Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

24 March 2022

PIN Number

20220324-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with industry partners, DOE, and DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS)

Summary

The FBI is warning that the group responsible for the deployment of TRITON malware against a Middle East–based petrochemical plant's safety instrumented system in 2017, the Russian Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), continues to conduct activity targeting the global energy sector. This warning follows the 24 March 2022 unsealing of a US indictment of a Russian national and TsNIIkhM employee involved in that attack. TRITON was malware designed to cause physical safety systems to cease operating or to operate in an unsafe manner. Its potential impact could be similar to cyberattacks previously attributed to Russia that caused blackouts in Ukraine in 2015 and 2016.

TRITON malware targeted the Schneider Electric Triconex safety instrumented system (SIS), which is used to initiate safe shutdown procedures in the event of an emergency. TRITON malware affected Triconex Tricon safety controllers by modifying in-memory firmware to add additional programming, potentially leading to damage of a facility, system downtime, and even loss of life should the SIS fail to initiate safe shutdown procedures. Schneider Electric addressed the vulnerability (with the Tricon model 3008 v10.0-10.4) when version 11.3 of

the Tricon controller was released in June 2018; however, older versions of the controller remain in use and are vulnerable to a similar attack. As a result, the FBI is alerting the ICS community of continued activity by this group and requests that any indicators of potential compromise be reported to the FBI.

Threat

In June and again in August 2017, TRITON malware (also known as TRISIS and HatMan) was used against a Middle East–based petrochemical facility's safety controllers. The US Government has publicly attributed TRITON malware to TsNIIKhM, a Russian government-controlled research institution that supports the Russian armed forces with advanced research, weapons, and cyber capabilities.

TRITON malware was designed to target a specific SIS controller model, with a specific firmware version, running a small range of specific versioned firmware, and used in critical infrastructure facilities to initiate immediate shutdown procedures in the event of an emergency. For more information on affected equipment and TRITON malware, see CISA ICS Advisory Schneider Electric Triconex Tricon (Update B) and CISA Malware Analysis Report (MAR) HatMan - Safety System Targeted Malware (Update B).

In the 2017 attack, the actor gained initial access and then moved laterally through the information technology (IT) and operational technology (OT) networks onto the safety system and installed TRITON malware. This provided the actor access to and control of Schneider Electric's Triconex devices used in the facility's ICS safety system. The facility automatically entered a safe state after several of the Triconex ICS safety controllers detected an anomaly, caused by software bugs in the TRITON malware. The subsequent investigation of the shutdown revealed the attacker's presence and the malware itself. The facility's automatic shutdown and detection of malware prevented the cyberattack from reaching its full capabilities.

TRITON malware's design gave the attackers complete remote control of the SIS, providing them the capability to cause significant physical damage and loss of life if the plant were to enter an unsafe state, according to investigations and analysis that followed the event. After the August 2017 cyberattack, the actors again obtained unauthorized access to a file server to collect information on how the facility responded to the incident.

The TRITON attack represented a notable shift in ICS targeting as the first attack designed to allow physical damage, environmental impact, and loss of life in the event of a plant's running in an unsafe condition. Critical infrastructure asset owners and operators should be mindful of the risks posed to SIS regardless of vendor, as these safety systems will likely continue to be targeted by sophisticated cyber actors.

Russian cyber actors have previously conspired to deploy malware and take other disruptive actions for the strategic benefit of Russia through unauthorized access to victim computers and ICS. These cyberattacks used some of the world's most destructive malware to date, including

KillDisk and Industroyer, which each caused blackouts in Ukraine in 2015 and 2016, respectively. Russian cyber actors have also deployed non-disruptive malware, such as Havex, which enables the actors to return to compromised and otherwise vulnerable ICS devices for future espionage purposes.

For additional information on the TRITON malware attack, see the FBI PIN titled *Unattributed Cyber Actors Exploiting Internet-connected ICS/SCADA Systems,* PIN 20180614-001.

For more information on Russian state-sponsored malicious cyber activity, see cisa.gov/uscert/Russia.

Recommendations

The FBI encourages potentially affected critical infrastructure asset owners and operators to maintain business continuity plans to minimize essential service interruptions, as well as preemptively evaluate potential continuity and capability gaps. Asset owners and operators should regularly assess and monitor their SIS systems, personnel with access to these systems, and practice contingency plans.

Furthermore, the FBI encourages those potentially affected to review Schneider Electric's guidance set forth in its Security Notification for the EcoStruxure Triconex Tricon, revision 3. Through the enhanced Tricon CX controller, version 11.4 and later versions, Schneider Electric has enhanced security and mitigated the risk of the TRITON malware's attack vector, reducing further the risks of these type of malware incidents; however, network defenders should remain vigilant.

Based on the attack framework and malware used in the original TRITON incident, a similar attack could be designed against other SIS. Therefore, the following recommendations are relevant to many SIS vendors and brands, along with their customers. The best practices listed below are applicable to most SIS products used in critical infrastructure facilities today.

SIS Best Practices

- Use a unidirectional gateway for applications that need to receive data the SIS provides.
- Implement change management procedures for safety controller run-state key positions and regularly audit physical keys.
- Ensure the cybersecurity features in SIS products are always enabled by following the manufacturers' security recommendations.

- Safety systems should always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment, or the safety network.
- All controllers should reside in locked cabinets and never be left accessible to unauthorized personnel.
- All engineering workstations should be secured and never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB, drives, DVDs, etc. should be scanned before use in the SIS engineering workstations or any node connected to this network.
- Operator stations should be configured to display an alarm whenever the SIS safety controller key switch is in the "PROGRAM" mode.
- Check network appliances, webservers, and third party vendor logs for early stage reconnaissance activity against: job postings, pages listing employee social media accounts, websites for facility subdomains, employee email addresses, pages listing third party vendors, and equipment specific to identified facilities.

Resources:

- CISA Joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)
- CISA MAR HatMan - Safety System Targeted Malware (Update B)
- NSA and CISA Joint Cybersecurity Advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems
- CISA's Fact Sheet Rising Ransomware Threats to Operational Technology Assets. Although tailored to ransomware, the Fact Sheet provides applicable guidance for critical infrastructure entities to reduce cyber threats to their OT assets.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.