# **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 empathetical 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.

### 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.

### 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.

## **4.0 Security Approaches**

## **5.0 Improving Security**

## **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]

Titles: 38

References: 76