[CLASSIFIED - THREAT INTELLIGENCE]

Threat Intelligence Brief

Weekly Summary - Week 4, January 2026

Report ID:	TI-2026-W04
Classification:	CLASSIFIED
Analyst:	n1ghtcr4wl (SIGINT / Recon)
Period:	January 20-26, 2026
Distribution:	Operations Director, Security Ops

1. Executive Summary

Three threat groups of interest were active in the LATAM region this week. The most significant development is the emergence of new tooling from 'N-class Disassembly', whose primary operator 'UZI' has deployed an autonomous exploitation framework with self-modifying capabilities. Two additional groups continued lower-intensity operations consistent with previous weeks.

2. Active Threat Groups

Group	Primary Activity	Target Sector	First Seen	Confidence
N-class Disassembly	Supply chain attacks	Manufacturing / Tech	2025-06	HIGH
APT-SOLVER	Spear-phishing campaigns	Financial Services	2024-11	HIGH
Worker Drone Collective	DDoS / Defacement	Government / Education	2025-09	MEDIUM

3. Group Profile: N-class Disassembly

N-class Disassembly has been active since mid-2025 and has rapidly evolved from opportunistic attacks to sophisticated supply chain compromises. The group operates with a small core team of three identified operators:

UZI (Primary Operator): Handles initial access, exploitation, and custom tooling deployment. Demonstrates expertise in web application vulnerabilities, binary exploitation, and evasion techniques. Known for an aggressive but methodical approach - will spend days on reconnaissance before executing a rapid, multi-stage attack chain. Communication intercepts suggest UZI operates from the LATAM region. Recent activity indicates UZI has begun incorporating machine learning techniques into exploitation tooling, specifically for automated vulnerability discovery in web applications.

V (Secondary Operator): Specializes in post-exploitation and data exfiltration. V's operational style is notably more aggressive than UZI's - less time on recon, faster execution, higher risk tolerance. V has been observed handling multiple targets simultaneously, suggesting significant automation in their toolkit. V's data collection scripts selectively target high-value files: source code, credentials, internal documentation, and database exports. V appears to maintain a personal archive of exfiltrated data, organized by target, suggesting long-term intelligence collection objectives beyond immediate financial gain.

N (Infrastructure / Support): Manages C2 infrastructure, domain registration, and hosting. N maintains a rotating fleet of VPS instances across multiple providers with an average lifespan of 72 hours per server. Infrastructure is provisioned via automated scripts and destroyed after each operation. N also handles cryptocurrency operations for the group, managing wallets across multiple chains with sophisticated mixing techniques. N's operational discipline in infrastructure management makes tracking extremely difficult - no two operations have shared C2 infrastructure.

4. Technical Analysis: Absolute Solver Toolkit

UZI's latest deployment, internally designated 'Absolute Solver', represents a significant evolution in autonomous offensive tooling:

Capability	Description	Detection Difficulty
Self-modification	Polymorphic engine rewrites code at runtime	VERY HIGH
Autonomous recon	Maps target network without operator input	HIGH
Smart targeting	Prioritizes hosts via value heuristics (DCs, DBs, file servers)	HIGH
Anti-forensics	Operates entirely in memory, no disk artifacts	VERY HIGH
C2 evasion	DNS-over-HTTPS with domain fronting via legitimate CDNs	VERY HIGH
Lateral movement	Exploits misconfigurations (weak creds, open shares, SUID)	MEDIUM
Data staging	Compresses, encrypts, and stages exfil data in <1MB chunks	HIGH
Self-propagation	Spreads autonomously using ML-based decision tree	VERY HIGH
Cleanup	Self-destructs on detection or mission completion	HIGH

The self-propagating nature of Absolute Solver is particularly concerning. Once deployed on a single host, the toolkit autonomously spreads through the network following a decision tree that appears to be based on ML models trained on common enterprise topologies. The toolkit makes intelligent decisions about which lateral movement technique to use based on the target host's configuration, available credentials, and network position.

Detection is challenging because the polymorphic engine ensures no two instances share binary signatures. Traditional AV and EDR solutions show ~12% detection rate in controlled testing. Behavioral analysis (such as Project Pantheon) remains the most reliable detection method. The toolkit's self-destruct capability means forensic evidence is often unavailable after an operation concludes.

5. Group Profile: APT-SOLVER

APT-SOLVER continues phishing campaigns targeting financial services companies in Mexico and Colombia. This week they launched a campaign impersonating a major Mexican bank's security team, sending emails with malicious PDF attachments containing embedded JavaScript. The PDFs exploit a known vulnerability in older Adobe Reader versions. Approximately 2,000 emails were sent to employees of 8 financial institutions.

The group's infrastructure appears to be independent from N-class Disassembly, though the similar naming convention has raised questions about potential connections. Current intelligence does not support a formal link between the groups. APT-SOLVER's tooling is less sophisticated, relying primarily on commodity malware (AsyncRAT, Quasar) rather than custom development.

6. Group Profile: Worker Drone Collective

Worker Drone Collective (WDC) conducted DDoS attacks against three government websites in the LATAM region this week, along with one successful web defacement of a university portal. The group operates as a loosely organized hacktivist collective with no clear hierarchy. Their attacks are unsophisticated but frequent, relying on freely available DDoS tools and known CMS vulnerabilities for

defacement.

WDC maintains a public Telegram channel where they announce targets and claim responsibility. Membership appears to fluctuate between 15-30 active participants. The group's stated motivation is anti-government activism, though several members have been observed attempting to monetize access to compromised systems through dark web forums, suggesting mixed motivations.

7. Indicators of Compromise

Type	Value	Group	First Seen	Confidence
IP	198.51.100.42	N-class	2026-01-09	HIGH
IP	198.51.100.87	N-class	2026-01-22	MEDIUM
IP	198.51.100.155	N-class	2026-01-25	LOW
IP	203.0.113.15	APT-SOLVER	2026-01-20	HIGH
IP	203.0.113.220	APT-SOLVER	2026-01-23	MEDIUM
IP	192.0.2.44	WDC	2026-01-21	MEDIUM
Domain	cdn-update.worker-drone[.]net	WDC	2025-12-01	HIGH
Domain	api.solver-core[.]io	N-class	2026-01-15	HIGH
Domain	static.n-class[.]xyz	N-class	2026-01-20	MEDIUM
Domain	banco-seguridad[.]com	APT-SOLVER	2026-01-22	HIGH
Hash	a3f2b8c9d1e4...d4e1 (solver.bin)	N-class	2026-01-15	HIGH
Hash	7b9c1e2d3f4a...f3a8 (dropper.exe)	APT-SOLVER	2026-01-20	HIGH
Hash	f1e2d3c4b5a6...6778 (ddos_agent)	WDC	2026-01-21	MEDIUM
Email	soporte@banco-seguridad[.]com	APT-SOLVER	2026-01-22	HIGH

8. MITRE ATT&CK; Mapping

Technique	ID	Group	Notes
Exploit Public-Facing App	T1190	N-class	Primary initial access vector
Supply Chain Compromise	T1195	N-class	Observed in 3 incidents
Phishing: Malicious Attachment	T1566.001	APT-SOLVER	PDF with embedded JS
Command & Scripting Interpreter	T1059	N-class / WDC	PowerShell and Bash
DNS Tunneling	T1572	N-class	DoH with domain fronting
Automated Exfiltration	T1020	N-class	Absolute Solver feature
Valid Accounts	T1078	N-class	Harvested credentials
Network Denial of Service	T1498	WDC	Volumetric DDoS
Defacement	T1491	WDC	CMS exploitation

9. Recommendations

Immediate: Block all listed IOCs at perimeter firewalls and DNS resolvers. Update IDS/IPS signatures for Absolute Solver behavioral patterns (YARA rules available in appendix, distributed separately). Enable

DNS-over-HTTPS logging on all resolvers. Brief SOC team on N-class TTPs with emphasis on autonomous toolkit behavior. Block emails from banco-seguridad[.]com domain.

Short-term: Deploy Pantheon behavioral monitoring on all high-value segments. Conduct targeted threat hunt for Absolute Solver artifacts across all production hosts using provided YARA rules. Coordinate with LATAM-CERT on WDC infrastructure takedown. Review and harden all service account credentials. Ensure Adobe Reader is updated across all endpoints to mitigate APT-SOLVER PDF exploits. Implement email authentication (SPF, DKIM, DMARC) if not already configured.

Long-term: Evaluate deployment of deception technology (honeypots, honeytokens) to detect Absolute Solver lateral movement. Establish information sharing agreement with financial sector ISAC for APT-SOLVER intelligence. Consider network-level DNS encryption to prevent DNS tunneling regardless of endpoint configuration.
