The ALPHV/BlackCat Ransomware Gang is Using Google Ads to Conduct Cyberattacks

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 16:01:27 UTC

Security researchers with eSentire, a top global cybersecurity solutions provider, are warning that Russian-speaking affiliates of the ransomware gang ALPHV/BlackCat are attacking corporations and public entities in the Americas and Europe. In the past three weeks, we have seen these affiliates attempt to breach a law firm, a manufacturer, and a warehouse provider within our customer network, alongside attacking other companies. However, their attacks were intercepted and shut down by eSentire's security research team, the Threat Response Unit (TRU). ALPHV/BlackCat threat actors typically achieve initial access into their victims' IT networks through one of three ways: valid credentials, exploitation of remote management and monitoring services, and browser-based attacks. This year, however, one of the affiliates has expanded into malvertising to execute browser-based attacks.

This affiliate is taking out Google ads promoting popular software, such as Advanced IP Scanner, Slack, WinSCP and Cisco AnyConnect, to lure business professionals to attacker-controlled websites. Thinking they are downloading legitimate software, the business professionals are actually downloading the Nitrogen malware. Nitrogen is initial-access malware that leverages Python libraries for stealth. This foothold provides intruders with an initial entry into the target organization's IT environment. Once the hackers have that initial foothold, they can then infect the target with the malware of their choosing. In the case with this attack campaign, the target victims are being infected with the ALPHV/BlackCat ransomware, according to Keegan Keplinger, Senior Threat Intelligence Researcher with TRU.

According to TRU, the malvertising attacks they shut down in the past three weeks on behalf of the law firm and manufacturer are a continuation of a June 2023 campaign, where an affiliate of the ALPHV/BlackCat Ransomware gang was observed using malicious ads to distribute the Nitrogen malware, which led to the ALPHV/BlackCat ransomware. eSentire was the first cybersecurity company to identify and name the Nitrogen malware in June 2023. TRU named the malicious software after an artifact found in the naming conventions used by the threat actors.

About Nitrogen

Nitrogen is labeled as initial access malware because it is malicious software that threat actors use to gain entry to a target victim's IT environment. Nitrogen malware is unique in that it uses highly obfuscated Python libraries to bypass security controls. Python libraries enhance the functionality and capabilities of Python code programs. They are pre-written collections of code that provide a wide range of functions, classes, and tools for specific tasks, making it easier for developers to build complex applications without starting from scratch. Because Python libraries are legitimate tools, they typically do not raise any suspicions with security defenders. The additional

layer of obfuscation acts to slow down analysts and security researchers in reversing and pinpointing the attack path taken by the malware once active in the operating system. See more technical details around Nitrogen here.

The Criminal Origins of ALPHV/BlackCat Ransomware Group

The ALPHV/BlackCat ransomware group and its affiliates are typically observed to be Russian-speaking, and various security teams report that the core ALPHV/BlackCat operators are based in Russia. The gang first appeared on the ransomware scene in November 2021. According to the FBI, the ALPHV/BlackCat gang compromised 60 businesses and public entities between November 2021 and March 2022. At the time of this reporting, in 2023, ALPHV/BlackCat lists 170 victims on their name and shame page, ranking them the third most active ransomware gang behind Cl0p & LockBit.

Some of ALPHV/BlackCat's recent and most publicized attacks include MGM Resorts, which is comprised of 19 U.S. properties, including the Bellagio, Mandalay Bay, and the Cosmopolitan. The attack caused considerable chaos at the resorts, forcing guests to wait hours to check in and crippling electronic payments, digital key cards, slot machines, ATMs, and paid parking systems. MGM Resorts reported that they expect a $100 million hit to its third-quarter results due to the breach.

ALPHV/BlackCat also recently named McClaren Health Care as a victim. It is one of Michigan's largest healthcare systems and is made up of hospitals, clinics, and healthcare facilities. McClaren administrators reported that the ALPHV/Black Cat threat actors accessed various data from 2.2 million patients. Among the type of data includes full name, SSNs, date of birth, healthcare insurance information, Medicare/Medicaid information, billing data, and treatment and prescription information. The ALPHV/BlackCat ransomware group also recently claimed to have hacked Clarion, a global manufacturer of audio and video equipment for cars and other vehicles, and the hotel chain Motel One.

When digging into ALPHV/BlackCat's lineage, TRU discovered that ALPHV/BlackCat has connections to the former BlackMatter ransomware group, whose ransomware code is said to be a combination of the notorious DarkSide and REvil ransomware software. Additionally, these ransomware operations have all counted FIN7, a sophisticated cybercrime group, among their affiliates.

Readers might recall that the DarkSide ransomware operators were responsible for compromising the Colonial Pipeline, the largest pipeline system for refined oil products in the U.S., which resulted in their pipeline systems being taken offline in May 2021.

Several of REvil's high-profile attacks include global computer manufacturers Acer and Quanta, top Mexican bank, CIBanco, Chilean bank, BancoEstado, and one of the entertainment industry's largest law firms, Grubman Shire Meiselas & Sacks. At the time of their breach, this firm represented Lady Gaga, Madonna, Bruce Springsteen, Jessica Simpson, and Mariah Carey, among others.

ALPHV/BlackCat Ransomware Group, Ruthless and Despicable

One might ask, "Why are the ALPHV/BlackCat ransomware operators and their affiliates so despicable?" It is the lengths these threat actors will go to force their victims to pay their ransom demands. In February of this year, ALPHV/BlackCat hackers broke into one of the largest healthcare networks in Pennsylvania, the Lehigh Valley

Health Network. It is estimated that the hackers stole data on approximately 500 patients, and for some of the patients this data included medical data, social security numbers, banking information, name, address, birthdate, etc., which the threat actors threatened to release on their data leak site. In March, the hackers went even further with their extortion attempts, shocking both security defenders and healthcare professionals around the world.

The ALPHV/BlackCat threat actors published photos of "topless" female breast cancer patients on their leak site after the health group refused to pay a $1.5 million ransom following their February attack. The clinical images were used by Lehigh Valley Health Network as part of radiotherapy treatment for their cancer patients. In July, the ALPHV/BlackCat gang went so far as to provide an API for their leak site to increase visibility for their attacks.

Browser-Based Cyberattacks—a Growing Attack Surface

While much of cybersecurity user awareness training is still focused on malicious email attachments, browser-based malware downloads have usurped email as a primary method of initial cyber infection access for hands-on ransomware intrusions. As previously mentioned, in this Nitrogen campaign, users are infected when they go looking for popular, legitimate software to download and then click through on a Google Ad that renders to a malware site instead. The software lures TRU has observed the threat actors using in the Nitrogen campaign include Advanced IP Scanner, WinSCP, Slack, and Cisco AnyConnect. Additionally, TRU has observed ALPHV ransomware stemming from Gootloader attacks, another successful browser-based initial access malware known to target law firms.

Initial Access Malware

Known examples of ransomware-associated initial access malware that leverage browser-based attacks include Gootloader, SocGholish, BatLoader, and now Nitrogen. Nitrogen uses an obfuscated python framework that leverages DLL side loading. Interestingly, ALPHV has been observed as an end-game for at least two of these browser-based initial access pieces of malware: Gootloader and Nitrogen.

Intrusion Tool Buffet

Since 2020, Cobalt Strike has been growing as the primary intrusion tool leveraged by ransomware affiliates. In response, the security community quickly developed detections and threat- hunting paradigms around Cobalt Strike. In turn, threat actors have begun to shift to new intrusion tools, including leveraging Remote Monitoring and Management (RMM) tools and remote access software (AnyDesk, TSDService, Atera and ConnectWise ScreenConnect™) and new intrusion frameworks (Sliver and Brute Ratel). In at least one Nitrogen incident, TRU observed a full buffet of Intrusion Frameworks being used by the ALPHV/BlackCat threat actors: Cobalt Strike, Sliver, and Brute Ratel.

Security Recommendations to Protect Against Nitrogen Attack Campaigns Leading to ALPHV/BlackCat Ransomware

1. Organizations need to start including browser-based attacks, including those that use fake advertising, as part of User Awareness Training (UAT). Browser-based attacks are increasingly leading to hands-on ransomware intrusions and infostealers that enable ransomware intrusions later.

2. Make sure you are implementing attack surface reduction rules around script files such as .js and .vbs, but keep in mind that when these attacks arrive in .ISO files, the “Mark of the Web” is lost so Attack Surface Reduction rules won’t detect the files from the Internet.
3. Employ endpoint monitoring to ensure you can catch malicious execution, when social engineering attacks bypass user scrutiny – and make sure that endpoint coverage is fully comprehensive. TRU has observed a tendency for ransomware attacks to make it further down the kill-chain when they begin on endpoints that are out of scope for endpoint monitoring.
4. Employ logging to ensure you are capturing telemetry – especially for devices and services that don’t support an endpoint agent, including VPN, device enrollment, and server software for applications that don’t generate endpoint telemetry, like Citrix, IIS, and cloud services).

If you’re not currently engaged with a Managed Detection and Response (MDR) provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more? Connect with an eSentire Security Specialist.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire’s Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.
