This is a BlackCat you don't want crossing your path

By Jeff Burt

Published: 2022-03-22 · Archived: 2026-04-05 23:35:08 UTC

Cybersecurity researchers with Cisco have outlined probable links between the BlackMatter/DarkSide ransomware ring responsible for last year's high-profile raid on the Colonial Pipeline, and an emerging ransomware-as-a-service product dubbed BlackCat.

In a write-up this month, Cisco's Talos threat intelligence unit said a domain name and IP addresses used in a BlackCat infection in December had also been used in a BlackMatter ransomware deployment three months earlier.

In addition, the team outlined tools, file names, and techniques that are common to both the BlackMatter and BlackCat ransomware variants. As a ransomware-as-a-service (RaaS) operation, BlackCat can be rented by criminal affiliates to infect and extort targets, with the malware's developers typically getting a cut of the ransom.

Given that the affiliates are individually responsible for compromising their victims' systems and deploying the actual ransomware binaries, "it is likely that attacks carried out by the same ransomware family may differ in techniques and procedures," Talos's Tiago Pereira and Caitlin Huey noted. In other words, affiliates infect victims in different ways with the same ransomware.

At the same time, RaaS operators often make training materials, general techniques, and tools available to affiliates – as shown by the documents leaked from the Conti ransomware gang – so you'd expect to see some similarities in the attacks carried out by these miscreants.

Still, each ransomware strain should have its own command-and-control (C2) systems, and yet overlapping C2 resources were seen in BlackMatter and BlackCat infections, fueling rumors of strong ties between the two. The Talos team further speculated that "a BlackMatter affiliate was likely an early adopter – possibly in the first month of operation – of BlackCat."

This is interesting because it sheds some light on the interconnected networks of criminals menacing organizations. It's also useful to know what to look out for when defending against or gaining early detection of this kind of ransomware.

Those rumors of a close connection began as soon as BlackCat caught the attention of cybersecurity vendors and researchers. The MalwareHunter Team tweeted about the ransomware group in December and other threat intelligence groups, such as S2W out of South Korea, reported similarities between some of configuration fields used by both BlackCat and BlackMatter.

However, there also were differences. For instance, BlackCat was written in Rust, while ransomware from both DarkSide and BlackMatter – the latter a rebranded DarkSide group – were written in C/C++, S2W wrote in an analysis.

Speaking of malware... Pradeo says it has spotted an **Android app** installed more than 100,000 times from the Google Play Store that has a trojan in it called Facestealer. This socially engineers victims into handing over their Facebook login details, which are passed to a Russian server. The app in question was Craftsart Cartoon Photo Tools, which has since been removed by Google. If for some reason you have it installed, get rid of it.

Mandiant has documented the activities of a team it's called **UNC2891** and its targeting of Solaris systems with backdoors dubbed TINYSHELL and SLAPSTICK and a rootkit called CAKETAP. It is believed CAKETAP was used to alter messages on ATM networks to pull off fraudulent withdrawals from banks using bogus payment cards. UNC2891, we're told, is skilled on Unix and Linux-flavored machines, is financially motivated, and has gone for years undetected in large systems.

A BlackCat representative in a February interview with Recorded Future said the two groups had a "connection" but that BlackCat was not a rebranding of BlackMatter.

The representative also said BlackCat is an affiliate of other RaaS groups, and that they took knowledge from other outfits. If true, BlackCat is an example of vertical business expansion – controlling the upstream supply chain by making a service better suited for their needs and adding another potential avenue for revenue, the Talos researchers wrote.

Vertical expansion also is a business strategy when there is distrust in the supply chain.

"There are several cases of vulnerabilities in ransomware encryption and even of backdoors that can explain a lack of trust in RaaS," they wrote. "One particular case mentioned by the BlackCat representative was a flaw in DarkSide/Blackmatter ransomware allowing victims to decrypt their files without paying the ransom. Victims used this vulnerability for several months, resulting in big losses for affiliates."

Double blow

BlackCat – also known as ALPHV – is being used in double-ransomware attacks, where the files not only are encrypted but victims are threatened with public disclosure of the files if the ransom isn't paid. BlackCat first appeared in November 2021 and has infected several companies in different parts of the world. That said, more than 30 percent of the compromises have hit US-based companies, according to Talos.

- Exotic Lily is a business-like access broker for ransomware gangs
- CISOs face 'perfect storm' of ransomware and state-supported cybercrime
- Has Trickbot gang hijacked your router? This scanner may have an answer
- LokiLocker ransomware family spotted with built-in wiper
- Ransomware crim: Yeah, what I do is bad. No, I don't care. Yes, infosec bods are all mouth and no trousers
- Ransomware crims saying 'We'll burn your data if you get a negotiator' can't be legally paid off anyway

When comparing the BlackMatter intrusion in September and the BlackCat one in December, the Talos team believed the pair of cyber-attacks were run by the same affiliate. Both raids went the usual way: an initial compromise followed by exploration and data exfiltration, preparation, and then execution of the extortionware.

There were further similarities: for both the BlackMatter and BlackCat infections, the methods to achieve persistence – a reverse SSH tunnel and scheduled tasks – were the same as well as lateral movements and the C2

domain. In addition, local and domain user credentials were collected on some key systems by dumping the LSASS process memory and extracting the credentials with Microsoft Sysinternals Procdump and Dumpert.

"In both attacks, before the actual execution of the ransomware, the attackers performed several actions preparing systems to make the execution as successful as possible," the researchers wrote. "On the day of the attack, the attacker logged in to the domain controller and opened the group policy management interface. The attackers then dropped and executed a file named 'apply.ps1.' We believe this script created and prepared the group policy to cause the execution of the ransomware throughout the domain."

The researchers admitted they still don't know how tightly related BlackCat is to BlackMatter, but that given the overlapping tools, techniques, and infrastructure of the two infections, they have "moderate confidence" that BlackMatter affiliates were probably among the early adopters of BlackCat.

"As we have seen several times before, RaaS services come and go," they wrote. "Their affiliates, however, are likely to simply move on to a new service. And with them, many of their TTPs [techniques, tactics and procedures] are likely to persist." ®
