

Cyber Insight

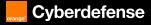
TWELVE Group

Cyber Intelligence Bureau

a division of Epidemiology Labs



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



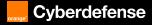


Methods & Neutrality

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.



TWELVE Group

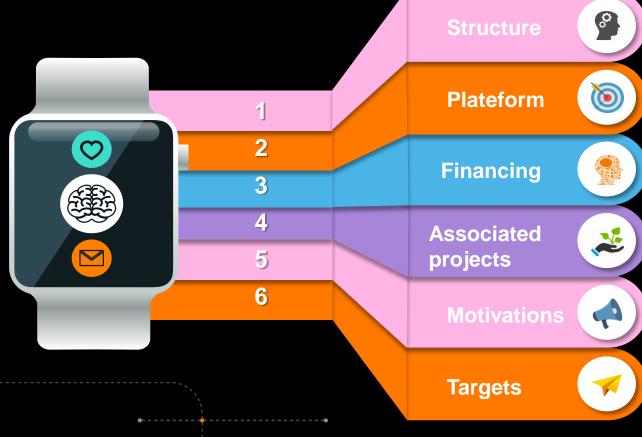
- Creation date: emerged in April 2023 (not confirmed)
- Strategies : Wiper, Ransomware, DDoS, Exploits, Data exfiltrations Coalitions with other groups
- Motivation: pro-ukrainian hacktivist group, motivated by the maximum damage to Russian organizations
- Geopolitics: opponent of Russia's regime and its policies
- Characteristics: moves laterally across networks to steal data and establish persistence
- Sectors: government organizations, telecommunication, energy



Identification



Key Points



A decentralized and collaborative structure

Multi-directional communications, with autonomous cells and multiple contact points on multiple secure and heterogeneous platforms

Independent financing (unconfirmed state sponsorship), with other Groups (coalitions), leaks and ransomwares

Open source tools, malware, ransomware, VPN, Exploits, Wipers, web shells

Motivated by hacktivist goals, seeking to inflict maximum damage on Russian organizations in response to the war in Ukraine

Mainly targets Russian and pro-Russian companies and government organizations

Cyberdefense

Vectors of Influence

Digital chaos

The digital chaos

generated by the

characterized by their

strategy of encrypting

infrastructure, aiming

to inflict maximum

seeking financial gain.

group Twelve is

victims' data and

subsequently

destroying their

damage without

Cyberresistance

The group uses sensitive information leak operations, which it then shares on certain deepweb and darknet platforms. It exposes compromising and sensitive information including phone numbers of Russian entities, thus influencing public opinion and potentially political decisions related to the Russian-Ukrainian conflict.

Cyberdefense

Democratization cyber threat

Twelve uses a set of widely available tools. The group appears to use no tools of its own creation, nor any proprietary ones, and relies solely on a modifiable public arsenal.

Credits Orange Cyberdefense

an approach that aligns with a broader trend of information warfare. It exfiltrates sensitive information from its victims and publishes it on the deep web/darknet to publicly discredit them and sow geopolitical discord

The group employs

Information warfare

Dark alliances

The group Twelve has

particularly through its

similarities with the

ransomware group.

The act of exfiltrating

sensitive information

raises concerns about

its dissemination, as it

may facilitate further

criminal activities

been observed to

connections with

organized crime,

have potential

DARKSTAR

Emotional Intelligence

The destructive actions of TWELVE, aimed at causing maximum damage without regard for human and economic consequences, suggest a lack of perception of emotions and the impact on affected individuals

The group demonstrates selfmanagement by maintaining control and ensuring that its actions remain strategic and calculated rather than impulsive

Twelve shows social awareness by recognizing the sentiments and reactions of the public and its adversaries, which helps it tailor its messaging and operations to maximize impact



Credits Orange Cyberdefense

The group influences public opinion through carefully organized leaks of sensitive information that resonate with the emotions of its audience

TWELVE exploits emotions, including understanding fear and anger, to manipulate public opinion, stir up tensions and weaken support for the Russian regime

Twelve's ability to manage conflict is evident in how they tactfully navigate tensions between various factions involved in the cyber landscape, aiming to create divisions among their adversaries while rallying support for their cause

6

Cyberdefense

Methods, Tools and services used



- Cobalt Strike: allows for command and control (C2) operations and is often used for lateral movement within networks.
- Mimikatz: A tool used for credential theft, enabling attackers to extract plaintext passwords, hash, PIN codes, and Kerberos tickets from memory.
- Chisel: A tunneling tool that allows for HTTP and TCP tunneling through a single outbound connection, facilitating remote access.
- BloodHound: Analysis Active Directory environments, helping attackers visualize relationships and paths for privilege escalation.
- PowerView: used for network and domain reconnaissance, allowing attackers to discover domain users and permissions.



Methods, Tools and services used



- CrackMapExec: A post-exploitation tool that helps automate the assessment of large Active Directory networks, enabling credential dumping and lateral movement.
- Advanced IP Scanner: used to identify devices on a local area network (LAN), aiding in reconnaissance efforts.
 - PsExec: allows execution of processes on remote systems, facilitating lateral movement and command execution.
- Web Shells (e.g., WSO): Malicious scripts deployed on compromised web servers to execute commands.
- FaceFish Backdoor: A specific backdoor used in attacks that exploits vulnerabilities in VMware vCenter servers.



Professional Sectors

List of targeted sectors

Government

Defense

Customs Service

Critical infrastructure (hydraulic systems)

Financial sector

Telecommunications

Industry

Logistics

Energy



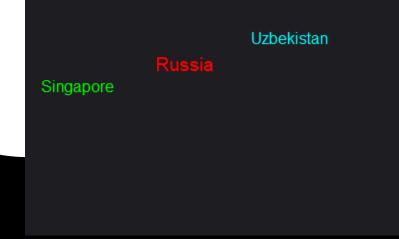
Note

The evolution of its targets, tactics and links with other groups and coalitions will have to be closely monitored depending on geopolitical situations.

Cyberdefense



Targeted Countries







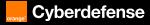
The most dangerous hypotheses

Based on the evolving geopolitical landscape in Europe and around the world, we can make certain hypothetical observations.

It is conceivable that Twelve could expand its targets directly to NATO countries to include organizations and critical infrastructure in those nations, namely:

- Governments: targeted for symbolic reasons
- Defense: organizations involved in the production and supply of weapons and military equipment to Ukraine
- Logistics: transportation of military and humanitarian aid

• Energy: organizations with vital needs to maintain national security and economic stability of the countries





Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society



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