Chapter 12

# A HISTORY OF CYBER INCIDENTS AND THREATS INVOLVING INDUSTRIAL CONTROL SYSTEMS

Kevin Hemsley and Ronald Fisher

**Abstract** For many years, malicious cyber actors have been targeting the industrial control systems that manage critical infrastructure assets. Most of these events are not reported to the public and their details along with their associated threats are not as well-known as those involving enterprise (information technology) systems. This chapter presents an analysis of publicly-reported cyber incidents involving critical infrastructure assets. The list of incidents is by no means comprehensive. Nevertheless, the analysis provides valuable insights into industrial control system threats and vulnerabilities, and demonstrates the increasing trends in the number and complexity of cyber attacks.

**Keywords:** Industrial control systems, cyber security, incidents, threats, trends

## 1. Introduction

Industrial control systems are embedded devices that operate critical infrastructure assets. These devices are typically unique to operational technology as opposed traditional (enterprise) information technology. This chapter describes the significant incidents involving industrial control systems along with their threats and vulnerabilities, and demonstrates the increasing trends in the number and complexity of attacks.

Cyber threats on industrial control systems manifest themselves in several ways. This chapter discusses the principal types of threats, which include directed attacks, malware attacks, cyber intrusion campaigns and cyber threat group activities.

Tables 1 and 2 detail the significant cyber incidents involving industrial control systems that are referenced in this study. The threat types, which include directed attacks, malware attacks, cyber intrusion campaigns and cyber threat group activities, are presented in chronological order. The open-source analy-

*Table 1.* Industrial control system incidents.

| Year | Type | Name | Description |
|---|---|---|---|
| 1903 | Attack | Marconi wireless hack | Marconi's wireless telegraph presentation was hacked using Morse code. |
| 2000 | Attack | Maroochy Water Services breach | Wireless attack released more than 265,000 gallons of untreated sewage. |
| 2008 | Attack | Turkish pipeline explosion | Attackers may have exploited vulnerable security camera software to access the pipeline control network. |
| 2010 | Malware | Stuxnet malware | World's first publicly-known digital weapon. |
| 2010 | Malware | Night Dragon malware | Attackers used sophisticated malware to target global oil, energy and petrochemical companies. |
| 2011 | Malware | Duqu/Flame/ Gauss malware | Advanced malware that targeted specific organizations, including industrial control system vendors. |
| 2012 | Campaign | Gas pipeline cyber intrusion campaign | Active series of cyber intrusions that targeted the natural gas pipeline sector. |
| 2012 | Malware | Shamoon malware | Malware targeted major energy companies in the Middle East, including Saudi Aramco and RasGas. |
| 2013 | Attack | Target Stores attack | Hackers gained access to Target's sensitive financial systems via a contractor that maintained its HVAC industrial control systems. |
| 2013 | Attack | New York dam attack | U.S. Justice Department claimed that Iran conducted a cyber attack on the Bowman Dam in Rye Brook, NY. |
| 2013 | Malware | Havex malware | Malware attacks targeted industrial control systems. |

sis is based on information provided by cyber security companies, independent security researchers, news media, published reports and government sources.

Attribution of attacks, as discussed in the open-source literature, is included for reader awareness. The list of incidents is by no means comprehensive. However, it covers the most significant incidents that have impacted industrial control systems and critical infrastructure assets. In some cases, the attacks focused directly on industrial control systems. In other cases, industrial control systems were indirectly targeted or impacted.

## 2. Cyber Incidents

This section discusses the cyber incidents listed in Tables 1 and 2. The incidents are discussed in chronological order.

*Table 2.* Industrial control system incidents (continued).

| Year | Type | Name | Description |
|---|---|---|---|
| 2014 | Attack | German steel mill attack | Cyber attack on a steel mill caused massive damage. |
| 2014 | Malware | BlackEnergy malware | Malware targeted human-machine interfaces of control systems. |
| 2014 | Campaign | Dragonfly/Energetic Bear campaign no. 1 | Ongoing cyber espionage campaign mainly targeting the energy sector. |
| 2015 | Attack | Ukraine power grid attack no. 1 | First successful cyber attack on a country's power grid. |
| 2016 | Attack | Kemuri Water Company attack | Attackers accessed programmable logic controllers and altered water treatment chemicals. |
| 2016 | Malware | Return of Shamoon malware | Thousands of computers at Saudi Arabia's civil aviation agency and at Gulf State organizations were wiped in another Shamoon attack. |
| 2016 | Attack | Ukraine power grid attack no. 2 | Attackers tripped breakers in 30 substations, turning off electricity to approximately 225,000 customers. |
| 2017 | Malware | CRASHOVERRIDE malware | Malware that caused the Ukraine power outage was finally identified. |
| 2017 | Group | APT33 Group campaign | Cyber espionage group targeted the aviation and energy sectors. |
| 2017 | Attack | NotPetya malware | Malware targeted Ukraine by posing as ransomware, but there was no way to pay ransom to decrypt files. |
| 2017 | Campaign | Dragonfly/Energetic Bear campaign no. 2 | Symantec claimed that the energy sector was being targeted. |
| 2017 | Malware | TRITON/Trisis/ HatMan malware | Malware targeted industrial safety systems in the Middle East. |

## 2.1 Marconi Wireless Hack

The world's first cyber incident likely involved the hacking of secure wireless communications. In 1903, the Italian radio pioneer, Guglielmo Marconi, prepared to present the first public demonstration of long-distance wireless communications using Morse code. The live demonstration intended to show that a wireless message could be sent securely from a cliff-top radio station in Poldhu, Cornwall (United Kingdom) to London, some 300 miles away.

However, before Marconi could begin his demonstration, the theater's brass projection lantern that displayed his slides began to click. To an untrained ear, it probably sounded as if the projection system was having technical difficulties. However, Marconi's assistant, Arthur Blok, recognized that the clickity-click

coming from the lantern was Morse code [17]. The Morse code spelled out the following unexpected message:

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

The message went on to mock Marconi. The demonstration had been hacked! But it was not apparent who the mysterious hacker was and why he hacked Marconi's demonstration.

A few days later, a letter in *The Times* confessed to the hack [46]. The hacker was British music hall magician, Nevil Maskelyne. It turned 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.

Vulnerabilities in industrial control systems are often identified and reported by independent cyber security researchers. Nevil Maskelyne may well have been the first to publicly report a vulnerability in modern technology.

## 2.2 Maroochy Water Services Breach

In March 2000, Maroochy Water Services, a utility operated by 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 [18].

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

On April 23, 2001, police chased the automobile of 49-year-old Vitek Boden and ran him off the road. In his car, the police found a laptop and supervisory control and data acquisition (SCADA) equipment he had used to attack systems at Maroochy Water Services [6]. Investigations revealed that Boden's laptop was used when the attacks had occurred. Software for controlling the sewage management control system was discovered on his hard drive [60].

Boden had used a radio transmitter and his laptop to control some 150 sewage pumping stations. Over a three-month period, Boden released millions of gallons of untreated sewage into waterways and local parks [59]. The judge in the case ruled that the act was Boden's revenge for failing to obtain a security position with the Maroochy Shire Council [18].

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

- 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 [59].

The Maroochy Water Services breach is an example of a cyber attack that can be launched on an industrial control system to cause physical damage. In this (rare) case, the attacker was identified and prosecuted.

## 2.3 Turkish Pipeline Explosion

The 2008 Turkish pipeline explosion has been attributed to a cyber intrusion, but it was actually caused by a physical attack. In August 2008, a segment of the Baku-Tbilisi-Ceyhan (BTC) oil pipeline in Refahiye, eastern Turkey exploded during the Georgian War. Media reports attributed the explosion to a cyber nexus [14–16, 57].

Bloomberg [57] published the original report of the attack on December 10, 2014. However, a subsequent story in a major German newspaper casts significant doubt on a cyber attack causing the explosion [65]. An analysis by Lee [41] concludes that the pipeline explosion was not caused by cyber means. In fact, Lee notes "there are numerous reported and unreported cases of failures at [industrial control system] 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."

This event is included to make readers aware that this incident is often inaccurately cited as one of the first cyber incidents involving industrial control systems. It is also included to highlight the fact that cyber attribution for physical events can be difficult to ascertain.

## 2.4 Stuxnet Malware

When it was identified in 2010, Stuxnet was arguably the most sophisticated malware ever encountered [38]. It infected control system networks and may have damaged one-fifth of Iran's uranium hexafluoride centrifuges [79].

Turner [68], a Symantec executive, testified before the U.S. Senate Homeland Security Committee that Stuxnet was a wake-up call to critical infrastructure asset owners and operators around the world. Stuxnet reportedly targeted specific equipment operating in Iran's Natanz uranium enrichment facility [40, 76]. The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Team (ICS-CERT) issued multiple advisories about the Stuxnet malware, which also infected systems in the United States [22].

Stuxnet was dangerous because it self-replicated and spread throughout multiple systems via multiple means, which included:

- Removable drives by exploiting a vulnerability that allowed auto execution.
- Local-area networks (LANs) by exploiting a vulnerability in the Windows Print Spooler.
- Server Message Block (SMB), which provides 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 human-machine interface (HMI) database server by copying and executing itself.
- Siemens Step 7 by copying itself into Step 7 projects so that it automatically executed when a Step 7 project was loaded.

Stuxnet exploited four unpatched Microsoft vulnerabilities, two vulnerabilities for self-replication and two for privilege escalation. These vulnerabilities were previously unknown and are referred to as zero-day vulnerabilities.

One of Stuxnet's significant features was its ability to install itself without being detected. This was accomplished using digitally-signed code produced by legitimate software developers, which had been stolen from two Taiwanese companies. Stuxnet leveraged these digital certificates to contact a command and control (C2) server that enabled the attackers to download and execute updated code.

Stuxnet was also stealthy in that it hid its binaries using a Windows rootkit. It attempted to evade detection by altering several security products if they were found on the targeted system. It also hid modified code in Siemens programmable logic controllers via a rootkit of sorts. Additionally, it modified the data sent from programmable logic controllers so that the human-machine interface displayed incorrect information to plant operators, making them believe that the system was operating normally.

Stuxnet was a precision weapon that looked for specific software to compromise and specific equipment to target. It terminated itself if it did not find the software and equipment as it propagated. When Stuxnet found what it sought, it modified and sabotaged Siemens programmable logic controller code by injecting ladder logic code.

The important lesson learned from Stuxnet is that a well-financed, sophisticated threat actor can likely attack any system. The ability to detect and recover from a cyber attack is also an important takeaway. This is because it is not possible to protect a system from all attacks.

## 2.5 Night Dragon Malware

Night Dragon is the name given by McAfee to the tactics, techniques and procedures (TTPs) used in coordinated, covert and targeted cyber attacks that

were initiated in November 2009 and made public in 2010 [47]. The attackers in China utilized Night Dragon command and control servers in the United States and The Netherlands to target global oil, energy and petrochemical companies.

The attacks involved social engineering, spear-phishing, exploitation of Microsoft Windows operating system vulnerabilities, Microsoft Active Directory compromises and the use of remote access Trojans (RATs) in targeting and harvesting sensitive operations-related data and project-financing information about oil and gas field bids and operations [47].

McAfee [47] reported that after the attackers had control of a targeted system, they exfiltrated password hashes and used a common cracking tool to obtain the passwords and access sensitive information. The exfiltrated files related to operational oil and gas production systems as well as financial documents pertaining to oil and gas field exploration and bidding. In some cases, the files were copied to and downloaded from company web servers by the attackers. In other cases, the attackers collected data from SCADA systems.

ICS-CERT issued an initial alert in February 2011 to warn U.S. critical infrastructure asset owners and operators of the Night Dragon threat [21]. 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 compromise industrial control systems. Equally concerning is that the tools used by the attackers enabled them to take complete control of systems using remote desktop capabilities. The attackers leveraged the tools to steal valuable information, but they could just as easily have seized control of human-machine interfaces, which would have enabled them to remotely control critical energy systems.

## 2.6 Duqu/Flame/Gauss Malware

In 2011, Hungarian cyber security researchers with the Laboratory of Cryptography and Systems Security at the Budapest University of Technology and Economics discovered the Duqu malware during an incident response investigation [1]. The Duqu malware was designed to gather information. According to the Hungarian researchers, Duqu bears a striking similarity to Stuxnet in terms of its design philosophy, internal structure and mechanisms, implementation details and the estimated amount of effort needed to create it.

Duqu leveraged a stolen digital certificate from a Taiwanese company, just as Stuxnet did. In both cases, the stolen certificates enabled the attackers to install malware on target systems. In fact, the digital certificates used by Duku and Stuxnet were stolen from businesses located in the same industrial park in Taiwan [80].

According to reports published by Symantec [61] and Kaspersky Lab [36], the Duqu executables share some code with Stuxnet and were compiled after the last Stuxnet sample was recovered. Duqu attempted to disguise its transmissions as normal HTTP traffic by appending the encrypted data to be exfiltrated in a JPG file [31].

Working with other international researchers, the same Hungarian researchers who identified Duqu also identified the Flame or sKyWIper malware. According to the researchers [1], Flame is extremely complex malware that steals information using:

- Microphones installed on systems.
- Web cameras.
- Keystroke logging.
- Extraction of geolocation data from images.

Flame could send and receive commands and data via Bluetooth, and it stored the collected data in SQL databases. It used network connections and USB flash drives for communications. Flame-infected computers masqueraded as proxies for Windows Update using a fake Microsoft certificate and employed an advanced collision attack on the MD5 hash function [1]. Kaspersky Lab researchers also found chunks of code from a 2009 Stuxnet variant inside Flame [36].

Kaspersky Lab subsequently identified malware they named Gauss, which is believed to be related to Duqu and Flame because they all used the same framework [1, 37]. The Gauss malware was also designed to steal information. In particular, it collected the following information from compromised systems:

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

Gauss also infected USB drives with a spy module to propagate to and steal information from other computers. It interacted with command and control servers to download additional modules and to send the collected information back to the attackers. ICS-CERT issued the initial reports on Duqu [31], Flame [28] and Gauss [29] in 2012.

The important takeaway from the Duqu, Flame and Gauss malware infections is that sophisticated threat actors perform reconnaissance to collect as much information as they can to further their objectives. The attackers used a number of methods to spread their information-stealing code, and they leveraged all the available information to learn about their targets. It is important to emphasize that the first step in the "cyber kill chain" is reconnaissance [44]. Information-stealing malware such as Duqu, Flame and Gauss are used by sophisticated attackers to initiate their cyber kill chain.

## 2.7 Gas Pipeline Cyber Intrusion Campaign

Beginning in late December 2011, ICS-CERT [19] identified an active series of cyber intrusions by a sophisticated threat actor that targeted natural gas pipeline companies. Analysis of the malware and artifacts associated with the intrusions revealed that the activities were part of a single campaign that leveraged spear-phishing. The spear-phishing attempts tightly focused on key personnel in pipeline companies. The emails were carefully crafted to appear as if they were sent by trusted company employees [19].

ICS-CERT issued an alert (ICSA-12-136-01BP) to the U.S. Computer Emergency Readiness Team (US-CERT) Control Systems Center secure portal library about the threat; information about the attacks was also disseminated to sector organizations and agencies to ensure broad distribution to asset owners and operators [20]. ICS-CERT recommended the implementation of defense-in-depth mechanisms and practices, and educating users about social engineering and spear-phishing attacks [25]. Organizations were also encouraged to review an ICS-CERT incident handling brochure for tips on preparing for and responding to incidents.

ICS-CERT, in coordination with the Federal Bureau of Investigation (FBI), U.S. Department of Energy, Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Transportation Security Administration (TSA) and the Oil and Natural Gas and Pipelines Sector Coordinating Council's Cybersecurity Working Group, conducted a series of action campaign briefings during the 2013 fiscal year to respond to the growing number of cyber incidents involving U.S. critical infrastructure assets. Fourteen classified or unclassified briefings were given to more than 750 total attendees in cities across the country to assist critical infrastructure asset owners and operators in detecting intrusions and developing mitigation strategies [53]. These information sharing efforts made the energy sector more aware of the efforts undertaken by federal agencies to identify threats and help protect critical infrastructure assets.

## 2.8 Shamoon Malware

On August 15, 2012, the Shamoon 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 that they knew they could inflict the most damage – the day that more than 55,000 Saudi Aramco employees stayed home to prepare for one of Islam's holiest nights – Lailat al Qadr or the Night of Power, which celebrates the revelation of the Quran to Muhammad [54].

The Shamoon malware overwrote data and displayed an image of a burning American flag on more than 30,000 computers. Shamoon was designed to steal information, but it incorporated a destructive module that rendered infected systems unusable by overwriting the master boot record, partition tables and most of the files with random data. The overwritten information was not recoverable. Symantec discussed the malware in one of its official blogs on August 16, 2012 [62]. ICS-CERT also issued a report on the malware [30].

Eleven days later, on August 27, 2012, Shamoon hit its second target, the Qatari natural gas company, RasGas, which is one of the largest liquefied natural gas companies in the world [77]. Despite its destruction of tens of thousands of computers, there is no evidence that Shamoon directly impacted industrial control systems at Saudi Aramco or RasGas.

After infecting a computer, the Shamoon malware attempted to spread to other devices in the local network. Shamoon was programmed to download and run executables from a command and control server, enabling the attackers to manage operations, spread the infection and download additional tools on the victim computers for network traversal.

ICS-CERT [24] has provided guidance on best practices for continuity of operations when dealing with destructive malware like Shamoon. Saudi Aramco and RasGas learned the hard way that malicious actors can and do launch destructive attacks. A key takeaway from the Shamoon experience is that, in addition to protection, organizations must focus on recovering from destructive cyber attacks.

## 2.9 Target Stores Attack

Cyber intrusions into industrial control systems typically occur by attackers gaining access to corporate networks and then pivoting to control networks. However, the opposite occurred on November 15, 2013, when hackers broke into the computing network of a contractor that maintained Target's heating, ventilation and air conditioning (HVAC) control systems [75].

The cyber attackers, who sought to steal credit card data from Target Stores, first stole the login credentials of an HVAC contractor employee. This was accomplished by sending phishing emails. The victim was fooled by the email and clicked on the bait, enabling the installation of a variant of the Zeus banking Trojan, which provided the attackers with the login credentials needed to access the HVAC systems in Target Stores. Next, the attackers gained access to Target's business network from its building control systems, following which they uploaded malicious credit-card-stealing software to cash registers across Target's chain of stores [39].

According to a U.S. Department of Homeland Security report [9], the attack was part of a widespread operation that used the Trojan.POSRAM tool. The code is based on an earlier malicious tool called BlackPOS, which is believed to have been developed in Russia in 2013. However, the new variant was highly customized to evade detection by anti-virus programs [74, 78].

The breach exposed approximately 40 million debit and credit card accounts. Customer names, credit/debit card numbers, expiration dates and CVV data were stolen. Seventy million customers were affected. The attack itself, along with security upgrades and lawsuits, cost Target about $309 million [45]. Financial institutions whose debit/credit cards were targeted incurred $200 million in expenses.

The Target breach demonstrates the importance of securing building automation systems from cyber attacks.

## 2.10 New York Dam Attack

According to the U.S. Justice Department [56], Bowman Dam, a small dam near Rye Brook, New York was accessed by Iranian hackers in 2013. The intrusion was not sophisticated, but is believed to have been a test by the Iranians to see what systems they could access.

The Bowman Dam controls storm surges. Its SCADA system was connected to the Internet via a cellular modem. Fortunately, the SCADA system was undergoing maintenance at the time of the attack; thus, no control was possible, just status monitoring. In fact, since the dam merely functioned as a sluicegate for a small village, there was no significant threat to public safety.

Technical details of the Bowan Dam intrusion are deemed protected critical infrastructure information (PCII) and cannot be released to the public. However, it is believed that the dam was not specifically targeted. Its vulnerable Internet connection and lack of security controls were exploited by the opportunistic attackers to gain access [2]. A U.S. federal indictment disclosed that the attack was conducted by entities from ITSec Team and Mersad Company, two private computer security companies based in Iran [71]. These companies perform work for various Iranian Government organizations, including the Islamic Revolutionary Guard Corps (IRGC).

The attack on the Bowman Dam is a concern due to the country of origin of the attackers and the technical capabilities they demonstrated in directly manipulating SCADA equipment. It is possible that the Iranian attackers selected the small Bowman dam simply because it was low-hanging fruit. The important takeaway is that critical infrastructure control systems connected to the Internet are easy for potential attackers to detect and surveil, and eventually target.

## 2.11 Havex Malware

In 2013, a remote access Trojan named Havex (or Oldrea) that targeted industrial control systems was discovered. In 2016, the U.S. Department of Homeland Security and FBI released a report [10] that tied Havex to Russia's civilian and military intelligence services (RIS). The U.S. Government refers to this malicious activity as GRIZZLEY STEPPE; it also goes by the names Dragonfly and Energetic Bear.

Havex communicated with a command and control server that deployed modular payloads; this enabled the malware to acquire additional functionality. ICS-CERT identified and analyzed a payload that enumerated connected network resources such as computers and shared resources [23]‘. The Distributed Component Object Model (DCOM) based version of the Open Platform Communications (OPC) standard was leveraged to collect information about network resources and connected industrial control devices.

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 obtaining

generic OPC server information, the Havex payload could enumerate OPC tags. However, Havex was not without flaws. It caused multiple common OPC platforms to crash intermittently; ICS-CERT has issued a warning that this could disrupt applications reliant on OPC communications [23].

The major concerns regarding Havex are its connection to Russia's civilian and military intelligence services, and the fact that it is advanced malware that targeted industrial control systems used in U.S. critical infrastructure assets. Another concern is that its command and control infrastructure enables the malware to acquire unknown enhanced capabilities.

## 2.12 German Steel Mill Attack

The 2014 annual report of the German Federal Office for Information Security (Bundesamt fur Sicherheit in der Informationstechnik (BSI)) mentions an attack on an unspecified German steel mill [11]. According to BSI, the attack was carried out using spear-phishing and social engineering tactics. The attackers initially gained access to the corporate 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 shutting down in a controlled manner. This resulted in "massive damage to the plant."

The technical abilities of the attackers were described as "very advanced" [11]. Specifically, the attackers had expertise in information technology security as well as detailed knowledge of industrial control systems and the steel production process. The description in the BSI report and historical information about process plant incidents lead many to believe that the damage to the plant was intentional [42].

The German steel mill cyber attack is significant because of the physical damage that resulted and the German Government's willingness to release information about the incident. According to the BSI [11], "[t]he 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."

## 2.13 BlackEnergy Malware

Starting in 2014, ICS-CERT published a series of alerts describing a sophisticated malware campaign that had compromised numerous industrial control systems using a variant of the BlackEnergy malware [26]. The analysis indicated this campaign had been ongoing since at least 2011. The 2016 U.S. Department of Homeland Security and FBI Joint Analysis Report [10], which identified Havex as coming from Russia's civilian and military intelligence services (RIS) group, connected BlackEnergy to the group as well.

Human-machine interface products from multiple vendors were targeted by the malware, including GE Cimplicity, Advantech/Broadwin WebAccess and

Siemens WinCC. The malware was modular and all its functionality was not necessarily used to target its victims. Typical BlackEnergy infections involved searches for network-connected file shares and removable media that could aid the malware in moving laterally in the infected environment [26].

In December 2014, the U.S. Department of Homeland Security confirmed that a BlackEnergy 3 malware variant was present in a Ukrainian energy system that was attacked to cause a power outage. ICS-CERT published a special (TLP Amber) version of an alert containing additional information about the malware, plug-ins and indicators. ICS-CERT strongly encouraged infrastructure asset owners and operators to use the indicators to look for signs of compromise in their control system environments.

In December 2014, ICS-CERT partnered with the FBI to give classified and unclassified threat briefings to critical infrastructure stakeholders across the country. Teams from ICS-CERT and the FBI traveled to fifteen cities across the United States. In total, nearly 1,600 participants involved in critical infrastructure protection across all sixteen sectors attended the briefings.

Like Havex, BlackEnergy targeted important industrial control system products. It is a major concern when adversaries target control systems used in the critical infrastructure. The BlackEnergy malware provided valuable insights into nation state actors and the tools they use to target critical infrastructure assets.

## 2.14 Dragonfly/Energetic Bear Campaign No. 1

On June 30, 2014, Symantec's MSS Global Threat Response described an ongoing cyber espionage campaign dubbed Dragonfly [49]. Other reports refer to the same campaign as Energetic Bear or Crouching Yeti [34]. The Dragonfly campaign primarily targeted the energy sector. The campaign focused on espionage and persistent access, with sabotage as an optional capability. The malware used the Havex (or Oldrea) malware as its favored tool and the Karagany remote access Trojan as a secondary tool. The Symantec group said that it had observed attacker activity in the United States, Turkey and Switzerland; some traces were seen in other countries as well [49].

The 2014 Dragonfly campaign was assessed to be exploratory in nature, where the attackers focused on attempting to gain access to the networks of the targeted organizations [49]. Dragonfly/Energetic Bear were later identified by the U.S. Department of Homeland Security and FBI as being connected to the GRIZZLEY STEPPE malicious activity perpetrated by Russia's civilian and military intelligence services (RIS) [10].

## 2.15 Ukraine Power Grid Attack No. 1

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

Reuters reported that a power company located in western 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 about 230,000 people without electricity for up to six hours. SCADA equipment was rendered inoperable and power had to be restored manually, further delaying restoration efforts [81].

Investigators discovered that attackers used the BlackEnergy malware to exploit macros in Microsoft Excel documents. The malware was planted in the company's network using spear-phishing [82]. ICS-CERT and US-CERT worked with the Ukrainian CERT and other international partners to analyze the malware, and confirmed that a BlackEnergy 3 variant was present [26]. The Ukrainian intelligence community blamed the attack on Russian actors [83]. BlackEnergy has also been publicly identified by the U.S. Department of Homeland Security and FBI as being connected to the GRIZZLEY STEPPE malicious activity perpetrated by Russia's civilian and military intelligence services (RIS) [70].

At the request of the Ukrainian Government, a U.S. interagency team comprising representatives from ICS-CERT and US-CERT, the Department of Energy, FBI and North American Electric Reliability Corporation (NERC), traveled to Ukraine to gather information about the incident and identify potential mitigations [53].

The Ukraine attack showed the world that it is possible to damage the power grid through cyber means. It was also a wake-up call to fortify the U.S. power grid against attacks. In the case of the Ukraine attack, relatively unsophisticated techniques were used to good effect. Indeed, the Ukraine power grid attack of 2015 will go down as a significant event in cyber attack history.

## 2.16 Kemuri Water Company Attack

In 2016, Verizon reported that an undisclosed water company experienced a cyber attack on its industrial control systems [72]. Verizon gave the water company the fictitious name "Kemuri" to protect its identity. According to Verizon, attackers accessed the water district's valve and flow control application responsible for manipulating hundreds of programmable logic controllers that managed water treatment chemical processing. The attackers then manipulated the system to alter the amount of chemicals entering the water supply. This affected water treatment and production capabilities, causing water supply recovery times to increase.

According to Verizon, a hacktivist group with ties to Syria was behind the attack. The Kemuri breach could easily have been much worse. Verizon noted that if the actors had a little more time and a little more knowledge of the industrial control systems, Kemuri and the local community could have suffered serious consequences.

A key takeaway from the Kemuri attack is that Internet-facing industrial control systems are a bad practice that can place critical infrastructure assets

at serious risk. The Kemuri attack is also a reminder that malicious cyber actors are not afraid to cross the line and cause harm.

## 2.17 Return of Shamoon Malware

In November 2016, a second wave of attacks by the Shamoon malware was launched at selected targets in Saudi Arabia [3]. Thousands of computers in the Saudi Arabian civil aviation agency and other Gulf State organizations were wiped by Shamoon after it resurfaced some four years after attacking tens of thousands of Saudi Aramco and Qatari RasGas workstations.

Symantec discovered a strong correlation between the Timberworm cyber attack group and the Shamoon malware [63]. Timberworm appeared to have gained access to the networks of the targeted organizations weeks and, in some cases, months before the 2016 Shamoon attacks.

In December 2016, the U.S. Defense Security Service issued a security bulletin to cleared contractors warning them of the Shamoon malware [5].

The concern raised by the second Shamoon attack is the repeated use of destructive malware to target critical infrastructure assets. Critical infrastructure asset owners and operators need to be vigilant and bolster their defense postures. They must draw on the lessons learned from the Shamoon attacks to protect their assets.

## 2.18 Ukraine Power Grid Attack No. 2

On December 17, 2016, almost one year after Ukraine suffered a major cyber attack on its power grid, Kiev suddenly went dark. Cyber attackers had caused power grid monitoring stations to go blind. Breakers were then tripped in 30 substations, turning off electricity to approximately 225,000 customers.

To prolong the outage, the attackers launched a telephone denial-of-service attack against the utility's call center to prevent customers from reporting the outage; the same tactic was used in 2015. The intruders also rendered devices, such as serial-to-Ethernet converters, inoperable and unrecoverable to make it harder to restore electricity to customers [43]. Despite these setbacks, power was restored in three hours in most cases. However, because the attackers had sabotaged energy management systems, workers had to travel to the substations and manually close the circuit breakers that the attackers had opened remotely [81, 82].

The second Ukraine power grid attack was much more sophisticated than the first attack [43]. While the first attack used remote control software to manually trip breakers, the second attack leveraged sophisticated malware that directly manipulated SCADA systems. Lee [7], a Dragos expert, said, "[i]n 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."

The sophisticated malware used in the second attack is now referred to as CRASHOVERRIDE.

## 2.19 CRASHOVERRIDE Malware

Dragos [7], working with the Slovak anti-virus firm ESET [4], confirmed that the CRASHOVERRIDE (or Industroyer) malware was employed in the December 17, 2016 cyber attack on a Kiev, Ukraine transmission substation (Ukraine power grid attack no. 2 above).

According to the Dragos report [7], CRASHOVERRIDE was the first malware framework specifically designed and deployed to attack electric power grids. It is the fourth piece of malware tailored to target industrial control systems, with Stuxnet, BlackEnergy-2 and Havex being the first three. It is the second malware designed and deployed to disrupt industrial processes, with Stuxnet being the first [7]. The Dragos report also states that the CRASHOVERRIDE framework served no espionage purpose – its only real feature was to launch attacks that caused electric power outages.

The CRASHOVERRIDE malware framework has modules specific to industrial control protocol stacks, including IEC 101, IEC 104, IEC 61850 and OPC. It is designed to allow the inclusion of additional payloads such as DNP3, but as of this time, no such payloads have been confirmed. The malware also contains additional (non-control-system-specific) modules, such as a wiper, to delete files and disable processes on a running system in order to disrupt operations or damage equipment [7].

The CRASHOVERRIDE modules were leveraged to open circuit breakers on remote terminal units (RTUs) and force them into infinite loops in order to keep the breakers open. When power grid operators attempted to close the breakers, the substations were de-energized; thus, the breakers had to be closed manually to restore power [7].

According to the Dragos report [7], CRASHOVERRIDE could be leveraged to disrupt grid operations that would result in power outages. The power outages could last up to a few days if an attack targeted multiple sites. However, the report also mentions that there is no evidence that CRASHOVERRIDE could cause power outages to last longer than a few days. The extended outages could be achieved by targeting multiple sites simultaneously, which is entirely possible, but not easy.

On June 12, 2017, the U.S. Department of Homeland Security used the National Cyber Awareness System (NCAS) to issue a Technical Analysis Alert on June 12, 2017 that notified the U.S. critical infrastructure community about the serious threat posed by the CRASHOVERRIDE malware. The main takeaway from CRASHOVERRIDE is that a nation state actor has created an advanced reusable malware framework designed to cause power outages. This same threat actor has demonstrated on multiple occasions that it is willing and able to induce electric power outages via cyber means.

## 2.20 APT33 Group

In 2017, FireEye published a report detailing a cyber threat actor they named APT33 [52]. According to FireEye's analysis, APT33 is a capable group

that has conducted cyber espionage operations since at least 2013. FireEye assessed that APT33 works at the behest of the Iranian Government.

APT33 has shown particular interest in aviation sector companies involved in military and commercial projects, as well as energy sector companies with ties to petrochemical production. According to FireEye, the targeting of companies involved in energy and petrochemicals mirrors previous targeting by other suspected Iranian threat groups, indicating a common interest in the sectors across Iranian actors. The targeted countries include the United States, Saudi Arabia and South Korea. FireEye also warns that APT33 may have ties to other groups with destructive capabilities.

APT33 delivered its malware by leveraging spear-phishing emails sent to employees of the targeted companies. The emails included recruitment-themed lures with links to malicious HTML application (HTA) files that contained job descriptions and links to legitimate job postings on popular employment websites. The spear-phishing emails were very relevant and appeared to be legitimate – they referenced specific job opportunities and salaries, provided links to spoofed companies' employment websites, and even included the companies' equal opportunity hiring statements.

A major concern is that the APT33 attack group has significant capabilities and ties to the destructive Shamoon malware. The group is also tied to the SHAPESHIFT malware that can wipe disks, erase volumes and delete files. FireEye believes that some of the tools used by APT33 may be shared with other Iran-based threat actors.

## 2.21 NotPetya Malware

Also in 2017, malware posing as the Petya ransomware surfaced in Ukraine. The earlier Petya malware targeted Microsoft Windows systems. After a system was infected, the malware encrypted the filesystem and displayed a message demanding payment in Bitcoin in order to regain access. However, while the new malware appeared to be based on and functioned like the Petya ransomware, it was different. It encrypted data on a hard drive just like Petya, but there was no way to decrypt the data. Unlike the Petya malware, the encryption was permanent; therefore, the new malware was given the name "NotPetya."

NotPetya is destructive malware. It has been enhanced to spread widely and is believed to have specifically targeted Ukraine [13]. On June 30, 2017, ICS-CERT issued an alert that warned the U.S. critical infrastructure community about the NotPetya threat [27].

In February 2018, the U.S. Government blamed the Russian military for developing and releasing NotPetya, stating that it was "reckless" and caused billions of dollars in damage [48]; it also called NotPetya the "most destructive and costly cyber attack in history" [67, 73]. The U.K. and Australian Governments also identified the Russian Government as being responsible for NotPetya [12]. The Russian Government has denied these accusations of its involvement with the malware [33, 66].

NotPetya is a significant concern because the nation state responsible for the malware – as confirmed by intelligence agencies in three countries – has demonstrated its ability and willingness to conduct destructive cyber attacks against critical infrastructure assets. A statement by the White House Press Secretary says that NotPetya has caused billions of dollars in damage across Europe, Asia and the Americas [67].

## 2.22 Dragonfly/Energetic Bear Campaign No. 2

In October 2017, Symantec published a report claiming that the energy sector was being targeted by a sophisticated attack group it referred to as a version of Dragonfly [58]. This group was well resourced, with a range of malware tools at its disposal and capable of launching attacks via a number of vectors. Symantec referred to this new Dragonfly activity as Dragonfly 2.0. In a vicious attack campaign, Dragonfly 2.0 compromised a number of industrial control equipment vendors, infecting their software with a remote access Trojan.

The Dragonfly 2.0 campaign shows that attackers may be entering 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 the Symantec report [58], this group is interested in 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 can sabotage or gain control of industrial control systems.

On October 20, 2017, the U.S. Department of Homeland Security and FBI issued an initial alert about an advanced persistent threat that targeted government entities and organizations in the energy, nuclear, water, aviation and critical manufacturing sectors [70]. The alert described it as a multi-stage intrusion campaign that initially targeted low security and small networks, and then moved laterally to major networks and high value assets in the energy sector. Based on malware analysis and observed indicators of compromise, US-CERT has indicated with confidence that the campaign is still ongoing, and that the threat actors are actively pursuing their objectives over a long-term campaign [70].

The Dragonfly and Energetic Bear threat groups were publically identified by the U.S. Department of Homeland Security and FBI as being part of the same group they call GRIZZLEY STEPPE [70]. This information about Dragonfly reveals that the threat actor has continued its activities and that its capabilities have evolved. The Symantec Security Response Attack Investigation Team [58] states 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."

## 2.23 TRITON/Trisis/HatMan Malware

At the end of 2017, FireEye reported the existence of a new industrial control system attack framework called TRITON that was designed to disrupt critical

infrastructure operations [35]. The report claims that the malware targeted industrial safety systems in the Middle East. Symantec Security Response reported this malware in late 2017, but referred to it as Trisis [64]. In December 2017, ICS-CERT also reported the same malware, but gave it a third name, HatMan [32].

The malware targeted Schneider Electric's Triconex safety instrumented system by modifying in-memory firmware to add malicious functionality. Specifically, the malware enabled the attackers to read/modify memory contents and execute custom code on demand upon receiving specially-crafted network packets from the attackers [32], as well as execute additional code that disables, inhibits or modifies the ability of a process to fail safely. The malware is especially dangerous because it targets safety systems [64].

It important to note that the TRITON malware is narrowly targeted and likely does not pose an immediate threat to other Schneider Electric customers or products. However, its capabilities, methodologies and tradecraft could be replicated by other attackers. Thus, it poses another serious threat to industrial control systems and the critical infrastructure assets they manage [8].

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

## 3. Lessons Learned

The cyber events discussed in this chapter provide insights into the technical capabilities of key threat actors and how they have evolved. Their willingness to cause physical damage is significant.

Stuxnet was a game changer. This piece of malware demonstrated that the physical infrastructure can be significantly impacted – even destroyed – by cyber means. A key Stuxnet takeaway for critical infrastructure owners and operators is that a sophisticated and well-financed threat actor can likely attack any system it desires.

The cyber events demonstrate that several critical infrastructure assets have been attacked. The attacks are expected to increase in number and sophistication. Therefore, critical infrastructure owners and operators must develop the abilities to detect and recover from cyber attacks. Protecting all the systems in a large critical infrastructure asset from all attackers is not possible. Attacks such as Night Dragon reveal that simple techniques applied by a skillful and persistent adversary are enough to break into critical infrastructure assets, including vital energy sector assets.

The cyber events discussed above also provide visibility into the advanced techniques used in cyber attacks. The Duqu, Flame and Gauss malware demonstrate that sophisticated threat actors perform reconnaissance to collect as much information as possible to ensure success. It is especially important to understand that the first step in the cyber kill chain is reconnaissance [44].

*Table 3.* Most prevalent industry weaknesses (2017) [50].

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

Information-stealing malware – as exemplified by Duqu, Flame and Gauss – is how sophisticated attackers begin the cyber kill chain.

The Target breach demonstrates that one of the weakest links may be the security of building automation systems. More than half-a-billion dollars in costs were incurred as a result of poor building automation security.

The most important lesson is that nation states are actively developing capabilities to attack critical infrastructure assets. The two Ukraine attacks demonstrate that cyber attacks can disrupt and damage an electric power grid. GRIZZLEY STEPPE malicious activity perpetrated by Russia's civilian and military intelligence services (RIS) shows that nation states have the resources to develop and deploy sophisticated attacks on the critical infrastructure. Just

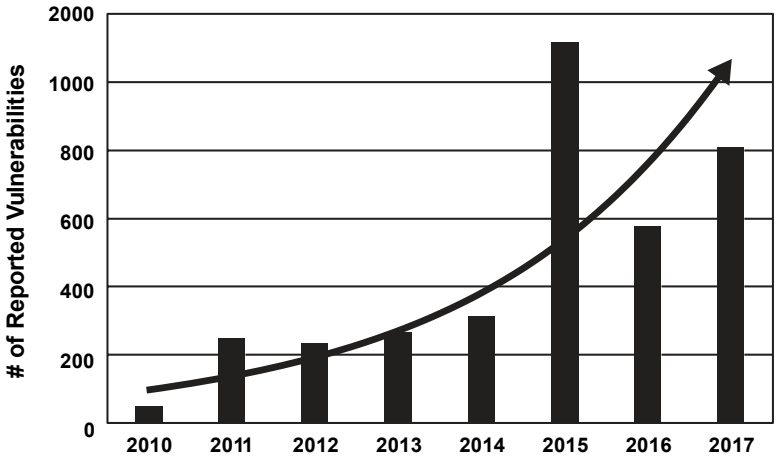


*Figure 1.* Reported industrial control system vulnerabilities [51].

as important is the fact that attackers are willing and able to launch destructive attacks.

The U.S. Department of Homeland Security conducted more than 130 industrial control system security assessments in 2017. Table 3 lists the top six areas of weakness. Boundary protection was ranked as the most prevalent weakness and has been the top weakness since 2014. The risks from boundary protection vulnerabilities are: (i) undetected unauthorized activity in critical systems; and (ii) weak boundaries between industrial control networks and enterprise networks.

Critical infrastructure asset owners and operators can undertake basic cyber hygiene actions to mitigate the risks [25]. However, more research and development efforts are needed to strengthen boundary protection for industrial control systems.

Figure 1 shows the number of industrial control system vulnerabilities reported annually to the U.S. Department of Homeland Security. Although not all vulnerabilities are reported to the U.S. Department of Homeland Security, the presented data is a good proxy for demonstrating the growth of industrial control system vulnerabilities. The massive increase in reported vulnerabilities from approximately 48 in 2010 to 806 in 2017 underscores the need to focus on protection as well as mitigation of the negative impacts of attacks.

Figure 2 highlights the trends in cyber attacks on industrial control systems. The notional graphic illustrates that the number and complexity of cyber attacks on industrial control systems are increasing. The increased complexity of cyber attacks makes them more difficult to detect and mitigate.

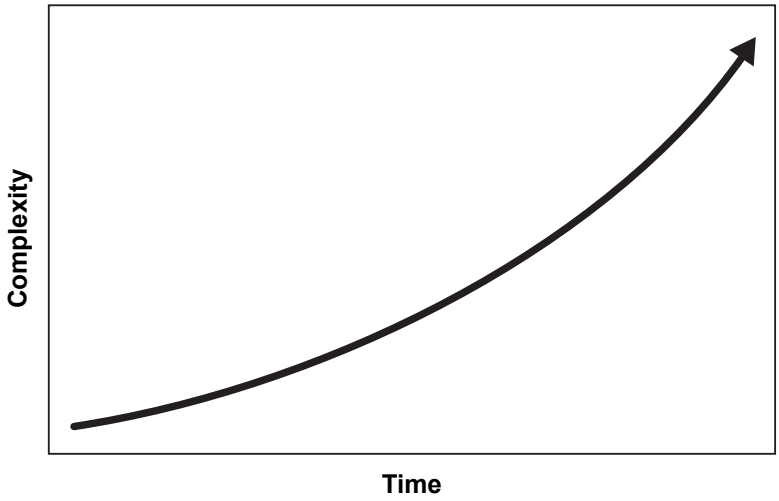


*Figure 2.* Trends in industrial control system cyber attacks.

## 4. Conclusions

The analysis of publicly-reported cyber incidents involving critical infrastructure assets provides valuable insights into industrial control system threats and vulnerabilities. Also, it highlights the changing landscape and growing threats to industrial control systems and, by extension, the critical infrastructure. The skill level of sophisticated threat actors is also increasing as is the frequency of attacks targeting critical infrastructures and the systems that control them.

Cyber threats are very real and appropriate investments in cyber security should be made by critical infrastructure asset owners and operators. Many of the threat actors targeting industrial control systems are well resourced and have advanced skills and knowledge. The defenders of these systems must have adequate resources as well as advanced skills and knowledge to prepare for and respond to cyber attacks.

Critical infrastructure protection, already an urgent problem in our time, will be compounded as the Internet of Things increases its penetration. The Internet of Things comprises ubiquitous networked devices – sensors and actuators – that support novel and innovative capabilities. These devices have become entrenched in our daily lives from the devices we wear to the vehicles we drive to the devices that manage critical infrastructure assets. Because Internet of Things systems are extensions of industrial control systems, cyber security will become more complex and require even greater attention to protect the critical infrastructure. This chapter is a call to arms to the critical infrastructure community to prepare for and respond to cyber attacks now and in the future.

## References

[1] B. Bencsath, Duqu, Flame, Gauss: Followers of Stuxnet, presented at the *RSA Conference Europe*, 2012.

[2] J. Berger, A dam, small and unsung, is caught up in an Iranian hacking case, *The New York Times*, March 25, 2016.

[3] S. Chan, Cyberattacks strike Saudi Arabia, harming aviation agency, *The New York Times*, December 1, 2016.

[4] A. Cherepanov, WIN32/INDUSTROYER: A New Threat for Industrial Control Systems, Version 2017-06-12, ESET, Bratislava, Slovakia (`www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf`), 2017.

[5] J. Cox, Department of Defense warns contractors about Iran-linked malware, *Motherboard*, December 16, 2016.

[6] M. Crawford, Utility hack led to security overhaul, *Computerworld*, February 16, 2006.

[7] Dragos, CRASHOVERRIDE: Analysis of the threat to electric grid operations, Hanover, Maryland (`www.dragos.com/blog/crashoverride/CrashOverride-01.pdf`), 2017.

[8] Dragos, TRISIS malware: Analysis of safety system targeted malware, Hanover, Maryland (`www.dragos.com/blog/trisis/TRISIS-01.pdf`), 2017.

[9] Department of Homeland Security (DHS), Backoff: New Point of Sale Malware, Washington, DC, 2014.

[10] Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), Joint Analysis Report (JAR-16-20296A): GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.

[11] Federal Office for Information Security, The State of IT Security in Germany 2014, BSI-LB15503e, Bonn, Germany, 2014.

[12] Foreign and Commonwealth Office, National Cyber Security Centre and Lord Ahmad of Wimbledon, Foreign Office minister condemns Russia for NotPetya attacks, News Story, London, United Kingdom, February 15, 2018.

[13] J. Fruhlinger, Petya ransomware and NotPetya malware: What you need to know now, *CSO*, October 17, 2017.

[14] B. Gourley, Most violent cyber attack noted to date: 2008 pipeline explosion caused by remote hacking, *CTOvision.com*, December 13, 2014.

[15] HazardEx, Russian hackers now thought to have caused 2008 Turkish oil pipeline explosion, Tonbridge, United Kingdom, December 21, 2014.

[16] Homeland Security News Wire, 2008 Turkish oil pipeline explosion may have been Stuxnet precursor, Washington, DC, December 17, 2014.

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

[18] G. Hughes, The cyberspace invaders, *The Age*, June 22, 2003.

[19] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Gas pipeline cyber intrusion campaign, *ICS-CERT Monthly Monitor*, p. 1, April 2012.

[20] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Gas pipeline cyber intrusion campaign – Update, *ICS-CERT Monthly Monitor*, p. 1, June-July 2012.

[21] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Advisory (ICSA-11-041-01A), McAfee Night Dragon Report (Update A), Idaho Falls, Idaho, January 2, 2014.

[22] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Advisory (ICSA-100-238-01B), Stuxnet Malware Mitigation (Update B), Idaho Falls, Idaho, January 8, 2014.

[23] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Advisory (ICSA-14-178-01), ICS Focused Malware, Idaho Falls, Idaho, July 1, 2014.

[24] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Best Practices for Continuity of Operations (Handling Destructive Malware), Idaho Falls, Idaho, January 22, 2015.

[25] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Idaho Falls, Idaho, 2016.

[26] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Alert (ICS-ALERT-14-281-01E), Ongoing Sophisticated Malware Campaign Compromising ICS (Update E), Idaho Falls, Idaho, December 9, 2016.

[27] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Alert (ICS-ALERT-17-181-01C), Petya Malware Variant (Update C), Idaho Falls, Idaho, July 10, 2017.

[28] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Joint Security Awareness Report (JSAR-12-151-01A), sKyWIper/Flame Information-Stealing Malware (Update A), Idaho Falls, Idaho, April 18, 2017.

[29] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Joint Security Awareness Report (JSAR-12-222-01), Gauss Information-Stealing Malware, Idaho Falls, Idaho, April 18, 2017.

[30] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Joint Security Awareness Report (JSAR-12-241-01B), Shamoon/DistTrack Malware (Update B), Idaho Falls, Idaho, April 18, 2017.

[31] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Joint Security Awareness Report (JSAR-11-312-01): W32.Duqu-Malware, Idaho Falls, Idaho, April 18, 2017.

[32] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Analysis Report, Malware Analysis, MAR-17-352-01 HatMan – Safety System Targeted Malware (Update A), Idaho Falls, Idaho, April 10, 2018.

[33] P. Ivanova, Kremlin rejects U.S. accusation that Russia is behind cyber attack, *Reuters*, February 16, 2018.

[34] K. Jackson Higgins, "Energetic" Bear under the microscope, *Dark Reading*, July 31, 2014.

[35] 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, *Threat Research Blog*, FireEye, Milipitas, California, December 14, 2017.

[36] Kaspersky Lab, Resource 207: Kaspersky Lab research proves that Stuxnet and Flame developers are connected, Press Release, Woburn, Massachusetts, June 11, 2012.

[37] Kaspersky Lab, Kaspersky Lab discovers "Gauss" – A new complex cyber-threat designed to monitor online banking accounts, Press Release, Woburn, Massachusetts, August 9, 2012.

[38] G. Keizer, Is Stuxnet the "best" malware ever? *Computerworld*, September 16, 2010.

[39] B. Krebs, Target hackers broke in via HVAC company, *Krebs on Security*, February 14, 2014.

[40] R. Langner, To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, The Langner Group, Arlington, Virginia, 2013.

[41] R. Lee, Closing the case on the reported 2008 Russian cyber attack on the BTC pipeline, *SANS Industrial Control Systems Security Blog*, SANS Institute, Bethesda, Maryland, June 19, 2015.

[42] R. Lee, M. Assante and T. Conway, German Steel Mill Cyber Attack, ICS Defense Use Case (DUC), SANS Industrial Control Systems, SANS Institute, Bethesda, Maryland, 2014.

[43] R. Lee, M. Assante and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC), Washington, DC, 2016.

[44] Lockheed Martin, The cyber kill chain, Bethesda, Maryland (`www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html`), 2018.

[45] V. Lynch, Cost of 2013 Target data breach nears $300 million, *Hashed Out*, The SSl Store, St. Petersburg, Florida (`www.thesslstore.com/blog/2013-target-data-breach-settled`), May 26, 2017.

[46] N. Maskelyne, Electrical syntony and wireless telegraphy, *The Electrician*, vol. 51, pp. 357–360, 1903.

[47] McAfee, Global Energy Cyberattacks: Night Dragon, Version 1.4, White Paper, Santa Clara, California, 2011.

[48] A. McLean, Australia also points finger at Russia for NotPetya, *ZDNet*, February 15, 2018.

[49] MSS Global Threat Response, Emerging threat: Dragonfly/Energetic Bear – APT Group, *Symantec Official Blog*, Symantec, Mountain View, California, June 30, 2014.

[50] National Cybersecurity and Communications Integration Center (NCCIC), Fiscal year 2017 ICS assessment summary, *ICS-CERT Monitor*, pp. 3–5, November-December 2017.

[51] National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2017 ICS-CERT Annual Vulnerability Coordination Report, Department of Homeland Security, Washington, DC, 2017.

[52] J. O'Leary, J. Kimble, K. Vanderlee and N. Fraser, Insights into Iranian cyber espionage: APT33 targets aerospace and energy sectors and has ties to destructive malware, *Threat Research Blog*, FireEye, Milipitas, California, September 20, 2017.

[53] A. Ozment and G. Touhill, DHS works with critical infrastructure owners and operators to raise awareness of cyber threats, Public Statement, Department of Homeland Security, Washington, DC, March 7, 2016.

[54] N. Perlroth, In cyberattack on Saudi firm, U.S. sees Iran firing back, *The New York Times*, October 23, 2012.

[55] P. Polityuk, Ukraine to probe suspected Russian cyber attack on grid, *Reuters*, December 31, 2015.

[56] S. Prokupecz, T. Kopan and S. Moghe, Former official: Iranians hacked into New York dam, *CNN*, December 22, 2015.

[57] J. Robertson and J. Riley, Mysterious '08 Turkey pipeline blast opened new cyberwar, *Bloomberg*, December 10, 2014.

[58] Security Response Attack Investigation Team, Dragonfly: Western energy sector targeted by sophisticated attack group, *Threat Intelligence Blog*, Symantec, Mountain View, California, October 20, 2017.

[59] J. Slay and M. Miller, Lessons learned from the Maroochy Water breach, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Boston, Massachusetts, pp. 73–82, 2007.

[60] T. Smith, Hacker jailed for revenge sewage attacks, *The Register*, October 31, 2001.

[61] Symantec Security Response, W32.Duqu: The Precursor to the Next Stuxnet, Version 1.4, Symantec, Mountain View, California, 2011.

[62] Symantec Security Response, The Shamoon attacks, *Symantec Official Blog*, Symantec, Mountain View, California, August 16, 2012.

[63] Symantec Security Response, Shamoon: Multi-staged destructive attacks limited to specific targets, *Symantec Official Blog*, Symantec, Mountain View, California, February 27, 2017.

[64] Symantec Security Response, Triton: New malware threatens industrial safety systems, *Threat Intelligence Blog*, Symantec, Mountain View, California, December 14, 2017.

[65] H. Tanriverdi, Die Tatwaffe fehlt (The murder weapon is missing), *Sueddeutsche Zeitung*, June 19, 2015.

[66] TASS, Kremlin slams "Russophobic" allegations that pin NotPetya cyber attack on Russia, February 15, 2018.

[67] The White House, Statement from the Press Secretary, Washington, DC (`www.whitehouse.gov/briefings-statements/statement-press-secretary-25`), February 15, 2018.

[68] D. Turner, Prepared Testimony and Statement for the Record of Dean Turner, Director, Global Intelligence Network, Symantec Security Response, Symantec Corporation, Hearing on Securing Critical Infrastructure in the Age of Stuxnet, Committee on Homeland Security and Governmental Affairs, United States Senate, Washington, DC (`www.hsgac.senate.gov/download/2010-11-17-turner-testimony-revised2`), November 17, 2010.

[69] United States Computer Emergency Readiness Team (US-CERT), Alert (TA17-163A), CrashOverride Malware, Washington, DC, July 27, 2017.

[70] United States Computer Emergency Readiness Team (US-CERT), Alert (TA17-293A), Advanced Persistent Threat Targeting Energy and Other Critical Infrastructure Sectors, Washington, DC, March 15, 2018.

[71] United States District Court, Southern District of New York, Sealed Indictment: United States of America v. Ahmad Fathi et al., New York (`justice.gov/opa/file/834996/download`), 2016.

[72] Verizon, Data Breach Digest: Scenarios from the Field, New York, 2016.

[73] D. Volz and S. Young, White House blames Russia for "reckless" NotPetya cyber attack, *Reuters*, February 15, 2018.

[74] S. Ward, ModPoS: Highly-sophisticated, stealthy malware targeting U.S. PoS systems with high likelihood of broader campaigns, *Threat Research Blog*, FireEye, Milipitas, California, November 24, 2015.

[75] D. Yadron and P. Ziobro, Before Target, they hacked the heating guy, *The Wall Street Journal*, February 5, 2014.

[76] K. Zetter, How digital detectives deciphered Stuxnet, the most menacing malware in history, *Wired*, July 11, 2011.

[77] K. Zetter, Qatari gas company hit with virus in wave of attacks on energy companies, *Wired*, August 30, 2012.

[78] K. Zetter, The malware that duped Target has been found, *Wired*, January 16, 2014.

[79] K. Zetter, An unprecedented look at Stuxnet, the world's first digital weapon, *Wired*, November 3, 2014.

[80] K. Zetter, Attackers stole certificate from Foxconn to hack Kaspersky with Duqu 2.0, *Wired*, June 15, 2015.

[81] K. Zetter, Everything we know about Ukraine's power plant hack, *Wired*, January 20, 2016.

[82] K. Zetter, Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired*, March 3, 2016.

[83] N. Zinets, Ukraine hit by 6,500 hack attacks, sees Russian "cyberwar," December 29, 2016.