PRACTICAL CONTROL ENGINEERING PRINCIPLES TO IMPROVE THE SECURITY AND PRIVACY OF CYBER-PHYSICAL SYSTEMS

UC SANTA CRUZ | Baskin Engineering

Fooling a Nation-State Malware Attacking the Power Grid

Luis Salazar, Juan Lozano, Keerthi Koneru, Sebastián Castro, Alvaro Cardenas
{luedsala, juclozan, kkoneru, scastro9, alacarde}@ucsc.edu

Problem

War is an act of force (physical harm or intimidation) for political purposes to motivate the enemy to do the attacker's will. Most nations who rely on their military for political purposes now **consider cyberspace as an official theater of conflict,** therefore opening a threat to new sophisticated adversaries.

There have been well-known examples of malware attacks targeting industrial protocol payloads **causing real-world physical damage,** which include **Industroyer and Triton.** These episodes have been attributed to two different entities within the **Ministry of Defense of Russia: the GRU (Industroyer) and TsNIIKhM (Triton).**

Industroyer and its variants represents the only known instance of malware specifically designed to cause power blackouts, **yet they have received little attention from the cybersecurity academic community.**

We must be prepared to analyze and respond to future cyber-attacks to critical infrastructure systems.

Timeline

December 23, 2015, First known instance where a cyberattack had disrupted a power grid. *Manual attack.*

December 17, 2016. Ukraine's capital Kyiv experienced a blackout because of *Industroyer v1*.

April 8, 2022. *Industroyer v2* attacking the power grid discovered during the Russian invasion of Ukraine (no blackout).

Industroyer

Goal: Disrupt the power grid of a nation by altering the behavior of specific substations.

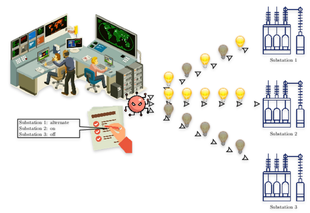
Industroyer v1: A post-exploitation attack framework that allows an attacker to launch attacks using multiple industrial control protocols.

IEC-60870-5-101: Legacy serial protocol. Configurable serial port, target device ID, and target circuit breakers IDs.

IEC-60870-5-104: Remote TCP protocol. Highly configurable: target IP, device ID, circuit breakers IDs, attack pattern, and command type.

IEC-61850-8-1: Object oriented protocol for local networks in a substation. Configurable IP addresses, with automatic network scanning capabilities.

OPC-DA: client-server standards for communicating with real-time devices. Does not require any configuration.



Industroyer v2: Post-exploitation stand-alone executable with hard-coded configuration.

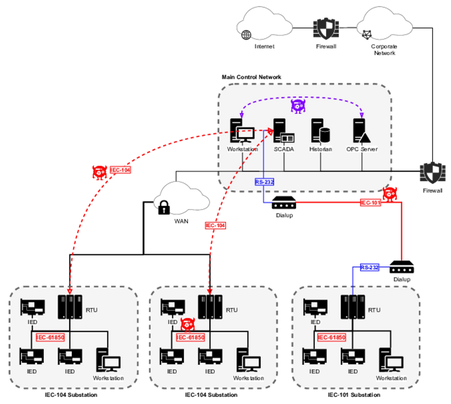
The attackers knew the target IP addresses, device IDs, and target circuit breakers for each target substation.

```
.rdata:00409818                 text "UTF-16LE", '192.168.122.2 2404 2 0 1 1 PService_PPD.exe 1 "D:\O'
.rdata:00409818                 text "UTF-16LE", 'IK\DevCounter" 0 1 0 0 1 0 0 8 1104 0 0 0 1 1 1105 '
.rdata:00409818                 text "UTF-16LE", '0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0 '
.rdata:00409818                 text "UTF-16LE", '1 5 1101 0 0 0 1 6 1102 0 0 0 1 7 1103 0 0 0 1 8 ",0
.rdata:004099AE                 align 10h
```

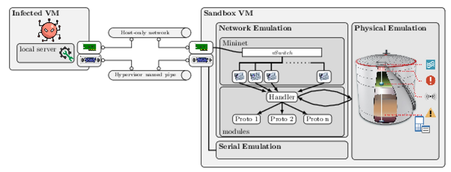
Evolution: The attackers decided the most effective attack using **IEC-60870-5-104** from the control center. Its behavior ***resembles a human operator*** making changes on multiple circuit breakers.

Sandbox

Each payload presents a different attack vector from which the malware launches the attack. The sandbox scenario must replicate these conditions to **fool the malware.**



Our sandbox creates the necessary network components and devices to provide a convincing interaction with a power grid, **reflecting any changes on a simulated physical process**.

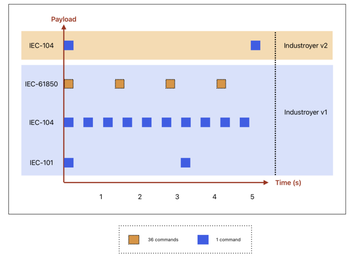


Supported Industrial protocols:
IEC-60870-5-101
IEC-60870-5-104
IEC-61850
Modbus

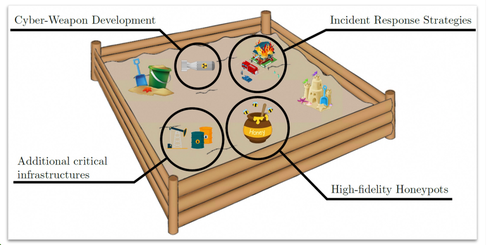
Evaluation

During our evaluation, we successfully executed a malware sample under controlled conditions. For each payload, we determined the timing of the attack performed by the malware, which provided some insights into the behavior and semantics of the attack. As each payload uses a different protocol intended for a particular communications channel, each attack presented a specific timing in relation to the available bandwidth.

Industroyer Attack Patterns



Future Work



Award ID#: 1931573