Cyber Insight

Hunt3r Kill3rs Group

aka: Hunter-Killers

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

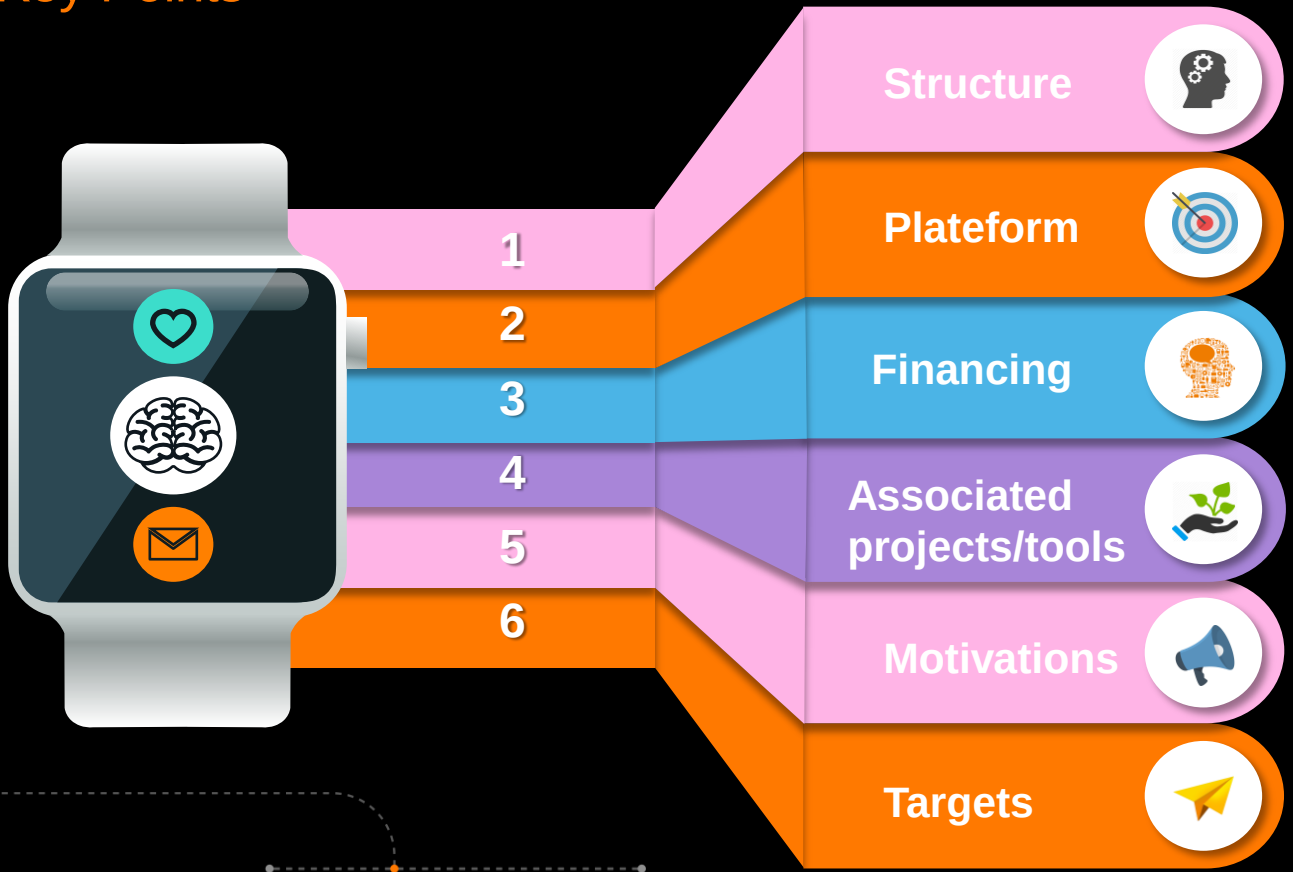
The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

Hunt3r-Kill3rs Group « aka Hunter-Killers Group »

- Creation date: Start 2024 (not confirmed)
- Strategies : Exploits, Infiltration of industrial control systems (ICS), Disruption of communication networks, Evasion and stealth techniques, CCTV espionage / Stream modifications, Coalitions with other groups
- Motivation: multiple and complex connections with Russia and the Middle East, mixture of ideological convictions, geopolitical objectives and financial interests
- Geopolitics: supports Russia and some Middle Eastern countries, notably Iran, while opposing the West, particularly the United States and Israel.
- Characteristics: hybrid strategies, combining geopolitical, ideological and financial objectives using sophisticated attack techniques
- Sectors: Energy (nuclear), ICS, Telecom, IP communications, video surveillance systems (CCTV)

Identification

Key Points



A decentralized and collaborative structure (coalitions with Cyber Army of Russia may have links to Iranian APT groups)

Multiple secure and heterogeneous communication platform uses

Adopts a hybrid financial model, combining ransoms, collaboration with other groups, and the sale of stolen information on the dark web

Uses a wide range of tools and techniques such as exploits, process injection techniques, and ICS perturbations.

Motivated by geopolitical objectives, in response to conflicts specifically targeting Israel and its allies

Critical infrastructure : industrial control systems (ICS), vital sectors such as energy, IP communications, CCTV streams and physical and cyber security

Credits Orange Cyberdefense

Vectors of Influence

1

"Name and Shame"

This tactic pushes victims to comply with the group's demands to avoid damaging public exposure. The group publishes the names of victims who refuse to pay a ransom to embarrass them and encourage them to pay to avoid further damage to their reputation. This tactic, known as 'name and shame,' is similar to that used by authorities and regulators to enforce compliance.

2

Uncertainty

This strategy sows doubt among the victims, who struggle to assess the true extent of the compromise. This atmosphere of uncertainty contributes to weakening the victims and making them more susceptible to manipulation.

3

Greed

The group exploits greed by promising significant financial gain in exchange for collaboration or sensitive information, including espionage activities. Hunt3r Kill3rs may use this tactic to recruit greedy employees into targeted companies.

4

Egocentrism

Incentives to disclose sensitive information or collaborate with the group. For example, disgruntled employees could be recruited and incentivized to sabotage their company's systems out of revenge or frustration, without measuring the impact of their actions.

5

Frustration

The target group targets individuals who face obstacles that prevent them from achieving their goals, causing them to act irrationally and impulsively. Frustration can prompt victims to make hasty decisions and mistakes that benefit the group.

orange Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1

Hunt3r Kill3rs analyzes the emotional reactions of its victims to refine its manipulation techniques. The group understands how fear, guilt, and uncertainty can influence victims' decisions and exploits these emotions to its advantage.

2

The group spreads fear by using threats and intimidation, compelling victims to comply with their demands. The threats can take various forms, ranging from revealing sensitive information to more direct attacks against critical infrastructure.

3

The group targets victims' emotional weaknesses to destabilize them and increase their dependence. By exploiting sensitive points, Hunt3r Kill3rs undermines the victims' psychological resilience

4

Hunt3r Kill3rs seeks to isolate its victims from their support network to increase their dependence and vulnerability. Professional and Social isolation contributes to creating a sense of helplessness and loneliness in victims.

5

By blaming victims for their own problems, the group strengthens its psychological control and avoids taking responsibility for its actions. This manipulation technique allows the group to maintain a positive image while making victims feel guilty.

6

Hunt3r Kill3rs may use gaslighting to sow doubt in victims by making them question their own perception of reality. The goal is to destabilize the victim by convincing them that their judgments and processes are faulty.

Techniques and Capabilities

- Industrial Control Systems (ICS) Infiltration: Targeting programmable logic controllers (PLCs) to disrupt industrial processes.
- Video Feed Access: Hacking CCTV systems to access video feeds for espionage, obtaining sensitive information, or disrupting surveillance operations.
- IP Telephony System Compromise: Intercepting or disrupting communications.
- ARP Spoofing: Redirecting network traffic to their own machines, allowing them to intercept communications and conduct Man-in-the-Middle attacks.
- Network Traffic Analysis: Using network traffic analyzers to collect sensitive information.
- **Collaborations:**
- Cyber Army of Russia: They collaborate with the Cyber Army of Russia (Народная Кибер Армия), sharing information and resources to conduct larger and more complex attacks.
- Iranian APT Groups: Potential links with Iranian APT groups (such as Cyber Av3ngers), enhancing their ability to carry out even more sophisticated cyberattacks

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

Energy (nuclear)

Industrial manufacturing (PLC)

Communication VOIP

CCTV video stream (stream manipulation)

Content Management System (CMS)

Note

It is crucial to strengthen the security of vital and essential businesses, particularly their industrial control systems and video surveillance, while not neglecting investigations of leaks on the deep web and dark web concerning these sectors of activity

Targeted Countries

South Africa

Russia

United States

Israel

Germany

Ukraine

Iran

Italy

Credits Orange Cyberdefense

The most dangerous hypothesis

The most dangerous hypothesis regarding the Hunt3r Kill3rs group is that it's a sophisticated group with ties to state actors, particularly Iranian, specifically targeting European critical infrastructure.

This hypothesis is based on several elements:

- The group primarily targets Industrial Control Systems (ICS) and Operational Technology (OT), which are crucial for the functioning of critical infrastructure.
- They have demonstrated advanced capabilities in exploiting vulnerabilities in industrial systems from recognized brands such as Siemens and Unitronics.
- Potential links have been established with the Iranian group Cyber Av3ngers, known for targeting critical infrastructure.
- They have claimed large-scale attacks, notably against Unitronics Programmable Logic Controllers (PLCs) in Italy.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

orange™ Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense