Cyber Insight

GoldenFalcon Group

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.

GoldenFalcon Group

- **Creation date:**
  The entity's origins date back to 2014, when its first cyber-espionage activities were detected under the aliases DustSquad or APT-C-34. Its emergence under the current hacktivist banner "Golden Falcon Team" is estimated around December 2024, coinciding with an escalation in global geopolitical tensions.

- **Probable Origin & Evolution**:
  Likely origins point to a Russophone actor with strong Russian ties (malware language, radio equipment purchase from Moscow supplier Yurion, digital signatures linked to Moscow).

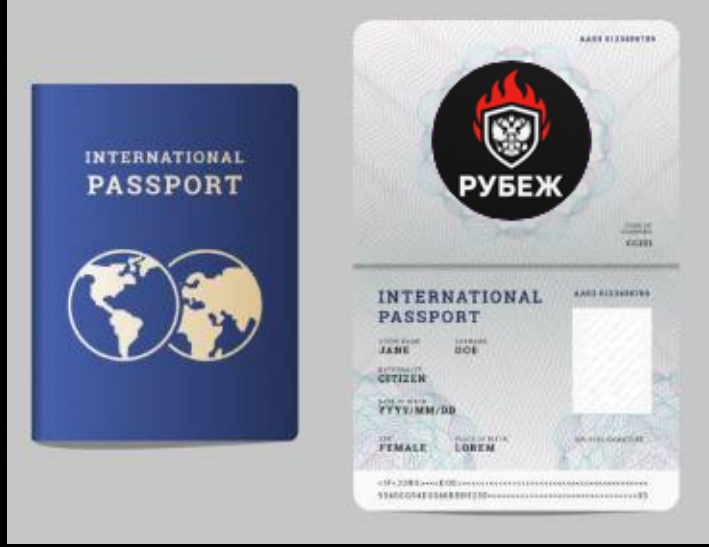
- **Timeline Evolution:**
  2014-2017: First Octopus campaigns, custom Windows/Android malware, discreet espionage targeting diplomats and dissidents.

  2018-2019: Publicized as Golden Falcon/APT-C-34 by Qihoo 360, revealing massive Kazakhstan operation (13 cities, RCS 10.3, proprietary backdoor).

  2020-2023: Continued Paperbug/Harpoon operations, enhanced RCS and radio interception capabilities.

  2024-2026: Label reused as "Golden Falcon Team" in pro-Russia (Z-Pentest, Dark Engine) and pro-Palestine hacktivist coalitions, with DDoS/ICS attacks synced to Ukraine and Israel-Iran conflicts.

- **Geopolitical Motivation:**
  Starting in 2014, the group functioned as a state-linked espionage unit focused on monitoring political dissidents and foreign diplomats across Central Asia.
  By late 2024, its mission shifted from quiet surveillance to aggressive, public hacktivism aimed at amplifying global geopolitical tensions.
  The collective is now driven by a pro-Russian and pro-Palestinian agenda, actively opposing NATO interests and Western military support for Ukraine.
  They prioritize sabotaging critical infrastructure, such as water and energy systems in France and the United States, to retaliate against foreign aid policies.
  This evolution highlights a move toward hybrid warfare where technical sabotage is used primarily to drive propaganda and spread public fear.



Identification

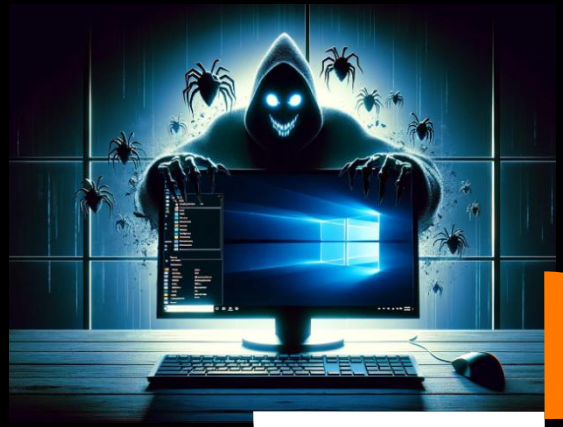
Golden Falcon (aliases: DustSquad, APT-C-34, Nomadic Octopus) operates as a hybrid cyber threat: state-sponsored espionage actor since 2014 and recent hacktivist collective. Active primarily in Central Asia (Kazakhstan focus) with expansion into pro-Russia/pro-Palestine campaigns targeting ICS infrastructure.

Known for sophisticated APT tools (Octopus backdoor, RCS implants) alongside DDoS and OT disruptions claimed via Telegram channels.

Reputation spans discreet surveillance of diplomats/media to noisy geopolitical hacktivism amplifying global conflicts.

Credits Orange Cyberdefense

Associated Adversary



- DustSquad / Nomadic Octopus / APT-C-34: As the group's state-linked Russian-speaking core since 2014, this entity provides the technical foundation for espionage operations. Its founding members include military intelligence experts and engineers specialized in using specialized radio interception tools (SIGINT) to monitor foreign diplomats and political dissidents.

- Specialized Russian Hardware Supplier: A crucial technical partner since 2014 that provides the group with specific radio wave interception equipment. This partnership allows the collective to conduct hybrid surveillance, combining direct radio signal monitoring with custom software implants for Windows and Android devices.

- NoName057(16): A primary partner since December 2024. This pro-Russian group collaborates closely with Golden Falcon to execute massive distributed denial-of-service (DDoS) attacks against Western and NATO-aligned infrastructure.

- Holy League: A large coalition consisting of approximately 70 different gangs that has been active since December 2024. It serves as a central coordination hub for global hacktivist campaigns and large-scale sabotage against NATO interests.

- Z-Pentest & Sector 16: Operational partners since late 2024 that specialize in Industrial Control Systems (ICS). They work with Golden Falcon to breach and tamper with critical water and energy utilities in the United States and France.

- INTEID: A Russia-aligned partner involved in joint operations since late 2024. This group focuses on exfiltrating sensitive data through sophisticated phishing campaigns targeting entities in Europe and Southeast Asia.

- Dark Storm Team: A recruitment and logistics network that became a key partner in 2024. It facilitates the aggregation of new members and coordinates group activities through encrypted Telegram channels.

- Dark Engine (Infrastructure Destruction Squad): A partner group that emerged in 2025 specifically for the physical disruption of critical infrastructure. They collaborate on operations targeting the energy, manufacturing, and agricultural sectors to maximize economic and social impact.

- WikiLeaks: A data dissemination partner in 2025. This alliance was used to leak massive amounts of confidential documents to the public, most notably during the high-profile "Phoenix Dossier" operation.

- OverFlame: A sophisticated network of hacktivist brands established in 2025. This partnership is designed to fragment the responsibility for cyberattacks, providing a layer of plausible deniability for the group's state-sponsored activities.

Credits Orange Cyberdefense

Vectors of Influence

1

Visual Exposure of Critical Vulnerabilities (ICS)

The group shares screenshots and videos of industrial control panels (pH, water temperature) to instill diffuse fear among the population. This staging of invisible technological threats aims to undermine public trust in utilities and local authorities.

2

Amplification via Digital Echo Chambers

Using Telegram and X, the group floods digital spaces with biased narratives and memes to create familiarity and subjective truth. This constant repetition in already polarized ecosystems facilitates viral propaganda spread and recruitment of new sympathisants.

3

Existential Threat Management (Terror Management Theory)

Golden Falcon uses mortality reminders like conflict imagery or martyrs to push individuals toward aggressively defending their cultural or national identity. This vector transforms cyber-violence into perceived "defensive" action, giving hackers heroic status within an ideological cause.

4

Strategic Attribution Ambiguity

Golden Falcon deliberately blurs lines between state-sponsored espionage (APT) activities and opportunistic hacktivist actions. This responsibility dilution complicates cybersecurity responses and enables state sponsors to maintain plausible deniability.

5

Moral Outrage Engineering (Outrage Culture)

The group times cyberattacks with media news peaks to maximize emotional engagement and coverage. By framing each intrusion as retaliation against Western "hypocrisy" or "crimes," it transforms technical incidents into global information warfare leverage.

Credits Orange Cyberdefense

Emotional Intelligence

1

The group uses cognitive reframing to transform technical intrusions into heroic acts of justice against imperialism. By consistently portraying their victims as "oppressors," they successfully shift public perception and stir moral indignation to legitimize their sabotage operations.

2

Emotional Anchoring:
This technique involves visually linking the group's name to images of industrial chaos or powerful cultural symbols like flags and religious slogans. This process strengthens message retention and creates a deep emotional bond that converts collective fear into a tool for ideological support.

3

Golden Falcon applies SWIFT communication models to establish immediate trust during recruitment and mobilize allies through a sense of critical urgency. By exploiting principles of reciprocity and authority, they manage to bypass the initial suspicion of new recruits on coordination platforms like Telegram.

4

Hacking Brains:
To amplify the impact of technically limited cyberattacks, the group publicly exaggerates the fragility of critical infrastructure to induce widespread panic. This "brain hacking" strategy is designed to bypass rational thinking in target populations and create deep-seated distrust in protective authorities.

5

Foot-in-the-door: The group radicalizes sympathizers by first securing small, symbolic acts of support, such as likes or content shares. Driven by a need for internal consistency, these individuals become much more likely to accept riskier assignments later, such as participating in DDoS attacks or providing illicit system access.

6

Dehumanization of the Adversary:
To overcome moral inhibitions against sabotaging civilian infrastructure (water, energy), the group uses rhetoric labeling targets as "monsters" or "criminals." This discursive technique makes cyber action more acceptable for members by framing collateral civilian damage as a "lesser evil" against the designated enemy.

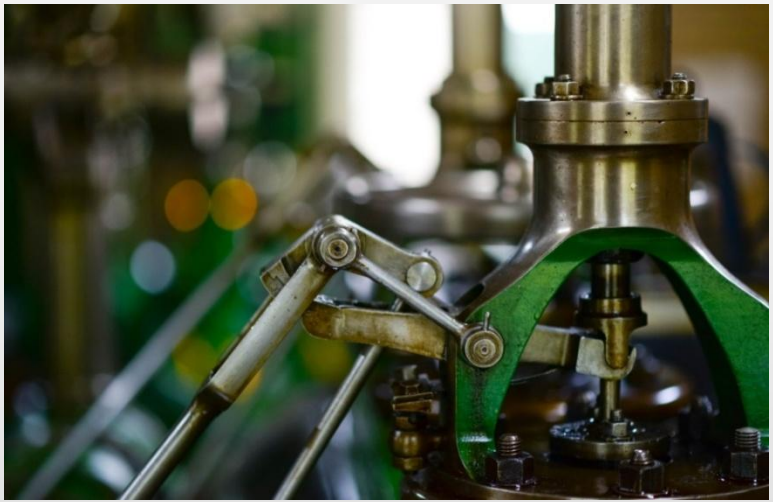
orange Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Critical Infrastructure (OT/ICS)
- Government
- Diplomacy
- Defense and Security
- Media
- Information Technology
- Education and Research
- Financial
- Digital Services
- Transport
- Extractive Industries



Note

The Golden Falcon collective merges state-sponsored espionage with aggressive pro-Russian hacktivism. Operating within the Holy League alongside NoName057(16), the group focuses on sabotaging critical infrastructure, notably water and energy utilities, via ICS intrusions.

Their technical operations utilize specialized radio wave interception (SIGINT) and custom malware like the Harpoon backdoor. Beyond technical strikes, they employ sophisticated psychological tactics, including NLP-based framing and Terror Management Theory, to cast their actions as "heroic justice" and incite public panic through visual leaks. This hybrid strategy effectively combines elite technical skills with emotional manipulation to destabilize NATO-aligned nations.

Targeted Countries

Brazil
Saudi Arabia
Ukraine
India
United States
France
Kazakhstan
Afghanistan
Israel
Russia
China

Middle Eastern Nations
Nigeria
NATO Member States
Indonesia
European Union Nations

- Hypothetical -
Countries at Risk

Credits Orange Cyberdefense

Most Probable Hypothesis on Future Activities

Geopolitical Targeting Hybridization (Espionage and Propaganda):
The group will maintain a dual model combining stealthy espionage for strategic intelligence with loud hacktivism for information warfare. Priority targets will remain government and diplomatic services in France, the United States, Israel, and other NATO allies. These actions will aim to punish Western policies regarding conflicts in Ukraine and the Middle East through selective data leaks.

Escalation of Critical Infrastructure Intrusions (ICS/OT):
An increase in attacks against industrial control systems, particularly in the water, energy, and transportation sectors, is highly probable. The primary goal will not necessarily be physical destruction but emotional destabilization through the distribution of visual proof of control on Telegram. These opportunistic intrusions will be synchronized with media peaks, such as military aid announcements or major diplomatic votes.

Cognitive Influence and Electoral Interference:
Golden Falcon will intensify its digital "echo chamber" tactics by using generative AI to spread massive disinformation campaigns and deepfakes. Future activities may target electoral processes in key regions like India, Brazil, or Nigeria to provoke crises of legitimacy. This vector will exploit moral outrage and cognitive biases to increase social polarization and erode trust in democratic authorities.

The most dangerous hypothesis

Mass Industrial Sabotage Scenario: The group could orchestrate a coordinated attack on industrial control systems (ICS) across multiple global metropolitan areas simultaneously. This scenario includes the deliberate contamination of drinking water supplies or the triggering of nationwide power outages during a major geopolitical crisis. The ultimate goal is to turn a technical intrusion into a “cyber-Armageddon” with irreversible physical and emotional consequences.

Targeting Critical Infrastructure and Finance: Future primary targets include water and energy distribution services, as well as global payment infrastructures such as the SWIFT system. The group specifically aims at NATO nations like France and the United States, seeking to punish their diplomatic stances by paralyzing public services. Dams and hospitals are identified as critical targets intended to cause vital service disruptions and indirect human casualties.

Hybrid Infiltration Methodologies: The offensive would rely on the use of the proprietary backdoor Harpoon, combined with generative AI tools capable of simulating official voices or financial directives. Massive DDoS botnets would be deployed synchronously to overwhelm incident response capabilities and conceal more discreet physical manipulations. This strategy blends long-term silent espionage with theatrical data leaks to maximize media and psychological impact.

Systemic and Geopolitical Consequences: Such a campaign would trigger cascading failures, leading to recovery costs worth billions of dollars and widespread financial asset freezes. Socially, the attacks aim to create total distrust toward protective institutions and deepen polarization within target populations. Geopolitically, the ambition is to undermine the digital sovereignty of Western allies and force strategic withdrawals in favor of Russian or Iranian interests.

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