Threat Intelligence Assessment

Author: Nikhil Birla

Date: 28 December 2025

Lab: Advent of The Relics 2 - Operation Winter Blackout (Part 2)

Difficulty Level: Easy

Campaign: Winter Blackout

Actor Designation: INTRUDER-LOGISTICS

EXECUTIVE SUMMARY

INTRUDER-LOGISTICS is a structured criminal collective preparing a high-value asset-theft operation under the cover of a legitimate cultural exhibition. The group exhibits strong operational security, specialized logistics knowledge, and multi-national infrastructure. This dossier details actor profiles, campaign phases, infrastructure, tradecraft, and strategic recommendations derived from analysis of their private coordination forum.

Key Judgments:

1. The group's primary objective is financial gain through theft and resale of high-value goods, not data exfiltration.
2. Execution is scheduled for **New Year's Eve**, leveraging global distraction during countdown events.
3. The group has established contingency protocols including a maritime escape route and evidence-destruction procedures.
4. Actors show moderate-to-high sophistication with clear role specialization and geographic dispersion.

---

1. THREAT ACTOR PROFILE

1.1 Collective Structure

Alias	Role	Responsibilities	Known Identifiers
Curator	Strategic Lead	Final decision authority, planning oversight, operational security enforcement.	–
Bellringer	Technical Operations	C2 infrastructure, malware deployment, GPS spoofing, digital wipe protocols.	–

Alias	Role	Responsibilities	Known Identifiers
SnowFox	Intelligence & Deception	Target reconnaissance, media narrative shaping, social engineering.	–
Driver_BUD	Physical Logistics	Transport, vehicle preparation, border crossing, physical security.	First name: **Daniel** (from forum OPSEC slip).
Ledger	Financial Operations	Cryptocurrency handling, shell-company management, payment routing.	Cat named **Satoshi** (Bitcoin reference).

1.2 Motivations & Capabilities

- **Motivation:** Primarily financial; no observed ideological or state-sponsored markers.
- **Capabilities:**
    - Malware development (PowerShell payloads, persistence mechanisms).
    - Document forgery (ATA carnets, insurance certificates, corporate paperwork).
    - GPS tracking spoofing and physical counter-surveillance.
    - Maritime smuggling coordination.
- **Resources:** Access to Balkan-based forgers, Serbian VPS hosting, and Eastern European transport networks.

2. CAMPAIGN TIMELINE & PHASES

2.1 Preparation Phase (October – November 2025)

- **2025-10-15:** Farmhouse (“Staging South”) established as air-gapped planning cell.
- **2025-11-12:** C2 listeners (health-status-rs.com) activated in Kragujevac, Serbia.
- **2025-11-14:** Spear-phishing launched against CALE logistics employee **Kamil Poltavez**.

2.2 Infrastructure & Cover Development (November – December 2025)

- **Forged Documentation:** “Miracles of Winter” exhibition cover created via Bucharest-based forger.
- **Shell Company Registration:** “Danube Event Solutions Ltd” established as backup cover.
- **Vehicle Preparation:** 2012 Volvo FH truck fitted with winter tires, GPS spoofers, and false signage.

2.3 Execution Phase (Scheduled: 31 December 2025)

- **Trigger Mechanism:** Code word **“FROST”** to be issued at **23:59:50 UTC**.
- **Simultaneous Activation:** All operational nodes receive trigger via NTP-synced timing.
- **Contingency:** SMS-based backup trigger using burner phones purchased in Romania.

2.4 Exfiltration & Dispersal (January 2026)

- **2026-01-03, 04:00 UTC:** Maritime escape via vessel **“Adriatic Wind”** (Captain **Stavros**) from Athens, Greece to Italy.
- **Post-Operation:** Planned dissolution of digital infrastructure and physical safe-houses.

---

3. INFRASTRUCTURE ANALYSIS

3.1 Digital Infrastructure

Asset	Type	Purpose	Location
health-status-rs.com	Domain	Primary C2 beacon, victim check-in.	VPS in Kragujevac, Serbia
advent-of-the-relics-forum.htb.blue	Forum	Operational coordination, document sharing.	Hosting unknown; likely offshore
Farmhouse Network	Air-gapped LAN	Storing technical plans, manifests, maps.	Rural Serbia (43.849476, 20.927157)

3.2 Physical Infrastructure

- **Farmhouse ("Staging South"):** Primary planning and storage location.
- **Bucharest Forger:** Produces high-quality forged customs and insurance documents.
- **Vehicle Fleet:** Volvo FH truck modified for cold-weather operations and tracking evasion.
- **Maritime Asset:** Cargo vessel *Adriatic Wind* (captained by Stavros) for Mediterranean extraction.

---

4. TRADECRAFT & OPSEC PROTOCOLS

4.1 Communication Security

- **Air-gapping:** Technical plans stored only on isolated systems at farmhouse.

- **What3Words:** Used for coordinate sharing (twitchy.develop.hulk = 37.936489, 23.68644).
- **Coded Language:** Phrases like “friends of Konstantin” for asset recognition.

4.2 Anti-Forensics Measures

- **Digital Wipe Script:** burn_cycle.sh – overwrites cryptographic headers, fills RAM with noise, triggers kernel panic.
- **Physical Destruction:** SSDs drilled through controller chips; paper records burned in diesel.
- **Printer Memory:** Laser printer drums and controller boards destroyed to prevent document recovery.

4.3 Evasion Techniques

- **GPS Spoofing:** OBD-II-based spoofer replays “parked at truck stop” loops to avoid tracking anomalies.
- **Cover Stacking:** Layered cover stories (“exhibition” → “emergency repairs”) to withstand scrutiny.
- **Burner Protocols:** Phones activated once, used once, then physically destroyed.

---

5. INDICATORS OF COMPROMISE (IOCs)

5.1 Network Indicators

Type	Indicator	Context
Domain	health-status-rs.com	C2 check-in endpoint
URL	https://advent-of-the-relics-forum.htb.blue/api/v1/implant/	Second-stage payload delivery
Credentials	svc_temp:SnowBlackOut_2026!	Forum authentication

5.2 Behavioral Indicators

- PowerShell execution with arguments: -nONi -nOp -eXeC bYPaSs -cOmManD
- Registry access to HKLM\SOFTWARE\MICROSOFT\CRYPTOGRAPHY\MACHINEGUID
- HTTP POST to /api/v1/checkin with JSON containing u, d, g fields

5.3 Operational Indicators

- Use of What3Words phrases in communications
- References to “Miracles of Winter” exhibition or “Danube Event Solutions Ltd”
- GPS anomalies showing vehicles “parked” for exactly 8-hour loops

---

6. MITRE ATT&CK MAPPING

Tactic	Technique ID	Technique Name	Observed Activity
Reconnaissance	T1595	Active Scanning	Forum intelligence gathering on target logistics
Resource Development	T1583.001	Acquire Infrastructure: Domains	Registration of health-status-rs.com
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Malicious ZIP sent to Kamil Poltavez
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	Obfuscated beacon script

Tactic	Technique ID	Technique Name	Observed Activity
Persistence	T1574	Hijack Execution Flow	GPS spoofing to evade tracking
Defense Evasion	T1485	Data Destruction	burn_cycle.sh and physical SSD drilling
Command & Control	T1573	Encrypted Channel	HTTPS beaconing to C2
Exfiltration	T1048	Exfiltration Over Alternative Protocol	Maritime physical extraction planned

---

7. STRATEGIC ASSESSMENT

7.1 Likely Success Factors

- **Timing:** New Year's Eve provides global distraction and reduced security staffing.
- **Cover Plausibility:** "Miracles of Winter" exhibition aligns with seasonal cultural movements.
- **Geographic Positioning:** Balkan base provides proximity to EU targets and smuggling routes.

7.2 Vulnerabilities & Weaknesses

- **OPSEC Slips:** Real name disclosure (Daniel), pet references, emotional posts in "Off-Topic" board.
- **Infrastructure Links:** VPS in Serbia creates jurisdictional exposure.
- **Maritime Dependency:** Escape requires cooperation of external captain (Stavros).

7.3 Predictive Analysis

- If initial heist succeeds, group likely to repeat similar operations across European logistics corridors.
- Possible expansion into counterfeit cargo or document-forging as a service.
- Increased anti-forensics measures expected in future campaigns.

---

8. RECOMMENDATIONS

8.1 Immediate Actions

1. **Network Blocking:** Blackhole traffic to health-status-rs.com and forum domain.
2. **Law Enforcement Coordination:** Share farmhouse coordinates with Serbian authorities; forger details with Romanian police.
3. **Maritime Alert:** Notify Greek and Italian coast guard regarding *Adriatic Wind* and Captain Stavros.

8.2 Defensive Posturing

- Train customs and border agents on forged ATA carnets and “Miracles of Winter” exhibition cover.
- Monitor cryptocurrency wallets associated with Ledger’s transactions.
- Implement GPS anomaly detection for fleet vehicles showing repetitive “parked” loops.

8.3 Intelligence Collection

- Deploy honey-documents referencing “Winter Blackout” or “Danube Event Solutions Ltd” to track attempted reuse.
- Establish surveillance on Bucharest forger network identified in forum.
- Monitor dark-web channels for sale of forged cultural-goods documentation.

---

9. SOURCES & METHODOLOGY

- **Primary Source:** Forum access via credentials (svc_temp:SnowBlackOut_2026!) recovered from malware.
- **Geolocation:** What3Words decoding and coordinate validation via Google Earth.

- **Timeline Reconstruction:** Cross-referencing forum post timestamps, C2 logs, and external events.
- **Confidence Levels:** Applied using Admiralty System (Source: B2; Information: B3).

---

10. APPENDIX

10.1 Forum Post Excerpts (Key Findings)

- *“Project ‘Winter Blackout’: Operational Scope & Goals” – Curator, 05 Mar 2025*
- *“Sync Logic: ‘Midnight’ Trigger Protocol Finalized” – Bellringer, 10 Dec 2025*
- *“Forged Manifests: ‘Miracles of Winter’ Exhibition” – Curator, 01 Nov 2025*
- *“Exfiltration Protocol: Staging South Exit Route” – Curator, 15 Oct 2025*

10.2 Tools Used in Analysis

- What3Words decoder
- Wireshark (for any PCAP follow-up)
- Google Maps / Earth Pro
- Metadata extraction utilities