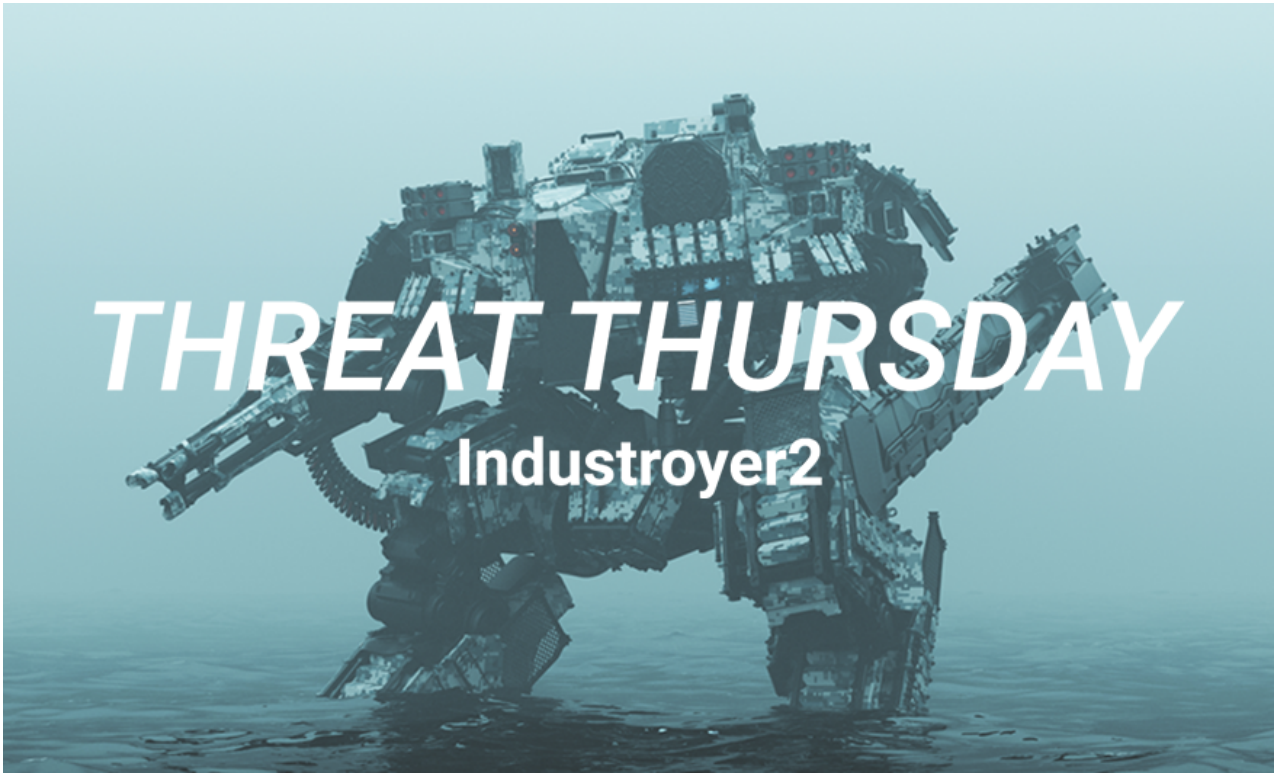
Threat Thursday: Malware Rebooted - How Industroyer2 Takes Aim at Ukraine Infrastructure

blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure



Since the outbreak of conflict in Eastern Ukraine in 2014, following Russia's annexation of Crimea, there have been several notable attempts to disrupt the electrical infrastructure of the country. While an attack with Industroyer2 was recently thwarted, analysis of this malware provides useful insight into threat actors' behaviors.

Industroyer2 was first reported by CERT-UA and confirmed by ESET on April 12, 2022, as the third major attempt at taking out part of Ukraine's electrical substations and controllers. This attack was repelled by CERT-UA in partnership with ESET.

This was just the latest in a string of attacks against Ukraine's electric grid. The first electrical disruption attempt occurred in December 2015, using an updated version of the BlackEnergy malware. This attack successfully caused power outages in several regions of Ukraine. In December 2016, the first version of Industroyer caused blackouts for several hours in the capital, Kyiv.

The 2015 and 2016 attacks were both attributed to the Sandworm group. It is likely Industroyer2 is yet another attempt by the Sandworm group to cause damage to the critical infrastructure of Ukraine in support of the ongoing Russian incursions. The U.S.

Department of Justice has previously released indictments accusing the Russian GRU of being behind BlackEnergy and Industroyer in an attempt to “undermine, retaliate against, or otherwise destabilize” Ukraine, among other geopolitical targets.

Operating System

Windows	MacOS	Linux	Android
Yes	No	Yes	No

Risk & Impact

Impact	High
Risk	Low

Technical Analysis

Overview

Sample:
D69665F56DDEF7AD4E71971F06432E59F1510A7194386E5F0E8926AEA7B88E00

Signature	00004550	
Machine	014C	Intel 386
Number of sections	0004	
Time/Date stamp (local)	623AF161	2022-03-23 03:07:29
Time/Date stamp (UTC)	623AF161	2022-03-23 10:07:29

Figure 1 – Compilation date

Industroyer2 was compiled on March 23, 2022, nearly a month after the initial invasion of Ukraine. This threat was deployed alongside several wipers, a worm, and a loader. CERT-UA reports that the wipers that came with the attack included CaddyWiper, SoloShred, and AwfulShred. CaddyWiper targets Windows® systems, while the other wipers target Linux® systems. The Linux worm OrcShred and the loader ArguePatch were also included.

To understand how Industroyer2 works, we first need to look into the IEC 60870-5-104 protocol used for communication on a TCP/IP network. This protocol is used in the Ukrainian electrical stations and substations that were targeted by this attack. By following the commands used by the malware, we can observe the execution flow of Industroyer2 and see what messages are sent to disrupt the targeted devices.

IEC-104

The IEC 60870-5-104 protocol, shortened as IEC-104, is a telecontrol equipment and systems standardization for TCP communication over port 2404. This protocol is used to interface with power control stations and substations.

An Application Protocol Data Unit (APDU) transmission frame contains the Application Service Data Unit (ASDU), which is a message structure carrying application data sent between stations. The ASDU transmits an Information Object Address (IOA), which is used to interact with the switches and breakers in a station. During normal everyday function, a controller can send an APDU frame with an ASDU that contains specific IOA commands to change the state of the stations and substations.

Status checking on the controller stations is carried out by sending a Test Frame (**TESTFR**) command – **TESTFR act** APDU, to activate – which is verified with a return – **TESTFR con** APDU, to confirm the system is online. The commands Start Data Transfer (**STARTDT**) and Stop Data Transfer (**STOPDT**) control data transfer from the control station. These actions are sent in an APDU.

Behavior

Once Industroyer2 is launched, a command prompt window opens and displays the commands that are being sent and received, as seen in Figure 2. In this instance, we see that port 2404 is being targeted. Port 2404 is used by IEC-104 to send TCP messages. This output also corresponds to the IOA commands found inside the file, which are shown in Figure 3.

```
00:48:09:0903> T281 00006800
00:48:09:0946> RNM 0015
00:48:09:0966> 10.          : 2404: 3
00:48:09:0967> T65 00006800
00:48:09:0977> 10.          M68B0 SGCNT 44
00:48:10:0010> RNM 0015
00:48:10:0025> T113 00006800
00:48:10:0026> 192.          2404: 2
00:48:10:0042> 192.          M68B0 SGCNT 8
00:48:10:0070> RNM 0015
00:48:10:0087> 192.          2404: 1
00:48:10:0102> 192.          M68B0 SGCNT 16
```

Figure 2 – Console output while executing

```
192.          2404 2 0 1 1 PService_PPD.exe 1 "D:\          " 0 1 0 0 1 0 0 8
1104 0 0 0 1 1 1105 0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0 1 5 1101 0 0 0 1 6
1102 0 0 0 1 7 1103 0 0 0 1 8
```

Figure 3 – Configuration found inside the file

A **TESTFR act** APDU is sent to establish a connection to a station, shown in Figure 4, along with a **STARTDT** command. Upon successful connection, a **TESTFR con** APDU is sent back from the station. With the confirmation received from the station, a **STARTDT** APDU is sent to open data transfer. As with **TESTFR**, **STARTDT** will need to send an **act** to activate, and to receive a **con** from the station to confirm, before data transfer can begin.

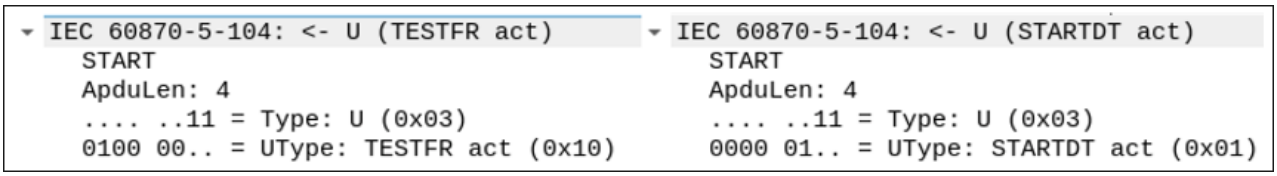


*Figure 4 – **TESTFR act** and **STARTDT act** commands*

Next, the ASDU frames will communicate commands to the station, as shown in Figure 5. An ASDU interrogation command determines the status of the station. The hardcoded messages in Figure 3 will get sent and modify the station's IOA.

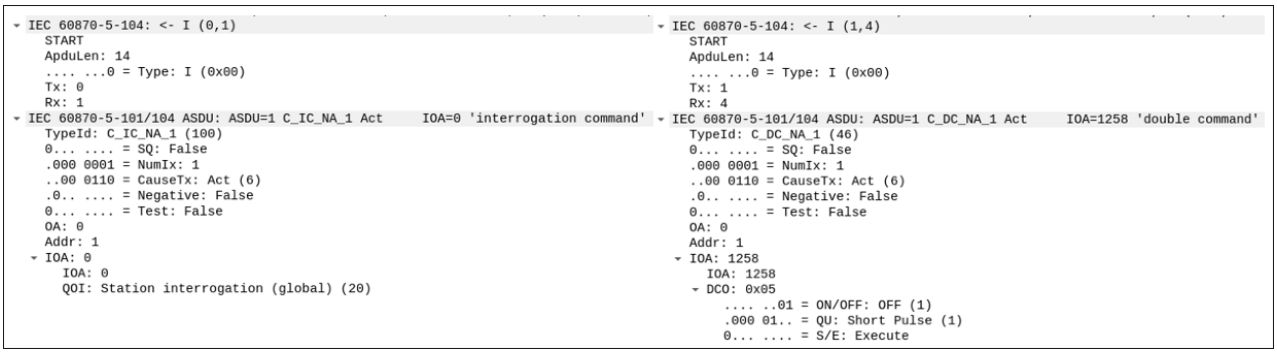


Figure 5 – ASDU IOA commands

Not much else can be discerned from these IOA modifications without knowledge of the specific systems that were being targeted. This points to the possibility that the malware authors have some level of access or insider knowledge of the systems they were attacking.

Industroyer vs. Industroyer2

While Industroyer2 is an updated version of the original Industroyer, it comes with a slightly narrower scope of action. The original version of the threat had four distinct modules targeting IEC 60870-5-101 (IEC-101), IEC 60870-5-104 (IEC-104), IEC-61850, and OLE for Process Control Data Access (OPC DA).

IEC-101 is a protocol for controlling and monitoring electrical stations, while IEC-104 utilizes IEC-101 and sends communications over a TCP/IP network. IEC-61850 is a communication standard for automated substation devices, and OPC DA is a client-server standardization for real-time data acquisition devices.

Industroyer2 focuses primarily on disrupting services by targeting the IEC-104 controllers. It's not clear why the focus was narrowed down to this one service, but judging from the compilation date of March 23, 2022, the malware was likely rushed through development. Additionally, Industroyer has a separate config file with the IOAs, while Industroyer2 stores that information inside its executable.

Conclusion

Industroyer2 is the latest attempt by state-level threat actors to cause what they hope will be severe damage to the critical infrastructure of the targeted region. This tactic has proven effective in the past as a method of spooking the populace, even when the attack itself was not successful.

Few details surrounding this specific attack are currently available to us, but what we do know is that the deployment of Industroyer2 represents an increasing escalation of cyberattacks on Ukraine's crucial resources. Attackers are now escalating their intrusion attempts far beyond the usual "smash-and-grab" tactics of infostealing, to focus on just the "smash" part. This method of operation not only causes population distress and widespread disruptions, but also has the potential to take out critical infrastructure in a way that causes immediate damage to the basic services that keep countries functioning.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
rule Industroyer2{


meta:
description = "Detects Industroyer2"
author = "BlackBerry Threat Research Team"
date = "2022-05-03"
license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"


strings:
$s1 = "02d:%lS" wide
$s2 = "M%X - %02d:%02d:%02d" wide
$s3 = "02hu:%02hu:%02hu:%04hu" wide
$s4 = "T%d %08x" wide
$s5 = "T%d %h" wide
$s6 = "%s M%X %d (%s)" wide
$s7 = "%s M%X SGCNT %d" wide
$s8 = "ASDU:%u | OA:%u | IOA:%u" wide
$s9 = "Cause: %s (x%X) | Telegram type: %s (x%X)" wide

$c1 = "TESTFR act" wide
$c2 = "TESTFR con" wide
$c3 = "STARTDT act" wide
$c4 = "STARTDT con"


condition:
uint16(0) == 0x5a4d and filesize < 50KB and all of them


}
```

Indicators of Compromise (IoCs)

```
D69665F56DDEF7AD4E71971F06432E59F1510A7194386E5F0E8926AEA7B88E00
43D07F28B7B699F43ABD4F695596C15A90D772BFBD6029C8EE7BC5859C2B0861
BCDF0BD8142A4828C61E775686C9892D89893ED0F5093BDC70BDE3E48D04AB99
87CA2B130A8EC91D0C9C0366B419A0FCE3CB6A935523D900918E634564B88028
CDA9310715B7A12F47B7C134260D5FF9200C147FC1D05F030E507E57E3582327
1724A0A3C9C73F4D8891F988B5035EFFCE8D897ED42336A92E2C9BC7D9EE7F5A
FC0E6F2EFFBFA287217B8930AB55B7A77BB86DBD923C0E8150551627138C9CAA
7062403BCCACC7C0B84D27987B204777F6078319C3F4CAA361581825C1A94E87
3851A064AABAB557CE162E01A77681B3954B006117EDD0563EDD2B3E5A082ACE
EA16CB89129AB062843C84F6C6661750F18592B051549B265AAF834E100CD6FC
```

References

https://cert.gov.ua/article/39518

https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

https://pylos.co/2022/04/23/industroyer2-in-perspective/

https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks

https://attack.mitre.org/groups/G0034/

https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

Related Reading

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back