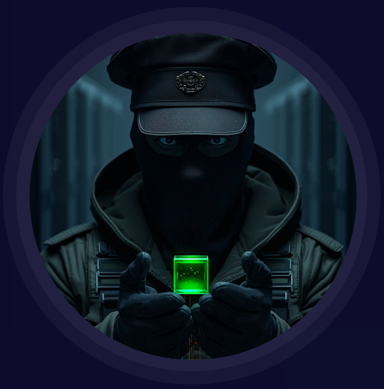

UAC-0102

[/juː eɪ siː zɪərəʊ wʌn zɪərəʊ tuː/]

A likely Russian-aligned espionage actor active since 2021, UAC-0102 targets Ukrainian government, military, and critical infrastructure through spearphishing and custom backdoor deployments — evolving from simple phishing into modular malware with cloud-based C2 channels for persistent, low-visibility access.

IDENTITY

Attribution : Likely Russian-aligned espionage actor.

Active Since : 2021.

Aliases : GreenCube, UNC3707.

Motivation : Strategic intelligence gathering, surveillance of governmental and defense-related entities, credential theft, long-term clandestine access.

TTPs

Initial Access

- Highly tailored spearphishing emails impersonating government or military institutions
- Embedded malicious documents with macros or exploit-based loaders
- Links to staged payload servers designed for short operational lifespans

Persistence

- Custom lightweight backdoors
- Scheduled tasks for recurring execution
- Registry-based persistence on Windows hosts
- Credential theft enabling session hijacking and prolonged covert access

Command & Control (C2)

- Cloud-based platforms used for beaconing and payload staging
- HTTPS-encrypted channels blending with legitimate network traffic
- Dynamic DNS domains to frequently rotate C2 endpoints

Tools & Malware

- Modular backdoors created for reconnaissance and data theft
- Obfuscated scripts designed for stealthy execution
- Information stealers focused on documents, communication archives, and credentials
- Custom loaders enabling multi-stage execution flows

Techniques

- Stealth-oriented infiltration and slow operational tempo
- Selective lateral movement with minimal footprint
- Reconnaissance of administrative and strategic systems
- Covert exfiltration designed to avoid spikes in traffic or alerts

TARGET PROFILE

Target Sectors

- Government ministries and agencies
- Military-affiliated bodies
- Public administration organizations
- Energy, communications, and other critical infrastructure sectors
- NGOs and research entities linked to national security

Geographies Targeted

Primarily Ukraine
Occasional targeting of institutions in neighboring regions tied to defense or policy.

THREAT ASSESSMENT

Risk Level : High.

Most Recent Activity : 2024–2025 campaigns leveraging modular backdoors, refined phishing lures, and cloud-integrated C2.

Evolution : Increasing sophistication in payload staging, improved OPSEC practices, cloud-centric communication, and enhanced reconnaissance capabilities.

NOTABLE OPERATIONS

2021–2022: Early reconnaissance-focused campaigns targeting Ukrainian administrative networks.

2023: Deployment of more advanced, encrypted backdoors supporting extensive reconnaissance.

2024: Increased volume of spearphishing linked to geopolitical escalations, targeting defense and government systems.

2025: Emergence of cloud-first C2 infrastructure, stronger obfuscation layers, and more selective intrusion workflows.