ICS attack classifications: differentiating between cyberwarfare, cyberterrorism, and hacktivism

June 13, 2023

Research & Threat Intel 13 Jun 2023
Written By
Beatriz Pimenta Klein Threat Intelligence Analyst, Outpost24

In this article, we build the bridge between the conceptual field of International Relations and the terminology employed by cybersecurity practitioners. We will translate all these understandings into real-life applications to empower the analyst to properly classify clusters of malicious activities. This way, we as a community strengthen our analytical capabilities to better assess collected intelligence material. All in all, qualified multi-skilled threat intelligence teams and solutions are strong foundations on which companies must rely to make informed security and business decisions.

Get ready to unlock the mysteries of the digital battlefield, where lines between virtual and physical realms blur, and the stakes are higher than ever before.

Bridging the gap between cybersecurity and International Relations

The cybersecurity industry often adopts certain terminology and conceptualization that is not spontaneously translated into other fields of knowledge. Therefore, practitioners from different areas investigate converging themes but fail to communicate with one another. So here we shed light on topics of confluence between cybersecurity and International Relations, as one can benefit from the other.

Are state-sponsored groups cyber proxies?

In the industry, we discuss the activities of state-sponsored threat actors, often personified in the notion of Advanced Persistent Threat (APT) groups. These understandings are not novel in the history of geopolitics; the employment of mercenaries is a widely acknowledged practice. Contemporarily, the adoption of proxies and the emergence of proxy wars rather than resorting to traditional state-waged total wars is an adopted practice that allows states to circumvent international law. The logic can be, and gradually is more and more, applied to the cyber realm. What academics would call cyber proxies – and what the industry calls state-sponsored threat groups – are essential actors in the translation of geopolitical conflicts into the cyber domain, for a series of reasons. For instance, cyber proxies provide added technical capabilities to their sponsors, filling the capacity gap within the state's apparatus, which makes this relationship costly-effective for the hiring nation. Besides, proxies add a layer of complexity to the accountability process, benefiting the state in terms of international law compliance.

In earlier stages of cyber development, nations would get their hands dirty by directly conducting attacks against geopolitical rivals – Stuxnet is one of the most remarkable examples of such conduct. However, through the years, cyber proxies have proven to be less costly, safer for diplomacy, and more practical in technical/capabilities terms. Thus, an evolutive example would be the attacks against Ukrainian infrastructure and companies conducted by the Russian group "*SaintBear*" since the beginning of the war between Russia and Ukraine in 2022. This group, likely at least partially state-sponsored, is believed to be behind the destructive WhisperGate attacks that impacted Ukrainian government agencies in January 2022. This last example reinforces the thesis of the increase in cyber proxies' employment.

Defining cyberwarfare, cyberterrorism, and hacktivism

Part of the cyber threat intelligence's attribution process involves identifying the threat actor's objectives. In the industry, standardized vocabulary like threat taxonomies defines a set of potential motivations for attacks and supports the analyst's comprehension of their object of study. Yet, it does not insulate the field of knowledge from often misconceptions and concepts that might be difficult to tell apart. One example is the categorization of cyberwarfare, cyberterrorism, and, lastly, hacktivism. The imprecise definition of each one of these phenomena, as well as the participation of different kinds of actors in them, lead to a classification mess that is hard to untangle. Two key factors that might determine the distinction between events are the intended goal of an attack and the nature of the perpetrators. Let us move on to definitions.

Only states can wage war. The use of force by other types of actors shifts the nature of the conflict to other classifications, such as riot, civil war, asymmetric war, etc. As only states can wage war, naturally, only states can wage cyberwar. Thus, cyberwarfare must involve two or more state agents. Naturally, it is not easy to determine if a threat actor is part of the state's apparatus; but for definition purposes, that shall be the understanding.

As for cyberterrorism and hacktivism, more subtle factors come into play. Both activities are defined by the pursuit of an agenda – be it political, religious, economic, you name it – and consequential use of cyberattacks to advance these objectives. The identity nature of the perpetrators of cyberterrorist attacks or hacktivist attacks is the same: both are necessarily non-state agents. This includes cyber proxies and independent actors, who could even be supported by a state – which might oversee their criminal acts, might finance the group, etc. – but they are still not part of the state machine. Then what differentiates a cyberterrorist act from a hacktivist one? The intended goal of the actor's attacks. Although the two categories are not mutually exclusive, a cyberterrorist act aims to cause disruption and harm, or the threat thereof, likely provoking a kinetic attack, to advance an agenda, or coerce a group to advance said objectives. On the other hand, while a hacktivist attack may also aim for the disruption of services, it does not intend to cause harm.

Finally, one particularity of cyberterrorist attacks is that they target critical infrastructure. The disruption of critical infrastructure is the core element of cyberterrorism, as only attacks with such magnitude could represent an act of violence capable of inspiring terror and pressuring governments into giving in to the cyberterrorists' exigencies.

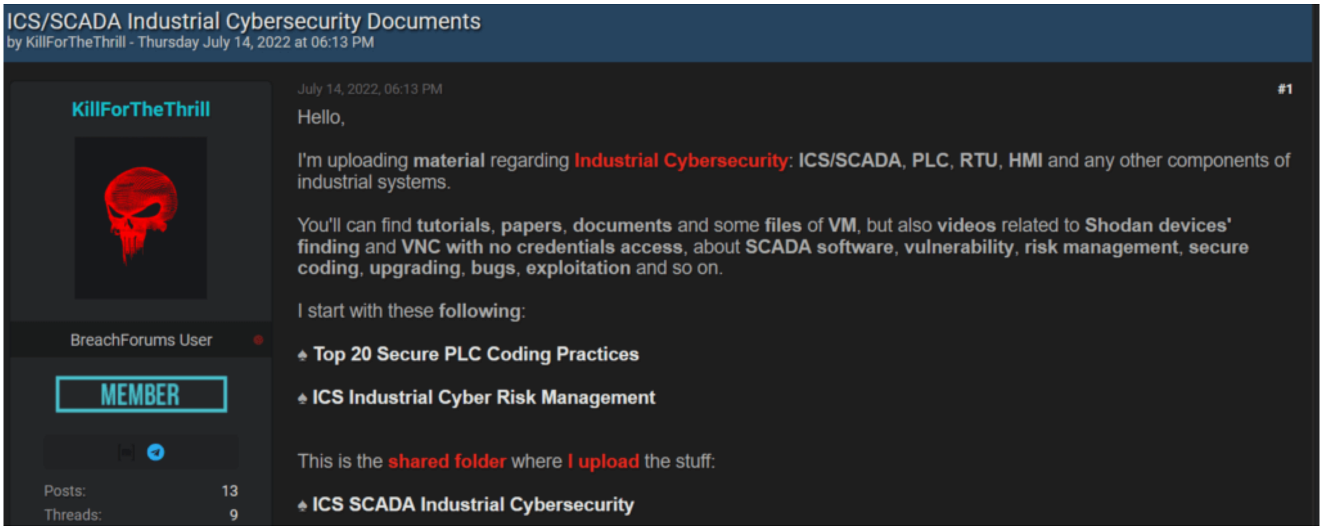
Cyber-attacks against Industrial Control Systems

Industrial Control Systems (ICS) and their software element, Supervisory Control and Data Acquisition Systems (SCADA), are prime examples of critical infrastructure control systems that are prone to vulnerability and, consequently, exposed to cyberterrorism. Inflicting significant damage to critical infrastructure raises attackers to an advantageous position of power that might push targets to relent.

But what is comprised under the critical infrastructure umbrella? It is up to each nation to define its national security interests, but in general terms, these are sectors that build up national capabilities. In the European context, legislative bodies have long worked to define the European Critical Infrastructures (ECIs), but based on Directive (EU) 2022/2557 (still under transposition into national laws) the pillars are the energy; transport; banking; financial market infrastructure; health; drinking water; waste water; digital infrastructure; public administration; space; production, processing and distribution of food sectors. In the United States, according to the Presidential Policy Directive/PPD-21, there are 16 sectors understood as critical infrastructure: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater. Each legislative body judged and formulated EICs based on specific national priorities, but we note overlaps between the European and the North American perspectives. Notably, cyberterrorists have a wide range of potential targets – and, on the other hand, nations have a lot to worry about. Even more worrisome: at least 5 out of the 11 sectors in the European perspective and 8 out of the US' 16 sectors use ICS management systems. Let us examine that in detail.

SCADA systems are usually employed to control processes in the oil/gas, manufacturing, air traffic/railways, power generation/transmission, and water management sectors. An impactful attack targeting such systems does not necessarily cause destruction solely by opening dams, causing aviation accidents, or exploding a factory. An impactful attack against SCADA systems may wreak havoc by producing failure cascading, for instance – which is possible through a supply chain attack. Some examples of potential attacks against SCADA systems are: "issuing unauthorized commands to control equipment; sending false information to a control-system operator that initiates inappropriate action[;] delaying or blocking the flow of information[;] making unauthorized changes to control system software to modify alarm thresholds or other configurations; and rendering resources unavailable”. We see that not only kinetic or destructive attacks need to be carried out to cause chaos, disruption, and national emergencies.

It is also worth highlighting the role of SCADA systems’ stakeholders when debating risks. It is not only national governments that oversee the administration of such systems for critical infrastructure entities; state, local, tribal, and territorial (SLTT) and private entities are also implicated in defending against attacks targeting critical infrastructure. Then, we have the following situation: it is in the best interest of cyber proxies and cyberterrorists, with all their technical capabilities and financial support, to target critical infrastructure, while we often rely on private actors and SLTT to defend nations’ most critical assets against cyber giants. Something in this equation is clearly off, and we, as societies, are the ones who end up paying the bill. It is exactly in this asymmetrical capability dynamic that lies our most dangerous flaws.



ICS/SCADA Industrial Cybersecurity Documents
by KillForTheThrill - Thursday July 14, 2022 at 06:13 PM

KillForTheThrill

BreachForums User

MEMBER

Posts: 13
Threads: 9

July 14, 2022, 06:13 PM #1

Hello,

I'm uploading **material** regarding **Industrial Cybersecurity**: **ICS/SCADA**, **PLC**, **RTU**, **HMI** and any other components of industrial systems.

You'll can find **tutorials**, **papers**, **documents** and some **files** of **VM**, but also **videos** related to **Shodan devices' finding** and **VNC with no credentials access**, about **SCADA software**, **vulnerability**, **risk management**, **secure coding**, **upgrading**, **bugs**, **exploitation** and so on.

I start with these **following**:

♠ **Top 20 Secure PLC Coding Practices**

♠ **ICS Industrial Cyber Risk Management**

This is the **shared folder** where **I upload** the stuff:

♠ **ICS SCADA Industrial Cybersecurity**

Figure 1. Threat actor shares for free ICS/SCADA systems documentation on the defunct Breached forum.

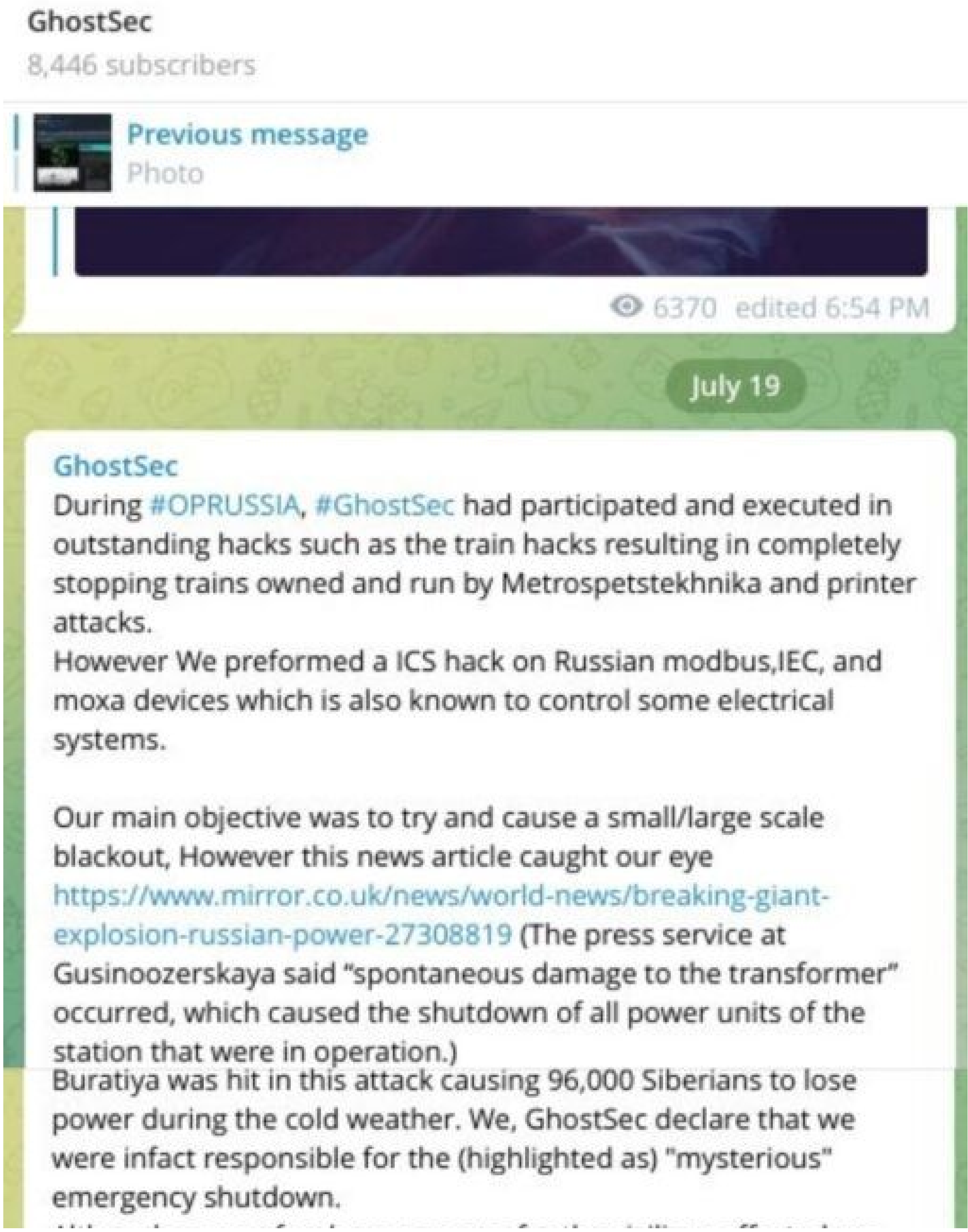
When it comes to terrorism, the word itself gives away that a key component is to instill fear. Therefore, conducting one massive, destructive, isolated attack against ICS might already do the job of spreading a message and subduing an enemy. However, cyberterrorists are likely to engage in hybrid attacks when targeting critical infrastructure. It means that attackers might (in a short time frame) conduct DDoS attacks against related targets; publicize that they have acquired access to SCADA systems (usually sharing some screenshots, leaking documents, or so); conduct information operations; or employ other techniques that put targets under pressure. Yet, as stated before, these activities are not conducted in isolation: the attacker concretely intends to provoke significant harm as a means to advance a message.

Real-life examples of attacks against ICS infrastructure

All things considered, it is time to showcase some real-life examples of attacks against ICS infrastructure that Outpost24's Threat Intelligence team, KrakenLabs, have observed throughout the past few years.

GhostSec

"*GhostSec*" is a highly organized threat group associated with the international hacktivists "Anonymous" network. The group first emerged in 2015 and it is often considered a hacktivist group: aligned with what was discussed in this article, *GhostSec* intends to cause disruption, but no harm with its actions. Let us analyze some material from the group to assess these claims:



GhostSec

8,446 subscribers

GhostSec

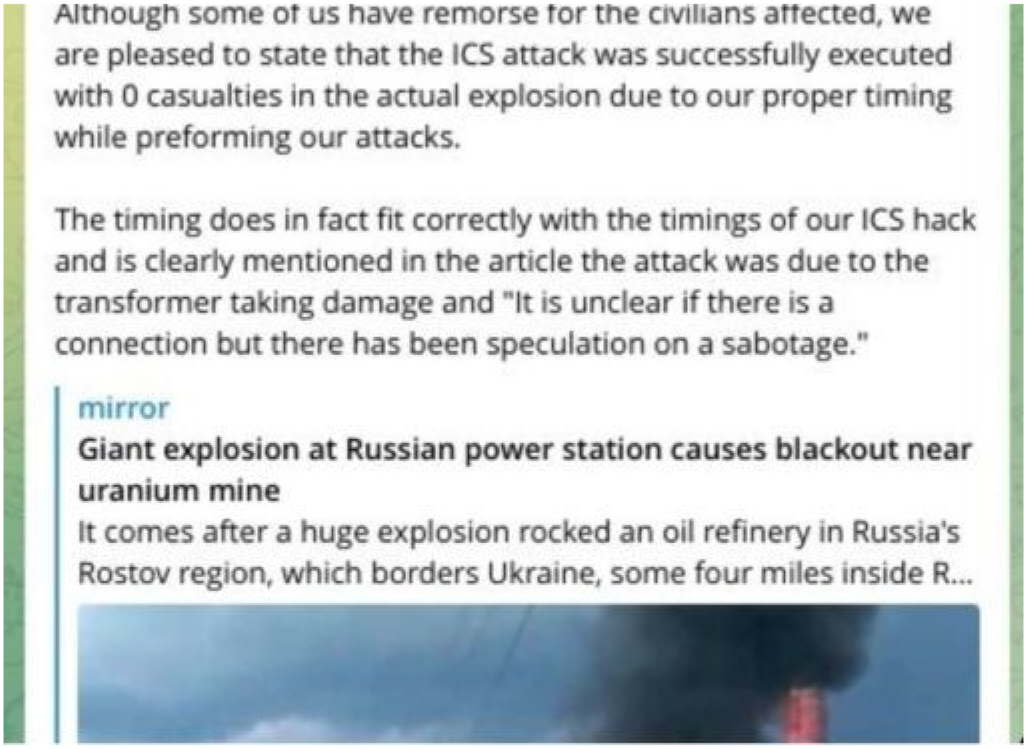
During #OPRUSSIA, #GhostSec had participated and executed in outstanding hacks such as the train hacks resulting in completely stopping trains owned and run by Metrospetstekhnika and printer attacks.

However We preformed a ICS hack on Russian modbus,IEC, and moxa devices which is also known to control some electrical systems.

Our main objective was to try and cause a small/large scale blackout, However this news article caught our eye https://www.mirror.co.uk/news/world-news/breaking-giant-explosion-russian-power-27308819 (The press service at Gusinoozerskaya said "spontaneous damage to the transformer" occurred, which caused the shutdown of all power units of the station that were in operation.)

Buratiya was hit in this attack causing 96,000 Siberians to lose power during the cold weather. We, GhostSec declare that we were infact responsible for the (highlighted as) "mysterious" emergency shutdown.

Figure 2.



Although some of us have remorse for the civilians affected, we are pleased to state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while preforming our attacks.

The timing does in fact fit correctly with the timings of our ICS hack and is clearly mentioned in the article the attack was due to the transformer taking damage and "It is unclear if there is a connection but there has been speculation on a sabotage."

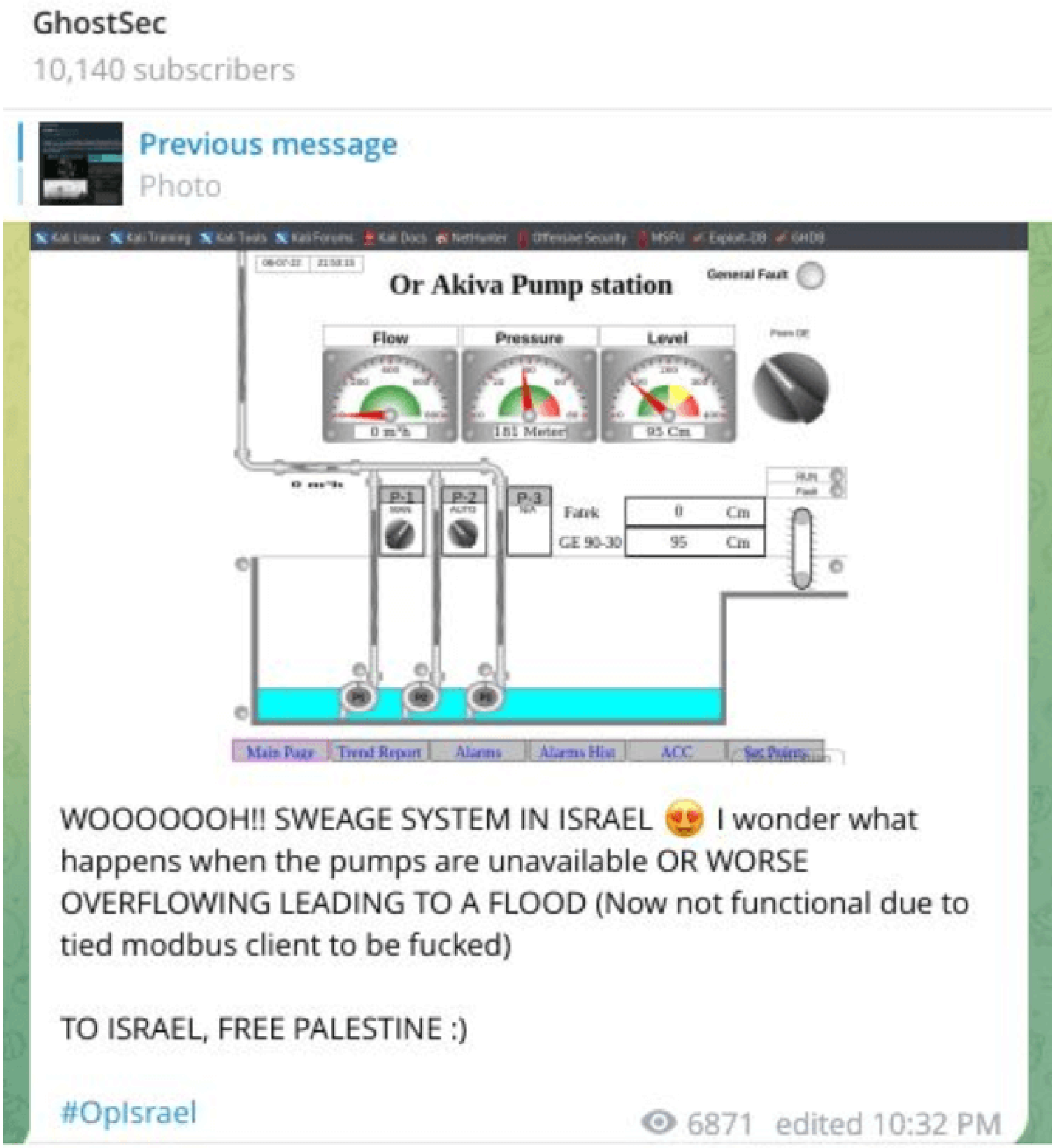
mirror

Giant explosion at Russian power station causes blackout near uranium mine

It comes after a huge explosion rocked an oil refinery in Russia's Rostov region, which borders Ukraine, some four miles inside R...

GhostSec's Telegram channel from July 19, 2022

The screenshot above was published on the group's Telegram channel in mid-2022, in which it claims to have hacked into the ICS infrastructure of Russian electric systems. The infrastructure in question is allegedly the Gusinoozerskaya hydro-power plant in Russia, and according to the news article by the Mirror (shared by the threat group in the Telegram post), the attack impacted the electric supply of the cities of Ulan-Ude and Krasnokamensk. The group claims that they intended to cause a blackout and emphasizes the fact that there were zero casualties involved in the attack, reinforcing their hacktivist nature.



GhostSec

10,140 subscribers

Previous message

Photo

WOOOOOOH!! SWEAGE SYSTEM IN ISRAEL 😍 I wonder what happens when the pumps are unavailable OR WORSE OVERFLOWING LEADING TO A FLOOD (Now not functional due to tied modbus client to be fucked)

TO ISRAEL, FREE PALESTINE :)

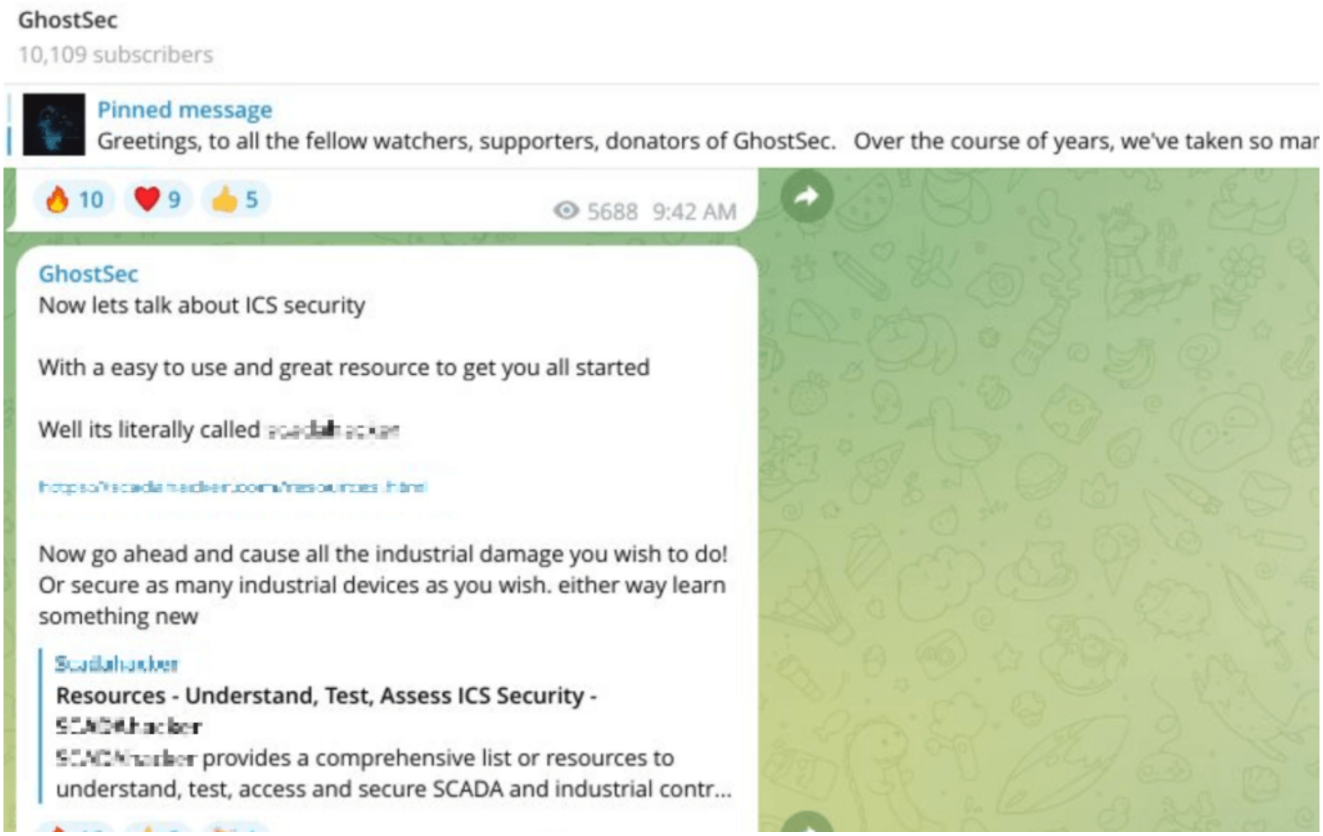
#OpIsrael

6871 edited 10:32 PM

Figure 3. GhostSec announces to have access to the Or Akiva sewage station in a post made on the group's Telegram channel on July 06, 2022.

Another example observed was in early July 2022. Although there was no disruptive attack in this case, *GhostSec* shared a screenshot to prove it had access to the Israeli city of Or Akiva's sewage stations. The threat group went on to say that the "*scale of these attacks will lead to industrial control systems being non-functional, including pump systems, electricity, etc*", implying that this post was more of a threat of what the group can do. According to the newspaper Haaretz, upon the publication by *GhostSec*, the journalist team reached out to the Israeli National Cyber Directorate, which in turn contacted the Or Akiva municipality on July 07, 2022, but the exposed sewage interface remained exposed – with no required password for access – until many hours later.

Interestingly, but not surprisingly, this team is not only interested in perpetrating attacks themselves. Instead, as they have a political agenda to follow, they encourage and incentivize other threat actors to commit attacks against ICS infrastructure, as per the following figure:



GhostSec
10,109 subscribers

Pinned message
Greetings, to all the fellow watchers, supporters, donators of GhostSec. Over the course of years, we've taken so mar

🔥 10 ❤️ 9 👍 5 5688 9:42 AM

GhostSec
Now lets talk about ICS security

With a easy to use and great resource to get you all started

Well its literally called [redacted]

[redacted]

Now go ahead and cause all the industrial damage you wish to do! Or secure as many industrial devices as you wish. either way learn something new

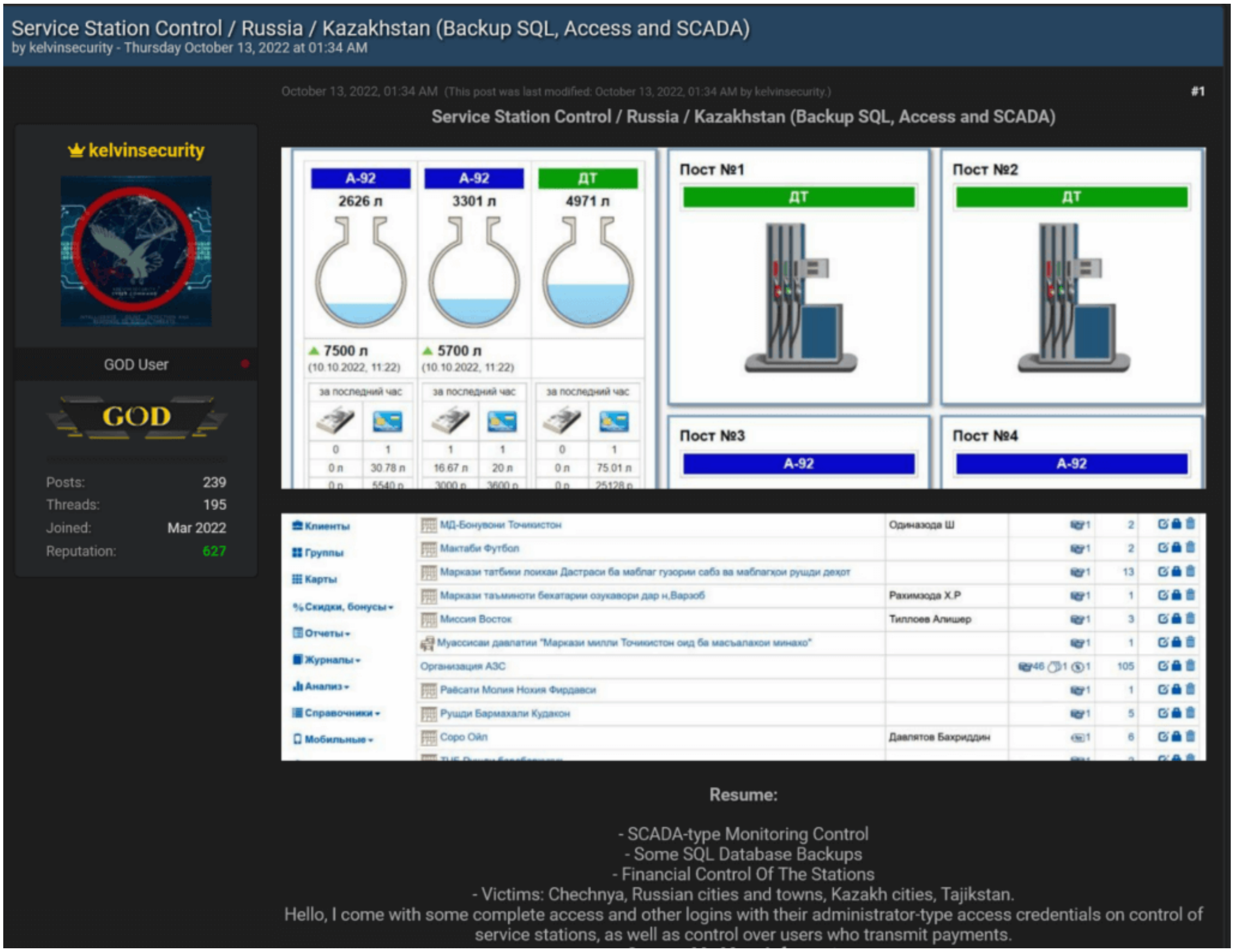
[redacted]
Resources - Understand, Test, Assess ICS Security - [redacted]
[redacted] provides a comprehensive list or resources to understand, test, access and secure SCADA and industrial contr...

Figure 4. GhostSec shares free material on how to target SCADA systems on its Telegram channel.

This screenshot, taken from *GhotsSec's* Telegram channel, corroborates the practice illustrated by Figure 1, in which cybercriminals share knowledge among themselves on how to conduct all sorts of attacks, in a true community sense.

KelvinSecTeam

"*KelvinSecTeam*" is a financially motivated threat actor, classified simply as a cybercriminal actor, that since 2018 sells stolen user databases from companies. Although the adversary does not follow a political agenda, it can also deeply impact ICS infrastructure, as seen in the following image:



Service Station Control / Russia / Kazakhstan (Backup SQL, Access and SCADA)
by kelvinsecurity - Thursday October 13, 2022 at 01:34 AM

October 13, 2022, 01:34 AM (This post was last modified: October 13, 2022, 01:34 AM by kelvinsecurity.) #1

Service Station Control / Russia / Kazakhstan (Backup SQL, Access and SCADA)

kelvinsecurity
GOD User
GOD

Posts:	239
Threads:	195
Joined:	Mar 2022
Reputation:	627

МД-Бонувони Точикистон	Одиназода Ш	1	2
Мактаби Футбол		1	2
Маркази татбики лоихаи Дастраси ба маблаг гузории сабз ва маблагхои рушди дехот		1	13
Маркази таъминоти бехатарии озукавори дар н,Варзоб	Рахимзода Х.Р	1	1
Миссия Восток	Тиллоев Алишер	1	3
Муассисаи давлатии "Маркази милли Точикистон оид ба масъалахои минахо"		1	1
Организация АЗС		46 1 1	105
Раёсати Молия Нохия Фирдавси		1	1
Рушди Бармахали Кудакон		1	5
Соро Ойл	Давлятов Бахриддин	1	6

Resume:

- SCADA-type Monitoring Control
- Some SQL Database Backups
- Financial Control Of The Stations
- Victims: Chechnya, Russian cities and towns, Kazakh cities, Tajikstan.

Hello, I come with some complete access and other logins with their administrator-type access credentials on control of service stations, as well as control over users who transmit payments.

Figure 5. kelvinsecurity sells credentials to access SCADA systems regarding a service station and related databases on the defunct Breached forum.

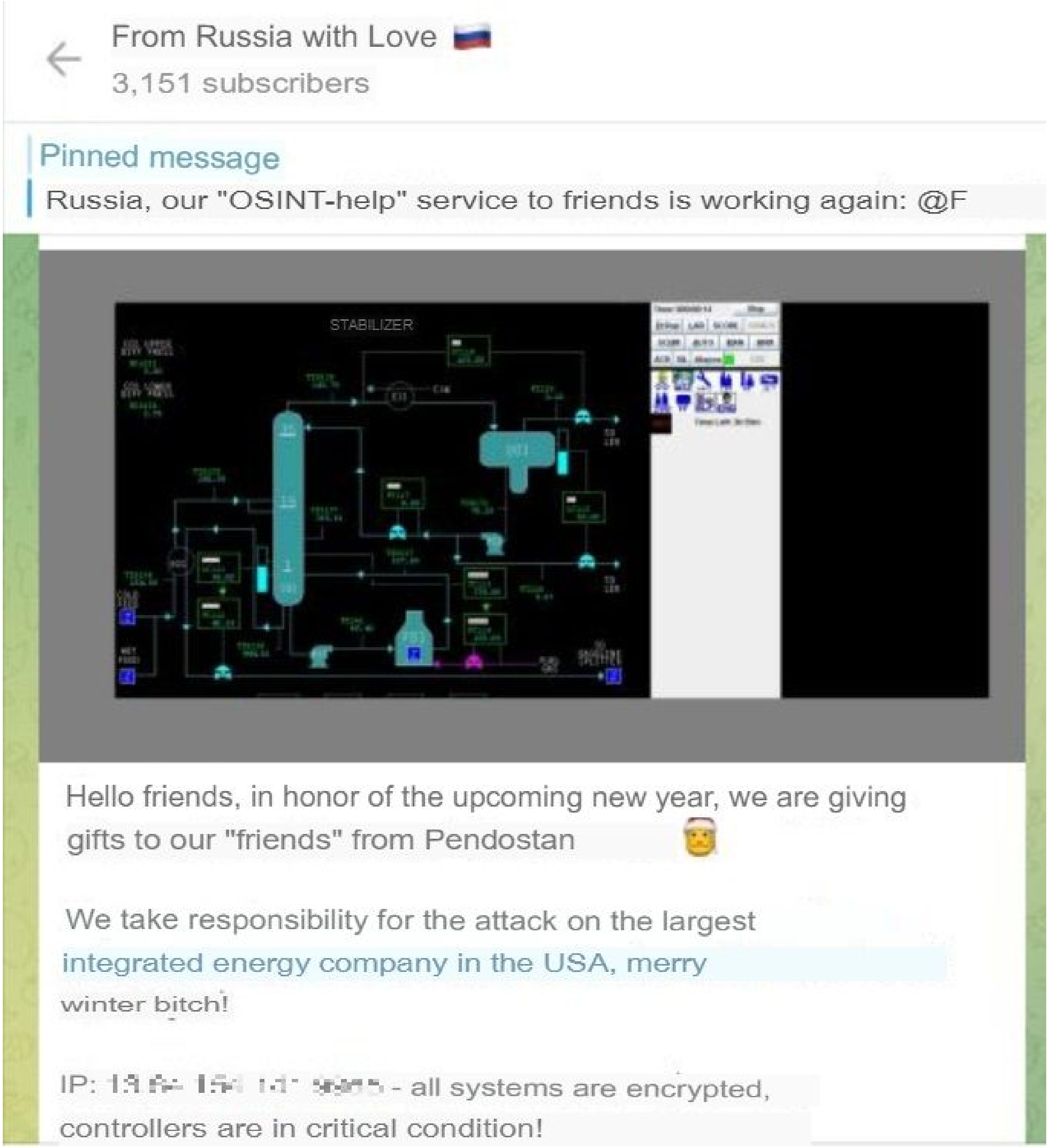
In the example above, *KelvinSecTeam* was selling access to the SCADA systems that monitor fuel stations in Russia – besides the already mentioned databases, financial control of the stations, and others. If access to these systems falls into the wrong hands, it entails great safety issues due to what a potential leak of fuel may generate – which is something that cyberterrorists would likely do, as it would cause harm. It is not clear whether this access has been sold, but as it was still available at the forum until its closure, chances are that it has not been commercialized – due to reasons ranging from high prices to a general lack of interest in the product.

From Russia with Love (FRwL)

"*From Russia with Love*" (also known as "*FRwL*") is, at first glance, a hacktivist group that emerged in the context of the Russia – Ukraine war in 2022. After a few months, the threat group started employing the Somnia ransomware against targets of interest, but it would use it as a wiper as, according to a Telegram post, "*we removed the decryption function, now the process is irreversible, and the decryption algorithm is just crazy!*".

In the context of the war, security researchers managed to establish a connection between some auto-proclaimed hacktivist groups and the Russian Main Intelligence Directorate (GRU), which makes these threat groups, at best, cyber proxies (when not directly part of the state apparatus). At the time of writing, no piece of evidence consistently can link *FRwL* to the GRU; however, it is possible that prominent state-aligned hacktivist groups active in Telegram such as *FRwL* coordinate activities at some level with the GRU – be it directly or through intermediaries.

FRwL usually leaks exfiltrated information obtained from Russia's opponents in its Telegram channels. However, on one occasion, the adversary implies having targeted SCADA systems belonging to two separate entities:



From Russia with Love 🇷🇺

3,151 subscribers

Pinned message

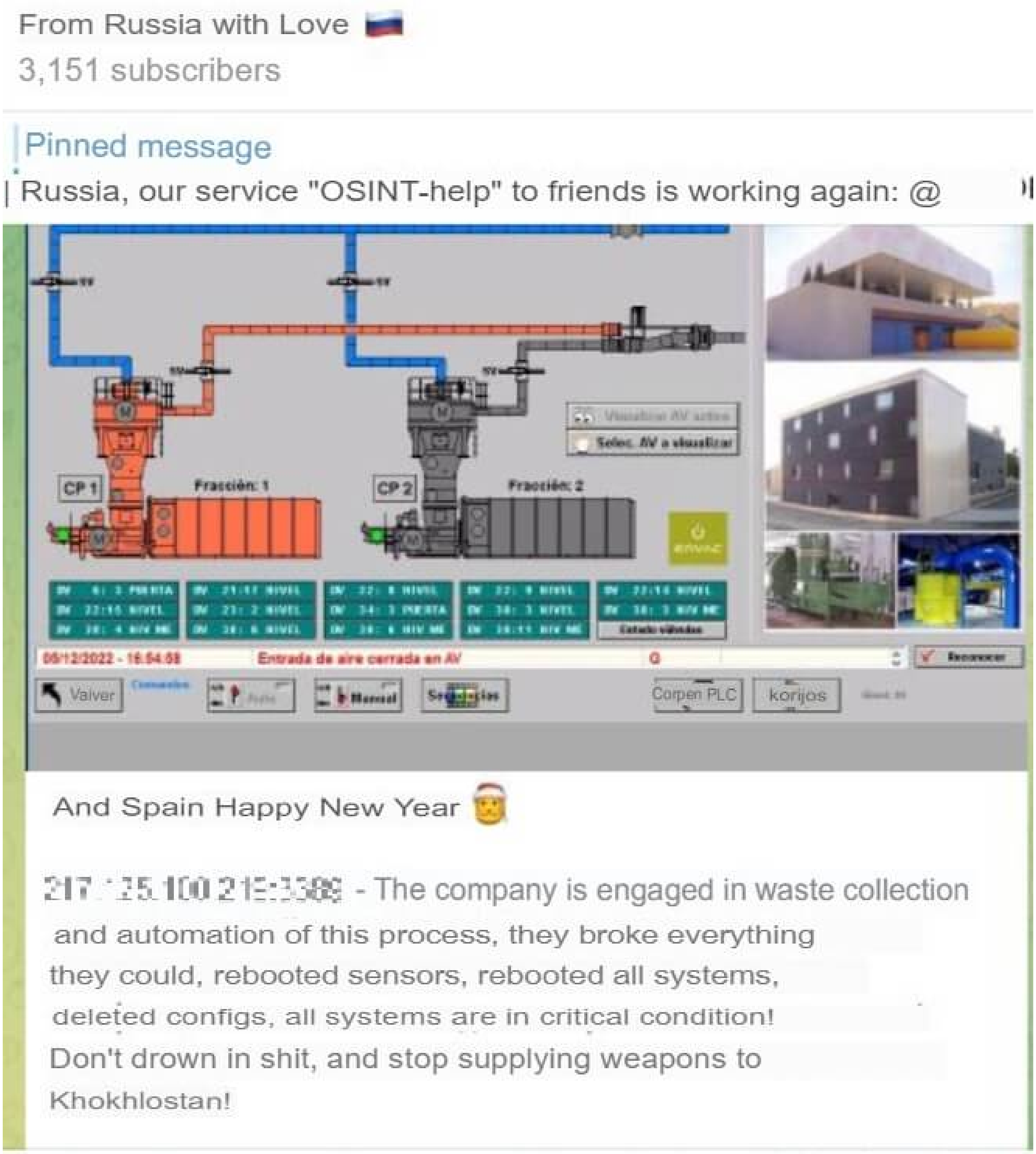
Russia, our "OSINT-help" service to friends is working again: @F

Hello friends, in honor of the upcoming new year, we are giving gifts to our "friends" from Pendostan 👳

We take responsibility for the attack on the largest integrated energy company in the USA, merry winter bitch!

IP: [redacted] - all systems are encrypted, controllers are in critical condition!

Figure 6. On December 23, 2022, FRwL shared claims of two hacks against SCADA systems: the first against Chevron/USA (automatically translated from the original in Russian).



From Russia with Love 🇷🇺
3,151 subscribers

Pinned message
| Russia, our service "OSINT-help" to friends is working again: @

And Spain Happy New Year 🤶

[redacted] - The company is engaged in waste collection and automation of this process, they broke everything they could, rebooted sensors, rebooted all systems, deleted configs, all systems are in critical condition! Don't drown in shit, and stop supplying weapons to Khokhlostan!

Figure 7. On December 23, 2022, FRwL shared claims of two hacks against SCADA systems: the second is from a waste management system in Spain – as per the shared screenshot, it is possible to infer that the company is active in Barcelona (automated translation from the original in Russian).

In the first case, illustrated by Figure 7, the system in question allegedly belongs to Chevron, a multinational energy corporation. *FRwL* claims to have encrypted all systems, which suggests that the threat group may have employed the Somnia ransomware against the target. In the second case, illustrated by Figure 8, the system in question belongs to a

Spanish waste management system. Here, the threat group claims to have messed with all the system's configurations, leaving it in critical condition. The attacks have not been confirmed by the targets, but both could have posed great danger to affected populations.

FRwL adopts an aggressive approach, and, differently from the *GhostSec* case in which the hacktivist group openly claims its intention not to cause harm, it is unclear what are the intentions of the former.

Therefore, the classification of this group is highly complex: it could be hacktivism, cyberterrorism, or even work as a cyber proxy.

Final words

As illustrated by the case studies, it is not an easy task to classify complex threat groups within the proposed taxonomy – especially one that bridges the gap between cybersecurity and International Relations. Cyberwarfare, cyberterrorism, and hacktivism are differentiated by a thin line that requires close attention to detail to tell them apart. A takeaway from these considerations is that one must cross-check the intended goal of an attack and the nature of the perpetrators to achieve a clearer vision of the potential classification of the group. This way we avoid falling into easy classifications that might disregard the true intent behind malicious actions and actors. Properly managing threat classification supports our cybersecurity understanding and preparedness as we harden our defense capabilities.

In Threat Context, the comprehensive threat intelligence module of our security solution Threat Compass, clients have access to the daily updated intelligence information about threat groups, their attack patterns, employed tools, exploited vulnerabilities, IOCs, campaigns, and more. Outpost24's KrakenLabs' researchers analyze and classify new threats daily, so clients can incorporate the latest developments and trends of the cybersecurity sphere into their business decisions.

About the Author

Beatriz Pimenta Klein Threat Intelligence Analyst, Outpost24

Beatriz Pimenta is a Threat Intelligence Analyst with the Strategic Research Team in Outpost24's KrakenLabs department. Her primary interests lie at the crossroads of cyber threat intelligence and international relations, dedicating her research time to topics that could enable conversation between the two areas.