



# TEAM82

# Analyzing CPS Attack Trends

Opportunistic attackers are leveraging  
CPS assets to amplify political and social causes.

By Team82

## Table of Contents

|                                                  |           |
|--------------------------------------------------|-----------|
| <b>Introduction</b>                              | <b>3</b>  |
| Key Findings                                     | 5         |
| <b>Methodology</b>                               | <b>8</b>  |
| Research Limitations                             | 9         |
| <b>Ideological Sympathies Define CPS Attacks</b> | <b>10</b> |
| Geographic Origins of the Threat                 | 10        |
| Trends in Regionalized Targeting                 | 11        |
| <b>Exploring the Anatomy of CPS Attacks</b>      | <b>14</b> |
| <b>CPS Asset Selection</b>                       | <b>17</b> |
| <b>Takeaways</b>                                 | <b>20</b> |
| Secure Internet-Facing CPS                       | 20        |
| Remedy Insecure by Design/Default                | 21        |
| Know Your Adversary                              | 22        |
| <b>About Claroty</b>                             | <b>23</b> |
| <b>About Team82</b>                              | <b>23</b> |



## Introduction

Geopolitical tensions are spilling into cyberspace, and Team82's latest research shows that cyber-physical systems (CPS) are increasingly becoming a preferred target of opportunistic threat actors. These groups are often inspired politically and socially by geopolitical events, yet may not be as skilled as their nation-state counterparts. Their aim is to disrupt critical infrastructure and the services vital to the way of life for people caught in the crossfire, while simultaneously calling attention to their political and social causes.

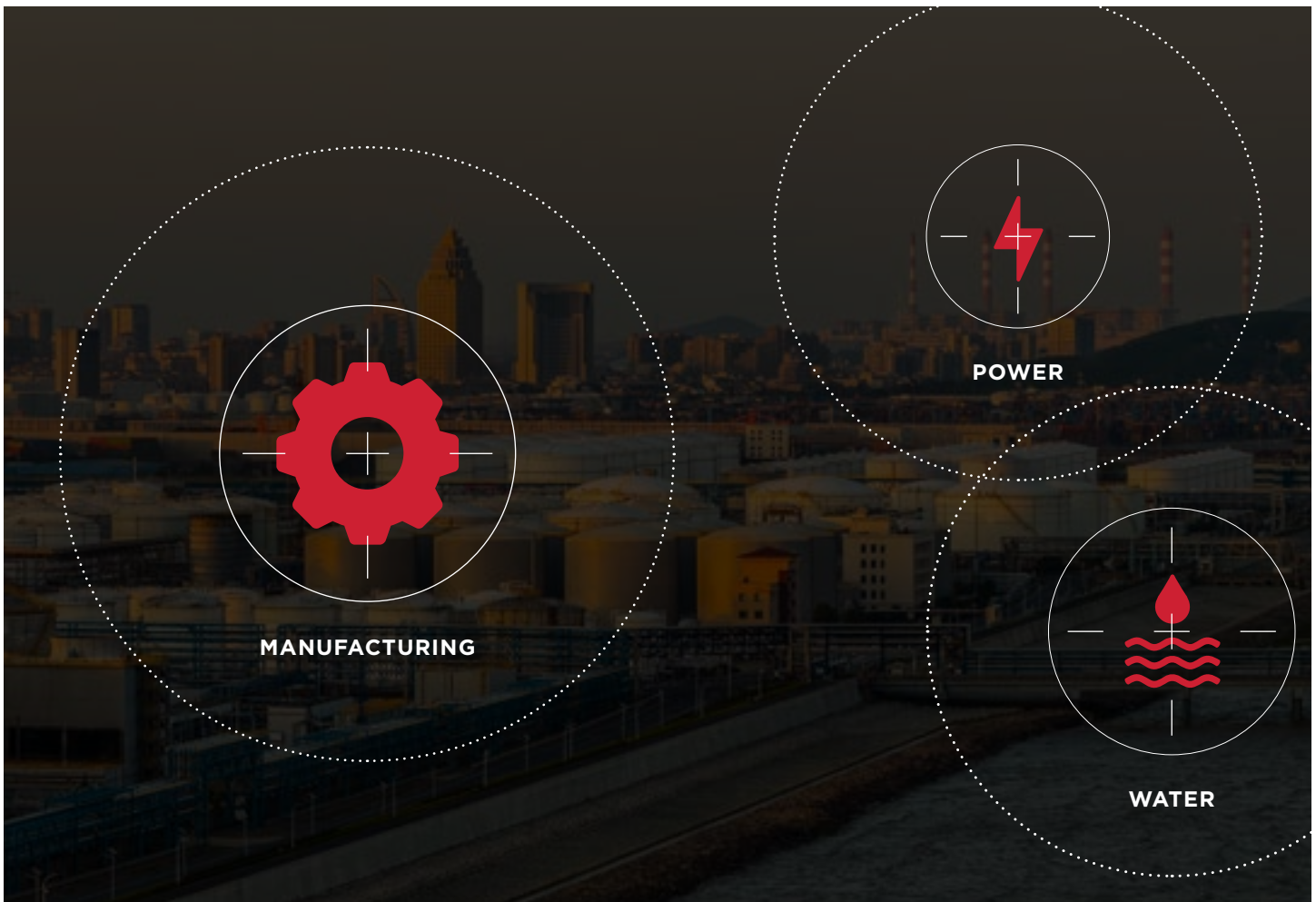
In this report, Team82 will share its research evaluating 200-plus attacks carried out by more than 20 such threat-actor groups against CPS in numerous industries, with a high concentration of these attacks impacting manufacturing, water and wastewater, and power-generation—sectors that represent enormous capital for a hacktivist entity intent on disrupting resources and sowing chaos in society.

Our research also shows that many of these incidents are regionalized and aligned with geopolitical ideologies. For example, tensions in the Middle East are pitting hacktivist groups against U.S.- and Israel-based interests, while Russia's ongoing war in Ukraine has motivated threat actors aligned with Russia's cause to target victims in Europe and other NATO allies. (The data represented here was collected before the Iran war began on Feb. 28 and does not reflect recent activity.)

Attackers are also shifting strategically, moving away from targeted attacks against specific entities, and instead are routinely selecting classes of internet-facing CPS devices to compromise at scale. A large number of these cyberattacks do not involve expensive-to-develop exploits or intimate knowledge of the inner workings of operational technology (OT), for example. Instead, attackers are finding success against CPS assets by using decidedly low-tech means of accessing devices that are guarded often by weak or default credentials, or an insecure connection to the internet.

Threat actors are also exploiting weaknesses in longstanding OT and internet of things (IoT) protocols that lack authentication, encryption, and other basic security capabilities. The barrier to entry is low for these groups who are successfully accessing and controlling CPS at scale.

This report represents a sample of collated threat intelligence by Team82 that sheds light on real risks to CPS from these groups and calls on critical infrastructure organizations to understand the commodity threats they face and the capabilities of groups targeting them.



## Key Findings

From our research, we identified the following key findings that defenders may use to shape their CPS protection strategies.

### A Shift to Opportunistic Attacks

In December 2025, the Cybersecurity & Infrastructure Security Agency (CISA) published an advisory warning of a [rise in opportunistic attacks](#) against U.S.-based critical infrastructure. The advisory singles out unprotected internet-facing OT assets, insecure access to devices, and a lack of authentication as major risks enabling this malicious activity.

Our research bears this out with a large majority of incidents having started with decidedly low-tech tactics, techniques, and procedures (TTPs) that don't require an exploited vulnerability or extensive knowledge of the devices or protocols being targeted.

Instead, hacktivist groups that are sympathetic to adversarial nation states are hurdling low barriers to

access and compromise CPS. They're primarily doing so by abusing virtual network computing (VNC) clients to remotely access exposed and internet-facing CPS. The VNC protocol and other insecure OT communication protocols such as Modbus are primary attack vectors identified in our research. Devices that speak Modbus, a common OT protocol that lacks security capabilities by default, are often accessed using VNC clients over the VNC protocol. This combination makes them easily enumerated and vulnerable to attacks that could negatively impact physical processes.

Meanwhile, human-machine interface (HMI) and supervisory control and data acquisition (SCADA) systems are far-and-away the most targeted CPS assets in the crosshairs of adversaries. Since both device classes oversee industrial processes in real time, any disruption to these systems or manipulation of the information they monitor can be consequential.



**82%**

Of attacks against CPS involve using VNC clients to remotely access exposed, internet-facing assets



**66%**

Of incidents include the compromise of HMI/SCADA systems that control industrial processes

Our research also shows attackers shifting away from targeted attacks against specific organizations, and instead are targeting classes of CPS assets that are internet-facing. Largely, threat actors are accessing CPS assets that are exposed in countries or regions that meet their politically or socially motivated goals, attacking almost aimlessly at assets rather than organizations.

### Politically Motivated

Of the more than 200 attacks against CPS that Team82 verified, we were able to align many of the incidents to Russia- and Iran-affiliated threat actors. Unsurprisingly, given the current geopolitical tensions in the Middle East and the four-year-old war between Russia and Ukraine, we identified most attacks originating from Russian-speaking groups as targeting European Union countries, while Iran-affiliated groups largely attempted to leverage CPS in attacks against Israel and the United States.



**Note:** the data represented in this report was collected between January and December 2025, before the Iran war began on Feb. 28; it does not reflect any cyber-related events related to this conflict.



**81%**

Of incidents carried out by Iran-affiliated groups were against U.S. and Israel targets



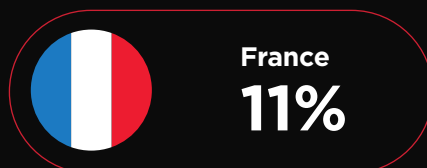
**71%**

Of incidents carried out by Russia-affiliated groups were against EU countries

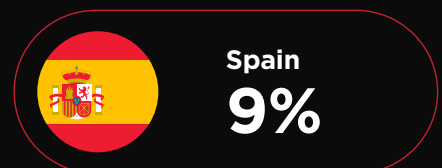
### Most Targeted Countries by Russia-affiliated groups



Italy  
**18%**



France  
**11%**



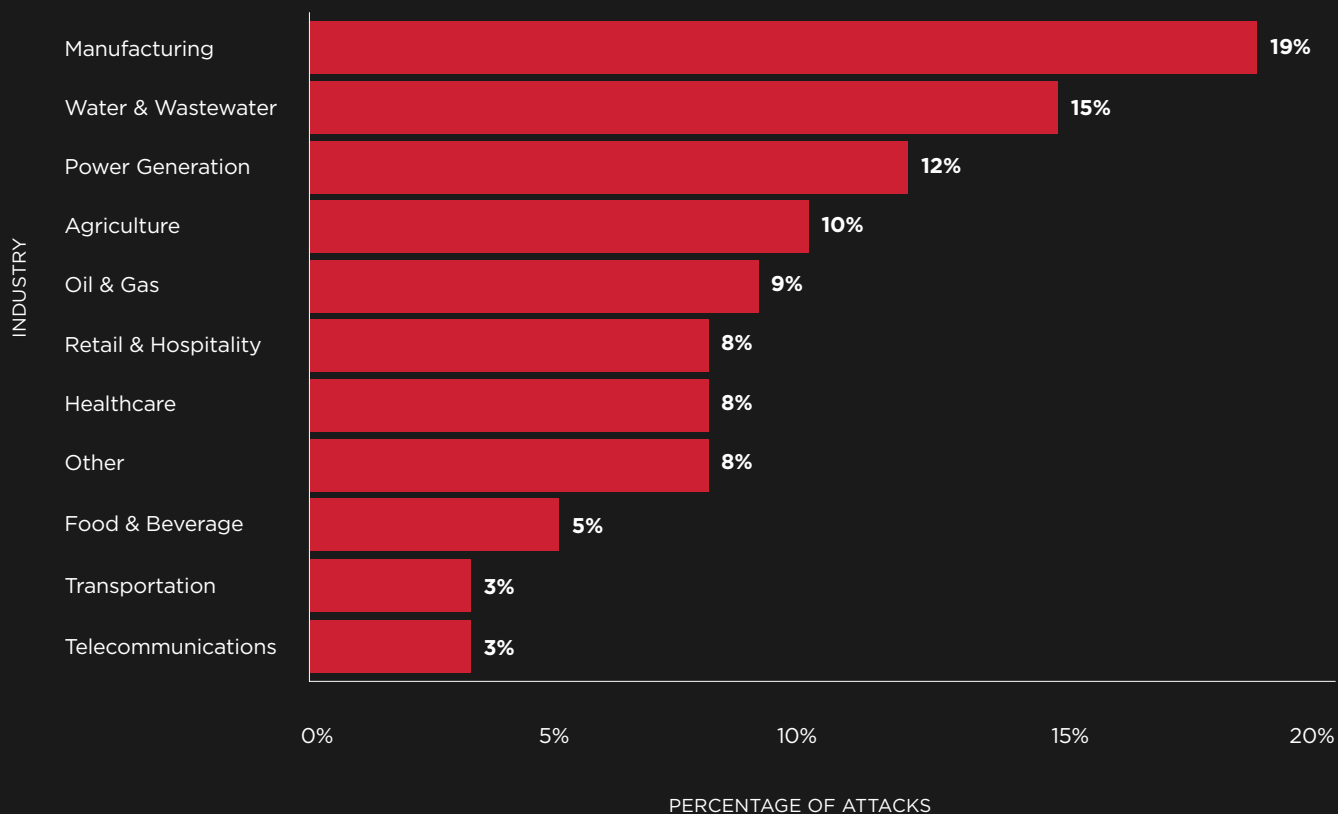
Spain  
**9%**

## Targeted Industries

Manufacturing, water and wastewater, and power generation—critical infrastructure sectors that if disrupted or damaged could instill the most chaos and fear in societies—are the most targeted sectors we observed. These three account for more than 45% of the attacks we observed in the 20 sectors where we recorded and verified incidents involving CPS assets.

**Manufacturing****19%****Water & Wastewater****15%****Power Generation****12%**

### Targeted Industries





## Methodology

To provide a comprehensive view of the evolving threat landscape regarding hacktivist-driven attacks in the CPS domain, we employed a multi-layered research methodology. Unlike highly targeted, bespoke campaigns, these drive-by incidents are characterized by opportunistic actors scanning the internet for exposed assets to amplify their political message or social cause. Our process was designed to filter out the “noise” of general cybercrime and focus specifically on verified incidents targeting CPS.

The research was conducted over a 12-month period—January to December 2025—and followed a four-stage pipeline: Source Mapping, Continuous Monitoring, Verification, and Attack Analysis.

**1**

### Source Mapping

The foundation of our research involved identifying and vetting relevant intelligence sources, primarily utilizing open source intelligence (OSINT) frameworks. We focused on a diverse array of digital environments to ensure a wide collection of threat actor activity:

- **Open Web:** Monitoring social media platforms (e.g., X).
- **Deep & Dark Web:** Monitoring threat actor indications on deep and dark web forums.
- **Encrypted Communication Channels:** Monitoring Telegram groups and channels frequently used by hacktivists and state-affiliated groups to claim responsibility for attacks and broadcast their political agendas.

**2**

### Monitoring & Collection

Once our sources were finalized, we began a continuous monitoring phase. We specifically looked for indicators of CPS-related incidents. Our focus remained on actors targeting:

- Internet-facing CPS devices (e.g., PLCs, HMIs, SCADA systems).
- OT protocols (e.g., Modbus).
- Critical infrastructure sectors as [defined by CISA](#).

## 3

### Verification

Because many of the attacks were self-reported by the threat actors, a thorough verification process was essential to ensure the credibility of our dataset. Every reported incident underwent the following verifications:

- **Actor Validation:** Assessing the history and credibility of the threat group.
- **Evidence Review:** Analyzing shared evidence and claims made by attackers, such as videos from the attacks or screenshots provided by the threat actors.
- **Noise Reduction:** We discarded any claims that could not be verified or were determined to be unrelated to CPS. This ensured our final dataset was accurate and focused.

## 4

### Attack Analysis

In the final phase, each verified attack was enriched with granular data points to identify patterns and strategic shifts. We analyzed each record across several dimensions:

- **Geopolitical Context:** Identifying the origin country of the threat actor (and any other hacktivist groups' affiliations) and the origin country of the victim.
- **Victim Profiling:** Categorizing the specific sector and identifying the targeted entity.
- **Technical Vector:** Determining their means of access (e.g., VNC, web-based interfaces), the device type, and, in some cases, the specific targeted product.

## Research Limitations

The following limitations should be considered:

- **Sample Representation:** This dataset represents a significant sample of 200-plus attacks; however, it is not intended to be an exhaustive catalog of every CPS attack occurring worldwide during this period. Many incidents go unreported or reported beyond the reach of external monitoring.
- **Source Subjectivity:** The primary data is derived from claims made by the threat actors themselves. Such reporting is inherently prone to bias because actors may exaggerate the scale or comprehensive nature of an attack to heighten the perceived impact of their social or political cause.
- **Data Validation:** To mitigate potential bias, we subjected every incident to a verification process. While we have analyzed each attack and removed those that were invalid or unverified; the initial reporting remains filtered through the evidence shared by the actors.

## Ideological Sympathies Define CPS Attacks

The modern geopolitical landscape is characterized by a “trickle-down” effect, where high-level state tensions empower low-skilled hacktivist collectives to strike at the heart of daily life: power, water, and manufacturing. Our analysis of 200-plus verified attacks shows a clear divide between two primary ideological blocs, the Soviet/Russian-aligned groups and the Arab/Iranian-aligned groups, each following a distinct strategic roadmap.

### Geographic Origins of the Threat

While threat actors often use deceptive names or self-identify with certain regions, forensic and intelligence mapping reveals that the majority of these attacks originate from specific geopolitical hubs:

- **The Soviet/Russian Bloc:** Dominating the dataset are groups like NoName057(16), Z-Pentest (Z-ALLIANCE), and SECTOR16. While some initial reports suggested Serbian origins, these groups are confirmed Russian entities, often operating as “volunteer” arms of state-aligned campaigns against NATO. Z-Pentest was notably formed by admins from Cyber Army of Russia Reborn (CARR) and NoName057(16) to target Western infrastructure.
- **The Arab/Iranian Bloc:** These groups focus on “OpIsrael” and retaliation against Western interests. Shadow Alarm is a known Iranian actor. Other groups, such as Arabian Ghosts and Anonymous Syria, are primarily Syrian or Syrian-aligned, motivated by regional conflicts in the Middle East.



Hacktivist communication referencing OpIsrael, an annual coordinated hacktivist attack against Israeli government agencies and private companies.

- **The Pro-Russian “Global” Alliance:** We observed an emerging trend of cross-regional alignment where groups outside the primary conflict zones adopt Russian geopolitical interests. Nullsec Philippines exemplifies this “double agenda.” At the same time, the group maintains its focus through anti-China operations, but it has also formally integrated into the pro-Russian/anti-Western bloc by participating in coordinated strikes against the U.S. The group acts as a regional force multiplier for Russian interests, often utilizing shared toolkits.



## Trends in Regionalized Targeting

Targeting trends follow a mirroring effect, where cyber-physical operations directly reflect real-world diplomatic alliances and military support.

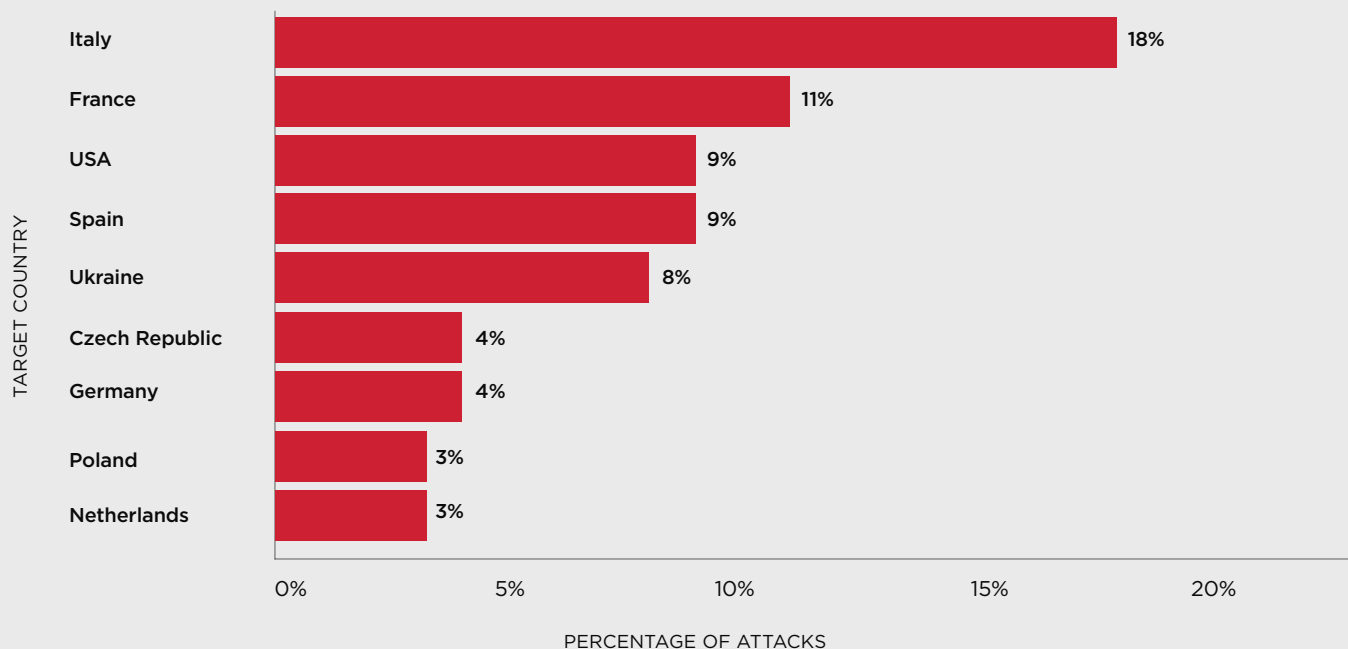
### Russia vs. Europe and Ukraine

Russia-aligned groups have extensively pivoted toward Western Europe, targeting nations that provide military and diplomatic aid to Ukraine. The data confirms that European infrastructure has become a secondary front in the ongoing conflict.

- **Primary European Targets:** Italy is the most frequent European target for these groups, accounting for 18% of the attacks. Spain follows with 9%, while France represents 11% of the “Soviet” origin activity.
- **Targeting Ukraine:** Direct attacks on Ukraine account for 8% of the documented activity within this bloc, focusing on critical infrastructure such as wood production and heating systems.
- **Critical Sector Focus:** Groups such as SECTOR16 and Z-ALLIANCE (Z-Pentest) have specifically targeted power generation and water treatment facilities in France, Poland, and Italy. Examples from our data collection include the breach of a small hydroelectric power plant in France (March 2025) and a hydroelectric station in Gdańsk, Poland (May 2025), to demonstrate the vulnerability of European life-support systems.



## Russia-Affiliated Attacks



**The following countries account for less than 3% each of the remaining attacks:**

**Other European Countries:** Bulgaria, Greece, Hungary, Lithuania, Norway, Portugal, Romania, Slovakia

**Other Americas Countries:** Brazil, Canada

**Asia-Pacific Countries:** China, India, New Zealand, South Korea, Taiwan, Thailand, Vietnam

**Middle East & African Countries:** Gaza, Iran, Israel, Morocco, Turkey, Uganda

This is a sample of countries targeted by Russia-affiliated groups.

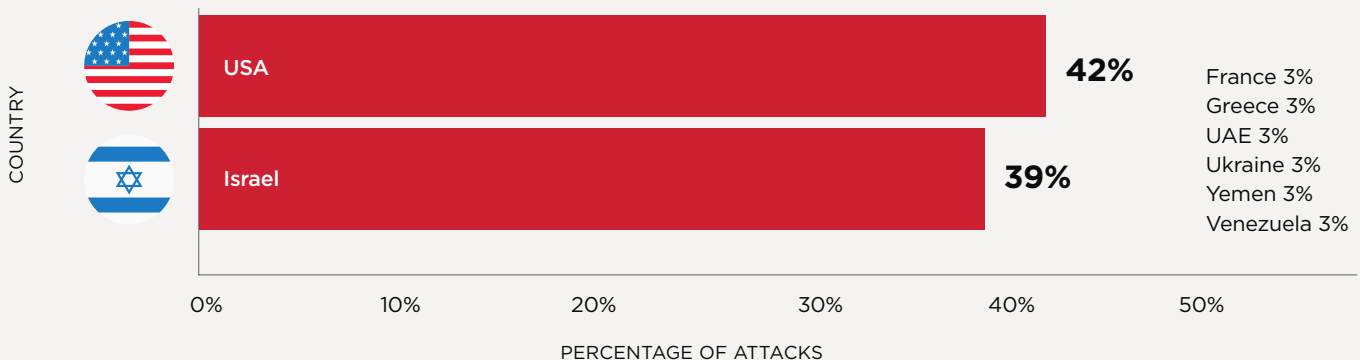


## The Middle East Tensions: The U.S.-Israel Nexus

The conflict in the Middle East has catalyzed a unification of fronts, where Arab- and Iranian-aligned groups target Western interests as a surrogate for their support of Israel.

- The U.S.: The United States is the most targeted country for the Iran bloc, suffering 42% of its attacks. Groups like Arabian Ghosts and Shadow Alarm frame these as direct responses to American foreign policy.
- Israel as the Hub: Israel remains a primary regional target for this bloc, accounting for 39% of attacks from Iranian-aligned sources. Overall, Israel accounts for 24% of the entire dataset's victim distribution.
- France, Greece, the United Arab Emirates, Ukraine, Yemen, and Venezuela also appear in this segment of our dataset, each accounting for 3% of attacks.

### Targeted Countries (Iran-affiliated Attacks)



## Exploring the Anatomy of CPS Attacks

In order to understand how to defend against attacks, we first need to understand how they are carried out. This idea led us to explore the “kill chain,” an anatomy of the stages of CPS attacks our research uncovered. By identifying common denominators between attacks, as well as uncovering crucial artifacts released by attackers, we were able to reduce the attack kill chain to the following steps:



**Target Selection:** Attackers identify the device type they want to target, such as a specific device—a certain programmable logic controller (PLC), HMI or SCADA system (such as in the [2023 Iranian attack on US critical infrastructure](#) that targeted [Unitronics devices](#))—or more often than not, an insecure, legacy protocol. In doing so, they will search for device classes that expose insecure services such as the VNC protocol or Modbus. Once a target is selected, the attackers can move on to the second step, searching for internet-exposed devices.



**Victim Selection:** The second step in the kill chain is finding potential victims' exposed devices. Using internet-scanning services such as [Shodan](#) and [Censys](#), which constantly scan the entire IPV4 IP range and map exposed services, attackers can look for internet-exposed devices. These are legitimate research tools, but like many others in technology these can be perceived as dual-use services that can be abused by malicious actors. This makes victim selection as simple as looking for devices that expose an insecure-by-design protocol such as Modbus, which was designed for trusted air-gapped deployments and lacks basic authentication or encryption by default. They may also look for devices that enable the VNC protocol without authentication (both Modbus and VNC, for example, are jointly searchable using the API exposed by the search engines named above).



**Target Enumeration:** After picking a specific target, the attackers move to the enumeration step. This step depends on the threat vectors the attackers choose to target. For example, if the device exposes its Modbus port, the attackers would use open source Modbus clients to enumerate Modbus registers/coils and their value. If VNC is the vector the attackers wish to exploit, they would search for the default credentials for this exact device, or brute-force authentication services looking for weak credentials.



**Destruction:** The last step these opportunistic attackers often take is to cause disruption or damage. While this also depends on the attack vector, the common denominator is to change parameters, values, or configurations that put the device out of commission or cause physical impacts to whatever the device governs. While the goal is the same in these attacks, the means by which they are able to disrupt devices differs based on the vector the attackers used. For example, if leveraging Modbus, the attackers would overwrite registers and coils with garbage data, creating physical damage to devices. If using VNC, an attacker would have the necessary access to change values or device configurations, also creating a physical impact on a service process.



**Taking Credit:** While the attackers wreak havoc on the device, changing its configuration and parameters and affecting its performance, usually they will take a screen recording of their actions. This will later be used to take credit for the attack by sharing the incident on social media platforms or closed channels, in order to gain political or social credibility.

From our analysis of the data, we can infer that attackers are shifting away from what are considered more traditional attacks. Instead of calculated attacks against specific targets, where attackers are trying to avoid detection, improve their stronghold over the victim's networks, maximize damage, and wait for the right time to attack, we are seeing a 180-degree shift in threat actor tactics.

In the attacks we researched—we call them “drive-by attacks”—they are not targeted, instead threat actors access assets that are exposed in countries or regions that meet their politically or socially motivated goals, attacking almost aimlessly at assets rather than organizations.



**Drive-by attacks target internet-facing assets in order to meet a threat actor's political or social goals.**

Another big difference between drive-by and traditional attacks is the methodology attackers employ. When we think of attacks on CPS networks, we believe attackers launch sophisticated attacks, involving exploitation of unpatched 1-day or even undiscovered 0-day vulnerabilities. However our research shows the opposite.

Instead of vulnerability exploitation, drive-by attacks simply rely on attacking assets that are insecure by design or default, largely leveraging insecure protocols or default credentials. By targeting devices that expose protocols that were not built with security in mind or have weak, default, or no credentials, attackers can connect to the device and then control, disrupt or otherwise damage it.

Devices that expose remote access protocols such as VNC and telnet are favored by threat actors among the incidents we researched. The reason is simple: organizations often leave these protocols not only exposed online, but also in their default configuration and protected by default or known weak credentials. This enables remote control and takeover of CPS assets; an attacker can then remotely change an asset’s configurations and parameters to suit their mission goals.



The threat actor Z-Pentest accessing a Greek industrial control system using a weak password.

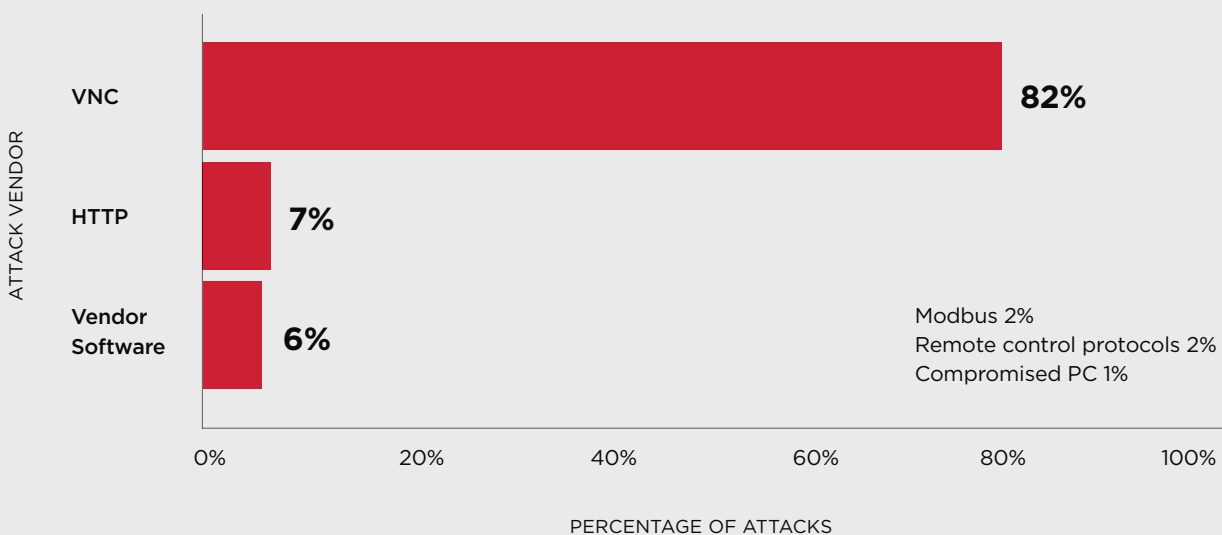
## CPS Asset Selection

After understanding the steps attackers take in their approach of attacking critical infrastructure around the world, we then sought to understand which asset classes are most targeted in these types of drive-by attacks. Our methodology was simple. If we had sufficient data about a CPS attack, we mapped two things: the protocol used in the attack and the type of device that was targeted. If possible, we would also try to identify the exact model/vendor of the device that was targeted, however in many cases this was not possible due to the attackers not supplying enough information to identify the device accurately.

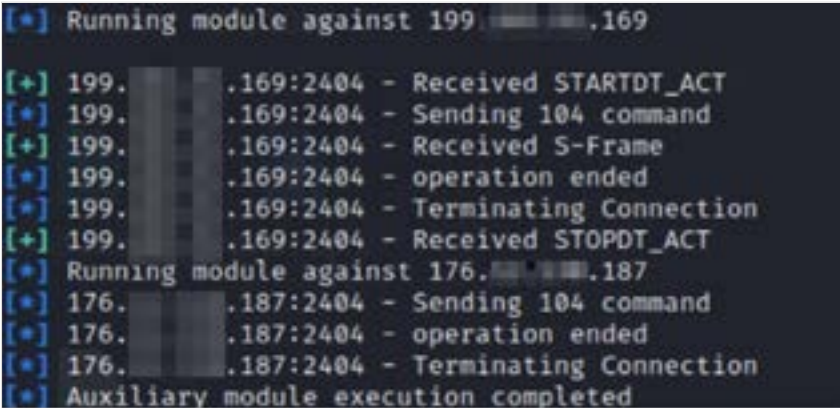
From our analysis of the evidence we observed in more than 200 attacks, we discovered that in more than 80% of cases, attackers targeted devices that expose a VNC service. Often, attackers share videos on the social and closed channels we relied upon to gather information on incidents demonstrating this approach. In most cases, we saw many of the attacked devices were configured with default or weak credentials—sometimes no credentials—that are easily brute-forced.

In addition to targeting VNC, we also observed incidents—albeit fewer—carried out leveraging compromised web servers over HTTP, or insecure OT protocols communicating with industrial devices. We also observed incidents where attackers with access to systems leveraging legitimate software such as engineering workstation (EWS) programs or native management software to connect and reconfigure the device. This was evident in the 2023 attacks against [Unitronics integrated HMIs/PLCs](#) that stemmed from [missing authentication](#) in the communication protocol with the device.

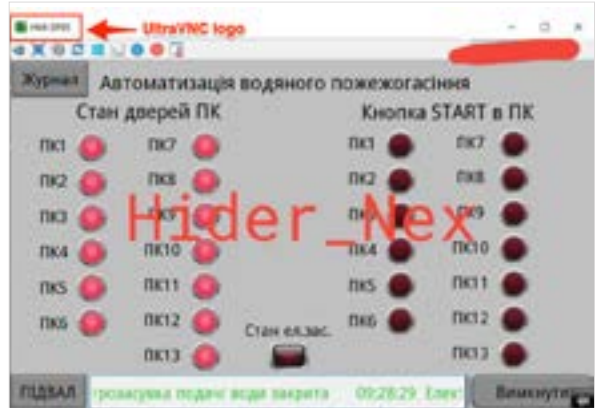
Attack Vector Distribution



From analyzing all the evidence supplied by attackers, another huge commonality that we observed was the toolsets used by attackers—almost all tooling used by attackers is either open-source software (OSS) or free-of-charge, be it VNC clients (the most common of which that were used by attackers are [UltraVNC](#) and [TightVNC](#)), open-source software tools such as [Metasploit](#) or modbus-cli, and even software supplied by vendors to configure or control their devices such as engineering workstations (EWS) or clients.

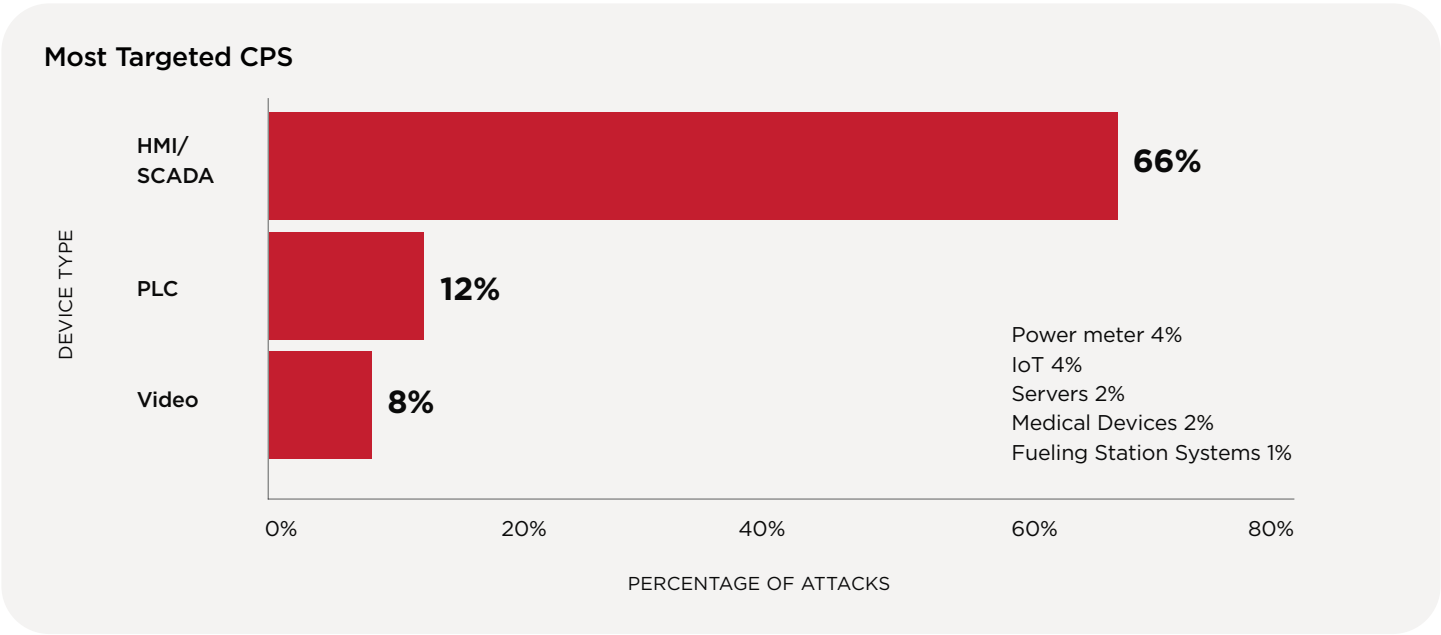


A Metasploit module used against an OT asset.



Evidence supplied by attackers, disclosing the VNC program used by the attackers (UltraVNC).

In addition, the majority of attacks we researched targeted HMI and SCADA systems. This aligns with attackers’ targeting of VNC since the remote-access protocol is supported by many HMI panels. From our data, we see that close to 65% of all attacks targeted HMI panels or SCADA systems. We then see a commonality between the rest of the targets, be it a PLC with exposed insecure protocols or default/no authentication, or IoT devices such as CCTV cameras with default configurations.



Lastly, we saw some recurring targets between different groups, including older PLC product lines that were heavily targeted by attackers in the past such as the Unitronics integrated HMI/PLC devices or gas station and fuel management systems, such as in the [IOCONTROL](#) incidents disclosed in 2024. Even mid-tier HMI panels from multiple makers were also targeted; we observed that these are often left in their default factory settings when it comes to credentials. One threat actor group solely targeted a specific model for three months, attacking multiple victims with factory settings enabled.



## Takeaways

Team82's research can safely conclude that hackers are taking a special interest in leveraging CPS for geopolitical, political, and social gain, and therefore, organizations should no longer tolerate lax cyber security practices around OT, medical devices and systems, and IoT devices.

The research demonstrates that internet-facing CPS are particularly at risk, given that many of these devices can easily be enumerated on the internet and accessed often because of poor credentials or weak configurations that leave them open to attack. We've identified three particular takeaways from our research that defenders of CPS should particularly adhere.



### Secure Internet-Facing CPS

Hackers have made child's play out of enumerating exposed CPS on the internet. Search engines that scan the entire IP address range are readily available and often used by threat actors to find vulnerable CPS assets that have been leveraged in attacks across the globe. This is particularly useful for attack groups with geopolitical motivations.

Enumerating internet-facing CPS is relatively simple using internet-scanning services such as Shodan or Censys, for example. It's important that defenders check the configurations of their OT, connected smart devices, and internet of medical things (IoMT) devices and ensure that there are proper precautions taken as these devices are increasingly connected to the internet.

Organizations cannot afford to have these critical devices and systems insecurely connected in any way to the internet. Illicit access to these devices can expose organizations to service disruption, physical damage to assets, or endanger the personal safety of workers or the general public. Hackers may also use these devices as an entry point onto the process network or enterprise network to cause further damage, including ransomware or extortion attacks, exploits against vulnerabilities.

## Remedy Insecure by Design/Default

CISA and similar agencies globally have urged device manufacturers to improve the overall quality and security of internet-facing CPS assets. The industry is plagued by a litany of legacy technology that is so deeply ingrained in current industrial processes, for example, that any alteration to these devices could cause significant damage.

Insecure by design or default is a critical flaw that must be addressed. Our research found that many legacy communication protocols are coveted by attackers when targeting CPS assets. Many insecure protocols, such as Modbus, are widely used in manufacturing in other industrial circles for device-to-device communication. Critical process data travels over these protocols and any alteration or disruption to process data traveling over these protocols could be detrimental.

Other protocols such as VNC, which enables remote access to devices, are often left in their default configuration or insufficiently protected, leaving a gap for attackers to take control. They lack critical security capabilities, such as authentication or encryption and often require compensating controls be put in place in order to minimize risk. This requires an audit and accurate inventory of CPS assets, as well as an understanding of which devices are exposed and how they are exposed.

Remediation can be challenging as the update process often requires vendor involvement, whether it's providing new firmware that addresses vulnerabilities or wholesale configuration changes that address other legacy security issues. Such updates may often require time to assess and develop, and deployments are often on a vendor's timetable. Therefore, defenders must be vigilant about default, or known, weak credentials, and proactively change them as devices are deployed online.

Defenders should evaluate and understand other insecure configurations, and any security issues must be addressed before devices are connected online.





## Know Your Adversary

One of the goals of Team82's research was to illustrate exactly how hacktivist groups are leveraging CPS in drive-by attacks. The problem is real. CPS are often exposed and insecure, and geopolitically motivated threat actor groups understand the potential impact of targeting CPS assets. They understand the disruption and damage they can cause. They also understand that even the mere possibility of negative outcomes such as water contamination or a power outage can bring chaos to societies.

Team82 has looked at more than 200 incidents involving CPS assets and has identified 20 threat actor groups with varying degrees of technical skill. While sympathetic to certain geopolitical affiliations, these actors are not on the same tier as nation-state attack groups. Instead, almost all of them target CPS assets, such as HMIs and SCADA systems, and other internet-facing exposed assets with attacks that don't rely on exploits or vulnerabilities.

These decidedly low-tech groups are often very willing to brag about their exploits online, whether in social media channels or closed online groups. They often share details about the systems they've compromised and the means by which they do so, often supplementing their bragging with video evidence of such attacks in order to gain credibility within their communities.

Team82 has seen some of this evidence, collected and analyzed it, and can infer many of the TTPs these attack groups use. As we mentioned often, these groups take advantage of lax security practices, insufficient authentication, and legacy protocols that don't require credentials and don't encrypt data in transit.

We identified some of the groups we researched yet there are commonalities among all of them that we have described throughout this report. While it's not always critical to know exactly who is on your network, it is important to understand their tactics and their motivations in order to determine whether you could be next within your industry to be targeted, or whether your CPS assets are similarly exposed as other organizations that have been compromised.

As we mentioned these attacks are real, and CPS is being leveraged often. The time is now to lock down authentication and other basic security hygiene practices: change your default passwords and consider moving to more modern communication protocols for connected device traffic. This activity should introduce new urgency to address the risk to CPS assets.

### About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit [claroty.com](https://claroty.com).

### About Team82

Team82, the research arm of cyber-physical systems (CPS) protection company Claroty, is an award-winning group of researchers known for threat research, OT and medical protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial product vulnerabilities. Committed to strengthening CPS cybersecurity and equipped with the industry's most extensive testing lab, the team works closely with leading vendors to evaluate the security of their products. As of March 2026, Team82 has discovered and disclosed more than 700 vulnerabilities. Visit: [Claroty.com/Team82](https://Claroty.com/Team82).