ALPHV/BlackCat ransomware family becoming more dangerous

computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous

Alex Scroxton

Sikov - stock.adobe.com

News

Researchers from Symantec share fresh insight into the ongoing development of the ransomware-as-a-service family known variously as ALPHV, BlackCat and Noberus

-
-
-
  -
  -
  -
  -

By

Alex Scroxton, Security Editor

Published: 22 Sep 2022 11:00

The developer or developers behind the ransomware-as-a-service (RaaS) family known variously as ALPHV, BlackCat and Noberus, have been hard at work refining their tactics, techniques and procedures (TTPs) and today are probably more dangerous than ever before, according to intelligence from Symantec.

The ALPHV/BlackCat/Noberus operation – which Symantec tracks as Coreid (aka FIN7, Carbon Spider) – is a major and long-established player in the wider family of Russia-linked or based ransomware crews and affiliates, many of which are related through a murky and often hard-to-decipher web of alliances and interconnections.

It is known to date back at least a decade, when it established the use of a malware called Carbanak, but these days is more famous for its ransomware op, with alleged links to the BlackMatter group, which in turn drew inspiration from the DarkSide operation that turned over Colonial Pipeline and via them possibly REvil.

The ALPHV/BlackCat/Noberus ransomware gained notoriety earlier in 2022 with a series of audacious heists targeting fuel logistics and transportation services operators in Europe, and on educational institutions in the US.

The malware itself is coded in Rust, one of a group of multiplatform languages that are becoming increasingly valued by RaaS operators for its flexibility, and ability to quickly and easily target both Windows and Linux environments.

Now, Symantec says it has observed a series of major updates to the ransomware and to Coreid's overall modus operandi.

"The continuous updating and refining of Noberus' operations shows that Coreid is constantly adapting its ransomware operation to ensure it remains as effective as possible," wrote Symantec's team.

"The FBI issued a warning in April 2022 saying that, between November 2021 and March 2022, at least 60 organisations worldwide had been compromised with the Noberus ransomware – the number of victims now is likely to be many multiples of that."

A new update, which dropped in June 2022, included an ARM build to encrypt non-standard architectures, and introduced a feature that adds new encryption functionality to its Windows build via rebooting into safe mode and safe mode with networking.

It also updated the locker itself, adding new restart logic and simplifying the Linux encryption process. An additional update in July added indexing of stolen data, making the group's data leak website(s) searchable by parameters including keywords and file types.

But the group did not stop there. In August, Symantec says it observed an updated version of the Exmatter data exfiltration tool being used alongside ALPHV/BlackCat/Noberus in attacks – this had previously been seen being used alongside the BlackMatter ransomware,

which is designed to steal specific file types from selected directories and upload them to the attacker's server prior to deployment of the ransomware.

As of this summer, Exmatter includes refinements to the types of files it steals, the addition of file transfer protocol (FTP) capabilities in addition to SFTO and WebDav, the ability to create reports listing processed files, the ability to corrupt them, and a self-destruct option, among other things. It has also been extensively rewritten, possibly in a bid to avoid detection.

One ALPHV/BlackCat/Noberus affiliate has also been observed using the Eamfo infostealer to target credentials stored by Veeam backup software – it does this by connecting to the Veeam SQL database and making a specific query, and may also have been used by LockBit and Yanluowang.

Targeting Veeam for credential theft is an established technique that comes in handy from a malicious point of view because it enables privilege escalation and lateral movement, and therefore gives one more access to data to steal and encrypt.

"There's no doubt that Coreid is one of the most dangerous and active ransomware developers operating at the moment," wrote the Symantec team.

"The group has been around since 2012 and became well-known for using its Carbanak malware to steal money from organisations worldwide, with the banking, hospitality and retail sectors among its preferred targets. Three members of the group were arrested in 2018, and in 2020 the group changed its tactics and launched its ransomware-as-a-service operation.

"Its continuous development of its ransomware and its affiliate programs indicates that this sophisticated and well-resourced attacker has little intention of going anywhere anytime soon," they said.

Read more about ransomware

- Current and former CISA members say the best methods for curbing ransomware attacks are organisations reporting attacks and assisting in investigations.
- Prevention and protection are often the focus of ransomware discussions, but IT teams must understand ransomware's effects on operations and how to react in an attack scenario.

Read more on Hackers and cybercrime prevention

- 

  Vice Society cyber gang targeted multiple UK schools

  

  By: Alex Scroxton

- 

  Vice Society ransomware 'persistent threat' to education sector

  

  By: Arielle Waldman

- 
  LockBit ransomware activity nose-dived in October

  
  By: Shaun Nichols
- 
  Ransomware crews regrouping as LockBit rise continues

  
  By: Alex Scroxton

Latest News

- Tech Nation to shutter after more than a decade
- Cyber training firm launches £20k data protection scholarship
- Russian DDoS hacktivists seen targeting western hospitals

- View All News

Download Computer Weekly

In The Current Issue:

- How the cost-of-living crisis is affecting IT
- Reverse cloud migrations: shifting IT back on-premise

Download Current Issue