UAC-0194

[/juː eɪ siː zɪroʊ wʌn naɪn fɔːr/]

UAC-0194 is a high-risk, Russian-affiliated threat actor identified by CERT-UA, active since at least 2024. The group specializes in credential theft and cyber-espionage, primarily targeting government and strategic sectors in Ukraine, Poland, and Romania. They are known for their rapid operationalization of zero-day vulnerabilities (e.g., CVE-2024-43451) to harvest NTLM hashes and deploy remote access tools like SparkRAT.

IDENTITY

Attribution	: Russian-affiliated threat actor tracked by CERT-UA
Active Since	: At least 2024
Aliases	: UAC-0194 (CERT-UA), no confirmed cross-vendor aliases
Motivation	: Cyberespionage, credential harvesting, NTLM hash theft, long-term access into government and strategic networks

TTPs

Initial Access	- Malicious emails sent through compromised Ukrainian government infrastructure - Delivery of .url, .lnk, and .library-ms files crafted to trigger NTLM hash disclosure - Exploitation of NTLM-related vulnerabilities CVE-2024-43451 and CVE-2025-24054 - Zero-click or single-click file execution requiring minimal interaction
Persistence	- Deployment of lightweight remote access tools (e.g., SparkRAT, open-source implants) - Use of stolen NTLM hashes for authentication replay into internal systems - Possible establishment of scheduled tasks or registry-based persistence via secondary payloads
Command & Control (C2)	- Cloud-hosted or compromised regional infrastructure for hosting payloads - Encrypted communications through web protocols - Use of redirectors to mask true C2 origin
Malware & Tools	- SparkRAT for remote access and post-compromise operations - NTLM hash relays and brute force tooling - Custom payloads delivered through .library-ms and .url file abuse - Open-source reconnaissance and data collection utilities
Techniques	- NTLMv2 hash harvesting via file-based exploits - Lateral movement using NTLM replay or cracked credential material - Targeted reconnaissance within government and public-sector networks - Stealthy communication patterns and low interaction exploit flow

TARGET PROFILE

Primary Sectors	Government ministries and agencies, Public sector institutions, Diplomatic and administrative structures, Education and academic research networks, Private companies supporting government operations
Geographic Focus	Ukraine, Poland, Romania, Potential expansion across Europe

THREAT ASSESSMENT

Risk Level	: High
Most Recent Activity	: Active exploitation of NTLM disclosure vulnerabilities from late 2024 through 2025; rapid adoption of newly patched CVE-2025-24054
Evolution	: Fast retooling cycle, improved lure sophistication, broader geographic targeting, increased reliance on open-source RATs and low-interaction exploit vectors

NOTABLE OPERATIONS

- **Late 2024:** Zero-day exploitation of CVE-2024-43451 via malicious .library-ms files targeting Ukrainian government entities
- **Early 2025:** Adoption of CVE-2025-24054 in phishing campaigns against Poland and Romania, indicating widening operational scope
- **Ongoing:** Continued NTLM hash harvesting and suspected follow-on network access leveraging SparkRAT and credential replay