AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2019 2nd Quarter Report

SPECIAL FOCUS:
CRITICAL INFRASTRUCTURE INDUSTRIES

BDO

In this issue

PREFACE 1

CRITICAL INFRASTRUCTURE - CHALLENGES & PROBLEMS 2

- Evolving Cyberattack Threats 2
- Legacy Systems' Vulnerability to Cyberattacks 4
- Vulnerable Off-the-Shelf IT Products and Computer Components 4
- Compromised and Weaponized Supply Chains 5
- The Rise of BEC Attacks 5
- Nigerian and Other BEC Bad Actors Expand Operations Globally 6
- BEC Campaign Targeting Marine Shipping Companies 6
- Exponential Growth of Ransomware Attacks 7
- Increasing Data Breaches Due to Human Error and Neglect 7
- Increased Cyberattacks on Air-Gapped Systems 8
- Chinese APT Operations Targeting Critical Infrastructure 9

CRITICAL INFRASTRUCTURE - NOTABLE ATTACKS AND EVENTS 9

RUSSIAN APT OPERATIONS TARGETING CRITICAL INFRASTRUCTURE 13

- U.S. Critical Infrastructure Possibly Compromised by Russian APT Energetic Bear 13
- Russian Nation-State APT Attacks on Saudi Oil and Gas Plants 13
- Russian Malware Attack Attempt on a Ukrainian Chlorine Distillation Plant 14
- North Korean APT Operations Targeting Critical Infrastructure 14
- Iranian APT Attacks on Critical Infrastructure 15
- Ransomware Attacks on Critical Infrastructure 16
- Sophisticated Ransomware Attack on Major U.S. Water and Sewer Utility 17
- Ransomware Attack on Australian Defense Shipbuilder Austal 18
- Ransomware Attacks on U.K. and U.S. Emergency Services 18
- NSA-Based Attack Tools Used Against Critical Industries Including Nuclear Energy Firms 18
- Cryptojacking Attacks on Industrial Operations, Including Tesla Automotive and a Water Treatment Plant 19
- Olympic Destroyer Attacks on European Biochem Labs and Financial Institutions 20
- Cyberattacks on Air Transportation Sector 21
- Cyber Threats to the Agriculture Sector 24

SPOTLIGHT: PROTECTING CRITICAL INFRASTRUCTURE THROUGH THREAT-BASED CYBERSECURITY 26

BDO CYBER THREAT INTELLIGENCE (CTI) SERVICES 30

BDO CYBERSECURITY SERVICES 32

CYBERSECURITY LEADERSHIP TEAM 33

Preface

Today, virtually all industries and governments are intrinsically and fundamentally dependent on critical infrastructure. A critical infrastructure can be defined as any system or asset, whether physical or virtual, that is vital to a country's national security. Critical infrastructure is a combination of multiple distinct sectors, which are comprised themselves from numerous different industries. For example, the U.S. Department of Homeland Security (DHS) identifies 16 critical infrastructure sectors[1].

Understandably, each has its own unique needs, challenges and threats. Yet, fundamentally they also share many of the same core issues. Historically, the threats to critical infrastructure industries were predominantly physical; be it from an attack or from natural disasters. But as operations increasingly became larger and more complex, so have the need for sophisticated Industrial Control Systems (ICS) and Distributed Control Systems (DCS) such as Modbus[2]. This shift, however, also brought with it the dangers of cyberattack threats.

Initially, the most prominent cyberattack threats were from nation-state or terror threat actors. A 2014 survey of 9,700 firms found that nation-states often target critical infrastructure providers and suppliers to advance their political and economic agendas[3]. But with the wide scale adoption of the internet, alongside proliferation of information, we have seen more and more critical infrastructure companies targeted by criminal actors with the intent of financial gain.

This report will review these threats, as well as break down the challenges and problems the sector currently faces. Due to the complexity and size of the matter at hand, this report will focus on several prominent sectors, including energy, water, manufacturing, aerospace, and telecommunications.

Our BDO Cybersecurity Advisory Services teams are located in 32 countries on six continents, providing a wide range of cybersecurity consulting services and managed security services every day. We support government agencies and commercial companies who are actively battling the continuous cyberattacks via nation-state cyberattack groups, criminal cyberattack groups and hacktivists worldwide. Our goal is to ensure all of our clients, especially those in the critical infrastructure industries, deploy efficient and cost-effective cyber defense by implementing what we call threat-based cybersecurity.

To implement threat-based cybersecurity, organizations must fully understand: the cyber threat actors targeting them; the cyber threat vectors the cyberattackers are using; the cyberattackers' most likely methods and tactics; and the information and intellectual property the cyberattackers are seeking to steal, disrupt or destroy. Understanding these variables are crucial to developing a customized cyber defense strategy and then implementing a timely and cost-effective cybersecurity risk management program.

We hope you will find this BDO Cyber Threat Insights Report, focused on critical infrastructure, both enlightening and interesting.

Regards,

GREGORY A. GARRETT, CISSP, CPCM, PMP
Head of U.S. & International Cybersecurity for BDO

1 https://www.dhs.gov/cisa/critical-infrastructure-sectors

2 http://www.modbus.org/

3 https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Critical Infrastructure - Challenges & Problems

EVOLVING CYBERATTACK THREATS

One notable issue plaguing many critical infrastructure industries is their difficulty in quickly adapting to new threats and adequately implementing new safety measures on a large scale. One example is the rapid proliferation of the leaked NSA attack tools that threat agents from North Korea, Russia, China and other countries quickly adopted[4]. These tools and exploits were leaked in April 2016 by a hacking group known as The Shadow Brokers[5], who later even began offering a "subscription plan" of monthly leaks[6].

As a result, threat actors experienced a significant increase in capabilities. A recent example is the ransomware attack on Baltimore, Maryland in which the attackers reportedly used the NSA-developed-tool EternalBlue. This tool, which exploits a vulnerability in Microsoft's SMB protocol, was previously used against other cities, chiefly San Antonio and Allentown, Pennsylvania. These attacks are unfortunately not isolated incidents.

Perhaps the most notorious event that leveraged EternalBlue is the May 2017 global ransomware attack WannaCry, which infected more than 230,000 computers across 150 countries over four days[7]. This event is also a pertinent example highlighting the difficulty many organizations, including those in critical infrastructure industries, face to efficiently implement security updates and software patches.

Microsoft, Cisco and numerous other software vendors have issued security updates to mitigate EternalBlue. However, due to the underlining difficulties organizations have in implementing them in a timely manner, WannaCry continued inflicting harm even several weeks after the event began. For example, on June 19, Honda had to shut down operations at one of their Japanese plants after its systems were infected by WannaCry malware[8]. Several days later, on June 22, it was reported[9] that 55 traffic lights and speed cameras in Australia were taken down after an employee used an infected USB drive. Perhaps the most noteworthy event in this regard is the attack on Ukraine's power grid in late 2015[10]. This was one of the most significant cyberattacks in recent years, with ramifications still being felt today.

4 https://www.theregister.co.uk/2017/04/10/shadow_brokers_open_sources_hacker_trove/

5 https://arstechnica.com/information-technology/2016/10/new-leak-may-show-if-you-were-hacked-by-the-nsa/

6 https://www.bleepingcomputer.com/news/security/the-shadow-brokers-announce-details-about-upcoming-monthly-dump-service/

7 https://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/index.html

8 http://news.softpedia.com/news/honda-shuts-down-car-production-plant-due-to-wannacry-infection-516583.shtml

9 http://news.softpedia.com/news/wannacry-virus-takes-down-traffic-lights-and-speed-cameras-in-australia-516614.shtml

10 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

In spring 2015, spear phishing emails containing the malware BlackEnergy 3 as a Word file, were sent to IT and system managers of several power plants in Ukraine. Employees who opened the email were requested to approve a macro. Doing so activated the malware, which enabled the attackers to remotely take control of the systems and collect data.

As the power plant's operational systems were separated from the ICS via a firewall, the attackers searched for a way to bypass this separation. Over the course of several months, the attackers studied the system power plants' method of operation. They located the Windows Domain Controllers and identified VPN communication between the ICSs to the operational systems.

Eventually the attackers gained VPN access credentials, used by the employees to remotely control the SCADA systems. The attackers leveraged their access to operational systems to study the operation methods of each power company. This was necessary because each company had different systems. This in turn required them to develop a unique custom-tailored malware for each one.

The attackers took control of the UPS system and reconfigured it to shut down during the attack, thus preventing the operators from operating the SCADA systems during the power outage. On Dec. 23, 2015 at 3:30am, the attack was initiated, with the intent of shutting down the power grid. Further, to prolong the outage, the attackers also executed a telephone denial-of-service (TDoS) attack against the utility's call center.

However, it should be noted that as the attackers did not destroy the power grid, despite having capabilities to do so, researchers believe the attack was executed as a Proof of Concept (PoC). In other words, Ukraine was used as a testbed to better develop the attacker's skills, tools and knowledge for future attacks against other countries[11].

11 https://www.wired.com/story/russian-hackers-attack-ukraine/

LEGACY SYSTEMS' VULNERABILITY TO CYBERATTACKS

The issue of vulnerable systems is often also intrinsic with the difficulty of replacing aging legacy systems. As many critical infrastructure organizations and companies must comply with outdated systems and standards—often still in place due to budgetary restraints and/or regulatory demands—this issue is both organizational and technical.

Beyond the exorbitant cost, a blanket re-platforming of core legacy systems is highly risky for a number of reasons[12]; not in the least are unpredictable costs and consequences. Processes and the ways in which legacy systems operate are often inextricably intertwined. If a legacy system is replaced, these processes also have to change with potentially unforeseen complications.

Consequently, upgrading/replacing legacy systems is seen as a risky and costly gamble, while not doing so is seen as the safer option. As a result, organizations may prefer having ongoing long-term costs, rather than a massive yet short-term cost that may only provide marginal operational efficiency[13]. Because of this, many systems remain vulnerable to fixable exploits. For example, according to ESET, as of May 2019 close to a million machines in-the-wild still using the obsolete and vulnerable SMB v1 protocol. Most of these devices are in the United States (more than 400K), followed by Japan (more than 74K) and Russia (more than 66K)[14].

VULNERABLE OFF-THE-SHELF IT PRODUCTS AND COMPUTER COMPONENTS

Even keeping the operating system up-to-date and/or using a proprietary software does not guarantee that a critical infrastructure system is fully protected. Off-the-shelf computer components may have flaws, potentially granting malicious actors an access point to otherwise protected systems. In early 2018, for example, it was revealed that AMD, Intel and Arm microchips are vulnerable to potential cyberattacks due to underlying Central Processing Unit (CPU) architecture design flaws dubbed Meltdown and Spectre[15].

This affects countless computer systems around the world, private and corporate. However, because this is a hardware vulnerability, the solution is highly complex. As it requires a massive organization-wide computer system update, this poses a massive challenge for large and complex organizations, such as critical infrastructure companies and governmental departments. Several months later, in late May 2018, Talos (Cisco's threat intelligence team) exposed a sophisticated modular malware dubbed VPNFilter. It should be noted that this malware's code overlaps with versions of BlackEnergy, which was used in a series of large-scale attacks against Ukraine. Accordingly, VPNFilter may also be destructive.

Talos estimated that the malware has infected at least 500,000 routers and networking equipment in at least 54 countries. Affected devices are from manufactures Linksys, MikroTik, NETGEAR and TP-Link. Additionally, VPNFilter compromised NAS (Network-attached storage) devices from QNAP. The malware is likely being used for gaining control of communication infrastructure, gathering intelligence and establishing an attack infrastructure for widescale destructive or disruptive attacks. The identity of the attacker is unknown, but initial attribution is to a Russian threat actor.

More recently, in May 2019, graphics card manufacturer NVIDIA released a security update due to three critical vulnerabilities found in their graphics cards' drivers[16]. According to the company, attackers could leverage the vulnerabilities to obtain an elevation of privilege, and thus enable them to execute code and/or conduct denial of service attacks.

12 https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Web/LegacySys/Risks.html

13 A joint research by McKinsey and Oxford University, showed that large IT projects run 45% over budget, while delivering 56% less value than predicted - https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

14 https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/

15 https://meltdownattack.com/

16 https://nvidia.custhelp.com/app/answers/detail/a_id/4797/~/security-bulletin%3A-nvidia-gpu-display-driver---may-2019

COMPROMISED AND WEAPONIZED SUPPLY CHAINS

The past two years have seen a significant increase in the number of successful attacks exploiting supply chains (i.e. third-party service or product providers) to compromise their targets. These attacks may also use hybrid attack vectors that exploit operating systems and/or information technology (IT) vulnerabilities concurrently via social engineering techniques. Illustrating this trend is the June 2017 widescale destructive cyberattack known as NotPetya. The attack corrupted tens of thousands of computers, disrupting the operations of numerous companies in Ukraine and additional countries that conduct business there. One of the worst-hit companies included shipping giant Maersk, which had to rebuild 4,000 servers and 45,000 personal computers (PCs) over the course of 10 days, while reverting to manual operation for many of their systems.

The propagation vector introduced was a weaponized software patch issued by a compromised program updater. An accounting software named M.E.Doc. was compromised and exploited to distribute malware to thousands of companies and organizations (including governmental organizations) in Ukraine[17]. This was the first time this type of vector was seen in a large-scale attack[18].

Another prime example of weaponizing supply chains comes from the Chinese APT group known as ShadowPad, who executed a global campaign (though considerably smaller in scale than NotPetya) via malicious software updates. The campaign, exposed in August 2017, compromised a software package produced by NetSarang, exploiting their software update system to propagate a backdoor. NetSarang's products are used by hundreds of companies around the world, including critical infrastructure companies.

THE RISE OF BEC ATTACKS

The BEC (Business Email Compromise) scam has been one of the most profitable and common types of cyberattacks in 2019. BECs (aka "Man-in-the-Email" or CEO scams) are carried out using a variety of social engineering methods and tools. Often this is done under the pretense of a highly important business deal or payment to a supplier that needs to be done for some reason in secrecy and urgently. The wired funds are sent to the attackers' bank accounts and then immediately transferred to different bank accounts around the world.

According to the latest data from the FBI's Internet Crime Complaint Center (IC3)[19], more than 78,000 incidents were reported, adding up to more than $12.5 billion stolen from October 2013 to May 2018. Moreover, this trend only appears to be growing, with global losses having gone up by 136 percent since December 2016.

According to IC3, the most prominent sector targeted by BEC actors in recent years has been real estate, with an increase of 1,100 percent in reported incidents, and almost 2,200 percent in report losses between 2015 and 2017. However, attackers are also increasingly targeting companies with global operations such as critical infrastructure industries, exploiting the nature of time differences to their advantage.

Moreover, a report published in late 2018 that analyzed 3,000 BEC attacks found that up to 60 percent of events don't involve a link in their correspondences, making it hard for many employees to identify malicious activity. Adding to this issue is that about half of BEC emails impersonate and/or target non-sensitive personnel rather than key HR/finance employees or C-level executives (CEO, CFO, etc.)[20]. As a result, simply protecting employees in sensitive departments or positions does not adequately protect companies from BEC scams.

17 https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

18 https://news.softpedia.com/news/security-flaw-discovered-in-nvidia-geforce-experience-update-recommended-asap-525460.shtml

19 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

20 https://threatpost.com/threatlist-60-of-bec-attacks-fly-under-the-radar/137156/

NIGERIAN AND OTHER BEC BAD ACTORS EXPAND OPERATIONS GLOBALLY

When reviewing the global online scam operation, it appears that Nigerian actors play a prominent role. Further, according to data from Palo Alto Networks, the number of BEC incidents is scientifically higher than the IC3 report suggests. It was found that in 2017 alone, about 17,600 Nigerian BEC attacks were executed per month—a 45 percent increase compared to the year prior.

In total, over a three-year period, they have attributed more than 300 actors or groups to nearly half a million attacks. Moreover, their method of operations has significantly evolved and become complex over the last couple of years, namely adopting the use of malware and RATs (remote administration tools).

One of the striking aspects of Nigerian BEC actors is that unlike other cybercriminals around the world, they make little to no effort to obscure their real-world identity. Many even create attack infrastructures associated with public social media accounts such as Google, Facebook, MySpace, Instagram, and various dating and blogging sites. The age range of Nigerian BEC actors appears to mostly be between 20s and 40s, with the vast majority in their 30s. Many are married with children, educated, and seemingly hold or have held legitimate jobs in various fields[21].

With that in mind, it should be noted that BEC scams are a global operation. For instance, in early March 2017, several law agencies around the world arrested 20 Israeli citizens who stole more than $13 million from more than 170 organizations in the United States, Germany, Spain, Finland and Portugal via BEC frauds.

BEC CAMPAIGN TARGETING MARINE SHIPPING COMPANIES

An example of a large-scale BEC campaign is one orchestrated by hacking group "Gold Galleon"[22], who stole at least $4 million from maritime shipping organizations between June 2017 and January 2018. The group targeted a wide range of companies, including those that provide ship management services, port services and cash-to-master services. Attacks on firms in South Korea, Japan, Singapore, Philippines, Norway, U.S., Egypt, Saudi Arabia and Colombia have also been attributed to the group[23].

Due to its global and complex operations, the shipping industry often coordinates its activity across multiple time zones, which makes it highly reliant on email for communication between various departments and offices, third-party service providers, governmental offices, clients, etc. This in turn makes the industry vulnerable to BEC scams, as it may be difficult to verify if someone is being impersonated.

This is further compounded when dealing with smaller companies and organizations. James Bettke, security researcher at SecureWorks who led research into the group, told Threatpost[24] that many small shipping companies also lack security measures, even to the point of not having two-factor authentications and running systems on Windows XP.

According to SecureWorks, Gold Galleon is likely based in Nigeria and comprised of at least 20 members who work together to execute various parts of BEC campaigns, from the initial compromise to gathering and extracting data. The group employs various spear phishing techniques to compromise their targets—notably emails with malicious attachments such as a remote access tool with keylogging and password-stealing functionalities. Stolen email account credentials are then leveraged for additional phishing attempts.

21 https://www.justice.gov/usao-dc/pr/19-people-indicted-following-investigations-international-fraud-and-money-laundering

22 Galleon is a sailing ship class - https://en.wikipedia.org/wiki/Galleon

23 https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

24 https://threatpost.com/gold-galleon-hacking-group-plunders-shipping-industry/131203/

EXPONENTIAL GROWTH OF RANSOMWARE ATTACKS

Ransomware is a massive business and is growing exponentially. In 2018, ransomware damages were estimated at $8 billion, with 2019 on track to surpass that with estimates at about $12 billion, and 2021 forecast to reach $20 billion. For comparison, just in 2015 the cost of ransomware damages was $325 million. While ransomware attacks on private individuals have seen a dramatic slowdown throughout 2018 and early 2019, ransomware attacks on businesses continue to be a major threat. According to recent data, ransomware attacks against businesses have seen an increase of more than 500 percent from Q1 2018, with an increase of 195 percent in detections just between Q4 2018 and Q1 2019[25].

Due to the sensitive nature of their operations, critical infrastructure industries are high-value targets for criminal actors. Many of these attacks are executed with the expectation that the targeted organization and/or facility cannot risk any operational downtime. A study published in March 2019 found that 90 percent of industrial control systems (ICS) and operational technology (OT) have experienced at least one damaging cyberattack over the past two years, with 62 percent experiencing two or more attacks[26].

INCREASING DATA BREACHES DUE TO HUMAN ERROR AND NEGLECT

Another major concern affecting the sector is the introduction of new technologies without the proper training of personnel. Even if the issue of legacy systems is irrelevant or has been resolved, major security incidents could happen due to neglect and/or improper staff training. For example, over the last couple of years we have seen increasing amounts of data leaks reported due to misconfigurations of Amazon cloud-based databases. These databases, known as AWS S3 bucket[27], are often used by companies and organizations to store a wide range of data.

Accordingly, a seemingly small misconfiguring error could result in a detrimental data leak. Below is a recent incident, poignantly illustrating the risks of such an event, as well as the need to address every aspect of the organization's infrastructure and operation when designing and creating its infosecurity framework.

In October 2018, security firm UpGuard detected a massive database of 73 gigabytes belonging to Washington-based internet service provider PocketiNet that had been publicly exposed. As a result, highly sensitive data including lists of plain text passwords and credentials of PocketiNet employees, internal network diagramming, configuration details, inventory lists and photographs of the ISP's equipment were compromised. The database, named "pinapp2", was detected on October 11.

UpGuard contacted and notified PocketiNet on the matter the same day, however it took the ISP a full week to confirm and secure the exposure. In the interim, due to the severity of this exposure, UpGuard expended significant effort following up on the matter, repeatedly contacting PocketiNet and relevant regulators.

If malicious actors would have obtained the databases, they could have executed a large number of targeted attacks, taking control of its infrastructure and systems, crippling the ISP's services or establishing a persistent foothold spying on the company and its clients for later attacks. Furthermore, the exposed data also included a list of "priority customers," with their location and contact details. Amongst the clients were major defense and automotive companies. This information could have easily been leveraged to execute various social engineering on the clients, including BEC attacks.

This incident is extremely concerning on several levels. Notably it shows how a "minor" human error (e.g. misconfiguring a database) could result in an egregious flaw within an organization's overarching security framework. The latter may be well-designed and robust, but without proper organizational infosec procedures, one such error could negate many security solutions. Because of the prevalence of data leaks due to misconfigurations of AWS S3 buckets, it is advised to follow Amazon's official guidelines[28] when creating a bucket. Moreover, it is recommended to conduct a comprehensive review of existing S3 buckets to confirm they are configured correctly, and that no information is publicly exposed.

25 https://resources.malwarebytes.com/files/2019/04/MWB-CTNT-2019-state-of-malware_FINAL.pdf

26 https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report

27 https://aws.amazon.com/s3/

28 https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html

INCREASED CYBERATTACKS ON AIR-GAPPED SYSTEMS

One tactic critical infrastructure companies and organizations employ to protect themselves from the above threats is by segmenting sensitive assets, such as certain industrial control systems (ICS) and keeping them "offline". This is known as air-gapped systems. However, in recent years we have seen several highly effective methods and vectors used to compromise such systems and/or exfiltrate data from them. For example, in June 2018, it was revealed that Chinese APT 'Tick' weaponizes specialized USB drives to compromise air-gapped critical systems.

The cyberespionage group (aka Bronze Butler) primarily targets organizations in South Korea and Japan. According to Palo Alto's Unit 42[29], in this attack, the group attempted to infect air-gapped systems via a unique type of USB drive created by a South Korean defense company and certified as secure by the South Korean IT Security Certification Center (ITSCC). The USB drives were likely compromised during the manufacturing stage (supply-chain attack) or by various social engineering tactics post-manufacturing.

According to the investigation, it appears that the malware used in this incident was a custom-made tool dubbed SymonLoader. An interesting aspect of the malware is that it was specifically designed to compromise Windows XP and Windows Server 2003 systems. This is despite the fact that it was created when newer versions of Windows software were available, suggesting the intentional targeting of older and out-of-support versions of Microsoft Windows that are often used in air-gapped systems.

Moreover, as critical infrastructure systems become more complex and Internet of Things (IoT) technologies are becoming more widespread, keeping systems air-gapped is not always a viable option. For example, the power grid is becoming exponentially more distributed and connected. Electric power grids have also heavily adopted information technology (IT) to perform real-time control, monitoring and maintenance tasks.

Older power plants have been largely spared from cyberattacks because they were not connected to the internet. Also, in contrast to other industry sectors, the energy system includes assets with long lifetimes, which often were not intended to interact with widespread communication layers.

This increased distribution of the network is a double-edged sword. On the one hand, it distributes risk and the consequences of a successful breach, but it also creates a broader "attack surface" with more vulnerabilities and opportunities for attackers to gain access[30]. Besides this risk, power systems face other structural security risks[31]:

- System reliability and electricity production regularly take precedence over threats to security and can result in high-security vulnerability.
- Absence of encryption in earlier communication protocols (plain text is often used).
- Today's systems are lasting longer than in the past, which means that hardware and software are operating beyond their supported lifespan.

One prime example of this is the European Union (EU) energy system. The EU has emphasized its urgent need for cybersecurity solutions due to the increased interconnectivity of the European power system[32]. In the past, there was greater focus on physical incidents. However, moving forward, as the sector continues to transition from an analogue to a digitized operation mode, additional focus on security solutions is essential.

29 https://researchcenter.paloaltonetworks.com/2018/06/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/

30 https://www.utilitydive.com/news/cybersecurity-and-the-distributed-grid-a-double-edged-sword/523285/

31 https://www.sciencedirect.com/science/article/pii/S2405959517303880#b15

32 https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf

Critical Infrastructure - Notable Attacks and Events

CHINESE APT OPERATIONS TARGETING CRITICAL INFRASTRUCTURE

Chinese Espionage Campaign Targeting Aerospace Companies

On Oct. 30, 2018, the United States Department of Justice (DoJ) announced[33] that it indicted 10 individuals for allegedly stealing intellectual property, confidential business information and proprietary aerospace technology including designs for a turbofan engine. The targeted companies are a number of U.S. aerospace companies including a gas turbine manufacturer by the name Capstone Turbine, as well as an unnamed French aerospace company.

The indicted individuals, two Chinese intelligence officers who recruited six Chinese hackers and two aerospace insiders, reportedly operated for more than five years between January 2010 and May 2015. The intelligence officers worked for Jiangsu Ministry of State Security (JSSD), a section of the Ministry of State Security (MSS). Two of the defendants have also been charged in a separate private hacking conspiracy that targeted a San Diego-based technology company. According to the DoJ, the hackers used a range of techniques, including:

- **Spear-phishing attacks,** where hackers target specific individuals, organizations or businesses using an email or electronic communications scam.
- **Watering holes attacks**, where the hackers took control of the companies' websites and leveraged them to compromise visitors' computers.
- **Domain hijacking through the compromise of domain registrars**, which the indictment states is an Australian domain registrar only referred as "Company L". According to several sources this may be Melbourne IT, who has since changed their name to Arq Group[34]. However, the company denies any relation to the event[35].
- **Injecting multiple different strains of malware into the companies' computer systems**, which reportedly include:
  - Remote Access Trojan (RAT) Sakula, which was previously used by Chinese nation-state APT Deep Panda[36]. The 2015 breach of the U.S. government's Office of Personnel Management (OPM) was attributed to this group, for example[37].
  - A Trojan known as Isspace, which was previously used in attacks against tech companies in Japan and Taiwan. The attacks have been attributed to the Chinese espionage APT DragonOK[38].

33 https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

34 https://www.zdnet.com/article/melbourne-it-now-arq-group-surprised-by-chinese-aerospace-hack-claims/

35 https://www.asx.com.au/asxpdf/20181101/pdf/43zy2qmwz4f1z2.pdf

36 https://threatconnect.com/blog/opm-breach-analysis/

37 https://www.ibtimes.com/every-federal-employee-hacked-cyberattackers-stole-more-personal-data-obama-1963492

38 https://securityaffairs.co/wordpress/62615/apt/dragonok-apt-changes-ttps.html

Chinese Hackers Target a Central Asia Country's National Data Center

In June 2018, Kaspersky Lab reported[39] a sophisticated country-level waterholing campaign against an unnamed country in Central Asia. The campaign, executed by APT27 (aka LuckyMouse and EmissaryPanda), compromised a key national data center, providing the attackers with "access to a wide range of government resources at one fell swoop". The campaign is believed to have been active since at least September 2017.

According to the report, the attackers leveraged this access to execute waterhole attacks via an unspecified number of the country's official websites, which were injected with malicious scripts. The weaponized sites would then redirect visitors to instances of both ScanBox and BeEF. The former is a reconnaissance framework that gathers data regarding the victim's machine. The latter, BeEF (short for The Browser Exploitation Framework), is a "penetration testing tool that focuses on the web browser"[40]. One of the tools found in this campaign is a variant of the HyperBro Trojan, which is regularly used by various Chinese-speaking actors.

Chinese APT Campaigns Against U.S. and U.K. Defense Contractors

According to a report by NCC Group, published on March 10, 2018[41], Chinese-affiliated threat agent APT15 has reportedly penetrated the systems of a U.K. government contractor, gaining access to highly sensitive military technology information.

The incident in question was discovered in May 2017, when a contractor providing a range of services to Britain's government suffered a network breach by the threat actor. NCC Group's analysis of the incident yielded that two new backdoors, dubbed RoyalCli and RoyalDNS, were used by the actor, as well as BS2005, a tool previously affiliated with APT15.

APT15 operated on the compromised network from May 2016 until late 2017 and impacted more than 30 hosts during that time. The initial point of entry into the network remains unclear; however, the attackers gained domain administrator credentials by using the open-source tool Mimikatz, which later facilitated the seizure of a VPN certificate which was then used to access the victim's network remotely.

Several months later, it was reported that Chinese hackers stole 614GB of data from an unnamed U.S. Navy contractor. The event supposedly took place between January and February 2018, when hackers linked to the Chinese government stole highly sensitive data, including plans for a supersonic anti-ship missile intended to be operational by 2020.

According to The Washington Post, the hackers also stole material related to a "project known as Sea Dragon, as well as signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library"[42].

The Post claims that further data was compromised, but at the request of the Navy, it is abstaining from further reporting because of national security concerns. It should be noted that the data was hosted on an unclassified network. Furthermore, while the compromised data is described by The Post as "highly sensitive", official sources have stated that when aggregated, the information could be considered classified.

The breach is being investigated jointly by the Navy and the FBI. No technical information regarding the attack vector or tools has been revealed. China on her part is denying any involvement, telling Reuters[43] that the Chinese government "staunchly upholds cybersecurity, firmly opposes and combats all forms of cyberattacks in accordance with law".

39 https://securelist.com/luckymouse-hits-national-data-center/86083/

40 http://beefproject.com/

41 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

42 https://www.washingtonpost.com/

43 https://www.reuters.com/article/us-usa-china-cyber/china-hacked-sensitive-us-navy-undersea-warfare-plans-washington-post-idUSKCN1J42MM

Chinese APT Targets U.S. Satellite and Defense Companies

According to a Symantec report from June 2018, a Chinese threat group has been targeting satellite, communications, geospatial imaging and defense organizations in the United States and Southeast Asia for espionage and/or destructive purposes[44].

In the latest wave of attacks, beginning in 2017, the threat actor, dubbed by Symantec as Thrip, has been launching attacks using a wide range of tools, including a mixture of custom-made malware, open-source tools and "living off the land" tactics. Among the targets in this campaign were a satellite communications operator and an organization involved in geospatial imaging and mapping.

Notably, the actor seemed to focus on the operational side of these companies, and deliberately sought to infect systems running software that monitor and control satellites and geospatial imaging applications. This focus suggests the threat actor had a destructive motive. In addition to these targets, the threat actor also targeted three different telecom operators based in Southeast Asia and a defense contractor.

Thrip uses a wide range of tools and custom-made malware on its targets. However, the group is increasingly relying on "living off the land" tactics and open-source tools. This renders the malicious activity more difficult to detect and attribute, as it blends in with a large number of legitimate processes.

In this campaign, the actor employed a previously unknown custom Trojan called Catchamas, an information stealer that contains additional features designed to avoid detection[45]. Catchamas is built to obtain various information from infected computers, including keystrokes, clipboard data, screenshots and network adapter information. Moreover, the threat actor used an updated variant of Rikamanu, a Trojan attributed to Thrip that logs keystrokes made on a compromised computer[46].

The threat actor leveraged PsExec, a legitimate Microsoft Sysinternals tool for executing processes on other systems to install the malware and move laterally on the compromised networks. In addition, the threat actor used the following legitimate/open-source tools for reasons outlined:

- PowerShell: A Microsoft scripting tool to run commands to download payloads, traverse compromised networks and carry out reconnaissance.
- Mimikatz: A freely available tool capable of changing privileges, exporting security certificates and recovering Windows passwords in plaintext.
- WinSCP: An open-source FTP client used to exfiltrate data from targeted organizations.

44 https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

45 https://www.symantec.com/security-center/writeup/2018-040209-1742-99

46 https://www.symantec.com/en/sg/security-center/writeup/2015-072710-4212-99

HP and IBM Breached by Chinese APT10, Compromising Dozens of Clients' Sensitive Data

In December 2018, a sophisticated and lengthy espionage campaign against numerous industries and across at least 12 countries was exposed. As it stands, this event appears to be one of the most significant from the last couple of years. The Chinese nation-state actor APT10 hacked Hewlett Packard Enterprise and IBM's networks, compromising hundreds of GBs of critical client data, which the group leveraged for additional attacks.

The U.S.-CERT (United States Computer Emergency Readiness Team) issued an alert on this matter but refrained from naming the clients, likely because of pressure from the clients to keep the information confidential. With that in mind, as HPE and IBM are two of the largest IT firms in the world, it is within reason to surmise that critical infrastructure companies or organizations are amongst the clients impacted.

This event became public when the U.S. indicted two Chinese hackers and members of the nation-state group APT10, who were involved in the attacks against IBM and HPE, as well as the subsequent attack on the clients. These supply-chain attacks were part of a larger campaign dubbed Cloud Hopper, which targeted managed service providers (MSPs).

Infosec firms reported on Cloud Hopper in 2017, and according to the indictments, it had been operating since at least 2014. As part of the campaign, the group breached IBM and HPE several times over the course of the last few years, maintaining a foothold for weeks and even months at a time. IBM and HPE were not the only major companies compromised by Cloud Hopper, however.

As of late December, the investigation has not revealed subsequent victims' identities. Further, both IBM and HPE have refused to share any information regarding the attacks and are claiming that no sensitive data was compromised.

This Chinese nation-state group (aka menuPass, Stone Panda, CVNX, Red Apollo and POTASSIUM) first appeared in 2006. Amongst the group's targets are construction and engineering, aerospace and telecom firms, and governments in the United States, Europe, and Japan. Their primary attack vectors are spear phishing and exploiting supply chains such as MSP.

Further, the indictment states that from 2006 until recently, the defendants worked for a Chinese company called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and operated in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

It appears from the investigation that in addition to HPE and IBM, other major companies were attacked and had their supply chain compromised.

The fact that one of the largest IT infrastructure companies in the world has been breached for such a long time is a hard blow to the world of cybersecurity. IBM is a market leader in cybersecurity solutions, and such a comprehensive breach demands an in-depth examination of the event to prevent recurrences.

Russian APT Operations Targeting Critical Infrastructure

U.S. CRITICAL INFRASTRUCTURE POSSIBLY COMPROMISED BY RUSSIAN APT ENERGETIC BEAR

In late July 2018, The Wall Street Journal reported that in 2017 the state-sponsored threat agent penetrated U.S. electric utilities suppliers' networks, gaining access to their control rooms. The attack took place during the summer of 2017, but it has now been confirmed that the group (aka DragonFly and Crouching Yeti), also compromised third-party suppliers.

The group achieved this by stealing credentials via spear-phishing email and watering-hole attacks. Once they gained access, the attacker stole confidential information and gathered intelligence regarding the operation of the facilities.

Moreover, according to The Wall Street Journal[47], the Department of Homeland Security (DHS) confirmed that the attacks had the ability to disrupt power flows. However, the extent of the potential disruption—including whether any nuclear-powered plants were among the facilities impacted—remains unclear.

RUSSIAN NATION-STATE APT ATTACKS ON SAUDI OIL AND GAS PLANTS

On Oct. 23, 2018, new findings were published that supported the attribution of the attack campaign TRITON to the Russian government[48]. This campaign targeted Saudi oil and gas plants' industrial control systems (ICS) and other critical infrastructure. FireEye discovered evidence that links the malware to a research lab supported by the "Central Scientific Research Institute of Chemistry and Mechanics" (CNIIHM)[49]. This Moscow-based institution belongs to the Russian government.

This was not the first time TRITON malware was used against critical infrastructure. In late 2017, an attack on critical infrastructure institutes and ICS in the Middle East via TRITON was exposed[50]. TRITON is a sophisticated malware designed to physically destroy critical infrastructure, but it also has several other capabilities. These include gathering intelligence, reading/writing programs, and reading/writing commands and queries to SIS controllers.

TRITON enables attackers to send and write malicious code across various critical infrastructure systems. This provides them with intelligence gathering and destructive capabilities. Further, it has advanced obfuscation capabilities. The tool injects the controllers with legitimate programs so they will continue to operate as usual without errors. If errors are identified, the tool tries to operate them manually. If the controller does not operate for a specific amount of time, the malware rewrites itself, making the code harder for investigators to detect and investigate.

47 https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?mod=djemCIO_h

48 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

49 http://cniihm.ru/

50 https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

RUSSIAN MALWARE ATTACK ATTEMPT ON A UKRAINIAN CHLORINE DISTILLATION PLANT

In July 2018, the Ukrainian Secret Service (SBU) reported that it had fallen victim to a cyberattack via the VPNFilter malware on a chlorine distillation plant[51]. However, according to the statement, the intelligence agency was able to successfully mitigate the attack.

As the plant provides drinking water and sewage treatment across the country, a disruption or shutdown of operations could have caused considerable damages. No technical details regarding the attack have been reported, but it is currently attributed to Russian APT attackers[52].

NORTH KOREAN APT OPERATIONS TARGETING CRITICAL INFRASTRUCTURE

Operation Sharpshooter Launches Cyberattacks on Critical Infrastructure Industries Worldwide

Operation Sharpshooter, first exposed in December 2018[53], exposed a sophisticated and long-lasting attack campaign on the defense and critical infrastructure sectors around the world. Initially, it appeared that the campaign took place between October and November 2018, however in March 2019, McAfee revealed additional information indicating that it in fact began as early as September 2017. Further, as of March 2019, the campaign still appeared to be active[54].

According to McAfee, at least 87 organizations across 24 countries around the world were attacked. The campaign targeted government, defense, nuclear, energy, telecommunications and financial organizations. Most of the attacked companies were in the U.S., but attacks were also detected in other countries including the U.K., Germany, Spain, Italy, Canada, Australia, New Zealand, Japan, Russia, Turkey, Israel, Thailand, Taiwan, South Korea, Hong Kong and India.

The attackers used social media platforms to contact their targets and propagate a malicious Word file via Dropbox. The document, which impersonated a resume, was written in English, but was edited on a Korean version of Word. Once opened, an embedded Shellcode is executed which in turn downloads and runs a malware known as “Rising Sun”.

After infection, the malware gathers information such as network, OS and IP details. Once finished, it encrypts the data with RC4 Base64 and exfiltrates it to the C2 server. It should be noted that this malware has similarities to the North Korean group Lazarus' Trojan Duuzer[55].

51 https://ssu.gov.ua/ua/news/1/category/21/view/5037

52 https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/

53 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

54 https://threatpost.com/sharpshooter-complexity-scope/142359/

55 https://threatpost.com/sharpshooter-complexity-scope/142359/

IRANIAN APT ATTACKS ON CRITICAL INFRASTRUCTURE

Over the last few years, Iranian APTs have been targeting numerous companies and organizations across multiple industries, including financial services, energy, chemical and telecommunications. Many of the groups, such as OilRig, focus their operation on entities in the Middle East[56].

Iranian Wiper Malware Attacks Saudi Aramco

In December 2018, the group executed a cyberattack against oil and energy companies in the Gulf area in response to U.S. sanctions. These attempts were not only intended to gather intelligence and compromise computer systems, but also to cause significant damage. Amongst the targeted companies were UAE National Oil Company (ENOC), Italian oil and gas company Saipem, and an unnamed heavy engineering company in the UAE[57].

The attackers used a variant of the malware Shamoon (aka Disttrack), which was previously used against Saudi Arabian oil giant Aramco in 2012 and again in November 2016. The 2012 attack was particularly devastating, corrupting more than 30,000 computers and impacting the company's operation for weeks[58]. As stated by ENISA (the European Union Agency of Network and Information Security), due to its advanced destructive capabilities, Disttrack is one of the most dangerous malware strains known to date[59].

Iranian Social Engineering Attack Targets Israel Electric Company

Between April 2016 and at least October 2018, attackers executed a phishing-based malware campaign against Israel Electric Company (aka Israel Electric Corporation), the largest supplier of electrical power in the country. The campaign, dubbed "Operation Electric Powder", was primarily conducted via fake Facebook profiles and pages, breached websites, self-hosted and cloud-based websites. In May 2019, new indicators of compromise (IoC) surfaced, showing a possible continuation of activity.

56 https://attack.mitre.org/groups/G0049/

57 https://www.clearskysec.com/iec/

58 https://www.forbes.com/

59 https://www.enisa.europa.eu/publications/info-notes/shamoon-campaigns-with-disttrack

RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE

LockerGoga - Ransomware Attacks Shut Down Three Major Industrial Plants

On March 18, 2019, Norsk Hydro, one of the largest aluminum manufacturers in the world, experienced a significant cyberattack. The attack took place in the firm's factories in the U.S. and led to a shutdown of all their computer systems. It also partially damaged manufacturing systems in some of its factories. As a result, they had to switch some of their factories to manual operation.

It's worth noting that the malware does not have a propagation mechanism. It most likely spread throughout the company's systems only after the attackers gained a foothold in their Active Directory. On March 19, shortly after midnight, an encryption process began running on numerous computers and servers. The exact number of impacted machines is unknown.

Part of the attack included logging out and locking employees' accounts. Consequently, the IT staff was unable to mitigate the event. The firm also likely physically disconnected part of the network in an attempt to slow down the attack. According to the Norwegian Cert, ("NorCert"), the attacker used a ransomware known as LockerGoga. Prior to this attack, the only known use of LockerGoga took place Jan. 24, 2019, against French-based engineering firm Altran[60].

According to analysis by Nozomi Network Labs[61], the ransomware is capable of encrypting the following type of files: DLL, ppt, pot, pps, pptx, potx, ppsx, sldx and pdf. Further, it encrypts the files with the relevant extensions for the attacks and then opens a window with a message explaining the steps needed to retrieve the files.

The firm's email services were protected because they're fully based on cloud services (Microsoft 365). Consequently, they were able to continue basic operations and maintain contact with clients. The employees logged in to their emails on the cloud with personal smartphones and tablets to maintain some workflow. The manufacturing systems were disconnected from the computers and operated manually.

As of early May 2019, the full scope of damage is unclear. Norsk Hydro's financial director, Eivind Kallevik, who was responsible for managing the crisis, said at the time that it was a serious attack which forced the company to rely on backup solutions to retrieve computer systems. He also stated that Norsk Hydro had no intention of paying the ransom for the decryption. Current assessments regarding the cost of restoring the company's IT systems have been estimated at more than $50 million[62].

The identity of the attackers is unknown, but capable actors likely executed the attack as it required a considerable amount of "manual work". At this stage, there are three assessments regarding the identity of attackers:

- Kaspersky[63] analyzed and identified parts of the ransomware that belong to the Russian criminal group Grim Spider.
- A cyber researcher[64] from Switzerland discovered indications that a North Korean attack group is responsible for the attack.
- Several sources have suggested that environmental hacktivists carried out the attack as a response against the firm's factories which pollute the environment in Brazil[65]. Hydro disputed these claims but still ceased their production in mining factories in Brazil[66].

60 https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

61 https://www.computing.co.uk/ctg/news/3072839/norsk-recovers-some-systems-following-confirmed-ransomware-breach

62 https://www.insurancejournal.com/news/international/2019/04/30/525093.htm

63 https://twitter.com/JusticeRage/status/1109065147186847745?s=08

64 https://twitter.com/markus_neis/status/1109040649687523328?s=12

65 https://www.computing.co.uk/ctg/news/3072839/norsk-recovers-some-systems-following-confirmed-ransomware-breach

66 https://www.thelocal.no/20180724/brazil-environmental-claims-hit-norsk-hydro-earnings

Several days after the attack on Norsk Hydro was reported, American chemicals companies Hexion and Momentive revealed that they too fell victim to a LockerGoga ransomware attack. The two companies, controlled by the same investment fund "Apollo Global Management"[67], both suffered an attack on March 12—six days before the attack on Norsk Hydro.

According to official statements, the companies "immediately took aggressive steps to isolate the issue by disabling certain systems" and notifying the appropriate government authorities. The statements further claimed that the companies are working closely with external cybersecurity experts to restore their affected IT systems, but they did not disclose any additional details regarding the compromised systems or measures taken.

SOPHISTICATED RANSOMWARE ATTACK ON MAJOR U.S. WATER AND SEWER UTILITY

On Oct. 4, 2018, Onslow Water and Sewer Authority (ONWASA)[68] was hit with a variant of a polymorphic Trojan known as EMOTET[69]. Polymorphic malware is an advanced and modular malware that obfuscates its activity by constantly changing its identifiable features.

The initial attack appeared to have resolved, but because of ongoing and persistent problems, ONWASA's IT staff contacted external security experts to assist them[70]. Nevertheless, despite the added security measures and personnel, on Oct. 13, ONWASA was hit again by a sophisticated ransomware dubbed RYUK . The organization's IT and the security team promptly took the systems offline, but by that point the malware already infected and encrypted databases and files.

ONWASA decided not to pay the ransom and as a result had to rebuild several of its databases. To prevent significant disruption, the organization had to continue its operations manually. Regarding the identity of the attacker, RYUK[71] ransomware, which shares code with the Hermes malware, was previously linked to the North Korean APT Lazarus.

Although this attack did not result in significant damages, it is just one of the latest attacks targeting critical systems. Perhaps the most noteworthy event of this sort is the large-scale attack on Ukraine's power grid in late 2015[72]. This was one of the most sophisticated and significant cyberattacks in recent years, with ramifications still being felt today.

As the attackers did not destroy the power grid, despite having capabilities to so, researchers believe the attack was executed as a Proof of Concept (PoC). In other words, Ukraine was used as a testbed to better develop the attacker's skills, tools and knowledge for future attacks against other countries[73]. Nonetheless, it also illustrated the threat to critical infrastructures, bringing attention to the required measures the public sector must undertake to prevent reoccurrences of such attacks.

67 https://www.apollo.com/

68 https://www.onwasa.com/

69 https://www.us-cert.gov/ncas/alerts/TA18-201A

70 https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A

71 https://threatpost.com/ryuk-ransomware-emerges-in-highly-targeted-highly-lucrative-campaign/136755/

72 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

73 https://www.wired.com/story/russian-hackers-attack-ukraine/

RANSOMWARE ATTACK ON AUSTRALIAN DEFENSE SHIPBUILDER AUSTAL

In late October 2018, Australia-based shipbuilding company and defense contractor Austal reported that its data management systems in Perth had been compromised and held for ransom. The company did not pay the ransom and instead restored its security and data systems[74]. Austal, which builds military ships for the Australian, U.S. and Oman navies among others, claimed that its other centers of operations, including those in the U.S., were unaffected by the attack.

RANSOMWARE ATTACKS ON U.K. AND U.S. EMERGENCY SERVICES

Ransomware attacks that target emergency services such as police and fire departments are particularly concerning. For example, in March 2019, the Police Federation of England & Wales (PFEW) was hit by a ransomware attack encrypting a number of databases and servers[75].

Another incident of note took place on Jan. 12, 2017 (just eight days before President Trump's inauguration), when a ransomware impacted 70 percent of the D.C. police department's public surveillance cameras. The attack was discovered after D.C. police noticed that four of their camera sites were not functioning properly, and that they could not access video from their DVRs.

The investigation further revealed that two ransomware variants compromised 123 of 187 network video recorders in total. Consequently, the affected CCTV cameras were unable to record public surveillance footage between Jan. 12-15. However, the system was designed to prevent ransomware from propagating onto other networks, and as a result did not spread outside of the department's environment. The police department decided not to pay the ransom (about $60,800 at the time of the event) and restored the system from backups.

Just weeks later, the Cockrell Hill, Texas Police Department reported that it fell victim to a ransomware attack, resulting in the department losing eight years' worth of video evidence and documents[76]. More recently, in 2018, Riverside Fire and Police Departments fell victim to a ransomware attack twice in one month.

NSA-BASED ATTACK TOOLS USED AGAINST CRITICAL INDUSTRIES INCLUDING NUCLEAR ENERGY FIRMS

In October 2018, security researchers from Kaspersky Lab reported on a sophisticated attack campaign, allegedly using NSA-developed spy toolkits against multiple critical industries related to telecommunications, nuclear energy, IT, aerospace and R&D[77]. As of late 2018, around 50 victims located in Russia, Iran and Egypt were identified.

The tools that are used in this campaign (DanderSpritz, FuzzBunch[78] and DarkPulsar) originally leaked online in March 2017 by the Russian nation-state group Shadow Brokers. They've since been used by various actors against multiple targets around the world.

DanderSpritz and FuzzBunch both provide frameworks that support other tools, yet each play a different role in an attack. While FuzzBunch plugins are reconnaissance and attack oriented, DanderSpritz's framework was developed for managing compromised assets. DarkPulsar is a backdoor that bridges FuzzBunch and DanderSpritz frameworks.

The detection of in-the-wild use of the above three toolkits shows how different tools, malware and frameworks can be chained together to execute a formidable attack with relatively little resources. Further, the discovery of DarkPulsar helps to better understand how backdoors can play a role in bridging different frameworks to create a uniform attack platform designed for long-term persistent compromise.

74 https://safety4sea.com/australian-defense-shipbuilder-austal-hit-by-cyberattack/

75 https://www.zdnet.com/article/police-federation-hit-by-ransomware-attack/

76 https://www.bleepingcomputer.com/news/security/police-department-loses-years-worth-of-evidence-in-ransomware-incident/

77 https://securelist.com/darkpulsar/88199/

78 https://medium.com/francisck/the-equation-groups-post-exploitation-tools-danderspritz-and-more-part-1-a1a6372435cd

CRYPTOJACKING ATTACKS ON INDUSTRIAL OPERATIONS, INCLUDING TESLA AUTOMOTIVE AND A WATER TREATMENT PLANT

The meteoric rise of cryptocurrency in 2018 created a new socioeconomic landscape in which almost anyone could generate large amounts of money, with little to no regulatory oversight. This naturally also attracted criminal and even nation-state cyber actors to take part. However, the growing need for large amounts of computing power and resources to mine coins resulted in increasingly daring attacks. For example, in early February 2018, a cryptocurrency miner was reportedly detected for the first time on an industrial control system (ICS)[79].

The malware was detected during a routine inspection of several SCADA network servers at an operational treatment plant for a water utility. The investigation revealed that the malware infected the network after an employee visited a malicious website. After infection, the malware laterally spread from the employee's station by exploiting an SMB[80] vulnerability.

In another incident later that month[81], electric car manufacturer Tesla confirmed that it fell victim to a malware attack that hit its cloud systems, siphoning its processing power to mine coins. According to a report by the RedLock[82] security firm, this breach shares many similarities with two previous incidents of compromise. The first involved British multinational insurance company Aviva, while the other involved Gemalto, the world's largest manufacturer of SIM cards. Additionally, in January 2018, a new variant of Satori botnet was detected attacking mining rigs of Ethereum crypto coin[83].

These types of attacks are facilitated by the rapid development of crypto-mining software and tools. For example, a North Korean mining malware for the cryptocurrency Monero[84], which uses the mining software xmrig[85], was first reported by AlienVault on Jan. 8, 2018. The report outlined the connection between the mining of Monero and sub-groups of the Lazarus threat group - Bluenorroff and Andariel.

In late 2018, a sophisticated python-based crypto-mining malware dubbed "PyRo Mine" was discovered by Fortinet researchers[86], which uses the NSA's exploit EternalBlue. This malware is of note, as the exploit provides attackers with system privileges on compromised computers, which enables them to quietly mine Monero without raising suspicion. According to a report by ESET, the reasons Monero mining is preferred over other coins such as Bitcoin is due to the existence of an algorithm called CryptoNight[87], which favors computer or server CPUs and GPUs as opposed to the specialized mining hardware needed for Bitcoin mining.

While these incidents were perpetuated by external threat actors, it is important to remember that such attacks can also be executed by employees. In May 2018, an Australian government IT contractor was arrested for illegally mining cryptocurrency on governmental computer systems. However, with the crash of several cryptocoins' value, alongside other factors including the shutdown of cryptocurrency mining tool Coinhive[88], Cryptojacking has experienced a major decrease in late 2018 and 2019[89]. Nevertheless, this threat should not be dismissed, as this may change back if cryptocurrencies go back up in value and new cryptocurrency mining tools are developed.

79 https://www.itwire.com/security/81698-in-a-first,-cryptocurrency-miner-found-on-scada-network.html

80 Microsoft's Windows Server Message Block - https://en.wikipedia.org/wiki/Server_Message_Block

81 https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247?utm_campaign=socialflow_gizmodo_facebook&utm_source=gizmodo_facebook&utm_medium=socialflow

82 https://blog.redlock.io/cryptojacking-tesla

83 https://www.bleepingcomputer.com/news/security/satori-botnet-is-now-attacking-ethereum-mining-rigs/

84 https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner

85 https://github.com/xmrig/xmrig

86 https://www.hackread.com/pyromine-malware-security-mine-monero-nsa-exploits/

87 https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

88 https://www.infosecurity-magazine.com/news/coinhive-monero-miner-set-to-close-1/

89 https://resources.malwarebytes.com/files/2019/04/MWB-CTNT-2019-state-of-malware_FINAL.pdf

OLYMPIC DESTROYER ATTACKS ON EUROPEAN BIOCHEM LABS AND FINANCIAL INSTITUTIONS

In February 2018, an attacker dubbed Olympic Destroyer executed a destructive malware attack on the Winter Olympics in South Korea. As of May 2019, the identity of the attacker remains unknown. However, Russia is suspected to be behind the operation after it was suspended by the Olympic Committee following athlete doping allegations.

Russian entities have previously carried various retributory attacks. For example, in September 2016, the Russian cyber espionage group APT28 (also known as Fancy Bear) attacked the World Anti-Doping Agency (WADA) and leaked sensitive information it collected about Olympic athletes. In late 2017, Crowdstrike detected espionage activity targeting various international sporting organizations[90]. These operations were attributed, with moderate certainty, to APT28. In addition, there are numerous similarities between the Olympic Destroyer and previous Russian attacks. However, these indications are not conclusive. Accordingly, Talos and the Olympic Committee have refrained from attributing the attack to any specific entity.

Kaspersky researchers who continued to monitor the threat actors behind the attack on the Olympics identified a new spear-phishing campaign that uses malicious documents containing malware that shares numerous similarities with the Olympic Destroyer malware. According to Kaspersky's report, the threat actor involved in the Olympics attack is now focusing on financial organizations in Russia, as well as biological and chemical threat prevention laboratories in the Netherlands, Germany, France, Switzerland and Ukraine[91].

90 https://www.scmagazineuk.com/russian-actors-mentioned-as-possibly-launching-olympics-cyberattack/article/743932/

91 https://www.kaspersky.com/blog/olympic-destroyer-biochem/22792/

CYBERATTACKS ON AIR TRANSPORTATION SECTOR

In 2018, three major airline companies, and two of the largest civil aircraft manufacturers—Boeing and Airbus—fell victim to cyberattacks. Below is an overview of these events.

Air Canada

The first attack took place between August 22-24, 2018 against Air Canada. The airline detected "unusual login behavior" with its mobile application. According to the notice, the breach compromised personal data of up to 20,000 customers. The airline has yet to confirm the nature of the breach, notably whether hackers breached Air Canada's systems, or rather malicious actors accessed users' accounts by using previously compromised data. Nevertheless, the relatively small number of accounts impacted suggests the latter[92].

British Airways

Just several days later in early September, British Airways reported[93] that it experienced a website-related breach affecting close to 400,000 customers, exposing sensitive information including billing and email addresses, as well as payment card information[94]. In late October, BA notified another 185,000 individuals. Of the affected customers, about 77,000 also had their cards' CVV number compromised. The attack affected customers who made payments via BA's main website and mobile app between August 21, 2018 and September 5, 2018.

According to security firm RiskIQ, the cybercriminal group Magecart is likely responsible for the attack[95]. The group often employs malicious skimming codes in their attacks and was previously attributed to a series of extensive digital credit card skimming campaigns, including the Ticketmaster breach reported in June 2018[96]. Although the group carried out attacks on multiple targets, Magecart set up custom infrastructure to blend in with the British Airways website. It is unclear how much reach the attackers had on the BA servers, but the fact that they were able to modify a resource for the site indicates that it was substantial. This was the second incident British Airways had been involved in. In July 2018, the airline had to delay and cancel some flights at Heathrow Airport after it experienced an unspecified "IT systems issue"[97]. It is unclear whether the two events were related.

Cathay Pacific

The third attack was reported on October 24, 2018 when Cathay Pacific Airlines revealed[98] that it was the latest major airline to fall victim to a data breach. This time, however, the magnitude of the attack, executed in March, was reportedly the largest airline data breach. It compromised the personal information of 9.4 million passengers, but unlike BA, only a handful of credit card numbers were accessed. Instead, most of the compromised records were personally identifiable information (PII).

According to the statement, the following data was accessed: passenger name, nationality, date of birth, phone number, email, address, passport number, identity card number, frequent flyer program membership number, customer service remarks and historical travel information. In addition, 403 expired credit card numbers and 27 credit card numbers with no CVV were accessed. The airline added that "no one's travel or loyalty profiles were accessed in full, and no passwords were compromised." Like BA, Cathay Pacific also claimed the information had not been used, further stating that there was no impact on flight safety as the IT affected systems were fully separate from their flight operations systems.

92 https://www.infosecurity-magazine.com/news/air-canada-presses-reset-app/

93 https://www.britishairways.com/en-gb/information/incident/data-theft/latest-

94 https://www.infosecurity-magazine.com/news/ba-breach-an-extra-185k-customers/

95 https://www.riskiq.com/blog/labs/magecart-british-airways-breach

96 https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/

97 https://www.welivesecurity.com/2018/07/19/british-airways-cancelled-flights-heathrow-system-issue/

98 https://infosecurity.cathaypacific.com/en_HK.html

Boeing Production Plant Hit by Malware Attack

On the morning of March 28, 2018, a Boeing production plant in Charleston, South Carolina was hit by a WannaCry ransomware attack that affected its systems and briefly caused widespread alarm among employees and customers alike.

Despite fears that the malware would affect critical aircraft production systems and even airplane software, company officials insisted the vulnerability was limited to several machines. Further, Boeing claimed that it had promptly deployed software patches after it discovered the infection, which resulted in the minimal damage witnessed.

Boeing attempted to minimize the concerns the attack generated by issuing a statement claiming that its cybersecurity operations center detected a limited intrusion malware only impacting a small number of systems. However, Mike Vander Wel, chief engineer of Boeing Commercial Airplane production, reportedly said in an internal memo that the attack was "metastasizing rapidly out of North Charleston" and could spread to Boeing's production systems and airline software[99].

WannaCry malware exploits older Windows software vulnerabilities to gain access to a network. Once it targets a system, it encrypts the victim's files and demands a ransom, typically in cryptocurrency. The malware first surfaced in May 2017 in a widespread campaign targeting various public and private institutions worldwide, which briefly paralyzed large portions of the U.K.'s health sector.

It should be noted that as of May 2019, no investigation reports or technical details regarding the attack vector have been reported. Nevertheless, in our assessment, if Boeing was indeed hit by WannaCry, the company was likely operating older versions of Windows without the 2017 patches installed[100].

Attack on Airbus Attributed to Chinese Group APT10

According to sources associated with Airbus, the breach in early 2018 was carried out by the Chinese attack group APT10, affiliated with the Chinese intelligence service. The group primarily targets construction and engineering, aerospace, telecom and aerospace firms[101]. However, according to researchers, in a recent attack the group used highly sophisticated methods that appear more complex than previously witnessed.

Based on the recent information, the attack was most likely carried out in two stages: First, the attackers took over one of Airbus' French contractors for several weeks, and second, they eventually impacted Airbus. This incident is another example of a firm which stored unencrypted sensitive information on vulnerable and main servers. Additionally, it was discovered that the information from the breach on Airbus, together with a dump file, was sold on the dark net under the name Collection #2-5[102]. This database size is 845 GB and contains other leaked databases as well, which house millions of usernames and passwords from numerous organizations and private individuals.

99 https://www.nytimes.com/2018/03/28/technology/boeing-wannacry-malware.html

100 http://news.softpedia.com/news/boeing-possibly-hit-by-wannacry-company-plays-down-cyberattack-520460.shtml

101 https://www.challenges.fr/entreprise/transports/cyberattaque-contre-airbus-la-piste-chinoise-avancee_640396

102 https://threatpost.com/airbus-data-breach/141368/

Additional Events Affecting the Aviation Sector

The above events do not appear to be related, but the recent increase in attacks against major entities in the aviation sector is concerning. Outside of the above-mentioned attacks, below are several additional events that have impacted the sector.

- Bristol Airport Falls Victim to Ransomware Attack, Disabling Flight Information Screens - In the middle of September 2018, there was an attempted ransomware attack on Bristol Airport's administrative systems. To contain the attack, the airport shut down several of its facilities for a few days, including its flight information screens[103]. Airport officials decided to decline paying the ransom demand, choosing instead to manually restore all affected systems.
- Drones Disable London's Gatwick Airport for a Day and a Half - Between December 19-20, 2018, unknown individuals disrupted the airport's flight operation by flying drones over the runways. It seems that this incident was intentional and well planned as it requires a considerable amount of batteries for such a long operation[104].
- Domodedovo Airport - In July 2018, Moscow International Airport received threatening emails from unknown actors claiming that they would disrupt the airport's navigation equipment unless they were paid a ransom in Bitcoin[105].
- Unnamed Major International Airport - In July 2018, it was revealed[106] that remote desktop protocol (RDP) access to the security and building automation systems of an unnamed major international airport was sold on a Russian market for as little as US$10.

103 https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport/

104 https://www.theverge.com/2018/12/20/18149819/london-gatwick-airport-drone-shutdown-reports

105 http://www.ehackingnews.com/2018/07/hackers-threaten-to-disrupt-moscow.html

106 https://www.darkreading.com/threat-intelligence/major-international-airport-system-access-sold-for-$10-on-dark-web/d/d-id/1332270

CYBER THREATS TO THE AGRICULTURE SECTOR

Like the other critical infrastructure industries, the agriculture sector is experiencing rapid changes and thus becoming more integrated and connected. Precision agriculture, or "smart" agriculture, relies on data monitoring and precise adjustment of agricultural tools to optimize yields. The sector is following the global trend of higher reliance on artificial intelligence and IoT.

Precision agriculture employs a variety of embedded and connected technologies that rely on remote sensing, global positioning systems and communication systems to generate big data, data analytics and machine learning. These technologies allow for more precise application of agricultural and livestock management inputs such as fertilizer, seeds and pesticides, resulting in lower costs and improved yields[107].

Cyberattack on Bayer AG Attributed to Chinese Threat Actor

German conglomerate Bayer, the world's largest agricultural supplies company[108], reported that between early 2018 and March 2019 it suffered a system breach. The company, however, claims that it has since "identified, analyzed and cleaned up the affected systems". Bayer's spokesperson added that there is no evidence of data exfiltration.

Nevertheless, this incident illustrates the cybersecurity threats the agricultural sector faces, particularly when it comes to supply chain attacks. The agriculture industry heavily relies on third-party service providers as well as other critical infrastructure such as water, electricity and transportation systems. If any of these systems were to be impacted, it could create a bottleneck for wide-scale agriculture production. Accordingly, with the continuing shift from a highly mechanical labor-intensive industry, to an online and integrated one, greater risks are introduced.

Additional vulnerable points in the system can be exploited by cyber criminals in ransomware attacks or by state actors to disrupt the food supply. Moreover, the industry does not have much experience with cybersecurity, leaving it unprepared. Farmers are less concerned with cybersecurity and more so with tangible threats such as pests or disease.

Other than the common cyber threats, the agricultural sector has its own unique challenges, especially in terms of the confidentiality and integrity of the data. Data collection and exploitation from massive sensor nets are valuable tools to assist in real-time farming and livestock decisions. Loss or misuse of the data can have dramatic financial and emotional impacts on farmers. As precision agriculture increasingly adopts equipment automation, robotics, machine learning and edge computing, threats to data integrity and confidentiality are manifesting and can cause harm in unpredictable ways[109].

107 https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

108 https://www.bayer.com/en/crop-science-division.aspx

109 https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Mitigation Attempts

One method several heavy machinery manufacturers are employing to mitigate this issue is using rigid software and firmware to develop their products. This supposedly provides better protection from cyber threats, but also greatly limits farmers from performing many repairs themselves. Moreover, manufacturers such as John Deere[110] sign farmers on license agreements that forbid them from performing almost any repair and/or modification to their machines. This requires them instead to shut down their machines and take them to official dealerships or "authorized" repair shops, which may result in large financial losses to agriculture operators[111].

Another issue is that operators fear that the manufacturers could, for numerous reasons, remotely shut down machines. Consequently, according to reports, some farmers in the U.S. have resorted to hacking their equipment with cracked firmware from Eastern Europe, which they purchase from invite-only, online forums. However, while resolving the firmware restrictions, operators are exposing themselves to a wide range of threats, from malfunctioning equipment to cyberattacks. This is a complex issue that affects additional critical infrastructure sectors; yet as consumers, operators, manufacturers and governments try to adapt to these new circumstances, we expect to see significant developments over the next few years.

110 https://www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf

111 https://www.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

SPOTLIGHT

Protecting Critical Infrastructure Through Threat-Based Cybersecurity

When does cybersecurity become an issue of national security? When critical infrastructure is at stake.

In 2017, the U.S. National Infrastructure Advisory Council warned of "a watershed, 9/11-level cyberattack" and urged the public and private sectors to take bold action. While that may seem like a false equivalency, it's not: Today's wars might be fought on the digital battlefield, but they can inflict physical damage.

Nor is it farfetched: In Finland, a distributed denial-of-service (DDoS) attack targeted computerized heating distribution centers, disabling heat to apartment buildings in frigid temperatures—compromising public health. A cyberattack on the Ukrainian capitol's power grid caused an outage in various areas of the city. In the U.S., Russian hackers conducted spear-phishing attacks and infiltrated the control rooms of small U.S. electric utility companies, seeking information on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Meanwhile, The New York Times recently reported on the U.S. government's more aggressive digital incursions into Russia's electric grid. The entire world seems to be caught up in a Cyber Cold War.

At the same time, the integration of new cyber-physical systems and networked systems between partners, suppliers and customers creates more potential access points for bad actors, leading to an entirely new set of security risks in the physical realm. The integration of information technology and operational technology systems means hackers are now launching attacks specifically designed to penetrate industrial control systems.

As this report illustrates, nation-state actors interested in attacking their adversaries' critical infrastructure have clearly identified the opportunity of a more connected supply chain. Their attempts to infiltrate their adversaries' critical infrastructure networks through supply chain partners are only increasing.

Organizations in the energy, critical manufacturing and transportation sectors arguably have the largest target on their backs and so are especially critical to secure—as they connect, distribute, manage and supply some of the world's most important resources. And as they adopt new technologies and implement more internet-connected devices at faster rates to improve services and trim costs, potential cyber vulnerabilities—and attack vectors—are increasing dramatically.

Employing an evolving threat-based cybersecurity approach will be key. Instead of (or in addition to) focusing solely on protecting critical data assets or following the basic script of a generic cyber program, a threat-based approach concentrates investments in the most likely risks and attack vectors based on an organization's unique threat profile.

Here are 10 initial steps to creating a threat-based cybersecurity program that critical infrastructure industries should keep in mind:

BDO HAS THE RESOURCES TO HELP YOU GET STARTED.

CONTACT

GREGORY GARRETT
Head Of U.S. & International
Cybersecurity Advisory Services
703-770-1019 / ggarrett@bdo.com

ESKANDER YAVAR
Partner, Manufacturing & Distribution
Industry Leader & Management
Technology Advisory Services Leader
713-407-3293 / eyavar@bdo.com

CLARK SACKSCHEWSKY
Tax Office Managing Principal,
Core Tax Services & National Leader,
Natural Resources Practice
713-548-0899 / csackschewsky@bdo.com

MICHAEL BARBA
National Security Compliance Leader
212-885-8120 / mbarba@bdo.com

BDO Cyber Threat Intelligence (CTI) Services

THREAT INTELLIGENCE – "PROACTIVE DETECTION OF A BREACH"

Situational awareness is "the perception of environmental elements and events with respect to time or space, the comprehension of their meaning and the projection of their future status," while intelligence is "the ability to acquire and applied knowledge and skills."

BDO Cyber Threat Intelligence (CTI) is a combination of both: the objective of acquiring knowledge and skills to support better organizational ability and anticipate cyber events that could impact the future status of the business environment.

The BDO CTI Reports are based on research performed by the BDO Cybersecurity Centers. Our Cyber Threat Intelligence Centers in the U.S. and Israel work as an integrated team to transform reactive organizational situational awareness into proactive situational awareness to Cyber Threats. This enables an organization to better understand the likelihood and characteristics of a breach and enables an additional layer of proactivity in the detection of unidentified breaches that might be happening.

HOW DOES IT WORK?

Cybersecurity Research

Our Cyber Research teams reverse-engineer cyberattack techniques, malicious code and lateral movement to identify actual targets and methods used by different perpetrators with different malicious agendas.

Online Fictitious Identities

Our Cyber Intelligence team maintains online fictitious identities to enable their activity within threat communities, to infiltrate an online forum or create a connection with suspected threat actors or hackers, and establish online 'chatter' platforms, to establish 'trusted' conversation environments.

Monitoring Cybercrime Forums

Our Cyber Intelligence team monitors various cybercrime forums to identify premeditated attacks on organizational networks or personnel by monitoring any type of hostile chatter regarding these 'targets.'

Monitoring Data Leakage Platforms

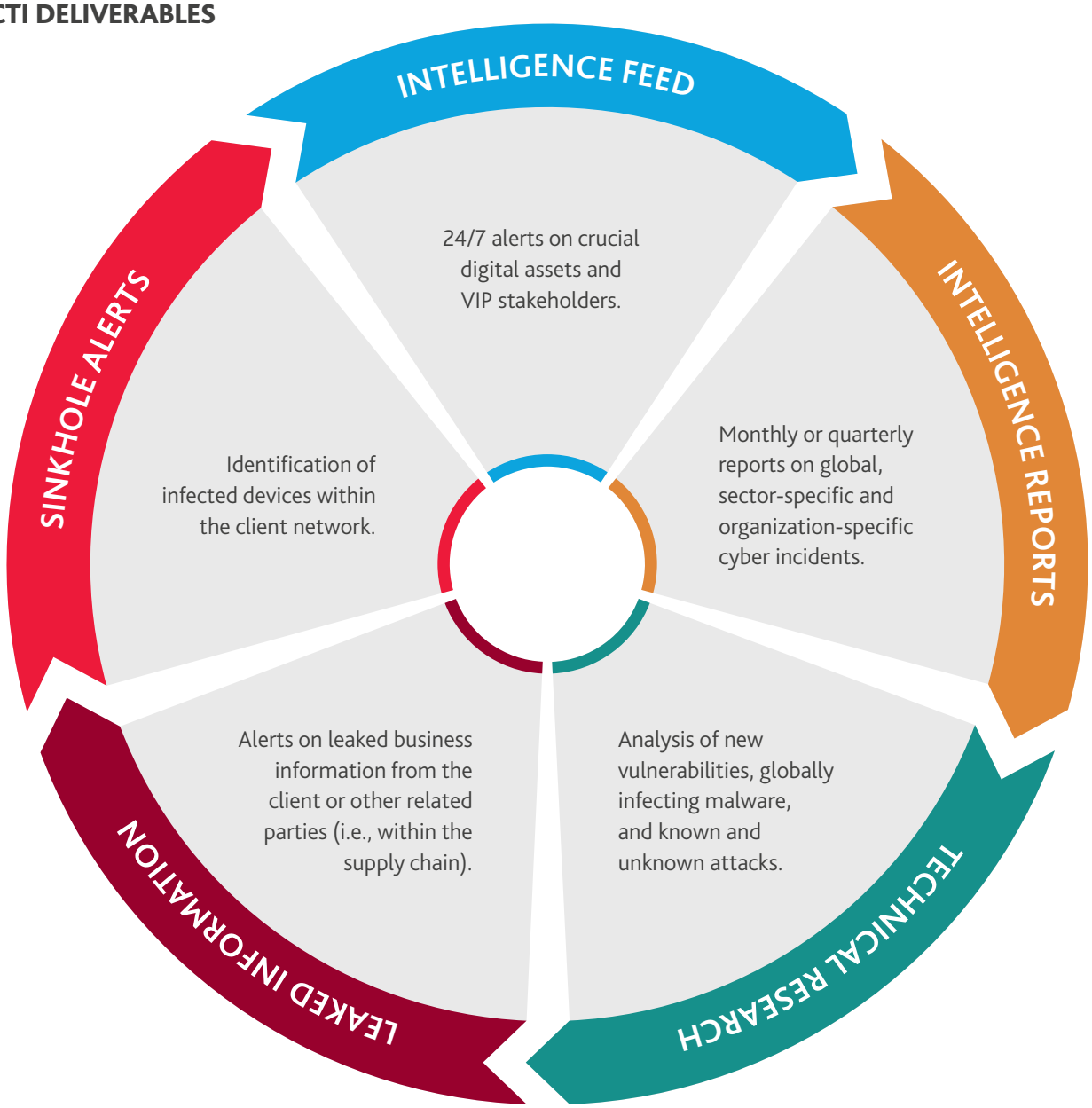
Our team can trawl hacker-oriented data leakage platforms to identify specific data leakage that might lead to a potential attack against an organization.

CONTACTS:

ERIC CHUANG
Managing Director,
Cybersecurity Advisory Services
echuang@bdo.com

ANDREW SILBERSTEIN
Director, Cybersecurity Advisory Services
asilberstein@bdo.com

BDO CTI DELIVERABLES



BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

CYBER RISK ASSESSMENTS

- Risk assessments against multiple frameworks
- Cyber risk remediation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

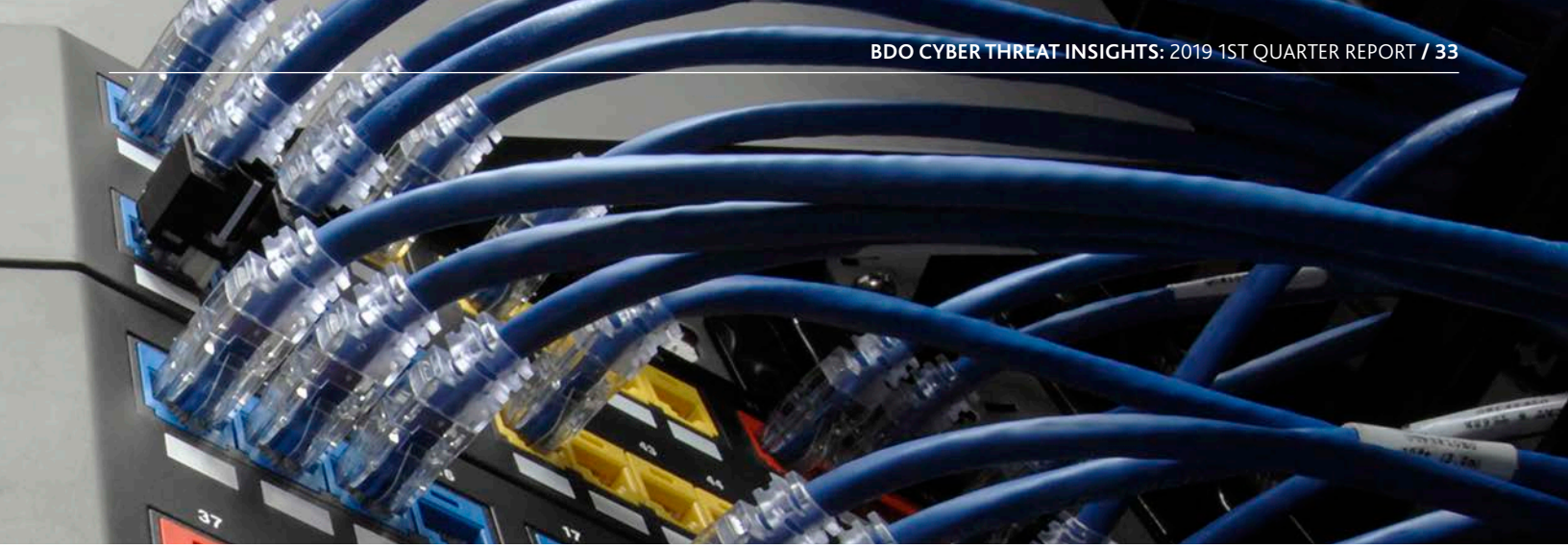
- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Email and network attack threat assessments
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cloud migration & security
- Virtual desk-top services
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)



Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703-770-1019 / ggarrett@bdo.com

GREG SCHU
Partner
612-367-3045 / gschu@bdo.com

MICHAEL STIGLIANESE
Managing Director
212-817-1782 / mstiglianese@bdo.com

ANDREW SILBERSTEIN
Director
703-770-0537 / asilberstein@bdo.com

ESKANDER YAVAR
Partner, Manufacturing & Distribution Industry Leader & Management Technology Advisory Services Leader
713-407-3293 / eyavar@bdo.com

MICHAEL BARBA
National Security Compliance Leader
212-885-8120 / mbarba@bdo.com

JEFF WARD
National Managing Partner,
Third Party Attestation Services
314-889-1220 / jward@bdo.com

JESSICA ALLEN
Director
513-592-2375 / jessica.allen@bdo.com

ERIC CHUANG
Managing Director
202-644-5435 / echuang@bdo.com

FRED BRANTNER
Director
206-403-4036 / fbrantner@bdo.com

CLARK SACKSCHEWSKY
Tax Office Managing Principal, Core Tax Services and National Leader, Natural Resources Practice
713-548-0899 / csackschewsky@bdo.com

People who know Cybersecurity, know BDO.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2019 BDO USA, LLP. All rights reserved.