RomCom (aka Void Rabisu)

[/ˈrɒm.kɒm/]

RomCom (aka Void Rabisu) is a high-risk, Russia-aligned APT active since at least 2022, focused mainly on espionage. It targets government, diplomatic, defense, and tech sectors in Ukraine, NATO/EU countries, and North America, and has recently escalated its operations by exploiting zero-day vulnerabilities and using more stealthy, flexible toolchains.

IDENTITY

Attribution	: Likely Russia-aligned threat actor, though definitive state attribution remains debated.
Active Since	: 2022.
Aliases	: RomCom, Void Rabisu, Storm-0978, UAT-5647.
Motivation	: Intelligence collection and espionage against NATO-aligned entities, with occasional financially motivated activity (links to ransomware deployment noted).

TTPs

Initial Access	- Spearphishing emails with trojanized installers for legitimate software (KeePass, PDF Reader, Advanced IP Scanner). - Fake websites spoofing conference/event portals (e.g., NATO Summit, Ukraine Recovery Conference). - Exploitation of zero-day vulnerabilities (e.g., in Microsoft Office and WinRAR in 2024–2025).
Persistence	- Registry modifications and scheduled tasks. - Deployment of lightweight custom backdoors. - Abuse of Windows utilities and LOLBins for stealth.
Command & Control (C2)	- HTTPS-based C2 with domain fronting. - Use of commercial hosting and cloud services. - Fast-flux and disposable infrastructure.
Malware & Tools	- RomCom RAT (custom remote access trojan). - Custom downloaders and droppers. - Use of commodity tools (Mimikatz, Rclone, PowerShell).
Techniques	- Credential theft (Outlook/Exchange, browser data). - Exfiltration via cloud storage. - Privilege escalation via exploitation and credential dumping. - Rapid toolchain swaps to evade detection.

TARGET PROFILE

Sectors	: Government ministries, defense contractors, diplomatic organizations, NGOs, media, and IT service providers.
Geographies	: Primary: Ukraine, Poland, United Kingdom. Secondary: Wider NATO/EU states and North America.

THREAT ASSESSMENT

Risk Level	: High.
Most Recent Activity	: 2024–2025: Leveraged two zero-day vulnerabilities in campaigns against European government and defense targets. Fake NATO/Ukraine-themed conference sites used to distribute backdoors.
Evolution	: Shift from simple phishing campaigns to sophisticated zero-day exploitation. Improved infrastructure resilience (rotating domains, layered encryption). Blended espionage and ransomware tactics to obscure attribution.

NOTABLE OPERATIONS

- **2022:** First observed trojanized installer campaigns delivering RomCom RAT against Ukrainian military and diplomatic entities.
- **2023:** NATO Summit lure operations; malicious PDF reader installers targeting Eastern European governments.
- **2024:** Ukraine Recovery Conference decoy sites; campaigns expanded into North America.
- **2025:** Two zero-day exploits leveraged in early 2025 operations; ongoing targeting of NATO member states.