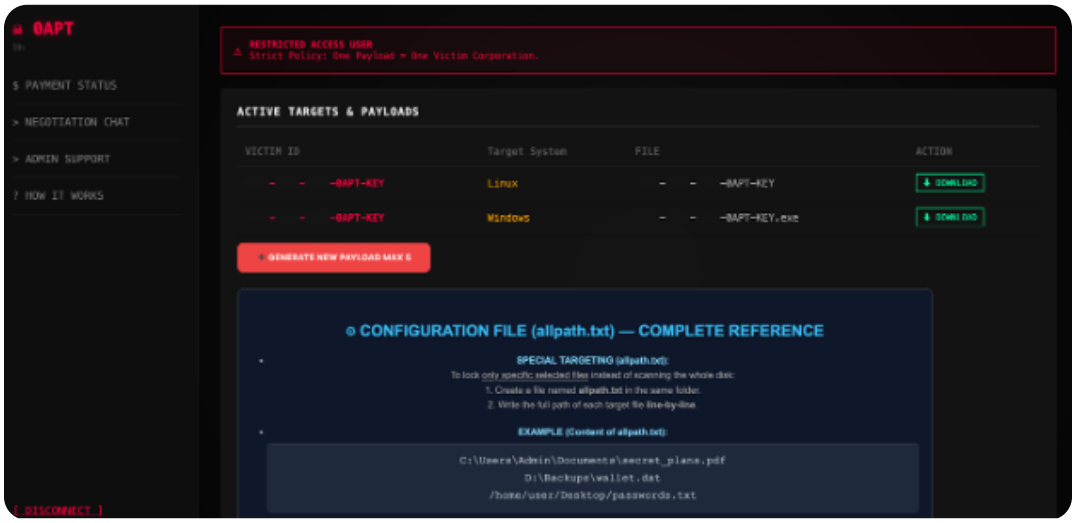
halcyon | Ransomware Research Center

0APT: Credible Technical Depth Despite Inflated Victim Claims

0APT is a ransomware operation first identified in late January 2026 that immediately gained attention by claiming hundreds of victims within its first 48 hours of observed activity. New Halcyon analysis indicates that 0APT:

- **Poses a legitimate threat:** The gang is aggressive during ransom negotiations and possesses a functional encryption capability that employs robust cryptographic implementation and customizable configurations for exclusion lists, file size limits, parallel processing threads, and memory management parameters.
- **Is not a rebrand or directly connected with other known groups:** While memory handling and certain encryption elements are consistent with standard encryptors, 0APT does not exhibit significant cross-over with any other ransomware code that Halcyon has analyzed across more than 100+ ransomware variants.
- **Likely used inflated or false victim claims to create momentum:** Although many of the gang's publicly claimed victims have not been independently verified and some leak-site data has proven non-authentic, inflated victim reporting has historically been used by emerging ransomware operators to establish credibility prior to confirmed attacks.

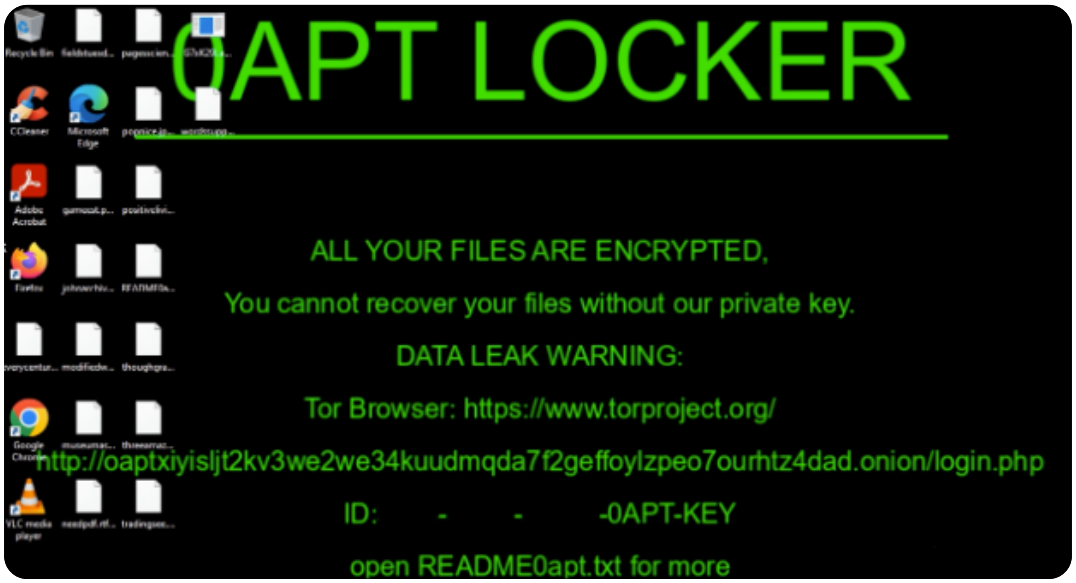
0APT uses the same code base to run on either Windows or Linux, which are compiled for each victim as shown in 0APT RaaS Panel (for Affiliates) screenshot below:



Ransomware Payload Analysis

SHA256 Hashes	388810cade3472336809550d020f210b54cb9479a76c114a66ad371b108a715a 13253c717371a7cb786804a96bedc0df2cc26f7137e37e9f652acac1e7fcf81b 258e4a48e8725e63d7223270f3fef2488edb26323a43807e63e71f77e9e81c23
Programming Language	Rust
Target Platform	Windows/Linux
Ciphers	AES-256 (file encryption) RSA (key encryption)
Encryption Schemes	Full encryption (entire file encrypted in single operation, up to 1 GiB default limit)
Cryptographic Libraries	aes-0.8.4 rsa-0.9.9 rand_core-0.6.4
Ransom Note File Name	README0Apt.txt
Encrypted File Extensions	.0Apt

Upon execution, the ransomware modifies the desktop wallpaper by dropping a new image file and setting it as the background before beginning encryption operations. This is different from most ransomware operations which change the wallpaper after encryption is completed:



The ransomware payload allows operators to include customizable configuration files under *config2.txt*. The configuration file loads settings that allow operators to customize exclusion lists, file size limits, parallel processing threads and memory management parameters.

If the configuration file does not exist, the ransomware payload will default to preset values. The ransomware operators can also customize encryption mechanisms by using individual RSA public keys via a *public_key.pem* file or by leveraging the embedded RSA-4096-bit default key.

The default exclusion list for file extensions, file names, and folder paths maintain the following values:

File Extension	File Name	Folder Path
.0Apt	company.txt	/
.bak	config2.txt	/$recycle.bin
.bat	public_key.pem	/appdata/local/temp
.com		/boot
.db		/cache
.dll		/dev
.exe		/etc
.ini		/google/chrome
.lnk		/lib
.log		/mozila/firefox
.msi		/proc
.old		/program data
.sys		/sbin
.temp		/sys
.tmp		/systemwindows
.thumb		/temp
.vbs		/tmp
		/windows

A notable implementation quirk exists in the file name exclusion logic. While the code is designed to perform case-insensitive filename matching, it only converts target filenames to lowercase without normalizing the exclusion list. This can result in the ransomware encrypting its own ransom note if exclusions are not specified in lowercase format.

During encryption, which defaults to RSA-4096 key size, 0APT exclusively uses full file encryption techniques. It targets all files up to 1 GB in size by default. For each file, the ransomware verifies that sufficient RAM is available by checking whether the sum of the target file size and a configurable memory threshold exceed available system memory.

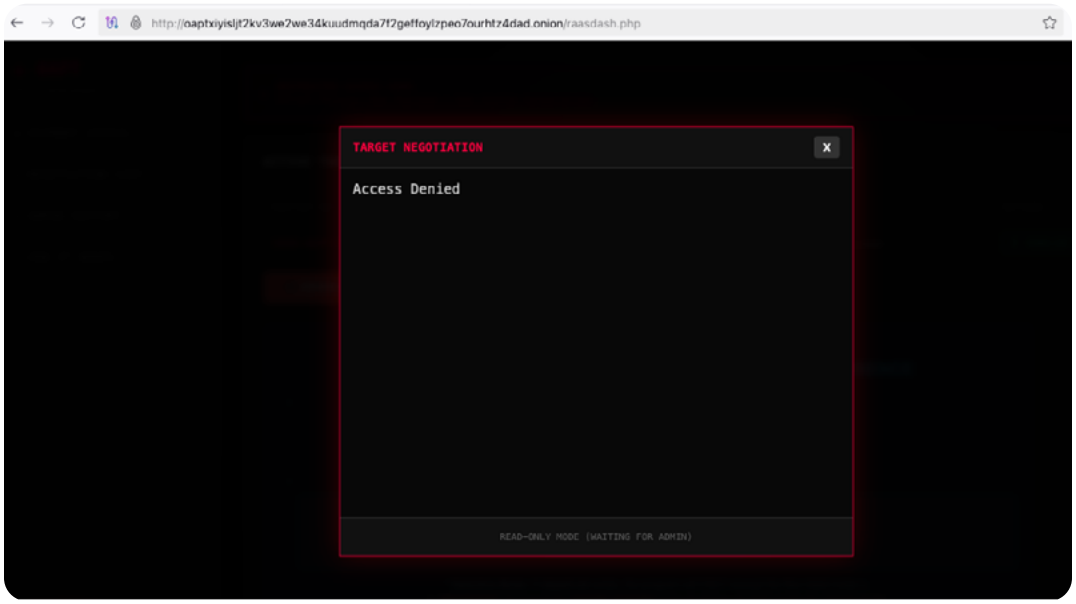
If insufficient memory is detected, the ransomware waits and retries once before skipping the file entirely. This approach helps prevent system crashes during encryption operations. All encrypted files are given the .0Apt extension. 0APT ransomware then drops a ransom note titled README0apt.txt in every directory that contains encrypted files:

README0apt-Redacted.txt

```
::: 0APT LOCKER :::

!!! ALL YOUR FILES ARE ENCRYPTED !!!

Hello,

If you are reading this message, it means your company's network has been breached
and all your data has been encrypted by "0apt" group.

WHAT HAPPENED?
We have exploited vulnerabilities in your network infrastructure. All your servers,
databases, and backups have been locked with military-grade encryption algorithms
(AES-256 & RSA-2048). You cannot recover your files without our private key.

DATA LEAK WARNING:
Before encryption, we downloaded your confidential data . If you refuse to pay or do not contact us, this
data will be published on our Tor blog for your competitors and regulators to see.

HOW TO GET YOUR FILES BACK?
We are not interested in destroying your business, we only want payment.
You must purchase a unique decryption tool from us.

>>> LEGAL & REPUTATION NOTICE (IMPORTANT):
We have analyzed your files If you do not pay:
1. We will send copies of this incriminating data directly to your GOVERNMENT
   agencies and regulators to trigger an investigation against you.
2. We will email your clients, business partners, and everyone in your CONTACT
   LIST to inform them that you lost their data.

INSTRUCTIONS:
1. Download and install Tor Browser: https://www.torproject.org/
2. Open Tor Browser and navigate to our chat portal:
   http://oaptxiyislj12kv3we2we34kuudmqda7f2geffoylzpeo7ourhtz4dad.onion/login.php
3. Enter your Personal ID to start the negotiation.

Your Personal ID:
REDA-CTED-REDAC-0APT-KEY

DEADLINE:
You have 24 hours to contact us. After this, the price will double.
If we do not hear from you within 48 hours, your data will be leaked permanently.

ATTENTION:
- Do not rename encrypted files.
- Do not try to decrypt using third-party software (you may lose data forever).
- Do not call the police or FBI (we will leak data immediately).

-- 0apt Team --

```

Extortion and Negotiation Tactics

Observed communications with the gang revealed more aggressive tactics than many other groups. The original 0APT administrator (admin) is willing to remove an affiliate and revoke their access from negotiations as shown below with the Access Denied screenshot:



Other ransomware gangs have used this tactic in an attempt to maximize profit, raise prices, and drive more aggressive negotiations. After the affiliate was removed, 0APT increased the ransom demand by 50%. The initial offer was in the low six-figure range. When a targeted entity counter-offered a significantly reduced price from the initial demand, 0APT immediately ended and deleted the chat.

Ransomware actors use this approach to signal that they are not flexible and will not tolerate delay tactics. Play and the now defunct BlackCat/ALPHV ransomware gangs have also used these tactics. This represents a very aggressive negotiation stance. Negotiations with 0APT should be approached with caution and a direct strategy.

Fake Claims Likely Used to Build Reputation

The security community has widely documented that the majority of claimed 0APT victims cannot be independently verified. 0APT data leak downloads contain infinite streams of random data or zero-byte files rather than legitimate exfiltrated data. Additionally, several high-profile organizations listed on the 0APT leak site have publicly stated they found no evidence of compromise.

But false claims do not automatically mean a group does not pose a threat. Groups such as Babuk2 and FunkSec have likewise claimed dozens of victims without substantiating evidence, notably eventually disclosing confirmed victims.

Since 0APT possess a functional encryptor, Halcyon assesses its fake victim strategy likely was designed to and/established reputation, gain media attention, recruit affiliates, or pressure organizations into paying simply to have their names removed from leak sites.

Indicators of Compromise (IOCs)

At the time of this report, Halcyon has not identified known exploited vulnerabilities (KEVs) or additional initial access tactics associated with 0APT. This is consistent with the group's recent emergence and lack of confirmed victim entities.

Type	Indicator	Description
SHA-256	388810cade3472336809550d020f210b54cb9479a76c114a66ad371b108a715a	0APT Windows encryptor
SHA-256	388810cade3472336809550d020f210b54cb9479a76c114a66ad371b108a715a	0APT Windows encryptor
SHA-256	388810cade3472336809550d020f210b54cb9479a76c114a66ad371b108a715a	0APT Linux Encryptor
Blog/ Leak Site	oaptxiyisljt2kv3we2we34kuudmqda7f2geffoylzpeo7ourhtz4dad[.]onion	0APT Blog/ Leak Site
Tox	oaptxiyisljt2kv3we2we34kuudmqda7f2geffoylzpeo7ourhtz4dad[.]onion	qTOX contact information for 0APT
Getsession.org ID	AE7FDDF4ADD95AC3DF29802662DA14C51E95A99992E8E087974AFE1A57481E5381FE429F8BC8	Getsession communication tool contact for 0APT

Mitigation Guidance

0APT's mixed risk profile requires a disciplined, evidence-based response rather than assumptions driven by leak-site claims. In similar cases of inflated claims, some actors such as Babuk2 relied primarily on fabricated or unsubstantiated claims, while others including FunkSec initially faced skepticism before confirmed victims emerged.

0APT currently sits between these patterns. A valid encryptor has been confirmed, but the extent of real-world victimization remains unclear. Organizations that discover their name on a leak site or receive extortion communications, regardless of the threat actor involved, should first confirm compromise before engaging or escalating response actions:

- **Validate Intrusion Evidence:** Determine whether there are confirmed indicators of unauthorized access, lateral movement, credential misuse, or encryption activity within the environment.
- **Authenticate Alleged Exfiltrated Data:** Assess whether any provided sample files can be independently accessed and verified as originating from current internal systems. If alleged exfiltrated data cannot be examined due to restricted access, corrupted files, or non-functional leak site downloads, the claim should be treated as unverified and not assumed to represent confirmed exposure.
- **Correlate Forensic Timelines:** Align claimed intrusion or exfiltration dates with endpoint telemetry, network logs, and security monitoring to determine whether technical evidence supports the actor's assertions.

Evidence, not visibility on a leak site or extortion pressure, should drive response decisions. Organizations should adopt layered defenses aligned to common ransomware tactics: :

- **MHarden Initial Access Vectors:** Reduce exposure from trusted relationships and third-party access pathways [T1199].
- **Limit Lateral Movement and Credential Abuse:** Monitor and restrict Remote Services [T1021] and misuse of Valid Accounts [T1078].
- **Detect Data Staging and Exfiltration:** Monitor for Archive Collected Data [T1560] and Exfiltration Over Command and Control Channel [T1041].
- **Protect Against Encryption Impact:** Ensure resilience against Data Encrypted for Impact [T1486] through tested recovery processes.
- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses to block malicious binaries pre-execution [M1038], detect runtime behaviors and data exfiltration attempts [M1040], prevent tampering and network intrusion [M1031], and protect the integrity of backups to reduce extortion leverage [M1053].

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources here.