Blekinges Tekniska Högskola

Cyber Threat Intelligence report: Industroyer

Gabriella Andersson
Civilingenjör inom Datorsäkerhet
Nätverksäkerhet 2, DV1591

May 16, 2025

Contents

1 Introduction

In the world of cybersecurity, Industroyer is a significant cause for concern. This particular type of malware poses a serious threat to the systems that control critical infrastructure like power grids. Industroyer is also known as CrashOverride and it gained reputation through a major attack on Ukraine's power grid in 2016. The repercussions of this attack highlighted the potential devastation that such malware could inflict on essential services. This report is all about breaking down Industroyer, figuring out how it works, and understanding the risks it brings to industrial control systems (ICS).

2 Attribution and Sources

Dragos researches discoverd strong links between the Industroyer attack and the Sandworm Team who was responsible for the 2015 outage in Ukraine. Futher investigation suggested that the group behind Industroyer, ELECTRUM, may have served as the ICS capability development team for Sandworm. There is a possibility that ELECTRUM had increased operational autonomy during 2016 events in Kiev. Aligned with Russian strategic interests, ELECTRUM is considered a capable and well-resourced adversary, demonstrating specialized development capabilities for ICS-specific software. Despite uncertainties, available information indicates that ELECTRUM remains operationally active [2].

3 Indicators of Compromise and Attack

3.1 Indicators of Compromise

The following indicators of compromise are retrived from ESET senior Malware Researcher, Anton Cherepanov report on Inustroyer [1].

3.1.1 SHA-1 hashes:

```
F6C21F8189CED6AE150F9EF2E82A3A57843B587D
CCCCE62996D578B984984426A024D9B250237533
8E39ECA1E48240C01EE570631AE8F0C9A9637187
2CB8230281B86FA944D3043AE906016C8B5984D9
79CA89711CDAEDB16B0CCCCFDCFBD6AA7E57120A
94488F214B165512D2FC0438A581F5C9E3BD4D4C
5A5FAFBC3FEC8D36FD57B075EBF34119BA3BFF04
```

B92149F046F00BB69DE329B8457D32C24726EE00
B335163E6EB854DF5E08E85026B2C3518891EDA8

3.1.2 IP addresses of C2 servers:

Note that most of the servers with these IP addresses were part of Tor network. Which implicates that these indicators could result in a false positive match.
195.16.88[.]6
46.28.200[.]132
188.42.253[.]43
5.39.218[.]152
93.115.27[.]57

3.2 Indicators of Attack

There were many techniques and tactics used during the attack on Ukraine in 2016. In Figure 1 the different techniques and tactics are displayed according to MITRE ATT&CK ICS database. The highlighted cells are techniques detected by KICS for Networks and KICS for Nodes [4]. Given that these methods and tactics have been used, all of these can be seen as potential indications of an attack, but beyond this, it is important to monitor abnormal network traffic and unusual behavior within the system that can suggest malicious activity.

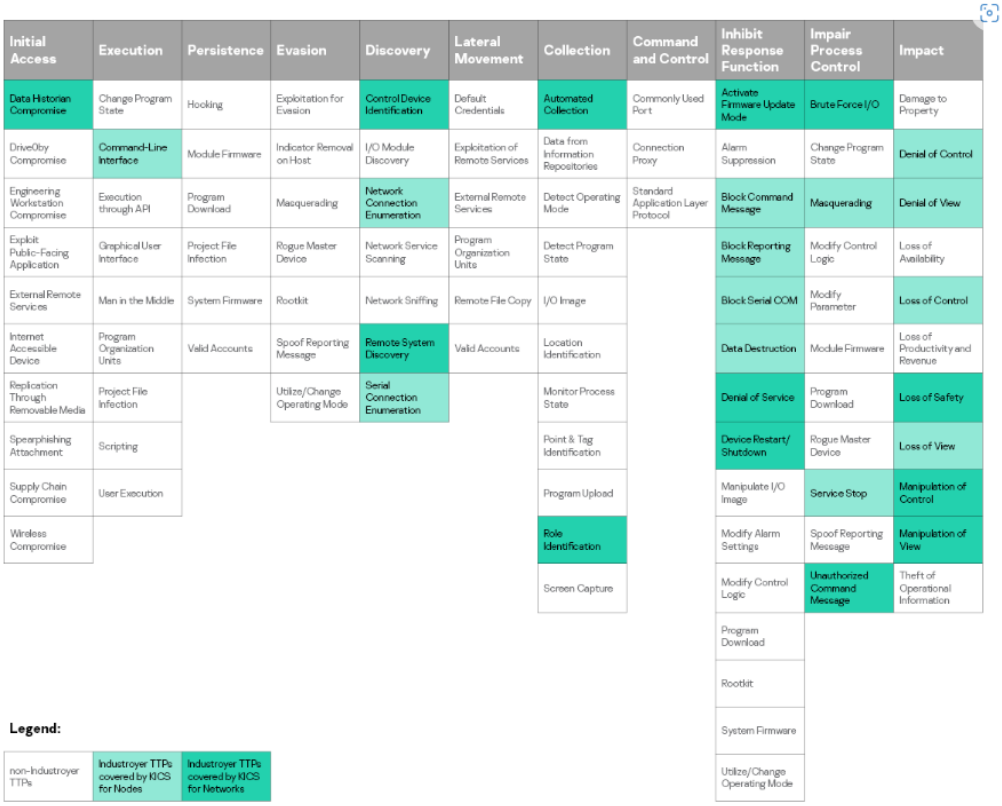

Figure 1: Techniques and tactics used during the Industroyer attack [4].

4 Components Overview

Industroyer is a modular framework that is composed of different parts. Such as a main backdoor, additional backdoor, loader module, data wiper, port scanner tool, DoS tool, and many other modules to support its operations. The main backdoor provides access to the infected system and to the loader module. The loader module enabels effect on the taget and the individual payload modules[1][2].

4.1 Main Backdoor

The central component of Industroyer is the main backdoor, which serves as the key element controlling all parts of the malware. It establishes a secure connection to a Command and Control (C2) server through a local network proxy, using HTTPS. The backdoor has a unique feature allowing

the attackers to specify a particular activation hour, making it harder to detect. However, the analyzed samples from the attack in 2016 operate continuously. When connected, the backdoor sends important data, including hardware profile GUID, malware version, hardcoded ID, and results of executed commands. Most associated C2 servers use Tor for added security [1].

To access the ICS network, the malware uses a backdoor module that communicates with a hardcoded proxy. It employs an internal proxy on TCP 3128, checks the system's default user agent, configures periodic beacons, and retrieves commands from the C2 server. The execution of the malware leaves behind various artifacts such as mutex values, file writing, and service manipulation, with the latter being the only method for persistence. This allows the adversary to specify a system service for the backdoor to load during system boot. Despite offering diverse options, the absence of a command for data exfiltration suggests a primary focus on enabling access, executing commands, rather than explicit espionage or data theft functionality [3].

4.2 Additional Backdoor

The additional backdoor serves as another way for attackers to persist in the network if the main backdoor is found or stopped. This alternative backdoor appears as a modified version of the Windows Notepad application, keeping all its normal functions but hiding malicious code. When attackers gain administrator privileges, they can swap the real Notepad with the tampered one. The concealed malicious code, when decoded, makes a connection to a different remote C2 server, not the one connected to the main backdoor. It then helps in fetching a payload, a piece of shellcode loaded directly into the computer's memory and executed. Additionally, the injected code decrypts the original Notepad code stored at the end of the file and guides the computer to run it [1].

4.3 Launcher Component

In the sequence of the attack, a specialized loader executable, referred to as the Launcher, plays a crucial role in loading ICS payload modules and the data wiper module. Dragos acquired a single sample of this file named the Launcher. Upon activation, this sample initiates a service named defragsvc, loads the module DLL through an exported function called "Crash" and creates a new thread with the highest priority. The control then shifts from the launcher to the loaded module, while the launcher awaits a one to two-hour

interval before triggering the execution of the data wiper [3].

4.4 101 payload

The 101 payload, named after the IEC 101 international standard for electric power systems control, manifests as a DLL file with the filename "101.dll." It partially implements the IEC 101 protocol standard, fostering communication between ICS and Remote Terminal Units (RTUs). Upon activation, the payload examines its INI configuration file, extracting details like process names, Windows device names (including COM ports), and Information Object Address (IOA) ranges [1].

The payload specifically targets a suspected application on the victim's machine, presumed to engage in serial communication with the RTU. Through the utilization of designated Windows API functions and communication channels via configured COM ports, the payload establishes control over the RTU. The methodical process involves iterating through defined IOA ranges, constructing packets to manipulate the On/Off states of both single and double command IOAs. This carefully synchronized approach, spanning three stages—switching IOAs to Off, inverting IOA states to On, and returning IOAstates to Off—empowers the 101 payload to exert control and manipulate the operational states of the RTU device [1].

4.5 104 payload

IEC-104 is quite similar to IEC-101, but it uses TCP/IP for communication. This means that the configuration file for IEC-104 payloads needs a target IP address, similar to how IEC-101 operates with an open/closed effect. The execution flow of the IEC-104 module is quite simple: the launcher calls the "Crash" function from the IEC-104 DLL, starts a client thread, initiates a new communication process or replaces an existing one based on configuration, creates a socket to send traffic to controlled devices, and logs the traffic. After completing this routine, control goes back to the launcher, waiting for the countdown to trigger the destructive module [1].

4.6 61850 payload

IEC-61850, a widely adopted standard for substation communications, has a more extensive reach compared to IEC-101 and IEC-104, causing heightened

concerns for operators globally. This attack module exists in two versions: an EXE with a specific configuration file and a DLL using the "Crash" export functionality. The initialization process for both closely resembles previous modules, with the EXE requiring a unique configuration file, "i.ini," in the same directory. The EXE operates as a standalone executable with fixed options, while the DLL relies on the launcher with specified parameters [1].

Both module types specify a configuration file with a list of IP addresses, and they also feature dynamic network discovery. This involves enumerating network adapters, connected IPs, and attempting connections to all IPs in the subnet through the broadcast address. While effective, this method is indiscriminate and generates considerable network noise for identifying other hosts [1].

Device communication takes place through TCP port 102, the default listening port for the targeted IEC-61850-compliant communication version. Actual communications utilize the Manufacturing Message Specification (MMS), with IEC-61850 providing the addressing standard within IEC-61850-1. The modules collect and enumerate control points from devices outlined in the configuration file, aiming to toggle designated control points to either OPEN or CLOSE states. This functionality aligns with the observed physical impact in the IEC-101 and -104 modules [1].

4.7 OPC DA payload

The Industroyer's OPC-DA module focuses on targeting the OLE for Process Control (OPC) Data Access (DA) standard, a specification facilitating real-time data transfer between devices. Unlike other modules, this standalone executable is invoked remotely without the need for support files. It leverages a command for execution, incorporating hardcoded default credentials for remote access but lacking the necessary hostname for the target device.
Analysis of the module's file reveals its utilization of source code from a publicly-available OPC client toolkit. Notably, it operates without a configuration file, indicating auto-discovery capability. The module allows both local and remote enumeration of OPC server instances, with local discovery being executed. Unlike other Indutroyer modules, it is designed to run on the host providing ICS-related functionality, enumerating local OPC server instances and interacting with specific items.
During enumeration, the module identifies local items, logs responding ones, and manipulates ctlOperOn, ctlSelOn, ctlOperOff, and ctlSelOff. This corresponds to specific actions like opening breakers or turning off selected path-

ways, aligning with the functionalities observed in other Industroyer modules [1].

4.8 Hybrid payload: OPC and 61850

ELECTRUM deployed a binary named "imapi.dll," incorporating functionalities of both the 61850 and OPC modules. This more complex sample, with a delayed execution time on 20 December 2016 at 06:30 UTC, was compiled before the initial outages, suggesting a pre-planned attack for a later time. The combination of the two protocols in this attack is designed to overcome environmental fail-safes, potentially impacting electric distribution by targeting breakers and switchgear [2].

4.9 Data wiper

The data wiper component, deployed as a concluding element in an attack, serves to obfuscate the attackers' actions and hinder recovery. Executable either through the Launcher or as a standalone tool, it employs various tactics to disrupt the system:

- Registry Modifications: It attempts to render the operating system unbootable by manipulating registry keys related to Windows services, setting the ImagePath registry value to an empty string.
- File Content Deletion: The component systematically deletes file contents on connected drives, excluding specific directories, to erase traces of its activity.
- Thorough Content Rewriting: It rewrites file content with meaningless data obtained from allocated memory, making two attempts to ensure comprehensive data destruction.
- Process Termination: The component attempts to terminate all processes (except its own) to induce system unresponsiveness and eventual crashing.
- Targeted File Types: The wiper specifically targets a range of file types, including Windows binaries, archives, backup files, Microsoft SQL server files, and various configuration files. It also erases files associated with industrial control systems, impacting both standard and specialized environments.

The data wiper is a destructive tool that aims to eliminate traces of an attack by manipulating the registry, deleting file contents, rewriting data, terminating processes, and targeting a diverse set of file types, impacting both general and ICS environments [1].

4.10 Port scanner tool

Among the tools employed by the attackers is a custom-built port scanner, uniquely crafted for mapping the network and identifying pertinent computers for their operations. Rather than utilizing existing software, the attackers developed their own port scanner, allowing them to define IP address and network port ranges for scanning [1].

4.11 DoS tool

The attackers possess a Denial-of-Service (DoS) tool targeting Siemens SIPROTEC devices. This tool capitalizes on the CVE-2015-5374 vulnerability to render the device unresponsive. Exploiting this vulnerability involves the tool's utilization of hardcoded IP addresses for the targeted devices. Upon execution, the tool dispatches specially crafted UDP packets to port 50,000 of the designated IP addresses, each packet containing only 18 bytes. The successful exploitation of this vulnerability results in the targeted device remaining unresponsive to commands until manually rebooted [1].

5 Defense Recommendations

In addressing the specific challenges posed by threats like Industroyer in the ICS environment, a tailored approach is crucial. Traditional antivirus defenses may fall short, emphasizing the need to focus on detecting authentication information, monitoring binary movement, and identifying system alterations. Increased visibility aligned with adversary behaviors, such as those exhibited by ELECTRUM, is essential for effective defense [3].

ICS defenders should transition from IT-centric to ICS-specific strategies, recognizing the unique nature of intrusions in this environment. This comprehensive approach, concentrating on essential adversary actions, offers a robust means of securing the ICS environment against various malicious activities [3].

Key recommendations include understanding and monitoring protocols, recognizing abnormal OPC usage, ensuring robust backups, and developing incident response plans. Leveraging YARA rules, IoCs, and behavioral analytics enhances threat detection. However, reliance on alternative protocols and passive defenses is discouraged, highlighting the critical role of human defenders against determined adversaries [3].

Glossary

C2 :A command and control server is a computer or software program that manages and directs the actions of other computers, devices, or software components within a network or system

COM :Component Object Model is a software framework developed by Microsoft that enables different software components to communicate and interact with each other on Windows-based systems.

DoS :Denial of Service is a type of cyber attack where the attacker floods a target system or network with excessive traffic or requests, causing it to become overwhelmed and unable to respond to legitimate users' requests.

GUID :Globally Unique Identifier is a unique identifier used in software development to uniquely identify objects or entities.

ICS :Industrial Control System it refers to a networked set of devices and systems used in industries such as manufacturing, energy, and utilities to monitor and control industrial processes.

IOA :Information Object Addresses are unique identifiers used in digital communication protocols to designate specific pieces of information or data within a system.

RTU :Remote Terminal Unit is a type of device used in industrial control systems to monitor and control various equipment and processes in remote locations. RTUs gather data from sensors and equipment in the field, then transmit this data to a central control system.

Tor :Tor is primarily designed to protect privacy and anonymity online, it can also be exploited by attackers for malicious purposes. Attackers might use Tor to hide their identity while carrying out various malicious activities.

6 References

[1] A. Cherepanov, WIN32/INDUSTROYER A new threat for industrial control systems. ESET, 2017.
[2] J. Slowik, Anatomy of an Attack: Detecting and Defecting CRASHOVERRIDE. Dragos inc, 2018.
[3] Dragos inc, CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Dragos inc, 2017.
[4] Kaspersky, ATT&CK for ICS: Industroyer. AO Kaspersky Lab, 2024. https://www.kaspersky.com/enterprise-security/mitre/industroyer