National Cyber Security Centre

a part of GCHQ

TRITON Malware Targeting Safety Controllers

22nd December 2017

About this Document

The NCSC is aware of reporting relating to malware dubbed 'TRITON', discovered to be targeting Triconex safety controllers. This advisory outlines mitigations to secure networks against these attacks. If you believe you may have been affected by this or similar ICS (Industrial Control System) malware, then please contact the NCSC Incident Management team.

Handling of the Report

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE, which means it can be shared within and beyond the CiSP community with no handling restrictions.

Disclaimer

Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

Background

Reporting (see below) suggests a single user of Triconex Tricon safety shutdown systems has been targeted, resulting in a safe shutdown of their plant operations.

The NCSC believes this to be a highly targeted attack. To deploy and successfully activate such malware, the attacker would need to know a target environment in depth. The process of acquiring this knowledge may take several weeks or months, during which the attacker is likely to have used engineering documentation and enumeration of the network to further their goals. Detection at this stage of the compromise is critical to successfully mitigating an attack.

This latest attack represents a further evolution in ICS attack methodology. As ICS becomes increasingly connected, threat actors will continue to develop their capabilities to exploit them. Such incidents underline the importance of organisations implementing effective mitigation approaches.

TRITON Malware

TRITON malware has the capability to reprogram Triconex controllers with custom attacker-defined payloads when a Triconex device is running in “PROGRAM” mode. From available reporting, we believe the malware can read/write programs, read/write functions and query the state of an SIS (Safety Instrumented System) controller.

To deploy the malware, the attackers compromised an SIS engineering workstation. Actions taken by the attackers from the compromised system resulted in the controllers entering a failed safe state, automatically shutting down the industrial process.

The NCSC has no information to suggest that the malware is more broadly deployable. However, we recommend that the following detection and mitigation activities are carried out not just for Triconex safety controllers, but for all SIS environments.

Detecting TRITON

As we believe TRITON to be highly targeted, it is unlikely that traditional indicators such as file hashes will be relevant to any other intrusion. On that basis, we recommend the following steps to detect malware which may impact upon safety systems:

1. Over the coming days and weeks, signatures and indicators of compromise (IoCs) will become available which will allow the detection of this specific class of malware. The NCSC recommends that operators deploy these signatures where possible and investigate any detected activity.

2. Consider deploying a host-based agent to key boundary systems in both the corporate and ICS environments. This will provide visibility of threat actor actions on the systems as well as aiding in the response to an incident. This is, of course, even more relevant if your SIS is not isolated from other systems.

3. Consider deploying application whitelisting technology and/or a host-based agent onto non-critical systems that support the SIS (such as laptops or workstations).

4. Where possible, aggregate host, network and log data from your OT (Operational Technology) environment into a high-security SOC (Security Operations Centre) and develop an approach to quickly identify key indicators in this data (such as new binaries dropped onto machines or anomalous network activity).

It may be possible for a threat actor to repurpose the “TRITON” malware to be used against UK infrastructure, but it would require significant further effort to do so. As this malware has been developed for a specific target system, it is highly likely that any future malware will not match initial signatures. It is therefore important to develop detection strategies which will identify signs of malicious activity without relying on specific malware signatures.

Mitigation Approaches

We recommend that organisations take the following steps to ensure that safety systems are protected appropriately:

1. **Discovery**: Identify the SIS which your organisation operates. If an appropriate forum does not already exist, consider bringing together safety and cyber security experts across your organisation to ensure that you can conduct the following mitigation steps.

2. Connectivity: For each of the systems identified, document whether or not the SIS is isolated from the rest of the control system. Where there is connectivity to another system, investigate and document the connection mechanism (IP/serial/bespoke).

3. Isolate: Where it is possible to do so, an SIS should be an isolated system and protected in accordance with the guidelines from the manufacturer. Where this is not possible, ensure that a complete risk assessment has been conducted and appropriate countermeasures deployed to maintain the integrity of the SIS.

4. Risk revalidation: Revalidate previous risk assessments and adjust to ensure continued protection of the integrity of the SIS.

5. Operating mode: Verify whether the SIS provides a mechanism which prevents re-programming or network access to the device during operation. If this feature is available, then visually verify that the devices are switched to 'run-mode' or equivalent. Log and investigate all exceptions to this. This may mitigate some actions a threat actor can take in the network; however, the best defence is to detect the threat actor before it gets to this point.

6. Physical protection: An SIS should be protected physically to prevent malicious or accidental breaches of the safety loop integrity.

7. Network and logical segmentation: Ensure that the trust model is such that the ICS boundaries and environments do not implicitly trust Active Directory (which is likely to be a target of compromise).

8. Authentication: Ensure that any systems which connect to the ICS from the corporate network are strongly authenticated and consider using 'browse-down' techniques to prevent exploitation of critical systems. Review authentication, authorisation and access control mechanisms for OT devices.

9. Internet access: End user devices and critical systems in the ICS or administrator’s environments should not have internet access (e.g. email/browsing). SIS administration systems such as laptops should also not have internet access. Consider whitelisting internet communications to prevent connectivity to unknown websites.

10. Patching and software updates: Only modern and patched components should be deployed on the boundaries of OT networks. Software deployed to SIS environments should be validated with the vendor using a suitable (and preferably cryptographically secure) mechanism.

Reporting References

- Schneider Security Notification
- FireEye
- Dragos

Relevant NCSC Guidance

- Making sense of cyber security in OT environments
- Good practice guides for securing Industrial Control Systems
- Getting started with the End User Device security guidance