International Journal of
Emerging Multidisciplinary Research

ISSN : 2546-1583
Volume 3, Number 2, June 2019
https://doi.org/10.22662/IJEMR.2019.3.2.013

ICS malware Triton attack and countermeasures.

Jin-woo Myung[1] and Sunghyuck Hong[2]

[1] Student, Division of ICT, Baekseok University, KOREA

[2] Professor, Division of ICT, Baekseok University, KOREA

Abstract

Background/Objectives: Triton is the world's most serious malware and it's now spreading by all over the networks. The hackers has deployed malicious code or malware which let them take over the plant's safety instrumented systems. Methods/Statistical analysis: In this study, the research structure of TRITON Attack and Countermeasure proceeds as follows. It describes the attack method of TRITON and TRITON, the attack type of TRITON, and explains the structure of simple ICS and countermeasures of TRITON. Findings: These physical controllers and their associated software codes are the last line of defense against life-threatening crisis. Many factories now perform automated processes using computers. However, in 2017 an attack aimed at this emerged. We have detected that a malicious program is installed in the emergency safety device. All of the automation equipment used in these industrial sites is called ICS, and Triton is one of the malicious codes targeting these ICSs. Improvements/Applications: After the hacker sets up the target, the attacker uses a secure shell (SSH) based tunnel to deliver the attack tool and execute remote commands of the program after accessing the IT and OT networks, installing back doors in the computer network, and then accessing the target safety instrumentation system (SIS) controller in the OT network while scouting the network, moving the internal network, and maintaining access. Therefore, we proposed ICS malware for countermeasure to prevent from Triton attack.

Index Terms

TRITON, ICS, SIS, IT Network, OT Network

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

• Manuscript received April 4, 2019.
• Revised April 30, 2019 ; Accepted June 20, 2019.
• Date of publication June 30, 2019.

I. INTRODUCTION

As factories grow, many factories use computers to perform automated processes or process controls.

However, a radical attack aimed at this emerged. In 2017, while a Tasnee-owned petrochemical plant facility was checking for a sudden shutdown, it discovered that a malicious program had been planted in an emergency safety device that started in an emergency, such as a plant's toxic gas leak.

FireEye has released six ICS security vulnerabilities that look at unauthenticated protocols, outdated hardware, vulnerable user authentication, vulnerable file integrity checks, and Windows operating systems that are vulnerable. And an undocumented third party relationship.

ICS (Industrial Control Systems) refers to all the devices and instruments used in the operation and automation of industrial processes at many industrial sites and related software and networks. Many of the ICS are connected to sensors and other devices through the Internet of Things (IoT), so the potential ICS attack surface is quite large.

The research structure of TRITON Attack and Countermeasure proceeds as follows. Chapter 2 describes the attack method of TRITON and TRITON, and the attack type of TRITON. Chapter 3 describes the structure of simple ICS and countermeasures of TRITON. The final chapter, Chapter 4, concludes with a conclusion that concludes the study of TRITON.

II. TRITON

A. TRITON

TRITON has not known much to date, and while checking for sudden shutdowns of petrochemical plant facilities, they found malicious programs installed in emergency safety devices that need to be started in case of plant toxic gas leaks and emergencies. The plant was shut down due to a defect in the malicious program itself.

TRITON is one of the few malicious codes that targets the Industrial Control System (ICS). One such is Industroyer, which is known to have been deployed by Stuxnet in Iran in 2010 and Sandworm Team in Ukraine in 2016. TRITON is consistent with the above attacks in that safety mechanisms can cause physical damage by preventing them from performing their intended functions [1].

Table 1. TRITON MALICIOUS CODE DESCRIPTION

Malware Family	Main Modules	technology
TRITON	trilog.exe	Main run file utilization libraryZip
	library.zip	Triconex A user-defined communication library for interaction with the controller.

In addition, TRITON, Malware, said, “It was designed to manipulate the behavioral characteristics of the Triconex Safety Instrumented System manufactured by Schnneider Electric.” [2]

And it implies that there will be a country behind TRITON. Without monetary purposes, he just attacked with the aim of killing. In general, cybercriminals are hard to see.

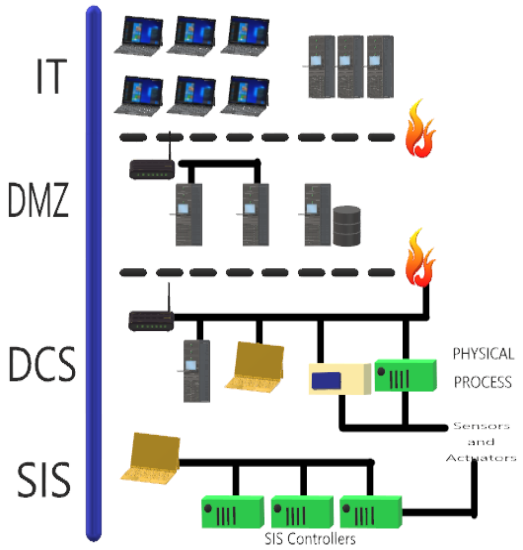

Fig. 1. Industrial Control System (ICS) Configuration

Industrial process control and automation systems are operated by various control systems and safety functions. These systems and functions are called Industrial Control Systems (ICS) or Operational Technology (OT).

Distributed Control System (DCS) gives operators the ability to remotely monitor and control industrial processes remotely. A computer control system consisting of a computer, a software application, and a controller. Engineering workstations are computers used for the configuration, maintenance and diagnostics of control system applications and other control system equipment.

SIS is an autonomous control system that independently monitors the status of processes under control. If a process exceeds the parameters that define a critical state, SIS attempts to return the process to a safe state or automatically performs a safe shutdown of the process. If SIS and DCS control fail, the design of industrial facilities, including mechanical protection of the equipment (for example, rupture disks), physical alarms, emergency response procedures, and other mechanisms to mitigate dangerous situations, becomes the final line of defense.

Asset owners use a variety of approaches to connect the factory's DCS and SIS. The traditional approach relies on separation principles for both the communications infrastructure and the control strategy. For at least the last decade, there has been a trend to integrate DCS and SIS designs for a variety of reasons, including cost savings, ease of use, and benefits from the exchange of information between DCS and SIS.

B. TRITON Attack Method

The attacker first targets and then attempts to secure and maintain the target's IT and OT networks using a variety of customized and general attack tools.

After successfully accessing the network, the attacker establishes an access path by installing a back door on the computer network and accesses the OT network. Most of the tools used were used for reconnaissance of the network, moving around the internal network, and maintaining access.

Attackers hide intrusion activity, move internal networks to thwart tools and forensic investigations, use normal user accounts that were compromised during execution during intrusions, and use KB77846376.exe to name Microsoft update files. Others used standard tools to change file names and to mimic normal administrators.

The normal files flogon, js and logoff.aspx files have been tampered with. At the same time, the attack tool is delivered using an encrypted Secure Shell (SSH) -based tunnel, and then the program is executed remotely using a directory that is infrequently used, and the attack tool, execution log, used files, and other files are continuously executed. Delete it regularly.

After successful access to the target's target SIS controller, attackers deploy Triton.

After deployment, attackers attacked TRITON

Through the framework, we attempted to improve and deliver the back door payload, and the target controller and interactions were carried out during off-hours of the target to minimize the possibility of detection while attacking relatively high risk activities.

The reprogramming of the safety measuring system might have been the purpose, but during this process, part of the safety measuring system controller entered the safe mode and failed due to interruption of the process. However, even if stopped by the safety program, the attack itself does not stop completely, so the objective is to cause physical damage.

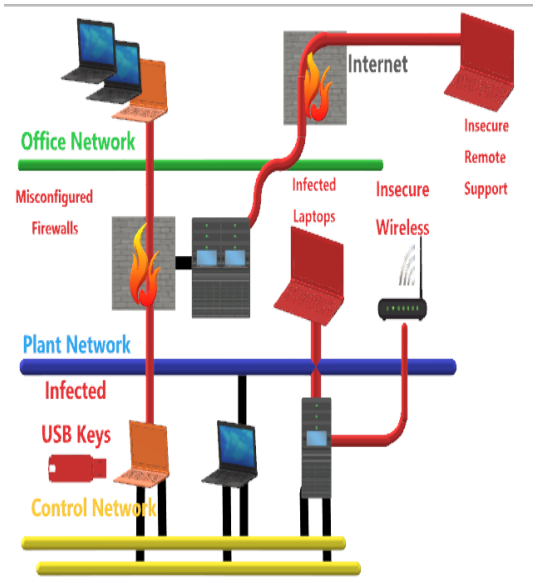

Fig. 2. TRITON Attack method

[Fig. 2] shows the widespread attackable main path of ICS. It is simply illustrated [4].

Table 2. TRITON INDICATORS

Filename	Hash
trilog.exe	MD5: 6c39c3f4a08d3d78f2eb973a94bd7718 SHA-256 : e8542c07b2af63ee7e72ce5d97d91036c5da56e2b091aa2afe737b224305d230
imain.bin	MD5: 437f135ba179959a580412e564d3107f SHA-256 : 08c34c6ac9186b61d9f29a77ef5e618067e0bc9fe85cab1ad25dc6049c37694
inject.bin	MD5: 0544d425c7555dc4e9d76b571f31f500 SHA-256 : 5fc4b0076eac7aa7815302b0c3158076e3569086c4c6aa2f71cd258238440d14
library.zip	MD5: 0face841f7b2953e7c29c064d6886523 SHA-256 : bef59b9a3e00a14956e0cd4a1f3e7524448cbe5d3cc1295d95a15b83a3579c59
TS_cnames.pyc	MD5: e98f4f3505f05bf90e17554fbc97bba9 SHA-256 : 2c1d3d0a9c6f76726994b88589219cb8d9c39

	dd9924bc8d2d02bf41d955fe326
TsBase.pyc	MD5: 288166952f934146be172f6353e9a1f5 SHA-256 : 1a2ab4df156ccd685f795baee7df49f8e701f2 71d3e5676b507112e30ce03c42
TsHi.pyc	MD5: 27c69aa39024d21ea109cc9c9d944a04 SHA-256 : 758598370c3b84c6fbb452e3d7119f700f970 ed566171e879d3cb41102154272
TsLow.pyc	MD5: f6b3a73c8c87506acda430671360ce15 SHA-256 : 5c776a33568f4c16fee7140c249c0d2b1e079 8a96c7a01bfd2d5684e58c9bb32
sh.pyc	MD5: 8b675db417cc8b23f4c43f3de5c83438 SHA-256 : c96ed56bf7ee85a4398cc43a98b4db86d3da3 11c619f17c8540ae424ca6546e1

C. *TRITON Attack Response*

TRITON is an attack on the ICS Network.

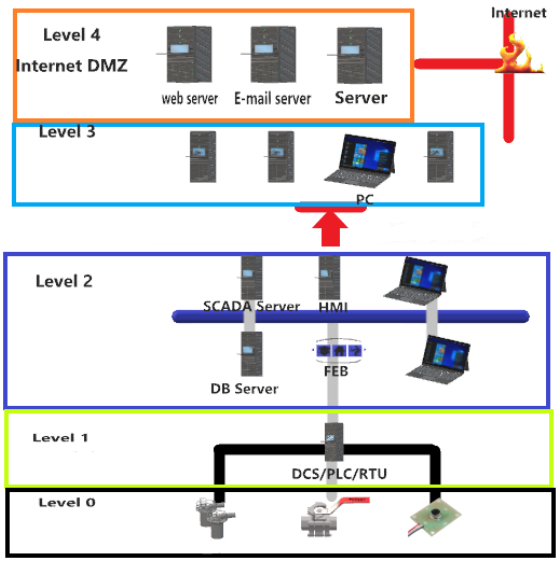

Fig. 3. ICS Basic Configuration

The general network configuration of the control system is largely divided into communication between control server and client and communication between control controller and field equipment. The control system connects the networks using unidirectional security equipment to provide real-time process information to the work network safely. One-way security devices can be divided into logical and physical methods, and both act to securely transfer data from the control network to the work network in a way that prevents data from entering the control network. [Fig. 2] is the basic structure of the industrial control system. It consists of sensors that measure the site status such as temperature, pressure, voltage, and flow in the field area (Level 0), and directly perform operations such as motors, valves, and breakers. The area of the control device (Level 1) receives control commands from the server SCADA and sends them to the devices in the field. The RTU (Remote Terminal Unit), PLC (Programmable Logic Controller and DCS (Distrubute Control Systems). The control center area (Level 2) is the area that operates and manages the control system. The SCADA server, DB server, human machine interface (HMI), and front end processor (FEP) are composed of console management and others. The internal business network area (Level 3) is an area that provides the company's business needs for the operation of the control system. It consists of the internal business server, the authentication server, and the PC. Finally, the Internet DMZ area (Level 4) is an area for servicing control system operation information to the outside (Internet). It is composed of servers for providing services such as web servers, email servers, and other servers [5].

I devised a way to secure them using Blockchain technology.

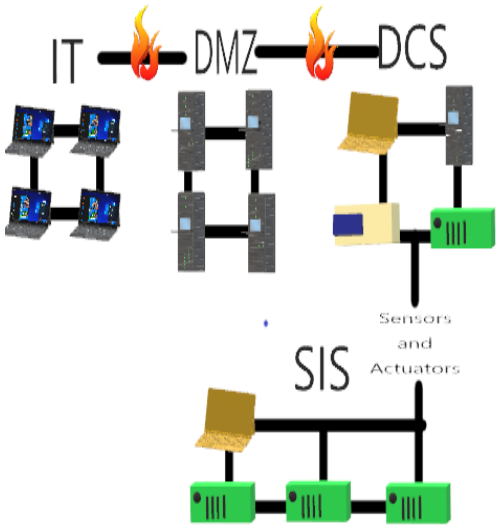

Fig. 4. ICS BolckChain security

As shown in the figure, each PC in IT secures through some degree of individual security, and the servers in the DMZ are connected to each other and the servers involved in the chain by verifying by chaining adjacent and mutually related servers. do. In other words, as in the blockchain technology, each server becomes a block and is verified by its hash value when communicating with each other. If you look at the TRITON attack from the above, it starts from one place, and gradually approaches it, and

after the successful approach, it attacks. If you use verification, you might be able to tamper with it and be safe from incoming attacks. In this way, each SIS device has its own block value and chains adjacent devices together.

The first of the existing ICS security methods is the recognition of the importance of the ICS network. Many people do not understand the importance of ICS security, and in reality there are many cases where no additional security measures are taken. Second, the input of manpower and technology. Currently, many companies are struggling with ICS protection by corporate IT security officers, and are delaying the hiring of staff with the appropriate level of ICS skills. Third, much attention is needed because ICS does not add security facilities and personnel to the management's lack of interest and lack of investment [7].

REFERENCES

[1] Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N. & Glyer, C. (2017). Attackers deploy new ICS attack framework "TRITON" and cause downtime to critical infrastructure. Threat Research Blog.

[2] Moon, Y. S., Lee, E. K., Kim, J. J. & Choi, H. R. (2014). A study on IoT-based container security devices. International Information Institute (Tokyo). *Information, 17 (11),* 5425.

[3] Franck, S., Cedric, E., Eric, Z. & Jean-Marie, F. (2018, October). Safety measures in ICS attack analysis: Implement filters based on behavioral model and critical state distance for ICS cybersecurity. *February 2018 Cyber Security (CSNET) (Pages 1-8).* IEEE.

[4] Jeon, H. H. (2009). Network design and structure for industrial control system security. *Journal of Information Security, 19(5),* 60-67.

[5] Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y. & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security* (pp. 355-366). ACM.

[6] Stouffer, K., Falco, J. & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

[7] *focus on security patching*. Master dissertation. KOREA University, Seoul.

[8] "National and public agency control system security guidelines. NIS National Intelligence Service", 2017, https://www.nis.go.kr:4016/main.do.

[9] Gostev, A. (2008). Kaspersky Security Bulletin. *Statistics*, 68-73.

[10] Baliga, A., Bickford, J. & Daswani, N. (2014). Triton: A carrier-based approach for detecting and mitigating mobile malware. *Journal of Cyber Security and Mobility*, *3*(2), 181-212.