

CrestCon 2025

Rise and Fall of RansomHub



 Triskele Labs

| ransomhub : ~#

Why RAAS?

Classifieds	HiPages
One-off transactions	Centralised Platform for repeat transactions
No Guarantees	Reliable payment methods
High Risk of Scams	Rules in place to minimise scams
No Brand Trust	Brand and Reputation established

The Predecessors

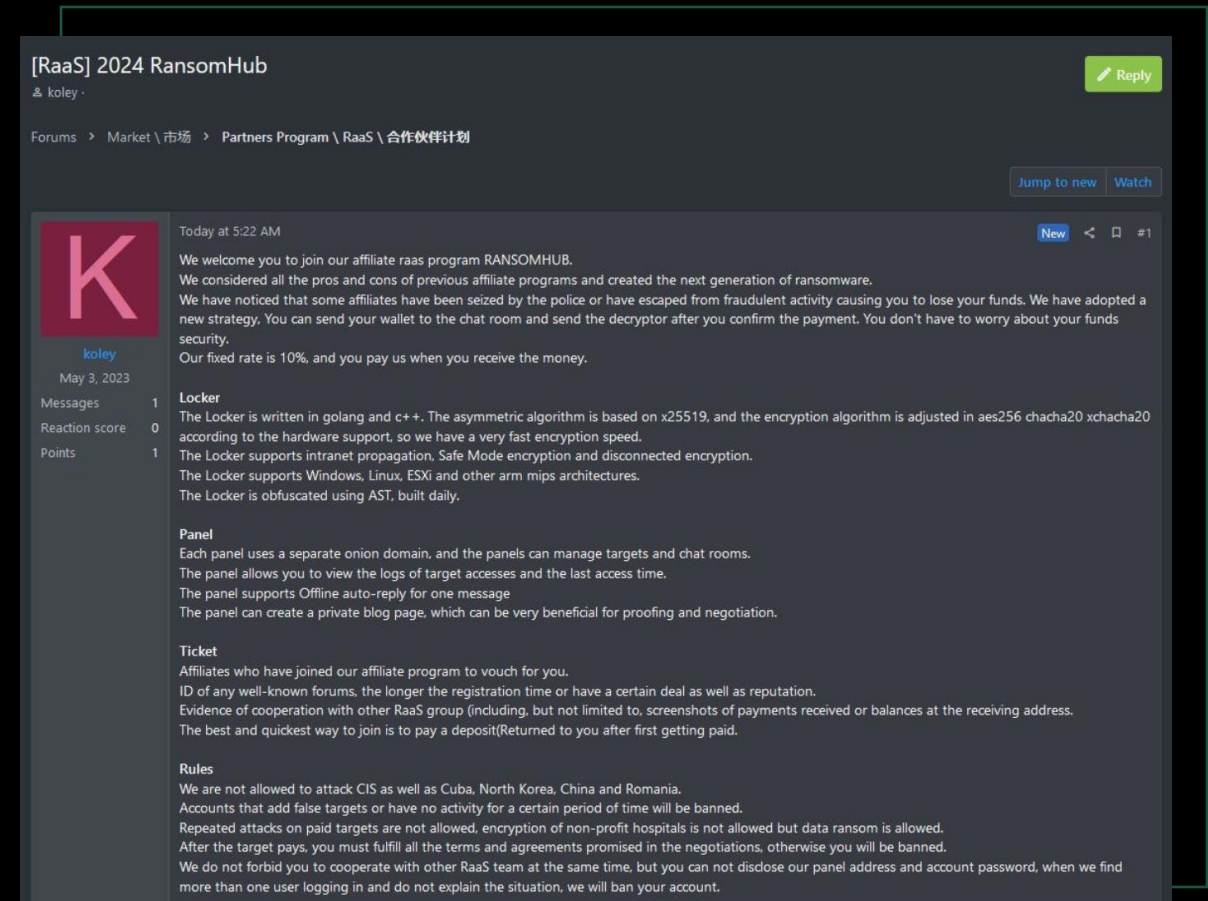
- Nov 23 ● LockBit releases strict negotiation rules for affiliates.
- Dec 23 ● FBI seizes BlackCat leak site; affiliate trust drops.
- Jan 24 ● BlackCat operations resume. Affiliates concerns over security and payments / LockBit affiliates found to be flaunting rules and attacking healthcare.
- Feb 24 ● Operation CRONOS takes down LockBit / ALPHV attack Change Healthcare.
- Mar 24 ● ALPHV site goes dark; affiliate claims to have been scammed by leadership.



RansomHub Launches

02 February 2024

- > Posting made on the popular underground forum RAMP.
- > Advert referenced other groups and advertised itself as “safer”.
- > RansomHub was to take **10%**, compared to **10-25%** at LockBit and BlackCat.
- > “You pay us” was appealing.



The Early Days

**45 victims in
the first 90
days**



First victim published on **10 February 2025**; proof that the group was live and the platform functioned.



Victims were global across US / UK / Europe and South America and seemingly growing.

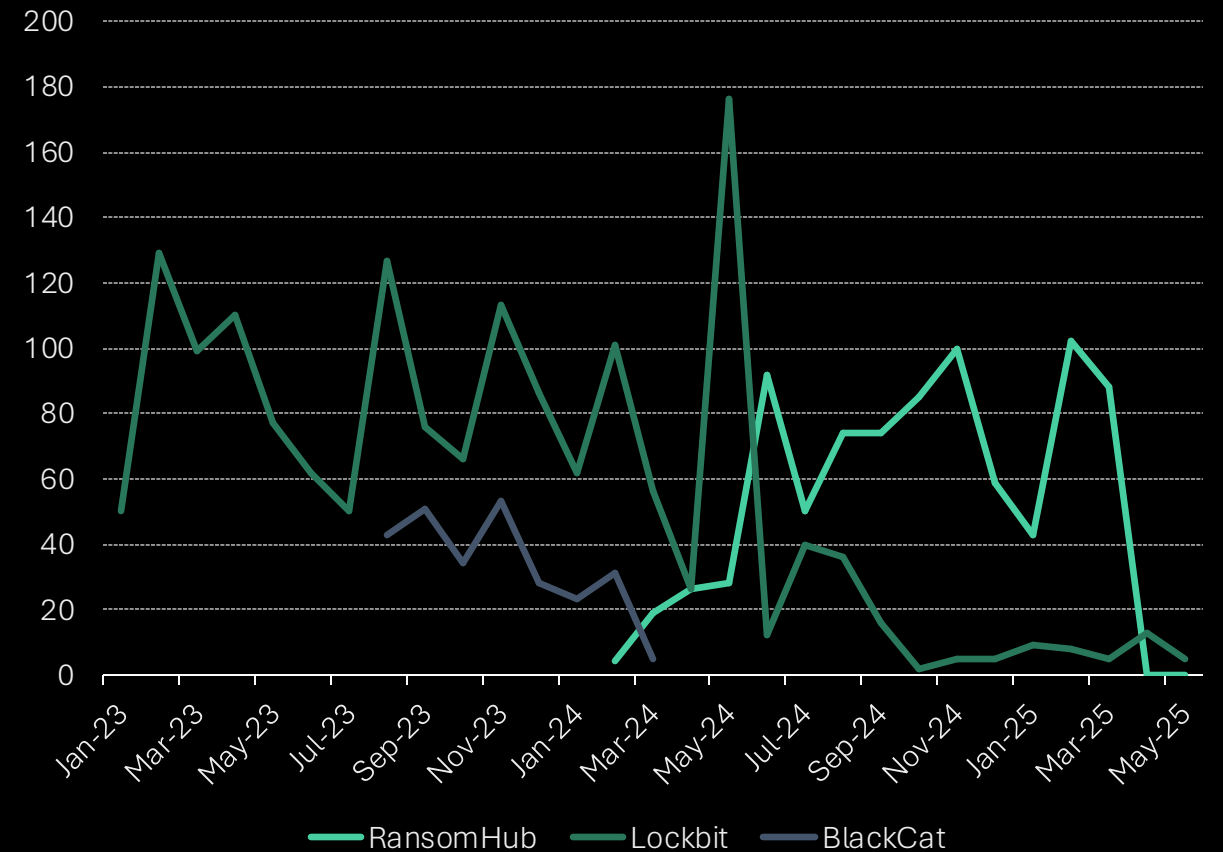


Change Healthcare published on the RansomHub site led to media attention. Evidence of affiliate migration.

The Trust Vacuum

May-June

- > The perfect storm for the emergence of a new ransomware group.
- > Quality leak site, versatile tooling and affiliate-first procedures.
- > Estimated 50M USD revenue in first 6 months.



Tactics

Overview

- > Triskele Labs responded to seven (7) RansomHub matters across 2024-25.
- > These victims were generally profiled as SME with low cyber maturity.

The TTPs of RansomHub

- > Brute Force VPN / RDP
- > SFTP Exfiltration via Mega
- > Backup Reconnaissance
- > Extended dwell times
- > Broad range of persistence mechanisms

Repeated Tactics

FTP IOCs

- > Two victims impacted only days apart.
- > During the first investigation, exfiltration was found to have occurred to a specific Mega IP range.
- > This IOC was used to detect exfiltration during the second response within 30 minutes of engagement.



Not so special

All **hype**, no
innovation



Affiliate Complaints



Overexposure and Visibility



Affiliate Migration to other platforms



Model easily replicated by other groups

RAAS age or Affiliate Age

The perfect conditions to start a RAAS only benefitted affiliates.

- > Affiliates became the life-blood for any RAAS operation.
- > Law enforcement targeted brands, not individuals
- > Affiliates multi-homed and leveraged multiple RAAS toolkits at once.



Decline of RansomHub_

Enter DragonForce

From Hacktivism to Hostile Takeover

- > Originally a hacktivist group, pivoted to ransomware late 2024.
- > Actively targeted RansomHub affiliates to join their program.
- > Disenfranchised affiliates continued to complain as RansomHub founder went quiet.
- > Ended in a suspected hostile takeover of RansomHub infrastructure.



**Absence of
direction and
transparency ...
koley is silent.**

- RansomHub Affiliate



Now What_

Ransomware in 2025

No one is safe... still

- > RAAS groups continue to support the bulk exploitation of low-maturity companies.
- > High-sophistication affiliates (i.e. Scatter Spider) can hide behind RAAS brand names.
- > RAAS groups are now a dime-a-dozen.

RansomHub

R.I.P. (03.03.2025)



Thank you

 Triskele Labs