VEDERE LABS

The Increasing Threat Posed by Hacktivist Attacks

An analysis of targeted organizations, devices and TTPs

Date: December 1, 2022

Contents

1. Executive Summary

This year has seen an enormous increase in the number and claimed impact of hacktivist attacks on critical infrastructure and enterprises operating in critical services. Many attacks target unmanaged devices such as Internet of Things (IoT) and operational technology (OT) equipment. Attacks are motivated by geopolitical or social developments across the globe, with the goal of spreading a message or causing physical disruption. Targets of such attacks include steel plants in Iran, a military vehicle repair facility in Russia, gas pumps in Israel and programmable logic controllers (PLCs) in the U.S.

These examples, and many others discussed in this report, should serve to dispel the myth that hacktivist attacks are a minor nuisance by showing how this type of threat actor has considerably expanded their arsenal.

Hacktivism has been around since the 90s, focusing traditionally on data theft or denials of service and defacement attacks against websites. To this day, many notable groups such as KillNet carry out these types of attacks. However, hacktivist groups have shown interest in critical infrastructure and internet-accessible OT for more than a decade.

This interest has taken on much greater proportions in 2022. Organizations are more connected than ever. There are thousands of highly critical devices still exposed online. Simple to moderately complex attacks are now commoditized due to the existence of public scanning and attack tools that do not require specialized knowledge. Finally, hacktivists are no longer only scanning IT devices (such as web servers) but are increasingly devoting their attention to OT devices. For instance, they are interacting with HMI and SCADA systems to change operational parameters and leveraging OT protocols to disable PLCs or write variables directly on their registers.

Organizations around the globe should look at this trend as a reminder to secure their assets using a holistic approach. Particular consideration should be given to unmanaged devices, IoT and OT. Those devices, often insecure by design, can represent an additional risk exposure, since they are not only being targeted by state actors or cybercriminal gangs but also by hacktivists. These hacktivists also share the details of their attacks on social media platforms, where they are likely to inspire new threat actors to go even further in their subsequent attacks.

In this report, we:

- **Describe two examples of active hacktivist groups**. GhostSec is a more established group that has been launching Denial of Service attacks, leaking stolen data and exploiting OT across the world to further their sociopolitical agenda. Team OneFist is a newer group exploiting several types of devices to disrupt Russian infrastructure in response to the ongoing war against Ukraine. We also mention other groups such as Gonjeshke Darande, SiegedSec, AnonGhost and NB65.
- **Present the device types, specific models and protocols these groups have targeted**. Most attacks targeted SCADA systems and PLCs, followed by networking and VoIP equipment, then uninterruptible power supplies (UPSs). Attackers show a preference for device models that are popular on targeted environments and can be fingerprinted over the internet.
- **Discuss their tactics, techniques and procedures (TTPs).** The main recent evolution in terms of TTPs for hacktivist groups has been a shift from distributed denials of service (DDoS) to targeting organizations by exploiting their unmanaged devices. These exploits include tried and trusted techniques such as defacement, data destruction and data encryption, but also an increasing number of changes to operational parameters of OT equipment via their human-machine interfaces (HMIs) and graphical user interfaces (GUIs) or specific protocols, resulting in claims of kinetic damage.
- **Explore the lessons for security practitioners.** Considering the increased scope of hacktivist attacks, cyber hygiene practices such as hardening, network segmentation and monitoring must be extended to encompass every device in an organization, not only those that are managed.

Disclaimer: all the provided attack examples and the analysis done on them are based on claims from the threat actors shared on social media. These claims are often accompanied by screenshots and data dumps that lend them some legitimacy. Nevertheless, some of the original claims may be exaggerated or untrue. Although we do

not discuss the identities of threat actors in this report, it is important to acknowledge that there is ongoing speculation that some of these groups could be composed of state actors disguised as hacktivists.

2. Relevant groups and targets

2.1. GhostSec

GhostSec, or Ghost Security, is an offshoot of Anonymous that has been active since at least 2015 and has joined many campaigns targeting institutions across the world. The group includes members from several countries, does not have a single political agenda and currently maintains a Twitter presence and a Telegram channel.

Table 1 lists the group's operations in 2022. These targets were located in Israel (to protest against the conflict with Palestine), Russia (to protest the war with Ukraine), Iran (to protest the government's treatment of women) and Nicaragua (to protest what the group saw as rigged elections). **Organizations attacked were in industries as diverse as retail, telecom, hotels and utilities**. Devices identified in these attacks include SCADA, HVAC controllers, energy measurement and several PLCs. These devices were attacked either via their internet-accessible HMI or by directly interacting with insecure protocols such as Modbus using custom-built scripts and publicly accessible Metasploit modules.

Table 1 – GhostSec targets

#	Date with link to reference	Targeted organizations (industry vertical)	Country	Devices identified in the attack	Actions identified on device
1	Mar 11	ASF-group.ru (Retail)	Russia	Pult.online SCADA	Change parameters via HMI/GUI
2	Jun 30	partner.co.il and MATAM industrial (Telecom)	Israel	SuperBrain Direct Digital Controller (HVAC)	Change parameters via HMI/GUI
3	Jul 6	Several (Several)	Israel	Phoenix Contact EEM-MA770 (energy measurement)	Change parameters via HMI/GUI
4	Jul 7	Or Akiva Pump Station (Utilities)	Israel	Unknown	Unknown
5	Jul 20	Gysinoozerskaya Hydro-Power Plant (Utilities)	Russia	Unknown	Use a custom script (KillBus) to rewrite modbus registers
6	Aug 23	UFINET (Telecom)	Nicaragua	Schneider Electric BMX P34 2020 v2.5 (PLC)	Use a custom script (theComposer.py) to set Modbus registers to 0
7	Sep 4	Several (Several)	Israel	Berghof DC2004 PLCs	Exfiltrate data via HMI/GUI

8	Sep 10	Hotels (Travel & Tourism)	Israel	ProMinent AEGIS II controller	Change parameters via HMI/GUI
9	Oct 3	Mobinnet, ITC, Asiatech, Khalij-Fars-Online, Fanap Telecom, Sabanet (Telecom)	Iran	MOXA E2214 and Rockwell PLCs	Use Metasploit Multi CIP module to issue STOPCPU commands and custom script (Modbus.py) to set Modbus registers to 0

2.2. Team OneFist

Team OneFist was founded in March 2022 by a group of international hacktivists from Ukraine, the U.S., Poland, Spain, Syria, Austria, Sweden and Germany. They are a pro-Ukrainian group and work in close collaboration with other similarly aligned groups, such as the IT Army of Ukraine. They maintain a presence on Twitter, with mainly two members who are very active: Voltage and Thraxman. The group also recently published a website and they are much more active than GhostSec, posting about new operations almost daily.

Table 2 lists some of Team OneFist's operations involving unmanaged devices in 2022. All their targets were located in Russia, since the team's main motivation is opposition to the ongoing war. The attacks focused on infrastructure organizations, especially in sectors such as telecommunications, utilities and manufacturing, with the goal of denying availability of services or causing physical destruction. The group showed a preference for specific internet-accessible device types such as UPS, SCADA, network routers and VoIP equipment. Some more distinctive device types were also attacked such as cinema projectors, a remote access gateway for ham radio and several modems for satellite communications. Their actions are somewhat different from GhostSec's: besides changing parameters via the HMI/GUI, TeamOneFist also deface these HMIs with pro-Ukrainian and anti-Russian messages, and they often wipe data on embedded devices via operating system commands. They do not seem to favor the use of OT-specific protocols such as Modbus.

Table 2 – Team OneFist targets

#	Date with link to reference	Targeted organizations (industry vertical)	Country	Devices identified in the attack	Actions identified on device
1	Jul 26	Electrical control systems in several cities (Utilities)	Russia	Unknown	Delete data on the device
2	Jul 31	RST cargo railway (Transportation)	Russia	Data center network switch	Change parameters via HMI/GUI
3	Aug 1	VoIP infrastructure in several cities (Telecom)	Russia	ELTEX SMG-1016M (VoIP router)	Unknown
4	Aug 4	SCADA in several cities (Several)	Russia	TELEOFIS 4G RTUs	Unknown

#	Date with link to reference	Targeted organizations (industry vertical)	Country	Devices identified in the attack	Actions identified on device
5	Aug 12	Electricity distribution operators in several cities (Utilities)	Russia	ADDAX transformer data collectors	Unknown
6	Aug 14	Power system substation PS-249 (Utilities)	Russia	UPSs	Change parameters via HMI/GUI
7	Aug 16	KUPROS paper mill (Manufacturing)	Russia	OpenSCADA	Change parameters via HMI/GUI
8	Aug 22	Khanty-Mansiysk city natural gas system (Utilities)	Russia	OpenSCADA	Change parameters via HMI/GUI
9	Aug 30	Sewer stations (Utilities)	Russia	TEKON SCADA	Unknown
10	Aug 31	Chicken farm (Agriculture)	Russia	OpenSCADA	Defacement
11	Sep 1	Several (Telecom and Utilities)	Russia	OpenSCADA, Tenda routers, ELTEX VoIP routers	Unknown
12	Sep 3	Several (Several)	Russia	iRZ RL01 industrial router	Delete data on the device
13	Sep 5	Factory in Crimea (Manufacturing)	Russia	WAGO Modbus controllers, Weintek cMT-SVR-100 controllers	Change parameters via HMI/GUI
14	Sep 7	Passage shopping mall (Retail)	Russia	SNR-ERD 4 router, Incotex Mercury 225 data concentrators, NAGRUZKA SCADA, MOXA controllers	Change parameters via HMI/GUI
15	Sep 15	Ham radio operator (Telecom)	Russia	Remoterig RRC-1258MkII (Remote access interface for ham radio)	Unknown
16	Sep 17	Metallurgical plant in Satka (Manufacturing)	Russia	Schneider Electric Smart-UPS SRT 10000	Change parameters via HMI/GUI

#	Date with link to reference	Targeted organizations (industry vertical)	Country	Devices identified in the attack	Actions identified on device
17	Sep 22	VoIP system for city of Udmurtia (Telecom)	Russia	Eltex SMG2016 PBX	Change parameters via HMI/GUI
18	Sep 26	Netbynet and Prov.ru ISPs (Telecom)	Russia	Extreme Networks routers	Unknown
19	Sep 26	Several (Several)	Russia	Schneider Electric Smart-UPS, Teradata UPS-ATS 3000 RM XL	Change parameters via HMI/GUI
20	Sep 26	ISPs (Telecom)	Russia	Network routers (ZTE, Zyxel, Upvel, Tenda, TP-Link, Technicolor), VoIP phones, Vigintos RT-FMS-251 RF transmitter	Unknown
21	Oct 3	ISPs and government agencies (Telecom and Government)	Russia	Network routers (ddwrt, Extreme Networks, Netis, Tenda, D-Link, TP-Link), ELTEX VoIP routers	Change parameters via HMI/GUI
22	Oct 6	Cinemas (Entertainment)	Russia	BARCO DP2K-20C cinema projector	Change parameters via HMI/GUI
23	Oct 10	Megafon (Telecom)	Russia	NovelSat NS3000 satellite modems	Change parameters via HMI/GUI
24	Oct 10	ISPs (Telecom)	Russia	Network routers (D-Link, Tenda TRENDnet, Upvel, ASUS, Cisco, Extreme Networks), IP cameras, DVRs, ELTEX VoIP switches	Unknown

2.3. Other groups

Many other hacktivist groups have hacked OT and IoT targets in 2022. Examples include:

- Gonjeshke Darande, also known as Indra or Predatory Sparrow. On June 27, the group attacked three Iranian steel plants and released a video that shows a fire breaking out at the facility as the claimed result of the attack. This group has been active since at least 2021, when they attacked the Iranian railways, causing train delays and cancellations, and the Ministry of Roads and Urban Development, causing the national fuel payment system to go offline. Due to the sophistication of their attacks, some researchers

believe the group is a state-sponsored, possibly military, organization disguising their true motivations as hacktivism.

- SiegedSec attacked Rockwell PLCs in the U.S. using the Metasploit Multi CIP module as part of #OpJane, a hacktivist operation against the overturning of the federal right to abortion in the U.S. The group is closely related to GhostSec, with one well-known member, "YourAnonWolf," claiming to be in both groups.
- AnonGhost, another group protesting the war in Ukraine, hacked Russian devices such as street lighting systems, Moxa OnCell Ethernet IP gateways, satellite interfaces for navigation systems, SCADA systems at power stations, IP cameras and printers.
- Network Battalion 65 (NB65) is yet another group that targeted Russia. Some of their operations include hacks on IP cameras and several open SCADA systems. Beyond attacks on critical infrastructure, NB65 has been very active in leaking sensitive files from Russian targets and even using the leaked Conti ransomware against several companies.
- Anonymous, one of the oldest and most well-known hacktivist collectives still active, targeted Russian IoT equipment soon after the invasion of Ukraine. Examples include hacked printers mass printing Tor installation instructions and IP cameras hacked to show live video feeds of Russian military personnel.

3. Analysis

3.1. Organizations and devices targeted

In some cases, hacktivist groups choose to attack a specific organization, often repeatedly, due to their value as a target. This is the case of Team OneFist attacking Rostelecom on multiple occasions, since Rostelecom is Russia's largest ISP. In most cases, however, these attacks are opportunistic, focusing on a country and sometimes a sector, such as telecommunications, rather than on a specific organization. Once the initial target scope is defined, some groups focus on large-scale attacks by finding similar device models in several organizations and attacking them at the same time.

As shown in Figure 1 (based on data from Table 1 and Table 2), threat actors have been targeting unmanaged devices in organizations not only in traditionally OT-heavy industries such as utilities and manufacturing but even more so in unexpected industries such as telecommunications and retail. **This is possible because of the widespread use of IoT and OT equipment – such as UPS, VoIP, building automation controllers and energy measurement devices – in almost every industry nowadays.** Organizations that are not typically considered critical infrastructure rely on much of the same equipment but may have less knowledge or fewer regulatory obligations to protect those devices.

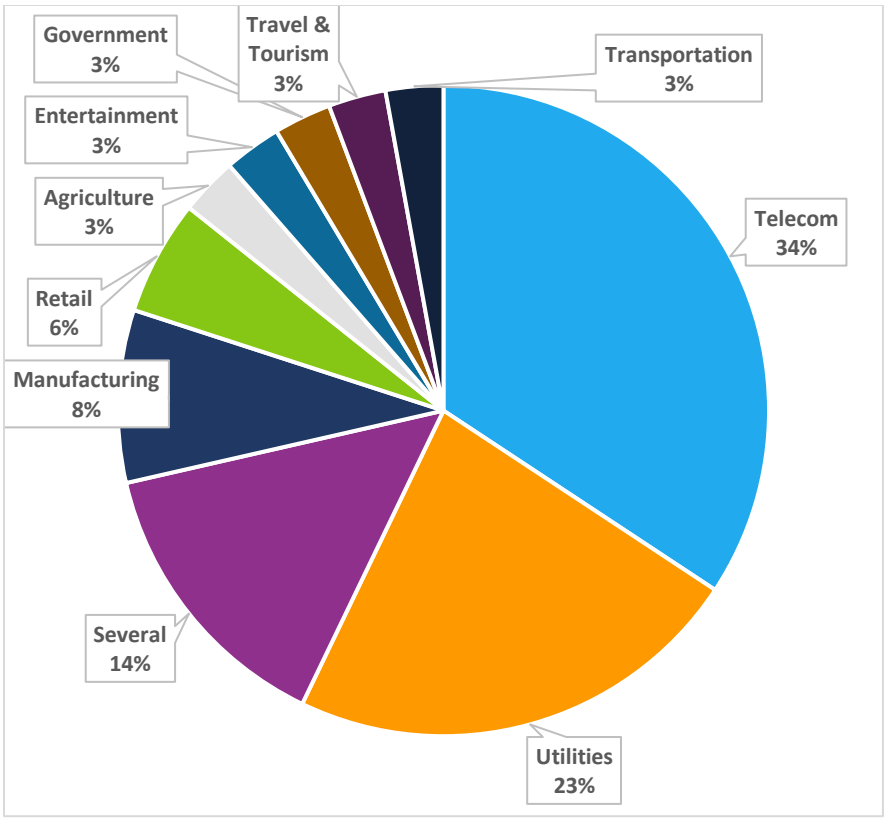

Figure 1 – Most targeted industries

Within these organizations, the most targeted devices are shown in Figure 2. The most popular were SCADA systems and PLCs, followed by networking and VoIP equipment, then UPSs. Attackers showed a preference for device models that are popular in targeted environments and can be fingerprinted over the internet. They seem to attack the same device models repeatedly, including ELTEX VoIP equipment, Schneider Electric UPSs and openSCADA systems.

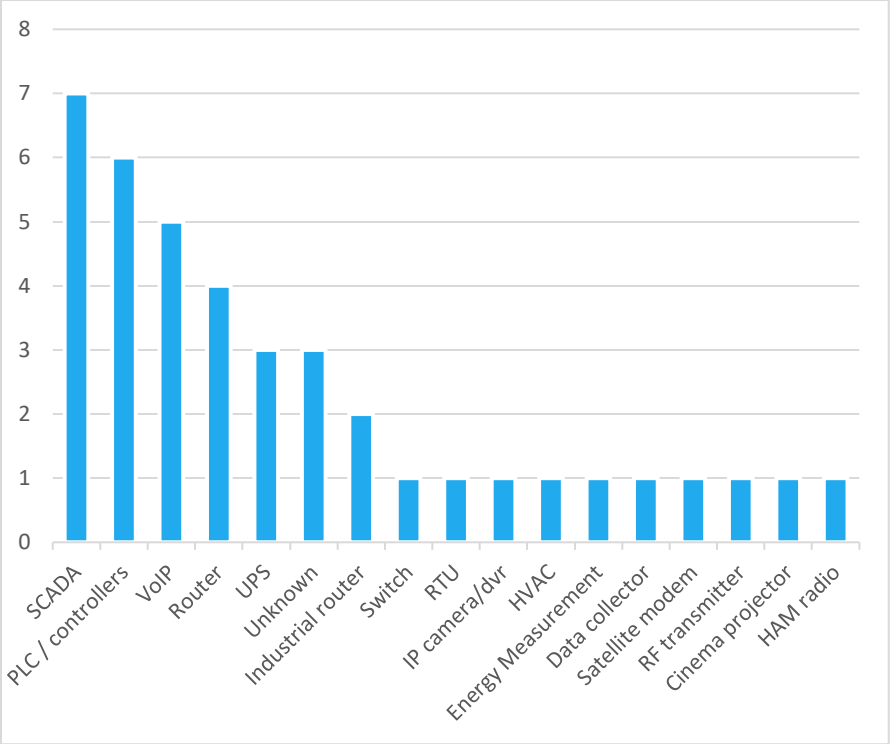

Figure 2 – Most targeted devices

3.2. Tactics, techniques and procedures

Most hacktivist groups practice division of labor, where some members define the scope of targets, others find targets by using open-source intelligence and search engines such as Shodan, others perform the actual attacks, and still others publicize operations by managing communications on channels such as Twitter, Telegram and websites.

As discussed in the executive summary of this report, the main recent evolution in terms of TTPs for hacktivist groups has been a shift from DDoS to damaging targeted organizations by exploiting their unmanaged devices. Figure 3 shows an example of GhostSec sharing target IP addresses and inviting their members or sympathizers to "leave DDoS as a last resort."

Figure 3 – GhostSec inviting attackers to "not simply DDoS"

Table 3 details the TTPs observed by the groups we reported, giving specific examples of procedures. Some techniques, such as Automated Exfiltration, are not in the table because they were not directly observed in the

groups' communications, but it is safe to assume that they are performed. Since these attacks mainly focus on internet-accessible unmanaged devices and are not prolonged campaigns that aim to remain undiscovered – as is the case with advanced persistent threats (APTs) – several tactics are either unnecessary or rarely executed, such as Persistence, Privilege Escalation and Defense Evasion.

Table 3 – Observed TTPs

Tactic	Technique	Procedure examples
TA0043 – Reconnaissance	T1595 – Active Scanning	Most hacktivist groups use publicly available tools such as Shodan, Censys and Kamerka to discover exposed devices in targeted countries.
TA0042 – Resource Development	T1584 – Compromise Infrastructure	There are a few examples of victim infrastructure being compromised, such as BGP poisoning by Team OneFist and changing DNS servers by NB65.
TA0001 – Initial Access	T1078 – Valid Accounts	Team OneFist mentions several devices such as routers and IP cameras that are compromised via either default or weak credentials.
	T1190 – Exploit Public-Facing Application	Team OneFist mentions known vulnerabilities being used to gain access to exposed routers.
TA0002 – Execution	T0823 – Graphical User Interface	Team OneFist changing battery voltages via the GUI of a UPS.
	T1059.004 – Command and Scripting Interpreter: Unix Shell	Team OneFist executing their "Orc Mind Harvester" tool for data collection.
TA0009 – Collection	T1119 – Automated Collection	Orc Mind Harvester tool developed by Team OneFist to read passwords and data from compromised routers.
	T1005 – Data from local system	Orc Mind Harvester tool developed by Team OneFist to read passwords and data from compromised routers.
TA0040 – Impact (Enterprise)	T1491 – Defacement	Team OneFist defacing an openSCADA instance to display the group's name and logo.
	T1485 – Data Destruction	Team OneFist deleting data from compromised industrial routers.
	T1486 – Data Encrypted for Impact	NB65 using Conti ransomware against victims.
TA0107 – Inhibit Response Function	T0816 – Device Restart/Shutdown	GhostSec issuing STOPCPU commands to Rockwell PLCs.

TA0106 – Impair Process Control	T0806 – Modify Parameter	GhostSec changing the parameters of pool controllers in Israel via their HMI.
TA0105 – Impact (ICS)	T0882 – Theft of operational information	GhostSec leaking data dumped from Berghoff PLCs they hacked.
	T0831 – Manipulation of Control	GhostSec writing 0 to all Modbus registers of a Schneider Electric PLC.
	T0828 – Loss of Productivity and Revenue	See below.
	T0879 – Damage to property	See below.

There are several examples of claims of hacktivist attacks causing T0828 – Loss of Productivity and Revenue and T0879 – Damage to property, such as the ones in Figure 4 and Figure 5. The veracity of those claims is very hard to ascertain. Even when attacks happen, often industrial facilities have safeguards – such as control logic with sanity checks on parameter values, safety instrumented systems and interlocking – that prevent catastrophic effects from happening due to malicious interaction with industrial equipment. In other cases, the malicious interaction itself may be immediately overwritten by a legitimate transmitter writing to the same variable that was just modified by the attackers.

Figure 4 – GhostSec claiming responsibility for a fire at a Russian power station

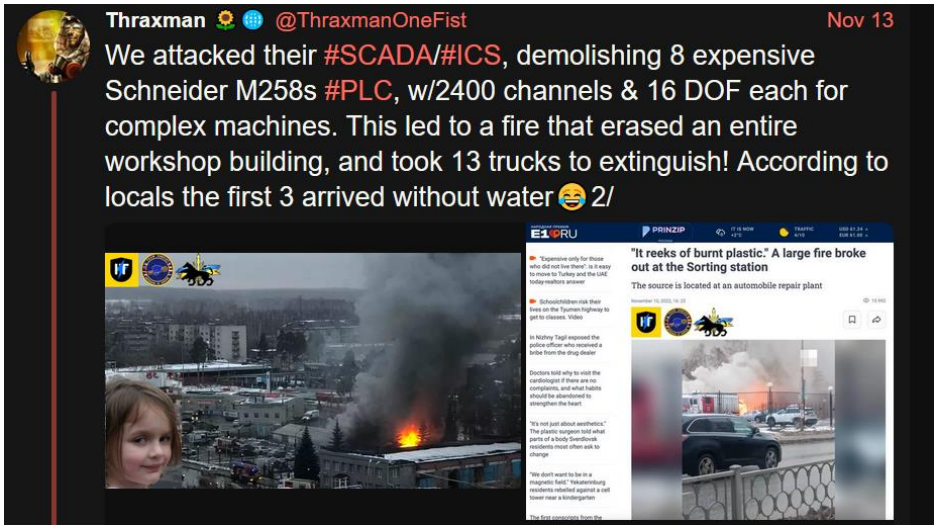

Figure 5 – Team OneFist claiming responsibility for a fire at a military vehicle repair facility in Russia

The most common techniques observed directly on the incidents reported in Table 1 and Table 2 are shown in Figure 6. The vast majority of the incidents (79%) achieved impact via T0831 – Manipulation of Control, which in turn was realized by modifying parameters via the HMI/GUI (in 85% of the cases) or via Modbus (in the remaining 15% of cases).

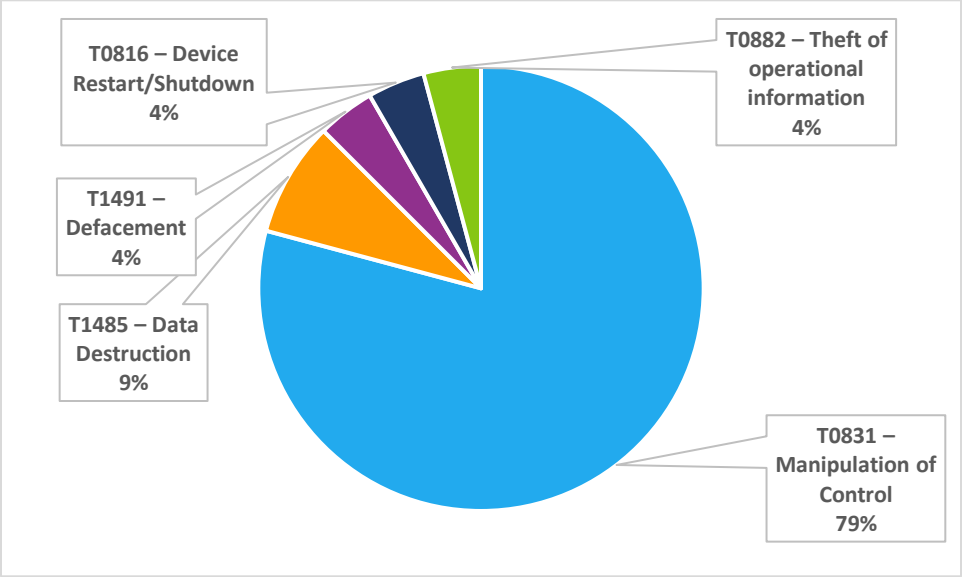

Figure 6 – Most observed techniques

4. Mitigation Recommendations

Considering the increased scope of hacktivist attacks, cyber hygiene practices such as hardening, network segmentation and monitoring must be extended to encompass every device in an organization, not only those that are managed.

- **Harden connected devices.** Start by identifying every device connected to the network and its compliance state and enumerating known vulnerabilities, used credentials and open ports. Change default or easily guessable credentials and use strong unique passwords for each device. Disable unused

services and patch vulnerabilities to prevent exploitation. The following recommendations are specific to the TTPs we reported:
    - Add authentication to administrative interfaces of IoT and OT devices, such as web UIs and proprietary engineering ports.
    - Enable IP-based access control lists on OT protocols such as Modbus.
    - Use secure PLC programming practices to ensure that PLC logic performs sanity checks on mapped variables.
- **Segmentation.** Do not expose unmanaged devices directly to the internet, with very few exceptions such as routers and firewalls. Follow CISA's guidance on providing remote access for industrial control systems. Segment the network to isolate IT, IoT and OT devices, limiting network connections to only specifically allowed management and engineering workstations or among unmanaged devices that need to communicate. The following recommendation is specific to the TTPs we reported:
    - Ensure administrative interfaces (such as web UIs and engineering ports) on connected devices are behind IP-based access control lists or are only accessible from a separate, VPN-protected management VLAN.
- **Monitoring.** Use an IoT/OT-aware, DPI-capable monitoring solution to alert on malicious indicators and behaviors, watching internal systems and communications for known hostile actions such as vulnerability exploitation, password guessing and unauthorized use of OT protocols. Monitor large data transfers to prevent or mitigate data exfiltration. Finally, consider monitoring the activity of hacktivist groups on Telegram, Twitter and other sources where attacks are planned and coordinated. The following recommendations are specific to the TTPs we reported:
    - Integrate OT device health monitoring into your alerting system. Unavailability of network links or sudden changes in status indicator variables (such as PLC operating mode or project checksum) could be indicators of malicious activity.
    - Ensure proper incident playbooks are available and understood throughout your organization and regularly tested in IR simulations. Possible cyberattack-related causes should be monitored and playbooks updated as part of responding to operational incidents.

5. References

- https://cyberint.com/blog/research/ghostsec-raising-the-bar/
- https://blog.cyble.com/2022/07/25/global-hacktivism-on-the-rise/
- https://research.checkpoint.com/2022/the-new-era-of-hacktivism/
- https://www.darkowl.com/blog-content/developing-impacts-of-ukraine-invasion-felt-across-the-darknet/
- https://www.securityweek.com/hacktivist-attacks-show-ease-hacking-industrial-control-systems