REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
10/14/2022

2. REPORT TYPE
Technical Paper

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Cyber Risk to Mission Case Study: Triton

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
BLAINE JEFFRIES; STEPHANIE SARAVIA; CEDRIC CARTER; ZACHARY ANKUDA;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-22-3170

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
The Under Secretary of Defense for Research and Engineering

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD(R&E)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In August of 2017, TRITON malware was used to target and disrupt Safety Instrumented System (SIS) controllers within a Saudi petrochemical refinery. A SIS controls critical processes that support safety and reliability within a control system. Fortunately, the targeted SIS initiated a safe shutdown when code validation failed, triggering an internal investigation that uncovered the malware. This is one of the few publicly reported incidents of control system malware designed to inflict physical damage and the first that targeted a SIS.

15. SUBJECT TERMS

Critical Infrastructure Protection; Computer Security; SIS controllers; TRITON; Safety Instrument System; malware; cybersecurity, TRISIS/HatMan

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Susan Carpenito
				7	**19b. TELEPHONE NUMBER** *(Include area code)* 781-271-7646

Cyber Risk to Mission Case Study

BLAINE JEFFRIES, STEPHANIE SARAVIA, CEDRIC CARTER, ZACHARY ANKUDA

Category: Operational Technology
Critical Infrastructure Sector: Energy / Chemical
Incident: TRITON (aka TRISIS/HatMan)

October 13, 2022

Figure 1: Triconex Safety Systems, *Schneider Electric*

Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-3170

The view, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004

Cyber Risk to Mission Case Study

Category: Operational Technology
Critical Infrastructure Sector: Energy / Chemical
Incident: TRITON (aka TRISIS/HatMan)

Executive Overview

In August of 2017, TRITON malware was used to target and disrupt Safety Instrumented System (SIS) controllers within a Saudi petrochemical refinery [1]. A SIS controls critical processes that support safety and reliability within a control system. The SIS can halt a control system process when unsafe conditions are detected, preventing operational failures that could result in damage, human injury, or loss of life. The TRITON malware attempted to disable a SIS by reprogramming the SIS controller firmware. Fortunately, the targeted SIS initiated a safe shutdown when code validation failed, triggering an internal investigation that uncovered the malware [2]. This is one of the few publicly reported incidents of control system malware designed to inflict physical damage and the first that targeted a SIS.

Incident

The TRITON malware attack was an adversarial incident attributed to a Nation-state actor. This section provides additional information regarding the target, attribution, malware, and Tactics, Techniques, and Procedures (TTPs) employed. TTP, impact, and mitigation description references can be found within the MITRE ATT&CK® for ICS knowledge base available at the following web address: https://attack.mitre.org/matrices/ics/.

Target

Open-source reporting identifies a Saudi Arabian petrochemical refinery as the target of the TRITON malware [1]. No company has been confidently identified by a third party or self-identified as the victim.

Attribution

The cyberattack was initially attributed to a Nation-state actor due to a lack of financial incentive and significant malware development cost. Furthermore, the high potential for physical impact resulting from the cyberattack is not typical of organized criminal groups. In 2018, Mandiant assessed with high confidence that the malware was developed by a Russian scientific research institute [3]. In 2020, the U.S. Department of Treasury publicly attributed the cyberattack to the same institution and imposed sanctions pursuant to the Countering America's Adversaries Through Sanctions Act [4]. Most recently, the U.S. Department of Justice unsealed an indictment charging Russian national Evgeny Viktorovich Gladkikh, a computer programmer employed by the Russian scientific research institute, with design and deployment of the malware [5]. The threat group is also known by the following aliases: XENOTIME and TEMP.Veles, respectively named by Dragos and Mandiant.

Malware

TRITON malware is a control system framework designed to target Schneider Electric Triconex SIS controllers. The malware was analyzed in depth by various cybersecurity firms like Mandiant and Nozomi and later by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). TRITON malware is also referenced as TRISIS or HatMan within open-source reporting.

Mandiant describes TRITON's feature set as, "*including the ability to read and write programs, read and write individual functions, and query the state of the SIS controller*" [2]. The malware gains these capabilities after modifying in-memory firmware of the controller and exploiting a vulnerable system call that allows for remote code execution. For a deep dive into the technical details of the malware, reference the CISA report [6].

Tactics, Techniques, and Procedures

Lateral Movement (Tactic)

The TRITON threat actor first established a foothold on the corporate network before using Lateral Movement techniques to pivot into the operational network. Mandiant reports that the threat actor was present on the corporate network at least one year prior to gaining access to the SIS.

Masquerading (T0849)

TRITON was configured to masquerade as trilog.exe, which is the Triconex software for analyzing SIS logs [6].

Execution through API (T0871)

TRITON leverages a reimplementation of the proprietary TriStation protocol within its framework to trigger APIs related to program download, program allocation, and program changes [6].

Program Download (T0843) & Exploitation for Privilege Escalation (T0890)

TRITON leverages a previously-unknown vulnerability affecting Tricon MP3008 firmware versions 10.0–10.4. An insecurely-written system call within the firmware is exploited by the downloaded program. The exploit achieves an arbitrary 2-byte write primitive, which is used to gain supervisor privileges and modify the firmware [6].

System Firmware (T0857)

TRITON was programed to read, write and execute code in memory on the safety controller at an arbitrary address within the device's firmware region. This functionality gives TRITON simplistic remote access toolkit capabilities on the compromised SIS [6].

Response

Cybersecurity incident response firms were called to the scene following the SIS failure, however, little else is known about the company's response actions presumably due to non-disclosure agreements.

The manufacturer of the affected product released a security notification in late 2017 that disclosed the vulnerability and provided recommendations for affected asset owners [7].

Outcome

Potential Impact

Loss of Safety (T0837)

TRITON has the capability to reprogram the SIS controller logic to allow unsafe conditions to persist or allow unsafe states. An unsafe state within an industrial process can lead to severe damage or loss of life. Fortunately, the malware was unable to bypass internal security mechanisms of the SIS controller which safely halted the monitored process.

Actual Impact

Loss of Productivity and Revenue (T0828)

While the malware failed to reprogram the SIS without alarm, the victim agency was forced to halt the petrochemical process to investigate the ongoing SIS failures. The shutdown and subsequent investigation caused production and financial losses for the asset owner.

Prognosis and Recommendations

The TRITON malware incident shows how SIS controllers can be targeted by threat actors to potentially cause extreme physical damage or loss of life, highlighting the importance of SIS cybersecurity. While TRITON was unsuccessful in causing physical damage, researchers have validated its capability within test environments [6]. Assuming the adversary did not intend to fail, they are likely investing resources to succeed in their next attempt. Mission owners must acknowledge and decisively act in response to the advancing threats within critical infrastructure cybersecurity. This section provides recommendations aligned with the Cyber Risk to Mission Defense in Depth layers.

Defense in Depth Layer 1: Incident Deterrence

Vulnerability Scanning (M0916), Update Software (M0951), Network Intrusion Prevention (M0931)

Mission owners can deter adversaries from conducting similar cyberattacks targeting SIS by reducing their boundary attack surface and hardening existing Information Technology (IT) infrastructure. Hardening is the process of securing a system by reducing its surface area to attacks and vulnerabilities. Mission owners must understand the different vectors an adversary can exploit to gain initial access to networks and influence those opportunities. They should also be diligent to update and patch their existing infrastructure in a timely manner.

Defense in Depth Layer 2: Remediations

Network Segmentation (M0930), Access Management (M0801), Data Backup (M0953), Redundancy of Service (M0811)

Asset owners should properly segment SIS from Operational Technology (OT) control systems, as well as segment the OT network from the IT network. Segmentation reduces the lateral movement opportunities for the adversary. Measures that prevent unauthorized program download should be leveraged to minimize risk. This can be accomplished by keeping OT systems in an operational mode (e.g. Run or Remote) when the system is active. Program mode should only be used when making legitimate programming changes. Furthermore, owners can implement alarms indicating when a safety system enters programming mode. The victim in this case did not properly segment the safety instrumentation network and allowed the SIS to be programmed due to poor security practices. Lastly, being prepared to restore a SIS controller during failure means keeping accessible software, firmware, and hardware redundancy (backups) when cost-effective and technically feasible.

Defense in Depth Layer 3: Restoration Mitigations

One of the major difficulties asset owners faced in this incident was understanding the cause of SIS failure. The victim's primary safety system support was unable to initially diagnose the failures as a cybersecurity problem. Only after repeated failures did the victim consult cybersecurity specialists who discovered an adversarial presence. Operators must be trained to recognize potential cyberattacks when handling system faults. Additionally, organizations need to understand the resources at their disposal to effectively manage similar incidents. If available, have a plan to call upon external response teams to conduct a thorough investigation of the failure and determine if a cyber event could be a contributing factor.

Defense in Depth Layer 4: Consequence Mitigations

Mechanical Protection Layers (M0805)

This incident highlights the importance of performing a *Layers of Protection Analysis* for missions where a failure could have significant consequences to safety, health, or environment [8]. There should be many layers of protection between initial access and the ultimate consequence, including physical barriers as well as digital equipment. Physical barrier examples include dikes to contain hazardous material, remote locations for potentially hazardous processes and equipment, and pressure relief valves. Safety systems can utilize relay-based logic which carries a reduced risk of cyberattack. By implementing additional layers of protection, mission owners can assume the risk of continued operations during SIS restoration activities.

Defense in Depth Layer 5: Mission Agility

Mission agility requires that mission owners protect their greatest asset, people. When the layers of protection for an industrial process begin to fail, the risk of a safety related event increases greatly. Control and safety operational plans must be documented and communicated to relevant personnel. When operations exceed the acceptable threshold, the safety system should engage. However, if the safety system is not fully operational, then a safe operating procedure or control of defeat should be enacted which may include manual observance and manual engagement of emergency shutdown. Emergency plans must be developed to address contingency operations and emergency response. The prevention of catastrophic industrial events and prioritization of personnel safety will ensure organizations are able to continue fighting in cyber-contested environments.

References

[1] Perlroth, N., & Krauss, C. (2018, Mar 15). *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.* The New York Times. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[2] Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., & Glyer, C. (2017, Dec 14). *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. Mandiant Threat Research. https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton

[3] Fireeye Intelligence. (2018, Oct 23). *TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers*. Mandiant Threat Research. https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools

[4] U.S. Department of Treasury. (2020, Oct 23). *Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware*. Press Releases. https://home.treasury.gov/news/press-releases/sm1162

[5] U.S. Department of Justice. (2022, Mar 24). *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*. Press Releases. https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

[6] CISA. (2019). *MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B).* https://www.cisa.gov/uscert/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

[7] Schneider Electric. (2017). *Security Notification - EcoStruxure Triconex Tricon V3*. https://www.se.com/ww/en/download/document/SEVD-2017-347-01/

[8] Summers, A. (2002). *Introduction to Layer of Protection Analysis.* Journal of Hazardous Materials. https://iceweb.eit.edu.au/sis/SISTech/LayerofProtectAnalysis.pdf

Additional Reading

Miller, S., Brubaker, N., Zafra, D., & Caban, D. (2019, Apr 10). *TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping*. Mandiant Threat Research. https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections

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.* Nozomi Networks. https://icscsi.org/library/Documents/Cyber_Events/Nozomi%20-%20TRITON%20-%20The%20First%20SIS%20Cyberattack.pdf

Sobczak, B. (2019, Mar 7). *The inside story of the world's most dangerous malware.* E&E News. https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/

Related Incidents

Stuxnet (Aug 2010)

The Stuxnet worm was first discovered in 2010 and gained notoriety as the first newsworthy piece of malware to target industrial control systems with the intent to cause physical damage. The malware propagated indiscriminately and was able to cross air-gapped networks via removeable drives. However, Stuxnet would only execute the later stages of its attack after the malware identified a specific set of characteristics associated with the target environment. Open-source reporting suggests the malware successfully damaged the Iranian Nuclear program by modifying centrifuge controller code.

Sources

Falliere, N., Murchu, L., & Chien, E. (2010, Nov). *W32.Stuxnet Dossier*. Symantec Security Response. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Kushner, D. (2013, Mar). *The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program.* IEEE Spectrum. https://ieeexplore.ieee.org/document/6471059

Industroyer/Crashoverride (Dec 2016)

In December 2016, another cyberattack occurred targeting the Ukranian power grid. Unlike the first attack, this instance used a highly customizable and modular malware framework specific to electrical sector systems and protocols. This malware, now known as Industroyer or Crashoverride, marked yet another milestone in adversary development of critical infrastructure malware.

Sources

Dragos Inc. (2017, Jun 12). *CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations.* https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Cherepanov, A. (2017, Jun 12). *WIN32/INDUSTROYER A new threat for industrial control systems.* ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf