REVISION: A
PUBLICATION DATE: 2022-05-02
DOC. IDENTIFIER: 8DAA003558
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY NOTIFICATION

Industroyer.V2

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of recent investigation reports from various cybersecurity researchers on the new version of Industroyer, called Industroyer 2 [1] or Industroyer.V2 [2] published in the timeframe between April 12, 2022 and April 25, 2022. Industroyer.V2 is designed to deploy on networks using the IEC 60870-5-104 (IEC 104) protocol to communicate with other industrial control equipment [1]. IEC 104 is commonly used in power grids system monitoring and control. Any kind of industrial control systems product that is a component of a system using the common IEC 104 protocol could be affected by an Industroyer.V2 attack.

As elaborated in multiple references [1, 2, and 3] below, Industroyer.V2 contains a detailed configuration hard-coded in its body in order to drive the malware actions. This also implies that the Industroyer.V2 malware needs to be recompiled for different environment. An attacker who plans to use Industroyer.V2 needs to compromise security layers to obtain access to the control systems network, identify the control targets prior to deployment. Upon a successful deployment, the Industroyer.V2 malware may alter processes in a specific industrial control system. Consequently, this may cause a disruption to a system that is controlled by the attacker

It is important to highlight that the original version of Industroyer/CrashOverride is the first malware ever seen to have been specifically designed to attack power grids.

This notification applies to the following Hitachi Energy products that support the industry standard IEC 104 protocol, for example: RTU500 Series, MicroSCADA Pro/X SYS600, Gateway Station, FACTS Control Platform, CoreTec 4.

Customers that have an industrial control system that uses the IEC 104 protocol, should refer to the “Preventing Malware Recommendation” and “General Cybersecurity Risk Mitigations Measures” sections.

Preventing Malware Recommendation

It is not yet known exactly how Industroyer.V2 is initially introduced to a target system, however, malware (short for malicious software) like Industroyer.V2 is typically installed on a computer when a user clicks on an online link, downloads a malicious attachment, or opens a rogue software program. Once installed, attackers can use the malware to perform illicit activities in the infected host or to attack other systems.

Malware protection management

Ensure that antivirus system is installed, working properly and updated to the latest support fingerprint database. Use two different antivirus-solutions where possible (in different segments). Portable computers and removable storage media should be restricted but if required, they must be carefully scanned for viruses before they are connected to a control system.

General Cybersecurity Risk Mitigation Measures

Hitachi Energy highly recommends customers to implement the following best practices/countermeasures as part of their cybersecurity management program for industrial control systems and generally systems using Hitachi Energy products. It is important to ensure that industrial control systems should not be used for Internet surfing, instant messaging, or receiving E-mails. Additionally, please refer as well to the Solution Section in US CISA CERT alert (TA17-163A) CrashOverride Malware [4].

Network security

When possible, enforce the necessary measures to isolate the critical systems from internet and from any untrusted network. Remote access should be enabled only on request basis. Limit network access and use security measures such as firewalls to segregate networks (also inside organization internal network).

- make sure that firewall configurations are properly configured and only required traffic is allowed
- always check firewall/access logs for any suspicious events and behavior
- industrial control system network should not have direct connections to the Internet

User access management

Enforcing a least privilege principle, good practice in account management and enable strong password policy (as it is typically the weakest link). Enable only access to the required individuals according to the role. Industrial control system should be physically protected from any direct access by unauthorized personnel.

System hardening

The following lists some of commons system hardening practices:

- where possible, use a software inventory list to gain visibility on the software and software components in your environment
- if software is not needed it should be removed
- disable/remove all OS services, components and 3rd party software which is not needed
- ensure to have a baseline that can be referred to for audit
- ensure only required ports are exposed/opened
- apply whitelisting whenever possible to make sure that only known/identified nodes can communicate with other nodes
- whenever possible, implement secure communication when using IEC 60870-5-104 according to IEC TS 62351-3 (TLS) and IEC TS 62351-5 (secure authentication)

Secure the industrial control systems configuration files

Industrial control system configuration files are confidential information that should be stored securely. The information should not be shared widely, as this may become a vector that can be used by malware to recognize the setup of the industrial control system.

References

1. Industroyer2: Industroyer reloaded, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
2. INDUSTROYER.V2: Old Malware Learns New Tricks, https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks
3. Industroyer2: Nozomi Networks Labs Analyzes the IEC 104 Payload, https://www.nozomi-networks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload/
4. Alert (TA17-163A) - CrashOverride Malware – https://www.cisa.gov/uscert/ncas/alerts/TA17-163A

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2022-05-02	A	Initial public release.