# TECHNIQUE T881: SERVICE STOP

| CyOTE Use Case(s) | MITRE ATT&CK for ICS® Tactic |
|---|---|
| Alarm Logs, HMI | Inhibit Response Function |
| **Data Sources** | |
| **Potential Data Sources** | Kernel Mode eBPF, kprobe, Kernel Trace, bcc, bpftrace, Network Traffic, File IO |
| **Historical Attacks** | Industroyer/CRASHOVERRIDE[1] |

**TECHNIQUE DETECTION**

The Service Stop technique[2] (Figure 1) may be detected when critical services are halted or rendered unavailable to users.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack within their operational technology (OT) networks. However, for the Service Stop technique, the CyOTE program recommends the use of the Extended Berkley Packet Filter (eBPF) technology to develop a capability for identifying Service Stop in an AOO's OT environment. Additionally, by referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

**PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS**

The Service Stop technique was used in the Industroyer attack in the Ukraine in 2016.[6,7] In this attack, the following observables were identified:

- Firmware updates to SIPROTEC relays causing them to fail to perform functions
- New processes being created or terminated

---

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] MITRE ATT&CK for ICS, T881: Service Stop, https://collaborate.mitre.org/attackics/index.php/Technique/T0881
[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.
[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.
[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.
[6] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[7] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Cybersecurity for the Operational Technology Environment

TECHNIQUE T881:
SERVICE STOP

Office of Cybersecurity,
Energy Security, and
Emergency Response

U.S. DEPARTMENT OF
ENERGY

- Modified Windows Registry keys

*Disclaimer: Past occurrences are not guaranteed to occur in future attacks.*

## COMPREHENSION

In the Industroyer attack, the adversary used the Service Stop technique in conjunction with forcing devices to shut down/restart to render devices unresponsive, stop them from performing intended functions, and execute further control of the system. They were able to do this once they had gained access to the Data Historian to initiate the compromise and had begun issuing malicious commands to devices. They were then able to take control of the system and manipulate it to cause impactful and damaging changes.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Service Stop technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

## CURRENT CAPABILITY

As previously noted, the CyOTE program recommends the use of the eBPF technology to develop a capability for identifying Service Stop in an AOO's OT environment. The eBPF technology, located in the Linux kernel, allows for visibility of service stops and provides a monitoring capability. This capability allows an AOO to monitor for potentially malicious activity, and software/service stops in the operating system, without affecting normal operations.

## POTENTIAL ENHANCEMENTS

Future enhancements of the published process monitor software are envisioned to include network logging that is triggered by an anomaly, located in Kernel process space, and running outside the operating system.

## ASSET OWNER DEPLOYMENT GUIDANCE

For operational technology (OT) deployment, users should consult the code examples and documentation provided by the Linux Foundation as part of the *IO Visor*[9] and *bcc suite*[10] of tools. These tools provide example *eBPF* functionality and working frameworks for use.

*AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.*

*AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.*
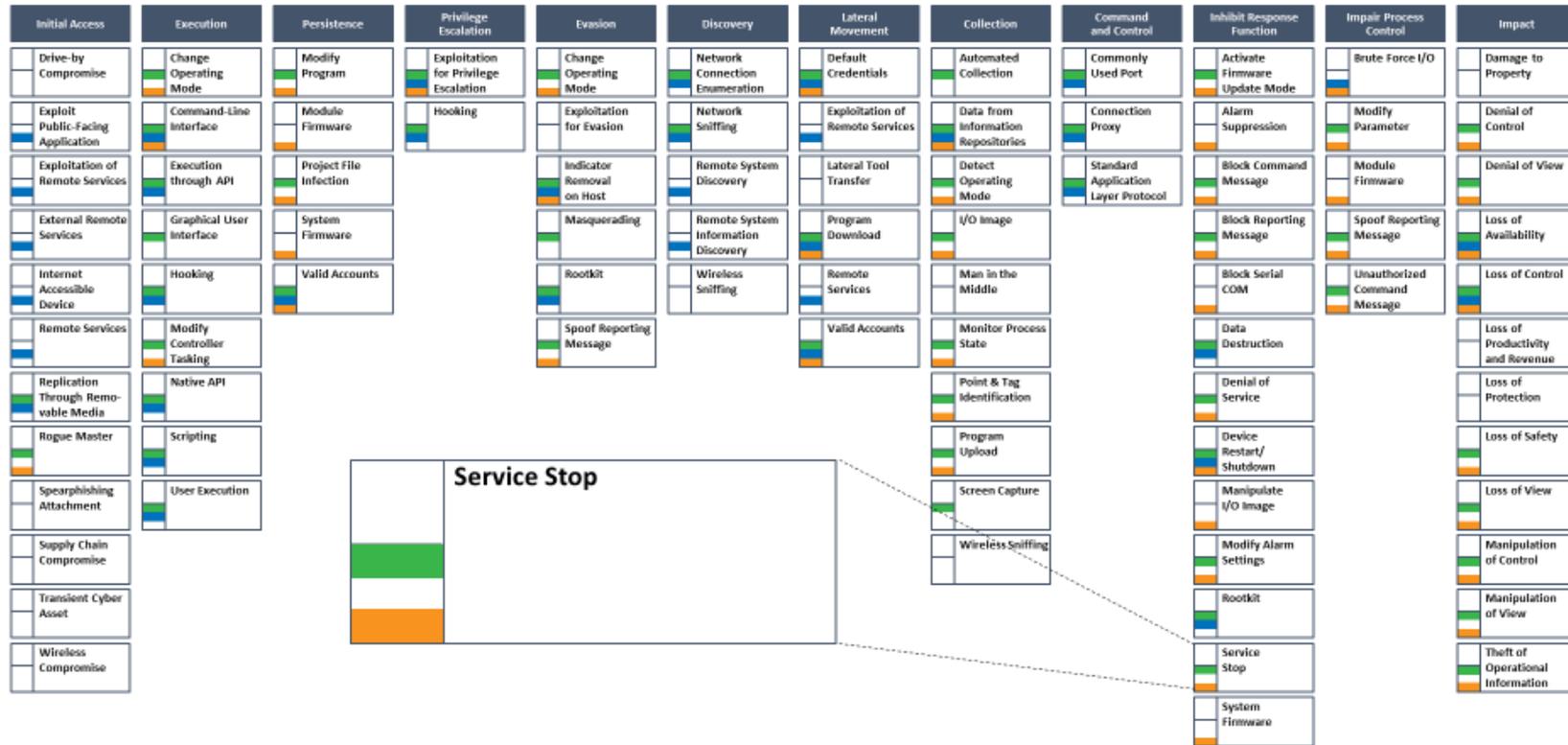
---

[8] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.
[9] https://www.iovisor.org/technology/bcc
[10] https://github.com/iovisor/bcc

**CyOTE** Cybersecurity for the
Operational Technology
Environment

Office of Cybersecurity,
Energy Security, and
Emergency Response

| Click for More Information | [CyOTE Program](#) || [Fact Sheet](#) || [CyOTE.Program@hq.doe.gov](#) |
|---|---|

Figure 1: ICS ATT&CK Framework[11] – Service Stop Technique