BIANLIAN AS RANSOMHUB AFFILIATE

CRITICALSTART®

Timeline

Jan 2023

- Avast develops a decryptor for BianLian ransomware.
  - https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/

Feb 2024

- ALPHV/BlackCat ransoms Change Healthcare, $22 Mil paid in Bitcoin.
  - https://www.cpomagazine.com/cyber-security/under-increasing-federal-scrutiny-blackcat-ransomware-gang-pulls-exit-scam-on-its-way-out/
  - https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/
- Law enforcement disrupts LockBit operations, taking down infrastructure and arresting some members. They are back up in ~6 days, continuing to claim victims.
  - https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
- Knight ransomware disbands and offers their source code for sale.
  - https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware
- RansomHub (likely a rebrand of Knight) claims their first victim and grows very quickly over the following months, offering affiliates direct control over ransom payments.
  - https://www.forescout.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/

March 2024

- ALPHV/BlackCat does not pay affiliate (attributed as “Notchy”) and appears to disband, pretending to have been seized by law enforcement. This is considered an exit scam by current BlackCat affiliates.
  - https://www.forescout.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/

April 2024

- RansomHub shares sensitive information from Change breach and threatens to publish. They claim they have the data and not ALPHV/BlackCat. This is likely Notchy attempting to extort funds that were not paid to them by APLHV/BlackCat.
  - https://www.tripwire.com/state-of-security/ransomhub-ransomware-what-you-need-know

May 2024

- LockBit claims “Longview & Salmon Creek Oral Surgery and Periodontics” (longviewoms.com) as a victim.
  - https://ransomwareattacks.halcyon.ai/attacks/lockbit3-ransomware-attack-on-dental-practice-vulnerabilities-and-impact

Timeline (continued)

June 2024

- The FBI announces they have 7000 LockBit decryption keys for victims of LockBit as ongoing disruption attempt starting in February.
  - https://www.fbi.gov/news/speeches/fbi-cyber-assistant-director-bryan-vorndran-s-remarks-at-the-2024-boston-conference-on-cyber-security
- BianLian claims “Longview Oral & Maxillofacial Surgery” (longviewoms.com) as a victim.
  - https://www.hendryadrian.com/ransom-longview-oral-maxillofacial-surgery/

July 2024

- Microsoft incident response announces Scattered Spider has switched to RansomHub and Qilin RaaS.
  - https://www.theregister.com/2024/07/16/scattered_spider_ransom/

Conclusions

After BianLian's encryptor was rendered obsolete by Avast in 2023, they seem to have moved to using RaaS like LockBit. Ongoing disruptions from law enforcement since February likely stopped them from getting paid by LockBit. In attempt to extort a victim (longviewoms.com) who's files may have been decrypted by FBI obtained keys, they seem to have claimed the attack under their own brand one month after LockBit did.

After BlackCat exit scammed, actors such as Notchy and Scattered Spider moved to RansomHub due to their policy of allowing the affiliate to accept ransom payments for themselves before forwarding a cut to RansomHub operators. This policy, combined with the recent BlackCat exit scam, would explain RansomHub's rapid expansion. Based on what we've seen from Bartlett Cocke, it is likely BianLian has also become a RansomHub affiliate.

About Critical Start CTI

To stay ahead of emerging threats, the Critical Start Cyber Threat Intelligence (**CTI**) team leverages a variety of intelligence sources, including open-source intelligence, social media monitoring, and dark web monitoring.

As a part of the Critical Start Cyber Research Unit (**CRU**), CTI monitors emerging threat developments and works closely with the Security Engineering and RSOC teams to implement any relevant detections. For future updates on emerging threats, follow our Critical Start Intelligence Hub.

For more information, contact us at:
https://www.criticalstart.com/contact/