



Cyber Insight

UserSec
aka: UserSec Team

Cyber Intelligence Bureau

a division of Epidemiology Labs

 Cyberdefense

 Cyberdefense



Methodology & 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 insight is analysis from a strictly cyber perspective.

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

UserSec

- Creation date: Formed in 2022, active since January 2023 (Unconfirmed)
- Strategies: Specialized in the analysis of exfiltrated data and image/photo analysis – Social engineering – Account compromises – Vulnerability exploits – DDoS attacks
- Motivation: Geopolitical, pro-Russian – financial (second plan) – Strong partnerships with other groups
- Characteristics: Ideological and financial threats, targeting of critical infrastructures, possible nation-state links
- Sectors: State organizations and defense, Financial organizations, transport, energy, health
- Funding: Sale of training, hacking services and correlations and interpretations of stolen data DDOS partnerships on the dark web - Russian state sponsor links



Identification

Coalitions



NoName(057)16

Cyber Army of Russia

Anonymous Russia

Killnet

Anonymous Sudan

Overload (service DDoS-as-a-Service)

Key Points



1

Structure



Decentralized organizational structure and collaborations

2

Platform



Telegram, private darknet forums with messengers, TOR, VPN

3

Financing



Ideological, state funding, training, partnerships

4

Tools



Remote Access Trojan, Botnets, Vulns Tools, SQLExploits, CMS

5

Motivations



Reputation, Notoriety
Geopolitics Support Russia and instrumentalization of the Israeli-Palestinian conflict

6

Targeting



Targeting many sectors of activity within NATO

Vectors of Influence

1

Ideology

Russian Nationalist Ideology: UserSec Seeks to Promote Russia's Geopolitical Interests

2

Resistance

The group actively targets countries and organizations supporting Ukraine and Israel

3

Collaboration / Coalition

UserSec partners with other groups that share similar goals to increase its impact. These collaborations and/or coalitions allow for the study and sale of correlated target data, accounts, vulnerabilities

4

Strategies

UserSec takes advantage of international crises, such as the Israeli-Palestinian conflict, to justify its attacks and rally support while maintaining pro-Russian propaganda.

5

Ideology

The group uses Telegram to spread propaganda, recruit new members and coordinate attacks, but uses private messaging on darknet forums to strategize targets.

Emotional Intelligence on Victims and Attackers subscribed to UserSec

1 Fear Exploitation: UserSec disrupts essential services, creating a sense of insecurity and vulnerability

2 Diffusion of anger and frustration: The group exploits social and political tensions to stir up anger against governments and institutions

3 Provocation and Humiliation: UserSec group attacks aim to humiliate victims and undermine their credibility with announcements and leaks of relevant and correlated stolen data.



4 Perception Manipulation: UserSec uses disinformation and propaganda to influence public opinion and sow doubt

5 Hate speech: UserSec stirs up anti-Western sentiment and encourages hatred towards countries supporting Ukraine

6 Ego Exploitation: Group flatters Russian and anti-NATO hackers' sense of activism to entice them to join their ranks

Tools and services

Proposals and sales of services:



DDoS-as-a-Service Services: Promoting OverLoad (DDoS service via IoT botnets)

DDoS amplification tools

Selling hacking training

Vulnerability and exploit analysis tools

SQL injection tools

Content exploitation kits (CMS)

Remote access tools

Obfuscation tools

Correlations and analysis of exfiltrated document containers

OVERLOAD

Professional sectors

List of targeted sectors

- Government and administrations
- Transportation (air, rail, road, public)
- Health services
- Education
- Defense
- Banking and financial services
- Retail trade
- Agri-food
- Culture and entertainment
- Research
- Justice
- Diplomacy
- Energy
- Media and audiovisual
- Technologies
- Tourism
- Construction
- Consulting
- Insurance



NOTE

The impact of UserSec on its victims is its ability to exploit geopolitical and social tensions. UserSec uses disinformation and provocation tactics to stir up fear, anger and division among the population and to question trust in institutions and companies.



Targeted countries

France
United-Kingdom
Egypt NATO Kenya
India Italy United-States
Latvia
Germany

The most dangerous hypotheses

Industrial: Supply chain compromise: UserSec could infiltrate the networks of companies supplying software or hardware to industrial infrastructure. The aim would be to introduce backdoors or malware into systems before their deployment in critical infrastructure, allowing UserSec to carry out stealthy and large-scale attacks.

Government and administrations: Symbolic targets to demonstrate the scope and impact of the attacks

Transportation: Sow chaos and disrupt the economy by targeting air, rail and maritime transport

Health services: Create panic and undermine public confidence by disrupting hospitals and emergency services.

Damage to France's image: Successful and publicized cyberattacks against French infrastructure could harm France's image and credibility on the international stage, particularly in terms of cybersecurity and resilience to cyber threats



Cyber Intelligence Bureau

a division of Epidemiology Lab

Build a safer digital
society