'GhostSec' Leverages ICS-Oriented Exploitation Tools Against Internet-Exposed Assets in Russia

Fusion (FS) | Cyber Physical (CP)

June 20, 2022 03:07:00 PM, 22-00014563, Version: 2

Executive Summary

- In June 2022, the threat actor "GhostSec" targeted a few hundred Russia-based IP addresses with exposed industrial control system (ICS) ports. GhostSec is an Anonymous-affiliated hacktivist collective that has recently been targeting various types of information technology (IT) and operational technology (OT) systems in Russia in response to the invasion of Ukraine.
- The threat actor leveraged three ICS-oriented exploitation tools in the operation: an IEC-104 Metasploit module, an EtherNet/IP CIP Metasploit module, and an unknown Modbus-based tool dubbed "Killbus." IEC-104 is used in electric energy systems mainly in Europe and the Middle East while EtherNet/IP CIP and Modbus are more general-purpose ICS network protocols. The actor also targeted serial-to-ethernet converters designed for legacy ICS assets.
- This activity follows a trend of hacktivists targeting internet-accessible ICS assets. The threat actor's use of ICS-oriented exploitation modules also demonstrates the adoption of these long publicly available attack tools, which Mandiant rarely observes deployed in the wild.
- We assess the threat posed by low-sophistication actors will grow as they begin to leverage publicly available ICS attack tools and learn from high-profile ICS security incidents. Defenders can mitigate this risk by removing ICS assets from internet-accessible networks and securing remote access methods with configurations that use multi-factor authentication (MFA).

Threat Detail

New Version Details

Version 2, June 20, 2022: Added analysis of additional posts by GhostSec in which the actor executed additional Modbus-oriented commands and targeted serial-to-ethernet converters in Russia.

Threat Detail

On June 3 and June 9, 2022, the threat actor "GhostSec" claimed on various social media platforms to target a few hundred industrial control systems (ICS) assets in Russia. GhostSec is an Anonymous-affiliated hacktivist collective that has recently been targeting various types of IT and OT systems in Russia in response to the invasion of Ukraine (22-00004492).

FIIP ENVIRONMENTS ORGANIZATION
german.simkin@mandiant.com

- The threat actor's social media posts were accompanied by several screenshots showing the use of ICS-oriented exploitation modules against public IP addresses geolocated in Russia. Mandiant selected a sample of these IP addresses and verified they had open ports associated with the ICS protocols leveraged by these exploitation tools.
- One of the screenshots shows the public Metasploit module IEC104 Client Utility (Figure 1). IEC-104 (aka IEC 60870-5-104) is a protocol used for Transmission Control Protocol (TCP) communications within electric energy systems (19-00002537). The standard is primarily used in systems in Europe and the Middle East.
    - The screenshot shows the configuration of the IEC-104 command that the actor is sending to the targeted devices.
        - rhost – the targeted Russia-based IP addresses.
        - command address – 5, indicating the targeted devices' Information Object Addresses (IOAs), which are used to interact with power line switches or circuit breakers in a remote terminal unit (RTU) or relay configuration. IOAs often differ between manufacturers and devices, so the selection of "5" could be considered arbitrary.
        - command type – 46, indicating a double command (2 bits).
        - command value – 5, indicating the action the targeted device should take against the actuator associated with the IOA. "5" in a double command means turn off (1) the device using a short pulse duration (4).
    - We identified the same configuration in an overview of the IEC104 Client Utility module, which could indicate that the threat actor simply copied this configuration and has a limited understanding of the protocol or attack tool.

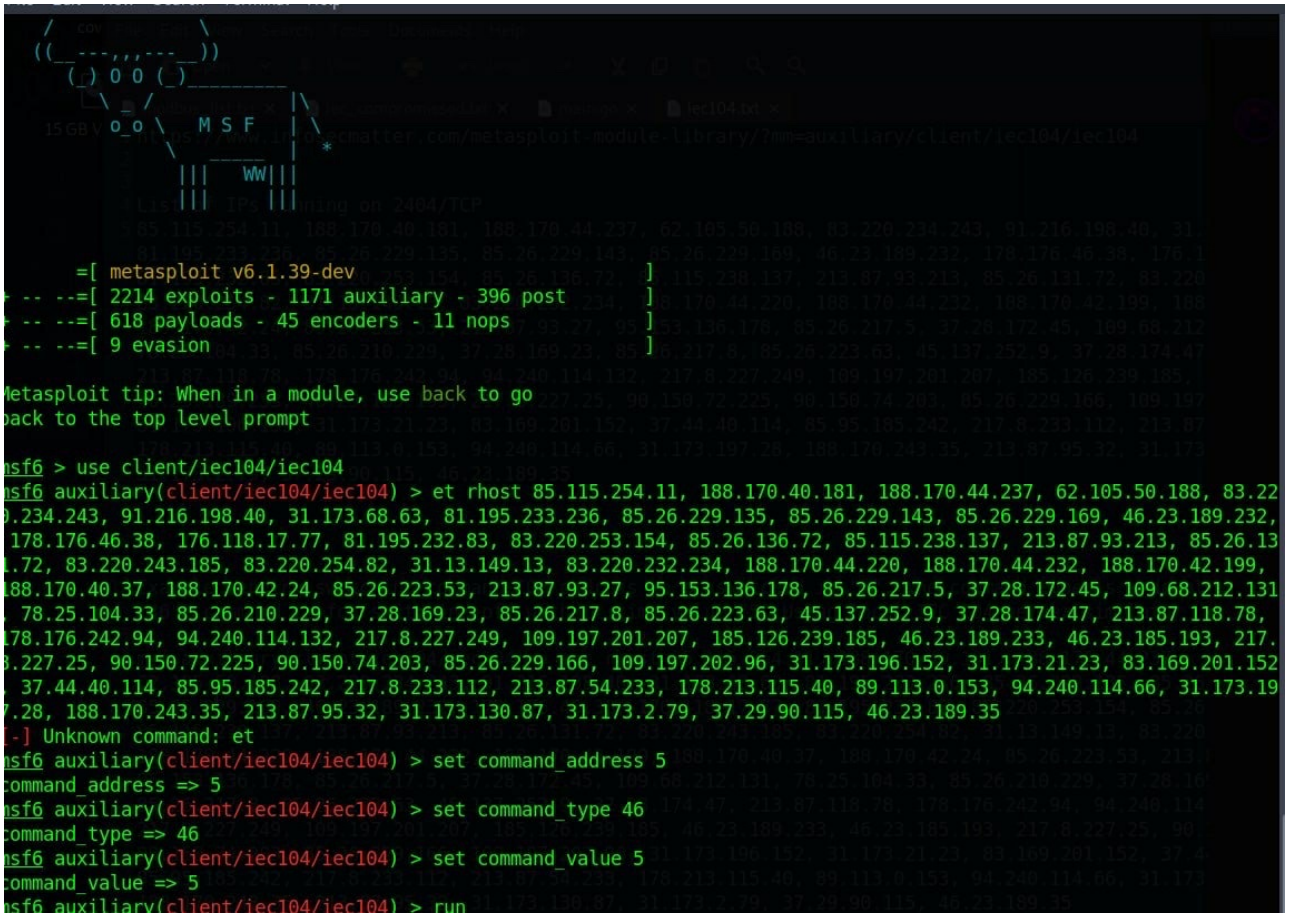

Figure 1: IEC104 Client Utility configuration used by GhostSec

- Another screenshot shows the public Metasploit module Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands (Figure 2). EtherNet/Industrial Protocol (Ethernet/IP) is an ICS protocol that adapts the Common Industrial Protocol (CIP) for use over the Ethernet standard (18-00014652). The screenshot shows the threat actor running the module's STOPCPU command against a single Russia-based IP address.

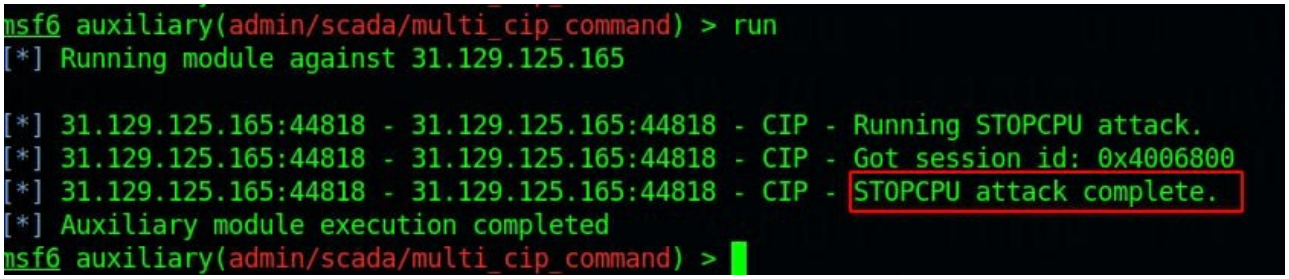

Figure 2: Metasploit EtherNet/IP CIP command used by GhostSec

- Another screenshot shows the actor using a previously unknown tool dubbed "Killbus," which appears to be a Modbus-oriented tool (Figure 3). Modbus is a general-purpose ICS network protocol that lacks authentication and encryption security features (18-00012164).
  - While we have not identified this tool in any ICS exploitation module repositories or in discussions in underground forums, we suggest it probably has similar capabilities to other Modbus-oriented attack modules given the relatively high level of gray hat security research into this protocol.
  - The threat actor is using a command "killAllCoils," which is possibly attempting to overwrite the status of the coils (typically outputs or actuators) to the off position. The screenshot is showing that there was an error against this particular target, but it is plausible that a Modbus-oriented attack would succeed against other targets given the lack of security features in the protocol.

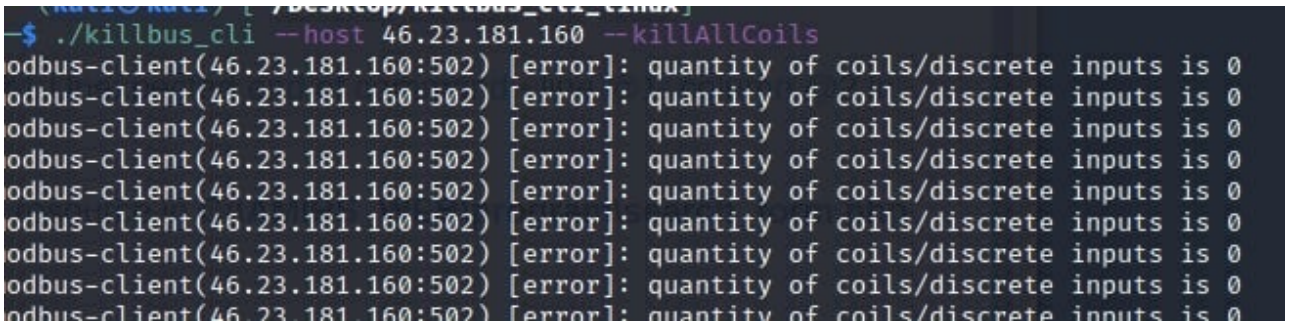

Figure 3: Output of Killbus attack tool

  - In a later June 19, 2022, post, the actor shared the output of an unknown command that we believe targeted Modbus-enabled devices (Figure 4). The command appears to flip the bits in Modbus registers, which could invert the status of physical actuators from "on" to "off" and vice versa, for example.

Figure 4: Output of unknown command likely inverting the bits of Modbus registers

- The actor also posted screenshots of what appears to be the remote management interface for a Schneider Electric Easergy T300 / HU250, which are used in electric energy distribution operations (Figure 5). The actor defaced the GUI by editing some of the fields, such as the description and the photo.

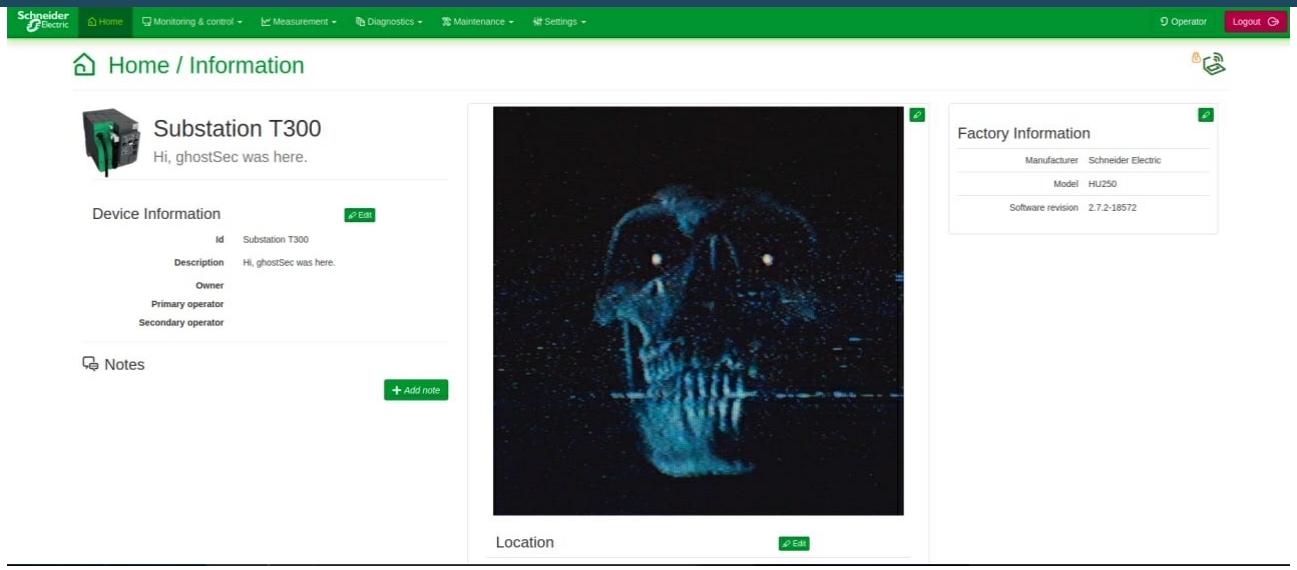

Figure 5: Defacement of a Schneider Electric Easergy T300 / HU250 management interface

GhostSec Also Purportedly Targeted Serial-to-Ethernet Converters

On June 19, 2022, GhostSec created additional social media posts in which the actor claimed to target Moxa NPort devices in Russia in addition to the IEC-104- and Modbus-enabled devices.

- Moxa NPort devices are serial-to-ethernet converters, which enable IP-based network connectivity for legacy ICS devices.
- GhostSec shared a screenshot showing Telnet access to an IP address geolocated in Russia hosting a Moxa NPort 5110 device (Figure 6).
  - It is unclear how the actor obtained valid credentials to access the device, but the screenshot shows a masked six-character password, which would be trivial to brute force. We also identified default credentials for this device in a corresponding user guide, but the default password appears to be four characters.
  - While we have no information on the threat actor's follow-on activity, the access could allow the attacker to change the configuration of the system, disable communication to the ICS assets, or potentially access the ICS devices.

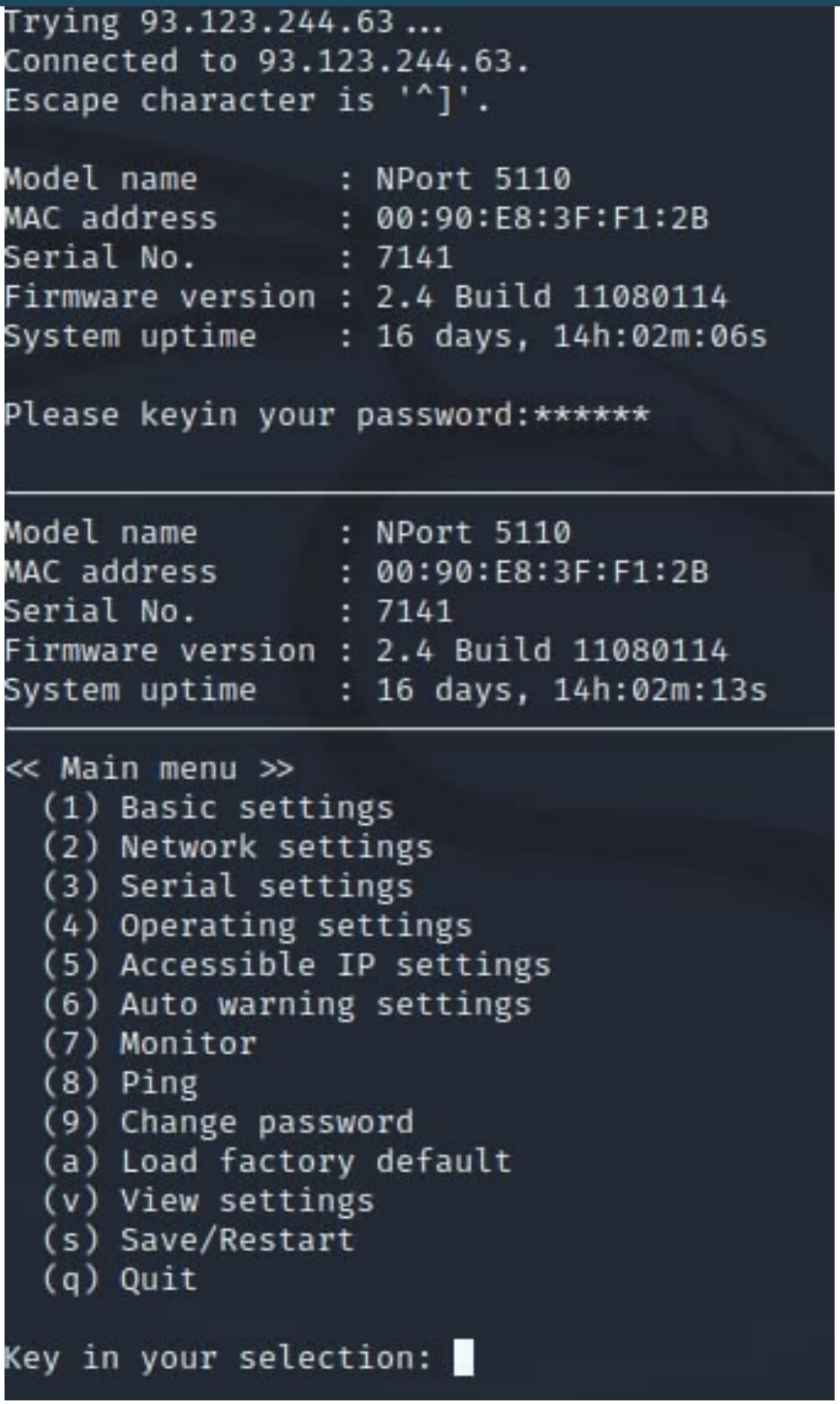

Figure 6: Moxa NPort 5110 targeted by GhostSec

- Serial-to-ethernet converters were previously targeted as a disruptive component to the 2015 Ukraine blackout (BlackEnergy3) attack (21-00026094). The make of the serial-to-ethernet devices in that incident was purportedly Moxa, so it is possible the threat actor was attempting to emulate that portion of the attack.

Publicly Available ICS-Oriented Cyberattack Tools Increase the Capabilities of Low-Sophistication Threat Actors

This activity follows a trend of hacktivists targeting internet-accessible ICS assets (21-

00011127). The threat actor's use of ICS-oriented cyberattack tools also demonstrates the adoption of these long publicly available attack modules, which we rarely observe deployed in the wild.

- Since 2010, we have tracked exploit modules for the Core Impact, Immunity Canvas, Metasploit, and Exploits and Security Tools (EaST) frameworks (20-00004127). We are also aware of ICS-specific exploit frameworks, such as Autosploit, Industrial Exploitation Framework (ICSSPLOIT), and Industrial Security Exploitation Framework. These frameworks collectively hold about 1000 ICS-oriented exploit modules.
- Low-skilled threat actors have recently demonstrated an increased awareness of publicly available ICS-related resources, such as ICS exploits and penetration tactics (20-00015235). Some actors have even developed and shared custom-made ICS-specific tutorials. The result is a growing community of threat actors who possess a basic level of ICS proficiency.

Outlook and Implications

We assess the threat posed by low-sophistication actors will grow as they begin to leverage publicly available ICS attack tools and learn from high-profile ICS security incidents. For instance, the recent INDUSTROYER.V2 attack and subsequent public analyses demonstrated the nature of IEC-104 communications, which could have inspired this threat actor to learn about the protocol and emulate the INDUSTROYER.V2 attack (22-00010611). Furthermore, we suggest ICS exploitation tools are likely to grow in number, as evidenced by the potentially novel Killbus tool leveraged in this operation.

In most instances, ICS threat activity by low-sophistication threat actors has been limited to internet-accessible assets. Defenders can mitigate this risk by removing ICS assets from internet-accessible networks and implementing best practice for remote access to ICS environments, such as by using multi-factor authentication (MFA) and separate IT/OT authentication domains (20-00006604).

Please rate this product by taking a short four question survey

First Version Publish Date

June 16, 2022 09:48:00 AM

Threat Intelligence Tags

Affected Industry

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Agriculture
- Energy & Utilities
- Manufacturing
- Oil & Gas
- Transportation

- Construction & Engineering

Target Geography

- Russia

Intended Effect

- Disruption
- Interference with ICS

Affected System

- Users/Application and Software
- Control Systems and Applications
- Industrial Network Protocols

Motivation

- Ideological/Religious
- Opportunistic

Tactics, Techniques And Procedures(TTPs)

- Defacement

Actor

- GhostSec

Version Information

Version:1.0, June 16, 2022 09:48:00 AM
'GhostSec' Leverages ICS-Oriented Exploitation Tools Against Internet-Exposed Assets in Russia

Version:2.0, June 20, 2022 03:07:00 PM
'GhostSec' Leverages ICS-Oriented Exploitation Tools Against Internet-Exposed Assets in Russia

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/22-00014563