We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems

mandiant.com/resources/blog/hacktivists-targeting-ot-systems

In January 2023, the Anonymous affiliated hacktivist group, GhostSec, claimed on social media to have deployed ransomware to encrypt a Belarusian remote terminal unit (RTU)—a type of operational technology (OT) device for remote monitoring of industrial automation devices. The actors' stated intention was to demonstrate support for Ukraine in the ongoing Russian invasion. Researchers, OT security professionals and media outlets analyzed the claims and concluded that the actor overstated the implications of the alleged attack.

Although there was no significant impact in this particular incident, the event highlights the increasing need for a wider discussion regarding the extent of risk hacktivists pose to OT environments. For the last several years, Mandiant has tracked various hacktivists' claims of targeting OT systems claiming physical damage as a result. Exacerbated by geopolitical tensions in different regions—such as Russia’s ongoing invasion of Ukraine—these actors have recently intensified their activity, resulting in more frequent claims and new avenues to impact targets.

In most cases, hacktivists’ claims are exaggerated or unsubstantiated. The number of false claims is at times challenging to debunk. However, despite the inaccuracy of most claims, when hacktivist activity targeting OT becomes commonplace, the likelihood of actual and even substantial OT incidents increases. The risk is higher for organizations that are perceptibly associated with political events or social disputes based on geographic location, nationality, language, or industry of relevance.

In this blog post, Mandiant offers a comprehensive analysis of recent hacktivist activity targeting OT systems. Mandiant was able to leverage information from previously undisclosed and known incidents to discuss the potential implications for OT defenders. Awareness about emerging hacktivism trends helps OT defenders to prioritize countermeasures and differentiate state-sponsored fronts leveraging the hacktivism cloak.

Hacktivists Increasingly Claim to Target and Impact OT

In 2021, Mandiant published a blog post describing an increasing trend in low sophistication compromises where actors targeted internet-exposed assets across multiple industries. Most of the cases we analyzed were seemingly conducted for financial or opportunistic motivations. But others were conducted with ideological motivations by hacktivist groups claiming to target OT devices or releasing training tutorials to inform other actors how to attack OT systems.

One year later in 2022, Mandiant observed more than twice as many hacktivist claims targeting OT as compared to 2021. The majority of cases Mandiant tracked in 2022 were conducted by actors in support of Ukraine—although we also observed instances in favor of Russia. Additionally, Mandiant noted an interesting trend where hacktivist actors focused their targeting on organizations in the Middle East, likely in response to political tensions in the region. Figure 1 illustrates some relevant keywords we observed across different hacktivist claims.

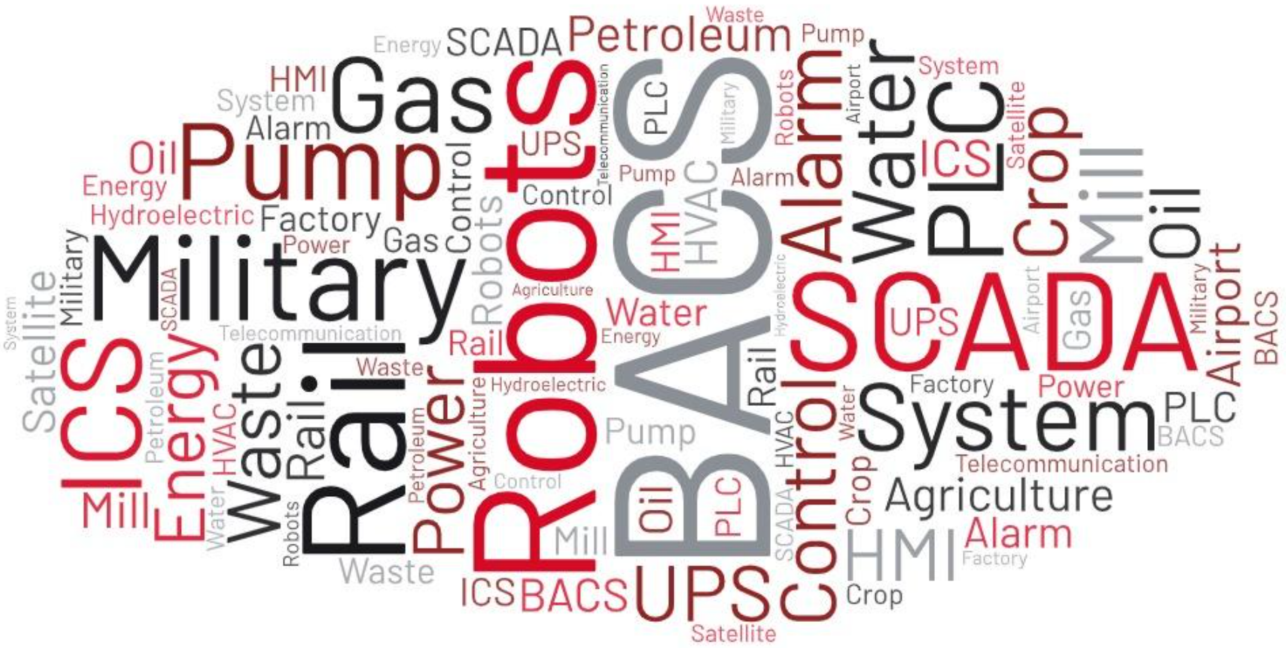


Figure 1: Common keywords observed across hacktivist claims

While in most cases, Mandiant was not able to fully validate the actors' claims, we assess with moderate confidence that hacktivist actors have more often than not, overstated the effects and impact of their attacks. In other cases, it is possible hacktivists provided questionable claims about their independence or non-affiliation with government-sponsored groups.

Nevertheless, in the majority of the cases, the actors provided evidence of at least being proficient in accessing unidentified internet-exposed OT assets. It is important to note that there are also multiple other cases, wherein the actors targeted IT assets from OT organizations, however for the purpose of this analysis, we are not including those instances.

Trends in Hacktivist Activity Targeting OT

Throughout 2022, the majority of hacktivist claims that Mandiant observed targeting OT followed similar techniques, tactics and procedures (TTPs) and behavioral patterns. The actors often leveraged similar social media and messaging channels and targeted victims in the same way.

Most often, the hacktivists likely gained initial access via insecure, internet accessible devices or public-facing applications. This allowed them to execute actions via command-line, or graphical user interfaces (See the Appendix for a list of MITRE ATT&CK for ICS tactics and techniques used by hacktivists targeting OT). While these types of techniques have historically been used to conduct low sophistication OT compromises, we recently observed some unique trends that indicate changes from baseline activity.

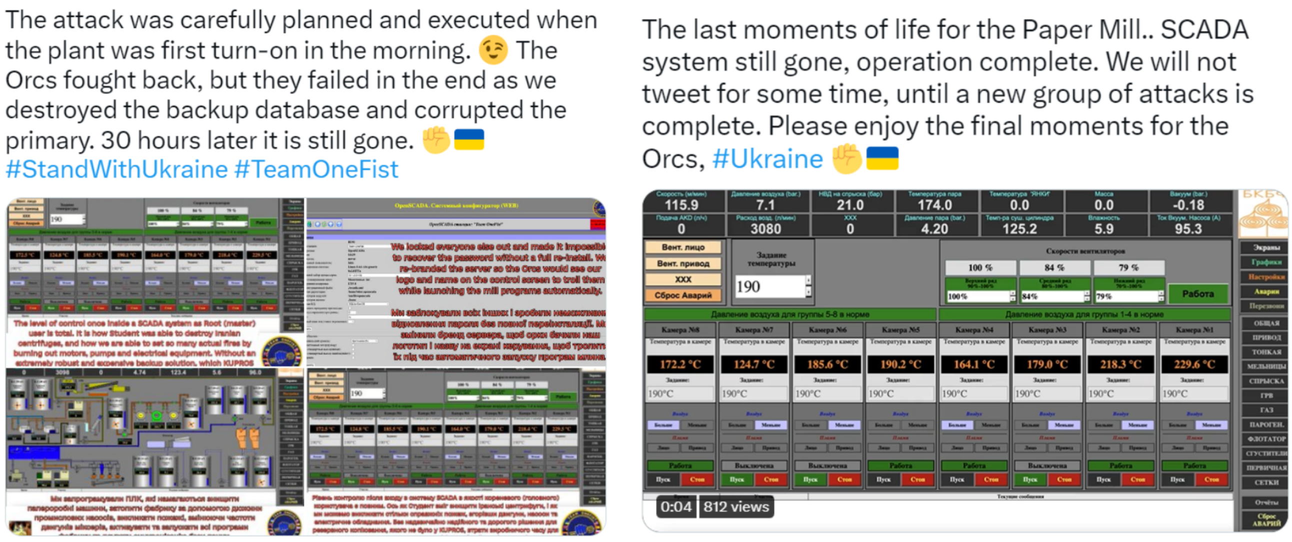
Hacktivists Increasingly Use Public Forums and Social Media Platforms to Post Claims

Historically, hacktivist claims of compromising OT systems were distributed exclusively across closed audiences via underground forums or private communication channels. However, recent claims have also been promoted via dedicated assets affiliated with the actors on public forums and popular social media platforms. These methods help the actors to gain public attention via media and specialized publications, enabling them to leverage claimed OT compromises to grow their reputations, gain notoriety, and spread their promoted messaging across broader audiences. A negative effect of this trend is that the amplification of such activity can also inspire other actors to build offensive OT-oriented capabilities.

Hacktivists Support Both International and Domestic Political Narratives

Most recent OT-oriented hacktivist activity was allegedly conducted in response to geopolitical events—with the vast majority of that activity targeting Russia as a result of its invasion in Ukraine, as well as targeting Israeli regional policies. These hacktivists often depicted their OT-oriented operations as contributing to militias fighting on behalf of Ukraine or Palestine.

The most active group we tracked in 2022 was Team OneFist (also known as Joint Cyber Center). Team OneFist issued multiple claims via social media, alleging to conduct attacks against power plants, an airport, uninterruptible power supply (UPS systems), a paper mill, and SCADA systems, among others. The actor's promoted narrative suggests the group's main motivation is to target Russian organizations in support of Ukraine.



The attack was carefully planned and executed when the plant was first turn-on in the morning. 😉 The Orcs fought back, but they failed in the end as we destroyed the backup database and corrupted the primary. 30 hours later it is still gone. ✊🇺🇦 #StandWithUkraine #TeamOneFist

The last moments of life for the Paper Mill.. SCADA system still gone, operation complete. We will not tweet for some time, until a new group of attacks is complete. Please enjoy the final moments for the Orcs, #Ukraine ✊🇺🇦

Figure 2: Social media posts claiming Team OneFist involvement in attack targeting Russian paper mill

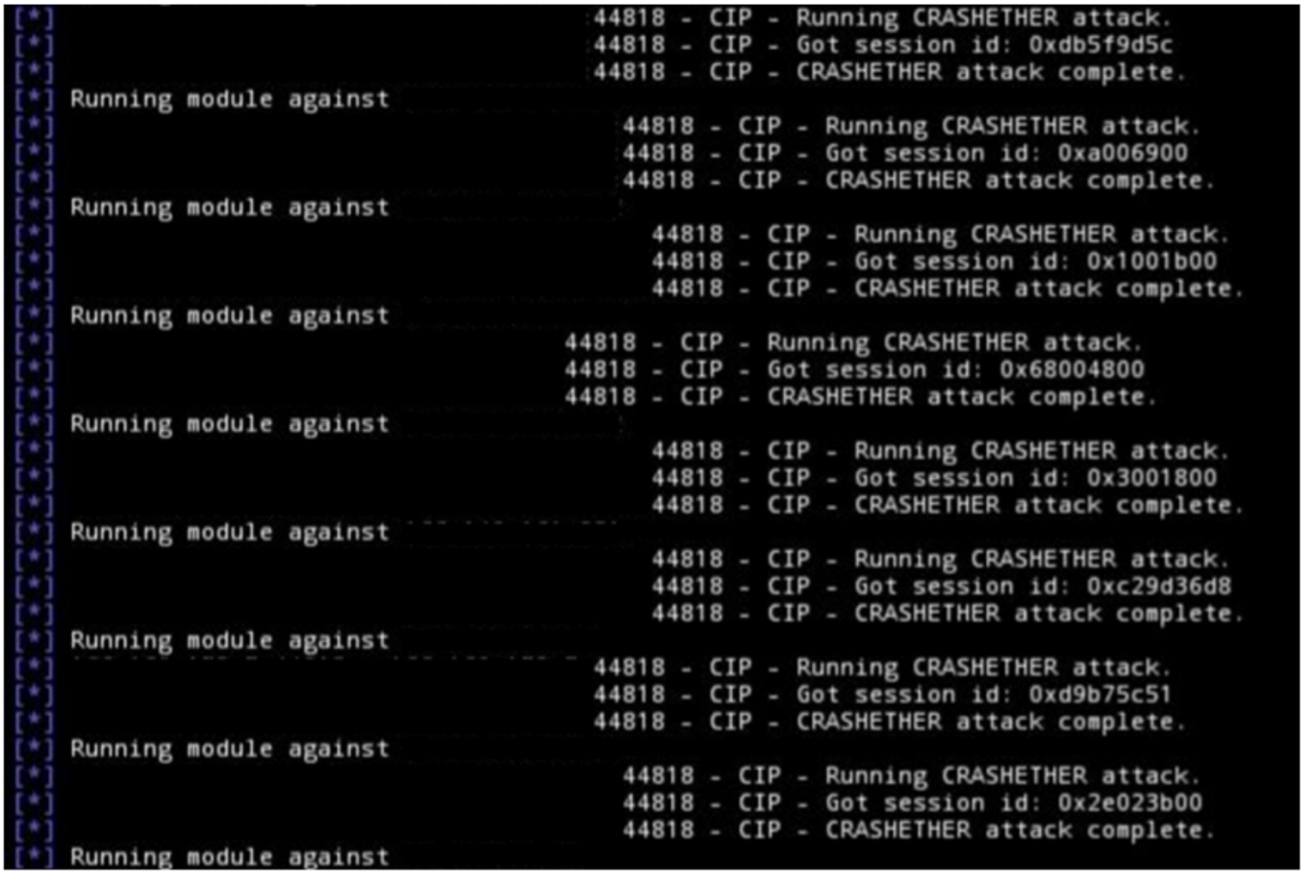
Although most messaging associated with hacktivist claims appeared responsive to geopolitical developments, we observed at least one case where the actor opposed domestic policies in the United States. In July 2022, the threat actor "SiegedSec" targeted U.S.-based

IP addresses with exposed ICS ports to protest abortion restrictions in the United States. The attack was part of a broader Anonymous-related hacktivism campaign known as Operation Jane (aka #OpJane).

Some Hacktivists Leverage Known OT Exploits to Target Victims Assets

Recently, we have observed hacktivist groups leveraging specialized exploits and exploit modules to increase the likelihood of impacting OT devices. Such evolution in hacktivist techniques results both from the existence of an active community sharing knowledge, and the increasing availability of resources shared publicly to interact with OT.

For example, in June and July 2022, actors "GhostSec" and "SiegedSec" targeted OT assets in the U.S., Israel, and Russia using OT-oriented exploit modules. The actors leveraged an IEC-104 and EtherNet-IP CIP Metasploit modules, and a custom Modbus-based tool dubbed "Killbus" (Figure 3).



```
[*]                                    44818 - CIP - Running CRASHETHER attack.
[*]                                    44818 - CIP - Got session id: 0xdb5f9d5c
[*]                                    44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                      44818 - CIP - Running CRASHETHER attack.
[*]                                      44818 - CIP - Got session id: 0xa006900
[*]                                      44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                        44818 - CIP - Running CRASHETHER attack.
[*]                                        44818 - CIP - Got session id: 0x1001b00
[*]                                        44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                  44818 - CIP - Running CRASHETHER attack.
[*]                                  44818 - CIP - Got session id: 0x68004800
[*]                                  44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                        44818 - CIP - Running CRASHETHER attack.
[*]                                        44818 - CIP - Got session id: 0x3001800
[*]                                        44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                        44818 - CIP - Running CRASHETHER attack.
[*]                                        44818 - CIP - Got session id: 0xc29d36d8
[*]                                        44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                    44818 - CIP - Running CRASHETHER attack.
[*]                                    44818 - CIP - Got session id: 0xd9b75c51
[*]                                    44818 - CIP - CRASHETHER attack complete.
[*] Running module against [redacted]
[*]                                      44818 - CIP - Running CRASHETHER attack.
[*]                                      44818 - CIP - Got session id: 0x2e023b00
[*]                                      44818 - CIP - CRASHETHER attack complete.
[*] Running module against
```

Figure 3: EtherNet/IP CIP Metasploit module commands executed by hacktivists

In other cases, actors exploited known vulnerabilities to reach their target. For example, in June 2022, pro-Ukraine threat actor Team OneFist targeted a cellular router allegedly supporting OT in Russia by exploiting a known cross-site request forgery (CSRF) vulnerability in the system that leads to remote code execution.

Between April and July 2022, multiple hacktivist groups targeted ELNet OT assets in Israel, possibly by exploiting a missing authentication vulnerability reported in the assets' web consoles. We have not identified evidence indicating formal collaboration between these actors, but it is possible that mutual awareness of each other’s activity prompted interest in reusing similar vulnerabilities to target their victims.

Hacktivists Share Documentation of Physical Incidents to Gain Credibility

In most of the hacktivist claims we tracked, the actors leveraged documentation, such as videos or screenshots, to provide evidence of their actions and gain credibility. Often, the actors shared images of real physical incidents to claim responsibility for the destruction of assets – even if they were not caused by their attacks. This is likely a strategy used by actors to help bring attention to their political and social messaging.

For example, in July 2022, Iraqi group Altahrea Team claimed it was responsible for a fire at the Orot Yosef power plant in the Negev in southern Israel. The actor shared a video of the fire to illustrate their claim (Figure 4). A couple days later, GhostSec shared a video of a physical incident at a hydro-power plant in Russia and claimed credit for the incident. The actor noted their recent activity targeting internet-accessible electricity assets in Russia as proof of their claims. In both cases, we found no evidence connecting the hacktivist actions to the physical incidents.

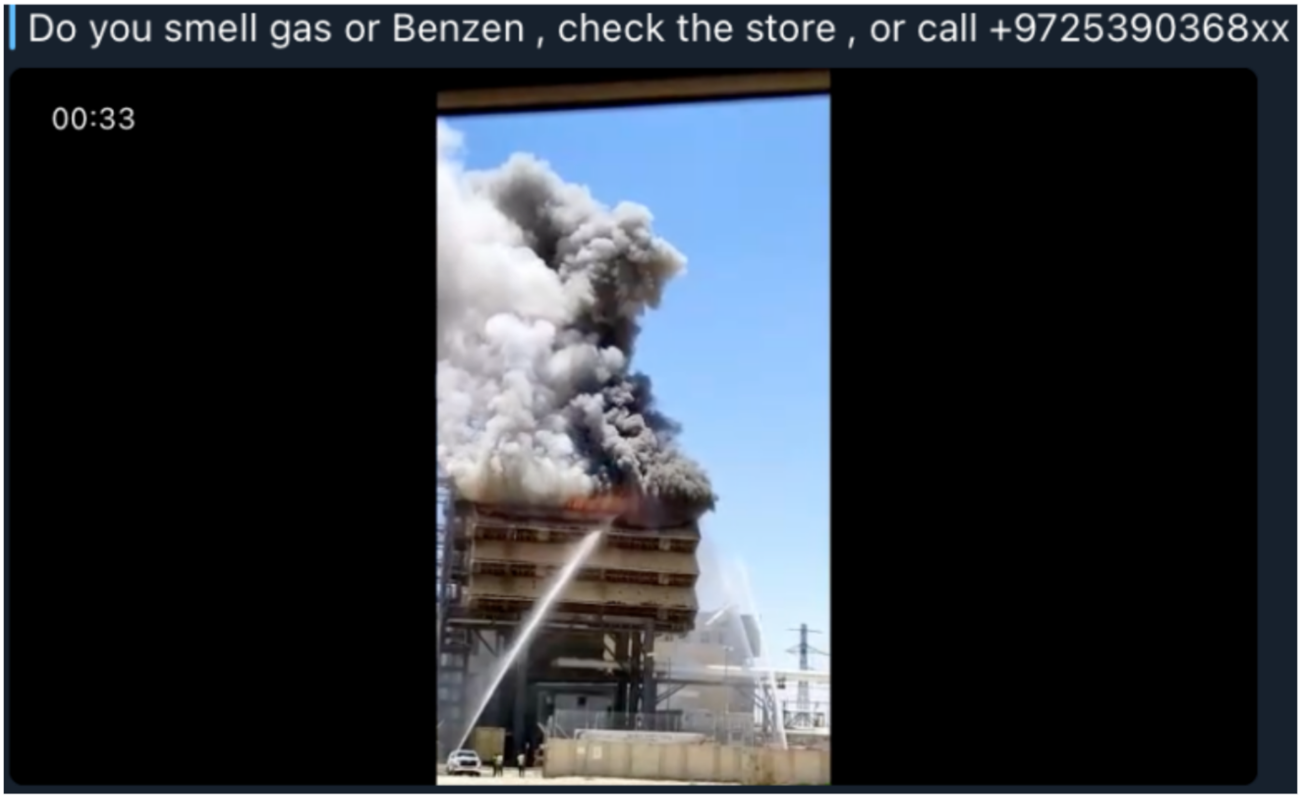

Do you smell gas or Benzen , check the store , or call +9725390368xx

Figure 4: Video of a physical incident shared by hacktivists to claim authorship

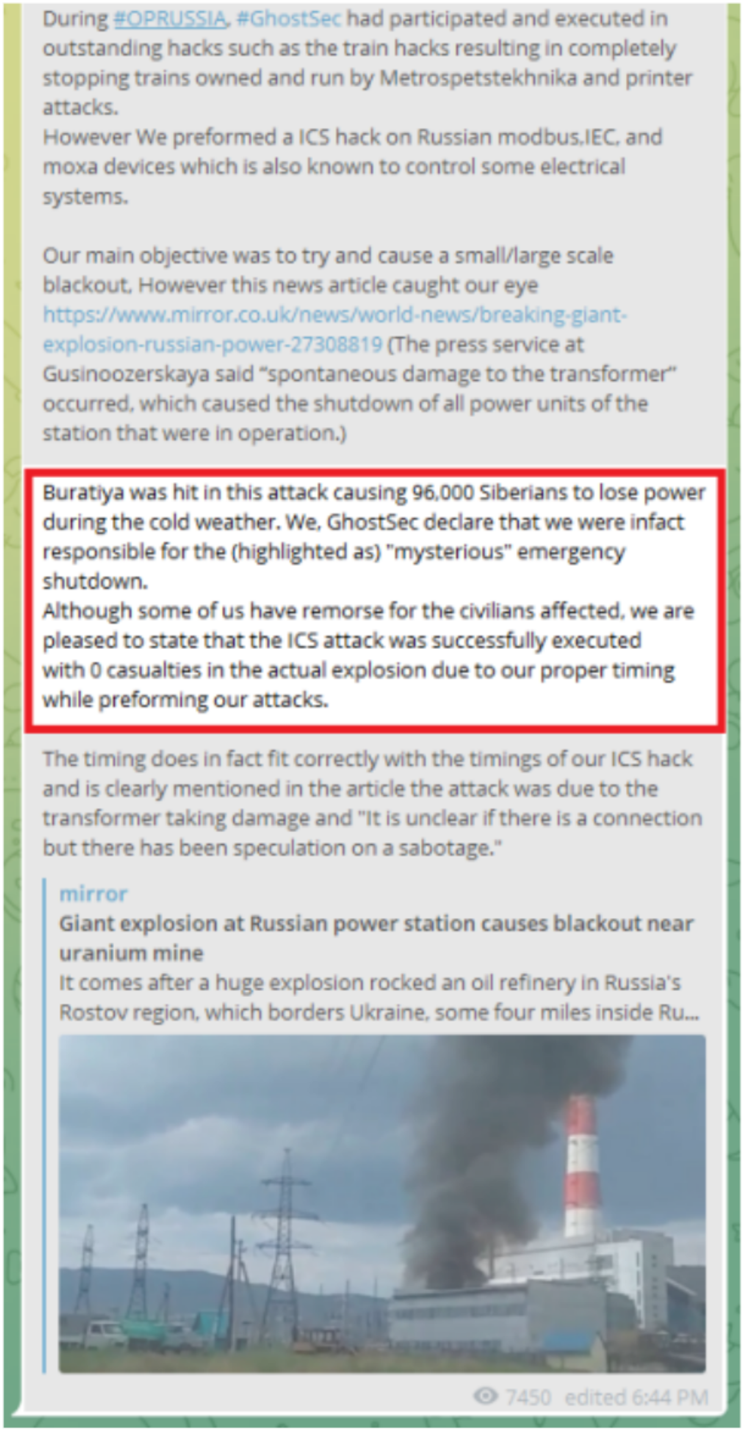
In June 2022, Team OneFist claimed to have disabled a cellular router supporting OT in Russia. The actor took advantage of a publicly reported physical incident at a nearby power plant and claimed that it was the result of their operation. However, the primary cause of the outage was reportedly a fire at a different power plant situated nearly 400 miles away.

This trend illustrates a common challenge for OT security professionals, which is the limited understanding of the field outside of specialized industry cliques and the lengthy process required to conduct root-cause analysis. As we observe an increasing number of claims from actors taking responsibility for physical damage, OT defenders require more resources to filter what information is relevant. Additionally, other information operations actors could potentially leverage such claims to further their own objectives in targeting a given population.

Some Actors Emphasize Intent to Avoid Impacts to or Endanger Human Safety

Some hacktivist actors have also claimed to avoid impacts to human safety. However, there is no evidence to verify their intentions. It is plausible that the hacktivists emphasized safety either because of the perception of OT-oriented attacks as potentially harmful or simply to improve their reputation and gain sympathy from their audiences.

One example was the case of GhostSec in July 2022, which claimed to cause an incident at a power plant in Russia. The actor then claimed the attack was "executed with 0 casualties in the actual explosion due to our proper timing while performing our attacks" (Figure 5).



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.)

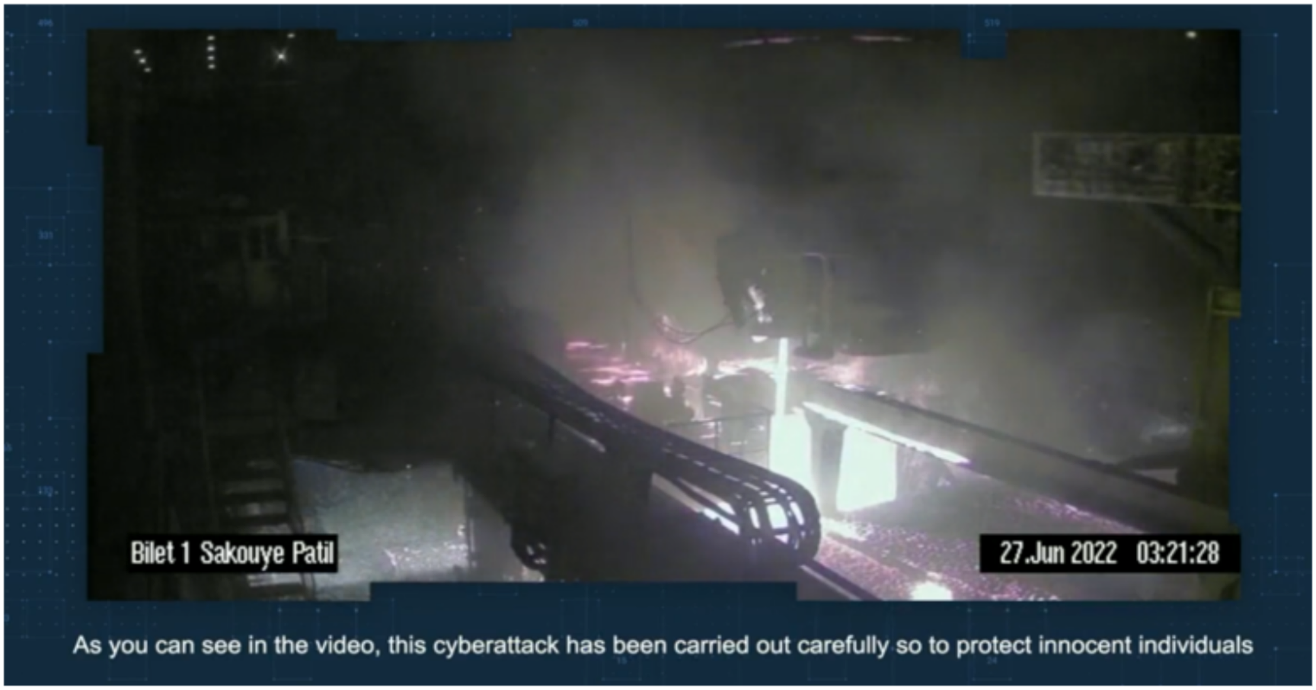
Buratiya was hit in this attack causing 96,000 Siberians to lose power during the cold weather. We, GhostSec declare that we were infact responsible for the (highlighted as) "mysterious" emergency shutdown.
Although some of us have remorse for the civilians affected, we are pleased to state that the 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 Ru...

Figure 5: Hacktivists emphasizing their alleged cyber-physical attack avoided human casualties

Another example is the self-proclaimed hacktivist Predatory Sparrow–also known as UNC4368–which in June 2022, claimed to conduct cyber attacks against three steel manufacturers in Iran, alleging it destroyed physical infrastructure. The actor shared a video showing an explosion in a manufacturing facility and emphasized the attack was carried out carefully to protect innocent individuals. We note that the techniques used by Predatory Sparrow in prior incidents are more complex than those from other hacktivists. This may indicate collaboration or sponsorship from sophisticated actors.



As you can see in the video, this cyberattack has been carried out carefully so to protect innocent individuals

Figure 6: Screenshot from video uploaded by Predatory Sparrow to provide evidence of the attack

While less common, we have also observed self-proclaimed hacktivists claiming direct intent to endanger human safety. On Jan. 29, 2023, Arabic-speaking hacktivist group `Force Electronic Quds` (FEQ) claimed several attacks against OT in Israel. In a post from one of those attacks, the actor shared screenshots from systems that allegedly belonged to chemical facilities. The post threatened the company's employees and stated they "will never hesitate to melt your bodies with chemicals".

Hacktivists Target OT to Make Political Statements

Hacktivism leverages cyber threat activity as a means to convey political or social narratives. As such, any attempts to inflict damage on a victim may only be a means to this end or one of multiple objectives. Historical hacktivist activity has largely focused on simpler attacks that are intended to get the attention of broad audiences, such as website compromises or denial of service attacks. The shift in hacktivist activity to also target OT can be explained by multiple factors:

- Attacks against OT systems are often perceived as impactful, given their potential to damage or modify physical processes. Prioritizing higher-profile targets increases the likelihood that an actor will attract the public's attention even if they do not damage OT systems or if their compromise results in trivial impacts. Similarly to information operations campaigns, these types of hacktivist claims can also serve to undermine the public's trust in governments and organizations.

- In some cases, targeting OT systems enables actors to participate and offer support for a cause from distant locations, such as during armed conflicts. This is illustrated by self-proclaimed hacktivist groups that currently conduct cyber operations in opposition or in favor of the Russian invasion of Ukraine.
- Self-proclaimed hacktivist cyber operations have also been used in the past to conceal state-sponsored activity and provide nation-states with plausible deniability—enabling states to conduct attacks with a lower risk of repercussions. An example is XakNet Team, which Mandiant has assessed with moderate confidence to be operating in coordination with APT28 actors. Given that hacktivist claims are often difficult to verify, nation-states can also use them to conduct false-flag operations.
- Some hacktivist actors have likely been inspired by prior cyber threat activity related to both low sophistication compromises and high-impact OT-oriented threat activity.

Situational Awareness to Prevent Hacktivist Compromises

In 2022, Mandiant observed a significant increase in the number of instances where hacktivists claimed to target OT. While we observed activity across different regions, most of these cases were conducted by actors that have mobilized surrounding the Russian invasion of Ukraine. The implication of this is that the increase in hacktivism activity targeting OT may not necessarily become consistent over time. However, it does illustrate that during political, military, or social events, OT defenders face a heightened risk.

These risks are also exacerbated by the quick evolution of hacktivist actors that have experimented with new tools and exploits during the war in Ukraine. The information and knowledge about OT compromises, which has been produced and shared during the last year, will likely help reduce the learning curve for different actors interested in targeting OT. This may increase the complexity of low sophistication compromises even after the end of the war. It is also possible that other more sophisticated actors will copy hacktivist techniques to limit the risk of facing consequences when targeting OT, or to support other types of information operations.

Asset owners and operators should maintain situational awareness of trends in hacktivist threat activity targeting OT systems to anticipate potential risks. We also highlight that most often, hacktivist threat activity can be prevented following common best practices for remote access to critical and internet-accessible systems.

Mandiant Threat Intelligence customers have access to the full list of incidents referred to in this blog post. For additional information, visit our website to learn more about Mandiant’s OT security practice or contact us directly to request Mandiant services or threat intelligence.

Appendix: MITRE ATT&CK for ICS Techniques Used by Hacktivists in 2022

Tactic	Technique
Initial Access	T0883: Internet Accessible Device
Initial Access	T0819: Exploit Public-Facing Application
Execution	T0807: Command-Line Interface
Execution	T0823: Graphical User Interface
Persistence	T0859: Valid Accounts
Evasion	T0872: Indicator Removal on Host
Lateral Movement	T0859: Valid Accounts
Collection	T0852: Screen Capture
Collection	T0811: Data from Information Repositories
Command and Control	T0885: Commonly Used Port
Command and Control	T0869: Standard Application Layer Protocol
Inhibit Response Function	T0816: Device Restart/Shutdown
Inhibit Response Function	T0809: Data Destruction
Impair Process Control	T0855: Unauthorized Command Message
Impact	T0831: Manipulation of Control
Impact	T0882: Theft of Operational Information
Impact	T0826: Loss of Availability