GAMAREDON

[/ ˈgæməˌrɛdɒn /]

Gamaredon Group is a Russia-linked APT active since 2013, targeting Ukraine, NATO, and critical sectors with phishing and malware. Evolving toward more sophisticated operations, it remains a high-risk, state-backed threat through 2025.

IDENTITY

Attribution	: Russia-linked, widely assessed to operate under the Russian Federal Security Service (FSB).
Active Since	: At least 2013.
Aliases	: Shuckworm, IRON TILDEN, BlueAlpha, Blue Otso, Primitive Bear, Trident Ursa, Actinium, Aqua Blizzard, DEV-0157, UAC-0010, G0047, Winterflounder.
Motivation	: Political and military espionage in support of Russian strategic and military objectives, primarily targeting Ukraine and NATO interests.

TTPs

Initial Access	: Spear-phishing emails with malicious attachments; exploitation of vulnerabilities in public-facing applications.
Persistence	: Use of scheduled tasks, registry modifications, and backdoors to maintain long-term access.
C2 Infrastructure	: Custom malware families and HTTP-based command-and-control servers; frequent domain switching.
Malware & Tools	: Pterodo (backdoor), PowerPunch, custom downloaders, malicious VBS and BAT scripts, remote access tools.
Techniques	: Fast malware deployment, fileless techniques using PowerShell, lateral movement via stolen credentials.

TARGET PROFILE

Target Sectors	: Government, military, defense contractors, critical infrastructure, NGOs, media, international organizations.
Geographies Targeted	: Primarily Ukraine; also Europe, NATO member states, and occasionally North America.

THREAT ASSESSMENT

Risk Level	: High – state-backed, persistent, and adaptive.
Most Recent Activity	: Active in 2025 with phishing and malware campaigns tied to the Russia-Ukraine war.
Evolution	: Evolved from crude, noisy operations with poor OPSEC to more refined campaigns, including better obfuscation, rapid malware iteration, and expanded geographic focus.

NOTABLE OPERATIONS

- **2013–2018:** Initial campaigns against Ukrainian government institutions with crude spear-phishing.
- **2019–2021:** Increased malware sophistication; deployment of Pterodo and widespread phishing waves against Ukrainian military and diplomatic entities.
- **2022:** Intensified operations during Russia's full-scale invasion of Ukraine, including disruptive cyber-espionage and phishing attacks.
- **2023:** Continued targeting of Ukraine's government and military, with evidence of opportunistic targeting of NATO members.
- **2024–2025:** Ongoing spear-phishing and malware campaigns; improved obfuscation techniques and diversification of malware families.