breach—e.g., a "smash and grab" attack where the threat actor wants to steal personal information to sell on the dark web—the legal response is fairly straightforward: hire a forensic firm to assist with the remediation and investigation, determine the scope of the unauthorized individual's access, and analyze the company's notification obligations.

Smash and Grab. Some nation-state actors operate this way; but, when they do "smash and grab," it tends to be on a larger scale. For example, the Lazarus Group (also known as APT38), which has connections to the North Korean government, is reportedly behind "the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack [John Miller and David Mainor, *WannaCry Ransomeware Campaign: Threat Details and Risk Management*, Mandiant (May 15, 2017)]; the 2016 theft of $81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment (SPE); and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities." Press Release No. 18-1452, Dep't of Just., North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018).

Mandiant describes the Lazarus Group (also known as APT38) as a group that "is unique in that it is not afraid to aggressively destroy evidence or victim networks as part of its operations. This attitude toward destruction is probably a result of the group trying to not only cover its tracks, but also to provide cover for money laundering operations." Nalani Fraser et al., *APT38: Details on New North Korean Regime-Backed Threat Group*, Mandiant (Oct. 3, 2018).

Dmitri Alperovitch, co-founder and former chief technology officer of CrowdStrike, believes the Russian government may target Western organizations in retaliation for sanctions recently imposed by the U.S. and other governments as part of the ongoing Russia-Ukraine conflict. *Russia Sanctions May Spark Escalating Cyber Conflict*, Krebs on Security (Feb. 25, 2022). Put another way, the Russia-Ukraine conflict has changed the landscape and motivations, and may motivate Russia to try to hurt Western organizations (more "smash"), or steal data or spread ransomware in an attempt to recoup lost money from sanctions (more "grab").

Persistence. Other nation-state threat actors operate differently. State-sponsored threat actors can use persistence mechanisms to lurk in the background on systems for a long period of time. This makes detection and remediation difficult. For example:

- In January 2022, threat hunters spotted a well-known Chinese-sponsored threat actor using a firmware implant to maintain a stealthy, persistent attack on its victims. Ryan Naraine, *Prolific Chinese APT Caught Using 'MoonBounce' UEFI Firmware Implant*, Security Week (Jan. 20, 20220). Threat hunters at Kaspersky said that data collected on the attack indicated that the attack was extremely targeted, and difficult to detect because "[t]he infection chain itself [did] not leave any traces on the hard drive, as its components operate[d] in memory only, thus facilitating a fileless attack with a small footprint." (The U.S. federal government banned the use of Kaspersky software in federal information systems on an interim basis in 2017, and on a formal basis in 2019, because of concerns about Kaspersky's links to the Russian government. See James Rundle, *S. Government Formalizes Kaspersky Ban*, Wall St. J. (Sept. 11, 2019)). This threat actor in particular is believed to carry out Chinese-sponsored espionage activity. Attacks like this one may persist over long periods of time because they are particularly difficult for companies to detect.

- Persistent attacks pose a particular threat to critical infrastructure and manufacturing. On Feb. 23, 2022, the US Department of Commerce and DHS published a 96-page report to support President Biden's Executive Order on securing America's supply chains. *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry*, S. Dep't of Com. & U.S. Dep't of Homeland Sec. (Feb. 23, 2022). In the report, the agencies warn that attackers gain a major advantage when successfully infecting a company's firmware. The agencies explain that firmware security "has not traditionally been a high priority for manufacturers or users and is not always well protected." Id. at 41. Firmware on items such as network cards, Wi-Fi adapters, and USB hubs are often not signed with public or private keys. "These devices have no way to verify that the operating firmware is authentic and can be trusted." Id. The difficulties in detecting attacks on firmware allow for hackers to persist in networks and devices for "extended periods of time while conducting attack operations, and inflict irrevocable damage." Id.

Because these attacks are so difficult to identify, entities may incorporate managed detection monitoring into their cybersecurity programs and protocols to engage in the sophisticated threat hunting necessary to spot a persistent mechanism as soon as technically possible.

Insider Threats. State-sponsored attacks can also involve unexpected insider attacks. In February 2022, a member of the infamous Conti ransomware group, hacked the gang's internal Jabber/XMPP server and leaked internal logs via email to multiple journalists and security researchers. Lawrence Abrams, *Conti ransomeware's internal chats leaked after siding with Russia*, Bleeping Computer (Feb. 27, 2022). This leak came after Conti officially announced "full support" of the Russian government in the developing Russia-Ukraine conflict and represented that "if anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use all possible resources to strike back at the critical infrastructures of an enemy." Id. The member responsible for the leaked logs announced that he was in the process of sharing this information with journalists and researchers, confirming suspected political motivations in punctuating the announcement with "Glory to Ukraine!"

While state-sponsored cyber-attacks pose exceptional risks, technical experts tend to recommend the same preventative measures to defend against a state-sponsored attack as any other type of cyber-attack. In addition to maintaining regular updates to software and instituting responsible patch management, companies should focus on the instituting multifactor authentication, implementing centralized logs and monitoring, and maintaining a written cyber incident response plan.

On Jan. 11, 2022, CISA, the FBI, and the NSA released a joint Cybersecurity Advisory warning critical infrastructure operators about the threat of Russian state-sponsored cyberattacks and recommended best practices to minimize disruption from such an attack. *Alert (AA22-011A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, Cybersecurity & Infrastructure Sec. Agency (Jan. 11, 2022). The Advisory was endorsed by NCSC. Within a few days, data security experts at Microsoft, Palo Alto Networks (PANW), and Mandiant confirmed reports of increasing Russian cyberactivity and offered their own recommendations for hardening measures (many of which overlap with the Advisory).

The Advisory, PANW report, and Mandiant report highlight several steps companies should take to prepare against state-sponsored attacks, including the following:

- **Require multi-factor authentication (MFA) for all users.** All users, without exception, should be authenticated with MFA for remote access to internal networks. Like an incident response plan, MFA has become a critical element of cybersecurity programs, as recent regulations from the New York Department of Financial Services and the Federal Trade Commission, among others, reflect. Both Microsoft and Mandiant identify MFA as one of the most important recommendations to mitigate risk.

- **Implement centralized log collection and monitoring.** The agencies recommend that organizations centralize log collection and monitoring capabilities to detect threat actor behavior and investigate incidents. Organizations can use the logs to look for password spray activity, identify unusual activity in dormant accounts, or identify when an IP address is not consistent with the user's expected location. Microsoft and Mandiant recommended that organizations also review logs for remote access infrastructure to confirm authenticity

- **Create, maintain, and exercise a cyber incident response plan.** An incident response and continuity of operations plan are increasingly common features in a credible cybersecurity program. The agencies urge organizations to regularly test their controls and backup procedures so that personnel are adequately prepared for an incident.

- **Develop and maintain threat intelligence.** Companies should prioritize the development and maintenance of information regarding relationships across US and international intelligence agencies. By coordinating closely with intelligence agencies—beyond merely tracking and complying with cybersecurity reporting requirements—companies can better position themselves to respond appropriately and effectively to attacks by state-sponsored threat actors.

These recommendations are a good start; but do not, of course, fully protect an organization from a sophisticated cyberattack. For example, multifactor authentication does not prevent a “man in the middle” attack (Catalin Cimpanu, *FBI warns about attacks that bypass multi-factor authentication (MFA)*, ZD Net (Oct. 7, 2019)), which has been known to be used by the Chinese government in multiple attacks. For example, in 2014, China launched a “man in the middle” attack against users of China’s research and education network who tried to search for information on Google in an attempt to monitor and sensor use of Google’s services. Phil Muncaster, *China Launches Man in the Middle Attack Against Google*, Info Sec. Mag. (Sept. 5, 2014). As threat actors develop tactics to circumvent security mechanisms, strong cybersecurity programs must continue to evolve in light of new technologies.

To assist with this, in March 2022, CISA and its Joint Cyber Defense Collaborative (JCDC) partners launched “Shields Up” webpage in an effort to assist organizations prepare for, respond to, and mitigate the impact of cyberattacks. Shields Up, *CISA*. CISA plans to continue to update the Shields Up Technical Guidance webpage as cyber threats are identified.

Alan Raul *and* **Joan Loughnane** *are partners,* **Stephen McInerney** *is senior managing associate, and* **Laura Sorice** *is an associate, at Sidley Austin.*