INL/CON-18-44411-Revision-2

History of Industrial Control System Cyber Incidents

Kevin E. Hemsley, Dr. Ronald E. Fisher

December 2018

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/CON-18-44411-Revision-2

History of Industrial Control System Cyber Incidents

Kevin E. Hemsley, Dr. Ronald E. Fisher

December 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Chapter 1

HISTORY OF CYBER INCIDENTS AND THREATS TO INDUSTRIAL CONTROL SYSTEMS

KEVIN HEMSLEY, CISSP, and DR. RONALD E. FISHER
National and Homeland Security, Idaho National Laboratory,
P.O. Box 1625, MS 3650, Idaho Falls, ID 83415, USA
Email: kevin.hemsley@inl.gov / Email: ron.fisher@inl.gov

Abstract For many years, malicious cyber-actors have been targeting the industrial control systems (ICSs) that manage our critical infrastructures. Most of these events are not reported to the public, and the threats and incidents to ICSs are not as well-known as enterprise cyber-threats and incidents. This paper is a brief study of publically reported cyber-threats to critical infrastructure, which sheds light on the growing cyber-threats to ICS devices. It is important to note this list is not all inclusive. The events selected in this study highlight the significant threats and incidents to ICSs, and demonstrate that significant cyber-incidents to ICS devices are growing and becoming more complex.

Keywords: industrial control systems (ICSs), cybersecurity, threats, history

1. Introduction

Industrial control systems (ICSs) are embedded cyber-devices that operate critical infrastructures (e.g., energy, transportation, water). ICS devices are lesser known and are typically unique to the operational technology (OT) framework of cyber, which differs from enterprise information technology (IT). This paper documents some of the more significant ICS threats, vulnerabilities, and incidents in helping to demonstrate the increase and complexity of ICS attacks.

Cyber-threats in ICSs manifest themselves in different ways. In this paper, we examine the different ICS threat types, which include directed attacks, cyber-intrusion campaigns, malware, and cyber-threat groups.

Table 1. ICS cyber-incident timeline.

Year	Type	Name	Description
1903	Attack	Marconi Wireless Hack	Marconi's wireless telegraph presentation hacked with Morse code.
2000	Attack	Maroochy Water	A cyber-attack caused the release of more than 265,000 gallons of untreated sewage.
2008	Attack	Turkey Pipeline Explosion (not quite cyber)	Did attackers use a security camera's vulnerable software to gain entrance into a pipeline's control network?
2010	Malware	Stuxnet	The world's first publically known digital weapon.
2010	Malware	Night Dragon	Attackers used sophisticated malware to target global oil, energy, and petrochemical companies.
2011	Malware	Duqu/ Flame/Gauss	Advanced and complex malware used to target specific organizations, including ICS manufacturers.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identified an active series of cyber-intrusions targeting the natural gas pipeline sector.
2012	Malware	Shamoon	Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.
2013	Attack	Target Stores	Hackers initially gained access to Target's sensitive financial systems through a third-party that maintained its HVAC ICSs, costing Target $309M.
2013	Attack	New York Dam	The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY.
2013	Malware	Havex	An ICS-focused malware campaign.

Table 1 and Table 2 detail the significant cyber-incidents to the ICSs referenced in this study. The threat types include directed **attacks**, cyber-intrusion **campaigns**, **malware**, and cyber-threat **groups**, and are presented in a chronological timeline. This open source analysis was compiled from cybersecurity companies, independent security researchers, news media, other published reports, and government sources.

When attribution is reported (in the open source literature) it is included for the reader's awareness. This list is not comprehensive, but focuses on significant cyber-threats, incidents, and campaigns affecting ICS devices and critical infrastructure. In some cases, attacks were deliberate to ICS devices; whereas in other cases, ICS devices were indirectly targeted or impacted.

Table 2. ICS cyber-incident timeline (continued).

Year	Type	Name	Description
2014	Attack	German Steel Mill	A steel mill in Germany experienced a cyber-attack resulting in massive damage to the system.
2014	Malware	Black Energy	Malware that targeted human-machine interfaces (HMIs) in ICSs.
2014	Campaign	Dragonfly/Energetic Bear No. 1	Ongoing cyber-espionage campaign primarily targeting the energy sector.
2015	Attack	Ukraine Power Grid Attack No. 1	The first known successful cyber-attack on a country's power grid.
2016	Attack	"Kemuri" water company	Attackers gained access to hundreds of the programmable logic circuits (PLCs) used to manipulate control applications, and altered water treatment chemicals.
2016	Malware	Return of Shamoon	Thousands of computers in Saudi Arabia's civil aviation agency and other Gulf State organizations wiped in a second Shamoon malware attack.
2016	Attack	Ukraine Power Grid Attack No. 2	Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.
2017	Malware	CRASHOVERRIDE	The malware used to cause the Ukraine power outage was finally identified.
2017	Group	APT33	A cyber-espionage group targeting the aviation and energy sectors.
2017	Attack	NotPetya	Malware that targeted the Ukraine by posing as ransomware, but with no way to pay a ransom to decrypt altered files.
2017	Campaign	Dragonfly/Energetic Bear No. 2	Symantec® claims energy sector is being targeted by a sophisticated attack group.
2017	Malware	TRITON/Trisis/ HatMan	Industrial safety systems in the Middle East targeted by sophisticated malware.

2. Cyber-Incidents

2.1 Marconi Wireless Hack

The first cyber-threat we present is a tongue-in-cheek example of the world's first malicious hacking of "secure communications." In 1903, an Italian radio pioneer, Guglielmo Marconi, prepared to present the first public demonstration of long-distance wireless communications using Morse code to an inquisitive audience. The live demonstration was to show that a wireless message could be sent *securely* from a cliff-top radio station in Poldhu, Cornwall, U.K., to London, some 300 miles away.

But before Marconi could begin his demonstration, the theater's brass projection lantern, used to display the lecturer's slides, began to click. To an untrained ear, it probably sounded like a projector having technical difficulties; but to assistant Arthur Blok, the clickity-click coming from the projector was the unmistaken sound of Morse code [1], which spelled out an unexpected message:

> *Rats, rats, rats, rats.*
> *There was a young fellow of Italy,*
> *Who diddled the public quite prettily.*

The message went on to further mock and insult Marconi. The demonstration had been hacked! But who was the mysterious hacker, and why did he hack Marconi's demonstration?

A few days after the demonstration, a letter was printed in *The Times* confessing to the "hack" [2]. It was British music hall magician Nevil Maskelyne. It turns out that Maskelyne wanted to disprove Marconi's claim that his wireless telegraph device could send messages securely. The magician, much like today's security researchers, wanted to reveal a security hole for the public good.

The identification of vulnerabilities in ICSs is most often reported by independent cybersecurity researchers. Nevil Maskelyne may have been the first to publically report a vulnerability in modern technology.

2.2 Maroochy Water

In March 2000, the Maroochy Shire Council in Queensland, Australia, experienced problems with its new wastewater system. Communications sent by radio frequency (RF) signals to wastewater pumping stations failed. Pumps did not work correctly, and alarms that were supposed to notify system engineers of faults did not activate as expected [3].

An engineer who was monitoring signals passing through the system discovered that someone was interfering with it and deliberately causing problems. The water utility hired a team of private investigators who located the attacker and alerted police.

On April 23, 2001, police chased the car of 49-year-old Vitek Boden and ran him off the road. In his car, police found a laptop and specialized Supervisory Control and Data Acquisition (SCADA) equipment he had used to attack Maroochy Water's system [4]. Follow-up investigations found Boden's laptop was used during times the attacks occurred, and software for controlling the sewage management control system was discovered on his hard drive [5].

Boden had used a radio transmitter and his laptop to control some 150 sewage pumping stations. Over a three-month time period, Boden

released millions of gallons of untreated sewage into waterways and local parks [6]. The judge in the case stated that the act was Boden's revenge for failing to get a job with the Maroochy Council [3].

Robert Stringfellow was the civil engineer responsible for the water supply and sewage systems at Maroochy Water Services during the time of the breach. In a post-incident analysis, Stringfellow noted:

- It is very difficult to protect against insider attacks.
- Radio communications commonly used in SCADA systems are generally insecure or improperly configured.
- SCADA devices and software should be secured to the extent possible using physical and logical controls.
- SCADA systems must record all device accesses and commands, especially those involving connections to or from remote sites [6].

The Maroochy Water Services incident is an example of the type of cyber-attack that can be launched on ICSs resulting in physical damage. In this rare case, the attacker was identified and prosecuted.

2.3 Turkey Pipeline Explosion

The 2008 Turkey Pipeline explosion has been attributed to cyber-intrusion, but was actually caused by a physical attack. In August 2008, a segment of the Baku-Tbilisi-Ceyhan (BTC) Oil Pipeline exploded in Refahiye, eastern Turkey, during the Georgian War. Many reports at the time attributed the explosion to a cyber-nexus [7], [8], [9], [10].

Bloomberg published the original report of the attack on December 14, 2014, with the title "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar" [7]. However, a subsequent story in a major German newspaper casts significant doubt on the reports of a cyber-attack causing the explosion [11]. Hakan Tanriverdi's article in *Seuddeutsche* focused on four claims made by the *Bloomberg* article and introduced new information surrounding them from an internal report.

In an analysis by the SANS ICS team, Robert Lee concurs with the *Seuddeutsche* conclusions that the Turkey Pipeline explosion was not caused by cyber-means [12]. Lee notes "there are numerous reported and unreported cases of failures at ICS facilities where a cyber-incident is to blame. Without the appropriate data, there will simply not be any lessons learned or resolution [as] to the root cause" [12].

This event is included to make the reader aware that this incident is often inaccurately cited as one of the first ICS cyber-incidents. It is also

included to highlight the point that cyber-attribution for physical events can be difficult to ascertain.

2.4 Stuxnet

In 2010, Stuxnet was among the most sophisticated malware known at the time [13]. It infected control system networks and was believed by some to have damaged as many as one-fifth of the nuclear centrifuges in Iran [14].

Symantec executive Dean Turner testified before the U.S. Senate Homeland Security Committee that the Stuxnet malware was a wake-up call to critical infrastructure systems around the world, as it was commonly believed to be the first publicly known threat to specifically target ICSs and grant attackers control of specific systems [15].

Stuxnet was believed to have targeted specific equipment operating in Iran's Natanz uranium-enrichment facility [16], [17]. The U.S. Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Team (ICS-CERT) issued multiple advisories on how to mitigate the Stuxnet malware, which also infected systems in the U.S. [18].

What made Stuxnet so dangerous was that it self-replicated and spread throughout multiple systems via multiple means, such as:

- Removable drives exploiting a vulnerability allowing auto-execution.
- Local area networks (LANs) exploiting a vulnerability in the Windows Print Spooler.
- Server Message Block (SMB) used for providing shared access to files, printers, and other devices by exploiting a vulnerability in the Microsoft Windows Server Service.
- Network file sharing by copying and executing itself.
- Siemens WinCC HMI database server by copying and executing itself.
- Siemens Step 7 by copying itself into Step 7 projects in such a way that it automatically executed when the Step 7 project is loaded.

Stuxnet exploited a total of four unpatched Microsoft vulnerabilities, two that were vulnerabilities for self-replication and two that provided an escalation of privilege vulnerabilities that were previously unknown or zero-day vulnerabilities.

One of the significant features that allowed Stuxnet to install itself undetected was its use of digitally signed code by legitimate software developers, which had been stolen from two different Taiwanese companies. Using these digital certificates, Stuxnet contacted a command and control (C2) server that allowed the attackers to download and execute updated code.

Stuxnet was also stealthy, in that it could hide its binaries through a Windows rootkit. It would attempt to evade detection by altering several security products if it found them on the targeted system. It hid modified code on PLCs by creating a rootkit of sorts for Siemens PLCs. It modified the data sent from the PLC so that the HMI displayed incorrect information to the operator making everything seem fine.

Stuxnet was a precision weapon that looked for exact software to be installed on and specific equipment to be connected to a system. If it did not find all of these things, it self-terminated. If it did find the precise configuration it was looking for, it modified and sabotaged the code on Siemens PLCs by injecting ladder logic code directly into them.

A key lesson learned from Stuxnet is that a well-financed sophisticated threat actor can likely attack any system that it desires. The ability to detect and recover from a cyber-attack is the important takeaway, as protecting all systems from any attacker is not possible.

2.5 Night Dragon

Night Dragon is the name given by cybersecurity company, McAfee®, to the Tactics, Techniques, and Procedures (TTPs) used in a series of coordinated, covert, and targeted cyber-attacks beginning in November 2009, and made public in 2010 [19]. These cyber-attacks targeted global oil, energy, and petrochemical companies. McAfee claims that attackers in China utilized the 'Night Dragon' C2 servers located in the U.S. and the Netherlands. Attackers collected information from computer systems, including ICSs.

According to McAfee, the attacks involved social engineering, spearphishing attacks, exploitation of Microsoft® Windows® operating systems vulnerabilities and Microsoft Active Directory compromises, and the use of remote access trojans (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information about oil and gas field bids and operations [19].

McAfee reported that once the attackers had complete control of a targeted system, they dumped account password hashes and used a common password cracking tool to leverage the attack in targeting other more sensitive information [19].

Exfiltrated files of interest focused on operational oil and gas field production systems, as well as financial documents related to field exploration and bidding. In some cases, the files were copied to and downloaded from company web servers by the attackers. In others, the attackers collected data from SCADA systems.

ICS-CERT issued a February 2011 alert on Night Dragon to warn U.S. critical infrastructure of the threat [20].

The Night Dragon attacks were not sophisticated, but they demonstrated that simple techniques, applied by a skillful and persistent adversary, are enough to break into energy-sector companies. More importantly, the attacks demonstrated that they could also compromise ICSs as well. Equally concerning is that the tools used by this adversary let them take complete control of compromised systems through remote-desktop-like capabilities. Night Dragon used these tools to steal valuable information, but it could just as easily have been used to take control of an HMI, which could then have provided the attackers with remote control of critical energy systems.

2.6 Duqu/Flame/Gauss

In 2011, Hungarian cybersecurity researchers with the Laboratory of Cryptography and Systems Security (CrySyS) located at the Budapest University of Technology and Economics, Department of Telecommunications, discovered the Duqu malware during an incident response investigation [21]. Duqu was malware designed to perform information-gathering. According to Dr. Boldizsar Bencsath, Duqu bears a striking similarity to Stuxnet in terms of design philosophy, internal structure and mechanisms, implementation details, and the estimated amount of effort needed to create it [21].

One of the interesting features of Duqu is that it made use of a stolen digital certificate from a Taiwanese company, just as Stuxnet did. The stolen certificates allowed the attackers to successfully install malware on target systems. The Stuxnet and Duqu digital certificates were stolen from businesses located in the same business park in Taiwan [22].

According to Symantec and Kaspersky reports, the Duqu executables share some code with Stuxnet and were compiled after the last Stuxnet sample was recovered [23], [24]. Duqu was an information-stealing malware that attempted to disguise data transmissions as normal HTTP traffic by appending encrypted data to be exfiltrated in a .jpg file [25].

While working with other international researchers, the same Hungarian researchers that identified Duqu also identified the Flame or Sky-

wiper malware. According to researchers, Flame is extremely complex malware also designed to steal information by using:

- Microphones installed on systems.
- Web cameras.
- Key stroke logging.
- Extraction of geolocation data from images [21].

Flame could send and receive commands and data through Bluetooth, and it stored its collected data in SQL databases. It used both network connections and USB flash drives for communication. Flame infected computers by masquerading as a proxy for Windows Update by using a fake certificate that looked like a valid Microsoft certificate and utilized an advanced collision attack on the MD5 hash function [21]. Kaspersky researchers also found chunks of code from a 2009 Stuxnet variant inside Flame [24].

Russian cybersecurity firm Kaspersky Lab later identified malware they named Gauss, which is believed to be related to Duqu and Flame as they all use the same framework [21],[26]. Gauss is also information-stealing malware. Gauss collected the following information from the systems it compromised:

- Passwords, cookies, and browser history by injecting its modules into different browsers in order to intercept user sessions.
- Computer network connections.
- Processes and folders.
- BIOS and CMOS RAM details.
- Local, network, and removable drive information.

Gauss also infected USB drives with a spy module in order to steal information from other computers. It interacted with C2l servers to download additional modules and to send collected information back to the attackers. ICS-CERT issued reports on Duqu [25], Flame [27], and Gauss [28] in 2012.

The important takeaway from the Duqu, Flame, and Gauss information-stealing malware is that sophisticated threat actors do perform reconnaissance to collect as much information as they need to further their operations. The threat actors behind this malware used a wide variety of methods to spread their information-stealing code, and they made

use of all available information on a system to learn about their targets. It is important to understand that the first step in The Cyber Kill Chain® is reconnaissance [29]. Information-stealing malware—such as Duqu, Flame, and Gauss—is how sophisticated attackers begin the cyber kill chain.

2.7 Gas Pipeline Cyber-Intrusion Campaign

Beginning in late December 2011, ICS-CERT identified an active series of cyber-intrusions by a sophisticated threat actor targeting natural gas pipeline sector companies. Various sources provided information to ICS-CERT describing targeted attempts and intrusions into multiple natural gas pipeline sector organizations [30].

Analysis of the malware and artifacts associated with these cyber-attacks positively identified this activity as related to a single campaign with spear-phishing activity dating back to as early as December 2011. ICS-CERT analysis showed that the spear-phishing attempts targeted a variety of personnel within these organizations; however, the number of persons targeted appeared to be tightly focused. In addition, the emails were convincingly crafted to appear as though they were sent from a trusted member internal to the organization [30].

ICS-CERT issued an alert (ICSA-12-136-01BP) to the United States Computer Readiness Team (US-CERT) Control Systems Center secure portal library regarding the threat, and disseminated information about the attacks to sector organizations and agencies to ensure broad distribution to asset owners and operators [31]. ICS-CERT recommends following Defense-in-Depth practices and educating users about social engineering and spear-phishing attacks [32]. Organizations were also encouraged to review ICS-CERTs Incident Handling Brochure for tips on preparing for and responding to an incident.

DHS ICS-CERT, in coordination with the Federal Bureau of Investigation (FBI), the U.S. Department of Energy (DOE), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the Transportation Security Administration (TSA), and the Oil and Natural Gas and Pipelines Sector Coordinating Councils Cybersecurity Working Group, conducted a series of Action Campaign Briefings throughout Fiscal Year 2013 in response to the growing number of cyber-incidents related to U.S. critical infrastructure. The 14 briefings were given to over 750 attendees in various cities throughout the country to assist critical infrastructure asset owners and operators in detecting intrusions and developing mitigation strategies. Briefings were held at both the classified and unclassified levels [33].

Throughout this experience, the energy sector became more aware of the important work that DHS, FBI, and other Federal agencies do in identifying threats to protect critical infrastructure. Information-sharing is important, and this intrusion campaign demonstrated how Federal agencies can work together with the private sector to share information at both the classified and unclassified levels.

2.8 Shamoon – Saudi Aramco and RasGas

On August 15, 2012, destructive malware attacked the computer systems of Saudi Aramco, the largest energy company in the world. The attackers carefully selected the one day of the year they knew they could inflict the most damage—the day that more than 55,000 Saudi Aramco employees stayed home from work to prepare for one of Islam's holiest nights of the year—Lailat al Qadr, or the Night of Power—celebrating the revelation of the Quran to Muhammad [34].

When the Shamoon malware triggered, it overwrote data on over 30,000 computers with an image of a burning American flag. Shamoon was an information-stealing malware, which also included a destructive module. Shamoon renders infected systems unusable by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the information is not recoverable. Symantec detailed the malware in its official blog on August 16, 2012 [35]. DHS ICS-CERT also issued a report on the malware [36].

Twelve days later on August 27, 2012, the Shamoon malware hit its second target, the Qatari natural gas company, RasGas, which is one of the largest liquefied natural gas (LNG) companies in the world [37]. There was no evidence that Shamoon had any direct impact on ICS or SCADA systems at either Saudi Aramco or RasGas.

Once a system is infected with the Shamoon malware, it attempts to spread itself to other devices on the local network. C2 communications are used to control the operation of the attack, but are not necessary if the threat actor has programmed a time for disk destruction before delivering the malware.

Shamoon supports the ability to download and execute arbitrary executables from the C2 server, giving the attacker the ability to potentially spread the infection or download additional tools on the victim device for network traversal.

ICS-CERT provided guidance on best practices for continuity of operations when dealing with destructive malware like Shamoon [38].

Saudi Aramco and RasGas were taught the hard lesson that malicious threat actors can and do conduct destructive attacks. The ability to recover from a destructive cyber-attack is an important takeaway.

2.9 Target Stores

Cyber-intrusions into ICSs often occur through attackers targeting an organization's business network, and from there pivoting into the control system network. However, the opposite happened on November 15, 2013, when hackers broke into a third-party that maintained Target Store's heating, ventilation, and air conditioning (HVAC) ICSs [39].

Cyber-attackers who had the objective to steal credit card data from Target Stores, first stole the login credential of a third-party HVAC contractor. The attackers did this by sending a phishing email to at least one of the contractor's employees. The employee was fooled by the email and clicked on the bait that allowed the attacker to install a variant of the Zeus banking trojan, which then provided them with the login credentials they needed to exploit the HVAC systems in Target Stores. Once the attackers gained access to Target's business network via its' building control systems, the attackers uploaded malicious credit card-stealing software to cash registers throughout Target's chain of stores [40].

According to a report released by DHS [41], the malicious program used to compromise Target was part of a widespread operation that used a trojan tool known as Trojan.POSRAM. The code is based on a previous malicious tool known as BlackPOS that is believed to have been developed in Russia in 2013, though the new variant was highly customized to prevent anti-virus programs from detecting it, according to iSight Partners and an internal report produced by the U.S. Secret Service and other government agencies investigating the breaches [42], [43].

The total cost to Target for the attack, security upgrades, and lawsuits is estimated at $309M [44]. Seventy million customers were affected. The breach exposed approximately 40 million debit and credit card accounts. Financial institutions incurred an additional $200M in expenses from the attack. Customer names, credit or debit card numbers, expiration dates, and CVVs were all involved in the information theft. All of these expenses were the end result of exploiting the security of a building automation system.

The Target breach demonstrated that the oft forgotten cybersecurity of building automation is indeed important.

2.10 New York Dam

According to the U.S. Justice Department, a small dam near Rye Brook, New York, was accessed by Iranian hackers in 2013. The intrusion was not sophisticated, but thought to be a test by Iranian attackers to see what they could access [45].

The small utility, known as Bowman Dam, is used for controlling storm surges. The Bowman Dam SCADA system was connected to the Internet via a cellular modem. The SCADA system was undergoing maintenance at the time of the attack, and no control was possible; only status monitoring. Most feel the dam was attacked because of its vulnerable Internet connection and a lack of security controls, rather than a targeted cyber-attack [46].

Technical details of the New York dam intrusion are deemed Protected Critical Infrastructure Information (PCII) and are not releasable to the public. Although the dam was actually a small village's sluicegate that did not have any significance in terms of threat to public safety, it is concerning because of the identified attackers. A Federal indictment disclosed the attackers as two groups called the ITSec Team and the Mersad Company [47]. These were private computer security companies based in the Islamic Republic of Iran that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps (IRGC).

The most concerning aspect of this cyber-intrusion is who was conducting the intrusion, and the technical capability they showed by directly manipulating SCADA equipment. It is possible that the Iranian attackers selected the small Bowman dam simply because it was "low-hanging fruit." When critical infrastructure control systems are directly exposed to the Internet, they become an easy target for any potential attacker to find. In this case, it turned out to be sophisticated threat actors from Iran.

2.11 Havex

In 2013, a RAT malware called Havex (or Oldrea) was discovered that focused on ICSs. In 2016, DHS and the FBI issued a Joint Analysis Report that ties Havex to the Russian Civilian and Military Intelligence Services (RIS) group referred to as GRIZZLEY STEPPE [48], and also known by the names "Dragonfly" and "Energetic Bear."

Havex communicates with a C2 server that can deploy modular payloads, providing the malware with additional functionality. ICS-CERT identified and analyzed one payload that enumerates all connected network resources, such as computers or shared resources, and uses the

classic Distributed Component Object Model (DCOM)-based version of the Open Platform Communications (OPC) standard to gather information about connected ICS devices and resources within a network [49].

The Havex control-system-specific payload gathered server information, including CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth. In addition to more generic OPC server information, the Havex payload also has the capability of enumerating OPC tags. Havex is not without flaws, however. It caused multiple common OPC platforms to intermittently crash. ICS-CERT warned that this could cause a denial of service effect on applications reliant on OPC communications [49].

The important aspect to Havex is that the U.S. Government identified the RIS as the group behind Havex. This is significant because Havex is advanced malware focused on ICSs. The malware communicated with a C2 infrastructure that could send instructions to provide enhanced, unknown capabilities to the malware. The threat actors that controlled the Havex malware specifically targeted ICSs used in U.S. critical infrastructure.

2.12 German Steel Mill

In December 2014, the German government's Bundesamt fur Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) released their annual findings report, "The State of IT Security in Germany 2014." In it, the BSI describes the general cyber-threat situation in Germany. The report briefly describes an attack on an unspecified German steel mill. According to BSI, the attack was carried out using spear-phishing and social engineering tactics.

The attackers initially gained access to the business network of the steel plant. From there, they worked their way into the production network. The attackers caused multiple failures of individual control systems, eventually preventing a blast furnace from being able to shut down in a controlled manner, which resulted in "massive damage to the plant." The technical abilities of the attackers were described as "very advanced." The attackers were knowledgeable not only in advanced IT security, but also possessed detailed knowledge of ICSs and the steel production process [50].

What was interesting in the brief report is the description that the attackers had an advanced understanding of ICSs, a knowledge of the steel plant process, and most importantly, were able to achieve massive damage to the process by causing multiple control system failures. The

description in the BSI report and accompanying knowledge on process incidents leads many to believe the process damage was intentional [51].

The German steel mill cyber-attack is significant because of the physical damage that resulted as well as the German government's willingness to release information regarding the incident. "The most significant component of this report is the demonstrated capability and willingness of an adversary to attack through traditional advanced persistent threat (APT) style methods and then advance to a cyber-physical attack with the intent to impact an operational environment" [51].

2.13 BlackEnergy

In 2014, ICS-CERT published a series of alerts describing a sophisticated malware campaign that had compromised numerous ICSs using a variant of the BlackEnergy malware. DHS analysis indicated this campaign had been ongoing since at least 2011 [52]. The 2016 DHS and FBI Joint Analysis Report identifying Havex as coming from the RIS group, GRIZZLEY STEPPE [48], connected BlackEnergy to them as well.

HMI products from multiple ICS vendors were targeted in the campaign, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. The malware is modular and not all functionality is deployed to all victims. Typical BlackEnergy infections have included modules that search out any network-connected file shares and removable media that could aid the malware in performing lateral movement within the affected environment [52].

In December 2014, DHS confirmed that a BlackEnergy 3 malware variant was present in a Ukraine energy system that was attacked, causing a power outage. ICS-CERT published a special TLP Amber version of an alert containing additional information about the malware, plug-ins, and indicators to the DHS secure portal website. ICS-CERT strongly encouraged asset owners and operators to use the indicators to look for signs of compromise within their control system environments.

In December 2014, ICS-CERT partnered with the FBI to conduct classified and unclassified threat briefings for private sector critical infrastructure stakeholders across the country. Teams from ICS-CERT and the FBI traveled to 15 cities across the U.S. In total, nearly 1,600 participants involved in the protection of critical infrastructure across all 16 sectors attended the briefings.

Like Havex, BlackEnergy targeted important ICS products. It is concerning when adversaries target control systems used in critical infrastructure. From BlackEnergy, we learn about nation state threat actors and the tools they use to target critical infrastructure.

2.14 Dragonfly/Energetic Bear

On June 30, 2014, Symantec Security Response released a whitepaper detailing an ongoing cyber-espionage campaign dubbed "Dragonfly" [53]. Other reports refer to this same campaign as "Energetic Bear" or "Crouching Yeti" [54]. Symantec described Dragonfly as an ongoing cyber-espionage campaign primarily targeting the energy sector. The campaign is focused on espionage and persistent access, with sabotage as an optional capability. The malware uses the Havex (or Oldrea) malware as its favored tool, and the Karagany RAT as a secondary tool. Symantec observed attacker activity in organizations in the U.S., Turkey, and Switzerland, with traces of activity in organizations outside these countries [53].

The 2014 Dragonfly campaigns were assessed to have been an exploratory phase where the attackers were focused on trying to gain access to the networks of targeted organizations [53].

Dragonfly/Energetic Bear were later identified by DHS and the FBI to be part of the same RIS GRIZZLY STEPPE [48] group.

2.15 Ukraine Power Grid

In 2015, two days before Christmas, a cyber-attack cut electricity to nearly a quarter-million Ukrainians. This is the first known successful cyber-attack on a power grid.

Reuters reported that a power company located in the western portion of the Ukraine suffered a power outage, which impacted a large area that included the regional capital of Ivano-Frankivsk [55]. Attackers shut off power at 30 substations and left 230,000 people without electricity for up to six hours. SCADA equipment was rendered inoperable, and power restoration had to be completed manually—further delaying restoration efforts [56].

Investigators discovered that attackers had facilitated the outage by using the BlackEnergy malware to exploit the macros in Microsoft Excel documents. The malware was planted onto the company's network using spear-phishing emails [57]. ICS-CERT and US-CERT worked with the Ukrainian CERT and international partners to analyze the malware and confirmed that a BlackEnergy 3 variant was present in the Ukrainian power system [52]. The Ukrainian intelligence community blamed the attack on Russian attackers [58]. BlackEnergy has been publically identified by DHS and the FBI to be part of the RIS GRIZZLEY STEPPE [59] group.

At the request of the Ukrainian government, a U.S. interagency team comprised of representatives from ICS-CERT and US-CERT, as well as

DOE, the FBI, and the North American Electric Reliability Corporation, traveled to the Ukraine to gather information about the incident and identify potential mitigations [33].

This attack taught the world that it is indeed possible to damage the power grid through a cyber-attack, and was a wake-up call to ensure that the U.S. power grid is fortified against such attacks. In the case of the Ukraine, the attackers used technically unsophisticated techniques to achieve their goal. The Ukraine power grid attack was a significant event in cyber-history.

2.16 "Kemuri" water company

In 2016, Verizon Security Solutions reported that an undisclosed water company experienced a cyber-attack on its ICSs. Verizon gave the water company the fictitious name of "Kemuri" to protect its identity. According to Verizon, attackers accessed the water district's valve and flow control application responsible for manipulating hundreds of PLCs that control water treatment chemical processing. They then managed to manipulate the system to alter the amount of chemicals entering the water supply and affect water treatment and production capabilities, causing water supply recovery times to increase [60].

According to Verizon, a "hacktivist" group with ties to Syria was behind the attack. The Kemuri breach was serious and could easily have been more critical. Verizon assessed that had the threat actors had a little more time, and a little more knowledge of the ICS/SCADA system, Kemuri and the local community could have suffered serious consequences.

A key take-away from this experience is that having Internet-facing ICSs is a bad practice that can place critical infrastructure at risk. Kemuri was also a reminder that cyber-threat actors are not afraid to cross the line to cause harmful damage.

2.17 Return of Shamoon

In November 2016, a second wave of attacks by the destructive malware Shamoon was launched at selected targets in Saudi Arabia. Thousands of computers in the Saudi Arabian civil aviation agency and other Gulf State organizations were wiped by the Shamoon malware after it resurfaced some four years after attacking thousands of Saudi Aramco workstations [61].

Symantec discovered a high correlation between a cyber-attack group they call "Timberworm" and the Shamoon malware [62]. Timberworm

appeared to have gained access to these organizations' networks weeks and, in some cases, months before the 2016 Shamoon attacks [62].

In December 2016, the Defense Security Service (DSS), part of the U.S. Department of Defense (DoD), issued a security bulletin to cleared contractors warning them of the Shamoon malware threat [63].

The concerning aspect to this second Shamoon attack is the ongoing use of destructive malware to target critical infrastructure. Critical infrastructure needs to remain vigilant in their defense posture, and learn how to protect themselves using information learned from these attacks.

2.18 Second Attack on the Ukraine Power Grid

On December 17, 2016, almost one year after Ukraine suffered a major cyber-attack on its power grid, Kiev suddenly went dark again. Cyber-attackers caused monitoring stations to suddenly go blind. Breakers tripped in 30 substations, turning off electricity to approximately 225,000 customers. To prolong the outage, attackers also launched a telephone denial-of-service attack (TDoS) against the utility's call center to prevent customers from reporting the outage, the same tactic that was used in 2015. The intruders also rendered devices, such as serial-to-Ethernet convertors, inoperable and unrecoverable on their way out to make it harder to restore electricity to customers [64]. Despite these setbacks in the original attack, power was restored in three hours in most cases, but because the attackers had sabotaged management systems, workers had to travel to substations and manually close breakers the attackers had remotely opened [56], [57]. However, the second attack was much more sophisticated than the first [64].

Where the first attack used remote control software to manually trip breakers, the second is believed to have used sophisticated malware that directly manipulated SCADA systems. Rob Lee with Dragos Security said, "In my analysis, nothing about this attack looks like it's singular. The way it's built and designed and run makes it look like it was meant to be used multiple times. And not just in Ukraine" [65]. The sophisticated malware used in that second attack would later be identified as "CRASHOVERRIDE."

2.19 CRASHOVERRIDE

Dragos Security, working in coordination with the Slovak anti-virus firm ESET, confirmed that the CRASHOVERRIDE (or "Industroyer") malware was indeed employed in the December 17, 2016, cyber-attack on a Kiev, Ukraine transmission substation, which resulted in the large power outage [65], [66].

According to Dragos, CRASHOVERRIDE was the first ever malware framework specifically designed and deployed to attack electric grids. It is the fourth-ever piece of ICS-tailored malware used against specific targets, with Stuxnet, BlackEnergy-2, and Havex being the first three. It is the second malware ever designed and deployed for disrupting physical industrial processes, with Stuxnet being the first [65]. Dragos also stated that the functionality in the CRASHOVERRIDE framework serves no espionage purpose, and the only real feature of the malware is for attacks leading to electric outages.

The CRASHOVERRIDE malware is a framework that has modules specific to ICS protocol stacks, including IEC 101, IEC 104, IEC 61850, and OPC. It is designed to allow the inclusion of additional payloads like DNP3, but at the time, no such payloads had been confirmed. The malware also contained additional non-ICS specific modules, such as a wiper, to delete files and disable processes on the running system for a destructive attack to operations [65].

The modules in CRASHOVERRIDE are leveraged to open circuit breakers on remote terminal units (RTUs) and force them into an infinite loop to keep the circuit breakers open, even if grid operators attempted to close them, which resulted in the de-energization of substations forcing grid operators to switch to manual operations in order to restart power [65].

Dragos says there are concerns CRASHOVERRIDE could be leveraged to disrupt grid operations that would result in power outages lasting hours. They assess that power outages could last up to a few days if an attack targeted multiple sites. However, Dragos also pointed out that there is no evidence that threat actors could use CRASHOVERRIDE to cause any power outages to last longer than that. But to even get a few days of power outages would require the targeting of multiple sites simultaneously, which is entirely possible, but not trivial [65].

Using the National Cyber Awareness System (NCAS), DHS issued a CRASHOVERRIDE malware Technical Analysis alert on June 12, 2017, notifying U.S. critical infrastructure of the serious threat the malware poses [67]. The significant takeaway from the discovery of CRASHOVERRIDE is that nation state threat actors have created an advanced reusable malware framework specifically designed to cause power outages. This same threat actor has demonstrated on multiple occasions that it is willing and able to cause power outages through cyber-means.

2.20 APT33

In 2017, cybersecurity company FireEye published a report detailing a cyber-threat actor they call "APT33." According to FireEye's analysis, APT33 is a capable group that has carried out cyber-espionage operations since at least 2013. FireEye assessed that APT33 works at the behest of the Iranian government [68].

FireEye reported that APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production. According to FireEye, the targeting of organizations involved in energy and petrochemicals mirrors previously observed targeting by other suspected Iranian threat groups, indicating a common interest in the sectors across Iranian actors. Targeted countries include: the U.S., Saudi Arabia, and South Korea. FireEye further warns APT33 may also have ties to other groups with destructive capabilities [68].

APT33 delivers its malware through targeted spear-phishing emails sent to employees. The emails included recruitment-themed lures and contained links to malicious HTML application (.hta) files that contained job descriptions and links to legitimate job postings on popular employment websites, which would be relevant to the targeted individuals. The phishing emails appeared legitimate—they referenced specific job opportunities and salaries, provided a link to the spoofed company's employment website, and even included the spoofed company's Equal Opportunity hiring statement.

One of the most concerning aspects of the APT33 attack group is that they have malicious capabilities and ties to the destructive SHAMOON malware. The group was also tied to the SHAPESHIFT wiper malware that is capable of wiping disks, erasing volumes, and deleting files. FireEye believes that some of the tools used by APT33 may be shared amongst other Iran-based threat groups.

2.21 NotPetya

Also in 2017, malicious malware posing as the "Petya" ransomware surfaced in the Ukraine. Petya is ransomware that targets Microsoft Windows-based systems. After a system is infected, the malware encrypts the file system and displays a message demanding payment in Bitcoin in order to regain access. But where the new malware seemed to be based on and functioned like the Petya ransomware, it was different. It does encrypt data on a hard drive just like Petya, but there is no way to decrypt what it has encrypted—it is a malicious, **permanent** encryption; therefore, it was given the name "NotPetya."

Where Petya is designed more to be "crimeware" that extorts money from victims, NotPetya is specifically designed to be destructive malware. It has been enhanced to spread widely and was believed to specifically target the Ukraine [69]. On June 30, 2017, DHS ICS-CERT issued an alert warning the critical infrastructure in the U.S. about this malicious new threat [70].

In February 2018, the U.S. Government blamed the Russian military for developing and releasing the NotPetya malware stating that NotPetya was "reckless" and caused billions of dollars in damages [71], and called it the "most destructive and costly cyber-attack in history" [72], [73]. The UK and Australian governments also judged that the Russian government was responsible for the NotPetya malware [74]. However, the Russian government has denied these accusations of its involvement with the malware [75], [76].

NotPetya is concerning because a nation state, confirmed by intelligence agencies in three countries, demonstrated its ability and willingness to conduct destructive cyber-attacks against critical infrastructure. According to the White House, NotPetya caused billions of dollars in damage across Europe, Asia, and the Americas [72].

2.22 Dragonfly/Energetic Bear Returns

In October 2017, Symantec published a report claiming the energy sector was being targeted by a sophisticated attack group it referred to as another version of "Dragonfly." The report stated this group was well resourced, with a range of malware tools at its disposal and was capable of launching attacks through a number of different vectors. Symantec referred to this new Dragonfly activity as "Dragonfly 2.0." In a vicious attack campaign, Dragonfly 2.0 compromised a number of ICS equipment vendors, infecting their software with a RAT [77].

The Dragonfly 2.0 campaign shows how attackers may be entering into a new phase, with new campaigns potentially providing them with access to operational systems—access that could be used for more disruptive purposes in the future. According to Symantec, this group appeared to be interested in both learning how energy facilities operate, as well as gaining access to operational systems. One of the report's most concerning assessments is that Dragonfly 2.0 has the ability to sabotage or gain control of ICSs [77].

On October 20, 2017, DHS and the FBI issued a joint Technical Alert on an APT targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors [59]. This Technical Alert assessed the activity as a multi-stage intrusion cam-

paign by threat actors targeting low security and small networks to gain access and move laterally to major networks and high value assets within the energy sector. Based on malware analysis and observed indicators of compromise, DHS indicated confidence that the campaign was still ongoing, and that threat actors were actively pursuing their ultimate objectives over a long-term campaign.

The Dragonfly and Energetic Bear threat groups were publically identified by DHS and FBI as being part of the same group they call GRIZZLEY STEPPE [59]. This information on Dragonfly from Symantec and DHS demonstrates that the threat actor has continued its activities, and that its capabilities have evolved. Symantec made an important statement that the attackers "may have entered into a new phase with access to operational systems that could be used for more disruptive purposes in the future" [77].

2.23 TRITON/Trisis/HatMan

At the end of 2017, FireEye published a report on a new ICS attack framework called "TRITON," designed to cause operational disruption to critical infrastructure. FireEye claims industrial safety systems in the Middle East were being targeted by TRITON [78]. Symantec released an additional late 2017 report on this same malware, but referred to it as "Trisis" [79]. Meanwhile, DHS ICS-CERT published a December 2017 Malware Analysis Report on this same malware, yet called it by a third name, "HatMan" [80].

Regardless of its true name, the malware targets Schneider Electric's Triconex safety instrumented system by modifying in-memory firmware to add malicious functionality allowing an attacker to read/modify memory contents and execute custom code on demand by receiving specially crafted network packets from the attackers [80], as well as additional programming to disable, inhibit, or modify the ability of a process to fail safely. By targeting safety systems, this malware can be physically dangerous [79].

It should be noted that TRITON's victim was narrowly targeted and likely does not pose an immediate threat to other Schneider Electric customers or products. However, the capability, methodology, and tradecraft used by TRITON could be replicated by other attackers, and thus represents an additional threat to critical infrastructure ICSs [81].

The most concerning aspect of TRITON is that it is the first known malware to specifically target industrial safety systems designed to protect human lives. This capability can now potentially be replicated by other attackers to cause physical damage or harm people.

3. Lessons Learned

From the cyber-events the world has experienced thus far, we have discovered the technical capabilities of threat actors have evolved significantly, and that their willingness to cause physical damage is startling. Stuxnet, in particular, was a game-changer. This malicious piece of malware taught us that the physical world can be significantly impacted through cyber-means. Stuxnet was an extremely sophisticated cyber-attack accomplished through advanced malware that targeted a specific ICS. A key lesson learned from Stuxnet is that a well-financed sophisticated threat actor can likely attack any system it desires, which should cause concern for critical infrastructure owners and operators.

For critical infrastructure, developing the ability to detect and recover from a cyber-attack is the most important lesson to be learned, because protecting all systems from any attacker is not possible. We learned from attacks like Night Dragon that simple techniques, applied by a skillful and persistent adversary, are enough to break into critical infrastructure, including companies in the energy sector.

We have also become knowledgeable of the advanced techniques that can be used in cyber-attacks. The Duqu, Flame, and Gauss malware taught us that sophisticated threat actors perform reconnaissance to collect as much information as they need to ensure success. It is important to understand that the first step in the cyber kill chain is reconnaissance [29]. Information-stealing malware—such as Duqu, Flame, and Gauss—is how sophisticated attackers begin the cyber kill chain.

The Target breach demonstrated that the weakest link may be the security of building automation systems. Over half-a-billion dollars in expenses were incurred as a result of poor building automation security.

But of the lessons learned through this study, the most startling is that nation states are actively developing capabilities to attack critical infrastructure. The two Ukraine attacks taught us that it is indeed possible to damage a power grid through a cyber-attack. The various malware deployed by the GRIZZLEY STEPPE threat actors demonstrates that nation states have the resources to develop and deploy sophisticated attacks on critical infrastructure. Equally important is the fact that attackers are willing and able to conduct malicious, destructive attacks.

DHS conducted over 130 ICS cybersecurity assessments in 2017. The top six areas of weakness are provided in Table 3. Boundary protection was ranked as the most prevalent weakness and has been the top weakness since 2014. The risks from boundary protection vulnerabilities are: (1) undetected unauthorized activity in critical systems; and (2) weaker boundaries between ICS and enterprise networks.

Table 3. 2017 most prevalent weaknesses in industry [83].

Weakness Area	**Rank**	**Risk**
Boundary Protection	1	∗ Undetected unauthorized activity in critical systems. ∗ Weaker boundaries between ICS and enterprise networks.
Identification and Authentication (Organizational Users)	2	∗ Lack of accountability and traceability for user actions if an account is compromised. ∗ Increased difficulty in security accounts as personnel leave the organization, especially sensitive for users with administrative access.
Allocation of Resources	3	∗ No backup or alternate personnel to fill a position if the primary is unable to work. ∗ Loss of critical knowledge of control systems.
Physical Access Control	4	∗ Unauthorized physical access to field equipment and locations provides increased opportunity to: – Maliciously modify, delete, or copy device programs and firmware. – Access the ICS network. – Steal or vandalize cyber-assets. – Add rogue devices to capture and retransmit network traffic.
Account Management	5	∗ Compromised unsecured password communications. ∗ Password compromise could allow trusted unauthorized access to systems.
Least Functionality	6	∗ Increased vectors for malicious party access to critical systems. ∗ Rogue internal access established.

Figure 1. Reported ICS vulnerabilities [82].

There are basic cyber hygiene actions that industry can take to mitigate these risks [32], but more research is needed to help strengthen boundary protection in ICSs.

Figure 1 shows a ten-fold increase in ICS vulnerabilities reported to DHS. Although not all vulnerabilities are reported to DHS, this data is a good proxy in demonstrating the growth of vulnerabilities to ICSs. The increase in reported vulnerabilities has grown from approximately 48 in 2010 to 806 in 2017.

Figure 2. Trend in ICS cyber-attacks.

Figure 2 highlights the trend in ICS cyber-attacks. This notional graphic illustrates that both the quantity and complexity of cyber-attacks to ICSs are increasing. During this same time period, the complexity of cyber-attacks on ICSs has become more difficult to detect and mitigate.

4. Conclusion

The Internet of Things (IoTs) is the collection of devices and sensors in a network that create new and innovative capabilities. IoT devices are entrenched in our daily lives from the devices we wear to the vehicles we drive to the devices in our critical infrastructures. Because IoTs are an extension of ICSs, cybersecurity will become more complex and require even greater attention in order to protect critical infrastructure. The incidents described in this study highlight the changing landscape and growing threats to critical infrastructures.

The skill level of sophisticated threat actors is also increasing, as are the frequency of attacks targeting critical infrastructures and the systems that control them. Cyber threats are very real, and appropriate investments in cybersecurity should be made by the companies and municipalities that own or operate critical infrastructures. Many of the threat actors targeting ICSs have advanced skills and knowledge. The defenders of these systems need to have equally advanced skills and knowledge to protect our precious resources.

These experiences are a call to arms for critical infrastructure to prepare for and respond to cyber-attacks.

References

[1] S. Hong, *Wireless: From Marconi's Black-Box to the Audion*, MIT Press, Cambridge, London, England, 2001.

[2] N. Maskelyne, Electrical syntony and wireless telegraphy, *The Electrician*, 51, pp. 359–360, June 19, 1903.

[3] G. Hughes, The cyberspace invaders, *The Age*, (`www.theage.com.au/articles/2003/06/21/1056119529509.html`), June 22, 2003.

[4] M. Crawford, Utility hack led to security overhaul, *Computerworld*, (`www.computerworld.com/article/2561484/security0/utility-hack-led-to-security-overhaul.html`), February 16, 2006.

[5] T. Smith, Hacker jailed for revenge sewage attacks, *The Register*, (www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/), October 31, 2006.

[6] J. Slay and M. Miller, Lessons learned from the Maroochy water breach, in *Critical Infrastructure Protection*, Springer, Boston, Massachusetts, pp. 73–82, 2007.

[7] J. Riley, Mysterious 08 Turkey Pipeline blast opened new cyberwar, *Bloomberg*, (www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar), December 10, 2014.

[8] Newswire, 2008 Turkish Oil Pipeline explosion may have been Stuxnet precursor, *Newswire*, (www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor), December 10, 2014.

[9] B. Gourley, Most violent cyber attack noted to date: 2008 pipeline explosion caused by remote hacking, *CTOVision*, (www.ctovision.com/violent-cyber-attack-noted-date-2008-pipeline-explosion-caused-remote-hacking/), December 13, 2014.

[10] Hazardex, Russian hackers now thought to have caused 2008 Turkish Oil Pipeline explosion, *Hazardex*, (www.hazardexonthenet.net/article/88497/Russian-hackers-now-thought-to-have-caused-2008-Turkish-oil-pipeline-explosion.aspx), December 21, 2014.

[11] H. Tanriverdi, Die Tatwaffe fehlt (The murder weapon is missing), *Sueddeutsche Zeitung*, (www.sueddeutsche.de/muenchen/maxvorstadt-warten-auf-das-korrigierte-modifizierte-1.3812771), June 19, 2015.

[12] R. Lee, Closing the case on the reported 2008 Russian cyber attack on the BTC Pipeline, *SANS*, (ics.sans.org/blog/2015/06/19/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline), June 19, 2015.

[13] G. Keizer, Is Stuxnet the 'best' malware ever?, *Computerworld*, (www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the--best--malware-ever-.html), September 10, 2006.

[14] K. Zetter, An unprecedented look at Stuxnet: The world's first digital weapon, *Wired*, (www.wired.com/2014/11/countdown-to-zero-day-stuxnet/), November 3, 2014.

[15] D. Turner, Prepared Testimony and Statement for the Record of Dean Turner, *United States Senate Committee on Homeland Security and Governmental Affairs*, (www.hsgac.senate.gov/download/2010-11-17-turner-testimony-revised2), November 10, 2010.

[16] R. Langner, To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve, *Langner*, (www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf), November 2013.

[17] K. Zetter, How digital detectives deciphered Stuxnet: The most menacing malware in history, *Wired*, (www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/), November 7, 2011.

[18] ICS-CERT, Advisory (ICSA-10-238-01B): Stuxnet malware mitigation, *ICS-CERT*, (ics-cert.us-cert.gov/advisories/ICSA-10-238-01B), September 15, 2010.

[19] McAfee, Global energy cyberattacks: Night Dragon, *McAfee*, (www.heartland.org/_template-assets/documents/publications/29423.pdf), February 10, 2011.

[20] ICS-CERT, Advisory (ICSA-11-041-01A): McAfee Night Dragon report, *ICS-CERT*, (ics-cert.us-cert.gov/advisories/ICSA-11-041-01A), February 11, 2011.

[21] B. Bencsath, Duqu, Flame, Gauss: Followers of Stuxnet, *RSA*, (www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf), October 10, 2012.

[22] K. Zetter, Attackers stole certificate from Foxconn to hack Kaspersky with Duqu 2.0, *Wired*, (www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/), June 15, 2015.

[23] Symantec, W32.Duqu: The precursor to the next Stuxnet, *Symantec*, (www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf), November 23, 2011.

[24] Kaspersky, Resource 207: Kaspersky Lab research proves that Stuxnet and Flame developers are connected, *Kaspersky*, (www.kaspersky.com/about/press-releases/2012_resource-207-kaspersky-lab-research-proves-that-stuxnet-and-flame-developers-are-connected), June 11, 2012.

[25] ICS-CERT, Joint Security Awareness Report (JSAR-11-312-01): W32. Duqu-malware, *ICS-CERT*, (ics-cert.us-cert.gov/jsar/JSAR-11-312-01), December 12, 2011.

[26] Kaspersky, Gauss: Abnormal distribution, *KasperskyContentHub*, (www.kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf), August 8, 2012.

[27] ICS-CERT, JSAR-12-151-01A: sKyWIper/Flame information-stealing malware, *ICS-CERT*, (ics-cert.us-cert.gov/jsar/JSAR-12-151-01A), June 5, 2012.

[28] ICS-CERT, JSAR-12-222-01: Gauss information-stealing malware, *ICS-CERT*, (ics-cert.us-cert.gov/jsar/JSAR-12-222-01), August 9, 2012.

[29] Lockheed Martin, The Cyber Kill Chain, *Lockheed Martin*, (www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html), n.d.

[30] ICS-CERT, Gas pipeline cyber intrusion campaign, *ICS-CERT Monthly Monitor*, (ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr2012.pdf), April 2012.

[31] ICS-CERT, Gas pipeline cyber intrusion campaignupdate, *ICS-CERT Monthly Monitor*, (ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jun-Jul2012.pdf), June-July 2012.

[32] ICS-CERT, Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies, *ICS-CERT*, (ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf), September 2016.

[33] A. Ozment and G. Touhill, DHS works with critical infrastructure owners and operators to raise awareness of cyber threats, *DHS*, (www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats), March 7, 2016.

[34] N. Perlroth, In cyberattack on Saudi firm, U.S. sees Iran firing back, *The New York Times*, (www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html), October 23, 2012.

[35] Symantec, The Shamoon attacks, *Symantec*, (www.symantec.com/connect/blogs/shamoon-attacks), August 16, 2011.

[36] ICS-CERT, JSAR-12-241-01B: Shamoon/DistTrack malware, *ICS-CERT*, (ics-cert.us-cert.gov/jsar/JSAR-12-241-01B), October 16, 2012.

[37] K. Zetter, Qatari gas company hit with virus in wave of attacks on energy companies, *Wired*, (www.wired.com/2012/08/hack-attack-strikes-rasgas/), August 30, 2012.

[38] ICS-CERT, ICS-TIP-15-022-01: Best practices for Continuity of Operations (Handling destructive malware), *ICS-CERT*, (ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01), January 22, 2015.

[39] D. Yardon, Before Target, they hacked the heating guy, *Wall Street Journal*, (blogs.wsj.com/digits/2014/02/05/before-target-they-hacked-the-heating-guy/), February 5, 2014.

[40] B. Krebs, Target hackers broke in via HVAC company, *Krebs on Security*, (krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/), February 14, 2014.

[41] US-CERT, POS malware technical analysis: Indicators for network defenders, Department of Homeland Security, Washington DC, USA, 2014.

[42] iSIGHT, ModPoS: Malware behavior, capabilities and communications, *iSIGHTpartners.com*, (info.isightpartners.com/ModPOS-malware-disclosure-report), November 24, 2015.

[43] K. Zetter, The malware that duped Target has been found, *Wired*, (www.wired.com/2014/01/target-malware-identified/), January 16, 2014.

[44] V. Lynch, Cost of 2013 Target data breach nears $300 million, *SSl Store*, (www.thesslstore.com/blog/2013-target-data-breach-settled/), May 26, 2017.

[45] S. Prokupecz, T. Kopan, and S. Moghe, Former official: Iranians hacked into New York dam, *CNN*, (www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html), December 22, 2015.

[46] J. Berger, A dam, small and unsung, is caught up in an Iranian hacking case, *The New York Times*, (www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html), March 25, 2016.

[47] United States District Court, Southern District of New York, Sealed indictment: Conspiracy to commit computer hacking – ITSEC Team, New York, NY, USA, 2016.

[48] US-CERT, GRIZZLY STEPPE – Russian malicious cyber activity: An FBI and NCCIC Joint Analysis Report, *US-CERT*, (us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY_STEPPE-2016-1229.pdf), December 29, 2016.

[49] ICS-CERT, Advisory (ICSA-14-178-01): ICS focused malware, *ICS-CERT*, (ics-cert.us-cert.gov/advisories/ICSA-14-178-01), June 30, 2014.

[50] BSI, Die Lage der IT-Sicherheit in Deutschland 2014 (The State of IT Security in Germany 2014), Bonn, Germany, 2014.

[51] R. Lee, M. Assante, and T. Conway, German steel mill cyber attack, *SANS*, (ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf), December 30, 2014.

[52] ICS-CERT, Alert (ICS-ALERT-14-281-01E): Ongoing sophisticated malware campaign compromising ICS, *ICS-CERT*, (ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B), December 10, 2014.

[53] Symantec, Emerging threat: Dragonfly (or) Energetic Bear – APT group, *Symantec*, (www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group), June 30, 2014.

[54] K. Higgins, 'Energetic Bear' under the microscope, *Dark Reading*, (www.darkreading.com/attacks-breaches/energetic-bear-under-the-microscope/d/d-id/1297712?), June 30, 2014.

[55] P. Polityuk, Ukraine to probe suspected Russian cyber attack on grid, *Reuters*, (www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231), December 31, 2015.

[56] K. Zetter, Everything we know about Ukraines power plant hack, *Wired*, (www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/), January 20, 2016.

[57] K. Zetter, Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired*, (www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/), March 3, 2016.

[58] N. Zinets, Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar', *Reuters*, (www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC), December 29, 2016.

[59] DHS/FBI Alert (TA17-293A): Advanced persistent threat activity targeting energy and other critical infrastructure sectors, *US-CERT*, (us-cert.gov/ncas/alerts/TA17-293A), October 20, 2017.

[60] Verizon, Data breach digest: Scenarios from the field, *Verizon*, (www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf), March 2016.

[61] S. Chan, Cyberattacks strike Saudi Arabia, harming aviation agency, *The New York Times*, (www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html), December 1, 2016.

[62] Symantec, Shamoon: Multi-staged destructive attacks limited to specific targets, *Symantec*, (www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets), February 27, 2017.

[63] J. Cox, Department of Defense warns contractors about Iran-linked malware, *Motherboard*, (www.motherboard.vice.com/en_us/article/ezp7j7/department-of-defense-warns-contractors-about-iran-linked-malware), December 16, 2016.

[64] R. Lee, M. Assante, and T. Conway, Analysis of the cyber attack on the Ukrainian power grid, *NERC*, (nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf), March 18, 2016.

[65] Dragos, CRASHOVERRIDE: Analysis of the threat to electric grid operations, *Dragos*, (www.dragos.com/blog/crashoverride/CrashOverride-01.pdf), June 12, 2017.

[66] A. Cherepanov, WIN32/INDUSTROYER: A new threat for industrial control systems, *Welivesecurity*, (www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf), June 12, 2017.

[67] DHS, Alert (TA17-163A): CRASHOVERRIDE malware, *US-CERT*, (www.us-cert.gov/ncas/alerts/TA17-163A), June 12, 2017.

[68] J. O'Leary, J. Kimble, and N. Fraser, Insights into Iranian cyber espionage: APT33 targets aerospace and energy sectors and has ties to destructive malware, *FireEye*, (www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html), September 20, 2017.

[69] J. Fruhlinger, Petya ransomware and NotPetya malware: What you need to know now, *CSOonline*, (www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html), October 17, 2017.

[70] ICS-CERT, Alert (ICS-ALERT-17-181-01C): Petya malware variant, *ICS-CERT*, (ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C), June 30, 2017.

[71] A. McLean, Australia also points finger at Russia for NotPetya, *ZDnet*, (www.zdnet.com/article/australia-also-points-finger-at-russia-for-notpetya/), February 15, 2018.

[72] The White House, Statement from the Press Secretary, *FireEye*, (www.whitehouse.gov/briefings-statements/statement-press-secretary-25/), February 18, 2018.

[73] D. Volz and S. Young, White House blames Russia for 'reckless' NotPetya cyber attack, *Reuters*, (www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ), February 15, 2018.

[74] GOV.UK, Foreign Office Minister condemns Russia for NotPetya attacks, *GOV.UK*, (www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks), February 15, 2018.

[75] Reuters Staff, Kremlin rejects U.S. accusation that Russia is behind cyber attack, *Reuters*, (www.reuters.com/article/us-britain-russia-cyber/kremlin-rejects-u-s-accusation-that-russia-is-behind-cyber-attack-idUSKCN1G00TM), February 16, 2018.

[76] TASS Staff, Kremlin slams 'Russophobic' allegations that pin NotPetya cyber attack on Russia, *GOV.UK*, (www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks), February 15, 2018.

[77] Symantec, Dragonfly: Western energy sector targeted by sophisticated attack group, *Symantec*, (www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks), October 20, 2017.

[78] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer, Attackers deploy new ICS attack framework 'TRITON' and cause operational disruption to critical infrastructure, *FireEye*, (www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html), December 14, 2017.

[79] Symantec, Triton: New malware threatens industrial safety systems, *Symantec*, (www.symantec.com/blogs/threat-intelligence/triton-malware-ics), December 14, 2017.

[80] ICS-CERT, MAR-17-352-01, Hatmansafety system targeted malware, *ICS-CERT*, (ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-

01_HatManSafety_System_Targeted_Malware_S508C), December 18, 2017.

[81] Dragos, TRISIS malware: Analysis of safety system targeted malware, *Dragos*, (www.dragos.com/blog/trisis/TRISIS-01.pdf), December 13, 2017.

[82] NCCIC, 2017 ICS-CERT Annual Vulnerability Coordination, Department of Homeland Security, Washington DC, USA, 2017.

[83] ICS-CERT, FY-2017 most prevalent weaknesses, *ICS-CERT Monthly Monitor*, (ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf), November-December 2017.