# Dark Web Profile: Hunt3r Kill3rs

Published: 2024-05-24 · Archived: 2026-04-05 16:37:52 UTC

In the ever-evolving landscape of cybersecurity threats, new groups like Hunt3r Kill3rs emerge with claims of disruptive capabilities. This analysis aims to provide an initial understanding of their activities, considering the limited timeframe and absence of concrete evidence substantiating their claims.

## Overview of Hunt3r Kill3rs:

Hunt3r Kill3rs, a recently surfaced threat group, assert their prowess in cyber operations, including **Industrial Control Systems (ICS)** breaches, communication network intrusions, and web application vulnerabilities exploitation. Despite their claims, the verifiable impact and sophistication of their operations remain unclear.

The group frequently claims to attack Operational Technology (OT) systems, including recent assertions of compromising companies using Unitronics PLCs. Unitronics PLC devices have been a common target for Iranian threat actors, particularly during the Israel-Hamas conflict. In response even CISA has issued advisories to enhance the security of these devices.

In a notable announcement, Hunt3r Kill3rs claimed to be launching a joint attack with **Народная Кибер Армия** (Cyber Army of Russia). Their stated targets include the US nuclear and electric power industries, specifically mentioning the Nuclear Energy Institute and the Electric Power Research Institute. They allege these resources have been disabled, though independent verification is lacking.

Collaboration announcement

It is observed that Iranian groups often collaborate with Russian threat actors or at least target similar objectives. In this context, it is plausible that information exchange occurs within this **pro-Russian** hacktivist sphere.

This hypothesis is supported by the group's claimed association with Cyber Army of Russia. Cyber Army of Russia's extensive network, encompassing pro-Russian or in some context anti-Israel hacktivist collectives like High Society from various countries including Yemen to India, likely facilitates the sharing of information and tactics.

## Techniques, Claims and Targets of Hunt3r Kill3rs

Some of the techniques and claims that we consider important are as follows:

**Industrial Control Systems (ICS) Allegations**

Hunt3r Kill3rs boast about infiltrating ICS, targeting prominent brands like **Siemens** and **Unitronics**. However, without corroborated evidence, the extent of their success in disrupting critical infrastructure remains speculative. Thus, they share screenshots.

Latest Telegram post, an alleged claim of Unitronics PLC infiltration

**Communication Network Intrusions:**

The group alleges breaches in communication networks, particularly targeting IP phone systems from vendors such as Cisco. Verification of these intrusions and their implications on communication services is pending.

Claims about Cisco IP Phone systems

**Web Application Vulnerabilities Exploitation**

Hunt3r Kill3rs claim to exploit vulnerabilities in web applications, citing instances like **SQL injection attacks** on platforms such as WordPress-based e-commerce sites. The actual impact on targeted websites and data integrity requires thorough investigation. If the claim is true, attacks made by such groups often only result in the website being defaced.

**Industries Supposedly Impacted**

Considering the claims they shared on their Telegram channels, we arrive at the following data.

Claims of disruptions in **manufacturing**, suggested breaches in **transportation systems.** Lastly, joint attacks with Народная Кибер Армия have allegedly targeted the US **nuclear and electric power** sectors, specifically the Nuclear Energy Institute and the Electric Power Research Institute.

### Geopolitical Targets

**Israel:** The group's claims of targeting Israeli cybersecurity centers and critical infrastructure, the first post on their Telegram channel is also about Israel.

One of the first posts in their Telegram channel

**Germany:** Alleged surveillance network breaches and infrastructure disruptions. Their latest alleged attack on Germany targeted a company called Mobotix. The claim suggested that the threat actors have fully penetrated the infrastructure and gained live access to cameras around the world.

**Ukraine:** Claims of strategic cyber actions in Ukraine highlight geopolitical motivations, yet evidence is inconclusive.

**United States:** The claimed joint attack with Народная Кибер Армия on US nuclear and electric power sectors and targeting companies with Unitronics products were a few examples of their targeting of the US.

## Conclusion

Hunt3r Kill3rs' emergence underscores the ongoing challenges in discerning genuine threats from exaggerated claims in the cybersecurity domain. As a relatively new group with unverified assertions, their activities warrant cautious monitoring and thorough investigation by cybersecurity experts and relevant authorities.

## Recommendations

Given the speculative nature of Hunt3r Kill3rs' claims, organizations should:

- Maintain heightened vigilance and threat intelligence monitoring without overestimating unverified threats.
- Conduct rigorous assessments and forensic analysis to validate alleged incidents and assess actual risks.
- Enhance collaboration and information sharing within the cybersecurity community to collectively address emerging threats.
- Stay informed about evolving tactics and techniques employed by threat actors to adapt defensive strategies accordingly.

Finally, it should not be forgotten that operations operating under the name of “hacktivism” can be a screen for more dangerous cyber operations, or individual small actions of these groups can cause devastating consequences when they act together.

Therefore, this analysis serves as an initial assessment and encourages a balanced approach in evaluating emerging cybersecurity threats like Hunt3r Kill3rs.

## The Ultimate Dark Web Compass

Meet the Dark Web Search Engine by SOCRadar, often referred to as the “Google of the Dark Web.” This tool is your ultimate guide for navigating the hidden corners of the internet. With state-of-the-art search algorithms and highly customizable news feeds tailored to your industry or region, it reveals potential threats with pinpoint accuracy. Think of it as your advanced radar, scanning the digital landscape and enabling your organization to identify and neutralize risks before they breach your defenses.

**Dark Web News:** Receive curated news feeds that provide industry-specific or country-specific intelligence exactly when you need it.

**Dark Web Search:** Effortlessly search for keywords, IP addresses, emails, domains, hashes, and URLs to conduct efficient and effective threat hunting.

---