Cyber Insight

CyberVolk Team

Cyber Intelligence Bureau

a division of Epidemiology Labs

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.

CyberVolk Team

- Creation date: It initially operated under the names GLORIAMIST India and Solntsevskaya Bratvaand and was formed in March 2024. The group then adopted its current name, CyberVolk, in May 2024. CyberVolk launched its Ransomware-as-a-Service (RaaS) operations and began claiming ransomware victims in June 2024.

- Probable Origin: pro-Russian alignment, but the group may have origins in India (not confirmed)

- Main strategies: Combinations of service disruption, extortion and psychological manipulation techniques.

- Geopolitical Motivation:
  CyberVolk motivates its attacks by exploiting geopolitical tensions and targeting entities that oppose Russia's interests. The group also uses ransomware with fixed ransoms demand to be paid extremely quickly, blurring the line between hacktivism and financial cybercrime.

- Characteristic:
  Hybrid Attacks: The group combines DDoS attacks to initially disrupt targets with ransomware deployments for financial extortion

- Targeted business sectors:
  CyberVolk particularly targets government entities and scientific institutions, but also attacks critical infrastructure, seeking to disrupt essential services.

Identification

CyberVolk embodies a reactionary techno-nationalism that fuses elements of identitarian neo-paganism and anti-globalization struggle. Their vision is based on preserving a 'digital soul of the people' (the Volk), perceived as threatened by globalization, mass immigration, and centralized control technologies (AI, metaverse). Their strategy is a hybrid cultural war aimed at re-establishing a 'rooted' technological sovereignty.

Credits Orange Cyberdefense

CyberVolk Team: Main collaborating groups

The main groups collaborating with CyberVolk are:

NONAME057(16)

LAPSUS$

Moroccan Dragons

Holy League

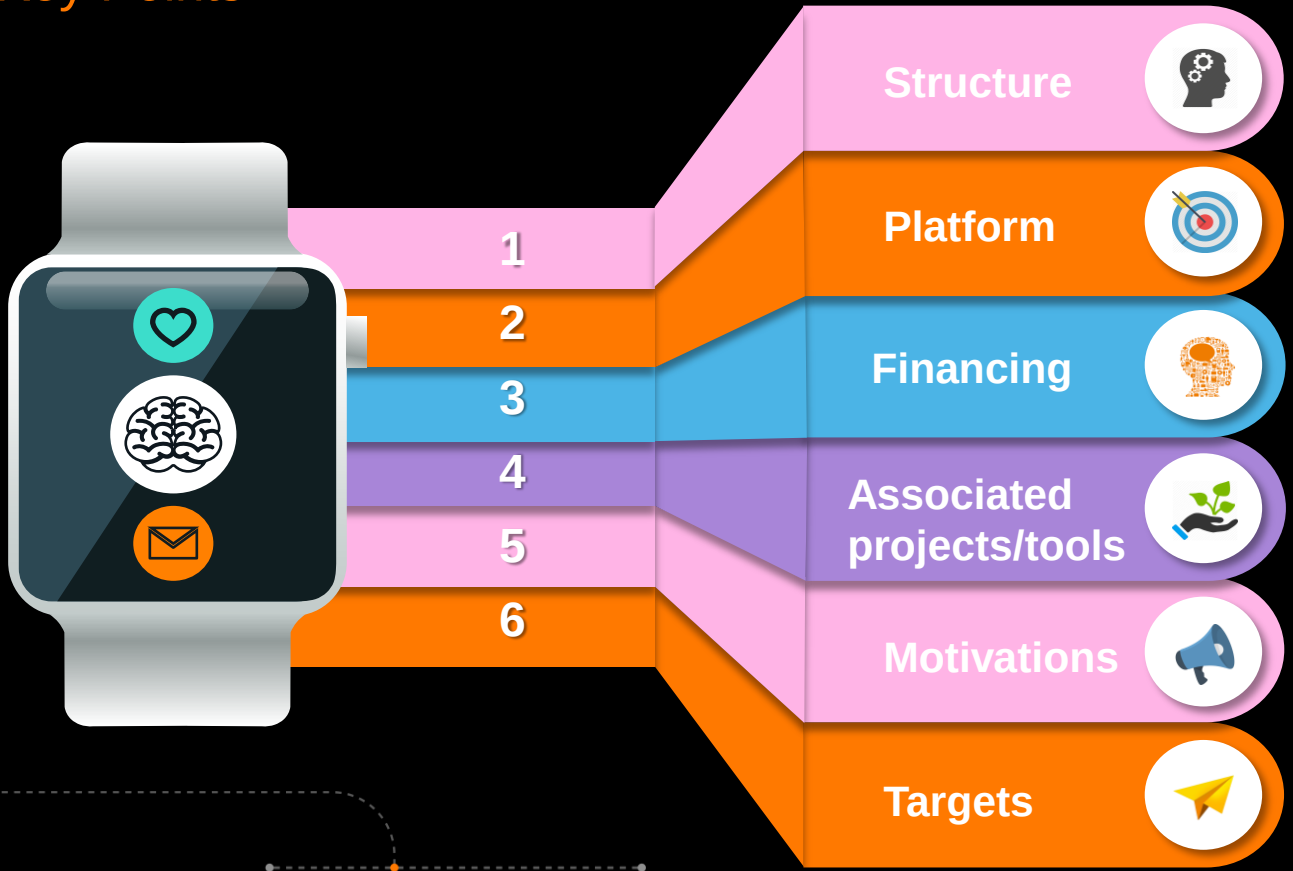
Mr. Hamza

APT 44

The Cyber Hunters

The Golden Society

Key Points



It is characterized by a certain fluidity and a hybrid model combining traditional aspects of hacktivism with a more structured organization centered around its Ransomware-as-a-Service (RaaS) activity

Social medias. The group also conducts internal exchanges using physical dead drop networks in the real world (USB keys installed in building walls)

Revenues generated from ransomware attacks and the RaaS model are the main sources of funding identified for this group.

Many codes used and/or developed by the group for ransomware attacks and their RAAS platform

The group appears to blur the line between politically and financially motivated cybercrime, but ransomware and Ransomware-as-a-Service aspects are identified as the main sources of funding

Gov, critical infrastructure, telecom, scientific research institutions (oceanographic and meteorological) but also those involved in biological, genetic and bioinformatics research

Credits Orange Cyberdefense

Vectors of Influence

1

Adaptability

The group is highly adaptable with a fluid structure allowing rapid changes in their membership and tactics. This flexibility enables them to respond quickly to threats and opportunities in the cyber landscape.

2

Technology

The group excels in developing various malware, including their own ransomware and data stealers. They adapt and evolve their tools, often inspired by other groups, showing a dynamic technological approach.

3

Alliances

They collaborate with other pro-Russian hacktivist groups, like NoName057(16), HolyLeague to amplify their impact. Resource sharing and coordinated attacks enhance their operational capacity.

4

Profitability

Despite their political motivations, CyberVolk engages in cybercrime for financial gains. They demand ransom payments and may sell their ransomware as a service to other actors.

5

Geopolitical Impacts

The group targets entities in countries opposed to Russia, particularly those supporting Ukraine or NATO. Their attacks aim to disrupt these entities to advance Russian geopolitical objectives.

Emotional Intelligence

1 CyberVolk uses hybrid systems to combine structured approaches with adaptive methods (like real-time AI).

2 The group quickly publishes large amounts of hacked data or claims to disorient their targets. This tactic aims to saturate public attention and complicate a rational analysis of their actions.

3 Their communications contain emotionally charged words, such as "freedom" or "justice," repeated to anchor positive associations. This strategy strengthens their image as "heroes" among their supporters.

4 CyberVolk spreads strong, ideologically driven messages to rally sympathizers to their cause. These simplified narratives often exploit confirmation bias to reinforce their audience's beliefs.

5 CyberVolk uses threats of data leaks or visible DDoS attacks to instil fear in their adversaries. These actions create a sense of urgency and powerlessness, amplifying their perceived impact.

6 By combining behavioral data and cognitive analyses, CyberVolk creates detailed psychological profiles of their targets. These profiles are used to tailor their attacks and maximize their emotional impact.

Cyberdefense

Credits Orange Cyberdefense

Tools Used and developed - Services

Tools used by CyberVolk:
- AzzaSec Ransom
- Diamond RW
- Forks of LockBit
- BlackCat
- Chaos
- Fork Low Orbit Ion Cannon (LOIC)
- Botnets
- Fake accounts (social networks)

Tools developed by CyberVolk:
CyberVolk Branded Ransomware (derived from AzzaSec)
- Uses AES-256, RSA-2048, ChaCha20-Poly1305 encryption algorithms
- Anti-analysis techniques (Task Manager monitoring, wallpaper modification, termination of Task Manager and MMC-related processes, anti-debugging, obfuscation)
- Webshells
- CyberVolk Stealer (based on LBX-Grabber)
- Parano Checker
- Parano Stealer
- Custom scripts to exploit vulnerabilities
- R-A-A-S Plateform

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

Government

Critical infrastructure

Telecommunications

Scientific research institutions:

- Oceanographic
- Meteorological
- Biological
- Genetic
- Bioinformatics

Note

CyberVolk is a dangerous pro-Russian hacktivist group due to its extremely rapid and sophisticated strategies. Primarily targeting telecom infrastructure and scientific research institutions, their attacks combine disruptive techniques such as ransomware, DDoS, and espionage through data exfiltration.

Targeted Countries

South Korea
Israel
Venezuela
Armenia
United Kingdom
India
Spain
Japan
France
United States
Italy
Ukraine
Taiwan

Credits Orange Cyberdefense

Most Likely Hypothesis

Targets:

CyberVolk primarily targets organizations and countries perceived as adversaries of their political or national ideologies, such as Japan, Ukraine, Israel, Spain, France and Western nations including the United States and the United Kingdom.
Their targeting strategy prioritizes entities with high media visibility to amplify their political messaging.

Methods:

Their methods include deploying ransomware like AzzaSec Ransom, Diamond RW, Forks of LockBit, Chaos, HexaLocker, and Parano to encrypt victim data even offline, combined with DDoS attacks and mass exfiltration of sensitive data.
They also employ rapid tactical adaptation (SWITCH), cycling through different techniques to evade detection and maximize success rates.

Impacts:

CyberVolk's operations cause significant disruptions to critical corporate and institutional operations, resulting in substantial financial costs for system recovery and loss of public trust.
Additionally, these attacks create a potential chilling effect on free expression and heighten geopolitical tensions among affected nations, amplifying broader social and economic consequences.

Credits Orange Cyberdefense

The most dangerous hypothesis

Targets:

CyberVolk could target critical infrastructure (Telecom, hospitals, power grids) in Western countries or NATO allies, seeking to cause major disruptions and physical damage to extend their geopolitical influence.

Methods:

They could merge devastating ransomware (like AzzaSec) with irreversible data destruction attacks (Wiper), exploiting zero-day vulnerabilities, and collaborate with groups with whom CyberVolk might create alliances to access ultra-secure systems.

Impacts:

CyberVolk's attacks could cause critical operational disruptions, massive financial losses, and threats to national security in targeted countries. These actions could also exacerbate geopolitical tensions.

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