WINTER VIVERN

[/ˈwɪn.tər ˈvaɪ.vərn/]

Winter Vivern (TAG-70 / UAC-0114 / TA473) is a Belarus-linked, Russia-aligned APT active since 2020, targeting NATO- and EU-affiliated entities. In 2024–2025, it focused on credential theft and Zimbra exploitation using advanced phishing, posing a high threat to government and military sectors.

IDENTITY

Attribution	: Belarus-based, Russia-aligned state-backed APT group.
Active Since	: At least 2020, ongoing through 2025.
Aliases	: TAG-70, UAC-0114, TA473.
Motivation	: Espionage—collection of political, military, and diplomatic intelligence.

TTPs

Initial Access	- Highly targeted spear-phishing emails. - Spoofed NATO/EU government portals. - Exploitation of Zimbra Collaboration Suite vulnerabilities. - Strategic compromise of government websites.
Execution	- PowerShell-based loaders. - HTML smuggling. - Custom web-based implants (e.g., WSS Loader). - Use of proxy execution to evade detection.
Persistence	- Scheduled tasks. - Malicious cron jobs. - Fake SSO login portals for repeated credential harvesting.
C2 Infrastructure	- Compromised WordPress sites. - Rotating Belarus/Russia VPS hosting. - Encrypted HTTP/HTTPS communications.
Lateral Movement & Collection	- Credential harvesting from browsers and SSO. - Reconnaissance scripts. - Targeted extraction of diplomatic, telecom, and military-related data.

TARGET PROFILE

Target Sectors	: Government ministries, military units, diplomatic missions, telecom operators, defense contractors, policy research institutions.
Geographies Targeted	: Ukraine, Poland, Lithuania, Latvia, Germany, France, the United States.

THREAT ASSESSMENT

Risk Level	: High — frequent targeting of sensitive political and military communication channels.
Most Recent Activity	: Ongoing Zimbra exploitation; new phishing domains replicating EU and NATO systems.
Evolution	: Improved anti-analysis measures, multi-layer staging servers, MFA bypass components, and AI-enhanced targeting.

NOTABLE OPERATIONS

- **2020:** Government-targeted phishing campaigns themed around COVID-19 and NATO.
- **2021:** Credential harvesting from diplomats and civil servants across Eastern Europe.
- **2022:** Escalated espionage aligned with the Russia–Ukraine conflict; extensive Zimbra exploitation.
- **2023:** Targeting telecom operators to intercept communications.
- **2024:** EU/NATO credential operations using advanced phishing kits.
- **2025:** Renewed campaigns and infrastructure rotation.