ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM MARCH 13, 2014

State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction

By Kimberly Peretti and Jared Slade

The lights go out. Connectivity is lost. Communications die. Darkness descends. Candles flicker in the distance. Groups of people huddle. Those with charged devices record the chaos. Shaky handcams capture snippets of confused conversations, as well as the portraits of panicked children and uncertain adults. Uniformed military sweep through cities, trying to maintain the peace. Word spreads: America has suffered from a catastrophic cyberattack. Eventually, conflicts erupt from the pressure of the continued blackout. Fights ensue, and mobs cruise streets and ransack stores for basic supplies. And so ends the trailer for National Geographic's *American Blackout*—a fictionalized account of a 10-day postcyberattack power outage.

Although this is fiction, the cyberthreat is certainly real and growing—especially in the space of state-sponsored cybercrime. Verizon's 2013 Data Breach Investigations Report (DBIR) estimated that nearly 20 percent of the more than 47,000 analyzed security incidents were attributed to state-affiliated actors. Indeed, American companies have seen nearly a decade of nation-state attacks that have slowly and stealthily exploited systems and networks, stealing everything from the CEO's email, to source code, to blueprints, to key research and development plans.

However, the nature of the attacks is changing. Banks are acutely aware of state-sponsored attacks that purport to disrupt—not exploit—systems by rendering consumer-facing websites unavailable to legitimate users. And nation-states have demonstrated the capability to destroy systems, as evidenced by a lethal worm recently unleashed on a state-owned oil company. Indeed, energy sector companies now know they may be the first targets of such destructive attacks.

Although destructive attacks have not yet been pervasive, their very existence leaves companies (especially those in the direct line of fire) grappling with cyberrisk assessment and effective preparation, given what could happen in a quickly evolving cyberthreat landscape.

Nation-State Attacks: Shifting Motives and a Growing Number of Actors

Cyberattacks come in a variety of flavors. Some attacks are merely individuals' criminal efforts to steal valuable data, like credit card information, user credentials and bank account information. These seemingly straightforward thefts are financially motivated and often supported by the black market for stolen customer information. Other attacks, particularly those attributed to state-affiliated actors, serve other purposes.

For state-affiliated actors, cyberattacks generally have been an extension of espionage, whereby the actors penetrate networks and systems to steal trade secrets and other confidential company information. Officials from various countries have pointed to China as the source of an extensive number of cyberattacks involving systems exploitation, including attacks on defense contractors and oil and gas providers. However, Chinese efforts have not been limited to the United States. For example, Chinese hackers were accused of stealing blueprints to Australia's new intelligence agency headquarters. According to FireEye, Inc., Chinese cybertactics focus on brute force—attempts to overwhelm cyberdefenses with volume—with a primary goal of access to confidential data. China, for its part, claims to be the victim of cyberattacks from the United States and others.

But China is not alone. India and Pakistan have pointed at each other regarding cyberattacks and espionage. Distrust has spread among other sets of rivals and about certain state-actors based on recent security leaks and public allegations. In particular, the Snowden leaks have increased practically everyone's distrust of the United States and its cyberefforts. Israel, too, has been active.

Moving along the continuum from exploitation to disruption, state-affiliated actors have increasingly begun to use cyberattacks to interfere with normal system operations, manipulate industrial machinery and control others' networks. Such control can lead to physical disruption of business and governmental operations. In this way, cyberattacks can be viewed as an extension of nation strength-projection, leaving open the question of whether such attacks could or would be used in conjunction with a physical attack on infrastructure. In fact, the United States has added "cyber" as a fifth domain of warfare, joining land, air, sea and space. The shift in motives of nation-state actors can be attributed to additional actors joining the playing field and, likely, developing capabilities.

The most public example of disruptive cyberattacks is Iran's alleged involvement in the campaign to disrupt legitimate operation of financial institution websites. The group Izz ad-Din Al-Qassam Cyber Fighters has publicly claimed responsibility for a series of sophisticated Distributed Denial-of-Service (DDoS) attacks beginning in Fall 2012 against many financial institutions. Though the group asserted it was motivated to stop certain alleged offenses to Islamic spiritual and holy issues, some well-recognized sources claimed Iran was behind the attacks, possibly in retaliation for Stuxnet (discussed below) and other alleged cyberattacks against it. This example points not only to the shifting motives and additional actors on the playing field, but also the challenges of cyberattack attribution.

Moving along the continuum from disruption to destruction, state-affiliated actors have embarked on the use of cyberattacks to destroy data and systems. The most notorious public example of destructive state-sponsored attacks was *Stuxnet*, a sophisticated and expensive cyberweapon—allegedly created as a joint effort by the U.S. and Israel governments—that targeted Iran's nuclear program. The computer worm, inserted into an Iranian fuel factory at Natanz, destroyed equipment, slowing Iran's uranium purification efforts and undermining the Iranian nuclear program. Stuxnet was discovered in 2010 because of a programming error that caused the worm to infiltrate the Internet generally, but earlier iterations of the worm may have been used as early as 2005. Additionally, it is believed that Stuxnet was the first cyberattack to effect physical destruction as opposed to mere computer disruption. In response to the attacks, the government of Iran announced that it had begun its own military cyberunit, to whom more recent disruptive and destructive attacks have been attributed. More recently, we have witnessed a destructive attack on a Middle Eastern oil company, discussed below, and a North Korean attack on South Korean banks and media companies, in which a virus successfully destroyed a limited number of systems.

Focus on the Energy Industry

In particular, the energy industry has been an initial target of the more destructive-type nation-state cyberattacks. Cybersecurity experts suspect that the energy industry is increasingly targeted because of the potential military advantage to have access to a potential adversary's energy systems. Not only would disruption of a country's energy infrastructure have significant ripple effects on the state-target, including impacting the public's psyche, but energy companies are replete with intriguing data and intellectual property that have significant value in the marketplace.

For example, in August 2012, the world's largest oil company, Saudi Arabia's Aramco, found itself a victim of cyberattack that damaged 30,000 computers and shut down the company's main internal network for more than a week. The company asserted the attack was aimed at disrupting oil and gas production in the country. An organized hacker group called Cutting Sword of Justice and operating from countries on four continents claimed responsibility for the politically motivated attack. Despite not fulfilling the ultimate goal, the attack, featuring a computer virus known as *Shamoon*, was nonetheless among the most destructive known attacks against a single business.

Energy companies in the Middle East do not stand alone as targets of cyberattacks. The United States has reported intrusions aimed at administrative systems of major American energy companies and designed to take control of those systems. Also, workers inadvertently downloaded malware that shut down networks on various rigs and platforms, highlighting additional potential harm. The Department of Homeland Security (DHS), through its Industrial Control Systems Cyber Emergency Response Team, reported that cyberincidents from the energy industry jumped to 111 in six months from only 81 in the whole previous year. DHS followed up with a memo to electric and nuclear sector CEOs outlining specific attacks that caused significant or attempted damage to systems and equipment. Partly in response, the United States government has proposed numerous initiatives to strengthen cybersecurity measures, including sponsoring the development of new tools and technologies to protect the nation's energy infrastructure.

Supervisory control and data acquisition (SCADA) systems are of particular concern. SCADA systems are software-based industrial control systems that are used to monitor and control a process that was previously manually controlled. These systems are often connected to the Internet to increase operations efficiency. However, security was not originally built into these systems, leaving software vulnerabilities ripe for exploitation. Several SCADA failures have been publicly reported, though none have been linked to cyberattacks. An infection or temporary disruption to SCADA systems caused by a computer virus, for example, could have major ramifications—power outages, unmonitored leaks from disabled safety mechanisms or worse could result.

Notably, in the electric industry, the generation plants, transmission and distribution lines, and substations are increasingly being integrated using devices and systems that are interoperable and easily combined with different vendors' technologies—the smart grid. The smart grid, and its increasing reliance on information technology systems and networks, exposes the electric generation and delivery systems to potential and known cybersecurity vulnerabilities associated with using such systems that, in turn, increase the risk of grid failures and power outages.

Recognizing the threat, regulators have attempted to establish and strengthen defenses. For example, the Federal Energy Regulatory Commission (FERC) announced a new version of the Critical Infrastructure Protection (CIP)

Reliability Standards, which were adopted last November. The revised CIP framework focuses on protections for bulk electric systems, which do not include the distribution system to end users. Although the framework specifies varying levels of cybersecurity protections based on whether the bulk electric system is classified as low-, medium- or high-impact, all levels require some level of cybersecurity protection. FERC Commissioner John Norris, in connection with the proposed rulemaking, stated: "We are essentially requiring private industry to support a national defense effort by contributing its time and money to protect the cybersecurity of the electric grid."

According to experts, thus far, publicized cyberattacks directed at the energy industry have not been especially complicated. Attempts to overwhelm systems by brute force or targeting old systems with simple computer viruses have been common. But the sheer size of major energy companies' operations creates opportunities for insiders to affect the systems of even the most diligent and responsible in the industry.

Response to Attacks

In a time when key components of a country's infrastructure—like its energy grid—may not be in the government's control, nation-states are responding by discussing and implementing cybersecurity protections. For example, the United Kingdom has debated agreements allowing for foreign investment in critical energy infrastructure, including concerns that Britain's energy infrastructure is at risk of shutdown from cyberattacks. Britain has since unveiled plans to help companies respond to cyberattacks, in part by connecting victims with companies that have experience responding to cyberincidents.

In the United States, regulators like FERC have attempted to establish specific protections for companies and utilities. Moreover, the National Institute of Standards and Technology (NIST) has issued a preliminary framework—Improving Critical Infrastructure Cybersecurity Executive Order 13636–Preliminary Cybersecurity Framework—after engaging more than 3,000 individuals and organizations about standards, best practices and the supply chain. Focusing on five key functions—identify, protect, detect, respond and recover—NIST encouraged the recipients to voluntarily secure their IT systems and turn best practices into common practices. NIST's final report is scheduled to be released in February 2014.

The U.S. government has also suggested that various incentives may be available to companies who implement the voluntary standards. Proposed incentives include, for example, lower rates for cybersecurity insurance and priority consideration for various governmental grants. Also floated were various protections designed to reduce a participant's legal exposure if a breach occurs, such as reduced tort liability, higher burdens of proof on plaintiffs and a possible federal legal privilege preempting state disclosure requirements. The incentives attempt to tip the scales of a company's cost-benefit analysis in favor of implementing the final framework.

Effects on Businesses

As the threats grow and potential cyberrisk exposure increases, businesses will find themselves spending more to defend against cyberattacks, with limited visibility into whether that expense is truly reducing the risk. And what risk should the organization protect against? Depending on the organization's industry, the risk may include—at least from state-sponsored actors—the exploitation, disruption, or destruction of systems. This means companies may need to reduce the risk not only that their crown jewels may be stolen, but that they may be destroyed.

In addition, if companies spend more to protect their systems and comply with certain cybersecurity standards, what certainty is there that they will have a defensible position against subsequent litigation or regulatory inquiries in the event of a state-sponsored attack? Alternatively, how can an organization prepare for a defensible response given a likely compromise looming in the future? Indeed, concern has been voiced that establishing a cybersecurity framework will inadvertently create a standard of care that can be thrown back at victims of cyberattacks by the plaintiffs' bar. Any deviation from the voluntary prescribed practices, even for valid security purposes, could be twisted to suggest a company should have done more to protect valuable information and infrastructure. Of course, the opposite may happen: companies could point to the framework as evidence of defensible policies and approaches to cyberthreats. A basic understanding of these key issues should be on every senior executive's radar in high-risk industries.

Companies' questions about an attack have moved from "if " to "when." Below are some practical steps companies can take now to be ready for "when":

1. *Get a checkup*. Assuming you already have protections in place (you do, right?), now is the right time to evaluate your particular weaknesses and current defenses against the particular cyberthreats you face. A cyber risk assessment is a good place to start.
2. *Educate your employees . . . and your senior leadership*. Weak or stolen credentials, social engineering and removable media continue to be a major foundation of cyberattacks. A company's defense can only be as strong as those who hold the keys to the kingdom.
3. *Prepare to respond*. Establish a plan to respond to a cyberattack before one is needed, including identifying outside vendors and advisors who can help your company navigate its response. Start with a data breach response plan to supplement an existing incident response plan.
4. *Repeat steps 1–3*. The cybersecurity landscape continues to change. Attacks are evolving, so your company's preparations must, too.

Conclusion

The new goals of state-sponsored cyberattacks are insidious—infiltrate, deploy, disrupt and destroy. Unlike more typical data heists designed to extract information of use to the thieves (or their end customers), certain cyberattacks have more terroristic purposes. Namely, they want to disrupt business and governmental operations, including destroying critical physical infrastructure. For a variety of reasons, the energy industry appears to be a prime target. As attacks continue to target energy companies, those companies must spend more time and resources strengthening both their frontline defense and secondary support. It is a new normal for which energy companies, and other critical infrastructure entities, should prepare; the only available indications suggest that the capabilities for significant disruption and destruction exist, and as various state-actors join and become more sophisticated players in the world of cyberattacks, the risk increases for all.

This article was originally published in the Winter 2014 edition of The SciTech Lawyer.

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jared Slade | 214.922.3424 | jared.slade@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com