

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

 theregister.com/2022/03/22/talos-ransomware-blackcat/

Jeff Burt



Security

Plus: Android trojan in 100,000+ app installs, Solaris malware

Jeff Burt Tue 22 Mar 2022 // 05:29 UTC

3 

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.

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." ®

Other stories you might like

- [Big Tech loves talking up privacy – while trying to kill privacy legislation](#)

[Study claims Amazon, Apple, Google, Meta, Microsoft work to derail data rules](#)

[Thomas Claburn in San Francisco](#) Fri 27 May 2022 // 21:48 UTC 

Amazon, Apple, Google, Meta, and Microsoft often support privacy in public statements, but behind the scenes they've been working through some common organizations to weaken or kill privacy legislation in US states.

That's according to [a report](#) this week from news non-profit The Markup, which said the corporations hire lobbyists from the same few groups and law firms to defang or drown state privacy bills.

The report examined 31 states when state legislatures were considering privacy legislation and identified 445 lobbyists and lobbying firms working on behalf of Amazon, Apple, Google, Meta, and Microsoft, along with industry groups like TechNet and the State Privacy and Security Coalition.

[Continue reading](#)

- [SEC probes Musk for not properly disclosing Twitter stake](#)

[Meanwhile, social network's board rejects resignation of one its directors](#)

[Katyanna Quach](#) Fri 27 May 2022 // 21:26 UTC 

America's financial watchdog is investigating whether Elon Musk adequately disclosed his purchase of Twitter shares last month, just as his bid to take over the social media company hangs in the balance.

A letter [[PDF](#)] from the SEC addressed to the tech billionaire said he "[did] not appear" to have filed the proper form detailing his 9.2 percent [stake](#) in Twitter "required 10 days from the date of acquisition," and asked him to provide more information. Musk's shares made him one of Twitter's largest shareholders.

Musk quickly moved to try and buy the whole company outright in a deal initially worth over \$44 billion. Musk sold a chunk of his shares in Tesla worth \$8.4 billion and [bagged](#) another \$7.14 billion from investors to help finance the \$21 billion he [promised](#) to put forward for the deal. The remaining \$25.5 billion bill was secured via debt financing by Morgan Stanley, Bank of America, Barclays, and others. But the takeover is not going smoothly.

[Continue reading](#)

- [Cloud security unicorn cuts 20% of staff after raising \\$1.3b](#)

[Time to play blame bingo: Markets? Profits? Too much growth? Russia? Space aliens?](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 19:19 UTC [2](#) 

Cloud security company Lacework has laid off 20 percent of its employees, just months after two record-breaking funding rounds pushed its valuation to \$8.3 billion.

A spokesperson wouldn't confirm the total number of employees affected, though told *The Register* that the "widely speculated number on Twitter is a significant overestimate."

The company, as of March, counted more than [1,000 employees](#), which would push the jobs lost above 200. And the widely reported number on Twitter is about [300 employees](#). The biz, based in Silicon Valley, was founded in 2015.

[Continue reading](#)

- [Talos names eight deadly sins in widely used industrial software](#)

[Entire swaths of gear relies on vulnerability-laden Open Automation Software \(OAS\)](#)

[Jeff Burt](#) Fri 27 May 2022 // 18:30 UTC 

A researcher at Cisco's Talos threat intelligence team found eight vulnerabilities in the Open Automation Software (OAS) platform that, if exploited, could enable a bad actor to access a device and run code on a targeted system.

The OAS platform is widely used by a range of industrial enterprises, essentially facilitating the transfer of data within an IT environment between hardware and software and playing a central role in organizations' industrial Internet of Things (IIoT) efforts. It touches a range of devices, including PLCs and OPCs and IoT devices, as well as custom applications and APIs, databases and edge systems.

Companies like Volvo, General Dynamics, JBT Aerotech and wind-turbine maker AES are among the users of the OAS platform.

[Continue reading](#)

- [Despite global uncertainty, \\$500m hit doesn't rattle Nvidia execs](#)

[CEO acknowledges impact of war, pandemic but says fundamentals 'are really good'](#)

[Dylan Martin](#) Fri 27 May 2022 // 16:08 UTC [1](#) 

Nvidia is expecting a \$500 million hit to its global datacenter and consumer business in the second quarter due to COVID lockdowns in China and Russia's invasion of Ukraine. Despite those and other macroeconomic concerns, executives are still optimistic about future prospects.


"The full impact and duration of the war in Ukraine and COVID lockdowns in China is difficult to predict. However, the impact of our technology and our market opportunities remain unchanged," said Jensen Huang, Nvidia's CEO and co-founder, during the company's first-quarter earnings call.

Those two statements might sound a little contradictory, including to some investors, particularly following the [stock selloff](#) yesterday after concerns over Russia and China prompted Nvidia to issue lower-than-expected guidance for second-quarter revenue.

[Continue reading](#)

- [Another AI supercomputer from HPE: Champollion lands in France](#)

[That's the second in a week following similar system in Munich also aimed at researchers](#)

[Dan Robinson](#) Fri 27 May 2022 // 15:30 UTC 

HPE is lifting the lid on a new AI supercomputer – the second this week – aimed at building and training larger machine learning models to underpin research.

Based at HPE's Center of Excellence in Grenoble, France, the new supercomputer is to be named Champollion after the French scholar who made advances in deciphering Egyptian hieroglyphs in the 19th century. It was built in partnership with Nvidia using AMD-based Apollo computer nodes fitted with Nvidia's A100 GPUs.

Champollion brings together HPC and purpose-built AI technologies to train machine learning models at scale and unlock results faster, HPE said. HPE already provides HPC and AI resources from its Grenoble facilities for customers, and the broader research community to access, and said it plans to provide access to Champollion for scientists and engineers globally to accelerate testing of their AI models and research.

[Continue reading](#)

- [Workday nearly doubles losses as waves of deals pushed back](#)

[Figures disappoint analysts as SaaS HR and finance application vendor navigates economic uncertainty](#)

[Lindsay Clark](#) Fri 27 May 2022 // 14:30 UTC 

HR and finance application vendor Workday's CEO, Aneel Bhusri, confirmed deal wins expected for the three-month period ending April 30 were being pushed back until later in 2022.

The SaaS company boss was speaking as Workday recorded an operating loss of \$72.8 million in its first quarter [[PDF](#)] of fiscal '23, nearly double the \$38.3 million loss recorded for the same period a year earlier. Workday also saw revenue increase to \$1.43 billion in the period, up 22 percent year-on-year.

However, the company increased its revenue guidance for the full financial year. It said revenues would be between \$5.537 billion and \$5.557 billion, an increase of 22 percent on earlier estimates.

[Continue reading](#)

- [UK monopoly watchdog investigates Google's online advertising business](#)

[Another probe? Mountain View is starting to look like a pincushion at this rate](#)

[Richard Currie](#) Fri 27 May 2022 // 14:00 UTC **3** 

The UK's Competition and Markets Authority is lining up yet another investigation into Google over its dominance of the digital advertising market.

This latest inquiry, [announced Thursday](#), is the second major UK antitrust investigation into Google this year alone. In March this year the UK, together with the European Union, said it wished to examine Google's "[Jedi Blue](#)" [agreement](#) with Meta to allegedly favor the former's Open Bidding ads platform.

The news also follows [proposals](#) last week by a bipartisan group of US lawmakers to create legislation that could force Alphabet's Google, Meta's Facebook, and Amazon to divest portions of their ad businesses.

[Continue reading](#)

- [Microsoft slows some hiring for Windows, Teams, and Office](#)

['Making sure the right resources are aligned to the right opportunity' ahead of next fiscal year](#)

[Richard Speed](#) Fri 27 May 2022 // 13:31 UTC **4** 

Microsoft has hit the brakes on hiring in some key product areas as the company prepares for the next fiscal year and all that might bring.

According to reports in the [Bloomberg](#), the unit that develops Windows, Office, and Teams is affected and while headcount remains expected to grow, new hires in that division must first be approved by bosses.

During a talk this week at JP Morgan's Technology, Media and Communications Conference, Rajesh Jha, executive VP for the Office Product Group, noted that within three years he expected approximately two-thirds of CIOs to standardize on Microsoft Teams. 1.4 billion PCs were running Windows. He also remarked: "We have lots of room here to grow the seats with Office 365."

[Continue reading](#)

- [Recession fears only stoking enterprise tech spending for Dell, others](#)

[Staving off entropy with digital transformation, hybrid office, and automation projects](#)

[Paul Kunert](#) Fri 27 May 2022 // 13:00 UTC 

Enterprises are still kitting out their workforce with the latest computers and refreshing their datacenter hardware despite a growing number of "uncertainties" in the world.

This is according to hardware tech bellwethers including Dell, which turned over \$26.1 billion in sales for its [Q1 of fiscal 2023 ended 29 April](#), a year-on-year increase of 16 percent.

"We are seeing a shift in spend from consumer and PCs to datacenter infrastructure," said Jeff Clarke, vice-chairman and co-chief operating officer. "IT demand is currently healthy," he added.

[Continue reading](#)

- [GitHub saved plaintext passwords of npm users in log files, post mortem reveals](#)

[Unrelated to the OAuth token attack, but still troubling as org reveals details of around 100,000 users were grabbed by the baddies](#)

[Richard Speed](#) Fri 27 May 2022 // 12:15 UTC 

GitHub has revealed it stored a "number of plaintext user credentials for the npm registry" in internal logs following the integration of the JavaScript package registry into GitHub's logging systems.

The information came to light when the company [today published](#) the results of its investigation into April's unrelated OAuth token theft attack, where it described how an attacker grabbed data including the details of approximately 100,000 npm users.

The code shack went on to assure users that the relevant log files had not been leaked in any data breach; that it had improved the log cleanup; and that it removed the logs in question "prior to the attack on npm."

[Continue reading](#)