Cyber Insight

EvilNet 2.0 Group

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

EvilNet 2.0 Group

- Creation date: EvilNet 2.0 has evolved its identity over the years. ShadowNet emerged between 2017 and 2019 as the group's supposed origin, focusing at the time on discreet attacks against local servers. DarkPulse marked a shift from 2019 to 2021, as the group transitioned to more visible attacks such as DDoS and data leaks. EvilNet became the official name between 2021 and 2023, representing a period of expansion and more pronounced ideological claims. NetReapers was temporarily adopted from 2023 to 2024, symbolizing their role as 'reapers' of sensitive data following massive leaks. EvilNet 2.0 appeared in 2024, with the return to the original name and the '2.0' indicating a restructuring or a new wave of sophisticated attacks.

- Probable Origin: According to our investigations, the origin of this group appears to align more closely with a transnational structure rather than a single geographic source.

- Main strategies: Hyper-Specific Targeting, Combined Hybrid Attacks, Ransomware, Phishing, Data Theft, DDoS, Zero-Day Exploitation

- Geopolitical Motivation:
  Complex and appear to align with evolving motivations targeting government censorship and mass surveillance. Seeks to provoke systemic crisis to expose vulnerabilities in modern democracies. Focuses on geopolitical adversaries who support or exploit conflicts between nations.

- Characteristic:
  Hybrid Cyberattacks (with Physical Sabotage): EvilNet 2.0 is capable of combining digital attacks with physical sabotage operations, leveraging recruitment capabilities to infiltrate employees within targeted organizations

- Targeted business sectors:
  Government entities, critical infrastructure, Telecom, Healthcare, E-commerce, Entertainment.

Identification

EvilNet 2.0 is a hacktivist group that emerged in 2024, marking a new phase after several name changes since 2017.
EvilNet 2.0 has demonstrated its capacity for sophisticated attacks on critical systems, including those in France during December 2024, accompanied by aggressive declarations.
The rebranding to 'EvilNet 2.0' and its recent organizational restructuring underscore a highly active and dangerous threat actor requiring sustained monitoring

Credits Orange Cyberdefense

EvilNet 2.0 Group: Main collaborating

Alliance

- Holy League

Hacktivist Groups

- Anonymous (Certain non-centralized factions)
- GhostSec

Criminal Groups

- Conti (Conti Leaks)
- LockBit (former contributors/developers)
- REvil (Sodinokibi)
- DarkSide

Underground Networks

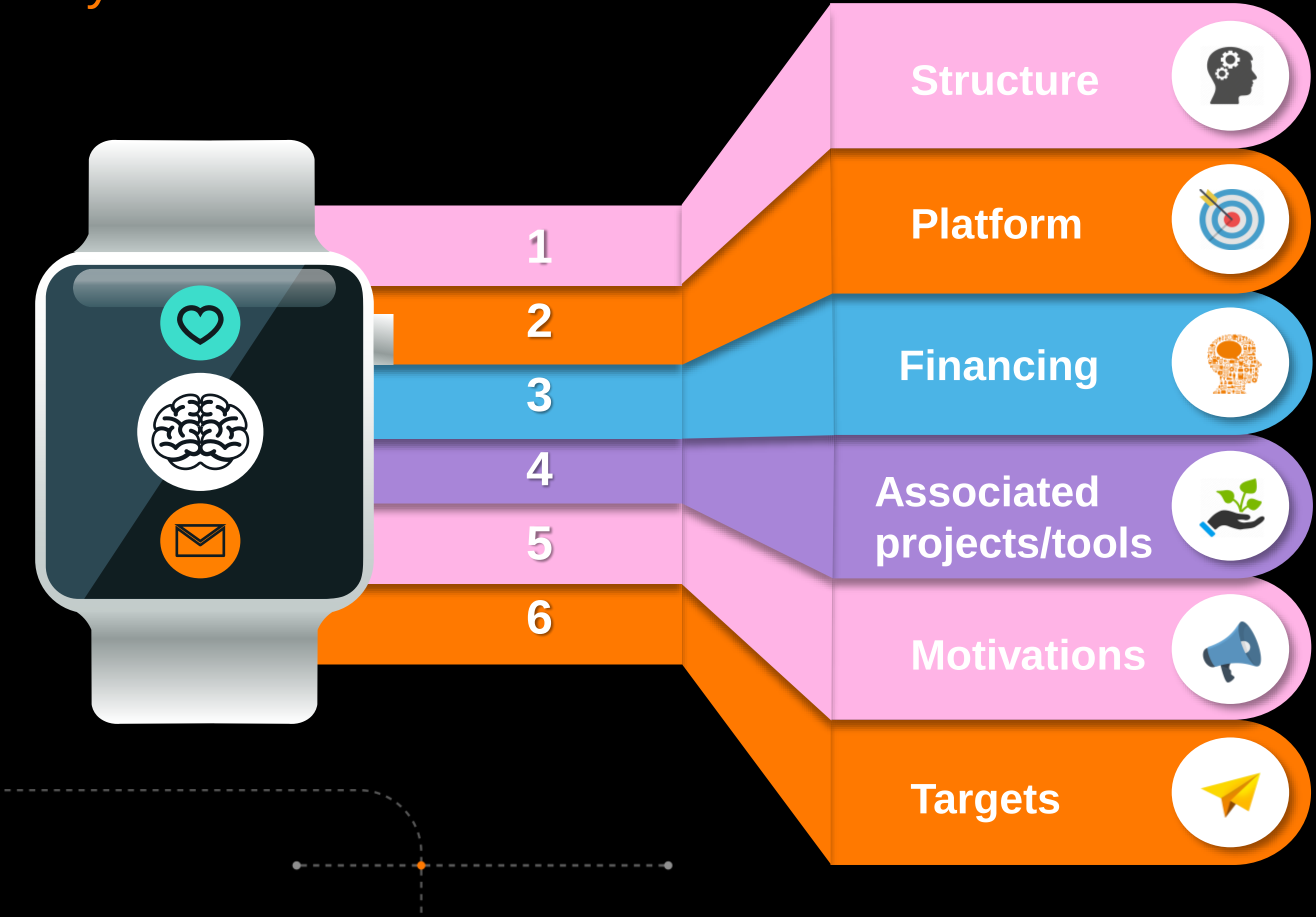
- The Shadow Brokers
- Lapsus$ (employee recruitments)

Independent Hackers and Mercenaries

- Independent hackers
- Cyber-Mercenaries (potentially including the Lazarus Group)

Credits Orange Cyberdefense

Key Points



EvilNet 2.0 operates under a decentralized yet coordinated structure, where members act autonomously while following directives through secure platforms and defined roles.

EvilNet 2.0 uses encrypted networks like Tor and I2P for internal communications and exploits secure channels like Signal and .onion forums for recruitment and coordination.

EvilNet 2.0 primarily funds itself through ransomware, the theft and sale of data, financial fraud, digital extortion.

Variety of tools, including Metasploit, reconnaissance tools, phishing tools and custom ransomwares.

Mix of ideology (fight against oppression, transparency), financial gains through cybercrime, and potentially a desire for geopolitical disruption and demonstrating the vulnerability of systems.

A wide range of sectors, notably healthcare, energy, e-commerce, hospitality, telecommunications, finance, and governmental institutions

Credits Orange Cyberdefense

Vectors of Influence

1 Profitability

Ransomware-as-a-Service (RaaS): The group develops and sells malicious tools such as ransomware, thereby maximizing its revenue.
By offering these services, EvilNet extends its influence by allowing other actors to carry out attacks on its behalf or in collaboration.

2 Alliances

Diverse Strategic Alliances:
EvilNet 2.0 establishes alliances with hacktivist groups, criminals, underground networks and independent hackers.

3 Underground

EvilNet 2.0 collaborates with underground networks such as The Shadow Brokers and Lapsus$. These alliances provide access to advanced hacking tools and stolen databases, enhancing their offensive capabilities and strengthening their coordination with the Holy League.

4 Strategic Targeting

EvilNet 2.0 focuses its attacks on high-impact sectors such as healthcare, finance, and energy.
By targeting these critical infrastructure systems, the group maximizes its economic disruption and media visibility

5 Geopolitical Impacts

EvilNet 2.0 leverages international conflicts (e.g., cyber warfare) to launch attacks against adversaries. These operations advance political agendas while disguising the group's underlying criminal motives.

orange Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1 Cognitive manipulation (framing): EvilNet 2.0 presents its cyberattacks as acts of justice or resistance, emphasizing ideals rather than selfish motives. This convinces members and partners that they are acting for a noble cause, while manipulating the public perception of their actions.

2 EvilNet 2.0 positions itself as an expert and powerful group in hacktivism, boosting their credibility with recruits and allies. This makes people trust them and follow their directives without questioning.

3 The group manipulates and spreads false information to confuse its victims or discredit targets. This technique complicates their adversaries' defense and strengthens their control over public narratives.

4 Recruitment technique through "love bombing"
To attract new members or employees in companies, EvilNet 2.0 showers them with attention and flattering promises at first. This creates a strong emotional bond, making recruits more likely to fully commit to the group.

5 EvilNet 2.0 offers rewards, such as honorary titles or financial gains, to motivate its members to take risky actions. This reinforces their loyalty and pushes them to work hard for the group's recognition.

6 Mind control through isolation: The group encourages its followers to cut off external opinions, like media or loved ones, to make them dependent on their vision. This limits doubts and ensures stronger obedience to EvilNet 2.0's objectives.

orange Cyberdefense

Credits Orange Cyberdefense

Services Used

List of the services that the group uses:

- Ransomware-as-a-Service (RaaS)
- DeFi protocols (quant4j)
- Cryptocurrency mixers (Tornado Cash)
- Cryptocurrencies (Bitcoin, Monero)
- Decentralized platforms (DAO)
- Dark web marketplaces (Hydra, Genesis Market)
- Telegram
- Anonymous VPNs
- Signal
- Private Discord servers
- Temporary websites hosted on .onion domains
- Encrypted newsletter
- Encrypted networks (Tor, I2P)
- VPN (NordVPN, ProtonVPN)
- Dedicated proxies

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

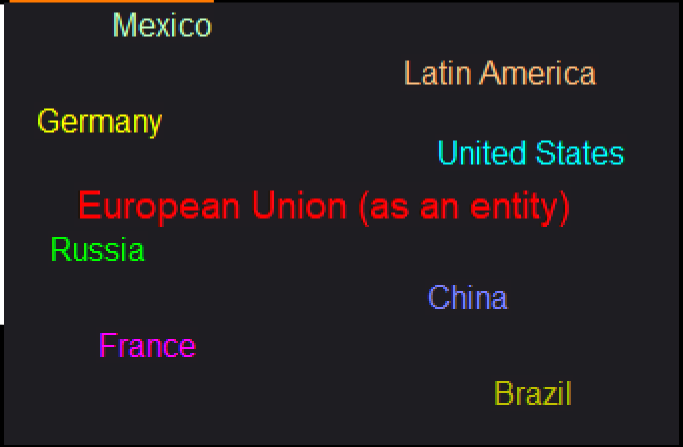
- Entertainment
- E-commerce
- Energy industry
- E-commerce
- Hospitality
- Telecommunications
- Pharmaceutical laboratories
- Public sector
- Finance
- Oil companies
- Telecommunications
- Health insurance companies

Note

EvilNet 2.0 embodies a hybrid cybercriminal threat, merging its hacktivist origins with advanced ransomware, extortion, and psychological manipulation tactics. Operating through decentralized networks and strategic alliances, the group focuses on critical sectors like healthcare, finance, and energy, deploying sophisticated technical attacks and tailored disinformation campaigns to amplify societal and operational disruption.

Credits Orange Cyberdefense

Targeted Countries



Mexico

Latin America

Germany

United States

European Union (as an entity)

Russia

China

France

Brazil

Credits Orange Cyberdefense

Most Likely Hypothesis

Strategic Targeting:

EvilNet 2.0 prioritizes critical infrastructure in NATO-aligned countries and geopolitical adversaries, particularly targeting healthcare, energy, and government sectors in Europe (e.g., France, Poland) and the U.S.

Hybrid Attack Methods:

The group employs DDoS-for-hire services, ransomware, and data leaks, paired with psychological manipulation tactics (e.g., humiliation campaigns, fear-inducing unpredictability). Recent operations suggest advanced capabilities, including OT system breaches using known vulnerabilities (e.g., VNC exploits, SCADA).

Systemic & Psychological Impact:

Attacks aim to destabilize public trust in institutions through service disruptions (e.g., water utilities, SCADA systems) and tailored disinformation campaigns.
By framing actions as resistance to Israel or Western policies, EvilNet 2.0 masks criminal motives (e.g., ransomware profits) while fueling societal polarization.

Credits Orange Cyberdefense

The most dangerous hypothesis

Targets:

EvilNet 2.0 would target vital infrastructure (power plants, healthcare systems, transportation networks) in strategic countries like France, Germany, and the U.S. Attacks would also aim at democratic institutions (elections, media) to erode public trust. Potential partnerships with rogue states could expand their geopolitical reach.

Methods:

Hybrid and synchronized cyberattacks exploiting zero-day vulnerabilities and insiders. EvilNet 2.0 could orchestrate complex attacks combining sophisticated ransomware, industrial sabotage software, and physical actions facilitated by internal complicity within targeted organizations. The coordinated use of unknown exploits would bypass conventional defenses.

Impacts:

Attacks could cause prolonged outages (water, electricity), leading to indirect casualties and localized economic collapse.EvilNet 2.0 might act as a cyber proxy in interstate conflicts, making attacks nearly impossible to attribute clearly.

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