ANGRY LIKHO

[/ˈæŋgri ˈliːkhoʊ/]

Callisto is a Russia-linked APT group focused on political and security espionage, recently using fake personas and cloud tools for advanced credential-theft campaigns. It targets government, defense, NGOs, and related sectors across NATO, the EU, the U.S., and Eastern Europe.

IDENTITY

Attribution : Believed to be aligned with Russian-state interests.

Active Since : 2021.

Aliases : Awaken Likho, Sticky Werewolf, Core Werewolf, GamaCopy, PseudoGamaredon.

Motivation : Strategic intelligence collection, credential harvesting, long-term espionage operations across Eastern Europe.

TTPs

Initial Access

- Spearphishing emails impersonating government or military institutions
- Malicious Office documents, LNK files, and compressed archives delivering staged loaders
- Fake PDF notices hosted on cloud storage platforms
- Direct outreach by crafted personas inside online communities

Persistence

- Registry-based run keys
- Scheduled tasks
- Credential reuse and session hijacking
- Lightweight backdoors left dormant for extended periods

Command & Control (C2)

- Disposable VPS and dynamic DNS domains
- Compromised WordPress sites
- Cloud file-sharing services used as dead-drop locations
- Encrypted HTTPS channels to blend with legitimate traffic

Tools & Malware

- Lightweight modular backdoors (PowerShell/C#)
- Script-based reconnaissance tools
- Document collectors and credential stealers
- Custom loaders with increasing obfuscation and modularity

Techniques

- Social engineering and persona-driven infiltration
- Slow and methodical lateral movement targeting high-value nodes
- Cloud-aware exfiltration to avoid detection
- Use of legitimate Windows utilities for living-off-the-land operations

TARGET PROFILE

Target Sectors

- Government ministries
- Military and defense-support organizations
- Public administration networks
- Universities involved in strategic or defense research
- Think tanks and political analysis centers

Geographies Targeted

- Ukraine
- Poland
- Baltic states
- Moldova
- Select Western European defense-linked institutions

THREAT ASSESSMENT

Risk Level : High

Most Recent Activity : Active campaigns through 2024–2025 involving modular malware, cloud-based C2, and advanced phishing techniques.

Evolution : Improving operational security, expanding use of cloud services, enhanced persona development, and more resilient infrastructure rotation

NOTABLE OPERATIONS

2015–2017: Early spear-phishing campaigns targeting Eastern European diplomatic corps and policy researchers; use of bespoke credential-harvesting domains.

2021–2022: Early Sticky Werewolf phishing waves targeting Ukrainian administrative bodies.

2022–2023: Expansion into defense volunteers, logistics organizations, and regional policy institutions.

2023–2024: Deployment of GamaCopy and PseudoGamaredon toolsets with Gamaredon-style code resemblances.

2024–2025: Adoption of improved C2 encryption, cloud exfiltration, and longer dwell times in high-value networks.