Industrial Cybersecurity Threat Briefing

www.boozallen.com/ICS

Booz | Allen | Hamilton

CONTENTS

EXECUTIVE SUMMARY

Industrial Control Systems (ICS) represent an increasingly diverse and extensively connected set of technologies. ICS control and automate significant portions of our connected society, including power moving through the electrical grid, oil flowing through pipelines, travelers commuting on rail systems, and systems controlling pharmaceutical and food manufacturing. The reality is that more incidents involving ICS operators—organizations that use and maintain ICS as part of their operations—occurred in 2015 and into 2016 than any year prior.

Those who have an interest in disrupting these systems ("threat actors") include:

+ **Nation state-backed groups** target ICS in pursuit of geopolitical objectives. They seek to inflict disruptions and damage on national adversaries, gain access for future contingencies, and promote national economic interests.
+ **Criminals** seek monetary gain by extorting money from operators or through the sale of unauthorized access to ICS.
+ **Hacktivists** seek to promote a social, political, or ideological cause by conducting disruptive attacks.
+ **Insiders** inadvertently, or maliciously, introduce vulnerabilities to or cause incidents in ICS networks. This threat includes associated risks emanating from partner organizations and vendors.

Awareness of the risks associated with these systems is important, not just for the operational technology cybersecurity professionals responsible for securing these networks and devices but also for information technology professionals, organizational leaders, and regular employees. The impacts of attacks on ICS can be devastating. Attacks can cause extended operational halts to production, physical damage, and even jeopardize the safety of employees and customers. Furthermore, an attacker targeting ICS may first gain a foothold in the organization on a non-ICS system in the corporate network and use it to pivot into the industrial environment. The attack surface for ICS is larger than just the ICS devices, equipment, and networks: It extends to all parts of an organization, including the extended supply chain.

In analyzing the incidents over the course of 2015 and into 2016, several key findings emerged:

+ Nation states, cybercriminals, and insiders will likely continue to drive increased risk for ICS operators in 2016 and 2017.
+ New targets, including light-rail operators, and new tactics, such as supervisory control and data acquisition (SCADA) access as a service (SAaaS) and ransomware against ICS, are likely to emerge or expand.
+ The barrier to entry for threat actors is getting lower. While notable incidents involving hacktivists were not observed, publicly available attack resources emerged that may lower technical barriers for limited-skill threat actors.

+ Insider threats and improper access management provided avenues for attack and will continue to create vulnerabilities in 2016 and beyond.

Organizational leaders and cybersecurity professionals have a range of options to address these threats. This should occur as part of a comprehensive risk management program that combines information on vulnerabilities, threats, and impacts of an incident. Combining this information provides a complete understanding of risk and allows for the prioritization of mitigations. Mitigating risk requires more than just tuning firewalls or applying patches: It also includes establishing policies and procedures (e.g., an incident response plan), training staff, and architecting networks to achieve proper segmentation. While ICS and the plants, refineries, and power stations they control are relatively static, ICS operators, process engineers, and cybersecurity professionals need to adopt a strategy that recognizes and adapts to the changing threat landscape as vulnerabilities increase and adversaries evolve their tactics and techniques.

INTRODUCTION

The cyber environment that Industrial Control Systems (ICS) operators face today is more hazardous than ever before. The volume, types, and severity of cyber attacks against ICS are rapidly increasing. In 2015, ICS operators reported more security incidents to U.S. authorities than in any year prior—15 percent more incidents than the highest year on record.[2,3] Operators across a range of industries disclosed that cyber attacks on their networks had physically disrupted, and in some cases destroyed, their systems.

Nation state-backed groups conducted sophisticated and widespread campaigns to steal operational data and establish footholds in ICS environments. Cybercriminals expanded traditional tactics and developed novel techniques for profiting off operational technology (OT) breaches, including selling access to supervisory control and data acquisition (SCADA) networks and targeting ICS operators with ransomware. In addition, the constant threat of inadvertent and malicious insiders continued to cut into ICS operator resources through costly network disruptions.

This report provides an overview of the diverse uses of ICS and the expanding list of industries that rely on these systems and provides cybersecurity professionals and organizational leaders a broad perspective on the current threat landscape, as indicated by major incidents over 2015 and into the first part of 2016. Assessments on trends in targeting, threat actor tactics and objectives, and the steps to mitigate risk complement the overview of events. By analyzing the methods used, targets selected, and impacts of observed incidents, this report highlights the most significant threats that ICS operators are likely to face in 2016 and 2017.

One-Third of Operators Breached in 2015

In a 2015 survey of 314 organizations operating ICS around the world, 34 percent of respondents indicated that their control systems were breached more than twice in the last 12 months, and 44 percent of these organizations were unable to identify the source of the attack.[1]

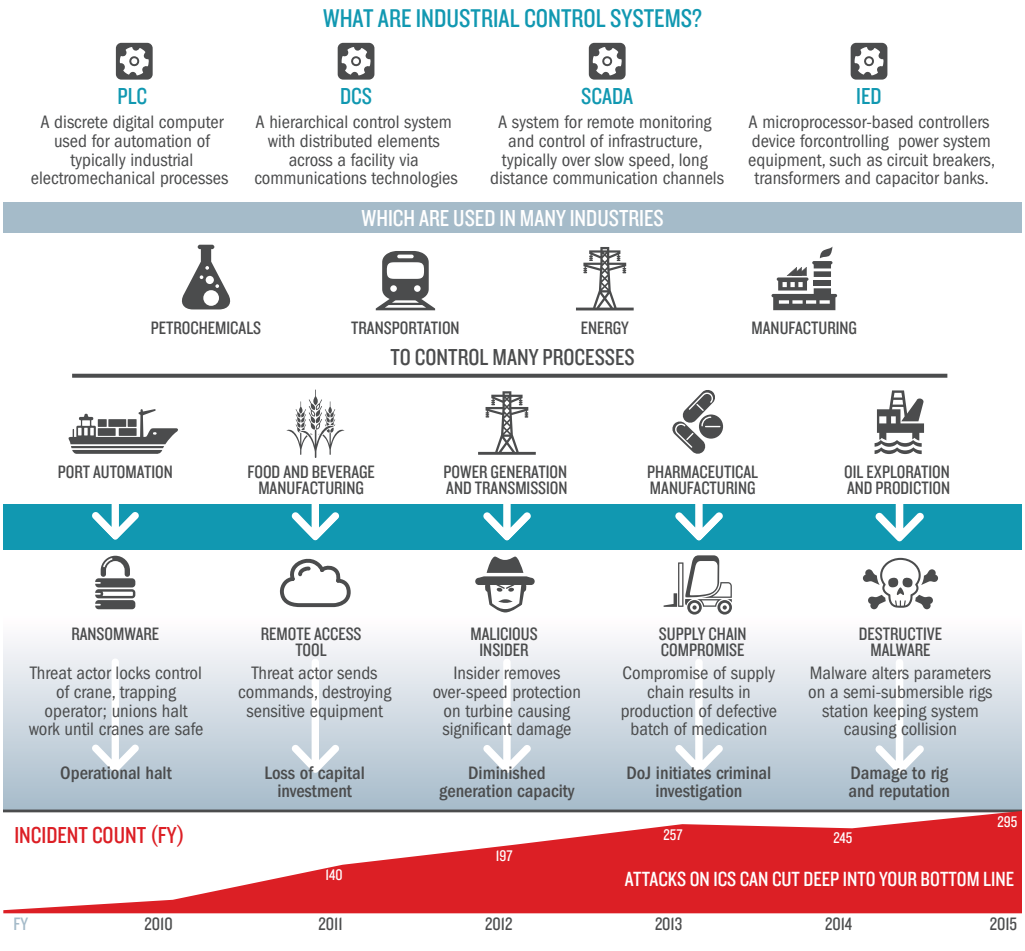
ICS ACROSS INDUSTRY

"We see continual and evolving challenges of a connected society that will extend well beyond what we are currently seeing with Internet of Things, telematics, and cyberthreats against IT networks. Modern ICS and the private and public businesses that operate them have benefited from Internet access to achieve efficiencies and better performance, but it is becoming difficult to separate traditional IT networks and OT used in industrial activities. As a result, we need to fully understand the threats presented to society's interconnected IT and OT networks."

—THAD ALLEN

Executive Vice President, Booz Allen responsible for the firm's Department of Justice and Department of Homeland Security business; presidentially appointed as National Incident Commander for the unified response to the Deepwater Horizon oil spill in the Gulf of Mexico

ICS represent a broad collection of computers, proprietary control devices, and networks and network architectures used to control industrial processes across a broad range of industries. ICS typically includes SCADA, distributed control systems, and programmable logic controllers (PLC). These devices can increase efficiency, accountability, and safety, but they can also introduce new vulnerabilities—and potentially enable cyber attacks to have physically destructive impacts. With the extensive deployment of these systems, potentially devastating impacts of attack, and constantly changing threat environment, it is important for business leaders and the engineering and cybersecurity professionals charged with providing



Sources

hxxps://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_S508C.pdf

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2012_Final.pdf

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf

hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf

security to be aware of the threats that their organizations face.

INCIDENT STATISTICS

Overall, ICS incidents are on the rise. The number of incidents reported to U.S. authorities rose by 20 percent in FY15.[6,7] With 295 reported incidents, 2015 had the most reported incidents to date.[8,9]

Primary industry targets: critical manufacturing, energy, water and dams, and transportation. For the first time since the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) began tracking reported incidents in 2009, critical manufacturing experienced more incidents than the energy sector.[10,11] This shift highlights a general trend toward targeting critical manufacturing, which began with a sharp increase in FY14, particularly manufacturers of control systems equipment.[12] This trend is largely attributed to a single, extensive campaign with attacks initiated by spearphishing.[13]

Spearphishing is the primary method of attack, with the number of attacks increasing by 160 percent—from 42 to 109—from FY14 to FY15.[15,16] Spearphishing was the initial attack vector for Operation Clandestine Wolf, one of the largest ICS attack campaigns of the year, as well as attacks on a German steel mill and Ukrainian electricity distributers, the two most destructive attacks disclosed in FY15.[ii]

Penetration of control networks from enterprise networks is on the rise. While still low at 12 percent of reported incidents, the number of incidents increased by 33 percent from FY14 to FY15.[17]

Although industry groups and government agencies such as ICS-CERT provide some data on ICS incident trends, investigators rarely publicly disclose details relating to particular incidents or campaigns. The following sections detail the major incidents from 2015, documented publicly.

ICS Operators

In this report, "ICS operators" refers to the organizational leaders and network security professionals at any firm using these systems to conduct business or engage in critical infrastructure operations.

ICS Attacks on the Rise

The total number of incidents reported by ICS operators rose by 20 percent in FY15.[4,5]

PRIMARY TARGETED INDUSTRIES REPORTED IN U.S., FY15[14]

INDUSTRY	INCIDENTS	PERCENT
Critical Manufacturing	97	33
Energy	46	16
Water and Dams	31	11
Transportation	23	8
Other[i]	98	33

i. Other sectors reporting incidents included the communications sector (13, 4%); commercial facilities (3, 1%); chemical (4, 1%); IT (6, 2%); healthcare and public health (14, 5%); government facilities (18, 6%); food and agriculture (2, 1%); financial (2, 1%); nuclear reactors, materials, and waste (7, 2%); defense industrial base (2, 1%); and uncategorized (27, 9%).

ii. Reported incident statistics detailed in this report are based on ICS-CERT's Fiscal Year 2015: Final Incident Response Statistics. The reporting period for FY15 is October 2014–September 2015.

KNOWN INCIDENT TIMELINE

April 25, 2016. Cybercriminals deliver ransomware via phishing to the corporate network of Board of Water & Light (BWL), a Michigan-based public electric and water utility. Administrators shut down the corporate network to isolate the ransomware to prevent it potentially moving into the OT environment. (Water and Dam)

April 25, 2016. Malware is discovered on a fuel assembly loading system at the Bavaria-based Gundremmingen nuclear power plant. (Electricity)

February 18, 2016. A system administrator for an unspecified shipping company discloses that a vessel in the company fleet was infected with Locky ransomware while underway. The ransomware was delivered via a malicious email attachment. (Transportation)

January–February 2016. An allegedly North Korea-affiliated group conducts a spearphishing campaign against two South Korean railway operators, in what the South Korean National Intelligence Service describes as a preparatory phase in targeting the railway traffic control system. (Transportation)

January 25, 2016. An unknown threat actor delivers ransomware via email to the Israeli Electricity Authority, Israel's electricity regulatory agency. Infected machines are taken off the corporate network for several days to prevent lateral movement, including into the OT environment. (Electricity)

December 23, 2015. An allegedly Russia-backed group establishes remote access to SCADA systems of three electricity distributers in Ukraine after procuring valid network credentials via spearphishing. The threat actors use access to systematically open breakers, causing blackouts for 225,000 customers. (Electricity)

December 2015. Security researchers disclose a campaign in which alleged Iranian threat actors gained access to networks operated by an American natural gas and geothermal electricity company. The threat actors stole engineering drawings of the firm's network architecture, including details on devices used to manage gas turbines, boilers, and other critical equipment. The breach was part of a campaign beginning as early as August 2013. (Electricity)

December 2015. North Korean hackers compromise the corporate network of a South Korean automatic train controller company and exfiltrate unspecified data which potentially could include OT related data. (Transportation)

December 2015. An allegedly Russia-backed group infiltrates systems at two unnamed Ukrainian companies in the railway and mining industries and deploys destructive malware previously observed in Ukrainian electricity distributer attacks. The attack was likely aimed at disrupting railway operations. (Transportation)

December 2015. Investigators disclose that an Iranian hacker established remote access to a SCADA system controlling the Bowman Dam in Rye, New York. The attacker gained access via the system's cellular modem and gathered information on water levels, temperature, and the status of the sluice gate. (Water and Dams)

August 2015. An allegedly China-backed group breaches the corporate network of Japan Railways Hokkaido and attempts to steal railway safety information. The threat actors used spearphishing emails to deliver the Emdivi remote access Trojan (RAT) and then unsuccessfully attempted to exfiltrate documents regarding railway crime prevention, railway communication systems, safety check procedures, security information, and railway safety, which may have been an attempt to carry out reconnaissance of OT related systems. (Transportation)

June 2015. A cybercriminal advertises the sale of SCADA access credentials on a Dark Web forum dedicated to selling stolen data. The post included a screenshot of SCADA graphical user interface, IP addresses, and virtual network computing passwords for a SCADA system managing a hydroelectric generator. (Water and Dams)

June 2015. An allegedly China-backed group is first observed conducting a large-scale phishing campaign against firms in the aerospace and defense, construction and engineering, high-tech, telecommunications, and transportation sectors. The group uses a zero-day Flash vulnerability to deliver a custom RAT to hundreds of targets which may have included and impacted the OT environment. (Manufacturing)

Early 2015. Cybercriminals deliver CryptoLocker ransomware onto American Electric Power's corporate network via phishing email to an employee. The malware was successfully contained on the corporate network by existing controls which may have prevented it from potentially moving into the OT environment. (Electricity)

Strong Interest ICS-Specific Malware

The emergence of multiple proof-of-concept malware has highlighted the strong interest in developing ICS-specific capabilities. In May 2016, German researchers developed a worm capable of propagating across Siemens PLC devices.[18] Similarly, in June 2016, researchers discovered another proof-of-concept malware targeting PLC devices in the wild.[19] The IRONGATE malware includes features to conduct Man-in-the-Middle (MitM) attacks by recording and replaying communications from a PLC back to the monitor, while sending modified data back to the PLC.[20] Though IRONGATE was designed to operate in simulated Siemens control environments, and was assessed as not viable against deployed devices, its development indicates the direction threat actors may be heading.[21]

EMERGING THREATS TO INDUSTRIAL SECURITY

In analyzing the incidents over the course of 2015 and into 2016, several trends emerged. Nation states, cybercriminals, and insiders will likely continue to drive risk for ICS operators in 2016 and 2017. New targets, including light-rail operators, and new tactics, such as SCADA Access as a Service (SAaaS) and ransomware against ICS, are likely to emerge or expand. Though notable incidents involving hacktivists were not observed, new attack resources emerged that may lower technical barriers for limited-skill threat actors. Insider threats and improper access management provided avenues for attack and will continue to create vulnerabilities in 2016 and beyond.

#1 — NATION STATE CAMPAIGNS

Nation state-backed groups have been and will continue to be the most significant single threat to ICS operators. North Korea and Russia are the threat actors most likely to conduct disruptive or destructive ICS attacks in the short term, and electrical generation and transmission and light-rail transportation operators are at greatest risk of such attacks. While China, Russia, and Iran have historically targeted U.S. ICS operators, China is the most likely to continuously seek to establish access on networks of U.S. operators.

Disruptive or destructive attacks against light-rail operators are likely based upon persistent North Korean reconnaissance targeting South Korea's rail sector over the past year. North Korea will likely continue to target light-rail operators in 2016. North Korea's demonstrated willingness to conduct destructive attacks against business-critical information technology (IT) systems in the banking and media sectors raises the likelihood that it would similarly attempt to disrupt a light-rail operator. While South Korea is North Korea's primary target, North Korea's history of targeting U.S. firms and explicit threat of cyber-retaliation against the U.S. make it the most likely threat actor to conduct a damaging attack against a U.S. operator. While not at first an obvious target, an attack against a transportation system such as a subway system in a dense, highly populated city environment could have significant effects on commerce, business, and productivity.

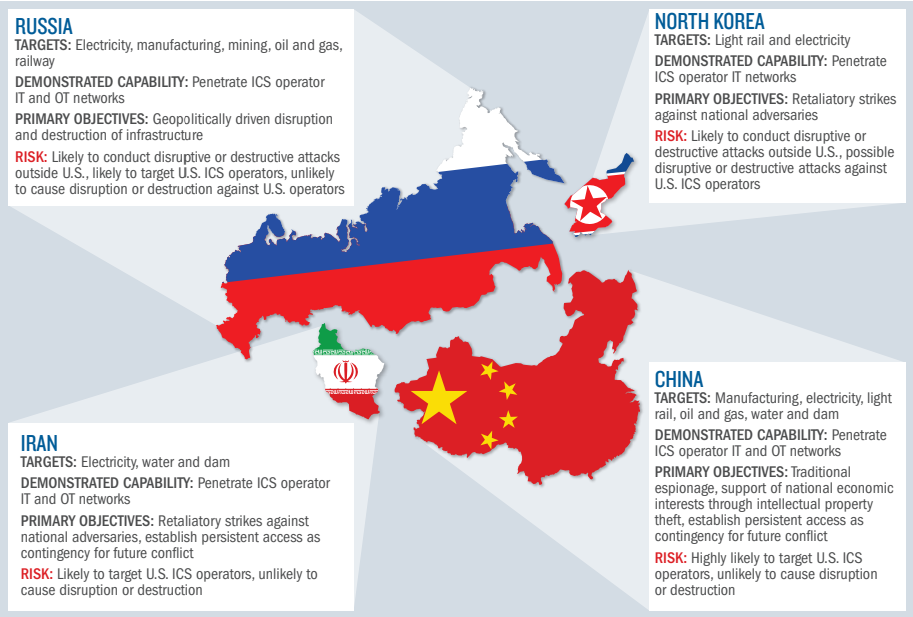
Disruptive or destructive attacks in Eastern Europe will most likely be conducted by Russia-backed groups. Russia will also continue to seek access to ICS in the U.S.—particularly in the energy sector—and is likely to conduct additional disruptive or destructive attacks that align with its broader geopolitical interests, but it is not likely to conduct such attacks against the U.S. Given the limited retaliation against Russia for previous destructive ICS attacks, Russia will continue to explore the use of such attacks, though targeting U.S. firms presents a more significant risk of retaliation.

Continued Chinese penetration of U.S. networks across many sectors is likely, but

"Attacks on ICS (which are inherently vulnerable to exploitation) increased last year and will continue to increase as a primary method of achieving degradation or destruction in critical infrastructure systems. Criminal elements will aggressively pursue attacks against ICS as a means to extort cash from critical infrastructure operators. Critical infrastructure operators need to think now about systematically reducing ICS vulnerabilities."

—MIKE McCONNELL

Senior Executive Advisor and former Vice Chairman of Booz Allen; served as the Director of National Intelligence from 2007 to 2009



Nation State Groups

Nation state-backed groups operate under the direction of, or in coordination with, national military and intelligence services. These groups represent the most sophisticated, well-resourced groups in the ICS cyberthreat landscape and the most significant threat to ICS operators.

Let the Hunt Begin!

Employing trained vulnerability researchers will help to discover previously unknown vulnerabilities that advanced actors could use. Establishing "hunt" teams to proactively search for adversaries on a network helps to decrease time from breach to detection.

the attackers are unlikely to use the access to cause disruptions or damage in the near term. China will likely continue to seek widespread and persistent access to U.S. ICS networks to conduct intellectual property theft and cyberespionage, and it is unlikely to engage in disruptive or destructive attacks. China is unlikely to escalate its operations' impact without a significant deterioration in U.S.-China relations.

So which nation state presents the most cyber risk to operators of critical infrastructure and ICS in the U.S.? In comparing the relative risk of the four nation state APTs, there are several factors at play that make a simple ranking difficult. China is the most capable and active in conducting attacks against U.S. ICS operators, and it is the most likely to be gaining access to U.S. networks. We believe that it is important to highlight that these nondestructive attacks are very likely to continue. Russia and North Korea are likely to cause destructive attacks outside of the U.S. Of the four, if North Korea were able to gain access to ICS networks in the U.S., it is the most likely to use that access to cause a disruptive/destructive attack. Fortunately, North Korea may have a legitimate shortfall in capability and experience; to date, it has only accessed corporate networks of ICS operators, not operational networks.

#2 — RANSOMWARE TARGETING ICS OPERATORS

Ransomware's use and variety grew massively in 2015 and early 2016. This emergence represents a significant threat for ICS operators: Infections on these systems may cause broadly impactful, tangible impacts, making them choice targets for many attackers. Ransomware targeting ICS may differ from IT ransomware; instead of encrypting files, the malware could disrupt operations or prevent access to an asset.

Ransomware is rapidly expanding, as illustrated by the increase of new samples of ransomware from less than 100,000 in the second quarter of 2014 to more than 1.2 million in the second quarter of 2015.[22] Total ransomware observed during this period increased from approximately 1.5 million to more than 4 million. This explosion in ransomware continued to rise, with 6 million observed samples in the fourth quarter of 2015.[23]

Ransomware is readily scalable and hugely profitable due to incorporation into exploit kits that facilitate a build once, infect many approach. Ransomware is often developed and incorporated into prebuilt exploit kits by a single author who collects a percentage of extorted fees from a large number of unsophisticated attackers using the tool.[24] This model provides a veritable army of attackers to ensure massive infection rates; infection for some variants were estimated at 90,000 machines per day in February 2016.[25] These massive rates of infection, in turn, yield huge returns for attackers: Between January and October 2015, campaigns for one variant—Cryptowall version 3.0—generated an estimated $325 million in revenue.[26]

ICS assets are vulnerable due to the incorporation of IT software into ICS assets, such as Human Machine Interfaces (HMI) and data historians. Malware[iii] infections on such systems are common and could affect ICS that rely on vulnerable IT software.[27] Multiple ransomware attacks against corporate networks of ICS operators have been observed, including the attacks against American Electric Power[28] and BWL.[29,30]

ICS represent potentially high-vulnerability, high-value targets, given that older systems may not be restorable from a backup, the difficulty in obtaining a clean version of system software and configuration settings, the difficulty accessing the device, or a lack of trained personnel available to restore the system.[31] An attack could bring production to a standstill, with limited options for operators other than paying the attackers. For example, Hollywood Presbyterian Medical Center was hit by ransomware in February 2016. Halting critical systems, such as machines required to deliver patient care, allows attackers to demand significantly higher payment relative to other ransomware attacks. Typical ransomware payments are several hundred dollars. The attackers demanded $3.4 million from Hollywood Presbyterian, but eventually allowed the hospital to pay $17,000 to restore its systems.[32]

Frequency and severity of ransomware infections on ICS networks are likely to increase. Publicly reported ransomware infections that impact ICS have been limited to several incidents in the water[33] and electrical[34,35] utility sectors, all of which have been contained to corporate IT networks. Ransomware attacks are likely to affect ICS operators in other sectors, potentially inadvertently, and a ransomware infection that spreads to a control network will likely occur in the near term. In addition, security researchers have developed proof-of-concept malware that targets ICS (e.g., a worm designed to propagate through PLC devices[36]). The weaponization of proof-of-concept code is likely if the monetary value of targeting ICS becomes clearer to cybercriminals.

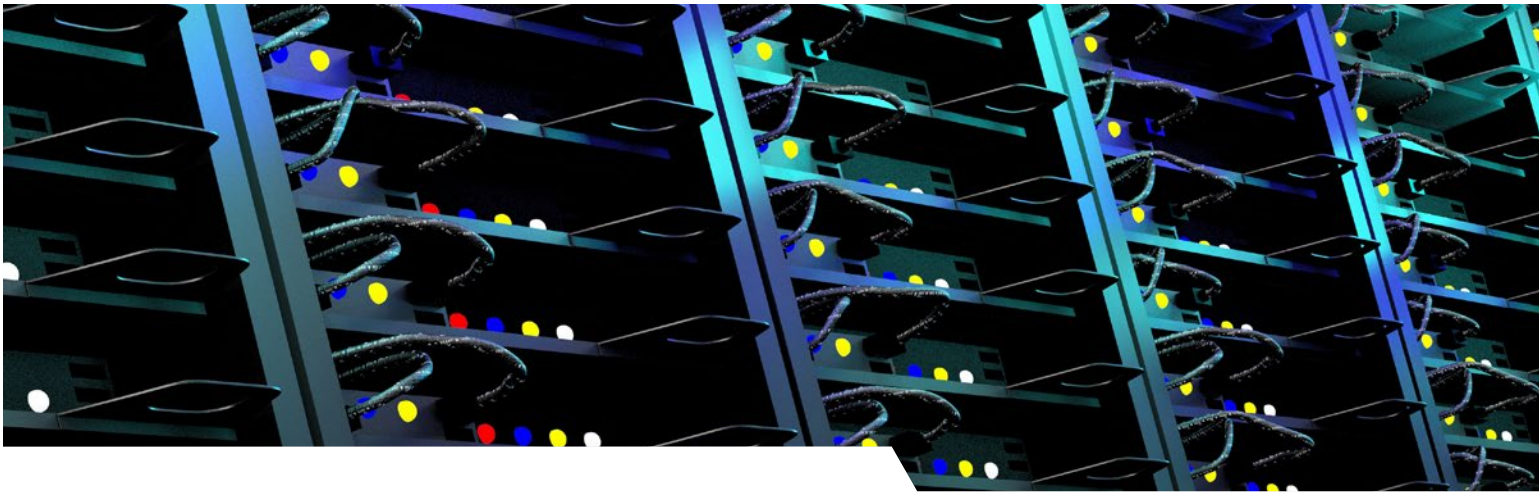
Threats to Corporate Networks

Malware infections, or unauthorized intrusions, on corporate networks are important for several reasons. Corporate networks are a likely entry point into control environments; as noted previously, rates of successful lateral movement increased by 33 percent in 2015. In addition, even without successful movement onto OT networks, disruption of business systems can have similar impacts to attacks on ICS, such as degrading productivity and availability of core production resources. This risk is particularly important because, in highly regulated spaces such as commercial nuclear and utilities, corporate networks fall outside of regulatory cognizance. Despite the regulatory blind spot, attacks on corporate networks could still degrade core delivery.

Wall Off the Gardens

Proper segmentation (e.g., the Purdue Model) of IT and OT networks, as well as sections of the ICS network, will help mitigate the risk of ransomware attacks. Ransomware is most likely to infect an operator's IT network as result of an employee opening a phishing email or visiting a compromised website. If the networks are properly segmented, the ransomware is unlikely to be able to migrate to OT assets and disrupt ICS.

iii. No incident specifically involving ransomware on ICS component devices has been disclosed publicly.



Access as a Service

Access as a Service is the process of identifying zero-day vulnerabilities and incorporating exploit of these vulnerabilities into a managed service, in which service providers sell clients' unauthorized access to third-party networks. SAaaS is the application of this process to control environments.

Scouts Out!

Incorporating threat intelligence into your cybersecurity operations will help to stay abreast of developments in the threat landscape. Using threat intelligence will improve understanding of risk and aid in the effective prioritization of mitigations. Threat intelligence may also provide near-real-time warnings of developments of threat actor capabilities and intent.

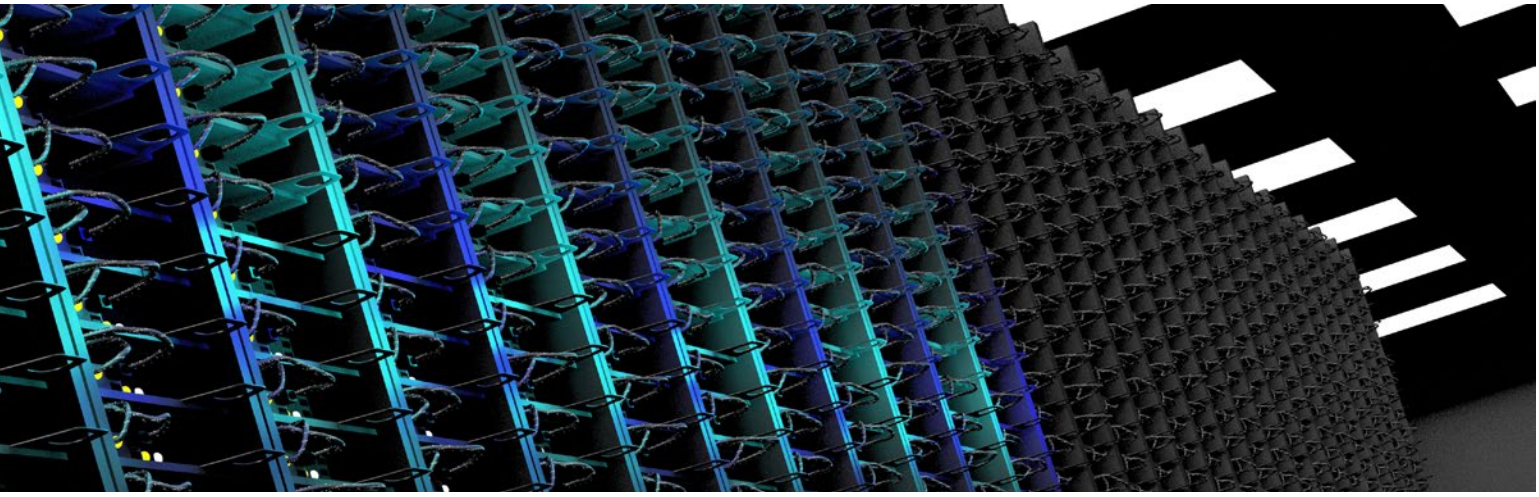
#3 — SCADA ACCESS AS A SERVICE

Selling Access as a Service is a well-established, lucrative business model in the cybercriminal world. In 2015, cybercriminals were first publicly observed selling access to ICS systems.[37] If SAaaS were effectively implemented, it would likely find substantial market demand. Terrorists and hacktivists have stated their intent to target ICS, and nation state-backed groups may leverage the service to reduce their operating profile and prevent the unnecessary discovery of custom tools.[38]

Access as a Service is an established business model of both white-hat cybersecurity firms and cybercriminals. Many companies, such as Italy-based Hacking Team[39] and France-based VUPEN Security,[40] have developed lucrative businesses based around this capability. Firms have also explored vulnerabilities in ICS systems specifically. In 2011, GLEG Ltd. announced the sale of the Agora SCADA+ Exploit Pack for use in the Immunity CANVAS penetration testing framework.[41] Furthermore, in 2012, Maltese cybersecurity firm ReVuln, which self-describes as an "offensive and defensive security" firm, advertised a series of remotely executable, zero-day vulnerabilities it had identified in SCADA and HMI systems.[42,43] Though it is unclear if the firm operationalized these vulnerabilities into an Access as a Service model, it acknowledged its intent to sell the details of its research.[44] As legal enterprises, these firms typically serve intelligence and law enforcement agencies,[45] though cybercriminals following this model are likely less scrupulous in the clients they serve.

SAaaS has existed on the black market since at least 2015, when there was the first publicly known attempt to sell access to a SCADA system.[46] The SCADA incident indicates that threat actors are aware of the potential opportunity—and that other technically skilled criminals may follow suit. The seller, alias Bonito, did not appear to have a specific interest in ICS. Previous posts indicate that he typically traded in personally identifiable information[47] and healthcare data,[48] and it appears he was applying skills developed through more traditional cybercrime to a new set of targets.

Demand for SAaaS is still low, and potential buyers are skeptical of the value. In the Bonito post, an individual using the handle cre8iv praised Bonito but was skeptical of the offer's value, noting that this access was "worthwhile only to terrorists/activists […] or groups pushing a message looking to start with a big bang."[49] Access to a control system would be valuable for its



disruptive or physically destructive potential. Hacktivists, terrorists, or even military or intelligence services, which may lack the technical skills to gain access on their own, might want to pay for the opportunity to cause such outcomes. Hacktivists[50] and terrorist groups have explicitly detailed intentions to conduct destructive cyber attacks against such targets as airports, hospitals, and electricity providers.[51]

Expansion of SAaaS operations is a credible near-term threat. If demand continues to increase, cybercriminals will be incentivized to expand their existing Access as a Service business model to these systems. Potential buyers, such as hacktivists and terrorists, would be interested in access for the explicit purpose of sending a message through physical destruction or disruption of operations. The risk of attack by less sophisticated threat actors is somewhat mitigated by the technical complexity of effectively using SAaaS to conduct an attack. Manipulating control systems requires specialized expertise, and threat actors that rely on purchasing access may not have the necessary skills to carry out their malicious intentions once they have it.

#4 — FREELY AVAILABLE ATTACK RESOURCES

Several developments in 2015 indicate that threat actors with relatively limited expertise and resources, such as hacktivists, may have more tools at their disposal to identify targets with known vulnerabilities and conduct purposeful attacks once they have gained network access.

Reconnaissance search engines became more plentiful in early 2015 with the deployment of Censys. The value of such a tool was not lost on malicious threat actors. Several Dark Web forums reference the tool[52,53,54] or include Censys in list of reconnaissance tools.[55] One post on a Russian-language forum even lists a targeted query and highlights the irony of the tool being released for security professionals.[56] Though no specific attacks have been explicitly linked to use of the tool, the project team discovered devices including ATMs, bank safes, and ICS for power plants.[57] The risk of potential abuse of this resource is likely.[58]

Increased interest in ICS programming skills from threat actors that currently lack the capability but possess the intent to target ICS. Implementing and operating ICS requires additional, ICS-specific programming skills. For this reason, purposefully

Expansion in Powerful Vulnerability Scanners

In January 2015, researchers deployed Censys, an open source tool designed to aid security experts and penetration testers in identifying devices and services exposed to the Internet. Though not the first tool of its kind, the Censys tool conducts and archives results from Internet-wide scans more frequently than existing tools; allows much more complex queries, including searches for specific vulnerabilities; and is not restricted by a pay wall, unlike existing tools.

Understand the Attacker

Looking at your organization from the perspective of the attacker (e.g., by using Censys or Shodan) can help you to better understand your attack surface and identify vulnerable assets. Relying on system architecture schematics can be misleading; implementation often differs from design.

Vulnerability Exploitation via Supply Chain Attack

Recently, Booz Allen identified a number of vulnerabilities in process control devices that are used extensively in the energy sector. Given the nature of the vulnerabilities, a significant concern is the possibility of threat actor exploitation through compromise of the supply chain for device updates. Reporting in 2014 revealed that Energetic Bear, an allegedly Russia-backed group, had compromised at least two manufacturers of ICS networking equipment. The attack allowed the group to embed the Havex RAT into the vendor's software. A future attack against the energy sector could combine a supply chain attack with malware that exploits the vulnerabilities in process control devices to obtain the ability to affect industrial processes that are otherwise inaccessible due to air gapping or network segmentation.

interfering with ICS in a controlled way is beyond the capability of most threat actors with programming backgrounds based in traditional IT systems. Unsurprisingly, interest among threat actors in developing ICS-specific capabilities, such as PLC programming, is on the rise. In January 2016, a file collection containing PLC programming courses for a range of ICS devices was shared in the Hack Turk forum, a Turkish Web forum for discussing hacking tools and methods.[59] The posted files contained pirated versions of a PLC training program produced by NFI Industrial Automation Training Academy, a company providing automation training for engineering students and industrial operators.[60] Though the post was not sensitive or inherently malicious, the target audience of the forum indicates interest in ICS among likely malicious individuals.

Loosely organized groups, such as hacktivist groups, often lack the coordination and resources to establish and maintain persistent network access. Instead, these groups typically rely on identifying easy-to-exploit Web-facing vulnerabilities. Scanning tools can reduce the technical barriers in finding potential targets. In the same thread, these groups have recognized the need to develop ICS-specific expertise and are actively pursuing the resources necessary to develop these skills. As more sophisticated tools become available, the already dubious value of security through obscurity will rapidly diminish, requiring ICS operators to take more effective steps to mitigate risk to their systems.

#5 — SUPPLY CHAIN COMPROMISE

Supply chain attacks also represent a persistent, and particularly dangerous, threat to ICS operators. Though not directly affecting OT, an incident in early 2016 involving the healthcare industry represents the latest attack in a string of supply chain compromises. On April 22, 2016, a user on DSLReports, a broadband Internet discussion forum, posted a screenshot of malicious code discovered on a USB device he received from the American Dental Association (ADA).[61] The code redirected users to a Chinese website known to host malware.[62,63] ADA noted that the USB drives had been manufactured in China by a subcontractor for one of its vendors.[64] They had distributed 37,000 of the devices to ADA members to provide dental procedure codes used to document billing and insurance claims.[65] Devices provided by trusted vendors have proven to be an effective attack vector for sophisticated threat actors. Recent incidents indicate that the threat is widespread in both targets and attack vectors, though primarily conducted by nation state-affiliated groups.

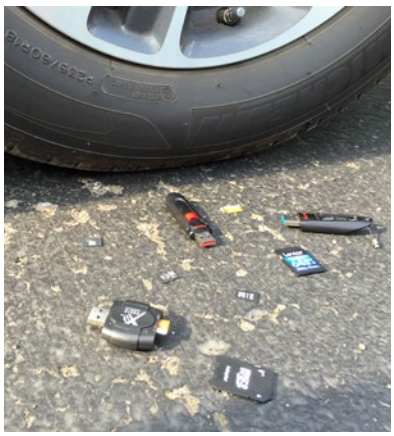
Supply chain attacks have affected a variety of targeted industries. In addition to the healthcare industry attack noted previously, the shipping, manufacturing, electricity, and oil industries are all identified targets. On November 5, 2014, security researchers reported on a hardware compromise involving devices used for scanning items at shipping distribution centers.[66] Though shipping companies were

the primary target, the report noted that the malicious hardware device had also been sold to a manufacturing firm.[67] In a campaign lasting from early 2013 through 2014, an allegedly Russia-backed group, alternatively known as Dragonfly and Energetic Bear, targeted operators via supply chain attack in electricity distribution, electricity generation, oil pipeline, and energy industry industrial equipment manufacturers.[68]

ICS hardware as the attack vector. Specialized devices used in OT environments are one potential vector. The device used in the malicious scanner incident included malware designed to launch automated attacks against corporate networks, establish connections to an external command and control server in China, and ultimately exfiltrate financial and operational data on targeted firms.[69]

Commodity hardware as the attack vector. Hardware-based supply chain attacks can also be conducted using ubiquitous devices, such as the USB drives used in the ADA compromise, or network infrastructure, such as modems and routers. Reporting in August 2014 indicated that Chinese routers manufactured by Netis and Netcore included hardcoded backdoors that allow attackers to monitor network traffic.[70] Though vulnerabilities such as backdoors can be the product of vendor negligence, China has been previously accused of instructing network device manufacturers, including Huawei and ZTE Corp., to leave backdoors in their devices to support cyberespionage efforts.[71]

Device firmware as the attack vector. In addition to attacks conducted using malicious hardware, firmware updates also present an effective supply chain attack vector. Toward the end of its campaign, the Dragonfly/Energetic Bear group compromised targets by inserting Trojans into firmware updates for PLC devices hosted on vendor websites.[72]



The threat of supply chain attacks has been predominately conducted by allegedly nation state-affiliated groups. China-backed groups have been a common element in most of the publicly reported supply chain attacks, though Russia-backed groups represent a significant threat as well. Supply chain attacks represent a uniquely dangerous vulnerability because malicious hardware or software can enable attackers to bypass network security measures implemented on corporate or external-facing networks and directly access ICS. The target in the compromised scanner attack, for example, had deployed firewalls, IPS, IDS, mail gateways, and other network monitoring systems—none of which detected the attack.[73] The malware-equipped scanner essentially enabled a reverse pattern to typical ICS attacks, where the attack initiated at operational facilities and migrated outward through corporate networks. These types of attacks also exploit an inherent trust that operators may have in their vendors, highlighting the

"Due to automated tools and cheap compute through botnets, a cyber attack costs a fraction of what it takes to defend. Security Automation through adaptive response, leveraging advanced analytics and machine learning, helps sift through the noise and focus on real threats against our critical infrastructure."

—SNEHAL ANTANI

CTO of Splunk

necessity to conduct due diligence investigations prior to engagements and security-focused assessments of the devices connected to their networks. Fortunately, these attacks have been limited to the most advanced nation state threats and, given the significant resources needed to conduct such attacks, will likely remain beyond the capabilities of all but the most well-resourced threat groups.

#6 — IMPROPER ACCESS CONTROL AND MAJOR DISRUPTIONS

While attacks against ICS would seem to be on the cutting edge of cyberthreats, successful attacks often rely on user error or oversight that allow access onto and across critical networks. Phishing, for example, was the primary attack vector in 2015 and was the first step in several of the most sophisticated and destructive attacks. In many cases, the incidents were possible because the victim's access control policy did not adhere to best practices (e.g., principle of least privileges).

Negligent and malicious insiders are some of the most significant threats to ICS operators. According a 2015 survey of control system operators, 25 percent of reported breaches were attributed to current employees.[74] Insider threats can be unintentional, such as the ransomware attack against the Michigan-based BWL[75] or the Israeli Electricity Authority,[76] or malicious, though impacts can be significant regardless of intent.

Vendors and partner organizations are a significant source of insider risk for ICS operators. In the breach of Calpine Corp.'s networks, the recovered diagrams and credentials were allegedly stolen from a contractor who works with the firm.[77] Negligence on the part of vendors also creates risk for ICS operators. In an attempt to prompt vendors to discontinue the use of hardcoded credentials in their devices in December 2015, researchers released a database of hardcoded passwords for PLCs, remote terminal units, HMIs, and other devices from 37 different vendors.[78]

Risks associated with employees, vendors, and partner organizations will remain a persistent and significant threat for all operators. Despite the pervasiveness of this threat, it is also the most readily mitigated. Instituting standard network security and personnel management best practices will greatly improve organizations' risk profiles.

ADDRESSING THE GROWING CYBERTHREAT AGAINST ICS

Addressing the threats against your process, ICS equipment, and systems does not mean that every possible risk will or can be mitigated. In most business organizations, constraints such as financial resources, the inability to implement mitigation techniques due to operational requirements or availability, an ever-changing landscape of threats and vulnerabilities, and skills and expertise gaps mean that there will always be some residual risk, irrespective of budget and expertise.

When developing strategies to protect and defend against these increasing threats, consider an incremental approach, adopting best practices that have been refined from years of defending the enterprise. When developing your roadmap, focus on high impact, low cost cost initial steps that buys down near-term risks while providing the foundation for a long-term strategy. Also, continue to plug into the innovation ecosystem where there is significant investment in emerging technologies and solutions that provide new techniques and solutions for securing the OT environment. Below are some basic steps we can all take.

UNDERSTAND AND ENUMERATE THE RISK

It is extremely difficult, if not impossible, to protect any environment without full visibility of the critical digital components that are deployed within the field. Without knowledge of digital components, you cannot assess vulnerabilities, threats, or impacts. Understanding the digital components, true network architecture, operational process roles and interdependencies with other systems support which operational processes is a critical step in translating the overall system risk. While many organizations stop at identifying assets, to deploy effective and cost-efficient risk mitigations, your organization must understand the potential cost to health, safety, environmental compliance, and of course to production and profitability of an incident for each asset and prioritize accordingly.

Adopt a comprehensive risk management strategy that looks across cyber and physical environments to help you understand your threats, risks, and consequences (both cyber and physical).

ICS THREAT INTELLIGENCE

Understand the threat actors (hacktivists, nation states, etc.), their motivations, their tactics and techniques. Pay attention to the socio-political environment. Look closely at the regions in which you operate, understand your supply chain and those of your partners, your IT outsource organizations, your ICS vendors and third party integrators, and your maintenance providers. Put yourself in the position of an adversary and try to imagine what you would attack if you were intent on causing some operational, financial, reputational, or catastrophic damage to your operating environment and to the surrounding community.

Evaluate the risk in your supply chain. Evaluate open source and subscription-based threat intelligence feeds, commercial service offerings, and other sources of information to help you in the changing threat landscape.

ICS ARCHITECTURE, MONITORING, AND SITUATIONAL AWARENESS

Cybersecurity represents another in a list of potential disruptors to your business operations. It is important that you identify potential risk early and that you quantify and communicate the potential impact to your business quickly. Implement a defense in depth architecture with segmentation to

Implement an OT-centric view of cyber risk for your operational staff. Distill the information and allow your operators and engineers to view the data in terms of potential business impact.

Provide an organizational foundation for education of threats against ICS, basic cyber hygiene principles, and targeted messaging for your OT operators that addresses threat vectors. Manifest mitigation into policies and procedures. Educate your workforce about threat vectors: wired networks, wireless networks, removable media, the supply chain, and insider threat.

Develop plans and procedures that coordinate operational, engineering, IT, and other support teams to respond properly to ICS cybersecurity events. Test them!

As technology changes and threat increases, it is important to have tight integration between operational plans, infrastructure changes, plant upgrades, and general technology updates.

provide lateral movement within the network. Architect your systems to minimize exposure from remote access and the Internet. Implement cybermonitoring of basic IT controls and device activity. By monitoring OT networks and relating the risk back to the business and operational processes they support, you can enable operators and engineers to become your first line of cyberdefense. Consider adding OT cybersecurity disruptors to your process safety management and risk management planning methodologies, to address cyber vectors early in design and commissioning phases of a facility.

AWARENESS AND TRAINING

Cyber risk in the OT environment is of growing concern around the globe. Effective training from C-level executives to the team of operators and engineers on the plant floor is a critical activity to create awareness around priority threats and risks to safety and environment. In addition, a solid ICS security awareness and training program will allow your organization to normalize communications around a basic language, so you do not lose critical minutes during an event trying to communicate on what may have just happened and how, and what to do to mitigate the effects, if any.

INDUSTRIAL INCIDENT RESPONSE

Understanding what areas to focus on, and what needs to be done in a complex environment in support of incident response, is critical to recover to a safe mode and to smoothly return to normal operations. The goal of any incident response plan is to minimize operational impact and the potential for a re-occurrence. Pre-defined procedures that have clearly defined roles, responsibilities, and actions will enable your organization to communicate effectively, minimize impact, and maximize control during and after an incident. Develop table top and real world exercises that test your cyber readiness, and exercise them often.

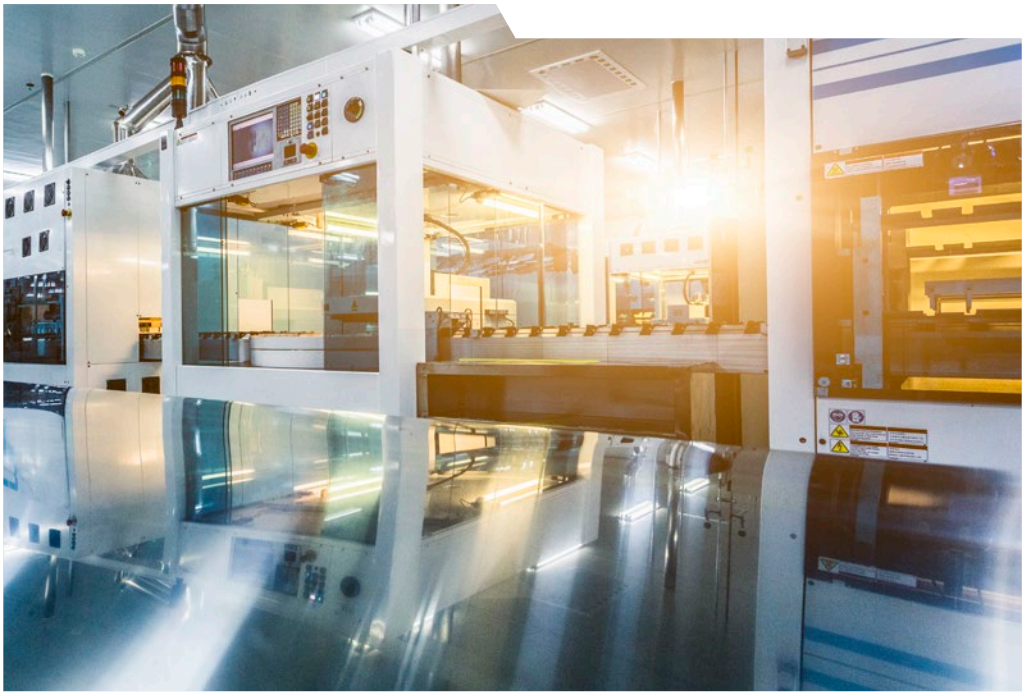
OT GOVERNANCE

Effective change management allows organizations to avoid costly incidents in the future. Defining effective governance is a key tool in bridging the gap between your IT and OT communities and will allow for the best solutions with minimal impact. A critical success factor for OT cybersecurity and the ability to manage risk going forward will be to ensure the teams liaise and communication regularly by putting in place a governance structure to enforce better collaboration! Make use of existing process safety, health protection, and environmental compliance programs to extend their proven methodologies (and regulatory requirements) to the cybersecurity of OT, ICS, and operating processes. Make sure that any OT governance model includes plant operations, controls, engineering, and maintenance management functions in significant roles, since these groups use ICS to manage the plant everyday, and understand the ICS relationship to safety and operability.

PARTING THOUGHTS

Threats to ICS are increasing, and the threat landscape is constantly changing. New threat actors bring new motivations and capabilities for attacking ICS. We currently measure the impact of their attacks by the thousands of customers affected or millions of dollars in damages. Before long, we may measure impact in millions of customers affected and billions of dollars in damages. Understanding the threat and potential methods for addressing the threat is an important first step to defending your organization.

Addressing ICS cybersecurity threats should be at the forefront of any operating organization's risk management program, and it should focus on the fact that risk changes over time. Take the time to create a detailed understanding of your critical infrastructure. This includes the threats to and vulnerabilities in specific systems—including software vulnerabilities, misconfigurations, and inadequate implementation of security controls—and the impact and consequences of compromise of your core operations' technology and processes. This will provide you with the ability to identify sources of risk, effectively prioritize them, and take steps to mitigate and manage them.



"At the end of the day, our clients are focused on health, safety, environmental compliance, and continuity of operations. The increasing cyber threats to their operational environments and extended enterprises represents a significant challenge that must be addressed. To be prepared, they must understand their environment, understand their adversaries and potential attack vectors, and put monitoring solutions in place to protect and defend their critical assets."

—BRAD MEDAIRY

Senior Vice President at Booz Allen leading the Cyber Futures team which focuses on delivering next generation enterprise and industrial cyber solutions

APPENDIX A: DETAILED DESCRIPTIONS OF INCIDENTS BY SECTOR

Economy of Scale

By reducing the time spent profiling targets, Gothic Panda more easily targeted multiple people within the same organization in a shorter timeframe.[80] Incident handlers at targeted organizations may have given less attention to the messages, given their unremarkable appearance as generic spam-like messaging.[81]

MANUFACTURING

Most of the reported incidents in the manufacturing sector relate to a single, large-scale phishing campaign.[82]

U.S. manufacturing sector, phishing campaign. In June 2015, a Chinese[83,84] threat group known as Gothic Panda[85] (a.k.a. UPS,[86] APT3,[87] Group 6,[88] and TG-0110[89]), launched a large-scale phishing campaign targeting firms in the aerospace and defense, construction and engineering, high-tech, telecommunications, and transportation sectors.[90] Gothic Panda used spearphishing messages that included hyperlinks to sites hosting an exploit script. After following the link, the malicious sites exploited a zero-day vulnerability (CVE-2015-3113) to deliver the SHOTPUT remote access Trojan (RAT) onto targeted systems.[91] The RAT used in Operation Clandestine Wolf, referred to as SHOTPUT,[92] was a variation of malware used solely by Gothic Panda[93] in previous campaigns, known as Backdoor.APT. CookieCutter[94] (a.k.a. Pirpi[95]). No publicly available sources document Gothic Panda ever successfully navigating into a target's Industrial Control Systems (ICS) environment. Operation Clandestine Wolf evolved from earlier attacks by Gothic Panda. While previous campaigns used spearphishing attacks, such as profiling specific personnel via social media and directly contacting them under false pretenses,[96] the Operation Clandestine Wolf campaign used generic messages often advertising sale of discounted Apple products.[97]

ENERGY

Despite the relative decline in the number of reported incidents in the energy sector in FY15, the few incidents covered in depth in public reporting were among the most significant in recent years in terms of demonstrating the disruptive potential of ICS cyber attacks.

German nuclear power plant, malware attack. On April 25, 2016, the Bavaria-based Gundremmingen nuclear power plant disclosed that it had discovered malware on its systems.[98,99] The plant's system audit uncovered W32.Ramnit and Conficker malware on the fuel assembly loading system,[100] which regulates the transport of spent fuel from the reactor core to the storage pool. Both of the malware are designed to self-propagate across an infected network, though W32.Ramnit also enables remote access to infected systems with Internet connectivity.[101] Reportedly, the system was not externally facing, and a Gundremmingen spokesperson stated that "sensitive areas" of the power plant are designed to be "manipulation protected."[102] Although details about how the system became infected were not disclosed, 18 USB drives used at the plant were also found to be infected with the malware, indicating that an employee may have introduced the malware onto the system using a removable media device.[103]

Ukraine energy grid, operational disruption. In December 2015, the first successful disruption of a public energy grid occurred in Ukraine. On December 23, 2015, blackouts affected more than 230,000 customers following cyber attacks against three major electricity distributers.[104] Attackers obtained credentials via spearphishing, established remote access via virtual private network, and used administrator services to access the supervisory control and data acquisition (SCADA) network.[105] The attackers used the SCADA network to systematically access Human Machine Interface (HMI) software and Serial to Ethernet adapters to disrupt communication and overwrite firmware, followed by accessing breakers and Universal Power Supplies to turn off power and ultimately create an outage. This was done in coordination with a denial-of-service attack on call centers, which delayed reaction time.[106] No specialized exploit tools were used to gain access; the spearphishing attacks relied on users enabling macros in a malicious Word document attachment.[107] The attackers used the SCADA network access to systematically open circuit breakers, halting electricity distribution to customers, and then wipe the master boot record of HMI systems using malware to draw out recovery time.[108,109] Ultimately, operators had to shut down their SCADA network to regain control. In addition, because the attackers had pushed malicious firmware updates to converters at many of the substations,[110] workers had to reset the breakers manually to bring electricity services back online. While requiring some customization in the attack method for the three distinct SCADA systems operated by the firms, the attack was well planned and effectively executed but not technically sophisticated.

Israeli regulator and American utility operator, ransomware. While not a risk unique to the energy sector, several operators and regulators sustained ransomware[iv] attacks in 2015. On January 25, 2016,[111] ransomware was delivered via spearphishing to the Israeli Electricity Authority.[112] After an employee opened the malicious attachment, ransomware spread across the network, prompting administrators to take the infected machines on the corporate network offline for several days.[113] The Israeli Electricity Authority, a regulatory body, is distinct from Israel's state-run utility, Israel Electric Corporation,[114] and the attack had no impact on grid operations.[115]

In early 2015, an operations supervisor at a subsidiary of American Electric Power, the largest U.S. grid operator, opened a personal email containing the CryptoLocker ransomware on the company's corporate network.[116] Ultimately, the anomalous network traffic was detected, and existing controls prevented the infection from spreading or establishing a connection to an external command and control (CC) server necessary for the malware to encrypt files.[v,117]

Complete Attack Analysis

An in-depth, technical analysis of the attack chain for the Ukrainian energy attack, as well as attribution details, will be released in a subsequent report.

iv. Ransomware is malware that encrypts files on the infected user's systems and then offers to decrypt the files for a fee.

v. After infecting a system, ransomware typically need to connect to a CC server via the Internet to receive a public encryption key before files can be encrypted.

U.S. electricity operator, data exfiltration attack. In December 2015, investigators disclosed a major reconnaissance and data exfiltration attack against Calpine Corp., an American natural gas and geothermal electricity company.[118] Security researchers noted that the breach likely began in August 2013, but it may have been active at the time of the disclosure.[119] During the campaign, attackers operating from IP addresses in Tehran, Iran,[vi] delivered a Trojan referred to as TinzZbot to establish remote access, conduct keylogging, and retrieve screengrabs from targeted networks.[120] After gaining access, attackers transferred data to a collection of FTP servers.[121] While reviewing the FTP servers, investigators discovered credentials that enabled remote access to Calpine Corp.'s networks, including its operational technology environment. Investigators also found engineering drawings detailing the firm's network architecture; the devices used to manage gas turbines, boilers, and other critical equipment; and a mapping of data flows between facilities around the country and the firm's cloud environment. In all, 19,000 stolen files were discovered on the servers. In addition to Calpine Corp., investigators identified data from several other organizations, including Pakistan International Airlines, Mexican oil firm Pemex, and the Israel Institute of Technology.[122]

WATER AND DAMS

In 2015, cybercriminals and hacktivists targeted ICS systems in the water and dams sector. One particularly troubling development was the emergence of postings in Dark Web[vii] forums offering to sell access to unspecified SCADA systems.

Water and electrical utility operator, ransomware attack. On April 25, 2016, the Board of Water & Light (BWL) in Lansing, Michigan, suffered a ransomware attack on its corporate network.[123] BWL immediately shut down the network to isolate the malware, which was delivered via spear-phishing, and reported that "no utility function had been lost," indicating that it was likely successful in preventing the malware from spreading to its operational network and ICS.[124]

U.S. dam, unauthorized access to ICS. Between August 28, 2013, and September 18, 2013, Hamid Firoozi, a hacker that the Federal Bureau of Investigation alleges was working on the behalf of Iran's Revolutionary Guards Corps, repeatedly gained unauthorized, remote access to SCADA systems controlling the Bowman Dam in Rye, New York.[125] After gaining

vi. Additional members of the group may have been operating out of the Netherlands, Canada, and UK.

vii. The Dark Web is the collection of Darknets, which are networks connected to the open Internet that require the use of specific software, configurations, or authorization to access. These networks are often used to host forums used by cybercriminals and online marketplaces for illicit goods.

initial access via the system's cellular modem, Firoozi gathered information on water levels, temperature, and the status of the sluice gate.[126] Ultimately, Faroozi was unable to manipulate the sluice gate or alter water levels and flow rates because the controls were manually disconnected for maintenance.[127] The attack, which was first publicly disclosed in December 2015,[128] was conducted as part of a larger campaign in 2012 and 2013 that primarily targeted major financial institutions across the U.S. with distributed denial-of-service attacks.[129,130]

Attempted sale of SCADA access. In June 2015, an individual using the handle Bonito claimed to be selling remote access to several SCADA systems.[131] To confirm the legitimacy of the offer, the individual included a screenshot of a graphical user interface (GUI) for what appeared to be a SCADA system managing a hydroelectric generator,[132] as well as three IP addresses and virtual network computing passwords. The IP addresses were located in France,[133] though a follow-on post by Bonito referenced the U.S., UK, and Italy.[134] Reporting on the incident assessed that the claims could have been a hoax aimed at defrauding potential buyers,[135] though Bonito had received several endorsements and was described as a "good seller" when joining the carding forum[viii] where the SCADA access post was listed.[136]

TRANSPORTATION

Light-rail operators have been a notable target in 2015. Though no incidents resulting in physical disruptions were disclosed publicly, several attacks have demonstrated threat actor interest in the industry.

Ukraine railway and mining operator, malware attack. The group behind the December 2015 attack on a Ukrainian power plant may have also infiltrated systems at two unnamed Ukrainian companies in railways and mining.[139] In the case of the railway company, this assessment of linked attacks is based upon the choice of targets, the similar deployment of the KillDisk utility, identical malware samples, and overlapping C2 infrastructure. In February 2016, a Department of Energy official publicly blamed the Russian government for these attacks, though the official did not provide evidence for this claim.[140] The attacks were consistent with a likely Russian strategy to disrupt critical industries in Ukraine, given their importance to the Ukrainian economy, to weaken the country as a whole or make the anti-Russian Kiev government appear powerless or ineffective. The type of malware and

2015 Research: Railway Attack via GSM-R Modems Vulnerability

In December 2015, security researchers at the Chaos Communication Congress cybersecurity conference in Zehdenick, Germany, presented on vulnerabilities discovered in the GSM-R modems deployed throughout the European Train Control System.[137] In their presentation, they detailed how disruptions in the connection between the train's modem and the rail network's control center could be used to force trains to stop automatically.[138] Sophisticated attacks against the modems can also be used to issue commands to the automatic train control system, potentially enabling attackers to control the train. This research is of particular concern, given the clear interest in targeting ICS managing rail systems in 2015.

viii. Carding forums are Dark Web forums used to sell stolen data, including credit card, banking, and other personally identifiable information data.

theorized attacker strategy consistently point to the attacker's intent to disrupt railway operations.

South Korea light-rail operator, phishing attack. From January to February 2016, an allegedly North Korea-backed group conducted a spearphishing campaign against two South Korean railway operators, in what the South Korean National Intelligence Service describes as a preparatory phase in targeting the railway traffic control system.[141]

South Korea light-rail operator, unauthorized access to corporate network. According to South Korean media, North Korean hackers compromised an automatic train controller (ATC) company in mid-December 2015. They used the access to establish C2 infrastructure on its servers and steal unspecified data.[142] The ATC company reportedly hosts the central processing unit that regulates speed and safety controls for various South Korean subways, including one for the Seoul metropolitan area. The adversary reportedly used malware that shared code with malware deployed in a July 2014 attack on the Seoul Metro. The 2014 attack was linked to a group with a preference for destructive attacks that disrupt companies' operations. (The 2014 attack and its attribution are further described the section titled Disclosures).

South Korea light-rail operator, data exfiltration. In October 2015, the South Korean National Intelligence Service accused North Korean hackers of compromising Seoul Metro transit servers in July 2014.[143,144] Affected servers were responsible for controlling personal workstations, not the central control system that manages rail traffic, which exists on a separate network. The adversaries exfiltrated 12 documents containing personally identifiable information (PII) related to "human resources and internal management." The intelligence agency attributed the attack to North Korean hackers based upon unspecified tactical similarities to a 2013 attack on six South Korean banks and broadcasters. That attack used time-delayed destructive malware to overwrite the master boot records (MBR) of thousands of computers at targeted institutions, disrupting business operations for up to several weeks. That same threat group is widely attributed to be the perpetrator of the 2014 Sony Pictures Entertainment hack and several other destructive attacks that crippled business operations with MBR malware. Based upon this tactical preference, it is likely that the group had the intent to conduct a similar attack on the metro; the theft of employee PII might have served to facilitate spearphishing individuals with access to the central control systems.

Japan railway operator, data exfiltration. In August 2015, hackers breached the corporate network of Japan Railways Hokkaido attempting to steal railway safety information.[145,146,147,148] Attackers used spearphishing emails to deliver the Emdivi

RAT and then unsuccessfully attempted to exfiltrate documents regarding railway crime prevention, railway communication systems, safety check procedures, security information, and railway safety.[149,150,151,152] The adversary bore technical and tactical similarities to the Blue Termite group. This group of likely Chinese hackers had previously used Emdivi in May 2015 to steal 1.25 million records from the Japan Pension Service.[153] The group's attacks do not suggest intent to disrupt operations, though the information the threat actors were attempting to steal would be valuable in planning future attacks. If the attacker was China, it is likely the object was to acquire business and technical information to improve Chinese railways, given similar objectives in previous cyberespionage campaigns.

Shipping operator, ransomware. In a February 18, 2016, post on Reddit's Malware "subreddit" page, a unspecified shipping company system administrator recounted the difficulties he encountered in restoring a vessel's IT/control system after being infected by the Locky ransomware. The system administrator complained about the difficulties of mitigating a ransomware infection via a satellite link and remote desktop protocol, suggesting that the vessel was at sea when the infection occurred.[154]

APPENDIX B: SUMMARY OF THREAT ACTOR ACTIVITY

NATION STATES

RUSSIA

Russia-backed groups are the most destructive groups conducting cyber attacks against Industrial Control Systems (ICS). Though Russia has targeted U.S. firms, particularly energy providers, Russia's disruptive attacks have been isolated to its western periphery.

Multiple disruptive and destructive attacks have been attributed to allegedly Russia-backed groups. In addition to the December 2015 attacks in Ukraine, Russia has also been linked to at least one destructive ICS attack against an oil pipeline in Turkey in 2008.[155]

Russia has targeted U.S. energy providers. In 2012 and 2013, Russian threat actors sent encrypted commands to U.S. power generators.[156] Beginning as early as 2011,[157] Sand Worm Team[158] has conducted a malware distribution campaign delivering BlackEnergy malware to Human Machine Interface servers of U.S. critical infrastructure operators.[159] The campaign was active as of March 2016, but no attempts to disrupt control processes of U.S. operators had been observed.[160]

Destructive attacks focused in Russia's western periphery. Though Russia has demonstrated that it has likely gained unauthorized access to U.S. ICS operator networks, using this access to interfere with physical processes or destroy equipment has not occurred outside its western periphery.

CHINA

China-backed groups are the most prolific, most active, and likely most successful in establishing persistent access to ICS operator networks in the U.S. They emphasize reconnaissance and intellectual property theft, though reporting on campaigns in previous years indicates their interest in reconnaissance attacks, which were likely in preparation for physical disruptions.

History of complex attacks and campaigns. Operation Clandestine Wolf is the latest in a string of campaigns conducted by Gothic Panda since 2014. Previous operations included Operation Clandestine Fox (April–May 2014), Operation Clandestine Fox 2 (initiated June 2014),[161] Operation Clandestine Fox 3 (initiated July 2014), and Operation Double Tap (initiated November 2014),[162] as well as a separate unnamed campaign using the Pirpi remote access Trojan (initiated October 2014).[163] Other notable incidents include a 2014 attack in which another Chinese group, Comment Crew, penetrated a decoy water control system for a U.S. municipality,[164] as well as a 14-month campaign in 2012 and 2013 in which the People's Liberation Army Unit 61398 targeted 23 natural gas pipeline operators, gaining access to 10.[165]

Wide range of targets. In the last 3 years, Chinese groups have targeted operators in the manufacturing, electricity, water and dams, transportation, and oil and gas industries, among others.

Focus on intellectual property theft. The likely objective of Gothic Panda's Operation Clandestine Wolf was espionage and theft of intellectual property relating to critical industries,[166] which would be consistent with Chinese national policy objectives[167] and previous attack campaigns, including attacks conducted to exfiltrate data from manufacturers of ICS devices.[168]

Focus on reconnaissance and establishing persistent access. Some attacks, including the 2012–2013 campaign against natural gas operators, have been assessed as explicitly conducted to prepare for potential disruptive or destructive attacks in the future.[169]

NORTH KOREA

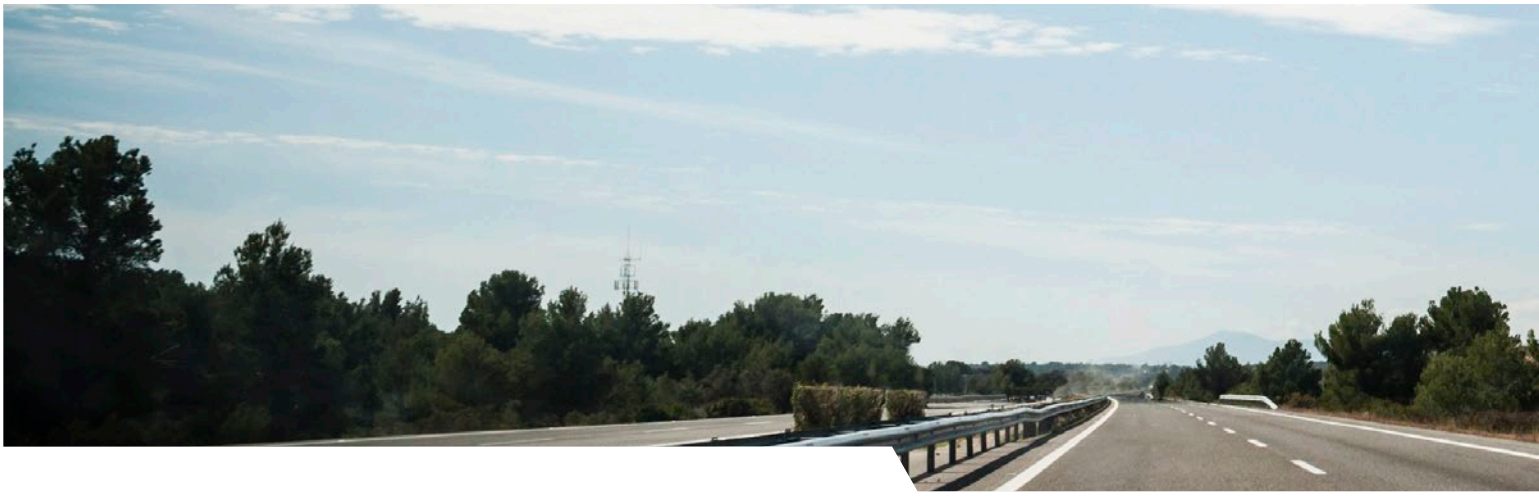
North Korea has adversarial relations with the U.S. and has demonstrated that cyberwarfare is a core foreign policy tactic. Interference with ICS systems is not an established tactic for North Korea, though recent incidents indicate that North Korean groups may be exploring this capability. Of the nation states profiled in this report, North Korea is the least risk averse and most likely to conduct disruptive attacks against U.S. ICS operators.

History of targeting the U.S. No public documentation indicates that North Korea has targeted U.S. ICS operators, though North Korea has conducted several high-profile attacks against U.S. firms, including the 2014 Sony Pictures

Entertainment hack[170,171] and a distributed denial-of-service campaign in July 2009, sometimes called the 7.7 DDoS.[172]

Explicit threat of cyber attack on the U.S. In June 2015, North Korea declared its intent to "wage Korean-style cyber war to hasten the final ruin of the U.S."[173] The threat was in response to disclosures that U.S. intelligence services had attempted to conduct a destructive attack against control systems used in North Korea's nuclear weapons program in 2010.[174]

Demonstrated interest in light-rail operators. No physically disruptive or destructive attacks against ICS systems have been attributed to North Korea, though North Korea threat actors have allegedly penetrated and stolen data from South Korea light-rail operators on multiple occasions in 2014[175] and 2015.[176]



IRAN

Iran has adversarial relations with the U.S. and has targeted U.S. firms, particularly in the financial and telecommunications sectors. Iran has also demonstrated an interest in disrupting core business operations in critical sectors and the ability to gain access to control systems. Iran is likely to continue to back reconnaissance and cyberespionage operations against ICS networks in the U.S., but it is not likely to conduct disruptive or destructive attacks given the minimal benefits and significant economic and military risks of such action.

Demonstrated interest in ICS. Multiple disclosures in 2015 revealed Iran's interest in U.S. water and electricity infrastructure. In 2013, an Iranian-government-sponsored hacker established remote access to the Rye Dam in New York.[177] Also in 2013, unidentified Iranian threat actors began a campaign that breached servers operated by Calpine Corp. and exfiltrated data on ICS network and devices.[178]

CYBERCRIMINALS

Cybercriminals constitute the most organized, well-resourced, and technically sophisticated threat actors, following nation state-backed groups. Cybercriminals are motivated primarily by financial gain, and advanced cybercrime groups operate very similarly to traditional businesses. In advanced groups, various members may conduct discrete tasks in a criminal process, ranging from software and network engineering to selling stolen data. The cybercriminal threat to ICS operators is in an early stage. As more threat actors target ICS and methods for consistently profiting off attacks are established, the cybercriminal threat to these systems is likely to increase.

Lack of proven methods to derive value. Enterprising criminals have long been interested in personal and enterprise computer systems but have traditionally shown little interest in conducting ICS attacks. The reason this threat has yet to materialize and the full resources of advanced criminal organizations have not been directed at ICS operators is likely due to the lack of proven methods for monetizing attacks. The ransomware attack against the Hollywood Presbyterian Medical Center indicates that moral qualms are not likely to deter cybercriminals. In this attack, the inflated ransom received by the

attackers will likely encourage future attacks against industries that rely on time-sensitive processes or uninterrupted availability in their operations.

Shift from other cybercrime. Attacks against ICS operators in 2015 and 2016 indicate that cybercriminals conducting traditional forms of cybercrime are beginning to explore new methods of targeting ICS. The attempted sale of supervisory control and data acquisition (SCADA) access detailed previously and the ransomware attacks against corporate networks were all likely conducted by threat actors with little or no prior interest in ICS. Even groups engaging in traditional organized crime, such as industrial theft, are beginning to incorporate cyber elements into their operations. In April 2016 at the Cloud Expo Europe conference, one of the speakers highlighted an incident in which cybercriminals modified settings in systems regulating temperatures in tanker trucks carrying gasoline. By decreasing the temperature in the tanks, the amount of fuel being transferred can be increased by 2 percent to 3 percent; criminals collected the remaining unaccounted-for fuel after daily deliveries.[179] In an incident disclosed publicly in September 2014, another organized criminal group allegedly stole tons of coal from a Russian mining firm by manipulating the reading of computer systems used to weigh the containers.[180,181]

HACKTIVISTS

Hacktivist groups seek to promote social, political, and ideological causes through cyber attacks. Typically, hacktivists lack the resources and organization of nation state-backed or criminal groups, but they may include highly skilled individual members. Though these groups have demonstrated an interest in targeting ICS to highlight a range of grievances from environmental to political, these groups have historically lacked the resources and technical skills to purposefully interfere with systems managing physical processes.

Historical interest in ICS. Hacktivist groups have demonstrated interest in targeting ICS on several occasions in recent years. In July 2011, the hacktivist group Anonymous announced the initiation of Operation Green Rights Project Tarmaggedon, citing environmental concerns over the Alberta Oil Sands project. Shortly after, an individual associated with the group claimed to have accessed multiple control systems and posted XML and HTML code used to query Siemens SIMATIC software. The code contained administrative commands that could create password dump files from Human Machine Interface (HMI), as well as code used in communications between the server and operational technology (OT) devices such as programmable logic controllers, remote terminal unit intelligent

electronic devices, and industrial controllers.[182] In January 2012, as part of Anonymous' Operation Free Palestine, another hacktivist posted a list of URLs for Web administration interfaces associated with a collection of Israeli SCADA systems.[183] In April 2012, the Syrian Electronic Army[ix] (SEA) allegedly gained access to an Israeli irrigation control system at Kibbutz Sa'ar, near Nahariya; the attackers released a screenshot of the HMI in May 2013 in response to Israeli Air Force bombing in Syria.[184]

Reliance on significant perimeter vulnerabilities. Hacktivists do not typically conduct the long-lasting, persistent campaigns associated with nation state-backed groups but rather rely on significant Web-facing vulnerabilities such as hardcoded credentials. In Operation Free Palestine, the attacker did not actually access systems but simply provided links to interfaces and default credentials.[185]

Lack of familiarity with ICS operation. Though hacktivists may possess the technical skills to gain access to OT networks, instances of these groups using this access to manipulate controls to change physical processes has not been publicly documented. Following Operation Green Rights/Project Tarmaggedon, investigators assessed that, while the individual was familiar with the control application, the posts did not indicate familiarity with ICS operation, design, or components, or even corroborate claims of achieving access.[186] Observed attacks in which threat actors did gain access, such as the alleged SEA penetration of the irrigation control system,[187] or another incident in which a threat actor accessed a Houston water utility,[188] the threat actors simply posted screen grabs of HMI displays. Despite reporting in early 2016 on hacktivists allegedly manipulating chemical levels at a water treatment facility,[189] these claims have not been substantiated.

INSIDERS

Insider threat represents a broad range of potential vulnerabilities for ICS operators. As noted previously, these threats can be categorized principally into negligent or malicious insiders. Employees typically possess extensive knowledge and access on ICS operator networks, both information technology and OT. This access enables these individuals to inflict significant organization harm, whether from accident exposure, intentional sabotage, or direct support of external threats.

Negligent insiders. Negligence on the part of employees constitutes a major threat for ICS operators. With their extensive access, employees can unwittingly grant access to highly sensitive networks. The spear-phishing attacks against the many electricity, water, and transportation sector operators described previously all represent instances of negligent insiders providing

ix. The group later denied involvement in the attack.

inroads onto ICS operator networks. Improper use of compromised media devices, such as USB drives, also poses a threat. This was likely the initial attack vector in the Gundremmingen nuclear power plant incident.

Vendors and partner organizations also increase the attack surface of an organization. Any of the vulnerabilities noted above, if they exist at organizations with access to an ICS operator's networks, represent a threat.

Malicious insiders. Malicious insiders represent employees and other individuals with privileged system access who may intentionally seek to cause organizational harm. The objectives of individuals within this category vary greatly; the most common motivation for malicious threat insiders is financial gain, though ideology; desire for recognition; a sense of loyalty to friends, family, or country; and revenge have also been observed.[190] Malicious employees may also be co-opted by criminal organizations or foreign governments. Between January and September 2014, state-owned Pemex lost 7.5 million barrels of oil, valued at $1.15 billion, via illegal taps in its pipeline infrastructure, which required the complicity or support of company workers familiar with timing and flow rates in the pipelines.[191] A similar arrangement was reported in June 2012, in which subcontractors for an oil producer regularly provided operational details to an

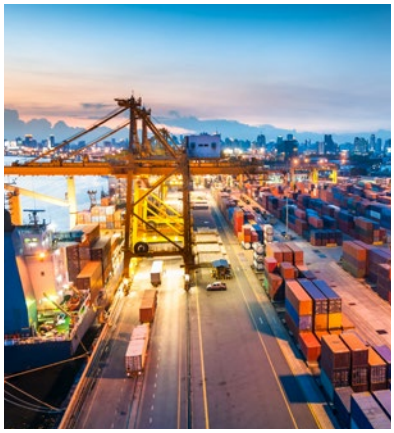
organized crime group operating in Samara Oblast, Russia.[192] In February 2016, a former Nuclear Regulatory Commission employee pled guilty to attempting to damage Department of Energy computer networks by spreading malware. The employee had previously attempted to sell information to a foreign intelligence service to enable a cyber attack on government networks.[193] While this incident occurred at a government agency, this threat could similarly be carried out by employees at an ICS operator.

APPENDIX C: RESEARCH METHODOLOGY

The incident overviews, threat actor analysis, and trend assessments included in this report were developed using publicly available documentation on cyber attacks targeting Industrial Control Systems (ICS) networks. Sources reviewed for this assessment included, but were not limited to, Booz Allen Hamilton proprietary sources, traditional media, published security research, cybersecurity blogs, publications from cybersecurity industry conferences, and published advisories from government agencies. Dark Web, or restricted access forums, known to be used by threat actors were also assessed to identify events and gauge threat actor interests as they relate to ICS systems. The focus of this report is on incidents occurring in 2015, though more recent events were also included.

APPENDIX D: SOURCES

1. *Derek Harp and Bengt Gregory-Brown, "The State of Security in Control Systems Today," SANS Institute, June 2015, accessed May 19, 2016, hxxps://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042.*
2. *"ICS-CERT Incident Response Summary Report 2009–2011," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, 2011, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_S508C.pdf.*
3. *Kyle Wilhoit and Stephen Hilt, "The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems," Trend Micro, August 2015, accessed May 6, 2016, hxxp://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems.pdf.*
4. *"ICS-CERT Monitor November–December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*
5. *"ICS-CERT Monitor September 2014–February 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.*
6. *"ICS-CERT Monitor November-December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*
7. *"ICS-CERT Monitor September 2014–February 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.*
8. *"ICS-CERT Incident Response Summary Report 2009-2011," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, 2011, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011)_S508C.pdf.*
9. *Kyle Wilhoit and Stephen Hilt, "The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems," Trend Micro, August 2015, accessed May 6, 2016, hxxp://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems.pdf.*
10. *"ICS-CERT Monitor October, November December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf*
11. *"ICS-CERT Monitor September 2014–February 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.*
12. *"ICS-CERT Monitor September 2014–February 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.*
13. *"ICS-CERT Monitor November-December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*
14. *"ICS-CERT Monitor November-December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*
15. *"ICS-CERT Monitor November-December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*



16. *"ICS-CERT Monitor September 2014–February 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.*

17. *"ICS-CERT Monitor November–December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*

18. *Catalin Cimpanu, "Researchers Create Self-Propagating Worm That Targets SCADA Equipment," Softpedia, May 9, 2016, accessed May 19, 2016, hxxp://news.softpedia.com/news/researchers-create-self-propagating-worm-that-targets-scada-equipment-503860.shtml.*

19. *Josh Homan, Sean McBride, and Rob Caldwell, "IRONGATE ICS Malware: Nothing to See Here…Masking Malicious Activity on SCADA Systems," FireEye, June 2, 2016, accessed June 7, 2016, hxxps://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html.*

20. *Josh Homan, Sean McBride, and Rob Caldwell, "IRONGATE ICS Malware: Nothing to See Here…Masking Malicious Activity on SCADA Systems," FireEye, June 2, 2016, accessed June 7, 2016, hxxps://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html.*

21. *Josh Homan, Sean McBride, and Rob Caldwell, "IRONGATE ICS Malware: Nothing to See Here…Masking Malicious Activity on SCADA Systems," FireEye, June 2, 2016, accessed June 7, 2016, hxxps://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html.*

22. *"McAfee Labs Threats Report March 2016," IntelSecurity, March 2016, accessed May 19, 2016, hxxp://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf.*

23. *"McAfee Labs Threats Report March 2016," IntelSecurity, March 2016, accessed May 19, 2016, hxxp://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf.*

24. *James Scott and Drew Spaniel, "Combatting the Ransomware Blitzkreig: The Only Defense is Layered Defense, Layer One; Endpoint Security," ICITech, April 2016, accessed May 6, 2016, hxxp://icitech.org/wp-content/uploads/2016/04/ICIT-Brief-Combatting-the-Ransomware-Blitzkrieg2.pdf.*

25. *Thomas Fox-Brewster, "As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin,"* Forbes, *February 18, 2016, accessed May 6, 2016, hxxp://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#28dff55a75b0.*

26. *"Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat," Cyberthreat Alliance, October 2015, accessed May 6, 2016, hxxp://cyberthreatalliance.org/cryptowall-report.pdf.*

27. *Robert M. Lee, "Context for the Claim of a Cyber Attack on the Israeli Electric Grid," SANS Industrial Control Systems Security Blog, January 27, 2016, accessed May 6, 2016, hxxps://ics.sans.org/blog/2016/01/27/context-for-the-claim-of-a-cyber-attack-on-the-israeli-electric-grid.*

28. *"The Nuts & Bolts of Ransomware in 2016," TitanHQ, accessed May 6, 2016, hxxp://www.titanhq.com/the-nuts-bolts-of-ransomware-in-2016.*

29. *Kevin Townsend, "Michigan Power and Water Utility Hit by Ransomware Attack," Security Week, May 3, 2016, accessed May 6, 2016, hxxp://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack.*

30. *Blake Visin, "Protect Your Plant: Cybersecurity 101," Treatment Plant Operator, December 16, 2013, accessed May 6, 2016, hxxp://www.tpomag.com/online_exclusives/2013/12/protect_your_plant_cybersecurity_101.*

31. *James Scott and Drew Spaniel, "Combatting the Ransomware Blitzkreig: The Only Defense is Layered Defense, Layer One; Endpoint Security," ICITech, April 2016, accessed May 6, 2016, hxxp://icitech.org/wp-content/uploads/2016/04/ICIT-Brief-Combatting-the-Ransomware-Blitzkrieg2.pdf.*

32. *Brian Barrett, "Hack Brief: Hackers Are Holding an LA Hospital's Computers Hostage,"* Wired, *February 16, 2016, accessed May 6, 2016, hxxps://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage.*

33. *Kevin Townsend, "Michigan Power and Water Utility Hit by Ransomware Attack," Security Week, May 3, 2016, accessed May 6, 2016, hxxp://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack.*

34. *Uzair Amir, "Israel's Power Authority Network Hit with Ransomware," HackRead, January 27, 2016, accessed May 6, 2016, hxxps://www.hackread.com/israels-power-authority-network-hit-with-ransomware.*

35. *"The Nuts & Bolts of Ransomware in 2016," TitanHQ, accessed May 6, 2016, hxxp://www.titanhq.com/the-nuts-bolts-of-ransomware-in-2016.*

36. *Catalin Cimpanu, "Researchers Create Self-Propagating Worm That Targets SCADA Equipment," Softpedia, May 9, 2016, accessed May 19, 2016, hxxp://news.softpedia.com/news/researchers-create-self-propagating-worm-that-targets-scada-equipment-503860.shtml.*

37. *Bonito, "SCADA | systems," Omerta, June 12, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1586/4818034?pageno=0&perpage=10&post_order_asc=1.*

38. *Kaspersky Lab, "2016 Predictions: It's The End Of The World For APTs As We Know Them," Kaspersky Lab, accessed November 18, 2015, hxxps://securelist.com/files/2015/11/KSB_2016_Predictions_FINAL.pdf.*

39. *"The Enemies of Internet," Reporters without Borders, accessed November 23, 2015, hxxp://surveillance.rsf.org/en/hacking-team.*

40. *Andy Greenberg, "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees),"* Forbes, *March 21, 2012, accessed December 4, 2015, hxxp://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pcand-get-paid-six-figure-fees.*

41. *"GLEG Agora SCADA+ Exploit Pack," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated October 23, 2014, accessed May 26, 2016, hxxps://ics-cert.us-cert.gov/advisories/ICSA-11-096-01.*

42. *ReVuln, "ReVuln - SCADA 0-day vulnerabilities," Vimeo, November 18, 2012, accessed May 26, 2016, https://vimeo.com/53806381.*

43. *Jeff St. John, "Maltese Cybersecurity Group Claims SCADA System Hacks," Green Tech Media, November 26, 2016, accessed May 26, 2016, http://www.greentechmedia.com/articles/read/Maltese-Cybersecurity-Group-Claims-SCADA-System-Hacks.*

44. *Jeff St. John, "Maltese Cybersecurity Group Claims SCADA System Hacks," Green Tech Media, November 26, 2016, accessed May 26, 2016, http://www.greentechmedia.com/articles/read/Maltese-Cybersecurity-Group-Claims-SCADA-System-Hacks.*

45. *Andy Greenberg, "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees),"* Forbes, *March 21, 2012, accessed December 4, 2015, hxxp://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pcand-get-paid-six-figure-fees.*

46. *Bonito, "SCADA | systems," Omerta, June 12, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1586/4818034?pageno=0&perpage=10&post_order_asc=1.*

47. *Bonito, "usa | citizen," Omerta, August 9, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1586/5379452.*

48. *Bonito, "Healtcare | usa," Omerta, August 7, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1586/5372738.*

49. *Bonito, "SCADA | systems," Omerta, June 12, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1586/4818034?pageno=0&perpage=10&post_order_asc=1*

50. *"A-0020-NCCIC/ICS-CERT –120020110916 ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, accessed May 6, 2016, hxxps://info.publicintelligence.net/NCCIC-AnonymousICS.pdf.*

51. *Dan Bloom, "ISIS trying to launch deadly cyber-attack on airports, hospitals and National Grid warns George Osborne," Mirror, November 17, 2015, accessed May 6, 2016, hxxp://www.mirror.co.uk/news/uk-news/isis-trying-launch-deadly-cyber-6845517.*

52. *Turanchocks_, "Censys - новый поисковый движок для хакеров," AntiChat, December 13, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/963/2428559.*

53. *TheWhiteHatter, "Censys - Search engine that lists every internet connected device," Hackforums.net, December 11, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1093/3298283.*

54. *Silviu, "Hacker-Friendly Search Engine that Lists Every Internet-Connected Device," RST Forums, December 11, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1060/5610597.*

55. *rkellyslovechild69, "PenTesting - Passive Recon/Discovery," Hackforums.net, February 4, 2016, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1093/4055723.*

56. *"Хочу написать что нибудь , ваши предложения!" Free Hacks, August 29, 2015, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1073/5567933.*

57. *Brian Bergstein, "Zakir Durumeric, 26: A computer scientist sees a way to improve online Security," MIT Technology Review, 2015, accessed May 6, 2016, hxxps://www.technologyreview.com/lists/innovators-under-35/2015/visionary/zakir-durumeric.*

58. *John Snow, "Shodan and Censys: the ominous guides through the Internet of Things," Kaspersky Lab, February 29, 2016, accessed May 6, 2016, hxxps://blog.kaspersky.com/shodan-censys/11430.*

59. *dlebookme "Learn 5 PLC's in a Day-AB, Siemens, Schneider, Omron & Delta," Hack Turk, January 10, 2016, accessed May 19, 2016, hxxps://aggregint.com/thread/hacker/1372/5628196.*

60. *"NFI Automation: About Us," NFI Automation, 2016, accessed May 6, 2016, hxxp://nfiautomation.org/about-us.*

61. *Mike, "ADA just sent me a surprise," DSLReports, April 22, 2016, accessed May 23, 2016, hxxp://www.dslreports.com/forum/r30717075-ADA-just-sent-me-a-surprise.*

62. *Mike, "ADA just sent me a surprise," DSLReports, April 22, 2016, accessed May 23, 2016, hxxp://www.dslreports.com/forum/r30717075-ADA-just-sent-me-a-surprise.*

63. *Brian Krebs, "Dental Assn Mails Malware to Members," Krebs On Security, April 28, 2016, accessed May 23, 2016, hxxp://krebsonsecurity.com/2016/04/dental-assn-mails-malware-to-members/.*

64. *Brian Krebs, "Dental Assn Mails Malware to Members," Krebs On Security, April 28, 2016, accessed May 23, 2016, hxxp://krebsonsecurity.com/2016/04/dental-assn-mails-malware-to-members/.*

65. *Brian Krebs, "Dental Assn Mails Malware to Members," Krebs On Security, April 28, 2016, accessed May 23, 2016, hxxp://krebsonsecurity.com/2016/04/dental-assn-mails-malware-to-members/.*

66. *"The Anatomy of the Attack: Zombie Zero," TrapX Security, November 7, 2016, accessed May 23, 2016, hxxp://deceive.trapx.com/rs/trapxcompany/images/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf?alild=1104745.*

67. *"The Anatomy of the Attack: Zombie Zero," TrapX Security, November 7, 2016, accessed May 23, 2016, hxxp://deceive.trapx.com/rs/trapxcompany/images/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf?alild=1104745.*

68. *"Dragonfly: Western Energy Companies Under Sabotage Threat" Symantec, June 30, 2014, accessed May 23, 2016, hxxp://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat.*

69. *"The Anatomy of the Attack: Zombie Zero," TrapX Security, November 7, 2016, accessed May 23, 2016, hxxp://deceive.trapx.com/rs/trapxcompany/images/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf?alild=1104745.*

70. *Swati Khandelwal, "HardCoded Backdoor Found in China-made Netis, Netcore Routers," The Hacker News, August 27, 2014, accessed May 23, 2016, hxxp://thehackernews.com/2014/08/hardcoded-backdoor-found-in-china-made_27.html.*

71. *Emily Protalinski, "Former Pentagon analyst: China has backdoors to 80% of telecoms," ZDNet, July 14, 2012, accessed May 23, 2016, hxxp://www.zdnet.com/article/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms/.*

72. *"Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec, June 30, 2014, accessed May 23, 2016, hxxp://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat.*

73. *"The Anatomy of the Attack: Zombie Zero," TrapX Security, November 7, 2016, accessed May 23, 2016, hxxp://deceive.trapx.com/rs/trapxcompany/images/AOA_Report_TrapX_AnatomyOfAttack-ZombieZero.pdf?alild=1104745.*

74. *Derek Harp and Bengt Gregory-Brown, "SANS Institute InfoSec Reading Room: The State of Security in Control Systems Today," SANS Institute, June, 2015, accessed May 6, 2016, hxxps://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042.*

75. *John Zorabedian, "Electric utility hit by ransomware shuts down IT systems for a week," Naked Security, May 4, 2016, accessed May 19, 2016, hxxps://nakedsecurity.sophos.com/2016/05/04/electric-utility-hit-by-ransomware-shuts-down-it-systems-for-a-week/.*

76. *Robertmlee, "Context for the Claim of a Cyber Attack on the Israeli Electric Grid," SANS Industrial Control Systems Security Blog, January 27, 2016, accessed May 6, 2016, hxxps://ics.sans.org/blog/2016/01/27/context-for-the-claim-of-a-cyber-attack-on-the-israeli-electric-grid. Robert M. Lee*

77. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

78. *Scadastrangelove "SCADAPASS," Github, April 21, 2016, accessed May 19, 2016, hxxps://github.com/scadastrangelove/*

79. *SCADAPASS/blob/master/scadapass.csv.*

80. *"ICS-CERT Monitor November-December 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, January 13, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*

81. *Michael Mimoso, "Emergency Adobe Flash Patch fixes zero day under attack," Threat Post, June 23, 2015, accessed May 6, 2016, hxxps://threatpost.com/emergency-adobe-flash-patch-fixes-zero-day-under-attack/113434/.*

82. *"Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," Reddit.com/r/netsec, June 2015, accessed May 6, 2016, hxxps://www.reddit.com/r/netsec/comments/3aujx5/operation_clandestine_wolf_adobe_flash_zeroday_in/.*

83. *"Global Threat Intel Report," CrowdStrike, last update February 10, 2015, accessed February 13, 2015, hxxp://go.crowdstrike.com/rs/crowdstrike/images/GlobalThreatIntelReport.pdf.*

84. *"Threat Expert Report: Backdoor.Trojan," ThreatExpert, last updated October 4, 2008, accessed February 26, 2015, hxxp://www.threatexpert.com/report.aspx?md5=6ab8eb00580c08dd6457bfa84aa9a109.*

85. *"Global Threat Intel Report," CrowdStrike, last update February 10, 2015, accessed February 13, 2015, hxxp://go.crowdstrike.com/rs/crowdstrike/images/GlobalThreatIntelReport.pdf.*

86. *Robert Falcone and Richard Wartell, "UPS: Observations on CVE-2015-3113, Prior Zero-Days and the Pirpi Payload," Palo Alto Networks, last updated July 27, 2015, accessed May 26, 2015, hxxp://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload.*

87. *Ned Moran, Joshua Homan, Mike Oppenheim, and Mike Scott, "Operation Double Tap" FireEye, last updated November 21, 2014, accessed February 19, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html.*

88. *Florian Roth, "APT Groups and Operations," Google Sheets, accessed May 26, 2015, hxxps://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml.*

89. *"Threat Group-0110 targets manufacturing and financial organizations via phishing," Dell SecureWorks, July 25, 2014, accessed February 12, 2015, hxxp://www.secureworks.com/resources/blog/threat-group-0110-targets-manufacturing-and-financial-organizations-via-phishing.*

90. *Erica Eng and Dan Caselden, "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," FireEye, June 23, 2015, accessed May 6, 2016, hxxps://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.*

91. *Erica Eng and Dan Caselden, "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," FireEye, June 23, 2015, accessed May 6, 2016, hxxps://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.*

92. *Erica Eng and Dan Caselden, "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," FireEye, June 23, 2015, accessed May 6, 2016, hxxps://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.*

93. *Mike Scott, "Clandestine Fox, Part Deux," FireEye, last updated June 10, 2012, accessed February 18, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html.*

94. *Robert M. Lee "ICS-CERT Monitor July–August 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, September 4, 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2015.pdf.*

95. *Mike Scott, "Clandestine Fox, Part Deux," FireEye, last updated June 10, 2012, accessed February 18, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html.*

96. *"ICS-CERT Monitor July- August 2015," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, September 4, 2015, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2015.pdf.*

97. *Erica Eng and Dan Caselden, "Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign," FireEye, June 23, 2015, accessed May 6, 2016, hxxps://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.*

98. *Tyler Durden, "Computer Virus Discovered German Nuclear Power Plant," Zero Hedge, April 25, 2016, accessed April 25, 2016, hxxp://www.zerohedge.com/news/2016-04-25/computer-virus-discovered-german-nuclear-power-plant.*

99. *"Detektion von Büro-Schadsoftware an mehreren Rechnern," KGG, April 25, 2016, accessed April 25, 2016, hxxp://www.kkw-gundremmingen.de/presse.php%3Fid%3D571&usg=ALkJrhjEviYtXLjxFYR1wsybb_zmzwQ8PA.*

100. *Christoph Steitz and Eric Auchard, "German nuclear plant infected with computer viruses, operator says," Reuters, April 27, 2016, accessed April 30, 2016, hxxp://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS.*

101. *Christoph Steitz and Eric Auchard, "German nuclear plant infected with computer viruses, operator says," Reuters, April 27, 2016, accessed April 30, 2016, hxxp://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS.*

102. *Jenny Schack, "Wohl kein gezielter IT-Angriff," BR.de, April 25, 2016, accessed April 25, 2016, hxxp://www.br.de/nachrichten/schwaben/inhalt/kkw-gundremmingen-schadsoftware-akw-100.html.*

103. *Christoph Steitz and Eric Auchard, "German nuclear plant infected with computer viruses, operator says," Reuters, April 27, 2016, accessed April 30, 2016, hxxp://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS.*

104. *Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed May 20, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

105. *Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed May 20, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

106. *SANS-ICS and Electricity-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," North American Electric Reliability Corporation, March 18, 2016, accessed May 23, 2016, hxxp://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.*

107. *Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed May 20, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

108. *Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed May 20, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

109. *"Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, February 26, 2016, accessed April 1, 2016, hxxps://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.*

110. *Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed May 20, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

111. *Uzair Amir, "Israel's Power Authority Network Hit with Ransomware," HackRead, January 27, 2016, accessed May 6, 2016, hxxps://www.hackread.com/israels-power-authority-network-hit-with-ransomware/.*

112. *Robert M. Lee, "Context for the Claim of a Cyber Attack on the Israeli Electric Grid," SANS Industrial Control Systems Security Blog, January 27, 2016, accessed May 6, 2016, hxxps://ics.sans.org/blog/2016/01/27/context-for-the-claim-of-a-cyber-attack-on-the-israeli-electric-grid.*

113. *Darlen Storm, "No, Israel's power grid wasn't hacked, but ransomware hit Israel's Electric Authority," Computer World, January 27, 2016, accessed May 6, 2016, hxxp://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html.*

114. *Uzair Amir, "Israel's Power Authority Network Hit with Ransomware," HackRead, January 27, 2016, accessed May 6, 2016, hxxps://www.hackread.com/israels-power-authority-network-hit-with-ransomware/.*

115. *Darlen Storm, "No, Israel's power grid wasn't hacked, but ransomware hit Israel's Electric Authority," Computer World, January 27, 2016, accessed May 6, 2016, hxxp://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html.*

116. *"The Nuts & Bolts of Ransomware in 2016," TitanHQ, accessed May 6, 2016, hxxp://www.titanhq.com/the-nuts-bolts-of-ransomware-in-2016.*

117. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

118. *Ruchna Nigam, "SCADA Security Report 2016," Fortinet, April 5, 2016, accessed May 6, 2016, hxxp://blog.fortinet.com/post/scada-security-report-2016.*

119. *Ruchna Nigam, "SCADA Security Report 2016," Fortinet, April 5, 2016, accessed May 6, 2016, hxxp://blog.fortinet.com/post/scada-security-report-2016.*

120. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

121. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

122. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

123. *Kevin Townsend, "Michigan Power and Water Utility Hit by Ransomware Attack," Security Week, May 3, 2016, accessed May 6, 2016, hxxp://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack.*

124. *Kevin Townsend, "Michigan Power and Water Utility Hit by Ransomware Attack," Security Week, May 3, 2016, accessed May 6, 2016, hxxp://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack.*

125. *"United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Amazdegan, Omid Ghafarinia, Sina Keissar, Nader Saedi," U.S. Department of Justice, last updated March 2016, accessed May 6, 2016, hxxps://www.justice.gov/usao-sdny/file/835061/download.*

126. *Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case,"* New York Times, *last updated March 25, 2016, accessed May 6, 2016, hxxp://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.*

127. *United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Amazdegan, Omid Ghafarinia, Sina Keissar, Nader Saedi," U.S. Department of Justice, last updated March 2016, accessed May 6, 2016, hxxps://www.justice.gov/usao-sdny/file/835061/download.*

128. *Danny Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," Wall Street Journal, last updated December 20, 2015, accessed May 18, 2016, hxxp://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559.*

129. *Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case,"* New York Times, *last updated March 25, 2016, accessed May 6, 2016, hxxp://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.*

130. *"International Cyber Crime Iranians Charged with Hacking U.S. Financial Sector," U.S. Federal Bureau of Investigation, last updated March 24, 2016, accessed May 6, 2016, hxxps://www.fbi.gov/news/stories/2016/march/iranians-charged-with-hacking-us-financial-sector.*

131. *Bonito, "SCADA | systems," Omerta, last updated June 12, 2015, accessed May 20, 2016, hxxps://aggregint.com/thread/hacker/1586/4818034?pageno=0&perpage=10&post_order_asc=1.*

132. *Image file, Imgur, accessed May 20, 2016, hxxp://i.imgur.com/bRxtZSM.png.*

133. *Idan Aharoni, "SCADA Systems Offered for Sale in the Underground Economy," infosecland, last updated June 22, 2015, accessed May 6, 2016, hxxp://www.infosecisland.com/blogview/24608-SCADA-Systems-Offered-for-Sale-in-the-Underground-Economy.html.*

134. *Bonito, "SCADA | systems," Omerta, last updated June 12, 2015, accessed May 20, 2016, hxxps://aggregint.com/thread/hacker/1586/4818034?pageno=0&perpage=10&post_order_asc=1.*

135. *Idan Aharoni, "SCADA Systems Offered for Sale in the Underground Economy," infosecisland, last updated June 22, 2015, accessed May 6, 2016, hxxp://www.infosecisland.com/blogview/24608-SCADA-Systems-Offered-for-Sale-in-the-Underground-Economy.html.*

136. *"Hola," Omerta, last updated May 31, 2015, accessed May 20, 2016, hxxps://aggregint.com/thread/hacker/1586/3628376?pageno=0&perpage=10&post_order_asc=1.*

137. *Sergey Gordeychik, Aleksandr Timorin and repdet, "The Great Train Cyber Robbery," Chaos Computer Club, last updated December 27, 2015, accessed May 20, 2016, hxxps://media.ccc.de/v/32c3-7490-the_great_train_cyber_robbery.*

138. *Darren Pauli, "Irked train hackers talk derailment flaws, drop SCADA password list," The Register, last updated January 4, 2016, accessed May 20, 2016, hxxp://www.theregister.co.uk/2016/01/04/irked_train_hackers_talk_derailment_flaws_drop_scada_password_list.*

139. *Kyle Wilhoit, "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," Trend Micro, last updated February 11, 2016, accessed February 12, 2016, hxxp://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.*

140. *Evan Perez, "U.S. official blames Russia for power grid attack in Ukraine," CNN, last updated February 11, 2016, accessed February 12, 2016, hxxp://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/.*

141. *"철도운영기관 노린 북한 해킹 공격, 피해 및 대응현황은?," Boannews, last updated March 8, 2016, accessed May 20, 2016, hxxp://www.boannews.com/media/view.asp?idx=49869&skind=0.*

142. 김경애, *"삼성전자-청와대 사칭-자동열타제어장치 업체까지 북한소행," 보안뉴스, last updated January 27, 2016, accessed January 28, 2016, hxxp://www.boannews.com/media/view.asp?idx=49391&page=1&kind=1*

143. *Choejongseok Reporter, "北, 서울메트로 서버 5개월 장악했다," Chosun, last updated October 5, 2015, accessed October 5, 2015, hxxp://news.chosun.com/site/data/html_dir/2015/10/05/2015100500286.html.*

144. *Lee Hyun-Jeong, "Seoul Subway Server Allegedly Hacked by N.K.,"* Korea Herald, *October 5, 2015, accessed October 5, 2015, hxxp://www.koreaherald.com/view.php?ud=20151005001125.*

145. *"標的型メールに関する一部報道機関による報道について," JR Hokkaido, last updated February 8, 2016, accessed February 8, 2016, hxxp://www.jrhokkaido.co.jp/press/2016/160208-1.pdf.*

146. *"JR北海道 サイバー攻撃受け鉄道安全情報など流出か," NHK, last updated February 8, 2016, accessed February 8, 2016, hxxp://www3.nhk.or.jp/news/html/20160208/k10010401831000.html*

147. *"Cyberattacks target JR Hokkaido; security info may have lleaked,"* Japan Times, *February 8, 2016, hxxp://www.japantimes.co.jp/news/2016/02/08/national/crime-legal/cyberattacks-target-jr-hokkaido-security-info-may-leaked/*

148. *"平成 27 年 8 月 28 日. 標的型メールの攻撃を受けたことについて," JR Hokkaido, last modified August 28, 2015, accessed February 8, 2016, hxxp://www.jrhokkaido.co.jp/press/2015/150828-1.pdf.*

149. *"標的型メールに関する一部報道機関による報道について," JR Hokkaido, last updated February 8, 2016, accessed February 8, 2016, hxxp://www.jrhokkaido.co.jp/press/2016/160208-1.pdf.*

150. *"JR北海道 サイバー攻撃受け鉄道安全情報など流出か," NHK, last updated February 8, 2016, accessed 8 February 2016, hxxp://www3.nhk.or.jp/news/html/20160208/k10010401831000.html.*

151. *"Cyberattacks target JR Hokkaido; security info may have leaked,"* Japan Times, *February 8, 2016 hxxp://www.japantimes.co.jp/news/2016/02/08/national/crime-legal/cyberattacks-target-jr-hokkaido-security-info-may-leaked/*

152. *"平成 27 年 8 月 28 日. 標的型メールの攻撃を受けたことについて," JR Hokkaido, last modified August 28, 2015, accessed February 8, 2016, hxxp://www.jrhokkaido.co.jp/press/2015/150828-1.pdf.*

153. *Kaspersky Lab, "Blue Termite: A Sophisticated Cyber Espionage Campaign is After High-Profile Japanese Targets," Kaspersky Lab, last updated August 20, 2015, accessed February 8, 2015, hxxp://www.kaspersky.com/about/news/virus/2015/Blue-Termite-A-Sophisticated-Cyber-Espionage-Campaign-is-After-High-Profile-Japanese-Targets.*

154. *"Any info on *.locky ransomware," Reddit, last updated February 18, 2016, accessed February 20, 2016, hxxps://www.reddit.com/r/Malware/comments/45xkn9/any_info_on_locky_ransomware/*

155. *Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, last updated December 10, 2014, accessed May 6, 2016, hxxp://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.*

156. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, last updated December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

157. *"Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated March 2, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B#footnotec_s1cyw55.*

158. *Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," iSightPartners, last updated October 14, 2014, accessed May 6, 2016, hxxp://www.isightpartners.com/2014/10/cve-2014-4114/.*

159. *"Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated March 2, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.*

160. *"Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated March 2, 2016, accessed May 6, 2016, hxxps://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.*

161. *Mike Scott, "Clandestine Fox, Part Deux," FireEye, last updated June 10, 2012, accessed February 18, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html.*

162. *Ned Moran, Joshua Homan, Mike Oppenheim, and Mike Scott, "Operation Double Tap," FireEye, last updated November 21, 2014, accessed February 19, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html.*

163. *Ned Moran, Joshua Homan, Mike Oppenheim, and Mike Scott, "Operation Double Tap," FireEye, last updated November 21, 2014, accessed February 19, 2015, hxxps://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html.*

164. *Tom Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," MIT Technology Review, last updated August 2, 2013, accessed May 6, 2016, hxxps://www.technologyreview.com/s/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/.*

165. *Michael Riley and Jordan Robertson, "UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat," Bloomberg, last updated June 13, 2014, accessed May 6, 2016, hxxp://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat.*

166. *Michael Mimoso, "Emergency Adobe Flash Patch fixes zero day under attack," Threat Post, last updated June 23, 2015, accessed May 6, 2016, hxxps://threatpost.com/emergency-adobe-flash-patch-fixes-zero-day-under-attack/113434/.*

167. *Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—And Must Be Challenged,"* Wall Street Journal*, last updated January 27, 2012, accessed May 6, 2016, hxxp://www.wsj.com/articles/SB10001424052970203718504577178832338032176.*

168. *Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," Krebs on Security, last updated September 26, 2012, accessed May 6, 2016, hxxp://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/.*

169. *Michael Riley and Jordan Robertson, "UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat," Bloomberg, last updated June 13, 2014, accessed May 6, 2016, hxxp://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat.*

170. *Nathaniel Beach-Westmorland, "If North Korea Did Hack Sony, It's a Whole New Kind of Cyberterrorism," Wired, last updated December 23, 2014, accessed May 6, 2016, hxxp://www.wired.com/2014/12/why-america-must-answer-north-korea/.*

171. *Oliver Laughlin, "FBI director stands by claim that North Korea was source of Sony cyber-attack,"* The Guardian*, last updated January 7, 2015, accessed May 6, 2016, hxxp://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey.*

172. *"Ten Days of Rain Expert analysis of distributed denial-of-service attacks targeting South Korea," McAfee, last updated 2011, accessed May 6, 2016, hxxp://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf.*

173. *Martyn Williams, "North Korea threatens cyber attacks on US," PCWorld, last updated June 9, 2015, accessed May 6, 2016, hxxp://www.pcworld.com/article/2933672/north-korea-threatens-cyber-attacks-on-us.html.*

174. *Martyn Williams, "North Korea threatens cyber attacks on US," PCWorld, last updated June 9, 2015, accessed May 6, 2016, hxxp://www.pcworld.com/article/2933672/north-korea-threatens-cyber-attacks-on-us.html.*

175. *김경애, "삼성전자-청와대 사칭-자동열타제어장치 업체까지 북한소행," 보안뉴스, last updated January 27, 2016, accessed January 28, 2016, hxxp://www.boannews.com/media/view.asp?idx=49391&page=1&kind=1*

176. *Lee Hyun-Jeong, "Seoul Subway Server Allegedly Hacked by N.K.,"* Korea Herald*, last updated October 5, 2015, accessed October 5, 2015, hxxp://www.koreaherald.com/view.php?ud=20151005001125*

177. *"United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Amazdegan, Omid Ghafarinia, Sina Keissar, Nader Saedi," U.S. Department of Justice, last updated March 2016, accessed May 6, 2016, hxxps://www.justice.gov/usao-sdny/file/835061/download.*

178. *Garance Burke and Jonothan Fahey, "Investigation: US power grid vulnerable to foreign hacks," Phys.org, last updated December 21, 2015, accessed May 6, 2016, hxxp://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html.*

179. *Steve Ranger, "Hackers help to steal petrol, coal and more as criminals eye industrial systems," ZDNet, last updated April 13, 2016, accessed May 6, 2016, hxxp://www.zdnet.com/article/hackers-help-to-steal-petrol-coal-and-more-as-criminals-eye-industrial-systems/.*

180. *Sophie Curtis, "Eugene Kaspersky: traditional crime 'is coming to cyberspace'," Telegraph, last updated September 30, 2014, accessed May 6, 2016, hxxp://www.telegraph.co.uk/technology/internet-security/11118866/Eugene-Kaspersky-traditional-crime-is-coming-to-cyberspace.html.*

181. *Steve Ranger, "Hackers help to steal petrol, coal and more as criminals eye industrial systems," ZDNet, last updated April 13, 2016, accessed May 6, 2016, hxxp://www.zdnet.com/article/hackers-help-to-steal-petrol-coal-and-more-as-criminals-eye-industrial-systems/.*

182. *"A-0020-NCCIC/ICS-CERT –120020110916 Assessment of Anonymous Threat to Control Systems," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated October 2011, accessed May 20, 2016, hxxp://www.wired.com/images_blogs/threatlevel/2011/10/NCCIC-AnonymousICS.pdf.*

183. *Lucian Constantin, "Anonymous Publishes Israeli SCADA Log-in Details," PCWorld, last updated January 12, 2012, accessed May 20, 2016, hxxp://www.pcworld.com/article/248010/anonymous_publishes_israeli_scada_login_details.html.*

184. *Gilad Zahavi, "Cyber Threats to Oil and Gas Industry," SenseCy, last updated January 30, 2014, accessed May 20, 2016, hxxps://blog.sensecy.com/tag/scada/.*

185. *Lucian Constantin, "Anonymous Publishes Israeli SCADA Log-in Details," PCWorld, January 12, 2012, accessed May 20, 2016, hxxp://www.pcworld.com/article/248010/anonymous_publishes_israeli_scada_login_details.html.*

186. *"A-0020-NCCIC/ICS-CERT –120020110916 Assessment of Anonymous Threat to Control Systems," U.S. Department of Homeland Security Industrial Control System-Computer Emergency Response Team, last updated October 2011, accessed May 20, 2016, hxxp://www.wired.com/images_blogs/threatlevel/2011/10/NCCIC-AnonymousICS.pdf.*

187. *Gilad Zahavi, "Cyber Threats to Oil and Gas Industry," SenseCy, last updated January 30, 2014, accessed May 20, 2016, hxxps://blog.sensecy.com/tag/scada/.*

188. *Eric Byres, "SCADA Security Breached at U.S. Water Utilities," Tofino Security, last updated November 21, 2011, accessed May 20, 2016, hxxps://www.tofinosecurity.com/blog/scada-security-breached-us-water-utilities.*

189. *"Data Breach Digest," Verizon, last updated March 2016, accessed May 6, 2016, hxxp://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf.*

190. *Ayhan Gucuyener, "Human Factor in Critical Infrastructure Security: The Insider Threat," Hazar Strategi Enstitusu, last updated July 29, 2015, accessed May 20, 2016, hxxp://www.hazar.org/blogdetail/blog/human_factor_in_critical_infrastructure_security_the_insider_threat_1331.aspx.*

191. *Mark Stevenson, "Drug Cartels Are Stealing Billions Worth Of Oil From Mexican Pipelines," Business Insider, last modified September 25, 2014, accessed September 14, 2015, hxxp://www.businessinsider.com/drug-cartels-are-stealing-billions-worth-of-oil-from-mexican-pipelines-2014-9.*

192. *Richard Behar, "Hess Oil's Russian Mob Problem," Forbes, last modified June 6, 2012, accessed September 11, 2015, hxxp://www.forbes.com/forbes/2012/0625/feature-moscow-bochkarev-hess-oil-russian-mob-problem.html.*

193. *"Former U.S. Nuclear Regulatory Commission Employee Pleads Guilty to Attempted Spear-Phishing Cyber-Attack on Department of Energy Computers," U.S. Department of Justice, February 2, 2016, accessed May 20, 2016, hxxps://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear-phishing-cyber.*

About Booz Allen

Booz Allen Hamilton (NYSE: BAH) has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading *Fortune* 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs about 22,600 people globally, and had revenue of $5.41 billion for the 12 months ended March 31, 2016. To learn more, visit www.boozallen.com.

For More Information

ANGIE MESSER
Executive Vice President
messer_angela@bah.com
+1-703-902-5666

BRAD MEDAIRY
Senior Vice President
medairy_brad@bah.com
+1-703-902-5948

SCOTT STABLES
Industrial Security Director
stables_scott@bah.com
+1-630-776-7701

Authors

JAKE STYCZYNSKI
Lead Author

NATE BEACH-WESTMORELAND
Author