# **Critical Systems Security: Analysis of Cyber Security Incidents in the Critical Infrastructure**

## **1.0 Abstract**

## **2.0 Introduction**

## **3.0 Threat Landscape**

There are numerous examples of past threats that have targeted critical infrastructure, some to a near disastrous degree. The landscape is fairly broad not only because there are many threats but also because the threats to critical structures tend to cross the multiple sectors of industrial systems, for example an insider threat may occur solely in the field sector but an infection may occur in the enterprise sector and spread via network to the control and field sectors. In this section we will explore the threats not only by the sector in which they are most likely to occur, but also the direct or indirect effects it will have on other sectors.

### 3.1 Enterprise Sector

This sector is the business front of the Industrial Control System, it is where the more office centric roles operate. Rather than working directly with the industrial systems, this sector handles operations directly related to said systems; this could be finance, legal, human resources, and so on.

The enterprise sector is reminiscent of your typical office network structure, usually being banks of computers connected to each other via conventional network topologies. All of this means that the Enterprise Sectors are open to all the threats that typical networks would be, such as Malware, Denial of Service, and other such attacks.

A particularly deadly example of an attack that could occur in the enterprise sector is Ransomware, which is a type of malware that encrypts files on the affected system and prompts for a ransom payment, in recent years this has been in Bitcoin but in the past it has occurred in other forms. The Ransomware often includes a countdown timer prompting for the payment by a certain time or the encrypted files will be deleted. There is no guarantee that files will be decrypted after the payment is made.

The reason this threat is particularly notable is its method of initial infection, phishing emails. These emails are considered a form of social engineering, playing on operational, financial, or empathetic factors in order to get the target to download the malicious file or follow the suspicious link.

A notable example of a particularly deadly Ransomware attack is the 2017 WannaCry outburst. WannaCry is a Ransomware Cryptoworm that propagates through networks via an exploit dubbed ‘EternalBlue’, which used older Windows systems Server Message Block (SMB) protocol. Once it propagated to a system, the worm installs a back-door called ‘DoublePulsar’ which would grant high levels of access on the infected system, allowing it to operate as it wishes *(ENISA, 2017)*.

In 2017 alone WannaCry grew to infect 230,000 systems around the world affecting many different businesses, including: Telefonica, UK National Health Service, Deutsche Bahn, Renault, and more *(ENISA 2017)*. Whilst Ransomware may not pose a direct threat to systems in the field sector, a particularly deadly attack could propagate to the control sector from the enterprise sector and vice versa if the systems involved are outdated or security features are lacking. Even so, an effective attack on the enterprise systems may be enough to cause sufficient damage indirectly. The estimated damages to the UK National Health Service *(Department of Health and Social Care, 2018)* was 92 million pounds, occurring from directly damaged systems and operational downtime. This is further compounded by possible damage to the NHS’ reputation due to the fact that the attack affected *(House of Commons Committee of Public Accounts, 2018)* 80 of 236 NHS trusts, a further 603 NHS organisations including 595 GP practices, which led to the NHS cancelling 20,000 hospital appointments and operations, and caused the closing of 5 accident and emergency departments. This was caused by the NHS utilising outdated systems, and is a clear exemplar of the financial and reputational damage that can be incurred by sophisticated malware attacks.

The cyber-attack on the Ukrainian Power grid in 2015 shares some similarities with the WannaCry attacks, mostly in its method of entry into the systems. The attack was a highly sophisticated and coordinated effort to bring down multiple energy stations around Ukraine, the objective appearing to be to create chaos and panic. Like WannaCry the initial infection was done via Phishing Emails typically phishing emails are akin to a “brute force” method, but the kind used in this attack were tailored to particular targets. This is what is known as Spear Phishing, the targets are usually ones considered to be the “weakest link in the chain” and they are typically observed in some fashion in order to garner information to use that would increase the effectiveness of the tailored phishing email. Unlike typical Phishing, Spear Phishing can also be undertaken over a longer period of time, waiting until a trust is built to be manipulated. All this creates an extremely effective method of infection, a study by *Lin et al (2019)* with a sample of 158 people of various ages and backgrounds showed showed that of the sample 43.3% (68 people) would click links contained in such emails.

The Spear Phishing campaign in this attack would have workers in the Enterprise sector of the Ukrainian Power stations download malicious documents which served as the delivery method, when the documents were opened it would prompt the user to enable macros. Once this was enabled, it would install the BlackEnergy3 malware on the system, which was connected to a command and control IP address allowing for communication and data exfiltration to the attacker. After this initial infection, the malware would scrape for credentials, escalate its privileges, and proceed laterally though the network. The attackers were quick to move from the foothold in order to avoid detection. Using the stolen credentials and elevated privileges, the attacker was able to pivot into network segments where the SCADA workstations and servers existed, the Control Sector. From there it would carry out its attack that would lead to the power outage affecting 225,000 people and last several hours *(E-ISAC and SANS-ICS, 2016)*.

### 3.2 Control Sector

The control sector is where the control centre operations occur, it is connected to the enterprise sector usually via a wide area network (WAN), and further connected to the field sector by serial radio communication. This sector typically contains the engineer’s workstations, the control servers, the Human Machine Interface (HMI), and the data historian. It is typically organised using typical network topologies.

The Ransomware threat detailed in the previous section can also occur in the control sector, and in a particularly deadly manner. It can occur here in similar ways to the enterprise sector, via propagation from said sector, through malicious emails, or a compromised USB containing the payload. There are many machines in the control sector that are absolutely vital to the overall operation of the control network. Ransomware could infect and encrypt data on: The Data historian, which would cause the loss of a considerable quantity of data should it be unable to be recovered; the HMI station, which would create a condition where engineers are no longer capable of observing the data from the field sector and therefore unable to make informed decisions; or even the control server, which would completely halt all communication between the control and field sector.

The Control Sector is where the attack stage of the Ukrainian Power grid attack played out. It began by learning how to interact with the three distinct Distributed Management Systems using the native control present in the system and operator screens, and developing malicious firmware for the serial-to-ethernet devices. During this attack stage, the adversary used native software to deliver themselves into the environment for direct interaction with the ICS components, they achieved this by using existing remote access administration tools on the operator workstations. In preparation for the final stage of the attack, the adversaries installed a modified version of KillDisk, which would allow them to erase the master boot record, effectively locking users out of systems, and erasing targeted logs. At the time of attack, the adversaries used the Human Machine Interface to open the breakers, shutting off the power. Simultaneously, the adversaries would upload the developed malicious firmware to the Serial-to-Ethernet gateways, this was to ensure that even if the workstations were recovered that they still would not be able to issue commands remotely.

During this period, attackers would also perform a remote telephone denial-of-service attack to prevent communication between the companies and customers, the objective of this particular part of attack is subject to debate.

### 3.3 Field Sector

This sector is where the Programmable Logic Controllers (PLC) and the Remote Terminal Units (RTU) interact and control various machinery. It is connected to the Control Sector alone via serial-based radio communication.

The Ransomware threats detailed in the previous sections will have little effect here, and programming them to affect PLC’s or RTU’s would be extremely difficult if not impossible. The only thing that Ransomware could affect in this sector is the remote access computer, the malware wouldn’t be capable of propagating via the Radio connection from the control sector, so therefore the only method of propagation to the remote access computer would be via infected USB.

In the case of the Ukrainian Power grid attack, the Field Sector wasn’t compromised, but the Control Sector machines that controlled them were. Theoretically, the only way the attack on the grid could directly compromise the field sector would be if a remote access machine local to the field sector was compromised, but given the method of propagation this is very unlikely.

### 3.4 Methodologies and Technologies By Killchain Stages

The previous section detailed threat capabilities on a case study basis, for a broad overview of various technologies and methodologies used in a variety of attacks refer to Appendix A. All information is drawn from *Tarun and Yadav (2016)*

## **4.0 Security Approaches**

+ Methodologies?

+ Compare Killchain models?

+ Managerial and Operational

## **5.0 Improving Security**

+ Current implementations.

+

## **6.0 Conclusion**

# **7.0 References**

ENISA (2017) *WannaCry Ransomware Outburst*. Available from: <https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst> [Accessed 03 February 2020].

Department of Health and Social Care (2018) *Securing Cyber Resilience in Health and Care: Progress update October 2018* [online]. London: Department of Health and Social Care. Available from: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf> [Accessed 07 February 2020]

House of Commons Committee of Public Accounts (2018), *Cyber Attack on the NHS: Thirty Second Report of Session 2017-2019* [online]. London: House of Commons. Available from: <https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf> [Accessed 07 February 2020]

Lin, T.L., Capecci, D.E.C., Ellis, D.M.E., Rocha, H.A.R., Dommaraju, S.D., Oliveira, D.S.O. and Ebner, N.C.E. (2019) *Susceptibility to Spear-phishing Emails: Effects Of Internet User Demographics and Email Content*. Acm Transactions on Computer Human Interaction [online]. 26 (5) [Accessed 16 February 2020].

E-ISAC and SANS-ICS (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid*[online]. Washington DC: E-ISAC and SANS-ICS. Available from: <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>

## **Appendices**

### Broad Scope Threat Methodologies and Technologies

All data from *Tarun and Yadav (2016).*

|  |  |  |
| --- | --- | --- |
| *Stage* | *Methodology / Technology* | *Description* |
| *Recon* | *Target Identification and Selection* | *Passive*  *Domain names, whois, records from APNIC, RIPE, ARIN* |
| *Target Social Profiling* | *Passive*  *Scraping social networks, public documents, reports and corporate websites.* |
| *Target System Profiling* | *Active*  *Pingsweeps, Fingerprinting, Port scanning* |
| *Target Validation* | *Active*  *Spam Messages, Phishing emails, social engineering* |
| *Weaponization* | *Remote Access Tool (RAT)* | *Executes on target system, giving remote, hidden, and undetected access to the attacker.* |
| *Delivery* | *Email Attachments* | *Content composed to entice the user by using appealing content.* |
| *Phishing Emails* | *Sensitive information like Usernames, passwords, credit card details are extract masquerading as a trustworthy source.* |
| *Drive By Download* | *Target is forced to download appealing malicious content from the internet. Images, PDF Word documents.* |
| *USB Removable Media* | *Removable media devices which silently infect other systems by opening files.* |
| *DNS Cache Poisoning* | *Divert internet traffic from legitimate servers to attacker controlled destinations.* |
| *Exploitation*  *(Exploits are usually combined into a singular, multi-exploit kit)* | *Operating System Level* | *Kernal, device drivers, denial of services, remote or local code execution.* |
| *Network Level* | *FTP, SMTP, NTP, SSH, router, privilege escalation.* |
| *Application Software* | *Browsers, MS Office, PDF, Java / Flash, Memory Corruption (Dangling-pointer,buffer overflow, use-after-free)* |
| *Installation* | *Droppers* | *Program to install and run malware on system. Will try and disable device security.* |
| *Downloaders* | *Similar to dropper, smaller, connects to a remote server and downloads the rest of the payload.* |
| *Anti-AntiVirus* | *Dropper and Downloader are usually “armoured”, containing toolsets for disabling security measures, changing DNS to prevent updates.* |
| *Rootkit and Bootkit* | *Payload file hiding, process hiding.*  *Bootkits hook and patch system to gain kernal access.* |
| *Targeted Delivery* | *Preventive measures against deploying malware in a virtual environment.* |
| *Host-based Encrypted Data Exfiltration* | *Critical data stolen is encrypted and sent over a clear text protocol such as HTTP or SMTP.* |
| *Command and Control*  *(Architecture)* | *Centralized* | *Single Server, no dependency on peer-to-peer. Infected machine failure wont affect the whole. Take down of C&C will bring down entire structure.* |
| *Decentralized* | *Peer-to-peer. Scalable. Fault Tolerant.* |
| *Social Networks Based* | *High Availability. Reliable. Profiles used to pass on information.* |
| *Command and Control*  *(Secure Communications)* | *IRC Chats* | *Application layer protocol. Client / server networking model.* |
| *TCP / HTTP* | *Secure, error checked, over the web communication protocols.* |
| *Steganography* | *Encoding information in images, video, or audio.* |
| *TOR* | *Hidden service protocol. Traffic directed through a worldwide volunteer overlay network.* |
| *Command and Control*  *(Obfuscation)* | *DNS Fast Flux* | *Rapidly changing network of machines* |
| *Domain Name Generation Algorithm* | *Pseudo Random Domain Names.* |
| *Act of Objectives* | *Mass Attack* | *Distributed attack on many targets. General target is credentials. Bigger picture is botnet creation.* |
|  | *Target Attacks* |  |

Titles: 38

References: 138

Word count: 1588