Cyber Insight

Sector 16 Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

orange Cyberdefense

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

Credits Orange Cyberdefense

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.

Credits Orange Cyberdefense

Sector 16 Group

- Creation date: active since January 2025
- Probable Origin: Due to the group's decentralized organization, it is impossible to confirm its origins but seems to have links with Russia.
- Main strategies:
  SECTOR16 adopts a strategy aimed at exposing abuses of power and corruption by carrying out targeted cyber attacks.
- Geopolitical Motivation:
  SECTOR 16 primarily targets US oil infrastructure, suggesting a geopolitical motivation related to control of energy resources. Some of their targets seem to indicate opposition to major world powers (such as the United States, Russia or the European Union).
- Characteristic:
  Use of advanced techniques to infiltrate and manipulate targeted systems, including exploitation of vulnerabilities, social engineering, manipulation of control interfaces, and data exfiltration
- Targeted business sectors:
  Sector 16 primarily targets oil and gas infrastructure, focusing on compromising SCADA systems and control panels of oil production facilities

Identification

Credits Orange Cyberdefense

Sector16 Group: Main collaborating groups

The main groups collaborating with Sector 16 are Z-Pentest and OverFlame

- **Z-Pentest:**

Sector 16 emerged by collaborating with Z-Pentest, a cybercriminal group known for its attacks against Western critical infrastructure, particularly in the water and energy sectors.

Together, they conducted an attack against a SCADA system managing oil pumps and storage tanks in Texas.

- **OverFlame:**

Sector 16 formed an alliance with OverFlame, another hacktivist group.

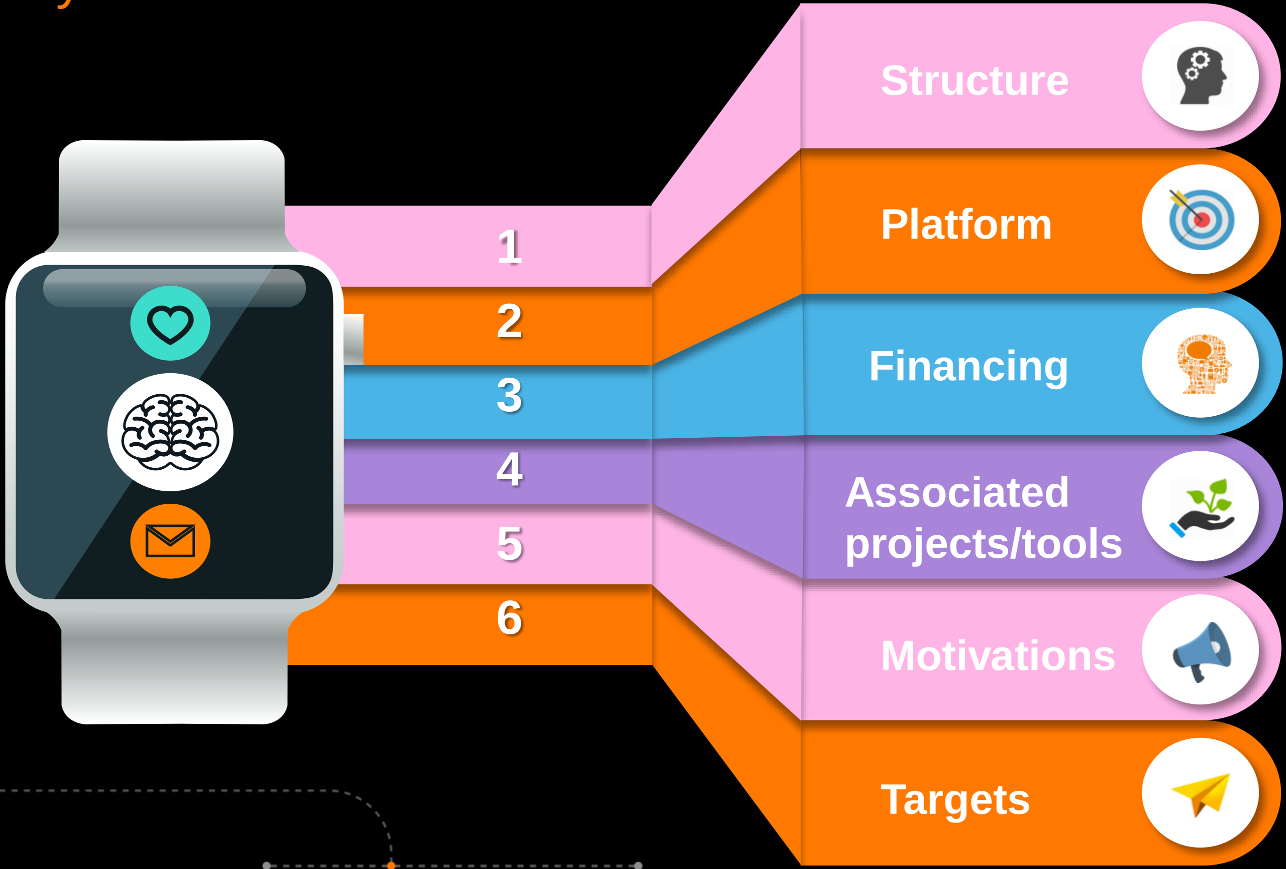
This collaboration increases their ability to conduct more sophisticated and large-scale cyberattack campaigns.

OverFlame has claimed to have an alliance with the DDOSia attack toolkit.

OverFlame claims to be allied with other pro-Russian hacktivists such as Cyber Army of Russia and CyberDragon.

Credits Orange Cyberdefense

Key Points



Structure

The structure of Sector 16 is defined by a collaborative approach, the group made a name for itself by joining forces with Z-Pentest and later forged an alliance with OverFlame.

Platform

Telegram as a communication platform, but also other platforms such as Youtube and darknet private forums.

Financing

Come from donations and crypto funding, and from the sale of leaks obtained during their attacks but also underground crowdfunding platforms

Associated projects/tools

SCADA exploits, network and vulnerability scanners, exploit frameworks, tools for Modbus / DNP3

Motivations

A combination of geopolitical objectives supporting Russia, along with a desire for propaganda and influence, aims to demonstrate technological superiority through sophisticated cyberattacks on critical infrastructure.

Targets

Oil, Gas, Water Treatment and Systems

Credits Orange Cyberdefense

Vectors of Influence

1

Technological Disruption

SECTOR 16 launches sophisticated cyber attacks on critical infrastructure, such as power grids and financial systems, causing widespread outages and economic turmoil. Their actions disrupt daily life and undermine confidence in national security, forcing governments to allocate significant resources to cyber defense.

2

Propaganda

Through coordinated disinformation campaigns, SECTOR 16 manipulates public opinion and sows discord within societies, influencing political outcomes and destabilizing democratic processes. Their propaganda efforts amplify existing societal divisions, creating an environment of mistrust and confusion.

3

Innovation

SECTOR 16 continuously develops innovative tactics not only increase the success rate of their attacks but also inspire other groups to adopt similar methods, amplifying their influence. SECTOR 16 is constantly searching for advanced techniques to infiltrate control systems, particularly SCADA systems in the oil and gas sector.

4

Strategic Alliances

By partnering with other hacktivist groups and criminal organizations, SECTOR 16 gains access to advanced tools and intelligence, enhancing their operational capabilities.

5

Psychological Impacts

High-profile attacks by SECTOR 16, such as industrial system penetrations, create a sense of vulnerability and fear among the public and policymakers. This psychological warfare erodes trust in industries and can lead to policy changes or increased surveillance, indirectly furthering their goals.

Credits Orange Cyberdefense

Emotional Intelligence

1

Emotional Intelligence in Recruitment: SECTOR 16 taps into recruits’ emotions by emphasizing a sense of belonging and purpose, portraying their mission as a fight against injustices. They use empathetic messaging to connect with marginalized or disillusioned individuals, making them feel understood and valued.

2

Cognitive Manipulation for Attacks: The group exploits cognitive biases like confirmation bias to strengthen their narrative among supporters and sow doubt in targets. They create cognitive dissonance to confuse targets, reducing their ability to counter attacks effectively.

3

SWICH (Rapid Change Strategy) in Operations: SECTOR 16 adapts swiftly to new cybersecurity defenses, keeping their attack methods unpredictable. This ensures their operations remain effective and challenging for defenders to anticipate.

4

NLP for Propaganda: They use neuro-linguistic programming (NLP) techniques in propaganda to subtly shape public perception and behavior. Carefully chosen language and imagery create emotionally and cognitively resonant narratives.

5

Exploiting Intellectual Vulnerabilities: SECTOR 16 targets individuals or systems with limited cybersecurity knowledge to gain access or spread misinformation. Social engineering tactics exploit these weaknesses to meet their goals.

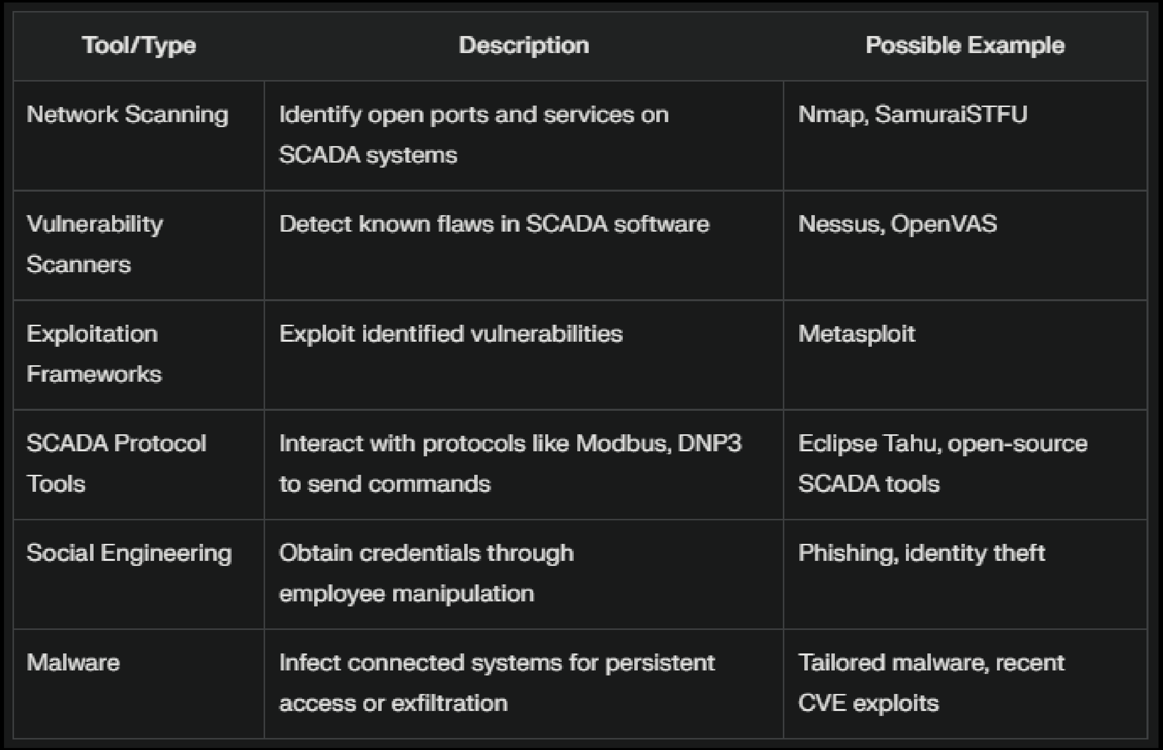
6

Triggering Emotional Responses in Attacks: During attacks, cybercriminals exploit emotions such as fear or urgency to manipulate victims into making hasty decisions or divulging sensitive information. This tactic bypasses victims' logical decision-making processes, making them more vulnerable to manipulation.

orange Cyberdefense

Credits Orange Cyberdefense

Tools Used



Tool/Type	Description	Possible Example
Network Scanning	Identify open ports and services on SCADA systems	Nmap, SamuraiSTFU
Vulnerability Scanners	Detect known flaws in SCADA software	Nessus, OpenVAS
Exploitation Frameworks	Exploit identified vulnerabilities	Metasploit
SCADA Protocol Tools	Interact with protocols like Modbus, DNP3 to send commands	Eclipse Tahu, open-source SCADA tools
Social Engineering	Obtain credentials through employee manipulation	Phishing, identity theft
Malware	Infect connected systems for persistent access or exfiltration	Tailored malware, recent CVE exploits

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

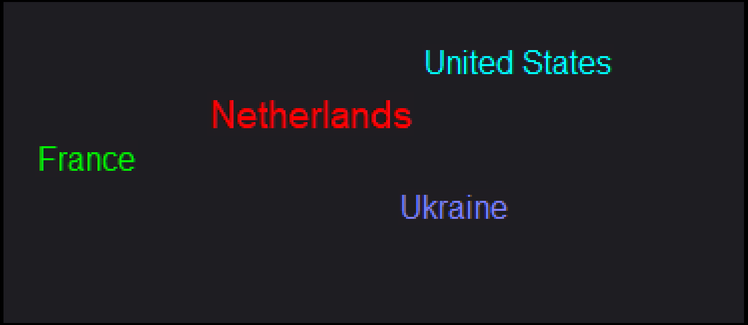
- Oil
- Gas
- Water Systems
- Water Treatment

Note

SECTOR16 has confirmed targets in the United States and a claimed target in the Netherlands (via Arionex Water Treatment), with possible expansion to other European countries like France and Ukraine based on allied activities. Their focus on critical infrastructure underscores the need for heightened cybersecurity measures in affected regions, particularly given their recent formation.

Credits Orange Cyberdefense

Targeted Countries



United States

Netherlands

France

Ukraine

Credits Orange Cyberdefense

Most Likely Hypothesis

Targets:

- Oil and gas facilities: Pipelines, refineries, and distribution networks, given their prior attacks on US oil infrastructure.

- Water treatment plants: Municipal water systems, as evidenced by their claimed breach of Arionex Water Treatment.

Methods:

- SCADA system hacks: Exploiting vulnerabilities in industrial control systems to manipulate operations, a technique they’ve demonstrated proficiency in.

- Social engineering: Phishing or pretexting to gain initial access to networks.

- DDoS attacks: Overwhelming targeted systems to disrupt availability of services.

- Malware deployment: Installing malicious software for data theft, persistence, or operational interference.

Impacts:

- Operational disruptions: Shutdowns of critical systems, such as oil pumps stopping or water treatment processes failing.

- Reputational damage: Public exposure of sensitive data or defacement of websites to undermine trust in targeted entities.

Credits Orange Cyberdefense

The most dangerous hypothesis

Targets:

• Nuclear power plants: Facilities with potential for catastrophic consequences if compromised.

• Healthcare systems: pharmaceutical supply chains critical to public safety.

• Transportation infrastructure: Air traffic control, rail networks, or shipping logistics, vital for societal function.

Methods:

• Coordinated multi-sector attacks: Simultaneous strikes across industries to overwhelm response capabilities.

• Collaboration with state actors: Leveraging sophisticated tools or intelligence from pro-Russian entities.

• Advanced persistent threats (APTs): Long-term infiltration for sabotage or espionage, using highly tailored malware or exploits.

•Impacts:

• Loss of life: Fatalities from compromised healthcare systems, transportation accidents, or nuclear incidents.

• Catastrophic physical damage: Environmental disasters or infrastructure failures with widespread consequences.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

Cyberdefense

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

Credits Orange Cyberdefense