Contents

[**G0088 Temp.Veles** 2](#_Toc179362643)

[**I. Introduction** 2](#_Toc179362644)

[**II. Tactics** 2](#_Toc179362645)

[**III. Techniques** 2](#_Toc179362646)

[**IV. Procedures** 3](#_Toc179362647)

[**V. Summary** 4](#_Toc179362648)

[**References** 6](#_Toc179362649)

## **G0088 Temp.Veles**

## **I. Introduction**

Temp.Veles, which is also known as XENOTIME and Triton, is an advanced persistent threat group that has been active since at least 2014. The group is notable for its focus on industrial control systems (ICS) and operational technology (OT) environments, particularly in the energy sector. Temp.Veles gained significant attention in the cybersecurity community for its development and deployment of the TRITON malware, which specifically targets safety instrumented systems (SIS).

## **II. Tactics**

Temp.Veles' tactical approach is characterized by

1. ***ICS/OT Targeting***

Specialized focus on compromising industrial control systems and operational technology environments.

1. ***Long-term Persistence***

Emphasis on maintaining extended access to compromised networks for potential future operations.

1. ***Custom Malware Development***

Creation of highly specialized malware designed to interact with and manipulate industrial systems.

1. ***Stealthy Reconnaissance***

Extensive network mapping and system analysis before deploying final payloads.

1. ***Potential for Destructive Impact***

Capability to not just gather intelligence but also potentially cause physical damage to industrial processes.

## **III. Techniques**

Temp.Veles employs a range of sophisticated techniques

|  |  |
| --- | --- |
| Techniques | Description |
| Network-Based Attacks (T1190) | Exploitation of internet-facing devices in target organizations. |
| Custom ICS Malware | Development and deployment of TRITON malware targeting Schneider Electric Triconex Safety Instrumented System (SIS) controllers. |
| Living off the Land (T1059) | Use of legitimate administrative tools and protocols to blend in with normal operations. |
| Credential Theft (T1003) | Harvesting of credentials to facilitate lateral movement within target networks. |
| Command and Control (C2) Infrastructure | Use of compromised websites and legitimate services for C2 communication (T1102.002) |
| Defense Evasion | Mimicking of legitimate system files and processes (T1036).  Use of custom obfuscation techniques for malware components (T1027). |
| Persistence | Establishment of multiple persistence mechanisms to ensure long-term access (T1505). |

## **IV. Procedures**

The group's typical attack chain follows this sequence

***1. Initial Access***

a. Exploitation of internet-facing systems, often leveraging known vulnerabilities.

b. Use of stolen credentials, potentially obtained through spear-phishing or purchased from other threat actors.

***2. Execution and Persistence***

a. Deployment of custom tools for network enumeration and lateral movement.

b. Establishment of multiple persistence mechanisms to ensure continued access.

***3. Discovery***

a. Extensive network reconnaissance to identify critical systems and potential targets.

b. Detailed mapping of industrial control system environments.

***4. Lateral Movement***

a. Use of stolen credentials and exploitation of network vulnerabilities to move laterally.

b. Leveraging of legitimate administrative tools to avoid detection.

***5. Collection and Impact***

a. Gathering of sensitive information about industrial processes and system configurations.

b. Potential deployment of TRITON malware to manipulate safety systems.

***6. Operational Security***

a. Use of custom obfuscation techniques to avoid detection.

b. Mimicking of legitimate system processes to blend malicious activities with normal operations.

## **V. Summary**

Temp.Veles has become one of the notable APT actors in the Threat Intelligence, and it has distinguished itself as a player specifically interested in attacking ICS and has the tools in its arsenal that allows it to create malware that can disrupt critical infrastructure. This group may be classified as one of the significant changes in threats in the cyberspace, from spy activities to those causing physical damage.

One of the most dangerous products of it is the TRITON malware of the group. Developed to target Schneider Electric’s Triconex Safety Instrumented System controllers, TRITON has the potential to disable injurious safety measures in industrial plants. Leveraging this capability to close the cyber-physical gap intensifies the mix greatly since cyber threats could result in critical, physically real-world harm. Temp.Veles’s operations are quite slow and calculated, as evidenced by the monitors which show the group often retaining persistent access for several weeks before unleashing their malware. This approach allows for detailed reconnaissance and increases the likelihood of a successful attack.

The activities of Temp.Veles underscore the growing importance of securing industrial networks and implementing robust segmentation between IT and OT environments. With such complex structures in industrial systems getting integrated with digital systems the risks posed by such groups are set to rise. Although the level of granularity in attributing such attacks to anyone is still problematic due to the outstanding operational security of this group, their activities have raised a lot of concern in both cybersecurity and industrial control systems. The ability of cyber threats to actually make physical changes to critical assets previews a fresh paradigm in the threat landscape requiring critical infrastructure sectors to reset their security posture and spark a discussion on the growing trend of the convergence of cyber and kinetic risks.

## **References**

1. FireEye. (2017). "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure." <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>

2. MITRE ATT&CK. (2024). "TEMP.Veles, G0088." <https://attack.mitre.org/groups/G0088/>