Ind.Cyber.Sec Letters

Cyber Threat Intelligence

CyberAv3ngers

Profiling Operational Technology Threat Actors Using StealthMole's Platform

Prof. Dr. Luiz F. Freitas-Gutierres
linkedin.com/in/lffreitas-gutierres
github.com/substationworm
luiz.gutierres@ufsm.br

Published:
August 11, 2025

Sumário

Prof. Dr. Luiz F. Freitas-Gutierres
linkedin.com/in/lffreitas-gutierres
github.com/substationworm
luiz.gutierres@ufsm.br

Published:
August 11, 2025

1 Abstract

This document highlights the Cyber Av3ngers' persistent targeting of operational technology (OT)-industrial control system (ICS) environments, their association with the online persona Mr. Soul, and the use of specialized malware such as IOCONTROL. Evidence from Telegram channels, Dark Web sources, and social media—collected through the use of the `StealthMole`'s platform—indicates both genuine and fabricated materials, underscoring the group's capabilities and propaganda efforts. The findings reaffirm the need for continued vigilance, the development and application of cyber threat intelligence for OT-ICS, and adherence to established cybersecurity recommendations.

2 Overview of the Threat Group 🔗

Since at least 2023, **Cyber Av3ngers** (G1027 [MITRE ATT&CK, 2024, March]) has been recognized as a threat group that targets supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLC), and industrial control systems (ICS). Its operations have affected water and wastewater systems (WWS), critical energy infrastructure, and the broader manufacturing sector (Dragos, 2023, July). Cyber Av3ngers is known to focus on organizations affiliated with Israel, the United States, and Ireland, with a particular emphasis on disrupting Internet-connected devices manufactured by Israeli companies. There is speculation linking the group to Soldiers of Solomon (MITRE ATT&CK, 2024, March), an entity reportedly associated with the Islamic Revolutionary Guard Corps (IRGC). The group is also referenced by alternative name variants, including **CyberAv3ngers**, **CyberAveng3rs**, **Cyber Aveng3rs** and **Cyber Avengers**. Figure 1 illustrates the logo used by Cyber Av3ngers on social media platforms and in the dissemination of their cyber operations.

Figure 1: Logo of the Cyber Av3ngers threat group. Source: Official profile on X (formerly Twitter).

This advanced persistent threat (APT) group frequently leverages default credentials and publicly known PLC-related common vulnerabilities and exposures (CVE)—well documented within the cybersecurity community—alongside free and open-source software (FOSS) tools for reconnaissance and exploitation of operational technology (OT) and ICS. However, certain alleged compromises of critical infrastructure in Israel, initially attributed to the group, have since been debunked (Kaspersky, 2023, October).

According to a report by OpenAI, **Cyber Av3ngers has used artificial intelligence (AI) models to conduct research on PLC** (Nimmo and Flossman, 2024). The report highlights observed activities such as reconnaissance efforts, inquiries into usernames and default passwords for various PLC, attempts to obfuscate malicious code, and questions regarding the use of well-known penetration testing tools. The

threat group also requested assistance in developing and refining scripts written in Bash and Python, as well as sought general information about companies and known vulnerabilities. OpenAI documents these activities in detail, mapping them to the **large language model (LLM)-themed tactics, techniques, and procedures (TTP) from the MITRE ATT&CK framework** (Microsoft Threat Intelligence, 2024, February; Nimmo and Flossman, 2024), as summarized in Table 1.

Cyber Av3ngers' activities can also be broadly categorized using the MITRE ATT&CK for enterprise

Table 1: Activities Attributed to Cyber Av3ngers and Their Mapping to LLM-Themed TTP From the MITRE ATT&CK Framework, as Reported by OpenAI.

Activity	LLM-Themed TTP
Request for a list of routers commonly used in Jordan	LLM-Informed reconnaissance
Request for a list of industrial protocols and ports potentially connected to the Internet	LLM-Informed reconnaissance
Inquiry about the default password for a Tridium device	LLM-Informed reconnaissance
Request for username and default password for a Hirschmann router	LLM-Informed reconnaissance
Request for information on vulnerabilities in CrushFTP, Cisco IMC, and Asterisk	LLM-Informed reconnaissance
Request for a list of electric sector companies and PLC commonly installed in Jordan	LLM-Informed reconnaissance
Question about why a Bash script returns an error	LLM-Enhanced scripting techniques
Request for the creation of a Modbus TCP/IP client	LLM-Enhanced scripting techniques
Request for a network scan to identify vulnerabilities	LLM-Assisted vulnerability research
Request for a scan of ZIP files to identify vulnerabilities	LLM-Assisted vulnerability research
Request for source code example in C for process hollowing	LLM-Assisted vulnerability research
Inquiry about how to obfuscate VBA scripts in Microsoft Excel	LLM-Enhanced anomaly detection evasion
Request for assistance in obfuscating malicious code	LLM-Enhanced anomaly detection evasion
Question on how to copy a SAM file	LLM-Assisted post-compromise activity
Inquiry about an alternative to mimikatz	LLM-Assisted post-compromise activity
Question on how to use pwdump to export a password	LLM-Assisted post-compromise activity
Question on how to access user passwords on macOS	LLM-Assisted post-compromise activity

IP: Internet protocol; VBA: Visual basic for applications; SAM: Security account manager.

tactics and techniques, as summarized in Table 2. The analyses presented in this table are primarily derived from technical reports, media coverage, and institutional press releases; as such, they may lack comprehensive technical detail and should be interpreted with appropriate caution regarding their accuracy.

Table 2: Cyber Av3ngers Ativities Mapped to MITRE ATT&CK Enterprise TTP.

Tactics	Techniques	Procedures
Reconnaissance	Active scanning	Conducting active scans to identify OT devices accessible via the Internet
Resource development	Acquire access	Potential purchase of access to compromised target systems
Credential access	Brute force	Use of brute-force techniques to obtain target login credentials
Credential access	Unsecured credentials	Exploitation of default passwords
Impact	Data destruction	Compromise and damage to critical systems

A notable campaign in 2023 (C0031) targeted Unitronics PLC and human-machine interfaces (HMI), resulting in the defacement of device interfaces with anti-Israel messages (Cybersecurity and Infrastructure Security Agency, 2023, November; Cybersecurity and Infrastructure Security Agency, 2024, December). This defacement is illustrated in Figure 2—the first published by JNS (2023,

Figure 2: Defacement of Unitronics HMI interfaces attributed to Cyber Av3ngers. (a) Image published by JNS (2023, April). (b) Image featured by CBS News (Stanish, 2023, November).

April) and credited to Geller and Harod; the second featured by CBS News and attributed to the Municipal Water Authority of Aliquippa (Stanish, 2023, November). The confirmed attacks primarily affected WWS in both Israel and the United States. In general, the compromised devices were Unitronics Vision Series PLC that had been exposed to the Internet with default credentials accessible via transmission control protocol (TCP) port 20256. In response to this incident, CVE-2023-6448 was published, addressing the underlying vulnerability exploited in these attacks.

Cyber Av3ngers maintains a presence on X (formerly known as Twitter), where they previously claimed responsibility for compromising water treatment facilities. Figure 3(a) displays an image dated October 30, 2023, which was attached to a post in which the malicious actors claimed responsibility for compromising OT-ICS within WWS. Figure 3(b) presents an image of an exposed HMI from a water treatment plant, also shared via X/Twitter in 2023. The threat actors are likewise active in Telegram groups. For example, Figure 3(c) displays a screenshot of a probable ICS or PLC interaction interface,

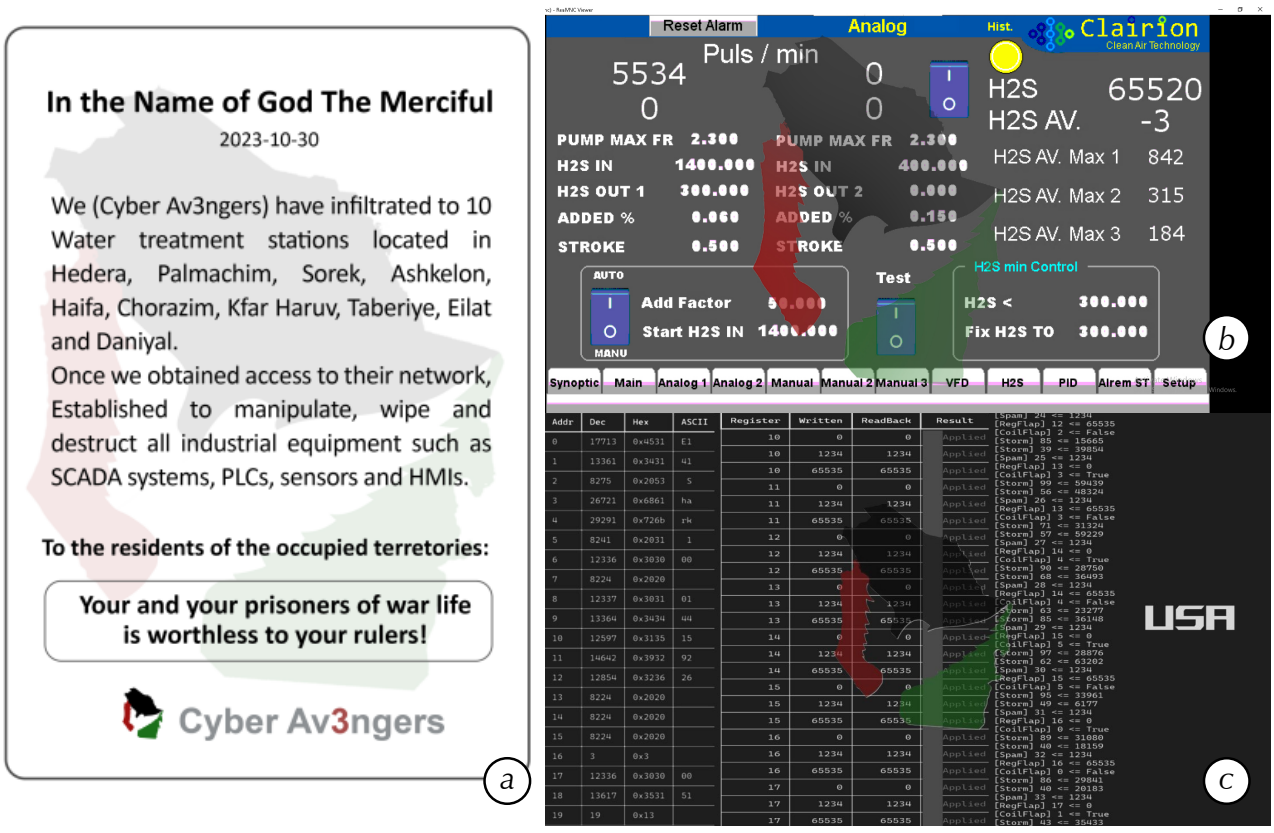

Figure 3: Social media records of Cyber Av3ngers' operations. (a) Image posted by Cyber Av3ngers on X, claiming compromise of OT-ICS within WWS. Dated October 30, 2023. (b) Image of an exposed HMI from a WWS. (c) Screenshot of a probable ICS or PLC interface.

showing register values along with write/read results.

Cyber Av3ngers has also claimed responsibility for a range of attacks, including:

- Targeting Israel's railway infrastructure (Tasnim News Agency, 2023, September).
- Attacks against the Israeli electric sector, allegedly resulting in a blackout.
- Distributed denial-of-service (DDoS) attacks on the website of an oil refinery (Dark Reading, 2023, July; Sharma, 2023, July).
- Intrusions into servers, security cameras, and smart city management systems across Israel (Greenberg, 2025, April).

However, some of these claims were later assessed as unsubstantiated or demonstrably false (Cybersecurity and Infrastructure Security Agency, 2024, December; Dragos, 2023, July; Kaspersky, 2023, October).

On February 2, 2024, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) **sanctioned six officials of the IRGC-Cyber Electronic Command (CEC) for their activities targeting critical infrastructure in the United States and other countries** (U.S. Department of the Treasury, 2024, February). They were listed as specially designated nationals (SDNs) pursuant to the counterterrorism authority of Executive Order 13224. Subsequently, the U.S. Department of State's Diplomatic Security Service, through the Rewards for Justice program, **offered a reward of up to $10 million** for information leading to the identification or location of these six officials in connection with their cyber operations targeting U.S. OT-ICS, in violation of the Computer Fraud and Abuse Act (CFAA). Figures 4 and 5 present official posters released in this context (U.S. Department of State, 2024, August), highlighting:

- The affiliation of Cyber Av3ngers with the IRGC-CEC, IRGC-Jangal Organization, IRGC-Electronic Warfare and Cyber Defense Organization, and Iranian security officials.
- The use of the **IOCONTROL malware** (Team82, 2024, December) to impact OT-ICS, as well as routers, firewalls, IP cameras, and Linux-based Internet of things (IoT) devices.
- The association with the **online persona Mr. Soul**.

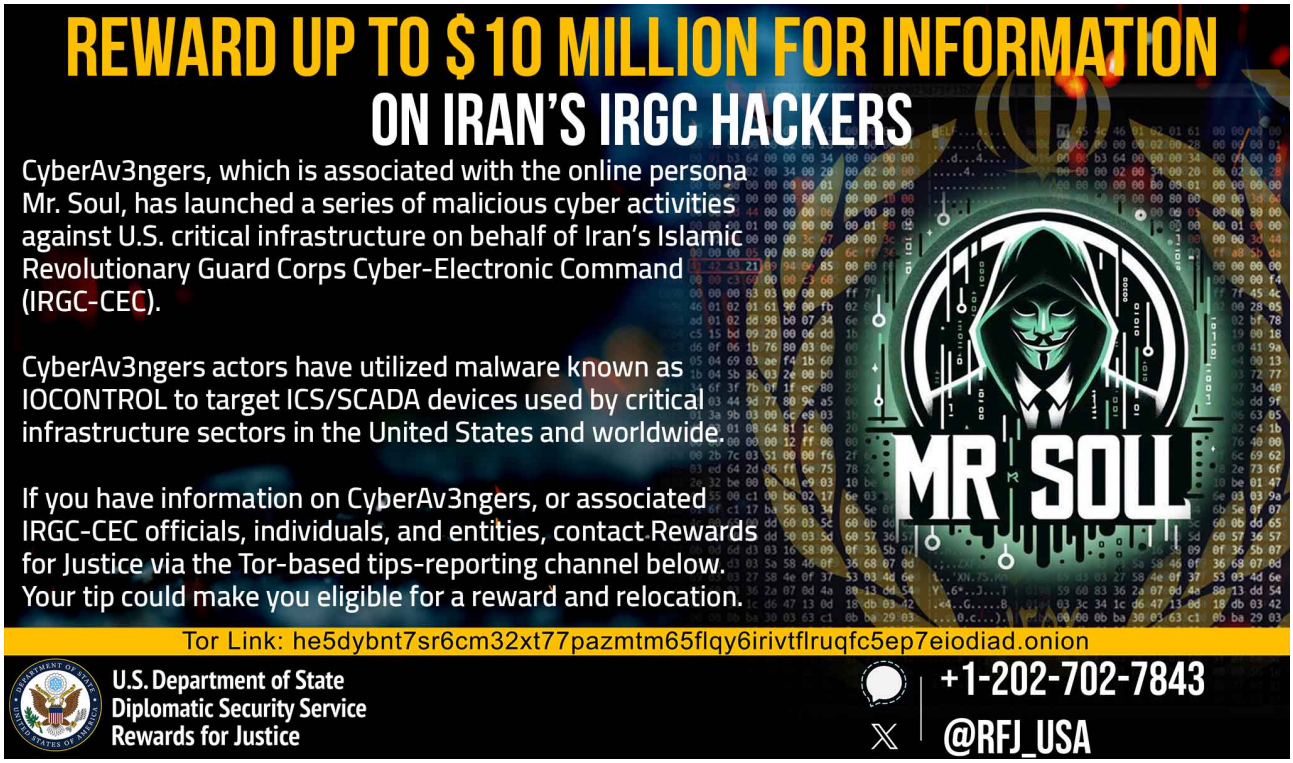

Figure 4: First poster released by the U.S. Department of State's Rewards for Justice.

Figure 5: Second poster released by the U.S. Department of State's Rewards for Justice.

3 Profiling via StealthMole's Platform 🔗

This section presents the main research findings derived from profiling conducted via the `StealthMole`'s platform. `Figure 6` provides an overview of this case study, comprising a total node count of 790. **Among the various cyber domain activities attributed to this threat group, this report focuses on operations that demonstrated impacts on OT-ICS**. The following key observations are subsequently presented:

- ❒ The initial stage of the investigation conducted via the `StealthMole`'s platform—particularly through its **Dark Web and Telegram trackers**—relied on the following keywords:
  - `CyberAv3ngers`.
  - `CyberAv3ng3Rs`.

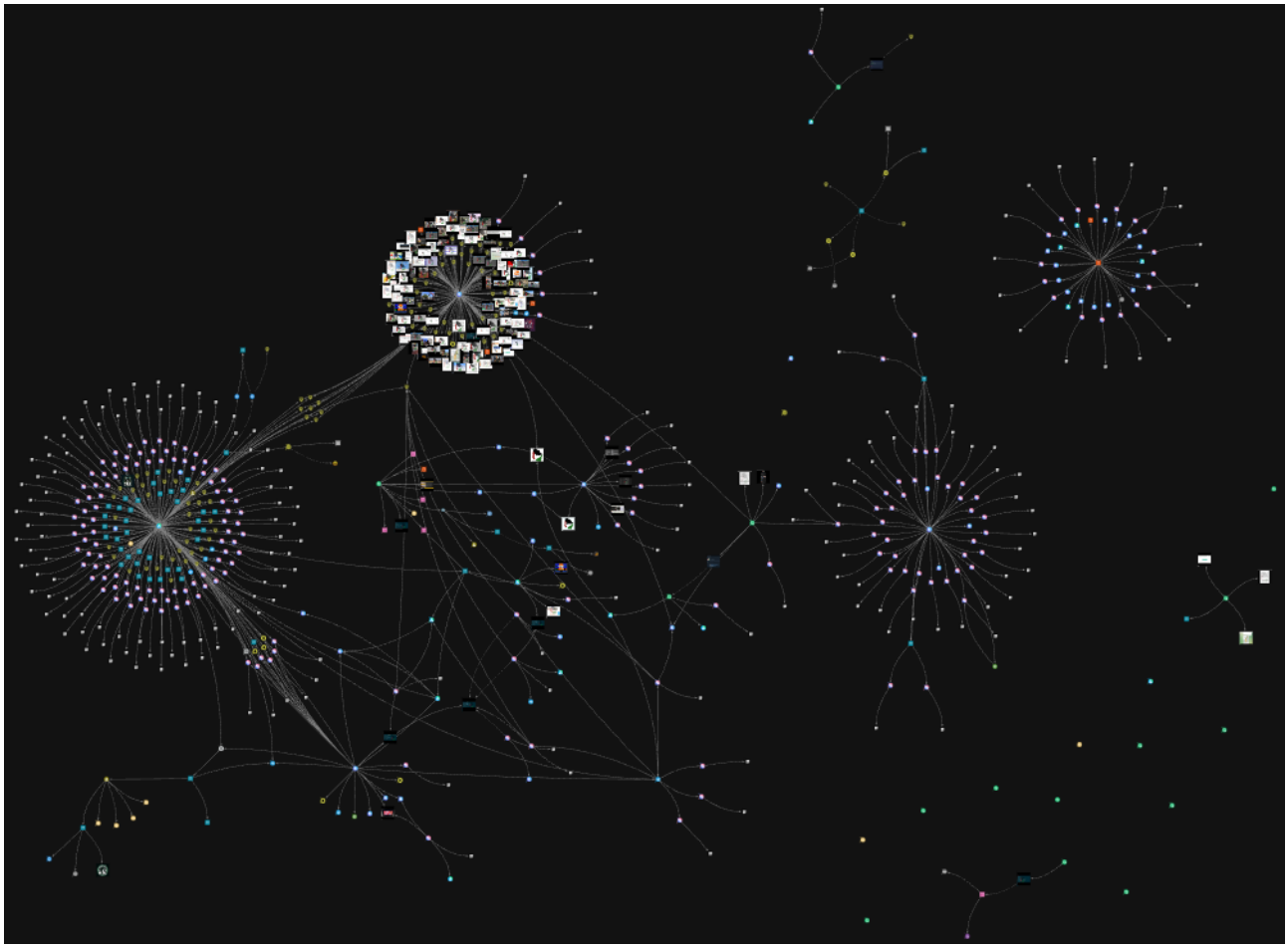

Figure 6: Overview of the case study conducted via the `StealthMole`'s platform.

  - `Cyberaveng3Rs`.
  - `Cyber Avengers`.
  - `Cyber Av3ngers`.
  - `( CyberAv3ngers )`.
  - `Soldiers of Soloman`.

❒ Among the identified **Telegram channels**, the following are of particular note:

  - `CyberAv3ngers`, a public channel with 1,193 subscribers as of August 8, 2025, created on October 1, 2024.
  - `CyberAveng3rs`, a channel with **366 archived messages** indexed on the `StealthMole` platform, created on September 13, 2023. Channel is no longer accessible.
  - `mrsoul_group`, a public channel with 1,983 members.
  - `Mrsoul_group`, a channel with **over 1,000 messages** indexed on the `StealthMole`'s platform. Channel is no longer accessible
  - `Mr. Soul Community`, a channel with **over 1,000 messages** indexed on the `StealthMole`'s platform. Channel is no longer accessible.
    * Caution is warranted when analyzing social media accounts allegedly associated with Cyber Av3ngers, as **there are mutual accusations among them of being fake and of disseminating false content**. `Figure 7` provides an example of this situation. The figure presents two images shared in the Telegram channel `mrsoul_group`, indicating that messages distributed via the `CyberAv3ngers` channel, as well as those from the Instagram account `mr.soul019`, are claimed to be fabricated.
    * Beginning on April 20, 2024, the Telegram channel `CyberAveng3rs` was allegedly compromised by another Israeli threat group, `WeRedEvils`. From that date onward, the channel disseminated purported personal information belonging to the "owner of Cyber Av3ngers," identified as **Mahdi Lashgarian**. The disclosed data reportedly included his passport number, national identification number, date of birth, mobile phone numbers, and residential address in Tehran, Iran, among other details. **Mahdi Lashgarian is one of the six officials from the IRGC-CEC sanctioned by the `U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)`.**

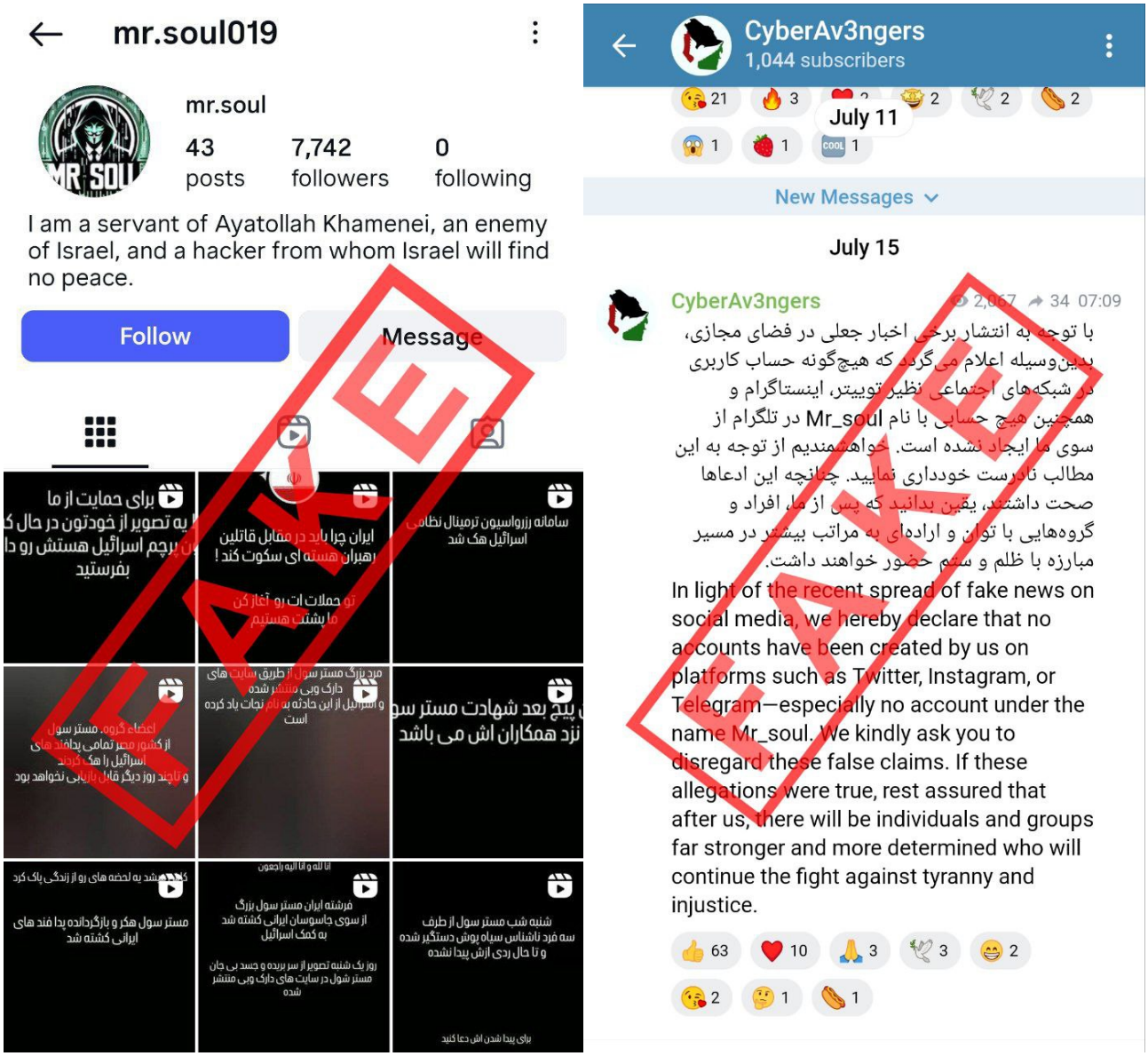

Figure 7: Images shared in the Telegram channel `mrsoul_group` on July 15, 2025.

- The following **X (formerly Twitter) profiles** were also identified:
  - `CyberAveng3rs`.
  - `mr_soul0`.
- Focusing on OT-ICS, Cyber Av3ngers has shared multiple images and videos on its social media platforms that allegedly depict system compromises. These materials generally consist of **screenshots of SCADA and HMI interfaces, Ladder logic or function block diagram (FBD) programming screens from PLC, as well as network maps and other technical documents (e.g.,**

single-line diagrams of electrical systems). Figure 8 presents a selection of such examples.

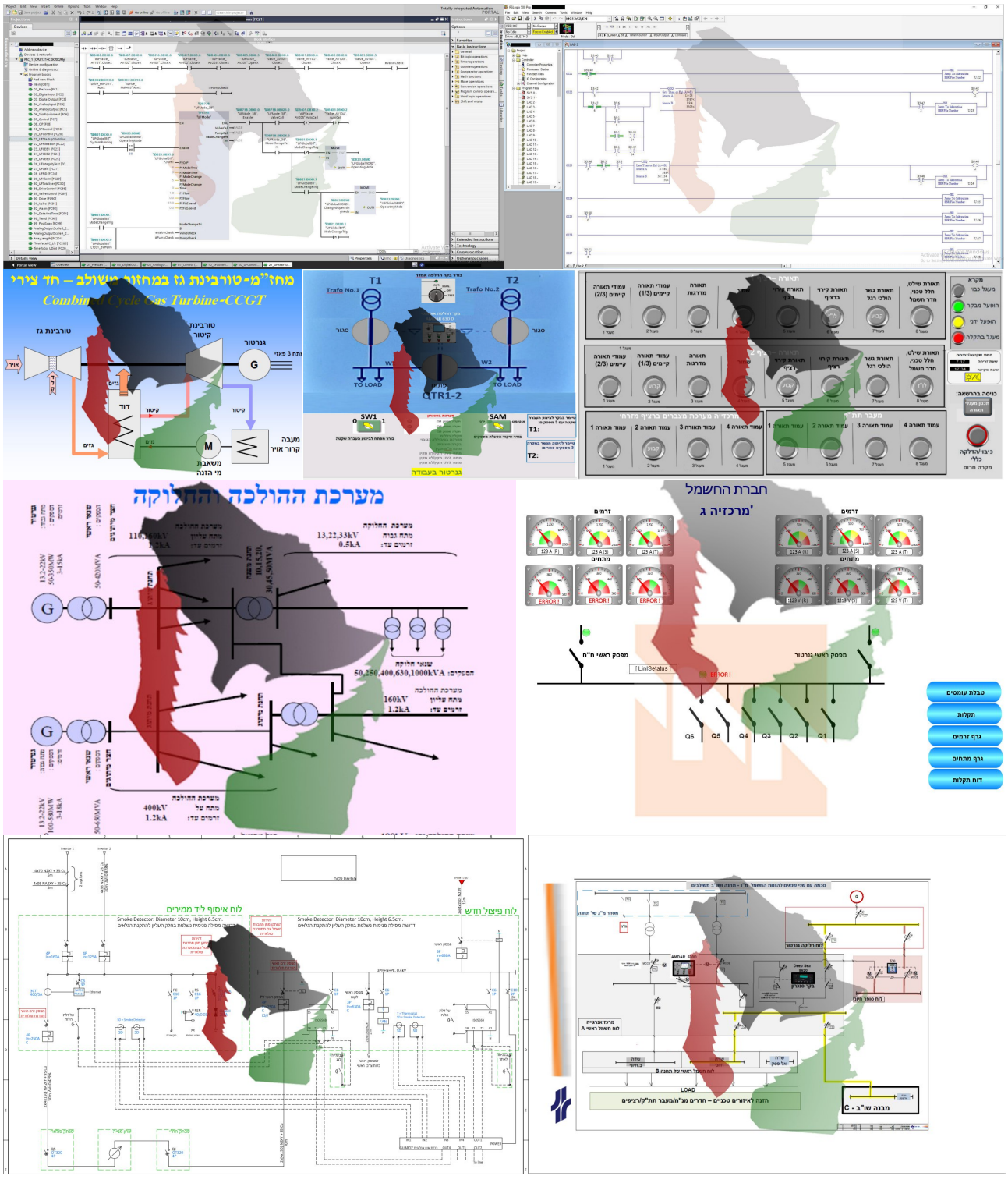

Figure 8: Collection of images shared by Cyber Av3ngers on its social media platforms, depicting OT-ICS interfaces and related technical documents.

- Caution must be exercised when evaluating leaked screenshots and videos, as they are often intended both to substantiate the threat actors' claimed compromises and to generate public and media attention. Some of the shared images consist solely of technical drawings of electrical systems or single-line diagrams of power networks. While such materials could indeed originate from a compromise of a corporate network or an engineering workstation, **they do not inherently indicate an ability to control OT-ICS environments**. Furthermore, certain images may have been fabricated by the threat actors themselves, as evidenced by the presence of grammatical correction marks from text editors, such as the screenshot with hash `81932d5b7e**********df0e1ec0fd`.
- Some electrical diagram screenshots bear the logo of `Israel Railways`, such as the images with hashes `c3d1a**********81cff` and `caf71**********b60f0` verified via the `StealthMole`'s platform. Cyber Av3ngers has, in fact, stated in messages on its Telegram channel—such as those with ID `18******84_33`, `18******84_34`, and `18******84_49`—that it has conducted cyberattacks against Israeli railway infrastructure. There are reposts suggesting the possibility of a cyberattack at that time, a claim denied by the operator (Dark Reading, `2023, September`). Additionally, expert analyses indicate that these alleged incidents are false and that the images were fabricated by the cybercriminals (Dark Reading, `2023, September`; Dragos, `2023, July`).
- Disseminated in Telegram messages with ID `18******83_6650` and `18******84_254`, the screenshot with hash `d406c**********36d93` depicts a PLC programming file containing Ladder logic symbols and function blocks. Following the investigation, it was identified that the software shown is `IPSoft`, which is used to configure `Delta` PLC. The screenshot with hash `6d0c3**********f7b77` (see `Figure 9`), disseminated in messages `18******83_6654` and `18******84_258`, depicts the process of transferring a programming logic from a workstation (specifically, the computer used by the threat actor) to the PLC. If Cyber Av3ngers indeed gained access to the PLC, **this image would demonstrate a capability to reconfigure the functions originally intended for that device**.
- Published on the `CyberAveng3rs` X/Twitter channel on October 30, 2023, the screenshot

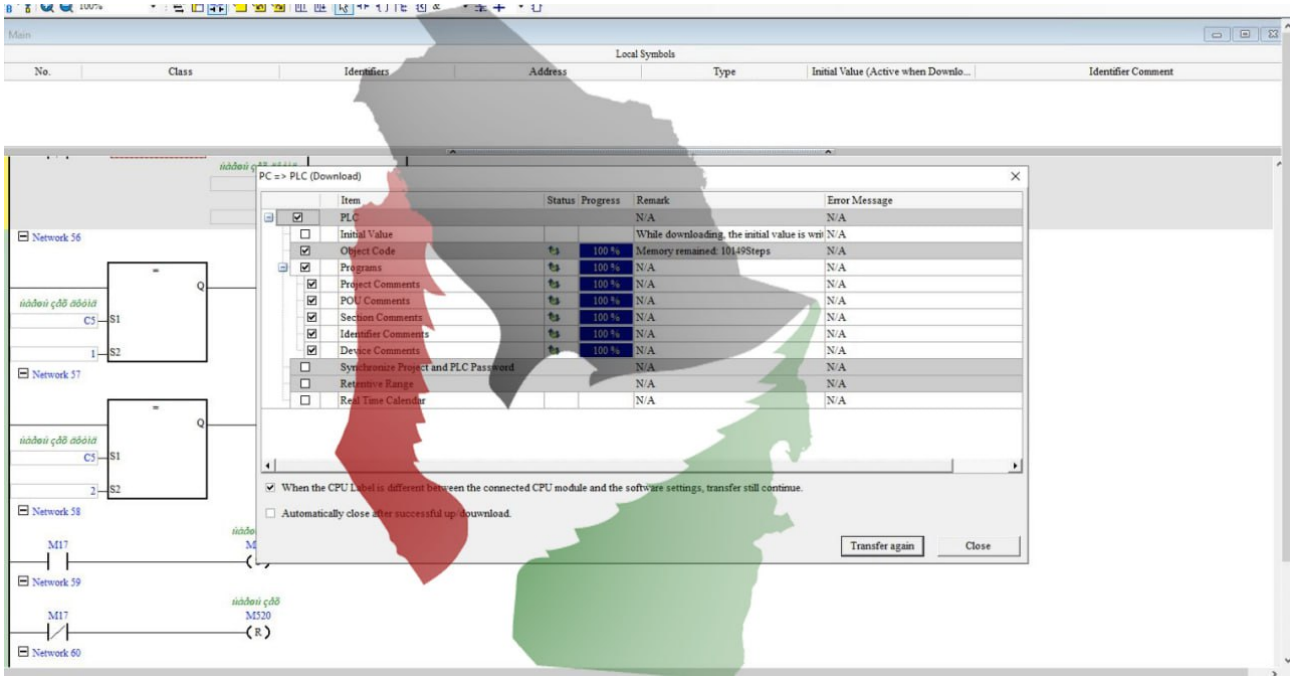

Figure 9: Screenshots allegedly depicting PLC programming activities, including Ladder logic editing in `Delta`'s `IPSoft` and the transfer of control logic to a PLC.

with hash `7c2f2**********10d64` (see `Figure 10`) depicts the programming interface of `RSLogix 500 Pro Edition`—a software platform used for programming and controlling `Allen-Bradley PLC, owned by Rockwell Automation`, such as the `SLC 500`, `MicroLogix 1100`, `MicroLogix 1200`, and `MicroLogix 1500` controllers.

  * The program is open in offline mode (upper-left corner displays `OFFLINE`), meaning there are no real-time variable values available to infer operational behavior.
  * The Ladder logic code shows comparison instructions (`GEQ`, `LEQ`) and jumps to subroutines (`JSR`); however, there are no descriptive tags that could reveal the control system's application.

– Also published on the `CyberAveng3rs` X/Twitter channel on October 30, 2023, the screenshot with hash `709e7**********4e4b3` corresponds to the project interface of `Siemens' Totally Integrated Automation (TIA) Portal`. The TIA Portal is a software framework used to program PLC, develop HMI, and parameterize drives. `Figure 11` presents this screenshot in detail, which is subsequently examined with further commentary.

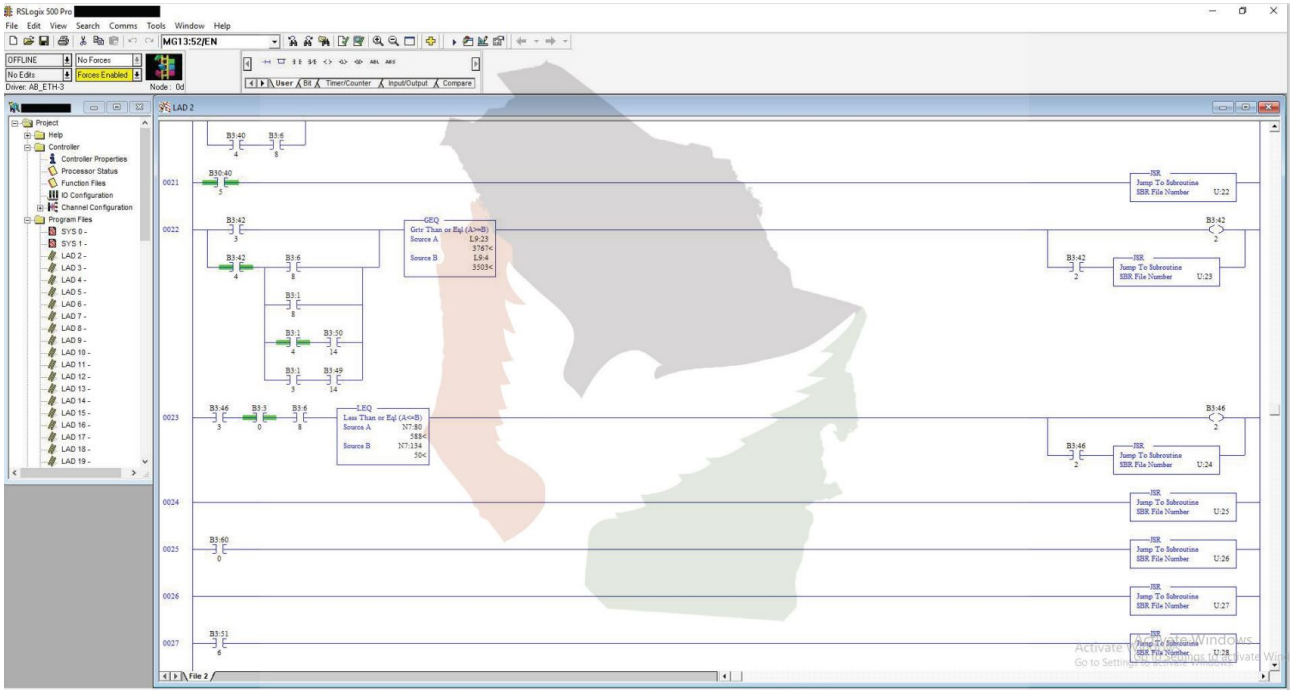

Figure 10: `RSLogix 500 Pro Edition` interface in offline mode, displaying Ladder logic for an unidentified control application.

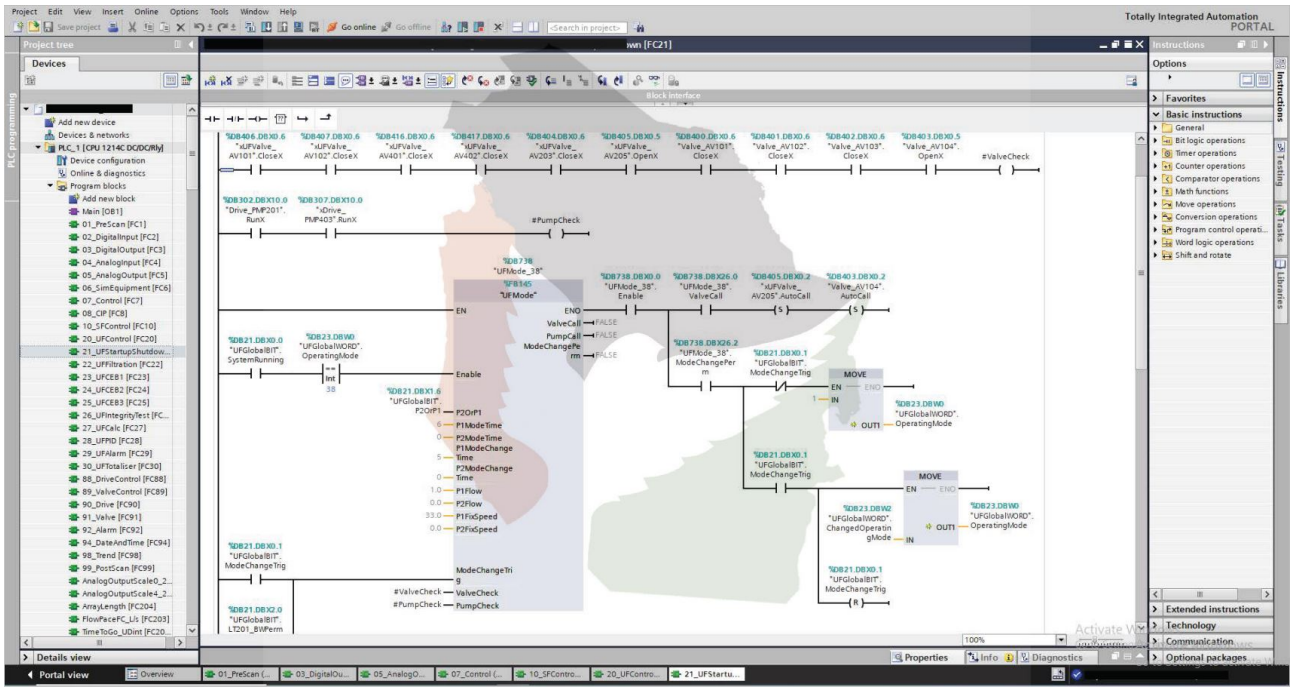

Figure 11: Screenshot of a `Siemens TIA Portal` automation project, published by Cyber Av3ngers on X/Twitter on October 30, 2023.

- On the left side of the screenshot, a project tree is visible, showing the term `CPU 1214C DC/DC/Rly`. This naming format and the CPU 1214C model code are characteristic of the `Siemens SIMATIC S7-1200` series. The suffix `DC/DC/Rly` indicates a 24 V DC power supply, DC digital inputs, and relay-based digital outputs.
- The abbreviation `UF` appears repeatedly (e.g., `20_UFControl`, `21_UFStartupShutdown`, `22_UFFiltration`, `27_UFCalc`, `29_UFAlarm`, `30_UFTotaliser`). `UF` may stand for **ultrafiltration**.
- The presence of blocks such as `28_UFPID` and `29_UFAlarm` suggests the existence of PID control loops and alarms specific to the automation process.
- The block `08_CIP` likely refers to a clean-in-place process, widely used in water treatment systems.
- Modules such as `ValveControl`, `PumpControl`, `DateAndTime`, and `AnalogInput/Output` complement equipment control and process data acquisition.
- **It is hypothesized that this PLC may be part of an ultrafiltration control system, which typically forms a stage in water treatment plants.**
- However, the screenshot indicates that there is no active connection to the PLC at the time it was taken. In the upper corner of the screen, the `Go online` button is visible (rather than `Go offline`), which means the project is currently offline. Furthermore, there are no online status indicators: such as green bars, real-time values, or connection icons in the project tree.
- Given the existence of a connection to the PLC and considering the hypothesis that it is part of a critical process within a water treatment plant, **the likelihood of causing damage to the infrastructure and posing risks to individuals is assessed as high**. Furthermore, specialized technical knowledge in engineering is required to program and understand an industrial automation application such as the one depicted in `Figure 11`.

❒ There are established links between the activities of Cyber Av3ngers and the online persona **Mr. Soul**, whose profile image used on social media is shown in `Figure 12`. Cyber Av3ngers have been reported to employ the **IOCONTROL malware**, a sample with the hash `1b39f**********84498` (Team82, `2024, December`), and Mr. Soul has been identified as one of the developers of this malware.

Figure 12: Profile picture of Mr. Soul. Source: Official `profile` on Telegram channel.

The following points provide more detailed observations.

- Mr. Soul has previously forwarded multiple messages on his Telegram channel from Cyber Av3ngers or containing news related to the group's operations and cyberattacks against Israel's WWS. Examples include messages with ID `20******54_1272`, `20******54_1518`, `20******54_1609`, `20******54_1610`, `20******54_1611`, and `20******54_2287`. Numerous additional messages in other Telegram channels also associate Cyber Av3ngers with Mr. Soul, such as those with ID `22******96_5359`, `20******35_2455`, `20******74_7923`, and `19*****65_936`, among others.
- The image with the file name `photo_2023-12-06*********.JPG` and hash `3889b**********************5b123` was published in Telegram message `20******54_2629` in response to message `20******54_2257` (on November 26, 2023) in the `Mr. Soul Community` channel, with an additional link to the `mrsoul_group` channel. The image depicts a defaced `Unitronics` HMI displaying an anti-Israel message, similar to the one shown in `Figure 2`.
- Mr. Soul offered the IOCONTROL malware for sale on `https://breachforums.st/****************************` (content hash: `9bf09**********************************************************5aa58`) on December 22, 2024, using the forum account `MrS0ul`. This information subsequently spread across various Telegram channels, including some pro-Palestinian groups. Examples include messages with ID `18******78_1971` and `18******78_1966`, among others. In the `breachforums.st` post, there is also a reference to the Telegram channel `mrsoul_group` and a TOX address `AE1C5*****<...>*****9EC2C`.

– Both Mr. Soul—in a video shared on October 30, 2023, in the Telegram channel `mrsoul_group`—and in screenshots posted in that same channel (e.g., message `20******54_304` with hash `e5f7b**********************136b0`) and others, demonstrate the use of a malicious script framework—`mr_soul_proxy`, `mr_soul_init`, and `mr_soul_controller`—executed in a Bash terminal on Kali Linux for the discovery, scanning, enumeration of services, and exploitation of OT-ICS devices. `Figure 13` shows one such screenshot. Displaying the Cyber Av3ngers logo (see `Figure 13`), the complete video reveals the following:

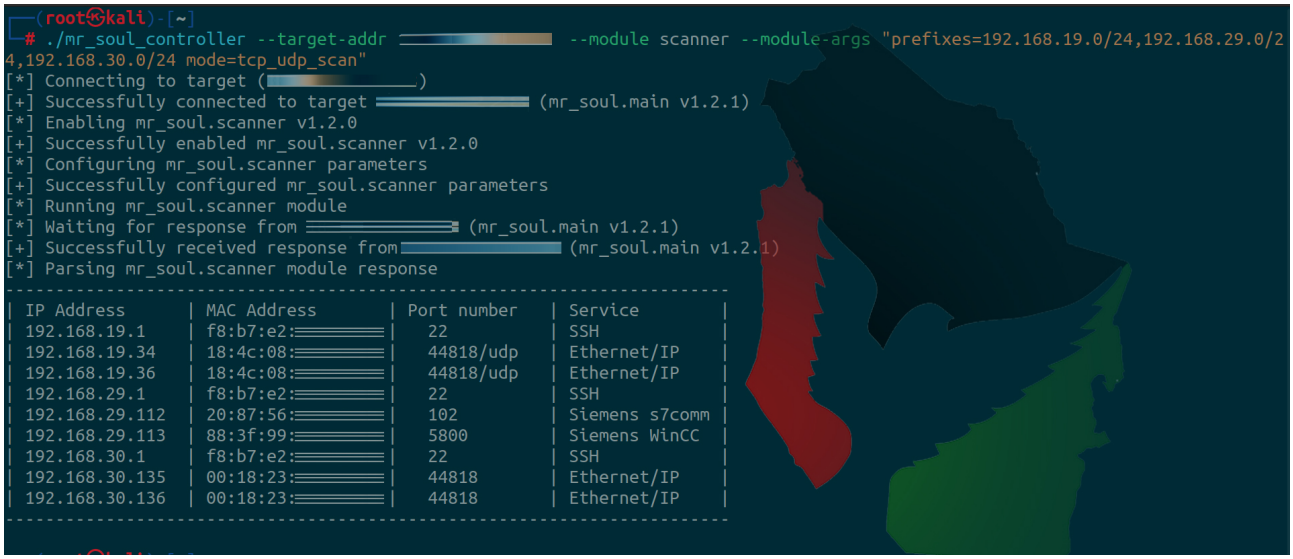

Figure 13: Screenshot showing the execution of the malicious framework in Kali Linux for OT-ICS reconnaissance, exploitation, and program-wiping operations targeting Siemens PLC.

* Multiple subnets (`192.168.19.0/24`, `192.168.29.0/24`, `192.168.30.0/24`) were scanned, identifying typical OT-ICS services, such as the Siemens S7Comm protocol (port 102/TCP), Siemens WinCC (port 5800/TCP), and EtherNet/IP (port 44818), as well as SSH (22/TCP).
* The terminal output shows the execution of an exploit named `program-wiper` against a target identified as Siemens, following a search for `siemens` in the framework's exploit database (`mr_soul_db`).
* **Activity flow:**
  1. Connection and activation of the scanner module.
  2. Network scanning.

3. Collection of OT-ICS targets.
4. Search within `mr_soul_db` for relevant exploits (weaponization).
5. Deployment of the exploit to the target. In a Siemens context, a "program-wiper" typically aims to erase PLC logic or data blocks (or to prevent their execution) resulting in process shutdown and requiring re-download and recommissioning.

* `MITRE ATT&CK for ICS` **mapping:**
  1. **Discovery:** `Remote System Discovery`. `Remote system information discovery`.
  2. **Execution:** `Command-Line Interface`. `Scripting`.
  3. **Impair Process Control:** `Data destruction`.
  4. **Impact:** `Denial of control`. `Denial of view`. `Loss of availability`. `Loss of control`. `Loss of view`. `Manipulation of control`. `Manipulation of view`.

– There are established links between Mr. Soul and digital footprints from the Telegram channel `CyberAveng3rs`. These include at **least nine IP addresses and a video file** with the hash `aee7a**********************************************76b9e`.

* `1**.2**.2**.1**`, Russia.
* `1**.1**.1**.9*`, United Kingdom/Netherlands.
* `1**.2**.4*.6*`, United States.
* `1**.2**.4*.1**`, United States.
* `1**.2**.4*.1**`, United States.
* `1**.2**.4*.*`, United States.
* `1**.6*.7*.1**`, United States/Canada.
* `1**.2*.*.1**`, United States/Canada.
* `1**.2*.*.1**`, United States/Canada.

❒ The investigation conducted via the `StealthMole`'s platform revealed references to, and associations with, the following CVE:

– `CVE-2000-0114`.

  - CVE-2008-1446.
  - CVE-2023-3519.
  - CVE-2023-36745.
  - CVE-2023-46747.

- ❒ The document titled ICS-_SCADA_systems_hacking.PDF, with hash 1524e5cbe6**********a32b458b9e, was shared in 17 messages by at least four Telegram users across 14 Telegram channels between March 28, 2023, and November 11, 2024. No direct links to Cyber Av3ngers were identified; however, the publication predates the main attacks of the 2023 campaign (C0031). The document serves as **a guide on how to identify, enumerate, and compromise ICS and SCADA systems**. Among the topics covered are:
  - Industrial protocols and their typical ports, including Modbus, DNP3, and PROFINET.
  - Recommendations for searches using Shodan.
  - Instructions for scanning Modbus services using nmap and specialized scripts (nmap scripting engine [NSE]).
  - Procedures for using modbus-cli, a command-line interface (CLI) tool that enables accessing and reading/writing registers on Modbus-enabled equipment.
  - Steps to access exposed devices via the vncviewer command without authentication or with default login credentials.
  - **Notably, methods for identifying vulnerable Unitronics PLC and HMI**, which may have been leveraged by Cyber Av3ngers.
  - Focusing on the exploitation of Unitronics devices, a Shodan search replicating the exact procedures recommended in the document identified a total of **772 exposed devices** (quantitative analysis only; no case-by-case assessment was conducted), as illustrated in Figure 14. Within Brazil alone, 19 such instances were observed. Alarmingly, some cases had Authentication disabled, with connectivity enabled via VPN. In Israel, 13 exposed devices were identified, again emphasizing that the assessment was purely quantitative.
  - Finally, the document provides instructions on using the VisiLogic software to establish connections with exposed PLC.

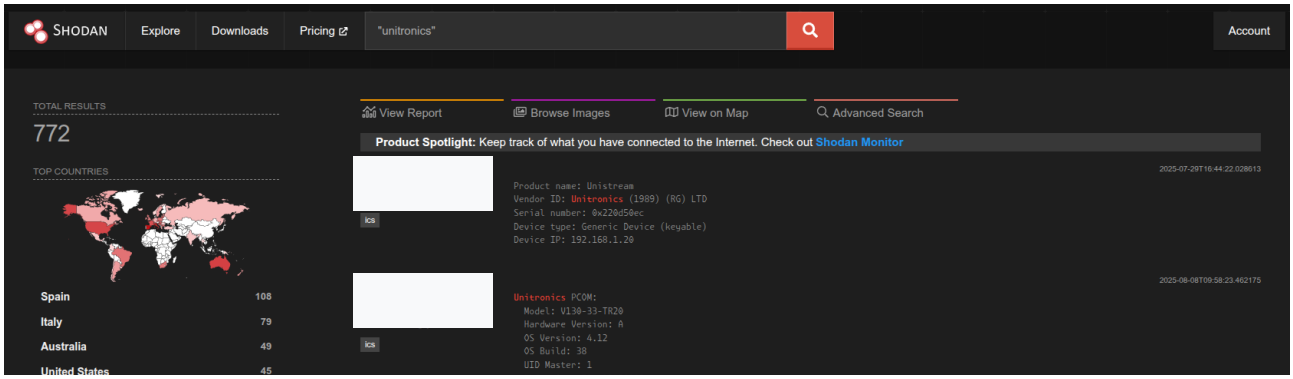

Figure 14: 772 exposed `Unitronics` devices identified via `Shodan` search replicating procedures from the `ICS-_SCADA_system_hacking.PDF` document.

4 Conclusion and Recommendations 🔗

Leveraging the `StealthMole`'s platform, the findings presented in this section underscore the operational scope, tactics, and capabilities attributed to the Cyber Av3ngers, as well as their affiliations with the online persona Mr. Soul. Evidence collected from Telegram channels, Dark Web sources, and social media platforms reveals a consistent focus on targeting OT-ICS environments, including the use of the specialized IOCONTROL malware and the exploitation of exposed industrial devices without authentication or with default credentials. While several materials disseminated by the threat actors are confirmed or highly plausible indicators of compromise, others appear to be fabricated or primarily intended for propaganda purposes. The findings highlight the cyber threat posed by the group; the dissemination of guides on compromising OT-ICS through Dark Web forums and Telegram channels; and the critical importance of OT-ICS-focused cyber threat intelligence. Finally, they reinforce recommendations previously disseminated by governmental agencies and industrial cybersecurity firms (Cybersecurity and Infrastructure Security Agency, `2023, November`; Cybersecurity and Infrastructure Security Agency, `2024, December`; Dragos, `2023, July`).

Given the extensive information obtained through the `StealthMole`'s platform and its relevance to the industrial cybersecurity community, this work will continue. The document will be updated as new developments arise, and a second part is planned.

5 References 🔗

Cybersecurity and Infrastructure Security Agency. (2023, November). *Cyber Av3ngers Hacktivist Group Targeting Israel-Made OT devices* (Cybersecurity Advisory). Retrieved August 7, 2025, from https://bit.ly/4fpyaIK.

Cybersecurity and Infrastructure Security Agency. (2024, December). *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities* (Cybersecurity Advisory). Retrieved August 7, 2025, from https://bit.ly/3J6AzvZ.

Dark Reading. (2023a, July). *Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers*. Retrieved August 7, 2025, from https://bit.ly/45po9G0.

Dark Reading. (2023b, September). *Pro-Iranian Attackers Claim to Target Israeli Railroad Network*. Retrieved August 7, 2025, from https://bit.ly/4fEgRUE.

Dragos. (2023, July). *Cyber Av3ngers Hacktivist Group Targeting Israel-Made OT devices* (The Dragos Blog). Retrieved August 7, 2025, from https://bit.ly/4ljIpQq.

Greenberg, A. (2025, April). *CyberAv3ngers: The Iranian Saboteurs Hacking Water and Gas Systems Worldwide*. WIRED. Retrieved August 7, 2025, from https://bit.ly/4mrn3Bq.

JNS. (2023, April). *Cyber Attack Shutters Galilee Farm Water Controllers*. Retrieved August 7, 2025, from https://bit.ly/4ow6QNi.

Kaspersky. (2023, October). *A Hack in Hand is Worth Two in the Bush* (Securelist). Retrieved August 7, 2025, from https://bit.ly/45kcvNv.

Microsoft Threat Intelligence. (2024, February). *Staying Ahead of Threat Actors in the Age of AI* (Blog, Threat Intelligence). Retrieved August 7, 2025, from https://bit.ly/47qhtea.

MITRE ATT&CK. (2024, March). *Cyber Av3ngers. Groups, ID G1027*. Retrieved August 7, 2025, from https://attack.mitre.org/groups/G1027.

Nimmo, B., & Flossman, M. (2024). *Influence and Cyber Operations: An Update* (Threat Intelligence Report). OpenAI. San Francisco, CA, US. Retrieved August 7, 2025, from https://bit.ly/4om6BV3.

Sharma, A. (2023, July). *Israel's Largest Oil Refinery Website Offline After DDoS Attack* (News, Security). BleepingComputer. Retrieved August 7, 2025, from https://bit.ly/4mxgZr2.

Stanish, E. (2023, November). *Municipal Water Authority of Aliquippa Hacked by Iranian-Backed Cyber Group*. CBS News. Retrieved August 7, 2025, from https://bit.ly/40WaGoR.

Tasnim News Agency. (2023, September). *Israeli Rail System Comes Under Cyberattack* (News). Retrieved August 7, 2025, from https://bit.ly/4m72oTD.

Team82. (2024, December). *Inside a New OT/IoT Cyberweapon: IOCONTROL*. Claroty. Retrieved August 7, 2025, from https://bit.ly/3J6Nu0T.

U.S. Department of State. (2024, August). *CyberAv3ngers*. Diplomatic Security Service, Rewards for Justice. Retrieved August 7, 2025, from https://rewardsforjustice.net/rewards/cyberav3ngers.

U.S. Department of the Treasury. (2024, February). *Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure* (Press Release). Office of Foreign Assets Control. Retrieved August 7, 2025, from https://bit.ly/3H0eH4U.

Cyber Threat Intelligence

CyberAv3ngers

Profiling Operational Technology Threat Actors Using StealthMole's Platform

Luiz F. Freitas-Gutierres (a.k.a substationworm) is a professor in the Department of Electromechanics and Power Systems at the Federal University of Santa Maria. His primary research interests include: industrial cybersecurity, cyber threat intelligence, and the automation of electric power systems.

Ind.Cyber.Sec Letters

Ind.Cyber.Sec Letters is a collection of studies and analyses of incidents in the field of industrial cybersecurity. Check out more content and full reports at:

`github.com/substationworm/IndCyberSecLetters`

StealthMole

This research made use of the ***StealthMole's platform***. Further details can be found at:

`stealthmole.com`

CC BY

Prof. Dr. Luiz F. Freitas-Gutierres
`linkedin.com/in/lffreitas-gutierres`
`github.com/substationworm`
`luiz.gutierres@ufsm.br`

Published:
August 11, 2025