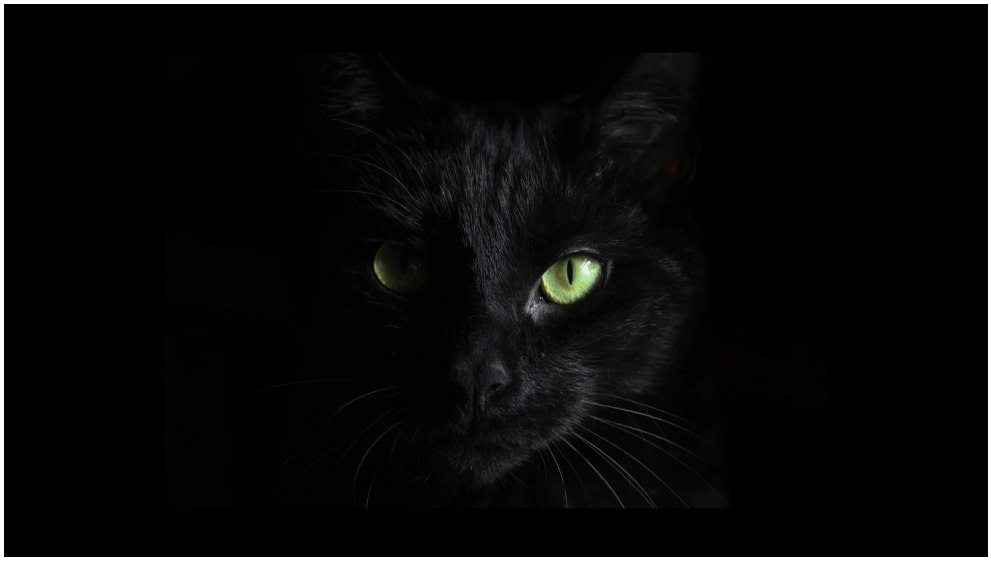
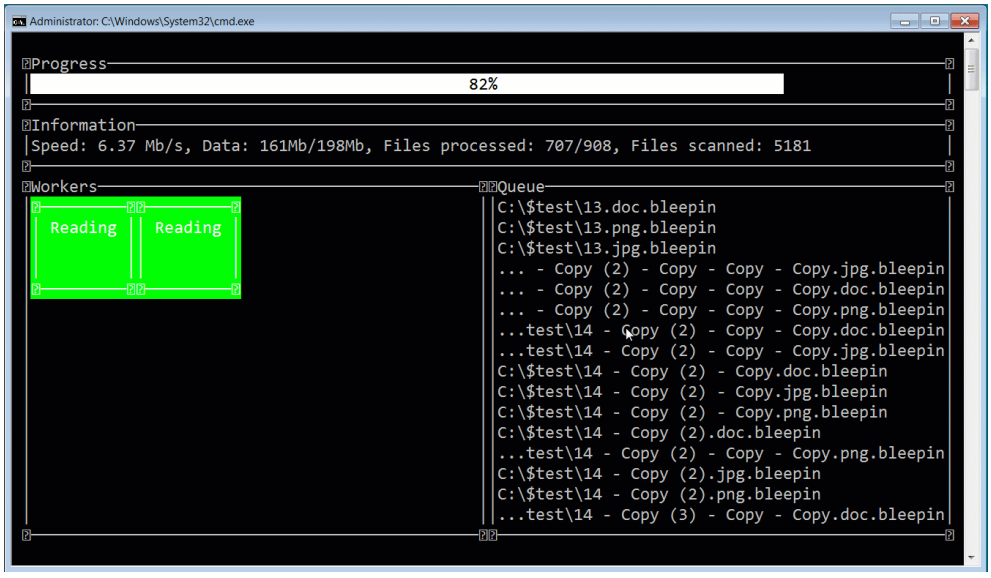
By
Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)

February 5, 2022 05:29 PM **0**



BlackCat/ALPHV is a new feature-rich ransomware operation (https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/) launched in November 2021 and developed in the Rust programming language, which is unusual for ransomware infections.

The ransomware executable is highly customizable, with different encryption methods and options allowing for attacks on a wide range of corporate environments.



BlackCat / ALPHV encrypting a computer

While the ransomware gang calls themselves ALPHV, security researcher MalwareHunterTeam named the ransomware BlackCat (https://twitter.com/malwrhunterteam/status/1468713125457371139) after the image of a black cat used on every victim's Tor payment page.

A brief history on ransomware rebrands

Many ransomware operations are run as a Ransomware-as-a-Service (RaaS), where core members are in charge of developing the ransomware infection and managing servers, while affiliates (aka "adverts") are recruited to breach corporate networks and conduct attacks.

As part of this arrangement, the core developers earn between 10-30% of a ransom payment, while the affiliate earns the rest. The percentages change based on how much ransom revenue a particular affiliate brings to the operation.

While there have been many RaaS operations in the past, there have been a few top-tier gangs that commonly shut down when law enforcement is breathing down their neck and then rebrand under new names.

These top-tier Ransomware-as-a-Service operations and their rebrands are:

- **GandCrab to REvil**: The GandCrab ransomware operation launched (https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/) in January 2018 and shut down in June 2019 after claiming to earn $2

(https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-via-fake-forums-on-hacked-sites/) in September 2019, which ultimately shut down in October 2021 (https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/) after law enforcement hijacked their infrastructure.

- **Maze to Egregor**: The Maze ransomware began operating in May 2019 (https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/) and formally announced its shutdown (https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/) in October 2020. However, affiliates, and likely the operators, are believed to have rebranded in September as Egregor (https://www.bleepingcomputer.com/news/security/crytek-hit-by-egregor-ransomware-ubisoft-data-leaked/), who later disappeared after members were arrested in Ukraine (http://law%20enforcement%20operations.).

2022 and shut down in May 2021 (https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/) due to law enforcement operations spurred by the gang's widely publicized attack on Colonial Pipeline (https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/). They returned as BlackMatter (http://returned%20as%C2%A0BlackMa) on July 31st but soon shut down (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-claims-to-be-shutting-down-due-to-police-pressure/) in November 2021 after Emsisoft exploited a weakness to create a decryptor (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-victims-quietly-helped-using-secret-decryptor/) and servers were seized.

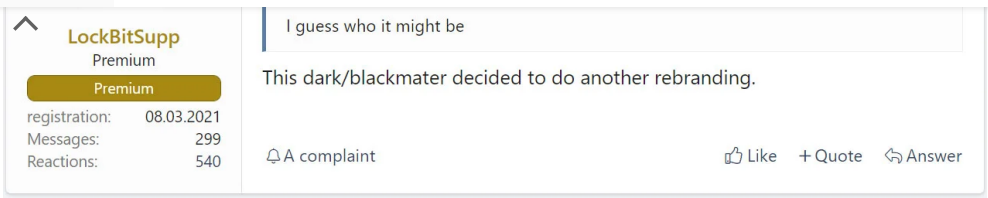
Some believe that Conti was a rebrand of Ryuk, but sources tell BleepingComputer that they are both discrete operations run by the TrickBot Group and are not affiliated with each other.

While some affiliates tend to partner with a single RaaS operation, it is common for affiliates and penetration testers to partner with multiple

For example, a ransomware affiliate told BleepingComputer that they worked with Ragnar Locker, Maze, and the REvil ransomware operations simultaneously.

BlackCat rises from BlackMatter's ashes

Since BlackCat ransomware launched in November, the representative of the LockBit ransomware gang has stated that ALPHV/BlackCat is a rebrand of DarkSide/BlackMatter.



LockBit representative stating ALPH is a DarkSide rebrand

The Record published an interview with the ALPHV/BlackCat gang (https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/), who confirmed suspicions that they were affiliated with the DarkSide/BlackMatter gang.

"As adverts of darkmatter [DarkSide / BlackMatter], we suffered from the interception of victims for subsequent decryption (https://blog.emsisoft.com/en/39181/on-the-matter-of-blackmatter/) by Emsisoft," ALPHV told The Record, referring to the release of Emsisoft's decryptor (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-victims-quietly-helped-using-secret-decryptor/).

While the BlackCat ransomware operators claim that they were only DarkSide/BlackMatter affiliates who launched their own ransomware operation, some security researchers are not buying it.

ransoms.

"While Alphv claim to be former DS/BM affiliates, it's more likely that they *are* DS/BM but attempting to distance themselves from that brand due to the reputational hit it took after making an error that cost affiliates multiple millions of dollars," Callow tweeted (https://twitter.com/BrettCallow/status/1489644504109895687) yesterday.

In the past, it was possible to prove that different ransomware operations were related by looking for code similarities in the encryptor's code.

As the BlackCat encryptor has been built from scratch in the Rust programming language, Emsisoft's Fabian Wosar (https://twitter.com/fwosar) told BleepingComputer that these coding similarities no longer exist.

However, Wosar said that there are similarities in the features and configuration files, supporting that it is the same group behind the BlackCat and the DarkSide/BlackMatter ransomware operations.

BlackCat is going to be a ransomware operation that all law enforcement, network defenders, and security professionals need to keep a close eye on.

Gang repeats their mistakes

Ironically, what led to the downfall of the DarkSide/BlackMatter operations may ultimately be what causes a quick demise for BlackCat/ALPHV.

After DarkSide attacked the Colonial Pipeline, the largest fuel pipeline in the US government.

This pressure continued after they rebranded as BlackMatter, with law enforcement seizing their servers and causing them to shut down again.

What may have thrust the BlackCat ransomware into the spotlight is ironically another attack on oil suppliers and distribution companies, leading to supply chain issues.

This week, BlackCat attacked Oiltanking (https://www.bleepingcomputer.com/news/security/german-petrol-supply-firm-oiltanking-paralyzed-by-cyber-attack/), a German petrol distributor, and Mabanaft GmbH, an oil supplier.

These attacks once again affected the fuel supply chain and caused gas shortages.

The BlackCat operators, though, told The Record that they could not control who their affiliates attack and ban those that are non-compliant with the gang's policies. These policies state that affiliates should not target government agencies, healthcare, or educational entities.