OT Threat Activity Claimed in Underground Forum and Social Media Posts: September 2022

Critical Infrastructure (CI) | Fusion (FS)

October 14, 2022 06:11:23 PM, 22-00023702, Version: 1

Executive Summary

- Mandiant monitors underground forum and social media posts to identify threat activity against operational technology (OT). In September 2022, we observed the threat actors "Joint Cyber Center," "Team OneFist," and "GhostSec" claim to target OT assets.
- Based on our analysis of the claims and observable tactics, techniques, and procedures (TTPs), most of the activity consisted of gaining initial access to the OT assets by accessing internet-accessible devices or exploiting public-facing applications. The actors leveraged the assets' command-line interfaces and graphical user interfaces to execute disruptive actions, such as destroying data, shutting down devices, and overwriting Modbus register values.
- The targets of the activity include web interfaces for programmable logic controllers (PLCs), serial-to-ethernet converters, uninterruptible power supply units (UPS), and satellite communication devices collectively located in Russia, Israel, and Iran.
- Asset owners can mitigate this activity by applying cyber security controls on internet-accessible OT assets, including complex passwords, multi-factor authentication requirements, and up-to-date security patches.

Threat Detail

Mandiant monitors underground public forum and social media posts to identify threat activity against operational technology (OT). In September 2022, we observed at least eight instances of threat actors claiming to target OT assets (Table 1). The majority of the incidents were conducted by the "Joint Cyber Center," a Ukrainian- and English-speaking hacktivist actor who we have observed targeting Russian critical infrastructure since June 2022.

Date	Actor	Target	TTPs	Report
Sept. 27, 2022	Team OneFist	Actor claimed to compromise Russian Satis satellite systems, further claiming to brick modems at ground stations.	• Command-Line Interface (T0807) • Graphical User Interface (T0823)	22-00022733
Sept. 26, 2022	Joint Cyber Center	Actor claimed to leverage a vulnerability to access APC (Schneider Electric) UPS devices in Russia.	• Internet Accessible Device (T0883)	22-00022520

			• Exploit Public-Facing Application (T0819) • Graphical User Interface (T0823) • Device Restart/Shutdown (T0816)	
Sept. 26, 2022	GhostSec	Actor claimed to target various OT assets in Iran, inverting Modbus register values, claiming to negatively affect electricity at Shatel, an Iranian mobile network company.	• Internet Accessible Device (T0883) • Commonly Used Port (T0885) • Standard Application Layer Protocol (T0869) • Unauthorized Command Message (T0885) • Manipulation of Control (T0831)	N/A
Sept. 17, 2022	Joint Cyber Center	Actor claimed to exploit a vulnerability in order to gain partial control of a Schneider Electric Uninterruptible Power Supply (UPS) in Russia multiple times.	• Internet Accessible Device (T0883) • Exploit Public-Facing Application (T0819) • Graphical User Interface (T0823) • Device Restart/Shutdown (T0816)	22-00022001
Sept. 7, 2022	Joint Cyber Center	The actor claimed to target OT devices specific to power control in Russia and shared screenshots of web interfaces for PL Controller's SNR-ERD-4, Moxa NPort 5130 serial-to-ethernet converters, and a "NAGRUSKA" metering system.	• Internet Accessible Device (T0883)	22-00021325
Sept. 3, 2022	Joint Cyber Center	The actor claimed to target an internet-accessible switch and accessed a WAGO Web-Based Management system in Russia, which	• Internet Accessible Device (T0883) • Graphical User Interface (T0823) • Indicator Removal on Host (T0872)	22-00021324

		is used to configure WAGO controllers.		
Sept. 3, 2022	Joint Cyber Center	Actor claimed to leverage a vulnerability to target two iRZ telecommunication routers in Russia.	• Internet Accessible Device (T0883) • Exploit Public-Facing Application (T0819) • Command-Line Interface (T0807) • Data Destruction (T0809) • CVE-2022-27226	22-00021324
Aug. 4, 2022 (reported Sept. 4, 2022)	GhostSec	Actor claimed to compromise several Berghof controllers in Israel.	• Internet Accessible Device (T0883) • Graphical User Interface (T0823) • Change Operating Mode (T0858)	22-00021079

Table 1: Threat actors claiming to targeting OT assets in September 2022

Analysis

Based on our analysis of the claims and observable tactics, techniques, and procedures (TTPs), most of the activity consisted of gaining initial access to the OT assets by accessing internet-accessible devices or exploiting public-facing applications. The actors leveraged the assets' command-line interfaces and graphical user interfaces to execute disruptive actions, such as destroying data, shutting down devices, and overwriting Modbus register values.

- Many of the targeted devices, such as WAGO's Web-Based Management system, have instances that can be easily identified online.
- The actors did not specify the vulnerabilities they allegedly exploited; however, we identified examples of recent vulnerabilities in the targeted assets that adversaries could leverage to obtain the actor's claimed outcomes if successfully exploited.
    - IRZ Mobile Routers exhibit a cross-site request forgery (CSRF) vulnerability that could allow unauthorized parties to execute arbitrary code through the creation of a crontab entry. We have previously observed this vulnerability being exploited by these threat actors (22-00015784).
    - Schneider Electric UPS systems are associated with recent vulnerabilities that could be leveraged to allow arbitrary code execution or firmware uploads from an unauthorized party.
- In one instance, the threat actor appeared to be leveraging an OT-oriented attack tool to impact Modbus-enabled devices.

Outlook

Throughout September 2022, we continued to observe hacktivist threat actors target internet-accessible OT assets for ideological purposes. We also continued to observe threat actors leverage OT-oriented attack tools and vulnerabilities when targeting these devices (22-00022003). We suspect that much of these low-

sophistication OT cyber incidents will continue to be geopolitically motivated in the short term as a majority of the activity appears fueled by the current Russia-Ukraine conflict. Asset owners can mitigate this activity by applying cyber security controls on internet-accessible OT assets, including complex passwords, multi-factor authentication requirements, and up-to-date security patches.

Please rate this product by taking a short four question survey

First Version Publish Date

October 14, 2022 06:11:23 PM

Threat Intelligence Tags

Actors

- GhostSec
  Aliases
  - GhostSec
- Joint Cyber Center
  Aliases
  - Joint Cyber Center
- TeamOneFist
  Aliases
  - TeamOneFist

Affected Industries

- Energy & Utilities
- Governments
- Manufacturing
- Oil & Gas
- Telecommunications

Affected Systems

- Industrial Network Protocols
- Regulatory and Supervisory Control
- Control Systems and Applications
- Communication Infrastructure

Intended Effects

- Interference with ICS
- Disruption

Motivations

- Anti-Corruption/Anti-Establishment/Information Freedom

Target Geographies

- Iran
- Israel
- Russia

Version Information

Version:1, October 14, 2022 06:11:23 PM

Common Vulnerabilities and Exposures

CVE ID:	CVE-2022-27226(CVE Description)Mandiant Vulnerability Analysis

MANDIANT ADVANTAGE

german[.]simkin@mandiant.com