

Cyber Insight

UserSec aka: UserSec Team

Cyber Intelligence Bureau

a division of Epidemiology Labs







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.

© Orange Cyberdefense



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



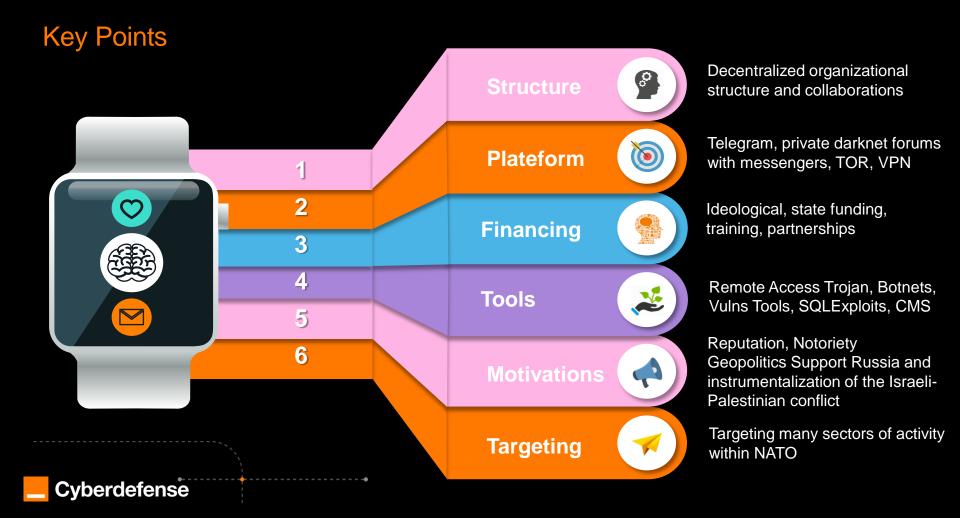
Identification

Coalitions



NoName(057)16

- Cyber Army of Russia
- Anonymous Russia
 - Killnet
- Anonymous Sudan
- Overload (service DDoS-as-a-Service)



Vectors of Influence

Ideology

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

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

Resistance The group actively targets countries and organizations supporting Ukraine and Israel that sh goals to i imp coll and/o allow for correl data

4

Ideology

The group uses

Telegram to spread

propaganda, recruit

new members and

coordinate attacks,

but uses private

darknet forums to

strategize targets.

messaging on

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.

Cyberdefense

Emotional Intelligence on Victims and Attackers subscribed to UserSec

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

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

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

Cyberdefense



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

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

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

6

Tools and services



Cyberdefense

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 © Orange Cyberdefense



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

Cyberdefense



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 Latvia Germany



© Orange Cyberdefense

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

© Orange Cyberdefense

Cyberdefense



Cyber Intelligence Bureau

a division of Epidemiology Lab

Build a safer digital society



© Orange Cyberdefense