TECHNIQUE T806: BRUTE FORCE I/O

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, Remote Login	Impair Process Control
Data Sources	
Potential Data Sources	Packet Captures, Operating System Stack Logs, Data Historian, NetFlow Logs, Alarm History, Application Logs
Historical Attacks	Industroyer/CRASHOVERRIDE[1]

TECHNIQUE DETECTION

The Brute Force I/O technique[2] (Figure 1) may be detected when there are unnecessary or excessive I/O connections to network systems or devices and unauthenticated messages being sent across these systems or devices.

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 for techniques like Brute Force I/O within their operational technology (OT) networks. 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 Brute Force I/O technique was used in the Industroyer attack in the Ukraine in 2016.[6,7] In this attack, the following observables were identified:

- An increase of packet traffic
- Unnecessary connections to the data historian or to devices
- Unfamiliar IP addresses noted in NetFlow logs

---

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] MITRE ATT&CK for ICS, T806: Brute Force I/O, https://collaborate.mitre.org/attackics/index.php/Technique/T0806
[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

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

COMPREHENSION

In the Industroyer attack, the adversary was able to change I/O values in the system once they had gained access to the Data Historian and initiated the compromise. They were able to brute force I/O point values to switch states of Information Object Addresses (IOA), and they caused impactful and damaging changes through the use of other techniques, including Device Restart/Shutdown, Service Stop, Manipulation of Control, and Manipulation of View.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Brute Force I/O 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

The CyOTE Proof of Concept tool implementation uses Zeek[9] (formerly Bro) to parse ICS protocols and extract data fields to Zeek logs. These logs are then analyzed with Splunk[10] and Gravwell[11] using each tool's standard ingestion process. Queries and dashboards have been developed which identify some commands and statistical anomalies indicative of a Brute Force I/O exploitation. Unique reports can be exported using the analysis tool(s) or viewed in already-developed dashboards.

Custom parsers were built for the following protocols: Schweitzer Engineering Labs (SEL) protocols (ASCII, Fast Message, Synchrophasor), Manufacturing Message Specification (MMS), Inter-Control Center Communications Protocol (ICCP) over MMS, and SES-92.

Parsers supported by native or other publicly available plugins include: BACnet, ETHER/IP, CIP, Profinet, S7comm, MS-TDS, Modbus, and DNP3.

POTENTIAL ENHANCEMENTS

The CyOTE Proof of Concept tool is available as a Zeek plugin for AOOs to integrate into their own Zeek infrastructure. The parsers may require additional research to be able to tailor them for other environments. An AOO could also tailor the Proof of Concept tool based on the protocols being implemented in their OT environment. Below are examples of fields that would be needed to detect Brute Force I/O attempts based on an AOO's OT environment:

- Commands addressed to device registers of I/O devices to repetitively overwrite data, manipulate processes, and possibly cause Denial of Service. Example commands: DNP3 "Write" and SEL ASCII "SET."
- Commands returning "tag" name, settings, and other information may reveal I/O addresses of analog and digital I/O modules to aid in enumeration.

[8] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.
[9] https://zeek.org/
[10] https://www.splunk.com/
[11] https://www.gravwell.io/

- Traffic from human-machine interface (HMI) user software to device analog and digital I/O modules containing values to assign or actions to perform.

ASSET OWNER DEPLOYMENT GUIDANCE

The operational tool should be able to deploy the fully developed parsers as plugins in their own Zeek infrastructure. The Zeek logs will then be sent to a log analysis tool such as Splunk or Gravwell. Example queries and dashboards will be provided in the plugin documentation specific to the Brute Force I/O technique.

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.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov

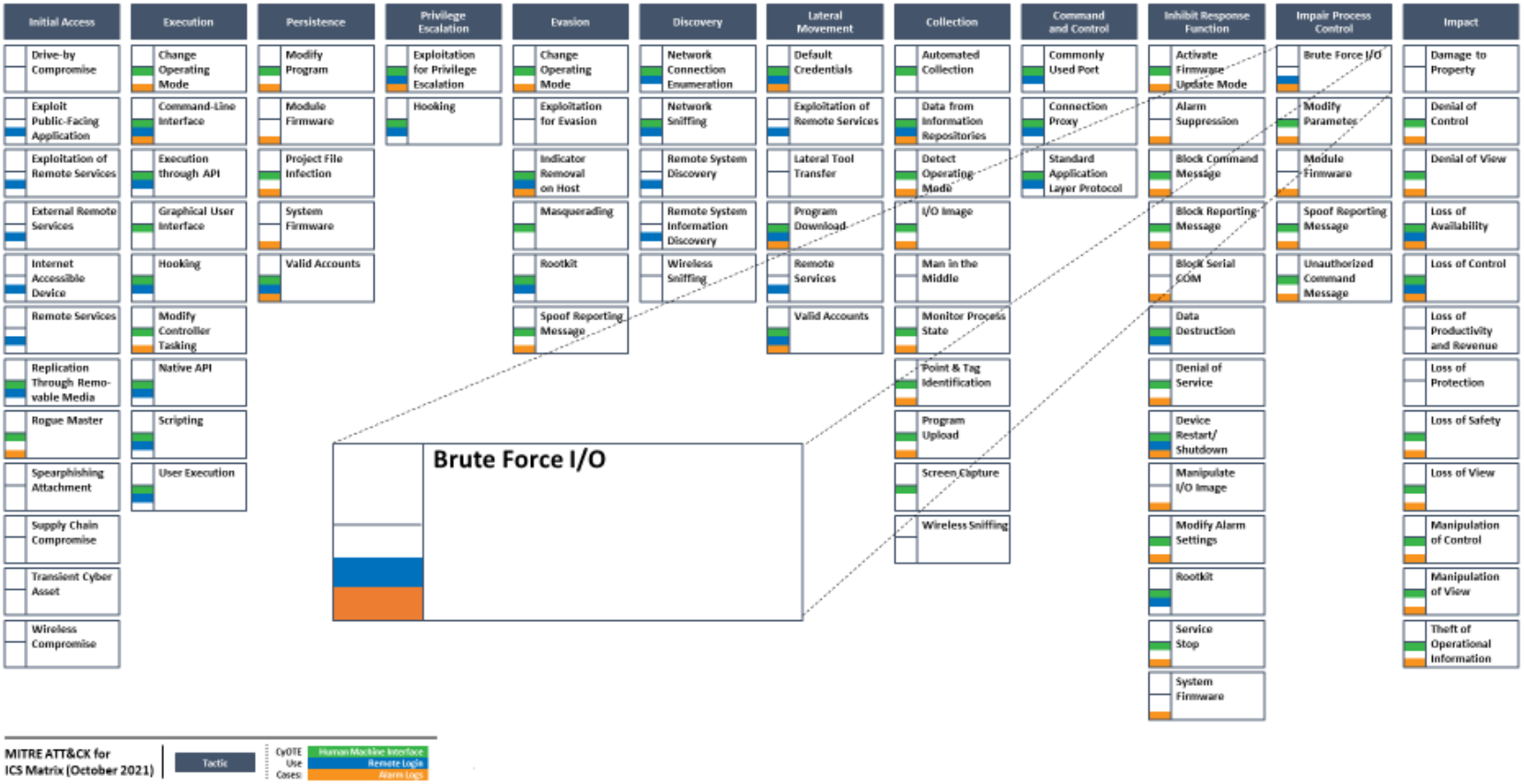

Figure 1: ICS ATT&CK Framework[12] – Brute Force I/O Technique

[12] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.