CSL1101 – Computer Security

Assignment 2: Analysis of Contemporary Computer Security Issues

Student Name: Glen Teakle

Student No: 10532981

Campus: ES (Joondalup, off-campus)

Lecturer/Tutor: Mr. Imran Malik

Contents

[Introduction 2](#_Toc80796674)

[An Overview of Triton 2](#_Toc80796675)

[Triton Malware Attack 3](#_Toc80796676)

[Safety Concerns 4](#_Toc80796677)

[Critical Infrastructure and Cyber Security 5](#_Toc80796678)

[Summary 6](#_Toc80796679)

[References 7](#_Toc80796680)

# Introduction

Malware or “malicious software” is computer software that is created with damage and disturbance in mind. It is usually installed without user knowledge or consent and contains program code that a computer translates and executes (Malik, n.d). There are many different types of malware; one in particular is called a Trojan horse. This is something harmful hidden inside something disguised as harmless (Malik, n.d). In 2017, a new type of Trojan horse was discovered inside a Safety Instrumented System (SIS) Triconex brand safety controller at an energy company, Schneider Electric, in Saudi Arabia. This malware was installed remotely without any knowledge from the company, using a “dropper” method. A dropper is how the virus installs itself into a system (Encyclopedia by Kaspersky, 2021). The purpose of this report is to give an outline of the Triton malware and what took place in the 2017 attack. It will also report on future safety concerns regarding Triton, Schneider Electric and malware in general, and finish with a view on critical infrastructure. Academic journals were researched, along with reports by companies and various information from websites.

# An Overview of Triton

The Triton malware is known by the names TriSIS or Hatman, but more commonly referred to as Triton (Di Pinto, Dragoni, & Carcano, 2018). It contains 2 main files called inject.bin and imain.bin. Code for these files was written in Python, a common programming language (Di Pinto, Dragoni, & Carcano, 2018; Stoler, 2018). It is believed that programming for the malware started somewhere around June 2016 (McMillan, 2018). The main files can be installed remotely to a system using any Windows PC connected to the same network, (see Figure **1**). Triton was designed to interact specifically with the SIS by connecting to a Windows PC connected to the SIS. The malware can then be downloaded and installed remotely (Symantec, 2017). From here it can lay dormant inside the system’s memory and remain hidden until activated (Stoler, 2018). Once installed in the system, a user can gain complete control over the system controllers by remote access (Di Pinto, Dragoni & Carcano, 2018). Any PC on the same network also has the potential to be destructive, as other machines on this network can also access the SIS controllers (Stoler, 2018). The attackers developed and wrote their program knowing this was how the controllers operated. (Di Pinto, Dragoni, & Carcano, 2018). In the attack on Schneider Electric, the plant owners only became aware after a shut down of the plant caused them to investigate (McMillan, 2018).

Figure **1**.

*Triton Files Being Remotely Installed* *via* t*he Dropper Phase*.

![Graphical user interface, text, application

Description automatically generated]()

*Note. Adapted from A schematic view of the dropper phase of TRITON. Di Pinto, Dragoni, & Carcano, 2018, (TRITON: The First ICS Cyber Attack on Safety Instrument Systems).*

# Triton Malware Attack

Figure **2** shows the steps of the attack. The dropper’s purpose was the delivery of the files into the controller’s memory (Di Pinto, Dragoni, & Carcano, 2018). The Triton program then downloaded its instructions to the SIS where it awaited remote execution (Sans, 2018). The design of the malware allowed it to elevate its own privileges inside the system and copy itself into memory (Stoler, 2018). Here it laid dormant and undetected inside the system’s memory. A virus that could be controlled remotely was now installed on the controllers and able to receive instructions from any PC on the same network as the SIS (Stoler, 2018).

Figure **2**

*The delivery of the malware into the safety controllers.*

Diagram

Description automatically generated

After Triton was successfully installed onto the Triconex controller however, no further malicious activity occurred, and no payload was delivered. In malware terms, the payload is the intended result of the virus (Encyclopedia by Kaspersky, 2021). Instead, an alarm was activated, and a power trip resulted in the system shutting down. As the SIS controllers rarely get reset or shut down (Stoler, 2018), this prompted the plant owners to investigate using a cyber security company called Fireeye (McMillan, 2018) who discovered the malware on the Triconex system (Di Pinto, Dragoni, & Carcano, 2018 ; McMillan, 2018 ; S4 Events, 2018). Schneider Electric first learned about the intrusion when one of their customers informed them about the power trip and subsequent plant shutdown. The shutdown was investigated, and the malware was discovered. Rob Lee, a spokesman for the cyber security company Drago Inc. remarked that the malware is very tough to notice without dismantling the entire system (McMillan, 2018). Schneider Electric have since developed a tool that can detect this specific malware intrusion in the Triconex controller. If a detection occurs it can then remove it from memory (S4 Events, 2018). Schneider also released some post attack guidelines to learn from as shown in Figure **3**.

Figure **3**

*Schneider Electric’s post attack response.*

![Graphical user interface, text, application, email

Description automatically generated]()

*Note. From Schneider Electric Analysis and Disclosure, S4 Events, 2018, (https://www.youtube.com/watch?v=f09E75bWvkk).*

# Safety Concerns

It is possible that Schneider Electric never considered they would be attacked in the manner they were, hence; they were ill-prepared when it happened. They do however use 16 year old workstations; the Triconex controllers (McMillan, 2018) that never get rebooted or reset so they are possibly never updated with current software and thus, open to such attacks. Schenider Electric seemingly had no virus detection on their PC’s, and no-one monitoring them for intrusion either. McMillan (2018) in his article comments on another safety concern regarding the safety controllers. They have a “program” switch that enables reprogramming of the controllers if turned to the “on” position. Andrew Kling, a Schneider Electric director, has suggested that customers using the Triconex do not leave this switch in the “on” position. This detail could easily be compromised or forgotten. A belief that Schneider were targeted was suggested in a report from Fireeye who commented that the Triton malware had been in development since 2016 and several months previous the research to write the code for it would have started (McMillan, 2018). Potential consequences of this attack could have included restricted or no access to the entire safety system, and the devices themselves (Stoler, 2018).

The SIS that operate inside plants and similar environments are the main systems concerned with safety processes. They prevent things such as explosions, fire and equipment malfunction. If a remote operator has access to them, they have the power to cause major damage (Di Pinto, Dragoni, & Carcano, 2018).

Accessing the SIS controllers without permission, the installation of outside files and the overall remote access of the Triconex system without knowledge classifies this attack as a breach of integrity (Malik, n.d). A breach of availability also occurred because of the power trip that took place and subsequent shut down of the system. The plant workers/owners were not able to access the system while this was happening (Malik, n.d).

# Critical Infrastructure and Cyber Security

As cyber security issues and breaches have become more prevalent over the last 18 months, the security of critical infrastructure is of great importance. Seemingly, no one is safe and any company or business no matter how small, or even the general population has the potential to have their security compromised. It is important for the Government to step up and realise what is at stake. The fabric of our society including things such as gas, oil, water, emergency services, banking, transportation and communication networks are all likely contenders for cyber breaches (see Figure **4**). It is of great importance that nations take cyber security regarding critical infrastructure seriously as it would be all too easy for hackers to “take over” and gain control of systems and infrastructure, as this report shows.

Figure **4**

*The**Critical Infrastructure Network*

Diagram

Description automatically generated with medium confidence

*Note. From Critical Infrastructures, Privacy 108, 2020, (https://privacy108.com.au/insights/new-security-obligations-critical-infrastructure-providers/).*

# Summary

Malware exists today under many different forms. Computers on the same network are in danger of security breaches, especially using remote access. As shown in this report; sometimes the malware may already be installed without user awareness, possibly laying dormant awaiting activation. It may even be found after the breach or attack has already taken place. At least victims of malware may learn how to better protect themselves from future breaches, hopefully without the loss of too much information, or at the expense of the future critical infrastructure.

# 

# References

Di Pinto, A., Dragoni, Y., & Carcano, A. (2018). *TRITON: The first ICS cyber attack on safety instrument systems. Understanding the malware, its communications and its OT payload*. Black Hat USA. https://i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-Control-Systems-Forever-wp.pdf

Kaspersky, (n.d). *Payload*. Encyclopedia by Kaspersky. https://encyclopedia.kaspersky.com/glossary/payload/

Kaspersky, (n.d). *Trojan droppers*. Encyclopedia by Kaspersky. https://encyclopedia.kaspersky.com/glossary/trojan-droppers/

Malik, I. (n.d), CSL1101 *Malware: Module 3* [Lecture notes]. Blackboard. https://blackboard.ecu.edu.au/

McMillan, R. (2018). New Type of Cyberattack Targets Factory Safety Systems; Malicious software Triton was able to manipulate Schneider Electric devices' memory and run unauthorized programs by leveraging a previously unknown bug. *WSJ Pro. Cyber Security*. https://www.proquest.com/trade-journals/new-type-cyberattack-targets-factory-safety/docview/2171064569/se-2?accountid=10675

Sans. (2018, January 29). *Triton/TriSIS* – *In search of its twin*. SANS. https://www.sans.org/blog/triton-trisis-in-search-of-its-twin/

Stoler, N. (2018, February 2). *Anatomy of the triton malware attack*. Cyberark. https://www.cyberark.com/resources/threat-research-blog/anatomy-of-the-triton-malware-attack

Symantec. (2017, December 15). *Triton: New Malware Threatens Industrial Safety Systems.* Broadcom.https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/triton-malware-ics