Cyber Insight

BO TEAM 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.

BO TEAM Group

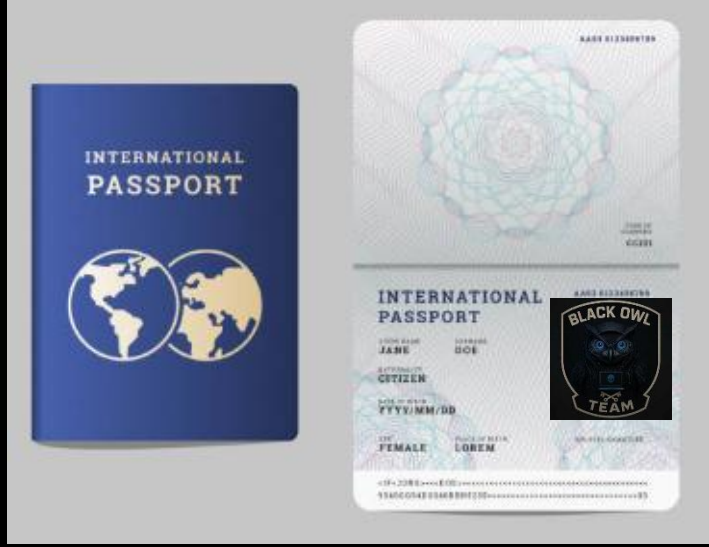
- **Creation date:**
  BO Team (also known as Black Owl) first appeared publicly in early 2024, marking its official debut with destructive attacks claimed on its Telegram channel. However, OSINT analyses suggest that its members or infrastructure were active as early as 2022 following the start of the full-scale invasion of Ukraine.

- **Probable Origin**:
  The group is originally from Ukraine, and its members are primarily local IT experts, developers, and cybersecurity specialists. Its formation resulted from a patriotic mobilization intended to transform civilian skills into asymmetric defense capabilities against the Russian military.

- **Main strategies:**
  BO Team tactics rely on long-term intrusions via spear-phishing, allowing them to remain stealthy for weeks or months before launching sabotage phases. The group specializes in massive data destruction (wipers), server sabotage, and the use of ransomware to paralyze the adversary's critical infrastructure.

- **Geopolitical Motivation:**
  Their primary motivation is to degrade the Russian military-industrial complex to weaken Moscow's operational capabilities on the battlefield. They also engage in cognitive warfare aimed at humiliating Russian institutions and demonstrating their vulnerability to Ukrainian digital resistance.

- **Targeted business sectors:**
  BO Team primarily targets Russian sectors such as defense (specifically drone manufacturers), energy, telecommunications, and logistics. Their attacks also strike state administration, including the judicial system and scientific research centers linked to the war effort.

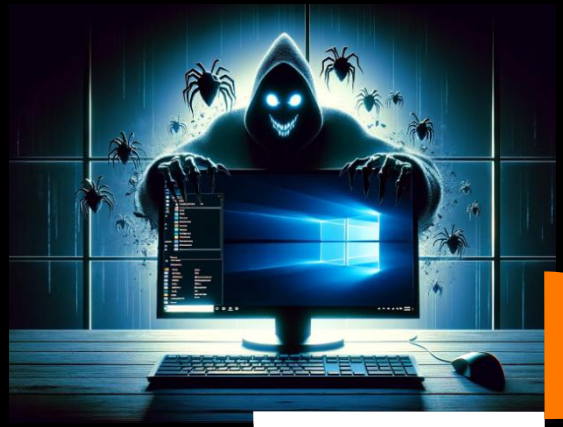


Identification

BO Team (also known as Black Owl) is a sophisticated pro-Ukrainian hacktivist collective that often operates as an elite unit coordinated with Ukrainian military intelligence (HUR/GUR). Unlike typical volunteer groups, they are distinguished by their high technical autonomy and their ability to conduct high-impact sabotage operations.

Credits Orange Cyberdefense

Associated Adversary Groups of BO Team Group



GUR (HUR): The Ukrainian military intelligence agency maintains a close operational relationship with BO Team, providing strategic targets and support while benefiting from plausible deniability regarding sabotage activities

Ukrainian Cyber Alliance (UCA): This long-standing organization of cyber volunteers regularly collaborates with BO Team to conduct joint intrusions against Russian military and industrial suppliers

Head Mare: This pro-Ukrainian hacktivist group has shared command-and-control infrastructure with BO Team since 2026, often specializing in sophisticated initial access via phishing before sabotage phases begin

Twelve: Identified by cybersecurity experts as a technical partner to Head Mare, this group shares tools and servers that facilitate the coordination of operations within the broader hacktivist alliance

IT Army of Ukraine: This large, decentralized mobilization structure coordinates target lists and served as the initial ecosystem for BO Team before it evolved into a more autonomous and professionalized entity

Cyber Partisans (Belarus): This independent group occasionally aligns with BO Team to strike regional logistical infrastructure, such as railways, to disrupt Russian military movements through Belarus

Vectors of Influence

1

Naming and Shaming

BO Team publicly posts evidence of breaches to intimidate Russian organizations and recruit sympathizers through dramatized displays of success.

2

Geopolitical Synchronization

Major cyberattacks are timed to coincide with symbolic dates or military milestones to maximize their global media impact and perceived relevance.

3

raming the Existential Struggle

By constructing a binary moral narrative of "defender versus aggressor," BO Team psychologically justifies extreme sabotage as a necessary act of resistance.

4

Media Amplification

The group repurposes external cybersecurity reports from firms like Kaspersky or Bitdefender to validate its own power and increase the adversary's sense of vulnerability.

5

The "Digital Partisan" Narrative

Using military terminology to describe digital actions symbolically transforms civilian IT experts into elite soldiers performing "heroic justice".

Emotional Intelligence

Cognitive Framing:
This technique redefines sabotage as "heroic justice," which removes moral guilt for participants and enhances the internal legitimacy of their actions.

1

Fear Appeals:
By highlighting their reach into vital sectors like judicial systems or satellites, BO Team creates a perception of total insecurity designed to paralyze the opponent's response.

2

Social Identity (In-group/Out-group):
The group exploits the need for belonging by creating a "cyber-soldier" identity, which strengthens collective loyalty and increases risk tolerance among members.

3

4

Emotional Anchoring:
The consistent use of specific icons and slogans associates the group's brand with feelings of inevitable victory, triggering automatic emotional responses in their audience.

5

Social Proof:
Leveraging strategic alliances and media recognition allows the group to build psychological authority, making their recruitment and mobilization efforts more effective.

6

Urgency and Scarcity (FOMO):
Tactics such as "Target of the Hour" campaigns create a fear of missing out on contributing to the war effort, which accelerates the rapid mobilization of volunteers.

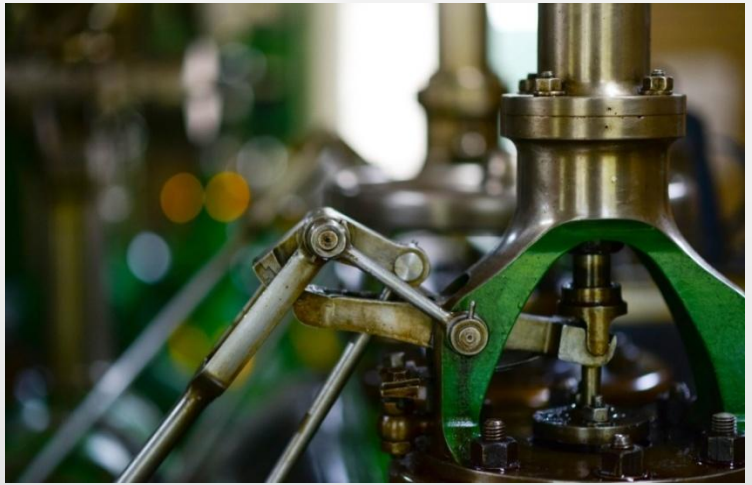
Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Government and state administration
- Defense and military suppliers, specifically drone manufacturers
- Judicial and legal systems
- Scientific, space, and hydrometeorological research
- Energy, oil, and gas
- Telecommunications and IT services, including cloud and data centers
- Transportation and logistics
- Manufacturing and heavy industry, such as electronics, electrical equipment, and cement
- Media and information agencies
- Federal digital signature and certification authorities
- Financial and online banking services



Note

BO Team targets the Russian military-industrial complex, specifically drone manufacturers and logistics providers, to directly paralyze the enemy's operational and battlefield capabilities. They employ aggressive "naming and shaming" and psychological warfare on Telegram to humiliate Russian institutions and create a climate of fear and institutional paranoia. Attacks on satellite centers and industrial IT networks are designed to "blind" military situational awareness and physically halt the production of critical war materiel.

Credits Orange Cyberdefense

Targeted Countries

Belarus

Russian Federation

Credits Orange Cyberdefense

High-Probability Future Targets Countries

NATO member states

Italy

Belarus

Russian Federation

Germany

France

Austria

Allies of the Russian Federation

Credits Orange Cyberdefense

Most Probable Hypothesis on BO Team Group Future Activities

Future Targets

BO Team is expected to maintain its focus on Russian military-industrial targets, including defense, aerospace, and energy sectors, to weaken the systems supporting the war effort. These operations will likely prioritize sectors like logistics and state administration where disruption has the most direct impact on military capabilities,

Hybrid Methods

BO Team will likely refine multi-stage operations that blend long-term espionage with timed sabotage using custom wipers and ransomware. They are also expected to increase technical coordination with allies like Head Mare, sharing command-and-control infrastructure to scale their attacks.

Systemic Impacts

These activities will lead to the gradual attrition of Russian administrative and logistical systems, compounding the effects of international sanctions. Psychologically, this reinforces the narrative of Ukrainian cyber resilience while fostering a climate of persistent internal insecurity within Russia.

Credits Orange Cyberdefense

The most dangerous hypothesis

The Most Dangerous Scenario
The highest risk involves the group expanding into trans-national, cascading attacks on interconnected critical infrastructure located outside the immediate theater of war. This scenario could see coordinated sabotage of global systems while maintaining plausible deniability for any state sponsors

Targets and Sectors Targeted
Primary targets would include national power grids, satellite constellations, and major transportation hubs in states deemed hostile, such as NATO members or Russian allies. Disruption of these sectors would aim to paralyze vital public services and military situational awareness on a global scale.

Methodologies
BO Team would likely use AI-augmented persistent access and supply-chain compromises to infiltrate and manipulate industrial control (OT) networks. These attacks would be synchronized with massive information operations designed to maximize public panic and discredit government responses.

Potential Consequences
Expected impacts include widespread blackouts, billions of dollars in economic losses, and threats to public safety like the failure of medical or traffic control systems. Such a catastrophic level of destruction could cross "red lines," potentially triggering a kinetic military retaliation and escalating the cyber conflict into total war.

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