Accenture Security

CYBER ADVISORY

INDUSTRIAL CONTROL SYSTEM ATTACK SUMMARY

DEALING WITH THE THREATS POSED BY **TRITON/TRISIS** DESTRUCTIVE MALWARE

In late 2017, a new malware threat targeting industrial control systems was uncovered known as TRITON/TRISIS. With safety instrumented systems (SIS) potentially at risk, companies with industrial operations must take steps to secure themselves against this imminent threat.

WHAT'S THE STORY?

In TRITON[1] (also known as TRISIS[2] or HatMan[3]) a new and disruptive malware and framework has been uncovered, capable of altering and disrupting operations of safety instrumented systems. SIS are used across Oil and Gas, Chemicals, Utilities, and other sectors, to provide a mechanism to safely shut down an industrial process when it has encountered unsafe operating conditions.

WHAT DOES IT MEAN?

SIS, like main process control systems used at industrial plants, can be susceptible to a cyber attack or malware. More common malware, such as ransomware, typically destroys a computer's data (or encrypts it for a ransom), crashing the system or causing a loss of situational awareness. TRITON, however, can replace safety-functional logic with alternative logic crafted by the attacker. Such logic changes could, for example, trip and shut down the process without a safety-related reason. Or worse, fail to engage the safety system when an unsafe condition occurs, leading to infrastructure damage and potentially even loss of life. TRITON was purposefully built to target a specific brand of SIS—Triconex, manufactured by Schneider Electric. Its modus operandi involves disguising itself as legitimate software that is normally used to analyze SIS data and event logs. At the time of the discovery, at least one victim in the Middle East was impacted by an inadvertent plant shut down resulting from the malware.

[1] Named by FireEye

[2] Named by Dragos. Inc.

[3] Named by US Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

WHAT CAN YOU DO?

Based on the attack framework, a similar attack could conceptually be designed against other safety instrumented systems. As such, the recommendations are relevant to many SIS brands and their users.

Take practical steps today to protect your organization from TRITON/TRISIS and similar destructive malware attacks.

The following key security controls could help mitigate the TRITON threat model:

- **Physical controls—**SIS controllers, like all other critical hardware components, should be kept in locked spaces, monitored and accessible to only authorized personnel. The physical mode switch on Triconex controllers should be kept in "Run" position during normal operations, to limit the window of opportunity for a configuration change and enforce requirement of physical presence.[4]
- **Logical access control**—Any form of connectivity to the SIS systems, whether via network interface, USB stick, programming laptop or directly by a user at a graphical interface, should require enforced authorization. Only authorized and properly controlled USB sticks, writable media, and programming laptops, should be used for system access. Portable media should be verified each time before being allowed to connect to SIS.
- **Network segmentation**—SIS components should reside in an isolated network.
- **Configuration and change management—**Industrial Control System (ICS)[5] governance roles, processes, and tools should be in place to facilitate the correct and authorized deployment, maintenance and verification of SIS equipment and its configuration. The ability to detect unauthorized configuration changes can reduce the risk of an attack.
- **Security monitoring and scanning**—It is essential to deploy network security monitoring technology, along with ICS vendor certified scanning technology, where possible. The proper implementation of security monitoring in ICS environments should address the following questions:
  - Is ICS network traffic being monitored for unexpected communication flows and other anomalous activity?
  - Can new devices connecting to the network be detected and trigger a notification?
  - Are all methods of mobile data exchange with the safety network, such as CDs and USB drives, scanned before use in SIS operator stations or any node connected to the network?
  - Have other secure file transfer methods been considered?

[4] Leaving the controller's mode switch in "Program" or "Remote" allows reprogramming activity, potentially circumventing an operator's change management process.

[5] A SIS is one type of ICS.

Analysis of the malware has been conducted by cybersecurity research firms, including the Accenture iDefense team, to provide customers with mitigation steps and strategies. Please refer to the iDefense TRITON/TRISIS Threat Analysis[6] for more information.

Schneider Electric released an Important Security Notification with specific mitigation steps regarding its Triconex safety controllers. Schneider Electric recommends regular checks for updates to the security notification including any specific technical configuration requirements.[7] Given this possibility, ABB also released a Cyber Security Notification on December 22nd, 2017 with similar mitigation steps for its safety controllers.

TECHNICAL REFERENCES

Threat Analysis: INDUSTRIAL CONTROL SYSTEM ATTACK SUMMARY— DEALING WITH THE THREATS POSED BY TRITON/TRISIS DESTRUCTIVE MALWARE, Accenture, 2018.

Important Security Notification: Malware Discovered Affecting Triconex Safety Controllers V1.1, Schneider Electric, 2017.

Cyber Security Notification—TRITON/TRISIS malware, ABB, 2017.

[6] Threat Analysis: INDUSTRIAL CONTROL SYSTEM ATTACK SUMMARY—DEALING WITH THE THREATS POSED BY TRITON/TRISIS DESTRUCTIVE MALWARE, Accenture, 2018.

[7] https://www.schneider-electric.com/en/download/document/SEVD-2017-347-01/

CONTACT US

For additional mitigation steps and more detailed information, please reach out to your Accenture contact. Where support is needed, Accenture Security can provide resources designed to mitigate risks and remediate gaps in ICS security programs.

Luis Luque

luis.luque@accenture.com

Jim Guinn

james.s.guinn.ii@accenture.com

Josh Ray

joshua.a.ray@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

LEGAL NOTICE & DISCLAIMER: All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from iDefense. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS REPORT.