Cyber Insight

Z-PENTEST ALLIANCE

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

Z-PENTEST ALLIANCE

- Creation date: first appeared in October 2023

- Probable Origin: Serbia but close ties to pro-Russian actors

- Main strategies:
  The Z-Pentest group is distinguished by its ability to penetrate operational control systems (OT) in critical infrastructures.

- Geopolitical Motivation:
  Z-Pentest's attacks aim to weaken industrial and control systems (ICS/SCADA) in Western countries, thereby strengthening Russia's geopolitical influence by exploiting the technological vulnerabilities of its enemies.

- Characteristic:
  The Z-Pentest group is characterized by its ability to penetrate operational control systems (OT) in critical infrastructures.

- Targeted business sectors:
  Z-Pentest mainly targets the energy (oil and gas) and water sectors.

Identification

Cyberdefense

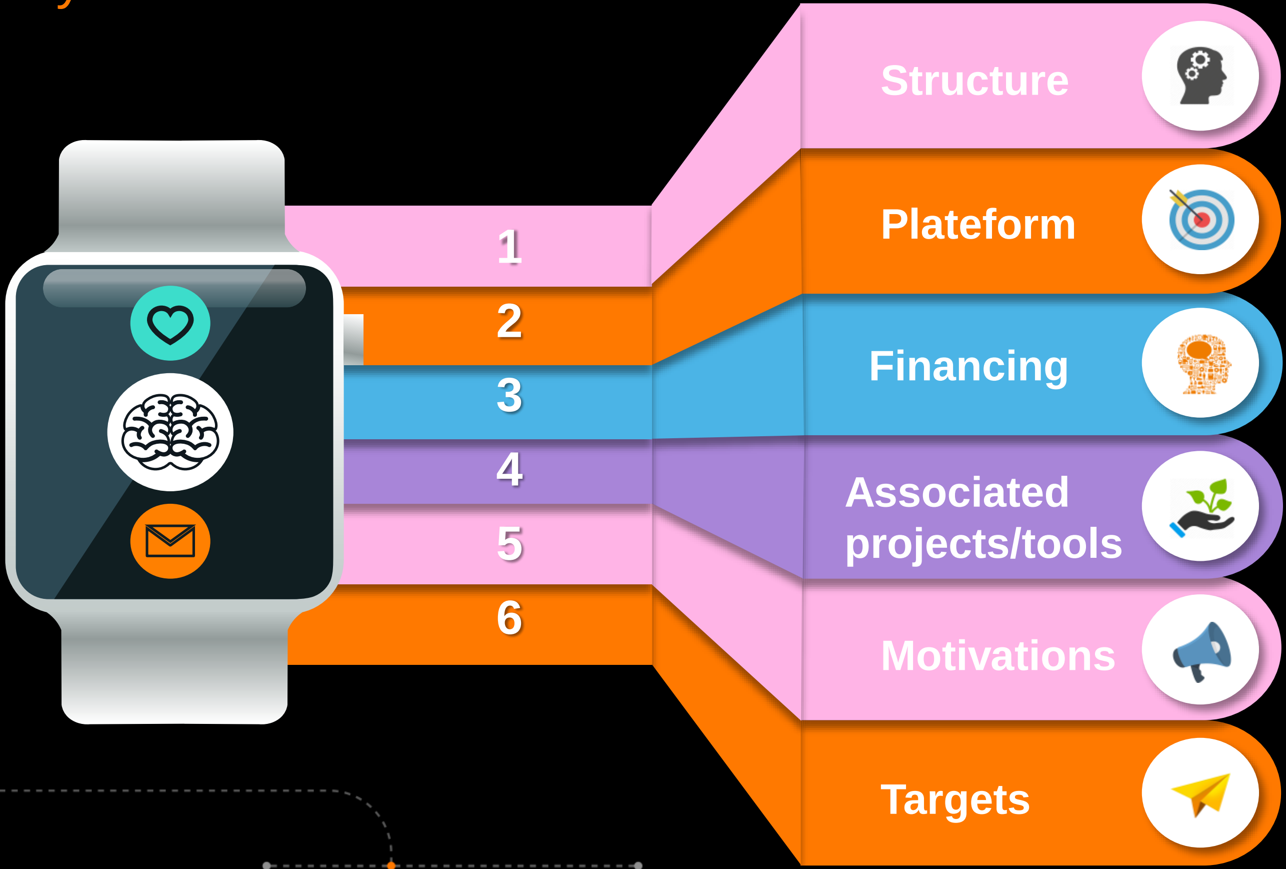
Credits Orange Cyberdefense

Z-PENTEST ALLIANCE: Main collaborating groups

- SECTOR16
- OverFlame
- Pro-Palestine Hackers Movement (PPHM)
- People’s Cyber Army (PCA)
- NoName057(16)
- KillNet
- Anonymous Russia
- Cyber Army of Russia Reborn
- XakNet Team
- From Russia with Love (FRwL)
- Volt Typhoon
- Cyb3r Dragonz
- ByteBlitz

Credits Orange Cyberdefense

Key Points



Structure

Decentralized operation. Its members remain anonymous and its organization is fluid, making its identification and tracking difficult for authorities

Plateform

Coordination of attacks on Telegram and Private Forums. Propaganda, amplification of the impact of its operations and influences on X (Twitter)

Financing

Sale of access to industrial systems, zero-day vulnerabilities on the dark web. Funding by state or non-state third parties (unconfirmed)

Associated projects/tools

Developing tools to penetrate operational control systems (OT) in the energy and water sectors. They exploit vulnerabilities in ICS/SCADA systems

Motivations

Z-Pentest also seeks to weaken Western solidarity and create divisions within NATO through its actions..

Targets

The energy and water sectors with manipulation of critical functions such as water pumping, gas and oil distribution management

Credits Orange Cyberdefense

Vectors of Influence

1

Sabotage

Z-Pentest targets the energy (oil and gas) and water sectors, disrupting critical systems like oil wells and water treatment plants.

2

Mobilization

The group uses platforms like Telegram and X to communicate with their supporters and recruit new members, offering a certain level of anonymity and security.

3

Psychological exploitation

Z-Pentest members may be influenced by cognitive biases, such as confirmation bias or optimism bias, which may lead them to overestimate their abilities or ignore the negative consequences of their actions.

4

Intimidation

Z-Pentest releases videos showing manipulations of operational control (OT) systems to instill fear and reinforce their image as a formidable group.

5

Manipulation

Z-Pentest uses disinformation campaigns to influence public opinion and spread their political message, exploiting social networks and forums to propagate narratives aligned with their goals.

Credits Orange Cyberdefense

Emotional Intelligence

1 Exploitation of Fear and Uncertainty:
Z-Pentest releases videos showing their access to critical systems to instill fear and uncertainty in their victims, pushing them to react impulsively or disclose sensitive information.

2 Manipulation of Cognitive Biases:
The group exploits victims' overconfidence in their security systems, leading them to underestimate risks and facilitating intrusions.

3 Use of Emotional Intelligence to Strengthen Alliances:
Z-Pentest shares evidence of successful attacks with its allies, building trust and motivation within their alliances through emotionally engaging communication.

4 Manipulation of Vulnerability Perceptions:
By targeting critical infrastructure like water and energy systems, Z-Pentest amplifies victims' perception of vulnerability, prompting disorganized reactions or negotiations.

5 Influence Perceptions:
The group disseminates selective or manipulated information to influence the perceptions of victims and allies, crafting a narrative favorable to their objectives.

6 Strengthening Cohesion Through Shared Goals
Z-Pentest aligns its actions with the geopolitical objectives of its allies, such as supporting Russia, thereby reinforcing cohesion and motivation within their alliances.

Cyberdefense

Credits Orange Cyberdefense

Techniques and Capabilities

Z-Pentest accesses and manipulates SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems), demonstrating their ability to cause major disruptions in critical infrastructure.

Z-Pentest infiltrates operational control systems (OT) to manipulate critical functions such as water pumping, gas flaring, and oil collection, demonstrating their ability to disrupt industrial infrastructure.

Z-Pentest exploits zero-day vulnerabilities to access critical systems, often using information obtained from the dark web or through collaboration with other groups.

The group specifically targets the energy, water, and oil sectors, disrupting operations and threatening the national and economic security of targeted countries.

Z-Pentest employs social engineering techniques to obtain sensitive information or system access by exploiting trust or human error.

The group uses information obtained from data leaks on the dark web to prepare and execute larger, more targeted attacks.

The group often works in tandem with groups like SECTOR16, OverFlame and People's Cyber Army (PCA) to coordinate attacks and share resources, thereby increasing their effectiveness.

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

Energy sector

Water and wastewater sector

Critical infrastructure

Industrial sector

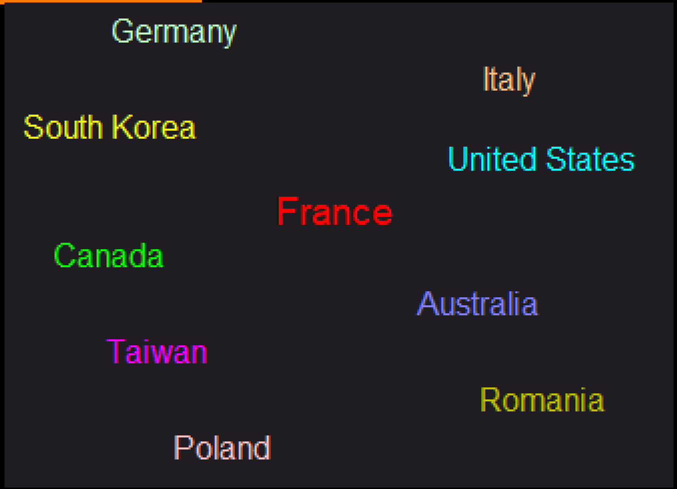
Oil sector

Note

A future target of Z-Pentest should remain highly vigilant and strengthen its cybersecurity measures, as the group frequently targets critical infrastructure with sophisticated attacks. Enhanced monitoring, regular audits, and incident response preparedness are crucial to mitigate risks and limit potential impacts.

Credits Orange Cyberdefense

Targeted Countries



Germany

Italy

South Korea

United States

France

Canada

Australia

Taiwan

Romania

Poland

Credits Orange Cyberdefense

The most dangerous hypothesis

Coordinated Cyberattacks on Energy Grids: During periods of heightened tension with Russia, Z-Pentest and its allies could launch coordinated attacks on European energy grids, causing widespread blackouts and disrupting essential services.

Coordinated Cyberattacks on water/oil sectors: Z-Pentest and its allies could disrupt water, gas, and oil distribution systems, causing service interruptions.

Exploitation of Zero-Day Vulnerabilities: The group may exploit unknown vulnerabilities in critical infrastructure systems to inflict significant damage, potentially leading to prolonged disruptions in key sectors.

Collaboration with State-Sponsored Actors: Z-Pentest could collaborate with state-sponsored entities to execute more sophisticated and impactful cyber operations, increasing the scale and sophistication of attacks.

Insider Threats: Collaborators within organizations could facilitate attacks by providing insider access, enhancing the impact and reach of cyber operations.

Wiper Malware on Critical Infrastructure: Z-Pentest might deploy targeted wiper malware on critical infrastructure, causing significant operational disruptions.

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