halcyon | Ransomware Research Center

0APT vs KryBit: Ransomware Actors List Opposing Operators as Victims

On 13 April 2026, the recently emerged Ransomware-as-a-Service (RaaS) actors 0APT and KryBit began leaking each other's operational and infrastructure data on their respective leak sites. 0APT also claimed to leak data from Everest and RansomHouse ransomware groups.

This type of activity is unusual: 0APT used their initially failing affiliate operation and turned it against not only KryBit, but other ransomware operators. However, the impact to Everest and RansomHouse operations was little to none. KryBit instead retaliated and took over full control of the 0APT data leak site. Both 0APT and KryBit operations likely will now attempt to move and rebuild their infrastructure because of the significant impact of the leaks on each of their operations.

Based on the leaked data, Halcyon assesses:

- 0APT is currently a nominal threat to corporations with its limited operational capacity and fully fabricated victim entries. 0APT maintains minimal levels of technical ability due to their success in obtaining other ransomware actor data.
- KryBit's current activity model gives them the ability to grow as a threat. At present it is an emerging Ransomware-as-a-Service (RaaS) with functional technical and operational skillsets. The ransomware has roughly 20 victims, although they have not obtained any ransom payments to date.
- Everest and RansomHouse are sophisticated ransomware operations and maintain their status as a threat to industry.

Timeline (Halcyon Threat Assessment - April 2026)

● 0APT action ● KryBit action

29 Jan 2026	31 Jan 2026	13 Apr 2026	14 Apr2026	14 Apr 2026	15 Apr 2026
0APT ransomware emerges	KryBit ransomware emerges	0APT leaks KryBit admin panels	0APT leaks Everest infrastructure data	KryBit overtakes 0APT servers	KryBit leaks 0APT operational data
190+ fabricated victim claims posted within first week.	RaaS launches with 80/20 affiliate model; 10 victims in 2 weeks.	Operator, affiliate, and victim negotiation data exposed.	SQL database with publication and user data from Jan to Sep 2025.	Full access gained; 0APT data leak site defaced with KryBit message.	Access logs, PHP source, and system files confirm all 190+ victims were fabricated.

Halcyon Ransomware Research Center - This timeline is derived from dark web monitoring, leak site observations, and published threat intelligence

Background

In January 2026, 0APT Ransomware-as-a-Service (RaaS) emerged with a rapid convergence of 190+ victims posted on its data leak blog within a week. These victim claims were quickly dismissed as fabricated due to the lack of evidence for compromise and the inability to verify leaked data posted to the blog. It is highly likely 0APT published this massive victim list to generate interest in its RaaS program as a means of recruiting affiliates. Halcyon verified the 0APT ransomware operation included functioning encryptors for both Windows and Linux operating systems. However, because of the lack of legitimate victims, the 0APT operation gained little traction and went dormant for 4 months.

KryBit RaaS emerged in late March 2026. The ransomware provided builders for Windows, Linux, ESXI, and NAS devices to affiliates and launched under an 80/20 incentive model, where the affiliates keep 80 percent of ransom payments, and the operator keeps 20 percent. KryBit posted 10 legitimate victims on its dedicated leak site within its first 2 weeks of operation.

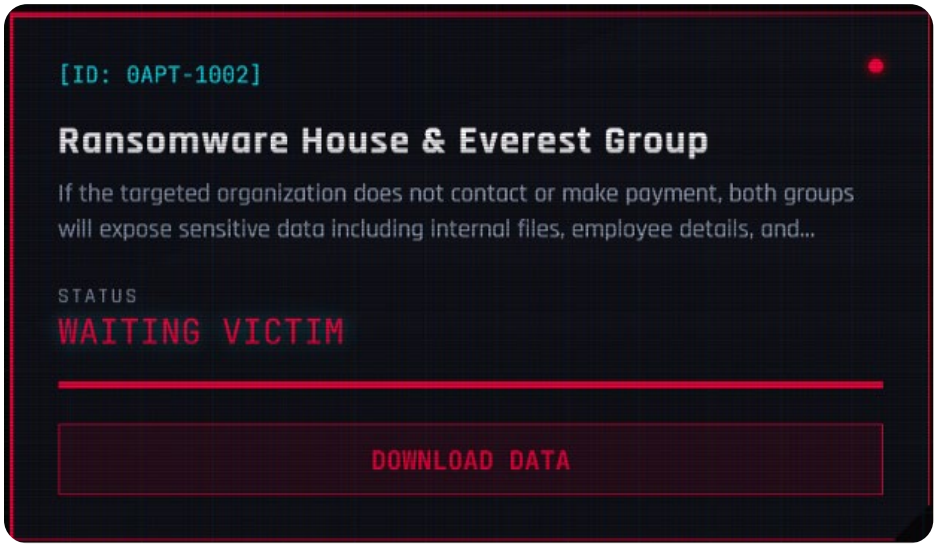
Ransomware Clash

0APT re-emerged in April 2026 by claiming multiple ransomware groups– KryBit, Everest and RansomHouse–as victims. While KryBit is a new operation, Everest Group and RansomHouse are more prominent and longer standing with activity reported as early as 2020.

- Everest is an established actor that has been active since December 2020, using varying data exfiltration-only and encryption campaigns with over 200 listed victims.
- RansomHouse is a RaaS that has been active since 2021 and is known to target education, manufacturing, and healthcare entities.

0APT removed all previous 190+ victim claims from its blog; then listed the ransomware group leaks on their data leak site.

Everest

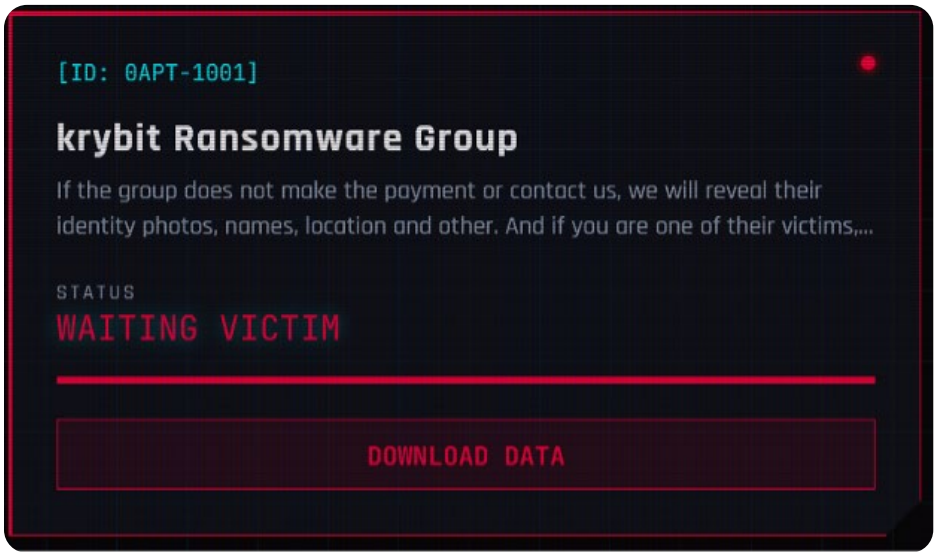


Everest victim post on 0APT leak blog

The SQL database leaked for Everest contains publication and user data. Unlike KryBit, the Everest database records are properly encoded and hashed; they do not contain plaintext information for critical fields. The data records span from 01 January 2025 to 18 September 2025. Notably, there is one administrator user entry that signed up on 29 August 2025. Everest has not publicly retaliated against 0APT or posted any public message regarding the leaked data.

RansomHouse was mentioned in the Everest listing, but RansomHouse data was not included in the leak and therefore not likely impacted by the leak.

KryBit



KryBit victim post on 0APT leak blog

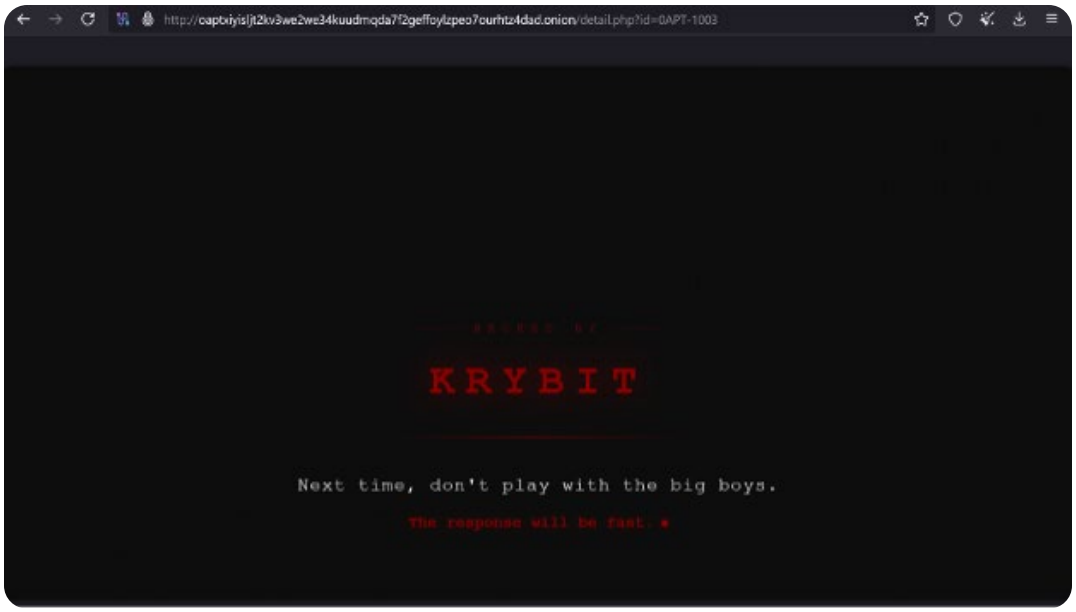
The Krybit leaked data reveals a compact RaaS operation that is ramping up its activity against opportunistic targets across multiple sectors. Due to the exposure of both infrastructure and personnel, Krybit likely will rotate leaked operational components to ensure impact on their activities is limited.

KryBit's leaked administrator panel included data for KryBit's primary operators, affiliates, and victim negotiation data. The activity spanned between 28 March 2026 and 12 April 2026. At the time of the leak, KryBit had 2 administrators and 5 affiliates along with 20 potential victims. The data exfiltrated for each victim ranged between 10 - 250GB and ransom demands between $40,000 - $100,000.

The operators maintained 5 BTC wallets that were reused across affiliates and victims. None of the identified Bitcoin wallets have any transactions, sent or received, nor do any of the victim entries have a "paid_amount" status. Meaning KryBit had no confirmed victim payments at the time of the data leak.

0APT

On 14 April 2026, KryBit retaliated against 0APT by gaining access to and exfiltrating 0APT's infrastructure, posting the 0APT data on the KryBit leak site as a victim, and defacing the 0APT leak site with a custom KryBit message.



Krybit Defacement of 0APT Data Leak Site

KryBit leaked the full 0APT operational data set the following day, which included full access logs, PHP source code, and system files. The access logs revealed that the 190+ victims initially posted by 0APT in January 2026 were entirely fabricated and no data was ever exfiltrated from any of the listed victims.

Additionally, the infrastructure for the ransomware data leak site was operating on an AnLinux-Parrot OS and pushing all content via an Android phone's internal SD card. 0APT has been unable to recover, and KryBit maintains defacement of the 0APT leak site.

Conclusion

0APT attempted to turn a failing affiliate model operation against opposing ransomware actors. The result was a full leak of KryBit and 0APT operations and a partial leak of Everest operations, followed by full disruption of 0APT's own operations. Due to the extensive leaks of both KryBit and 0APT, the operators will likely have to rebuild, rebrand, and spin up new infrastructure over the next few weeks to months to remain active.

Mitigations

- **Gauge Data Leak Site Posts:** Halcyon maintains the assessment that 0APT blog site claims for legitimate companies are unreliable. Companies should not spin up resources investigating 0APT claims. The leaked operational data confirms that all 190+ initial victim entries were fabricated with no evidence of data exfiltration. KryBit and Everest are functional ransomware operations with verified victims and should be treated as legitimate threats to company environments.
- **Monitor for Data Staging and Exfiltration:** KryBit victim data ranged from 10 to 250GB per target, indicating potential dwell time and staging activity prior to encryption. Deploy monitoring for anomalous outbound data transfers, large archive creation, and use of common exfiltration tools [M1057]. Establish baseline thresholds for data egress and alert on deviations.
- **Validate Backup Resilience:** Ensure backup systems are isolated from production networks, tested regularly for restoration integrity, and protected from ransomware encryption and deletion [M1053]. Given that KryBit and similar operations increasingly pursue double-extortion strategies combining data theft with encryption, organizations should assume that backups alone are insufficient without complementary exfiltration detection capabilities.
- **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].

Indicators of Compromise

0APT vs KryBit Threat Assessment - April 2026

Type	Indicator	Description
KryBit Username	KRYBIT	Administrator
Tox ID	F65E1621B7A5DC0139FE108B9CD48404082951E7E7F421A07A7B88A8E8111C13C552EA2B0C4C	Contact Information: KRYBIT
KryBit Username	GREP	Administrator
Tox ID	48B547A7A6195593B9158E4B6160ED0310B2F9AD080992D44EA299878DCCD0551CC7CAD168CD	Contact Information: GREP
KryBit Username	fsociety	Affiliate
Tox ID	0D72935BE65992C164D5BFAFD668ACE2004A317859E360A0851B864AA422EA2E43179699DBE3	Contact Information: fsociety
KryBit Username	M*A*R*S	Affiliate
Tox ID	B7EA3E6CD89496CDC27FC7A4010DCA634D8EED1282EFD5E1FF876C91DD4AA94193403F29B58C	Contact Information: M*A*R*S
KryBit Username	D9D938D9AC9	Affiliate
Tox ID	590586B43A7F5101002EA0167A6E627402512D50B41E1178E484B3DB9616F31ABD9D938D9AC9	Contact Information: D9D938D9AC9
KryBit Username	464D03CA2AF05	Affiliate
Tox ID	AD8A7E310F6A6DA2D39A57B1EB034A28EBD35367FA4CCD832CF74F80C464D03CA2AF0547CBCF	Contact Information: 464D03CA2AF05
KryBit Username	753766EFA0462B	Affiliate
Tox ID	515C7E4F8048813CAFCDEBD915D72E9ACDEC588201B6E941422717D4F80753766EFA0462B8BD	Contact Information: 753766EFA0462B

Type	Indicator	Description
KryBit BTC Wallet	bc1ql2f3mhw6yxammrs9ufklpqf9qlcwrr85u72v4h	Used in 6 negotiations
KryBit BTC Wallet	bc1q5fvym0l0vvzhenhynzduf3qyp85zjdsrn7j8ju	Used in 3 negotiations
KryBit BTC Wallet	bc1qznfsaeyd4j4mzcsgu2a4m0sj5pw6tvrx2vdscl	Used in 3 negotiations
KryBit BTC Wallet	bc1q7uhjsc6qtx933v2wjgmevh63yssjvzfx7cegud	Used in 5 negotiations
KryBit BTC Wallet	bc1qvd3ucrrgzq5eyay5xxn8jerjh669ua6qyz3urk	Used in 1 negotiation
Data Leak Site	oaptxiyisljt2kv3we2we34kuudmqda7f2geffoylzpeo7ourhtz4dad.onion	0APT
Data Leak Site	krybitxdpxohsmjooeb3gbgpmdddreh6mnflzac6bnezz74b7yje67yd.onion	KryBit
Data Leak Site	Ransomocmou6mnbquqz44ewosbkjk3o5qjsl3orawojexfook2j7esad[.]onion	Everest
Data Leak Site	zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion	RansomHouse

References

- Threat Intelligence Report KryBit Ransomware Panel Breach by 0APT
- Everest
- Emerging Ransomware Group 0APT

This report is based on information from dark web monitoring, leak site observations, malware analysis, and published threat intelligence. Assessments may be revised as additional evidence becomes available.

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.