THREAT ADVISORY

0APT – Ransomware Group

February 2, 2026

Executive Summary

0APT (also stylized as 0apt) is a newly emerged ransomware group first publicly detected around January 28, 2026. It operates as a **Ransomware-as-a-Service (RaaS)** syndicate using a double-extortion model (file encryption via AES-256 and data exfiltration, with threats to leak the victim's data). The group describes itself as a "politically neutral underground syndicate" focused solely on financial gain, with examples of demands such as "a sudden tax on your security negligence".

However, this appears to be **a low-effort operation aimed at building hype or scamming affiliates rather than conducting real attacks.** CTI firms have removed most 0APT entries from their trackers, leaving only a handful under "potential" investigation. Organizations should continue to monitor for any changes, but the current assessment is that 0APT poses minimal real risk. If you're associated with a listed entity, verify internally rather than engaging with the group.

Key Characteristics

- **Model**: RaaS. Affiliates supply targets; the core group provides tools (phishing C2 infrastructure, locker/encryptor, negotiation/chat support), handles extortion, and takes a revenue share. Access to their darkweb portal reportedly uses browser signatures for filtering.
  - Multiple CTI platforms, including DarkFeed and RansomLook, have conducted reviews and concluded that the majority of listed "victims" are fictitious. Many company names do not correspond to real entities, and some appear to be AI-generated or pulled from sandbox environments rather than actual breaches.
  - No ransomware samples, payloads, IOCs, or YARA rules have been identified or shared by researchers. There's zero evidence of a functional encryptor or exfiltration tooling.
  - Despite countdown timers expiring for numerous claimed victims, no data has been leaked or published on their site. This is a major red flag for legitimacy in ransomware operations.
  - The group has shifted to recruiting "black hat hackers" or affiliates, which analysts interpret as a potential scam to steal cryptocurrency from would-be partners rather than a genuine RaaS model.
- **Leak Site**: Dark web Onion/Tor-based "leak blog" or victim portal where victims are listed with countdown timers ("T-MINUS" style, often 14–17+ days). Some victim announcements include claimed data volumes (e.g., 200GB, 450GB) and sample descriptions. Trackers like ransomware.live report ~91 victims listed (as of early February 2026).

- No independent confirmations from victims, forensic reports, or regulatory filings (e.g., SEC disclosures) have surfaced. Aggregators like Ransomware.live and RedPacket Security list the claims but note they are unverified and based solely on the group's announcements.
- A few real companies are interspersed among the fake ones (e.g., Liberia Revenue Authority, Liberia Electricity Corporation), possibly to lend credibility, but even these lack any public acknowledgment of breaches.

- **Aggressiveness**: Claims extremely high volume of intrusions (e.g., 71 in ~48 hours) (late Jan 2026: 9 on Jan 28, 1 on Jan 29, 61 on Jan 30), with reports of 60 victims added in a single 24-hour period. This suggests rapid affiliate scaling or industrialized operations.
    - Sources that initially reported the surge (e.g., CtrlAltNod claiming 3 exposures) have not provided follow-up evidence, and subsequent intel corrections have downgraded the threat.

Activity Timeline (as of Feb 2, 2026)

- **Jan 28**: Initial detection; ~8 victims listed (e.g., Metropolis City Municipal, Apex Logistics Solutions, TechnoSoft IT Services, GreenValley Regional College, Sunrise Manufacturing Ltd., Rapid Food Distributors, Dr. Smith Dental Clinics, Orion Legal Partners).
- **Jan 30**: Surge claims 19+ new victims announced rapidly; 60 global victims added to leak site; total claims reaching dozens to 71 within a short window. Examples include Aegis Defense Systems and Metro General Hospital.
- **Early Feb**: Continued claims (e.g., Liberia Revenue Authority, Liberia Electricity Corporation). Trackers list 90+. Reports indicate that data from at least 3 companies have already been published/leaked on the site; many others face active countdowns. Some victims reportedly "reach an agreement" quickly (possible payments or unverified resolutions).

Targets and Victims

Broad, opportunistic targeting across critical and high-value sectors worldwide (US, UK, Serbia, South Africa, Liberia, etc.). No strong geographic or sector focus evident; appears to be volume driven.

Notable 'claimed' victims (partial list from announcements):

- **Healthcare**: Metro General Hospital (surgery videos, patient HIV status, billing), Silverline Hospitals, Noble Pharma (clinical trials).

- **Defense/Energy/Critical Infra**: Aegis Defense Systems (weapon blueprints), Solaris Renewable Energy (patents, grid data), Diamond Deep Drilling (seismic/oil data), National Rail Network (signal codes), Harbor Port Authority (container tracking), Solstice Energy Grid (SCADA).
- **Finance/Crypto**: Quantum Financial Corp, CryptoVault Exchange (KYC, wallet keys), Silver City Bank.
- **Logistics/Transport**: Apex Logistics Solutions (~450GB invoices/passports), Rapid Courier Services, Pacific Ocean Cargo.
- **Tech/IT/AI/Research**: Obsidian Tech Labs (BIOS/prototypes), FutureTech AI (datasets/model weights), NeoTech Solutions (source code/API keys), Quantum Physics Lab.
- **Education/Gov/Public**: GreenValley Regional College, Summit Education Trust, Metropolis City Municipal, Liberia Revenue Authority/Electricity Corp.
- **Others**: Visionary Architects (CAD files), IronClad Security (client/access data), Global News Corp (sources/interviews), Sapphire Jewelry, Elite Hospitality, Urban Outfitters, etc.

Claimed data types: Highly sensitive PII (passports, SSNs, medical/HIV records, student data), IP (patents, CAD/blueprints, source code, AI models, weapon/SCADA/seismic/GMO data), financial (KYC/wallet keys/tax returns/SWIFT), corporate (client lists, contracts, surveillance footage), etc.

TTPs, Capabilities, and Verification

- **Known/Claimed TTPs**: AES-256 encryption. Initial access likely via phishing (affiliate-provided C2).
  - Graduated pressure: intrusion → encryption → countdown/leak threat.
  - No public ransom notes, specific malware variants, YARA rules, CVEs, or IOCs released by researchers yet.
  - No confirmed attribution beyond cybercrime RaaS.
- **Verification Status**: All activity is based on the group's own leak site announcements and trackers, aggregating them. No widespread independent confirmation of compromises (e.g., via public data dumps, forensic reports, or victim disclosures). Skepticism exists in threat intel communities (e.g., no leaks observed in some early cases; rapid "agreements" by victims; potential for inflated claims, selective/fake postings, or LARP-style operations to build reputation). A few sources note 3+ actual publications. Monitor leak sites directly for confirmation.

Potential Impact and Risk

High-volume claims pose risks to critical infrastructure (energy, transport, healthcare, defense, finance) via data exposure (PII breaches, IP theft, regulatory violations) even without full encryption/disruption. Rapid scaling could indicate effective recruitment or automation, increasing the likelihood of hits on unprepared organizations. If legitimate, expect more leaks as countdowns expire.

Recommendations

- **Prevention**: Robust phishing defenses, MFA everywhere, patching, EDR/XDR, network segmentation, offline 3-2-1 backups, least-privilege access, email/web filtering.
- **Detection/Monitoring**: Monitor dark web/leak sites (e.g., via ransomware.live or commercial intel), anomalous exfil/activity, phishing attempts.
- **Response**: Assume breach if named; do not pay ransoms (fuels the model); engage IR/forensics; notify regulators/law enforcement (e.g., FBI IC3); test backups.
- **General**: Treat claims skeptically until verified; prioritize high-value sectors (healthcare, critical infra, finance, IP-heavy orgs).

Sources: Primary X alerts (Hackmanac Jan 28, DailyDarkWeb & JustaBreach Jan 30), ransomware.live group profile, ZATAZ darkweb contact report, DailyDarkWeb article, aggregator reports (DeXpose, Malware.news, RedPacket Security, etc.). No specific IOCs available at this time.