SAND2019-14527C

# ADVANCED MALWARE AND NUCLEAR POWER: PAST, PRESENT, AND FUTURE

C.C. LAMB
Sandia National Laboratories
Albuquerque, NM, USA
Email: cclamb@sandia.gov

R. E. FASANO
Sandia National Laboratories
Albuquerque, NM, USA

T. ORTIZ
Sandia National Laboratories
Albuquerque, NM, USA

**Abstract**

Malware techniques and practices are beginning to converge, creating a uniquely hazardous environment for critical infrastructure technology. Today, we are in an accelerating threat environment, where adversaries are leveraging a mature black market populated by criminal organizations with an unprecedented level of technical expertise. Recent developments include the mass exploitation of ransomware, the emergence of clear information sharing between advanced organizations and new criminal organizations, and the migration of malware into the business networks of nuclear power plants. The paper will outline current trends in malware developed for both information and operational technological environments. It will also cover notable campaigns in both environments, and extract from past behaviours likely future developments.

## 1. INTRODUCTION

Cybersecurity in nuclear power is difficult to manage, overall. It is expensive to implement, regardless of the regulatory regime a plant is under. Technical controls are challenging to profile in many cases, as digital failure modes can be both difficult to model and can have wider ranging consequences than typical physical failures. Furthermore, intrusion detection and prevention controls for industrial systems can be much more expensive to deploy, as well as purchase or build. As a result, insight into likely future attack approaches, goals, and techniques will be invaluable in guiding future cybersecurity investment.

In the first section of this paper, we examine noteworthy malware campaigns released over the past decade. We will identify key trends and areas of technical and procedural convergence between individual strains. We examine current techniques, tactics, and procedures from both operational and technical perspectives. In the second section, we conduct the same analysis over advanced malware strains that deliberately target industrial control systems. This includes older threats like Stuxnet and Flame, as well as new threats like Hatman and CrashOverride. The main thrust of these two sections is to clearly outline the evolution of today's general malware threats to establish a baseline of malware technical and procedural trending that we can compare with similar trends in advanced industrial malware strains. We then identify key trends in malware capabilities and outline the impact of these trends on nuclear power plants, their operators, and industrial system manufacturers.

Over the past 10 years, we have seen a remarkable change in malware sophistication and the adoption of new strategies by malware authors. These kinds of approaches are beginning to appear in industrial malware strains as well. Although there are clear similarities in how malware is developed and deployed when comparing general purpose and industrial malware strains, there are distinct differences as well that are beginning to emerge. Both these differences and similarities have profound implications for nuclear power plant protection.

## 2. NOTEABLE GENERAL PURPOSE MALWARE CAMPAIGNS AND TRENDS

Traditionally, general purpose malware has only affected devices that did not interfere with physical processes. Today the line between general purpose malware and industrial malware has begun to blur. In this

section, we will give a brief overview of some of the notable general-purpose malware campaigns and the trends associated with them. The initial release dates of each of the campaigns we discuss can be seen in Figure 1

In 2007, the ZeuS toolkit emerged [1]. This toolkit creates networks of credential-stealing trojans that run in the background of infected computers. These trojans can steal any private information an attacker specifies [1], [2]. ZeuS spreads through phishing, unintentional downloads, or by getting a user to click on an infected link [2]. In 2011, the source code for a second version of ZeuS was leaked leading to the creation of variants of ZeuS such as Citadel. The first two versions of ZeuS were built with a centralized command and control (C2) server [2], [3]. These C2 servers were trackable and could be shutdown. This lead to, in 2011, a decentralized version of ZeuS known as *GameOver ZeuS* or *P2P ZeuS* that was more resilient to centralized shutdown techniques [2], [3]. ZeuS avoids detection by applying obfuscation techniques like metamorphic encryption and custom code packers, and will re-encrypt itself during each infection to generate a new signature that cannot be detected by signature-based detection methods [3]. The ZeuS binary gains persistence by copying itself to a different directory and deleting the original binary [1]. P2P ZeuS includes other attack capabilities such as distributed denial-of-service (DDoS), malware dropping, and Bitcoin theft [2].

The first advanced persistent threats (APTs) to attack commercial entities was released in 2009 [4], [5]. Prior to 2009, government entities and the defence industry had been the main target of APTs. That changed with Operation Aurora. It targeted companies such as Google, Adobe, and other security and defence contractors to steal intellectual property (IP) and modify source code [5]. The attackers could modify source code to include hidden backdoors for exploitation in production releases of products [4]. Also, they could search through the stolen source code to find bugs and weaknesses they could exploit or try to pivot into other portions of the organizations' network [4], [5]. Aurora utilized phishing to get a targeted user to click on a malicious link from a "trusted" source. The link would lead the user to a website hosted in Taiwan where a malevolent JavaScript payload was downloaded and executed. This payload used a zero-day exploit for Internet Explorer and Adobe to download an executable disguised as an image. The executable would open a back door that connected to a C2 server. The attackers then had full access to the software configuration management (SCM) systems [4], [5]. Aurora showed that nation-state level actors were starting to shift their focus from just targeting governments entities and military industry to include commercial entities.

Early ransomware campaigns would extort its victims, threatening the release of sensitive or embarrassing information. It would also prevent users from using their computers as normal. Victims could use standard anti-virus software to get rid of the malware [6]. The CryptoLocker campaign took a different approach, encrypting individual files on infected computers and decrypting them if the victims paid a ransom [6], [7]. The invention of anonymous digital currency allowed these attackers to maintain some degree of privacy and extort their victims. The initial release of CryptoLocker in 2013 primarily targeted business professionals through fake customer complaint emails. The emails had an attached ZIP folder with executables that would encrypt files when opened. CryptoLocker would gain persistence on a machine by copying itself in the %AppData% or %LocalAppData% folders and then deleting the original file [6], [7]. CryptoLocker also creates a start-up service that would execute the malware even if the machine booted into "safe mode". Once the service is created and the original copy is deleted, it then attempts to connect to a C2 server, encrypts files on connected drives, and reveals itself to the host. CryptoLocker uses Microsoft's CryptoAPI to encrypt files instead of using a custom encryption [6].

In 2014, Emotet, which is like ZeuS, emerged. It originally started out as a baking trojan designed to steal financial information through man-in-the-browser (MITB) attacks. In the beginning, Emotet targeted a few banks and a small number of countries that could make the most revenue. In recent years, Emotet has shifted its focus to attack any and all businesses or countries [8]. This shift has led the evolution of Emotet to include capabilities such as malware dropping, brute force password cracking, phishing campaigns from infected hosts, and spreading laterally across networks [9]. Emotet evolved from a standard banking trojan to a malware distributor and botnet.

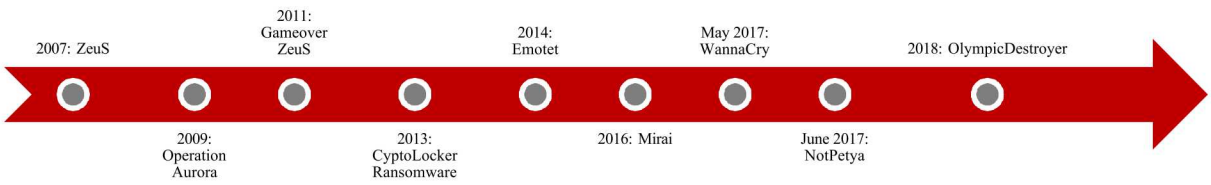


*FIG. 1. Timeline of Malwares Over the Last Decade*

Like Operation Aurora and ZeuS, Emotet infected hosts utilizing phishing. It used infected links, Microsoft Word documents with malicious macros, JavaScript, and PDFs to gain a foothold in victim machines [8], [9]. Emotet has avoided detection by incorporating a polymorphic packer, encrypted imports and function names, a multi-stage initialization process, and an encrypted C2 server [8]. Again, we see this pattern in the change of malware types from a banking trojan into a more fully-fledged platform for other functionality.

The Internet of Things (IoT) has been a topic of security concern in recent years. Mirai creates a botnet from vulnerable IoT devices. It was used on one of the most notable DDoS attacks on the DNS provider Dyn, which made websites such as GitHub, Twitter, Reddit, Netflix, and others inaccessible [10]. Mirai's source code is broken up into three parts: *bot*, *c2 server*, and *loader*. The *bot* portion will scan for IoT devices that have telnet remote access enabled using randomly generated IP addresses. Vulnerable devices are reported to the *loader* which will login to the device and install the malware payload. Then the payload is executed in RAM and deleted. Mirai does not achieve persistence like traditional malwares but gains persistence through disabling the devices watchdog timer so that it cannot restart unless the device is power cycled. Once the malware is running the bot will wait for DoS commands from the C2 server [10].

Also known as MS17-010, EternalBlue was a vulnerability in the Microsoft Windows Server Message Block (SMB) protocol leaked by a group known as the Shadow Brokers. It allowed attackers to infect an organization's entire network faster than any exploit had before it. In May 2017, the ransomware WannaCry was able to infect hundreds of thousands of computers in over 150 countries using EternalBlue as the primary attack vector [11], [12]. It took down the U.K. National Health Service hospitals and the Honda Motor Company in Japan [12]. WannaCry first attempts to use the EternalBlue exploit. If the exploit is successful, it will install the DoublePulsar backdoor allowing the attackers to access the infected machine and execute the ransomware payload. If EternalBlue fails and DoublePulsar is already installed, WannaCry will execute the payload through DoublePulsar. While WannaCry is infecting a host, it will scan the LAN of that host and the wider internet for potential victims [11]. WannaCry utilizes a custom encryption method using a root public/private RSA key pair, an RSA-2048 public/private key pair, and a randomly generated AES-128 encryption key for each file encrypted [13].

A month following WannaCry, the Ukraine was targeted by NotPetya. This malware was thought to originate from the GoldenEye variant of the Petya ransomware that would infect the master-boot record (MBR) to prevent a machine from booting properly [14]. However, NotPetya was actually a "wiper" disguised as ransomware [14], [15]. The authors of NotPetya used a corporate tax paying application (MEDoc), mandated by the Ukrainian government, as their initial infection vector. The authors of NotPetya were able to get admin credentials to gain root access and modify the software update configurations [14]. The authors pushed a "legitimate" software update that contained a hidden backdoor called "MeCom". MeCom allowed the attackers to infiltrate the machines to overwrite and encrypt sections of hard drives and C: drives. MeCom also allowed NotPetya to propagate across all the organizations' networks that were using MEDoc through the same SMB EternalBlue and EternalRomance exploits used in WannaCry [14]. If these SMB exploits failed, the attackers would use credentials taken from the first infected machine to attempt to spread through the network. Once NotPetya harvested credentials and had escalated authority, the computer would be scheduled for a shutdown. On reboot users would find that their files and the MBR had been encrypted and could only be accessed if they paid the ransom [14], [16]. The authors utilized a random generation function for encryption which meant that any encrypted data was lost immediately after encryption [14], [16].

The last malware campaign we will discuss is Olympic Destroyer (OD). OD targeted the Winter Olympic Games in PeyongChang, South Korea. Like NotPetya, OD was a wiper and had a credential harvesting module used for post-exploitation [17], [18]. The difference was that OD would update itself with newly captured credentials before spreading to other computers. This improved its ability to propagate to other machines and stay hidden as each time the credential list was updated with new credentials the hash used for detection would change [18]. OD also differed from NotPetya as it did not aim to destroy data on local machines. Instead it would only wipe data on network drives, disable services in Windows, and change boot system configurations to stop a system from booting [18]. The initial infection vector of OD is currently not known.

## 3. NOTEABLE INDUSTRIAL MALWARE CAMPAIGNS AND TRENDS

The primary difference between industrial and general malware is that industrial malware focuses on impacting a physical process, while historically general malwares have not [19], [20]. Industrial malware has been defined in the past decade mainly by four attacks: Stuxnet, Shamoon, CrashOverride, and Hatman. These attacks represent rigorous malware campaigns by advanced persistent threats (APTs) to act on geopolitical goals, cause economic damage, or to serve as a deterrent by targeting critical infrastructure [21]. Recently however, as less technically advanced cybercriminals learn the tradecraft used by APTs to target operation technology (OT) networks and the emergence of MaaS, there is an emerging trend of lower level threat attackers targeting OT networks [19]. Nation states, cybercriminal, and hacktivists groups have different goals and forensic analysis of malware can, in most cases, show the distinction between these threat actors. An increasing trend of shared code bases in malware is complicating attribution. Similarly, with an increased reliance on cloud computing, IoT, and automation the distinction between general purpose malware and industrial malware is beginning to blur. In this section, we will review the Stuxnet, Shamoon, CrashOverride, and Hatman malwares with an eye toward emerging trends in industrial malware. Although Shamoon did not specifically target Aramco's OT network, by executing a denial of service attack against Aramco's IT networks the industrial process was in effect compromised [22].


*FIG.2. Timeline of Industrial Malwares Over the Last Decade*

The first state of the OT cyber kill chain, or any malware campaign, is to prepare to infiltrate a system by conducting reconnaissance and characterizing the attack surface [23]. Depending on the desired outcome of the malware campaign different approaches will be taken at the reconnaissance stage. For example, the primary goal of Stuxnet was to sabotage the Iranian Natanz nuclear enrichment facility without alerting operators that the system had been compromised. To accomplish the desired outcome the developers of Stuxnet not only had to have complete knowledge of the Natanz facility, but an adequate testing environment built to exact specifications [24]. Shamoon on the other hand did not need to have the same level of detailed reconnaissance to accomplish its intended attack against Aramco.

| Malware Name | Associated Names | Techniques Used | Year First Seen |
|---|---|---|---|
| Flame | Flamer, sKyWIper | Records media on infected host hardware [25], [26], Windows authentication packages for persistence [27], Limbo module creates backdoor by using users accounts [25], [26], Beetlejuice module transmits encoded information from the infected system to other Bluetooth enabled devices [28], lateral movement using MS10-061 [25], [26], lateral movement using USB drives with autorun functionality [25], Executed from the command line by rundll.exe [27], Security module scans for security software [25], [26] [29] | 2010 |

| | | | |
|---|---|---|---|
| Duqu | ~ | User tokens used for program execution [30], [31], information collected on open windows using Discovery modules [30], C2 server with HTTPS and HTTP network communication, updates pushed via peer-to-peer communication for infected hosts without an internet connection, sends blank JPEG with data appended to the image to C2 server, valid private key for a system driver is used to start new services, keyboard logger module, Process hollowing and injection modules, lateral movement via task scheduling communicated by a C2, signed binary proxy execution to execute malicious Windows installer packages, C2 data stream is encrypted using AES-CBC, information on network configuration is collected [30] [29] | 2010 |
| Dragonfly | HAVEX | Backdoor.Oldrea: credential dumping using an open source web browser password recovery tool, encrypts collected data before exfiltrating to a C2 server, data from the C2 server is encrypted, implements a kill switch, (collects outlook address books, information about running processes, OS version, computer name, available drives, default browser, file lists, internet history, root of available drives, internet adapter configuration, current username, and ICS-related files) Trojan.Karagany: saves dumped passwords into \programData\Mail\MailAg\pwds .txt, creates directory \programData \Mail\MailAg \gl to upload files, creates a link in the Start-up folder to start upon system boot, uses remote file copy to upload, download, and execute files, takes desktop screenshots, obfuscates executables through opensource and custom binary packers [32] [29] | 2011 |

Table 1: Malware developed by APTs for high level reconnaissance

As highlighted by Stuxnet and Shamoon the appropriate level of reconnaissance and planning required is determined by the desired outcome. The Purdue model offers a general guide to the reconnaissance required for a given attack vector. Going to a lower level increases the level of reconnaissance required due to the customized nature of lower levels. Furthermore, manipulating the targeted system at lower network levels in a way that will not alert operators is very difficult. The increased difficulty is because at the lowest level of the Purdue model OT networks typically have safety systems that operate within narrow ranges, with redundancy, and are frequently air gapped. Compromising these systems in a way that will not alert operators is difficult and requires detailed knowledge of the systems configuration in order to avoid detection. Had Hatman not of triggered a plant shut down it could have theoretically continued to propagate throughout the network and manipulated the plant into an accident scenario. At a more fundamental level an understanding of the physics of the industrial process in question is also required if the attack is specifically tailored to a desired outcome. Without an understanding of the physics involved in centrifuges, for example, the designers of Stuxnet would have had a nearly impossible task of determining the optimal way to cycle the centrifuges to cause maximum rotor fatigue. An attack scenario that causes a prompt failure would be suspicious and a forensic analysis would most likely lead to malware artefacts being discovered.

Shamoon focused on the higher levels of the Purdue model and was readily able to acquire the intelligence needed through spear phishing and lateral movement inside the network. More advanced threats like Stuxnet, Hatman, and CrashOverride require a more advanced level of reconnaissance most likely utilizing tools like Flame, Duqu, and Dragonfly (Table 1). Current forensic evidence suggests that Stuxnet and Duqu were codeveloped; CrashOverride also shares many commonalities with the Dragonfly campaign. [30], [33] Although there is suspicion that Flame is related to Stuxnet and Duqu there are enough differences in the code that suggest they were developed by different teams. The fact that Flame, Stuxnet, and Duqu were all primarily concentrated around the same time in Iran suggests that the malware campaigns could have conceivably been related. Due to C2 servers that can send malware removal commands, it is difficult to obtain software samples of advanced reconnaissance malware or even prove the existence of such malware.

Once reconnaissance is completed, an exploit leveraged, possible C2 established, and multiple backdoors put in place stage 2 of the OT cyber kill chain begins. The attack needs to be developed and tested to ensure that when it is initiated that the desired outcome will be achieved. It can be conservatively assumed that defenders are

actively monitoring the network and suspicious activity will alert network administrators. Therefore, attackers might only get one chance to exploit a system with a known vulnerability before it is patched, or defensive action is taken. Hatman exemplifies the technical barriers attackers must overcome to validate their final attack vector. In order to take control of the Schneider Electric Triconex Safety Instrumented System (SIS) the attackers reverse engineered the proprietary TriStation protocol. At a minimum, the attackers had physical access to a Schneider Electric Triconex SIS and could test their malware in a sandbox environment. Labs specifically setup to find the vulnerabilities of SCADA systems, programmable logic controllers (PLCs), and remote terminal units (RTUs) pose a significant risk to production environments assuming the intelligence gathered in Stage 1 is reliable.

| Malware Name | Associated Names | Techniques Used | Year First Seen |
|---|---|---|---|
| Stuxnet | ~ | Lateral movement using USB drives with Autorun functionality (BID 41732), lateral movement through LAN exploiting Windows Print Spooler (BID 43073), lateral movement through SMB exploiting Windows server service RPC (BID 31874), lateral movement through network shares and WinCC database server, code injection into Step 7 Siemens PLC code with autorun, code updates utilizing peer to peer communication, two zero days for privilege escalation, communication with C2 server, Windows rootkit for binary obfuscation, security application recognition module, primarily targets ICS systems specifically Siemens 315 and 417 controllers [24], [34], first ever PLC rootkit observed in the wild [24] | 2010 |
| Shamoon | Disttrack | Disables UAC remote restrictions by modifying registry, uses port 8080 for C2 communication [35], wipes or encrypts system files and shared drives [35], [36], overwrites MBR [22], [35]–[37], creates a service named "ntssrv", contains base64-encoded strings [35], scans C-class subnet [37], obtains targets IP address, OS version, keyboard layout, and local network topology [35], utilizes hardcoded user credentials [37], obtains system time for task scheduling [35], [37] [29] | 2012 |
| CrashOverride | Industroyer | Communicates with a local proxy before backdoor installation, after local authentication external communication with C2 server, modifies local filesystem, code injection into an existing service to point to backdoor, launcher loads ICS manipulation and wiper modules from C2, wiper payload automatically executes 1-2 hours, after installation, ICS module launches as a service, IEC 104 module kills master process and toggles valid information object addresses (IOAs) between open and closed, IEC 101 module similar to IEC 104 but utilizes serial communication, IEC 61850 module enumerates targets using configuration files and local network scanning, OPC DA module identifies all OPC servers and overwrites values in ABB MicroSCADA products effectively creating a denial of visibility, SIPROTEC DoS module exploits CVE-2015-5374 targeting SIRROTEC digital relays [33] | 2016 |
| Hatman | TRISIS, Triton | Compiled Python script, targets Triconex 3008 processor modules, verifies communication with SIS, identifies memory location for logic upload, copies "Start Code" for logic replacement and verify, uploads new ladder logic to SIS [38] | 2017 |

Table 2: Malware designed by APTs to disrupt or compromise industrial systems

Of course, complete knowledge of a system is impractical given time and resource constraints leading to uncertainty during the actual attack. Having the ability to obfuscate a malware arsenal and only deploying the modules needed to adapt in real-time is a general feature of modern malware. This tradecraft can be traced back Flame which employed multiple malware modules and would only use what was necessary to accomplish the desired outcome on a specific infected host. Having plugins to a larger framework decreases malware development costs despite a changing defence landscape, the risk of detection, and the ability for attacks to respond in real time via C2 servers. Given the value of OT network design for critical infrastructure and the emergence of for profit MaaS, actionable intelligence on OT networks has the potential to establish a black market for detailed design information. MaaS and the significant return on investment captured by cybercriminals also further complicates attribution of cybercrime and the incentives to carry out cyber-attacks on OT networks.

Modern industrial malwares are now moving to shared code bases, plugin architectures, and anti-sandboxing all of which support MaaS. These trends are reducing cost and lowering the technical bar to entry. With evidence of ransomware such as Killdisk now targeting industrial systems and leveraging cryptocurrencies the industrial malware threat landscape is changing. Cybercriminals and hacktivists now have technologically advanced tools and an awareness of the vulnerabilities present in OT networks that in the past were only available to APT groups.

## 4. COMPARE, CONTRAST, TRENDS, AND IMPACT ON NUCLEAR POWER SYSTEMS

The line between general purpose malware and industrial malware is beginning to blur. This trend is lowering the cost of entry into industrial system attacks. Overall, this promises to make attacks on such critical infrastructure as nuclear power systems more attainable by new threat groups, including groups that have traditionally targeted the nuclear power industry (e.g. environmental groups) and groups that have not (e.g. criminal and terrorist organizations). APT groups have been technically sophisticated enough to attack nuclear systems for over a decade. Other groups are starting to catch up. This will open a much larger potential threat surface than has existed historically.

**Lowering cost-of-entry and information sharing.** Industrial malware is currently dominated by APT groups due to high technical rigor, system knowledge, and cost. BlackEnergy exemplifies this trend of a general malware being modified and reused to launch attacks on industrial systems. BlackEnergy was originally an open DDOS tool available on the criminal black market. It was modified to deliver specific payloads targeting energy distribution systems, but still retained its original functions – which were, in fact, used to bring down customer support systems when distribution infrastructure in the Ukraine was first attacked [33]. Using general malware can be appealing to APT groups because additional functionality can easily be added into the malware's framework and the availability of the malware increases plausible deniability. Shared open code bases also give malicious groups immediate reusable functionality from which they can develop new malware. ICS specific exploits are available today from a variety of open and commercial sources [39], [40].

**Dynamic extendibility.** Plugin architectures becoming more common, providing malicious actors the ability install implants with arbitrary functionality in compromised systems. A modular platform can make a general-purpose malware into an industrial malware by simply adding an ICS module. There are many ICS exploits freely or commercially available today [39], [40]. This pattern is common in both informational and operational malware. All CrashOverride modules are invoked via a simple API through which the dropper can download new modules from C2C, install them in the local filesystem, dynamically load them, and invoke them. DTrack, recently found in the business networks in the Kudankulam nuclear power plant, contains both spyware and a Remote Access Trojan (RAT). The RAT is able to download and install new, arbitrary payloads from C2C [41].This makes DTrack's compromise of nuclear power-related business systems is particularly troubling. This malware may have been financially targeted, but its reconnaissance and dynamic payload capabilities enable it to recognize where it is and download new payloads customized to its new environment. This gives DTrack-connected actors the ability to transform from financial to industrial malware as quickly as the actors can develop (or buy) new payloads.

**Capability migration.** We have many examples of capability migration from sophisticated to less sophisticated actors. Exploit migration facilitated by the Shadow Brokers into WannaCry and related malware is

typical of this kind of migration. Not only specific exploits migrate in this way however. Tactics, techniques, and practices also migrate from sophisticated to less-sophisticated actors as sophisticated techniques are exposed. We not only see this in malware, but in organizations as well [42]. Furthermore, capability can be purchased and repurposed. High levels of customer service and technical capabilities do exist in the black market today. 0-day exploits and custom malicious software are also available, giving reasonably-funded organizations an immediate advantage in developing targeted malware.

**Ransomware.** Ransomware is currently commodity malware and has targeted individuals or small organizations with poor IT infrastructure and processes. Though this is likely to remain the case, recent trends of ransomware targeting specific organizations and municipalities is troubling. These organizations, including healthcare organizations and small towns and cities, have paid the ransomware authors to regain system access. This has made infrastructural ransomware very profitable. Power systems, including nuclear power systems, are a natural target for these kinds of groups as they can expect such compromise to be very lucrative. The consequences of critical infrastructure attacks of this nature are certainly high, but the financial incentives are so great that some criminal group will eventually target this kind of system.

Nuclear facilities historically have not been impervious to cyber incidents, Table 3 shows a historical overview of cyber incidents that occurred at nuclear facilities around the world. The latest attack against the Kudankulam Nuclear Power Plant using the DTrack malware is an example of general-purpose malware being repurposed to attack an industrial system.

| Year | Nuclear Facility | Cyber Incident | Malware |
|---|---|---|---|
| 1992 | Ignalina Nuclear Power Plant | Insider Threat, Malware Infiltration | |
| 1999 | Bradwell Nuclear Power Plant | Insider Threat | |
| 2003 | Davis-Besse Nuclear Power Station | Malware Infiltration | Slammer Worm |
| 2005 | Japanese Nuclear Power Plants | Espionage | |
| 2006 | Browns Ferry Nuclear Plant | Software Error | |
| 2006 | Syrian Nuclear Program | Espionage | |
| 2009 | Energy Future Holdings | Insider Threat | |
| 2010 | Natanz Nuclear Facility | Malware Infiltration | Stuxnet, Duqu, Flame |
| 2011 | Oak Ridge National Laboratory | Espionage | |
| 2011 | Areva | Espionage | |
| 2014 | Monju Nuclear Power Plant | Espionage | |
| 2014 | Korea Hydro and Nuclear Power Company | Espionage | |
| 2016 | Nuclear Regulatory Commission, U.S. Department of Energy | Insider Threat | |
| 2016 | Gundremmingen Nuclear Power Plant | Malware Infiltration | W32.Ramnit, Conficker |
| 2016 | University of Toyama | Espionage | |
| 2018 | Wolf Creek Nuclear Power Plant | Espionage [43] | |
| 2019 | Kudankulam Nuclear Power Plant | Malware Infiltration | DTRACK [44] |

Table 3: Cyber Incidents at Nuclear Facilities [45], [46]

As nuclear power plants seek to reduce operation, maintenance, and security costs plants will increasingly move towards automation and algorithms driven by large amounts of data gathered by sensing and actuating devices. Increasing the digital footprint of nuclear power plants could have large potential cost savings, but at the same time increases the cyber-attack surface. Furthermore, physical damage to nuclear power plants should not be the only criteria for regulators and governments to be alarmed. As stated in the subsequent section on Industrial malwares the knowledge of the OT network is a critically important step in the OT cyber kill chain. In 2014 Korea Hydro and Nuclear Power company was hacked and the design of two operating nuclear power plants in South Korea stolen [45]. With this information attackers can study the plant design and develop malware that could alter

the normal operation of the plants putting them at increased risk. Industrial sabotage can be equally as damaging to nuclear power plants given the already low public approval of nuclear power plants in a post-Fukushima world. As trends in malware keep evolving, cybersecurity for nuclear powers needs to also evolve for the industry to prevent future cyber-attacks and integrate emerging technology for increased operating efficiency.

Overall, lowering cost-of-entry into high impact industrial system attacks coupled with expanding capabilities and potential high financial gain associated with nuclear system compromise makes sophisticated cyber-attacks against nuclear facilities more likely than ever before.

## ACKNOWLEDGEMENTS

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

## REFERENCES

[1] J. Wyke, "What is Zeus?," 2011.

[2] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, "Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus," *Proc. 2013 8th Int. Conf. Malicious Unwanted Softw. "The Am. MALWARE 2013*, pp. 116–123, 2013.

[3] N. Etaher, G. R. S. Weir, and M. Alazab, "From ZeuS to Zitmo: Trends in Banking Malware," *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 1386–1391, 2015.

[4] McAfee, "Protecting Your Critical Assets Lessons Learned from Operation Aurora," 2010.

[5] T. Terpandjian, "Advanced Persistent Threats (APT): Operation Aurora, its Perpetrators, Incentives and Administrative Responses to Alleviate Dangers," 2012.

[6] K. Jarvis, "CryptoLocker Ransomware Threat Analysis," *SecureWorks*, 2013. [Online]. Available: https://www.secureworks.com/research/cryptolocker-ransomware.

[7] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin," *eCrime Res. Summit, eCrime*, vol. 2016-June, pp. 1–13, 2016.

[8] Bromium, "EMOTET: A Technical Analysis of The Destructive Polymorphic Malware," 2019.

[9] B. Mane, V. Chole, P. Saxena, and P. Galande, "The Complete story of EMOTET Most prominent Malware of 2018," 2018.

[10] H. Sinanovic and S. Mrdovic, "Analysis of Mirai Malicious Software," *2017 25th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2017*, 2017.

[11] CERT-MU, "THE WANNACRY RANSOMWARE," 2017.

[12] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," *Proc. - 16th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2017*, vol. 2017-Decem, pp. 454–460, 2017.

[13] D. Y. Kao, S. C. Hsiao, and R. Tso, "Analyzing WannaCry Ransomware Considering the Weapons and Exploits," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2019-Febru, no. 2, pp. 1098–1107, 2019.

[14] K. Johnson, "NotPetya: One Year Later," *Anomali*, 2018. [Online]. Available: https://www.anomali.com/resources/whitepapers/notpetya-one-year-later.

[15] R. A. Lika, D. Murugiah, S. N. Brohi, and D. A. P. V. Ramasamy, "NotPetya: Cyber Attack Prevention through Awareness via Gamification," *2018 Int. Conf. Smart Comput. Electron. Enterp. ICSCEE 2018*, pp. 1–6, 2018.

[16] C. Fenton, J. Landry, N. Izraeli, I. Liba, and S. Udi, "Dissecting NotPetya So You Thought It Was A Ransomware," *SentinelOne Labs*, 2017. [Online]. Available: https://www.sentinelone.com/blog/dissecting-notpetya-so-you-thought-it-was-ransomware/.

[17] P. Rascagnères, W. Mercer, and C. Talos, "Who Wasn't Responsible for Olympic Destroyer." 2018.

[18] V. Ventura and M. Lee, “Wiper Malware: Attacking From Inside,” pp. 1–11, 2018.

[19] U.S. Department of Homeland Security ICS-CERT AAL, “Malware Trends,” 2016.

[20] N. Kshetri, “Hacking Power Grids: A Current Problem,” *IEEE Comput. Soc.*, pp. 91–95, 2017.

[21] J. P. Farwell and R. Rohozinski, “Stuxnet and the Future of Cyber War,” *Surviv. Glob. Polit. Strateg.*, vol. 53, no. 1, pp. 23–40, 2011.

[22] Symantec Security Response, “The Shamoon Attacks,” *Symantec*, 2012. [Online]. Available: https://www.symantec.com/connect/blogs/shamoon-attacks.

[23] M. Assante and R. Lee, “The Industrial Control System Cyber Kill Chain,” SANS Institute, 2015.

[24] N. Falliere, L. O. Murchu, and E. Chien, “W32. stuxnet dossier,” 2011.

[25] A. Gostev, “The Flame: Questions and Answers,” *Securelist*, 2012. [Online]. Available: https://securelist.com/the-flame-questions-and-answers/34344/.

[26] A. Gostev, “Flame: Bunny, Frog, Munch and BeetleJuice…,” *Securelist*, 2012. [Online]. Available: https://securelist.com/flame-bunny-frog-munch-and-beetlejuice-2/32855/.

[27] SKYWIper-Analysis-Team, “sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks,” 2012.

[28] Symantec Security Response, “Flamer: A Recipe for Bluetoothache,” *Symantec*, 2012. [Online]. Available: http://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache.

[29] MITRE, “Mitre Att&Ck,” *MITRE ATT&CK*, 2019. [Online]. Available: https://attack.mitre.org/.

[30] Symantec Security Response, “W32.Duqu,” 2011.

[31] Kasperky, “The Duqu 2.0 - Technical Details (V2.1),” 2015.

[32] Symantec Security Response, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” 2014.

[33] Dragos, “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations,” 2017.

[34] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Secur. Priv.*, no. June, pp. 49–51, 2011.

[35] R. Falcone, “Shamoon 2: Return of the Disttrack Wiper,” *Palo Alto Networks*, 2016. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/.

[36] R. Falcone, “Shamoon 3 Targets Oil and Gas Organization,” *Palo Alto Networks*, 2018. [Online]. Available: https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/.

[37] FireEye, “FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region,” 2016. [Online]. Available: https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html.

[38] Dragos, “TRISIS Malware Analysis of Safety System Targeted Malware,” 2017.

[39] GLEG, “GLEG - Information Security Company,” 2019. [Online]. Available: http://www.gleg.net/.

[40] Rapid7 Inc., “Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit,” *Metasploit.Com*. 2019.

[41] K. Zykov, “Hello! My name is Dtrack Securelist,” *Securelist*, 2019. [Online]. Available: https://securelist.com/my-name-is-dtrack/93338/.

[42] C. Bing and J. Schectman, “Inside the UAE’s Secret Hacking Team of American Mercenaries,” *Reuters*, 2019. [Online]. Available: https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[43] M. Londberg, “Russian Agents Hacked into Wolf Creek’s Business Network,” *The Kansas City Star*, Kansas, 16-Mar-2018.

[44] D. Das, “An Indian Nuclear Power Plant Suffered a Cyberattack,” *The Washington Post*, Washington D.C., 04-Nov-2019.

[45] A. Van Dine, M. Assante, and P. Stoutland, “Outpacing Cyber Threats Priorities for Cybersecurity at Nuclear Facilities,” 2016.

[46] G. Desarnaud, “Cyber Attacks and Energy Infrastructure: Anticipating Risks,” 2017.