Cyber Insight

RedEvils Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

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

RedEvils Group

- **Creation date:**
  The Red Evils group (WeRedEvils) emerged in October 2023 during the Israel-Hamas conflict, claiming to be former Israeli Defense Forces tech unit members and high-tech professionals. However, linguistic inconsistencies in their communications—such as Persian phrasing and poor Hebrew—have led analysts to suspect the group may actually be Iranian hacktivists posing as Israelis, exemplifying the use of false flag tactics in modern cyber warfare.

- **Probable Origin**:
  There are still doubts about the true origin of Red Evils. Some sources suggest they could be Iranian hacktivists pretending to be Israelis. However, other reports describe Red Evils as a “highly focused and active” group, confirming their pro-Israel stance through targeted attacks against both Hamas and Iranian infrastructure.

- **Main strategies:**
  Their tactics show a clear shift from basic hacktivist activities to more advanced and coordinated operations. This evolution suggests the group is becoming increasingly sophisticated, operating with the skills and organization of a highly capable cyber team.

- **Geopolitical Motivation:**
  Red Evils’ activities are closely tied to the broader geopolitical landscape of the Israel-Hamas conflict, also known as the Iron Swords War. By positioning themselves as defenders of Israeli interests in cyberspace, they aim to counter the operations of opposing groups and reinforce Israel’s cyber defense posture.

- **Targeted business sectors:**
  The Red Evils group primarily targets critical infrastructure, such as energy, telecommunications, and water networks. They also attack government and military sectors, including defense systems. Additionally, healthcare institutions have been among their targets.

Identification

Red Evils, also known as WeRedEvils, is a pro-Israeli hacktivist group that emerged during the Israel-Hamas conflict in October 2023. While they claim to be former Israeli tech and military professionals, some analysts suspect they may actually be Iranian operatives due to linguistic inconsistencies. The group targets critical infrastructure, government, military, and healthcare sectors linked to Israel’s adversaries, using tactics like data breaches and DDoS attacks

Credits Orange Cyberdefense

Red Evils Group: Main collaborating

These points show that Red Evils operates in a complex ecosystem, leveraging both formal partnerships and informal alliances to amplify its geopolitical and technical impact

Anonymous Sudan

Anonymous Sudan, an anti-Western hacktivist group, claimed in November 2023 to know the identity of a Red Evils member. They also alleged that Red Evils purchased DDoS attack services from them, showing a transactional relationship between the two groups.

Team UCC (UCC Team)

Red Evils has a confirmed partnership with Team UCC, coordinating attacks and sharing target information, especially during operations against Lebanon and Iran. This collaboration highlights their ability to network with other pro-Israeli hacktivist groups for greater operational impact.

Other Pro-Israeli Groups (Israeli Cyber Defense, SilentOne, Indian Cyber Force, Indian Cyber Sanatani)

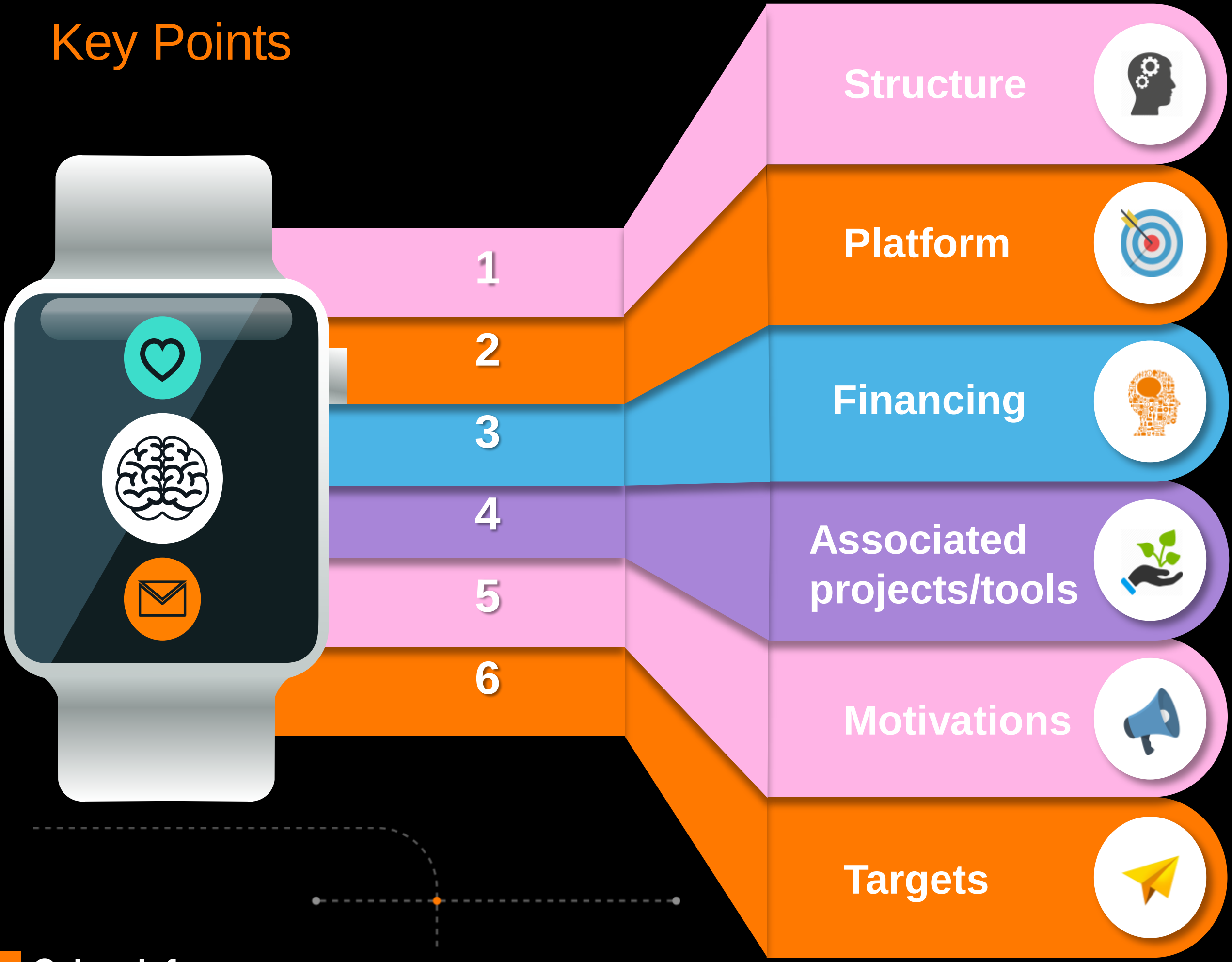
Red Evils is often mentioned alongside other pro-Israeli hacktivist groups in cyberwarfare mappings, suggesting informal coordination or coalitions during campaigns against common adversaries. These alliances boost their reach and effectiveness, particularly during major conflicts like the Israel-Hamas war.

Temporary Coalitions During Major Operations

During significant geopolitical events such as the Israel-Hamas conflict (2024-2025), Red Evils has participated in joint DDoS campaigns with other groups to overwhelm enemy digital infrastructure. These temporary coalitions enable synchronized attacks that maximize disruption and draw greater media attention.

Credits Orange Cyberdefense

Key Points



1 Structure

The Red Evils group claims to be made up of former members of Israeli Defense Forces (IDF) technology units (unconfirmed) and high-tech industry professionals, suggesting a highly skilled but likely decentralized operational structure.

2 Platform

Red Evils primarily operates and communicates through its Telegram channel. They use this platform to announce operations, share alleged evidence of their attacks, and most likely for coordination and recruitment purposes as well.

3 Financing

Red Evils primarily funds its activities through ransomware, demanding Bitcoin from victims. They may also profit by selling stolen data or offering DDoS-for-hire services, demonstrating an opportunistic approach to financing their OPs.

4 Associated projects/tools

Red Evils uses a mix of ransomware, DDoS attacks, and hacking communication systems to carry out its cyberattacks.

5 Motivations

Red Evils is primarily driven by a strong pro-Israeli and nationalist ideology, with the stated goal of disrupting entities perceived as threats to Israel, including Hamas, Hezbollah, and Iran.

6 Targets

The group mainly targets critical infrastructure such as energy, telecommunications, and water systems. They also focus on government, military, and healthcare sectors, aiming to disrupt key services linked to Israel's adversaries.

orange Cyberdefense

Credits Orange Cyberdefense

Vectors of Influence

1

Immediate Operational Impact

Red Evils can paralyze critical infrastructure by causing massive power outages and disrupting essential services such as public transportation. These attacks aim to shock and rapidly disrupt the daily lives of targeted populations.

2

Theft and Publication of Sensitive Data

The group exfiltrates confidential information, including development plans, and identity documents. Publicly releasing this data exposes victims to additional security risks.

3

Extortion Tactics

Red Evils encrypts servers and computers to disable targeted systems, a method typical of ransomware. Although financial extortion is not always explicit, the threat of not restoring access or publishing data remains a powerful leverage.

4

Strategic Targeting

Red Evils primarily targets infrastructure related to energy, nuclear construction, or the Iranian armed forces. This choice reflects a desire to strike of the opposing country.

5

Repetition of Attacks

The group carries out major cyberattacks in rapid succession, such as two significant operations within a week. This repetition demonstrates quick reaction capabilities and a determination to maintain pressure on the target.

orange Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

1

Cognitive Bias Tricks
Red Evils exploits authority bias. They trigger curiosity with fake offers. People react quickly without thinking.

2

Emotional Manipulation
The group pretends to be in distress.
They use fake charity stories.
They scare targets with threats..

3

Bait-and-Switch Tactics
Red Evils lures victims with believable alerts.
They switch to harmful actions.
Victims want to fix the problem.

4

Emotional Rollercoaster
They scare people with threats.
They offer fake help.
People feel confused and controlled.

5

Media and Social Amplification
They use bots to spread stories.
They focus on trending topics.
They make stories look popular.

6

Dividing People
Red Evils spreads divisive narratives.
They target specific communities.
They increase social tensions.

orange Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

Critical Infrastructure

Energy Sector (including electricity, oil, and nuclear facilities)

Telecommunications

Water Systems

Financial Institutions

Ports and Transportation

Government Sector

Military / Defense Sector

Healthcare Sector

Judicial Systems

Media and Social Media Platforms

Note

Red Evils represents an asymmetric threat where cyber activism blends with unconventional warfare. Their ability to disrupt essential services forces businesses and governments to rethink their resilience strategies, going far beyond just technical cybersecurity measures.

Cyberdefense

Credits Orange Cyberdefense

Cyprus

Jordan

Lebanon

Iran

Bangladesh

Yemen

Turkey

Greece

Targeted Countries

Middle Eastern nations

Spain

EU countries

Ireland

Norway

Hypothetical - Countries at Risk

Credits Orange Cyberdefense

Most Likely Hypothesis

Strategic Targeting

Red Evils is expected to continue strategically targeting entities perceived as anti-Israel, focusing primarily on adversaries like Hamas, Hezbollah, and Iranian infrastructure. Their operations will likely impact countries in the Middle East, including Iran, Lebanon, and potentially Jordan and Turkey, especially during escalations of the Israel-Hamas conflict. This focus extends to cross-border critical infrastructure, such as energy and water systems.

Hybrid Attack Methods

The group is anticipated to use hybrid attack methods, combining ransomware, DDoS campaigns, and data theft to maximize disruption and visibility. They are also likely to conduct precision attacks on SCADA systems and leverage social media hacks. Financial motivations may drive them to demand cryptocurrency ransoms and possibly sell stolen data or offer DDoS-for-hire services.

Systemic Impacts

These attacks could cause widespread disruptions to critical infrastructure, leading to economic losses, operational downtime, and social instability in targeted regions. Sectors most at risk include energy, telecommunications, healthcare, and government systems. Prolonged outages may also disrupt trade routes, agriculture, and urban life, potentially paralyzing supply chains in the Mediterranean.

Credits Orange Cyberdefense

The most dangerous hypothesis

Feared Scenario

The most severe scenario involves Red Evils launching coordinated cyberattacks on multiple critical infrastructures across several countries at once. This could target essential systems like power grids, water supplies, and financial networks. Such an operation would represent a highly sophisticated and widespread assault designed to maximize disruption. The goal would be to trigger systemic failures, not just isolated incidents.

Primary Targets

In this worst-case scenario, the main targets would be infrastructures crucial to national stability, such as energy grids, financial institutions, and communication networks in countries like Iran or Lebanon. Regional hydroelectric dams, oil refineries, and telecom hubs could also be at risk. There is even a hypothetical threat of counter-AI attacks on NATO ally systems during joint exercises with Israel. These targets are chosen for their potential to cause maximum chaos and destabilization.

Methodologies

Red Evils would likely use advanced tactics, including sophisticated ransomware, zero-day exploits, and supply chain attacks to evade defenses and inflict maximum damage. They could exploit outdated industrial systems with weak cybersecurity protections. Attack vectors may include targeted files paired with operational technology (OT) malware. Insider threats could also be used to gain deep access to critical systems.

Potential Consequences

Such attacks could result in massive economic losses, widespread social unrest, and potentially escalate regional conflicts. Cascading failures across sectors might lead to loss of life due to the disruption of essential services. The situation could spark humanitarian crises, retaliatory cyber campaigns, and global price shocks in key commodities. In the most extreme case, even allied missile defense systems could be temporarily neutralized (Naval radar networks, drone command systems, etc).

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

orange Cyberdefense

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

Credits Orange Cyberdefense