New TRITON attack

Reference: Memo [190411-1] – Version: 1.0
Keywords: Industrial control system (ICS), disruptive malware
Sources: publicly available information

Key Points

- TRITON is a sophisticated malware framework with the capacity to manipulate industrial safety systems, cause physical damage and shut down operations.
- TRITON authors are believed to have ties with a Moscow-based scientific research institute.
- Victims have been identified in the Middle East and in North America.
- A comprehensive analysis of techniques and tools linked to TRITON have been recently published to help detecting and hunting related attacks.

Summary

On December 14, 2017, cyber-security firms uncovered a new malware dubbed TRITON. TRITON can purportedly manipulate industrial safety systems, cause physical accidents and shut down operations. It is an attack framework built to interact with the Triconex Safety Instrumented System (SIS) developed by Schneider Electric. Safety instrumented systems are a type of industrial control system designed to monitor the performance of critical systems, and take remedial action should an unsafe condition be detected. This could include overly high temperatures or pressure readings in industrial systems. SIS is designed to detect such conditions and initiate actions that will put the affected systems back into a safe state. TRITON is one of a limited number of publicly identified malicious software families targeting industrial control systems (ICS), such as Stuxnet, which was employed against a nuclear plant in Iran in 2019 and Industroyer, which was used in the cyberattack on Ukraine's power grid in 2016.

On October 23, 2018, FireEye security firm reported on the malware development activity that led to the creation of TRITON and codename the author TEMP.Veles. According to FireEye, the 'intrusion activity that led to deployment of TRITON was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM; a.k.a. ЦНИИХМ), a Russian government-owned technical research institution located in Moscow.' The project allegedly started at least in 2013 and the authors continually modified their tools to make them stealthier, by reducing for example the probability of anti-virus detection.

On April 10, 2019, FireEye reported they have detected additional intrusion by the attacker behind TRITON at a different critical infrastructure facility. In this case, the threat actor deployed a new custom tool set. The threat actor was allegedly present in the target networks, for almost a year; before gaining access to the Safety Instrumented System (SIS) engineering workstation.

The identity and location of TRITON victims have not been disclosed. However, according to the MIT Technology Review, TRITON was first discovered in the Middle East and has more recently targeted companies in North America.

Comments

Sophisticated targeted attacks against ICS often take years. Attackers must prepare for such an attack by learning about the target's industrial processes and building custom tools. Threat actors may be interested in preparing for contingency operations rather than conducting an immediate attack (e.g. install malware like TRITON and wait for the right time to use it).

To the best of our knowledge, only a small number of malware has been designed to attack ICS and TRITON seems to be the first to specifically target SIS devices. One of the most notable examples of ICS malware was Stuxnet allegedly designed by a nation state to attack programmable logic controllers (PLCs) being used in the Iranian uranium enrichment program.

In its most recent report, FireEye has provided a comprehensive analysis of techniques, tactics and procedures (TTPs) used by TRITON actors. These TTPs are not necessarily exclusively used in TRITON attacks. However, they can be useful to develop suitable detection and hunting strategies. Consequently, CERT-EU will integrate them in its threat actor and TTP knowledge bases so they can be used, when necessary, in its hunting project. For more information, please contact CERT-EU.