ALPHV, BlackCat Gang - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:08:59 UTC

APT group: ALPHV, BlackCat Gang

Names	ALPHV *(self given)* ALPHVM *(self given)* BlackCat Gang *(?)* UNC4466 *(Mandiant)* Ambitious Scorpius *(Palo Alto)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2021	
Description	(Palo Alto) BlackCat (aka ALPHV) is a ransomware family that surfaced in mid-November 2021 and quickly gained notoriety for its sophistication and innovation. Operating a ransomware-as-a-service (RaaS) business model, BlackCat was observed soliciting for affiliates in known cybercrime forums, offering to allow affiliates to leverage the ransomware and keep 80-90% of the ransom payment. The remainder would be paid to the BlackCat author. The threat actors leveraging BlackCat, often referred to as the 'BlackCat gang,' utilize numerous tactics that are becoming increasingly commonplace in the ransomware space. Notably, they use multiple extortion techniques in some cases, including the siphoning of victim data before ransomware deployment, threats to release data if the ransom is not paid and distributed denial-of-service (DDoS) attacks. Known affiliates are: 1. Subgroup: Scattered Spider	
Observed	Countries: Worldwide.	
Tools used	BlackCat, GO Simple Tunnel, Impacket, LaZagne, MEGAsync, Mimikatz, Munchkin, PsExec, Remcom, WebBrowserPassView.	
Operations performed	Dec 2021	Global IT services provider Inetum hit by ransomware attack <https://www.bleepingcomputer.com/news/security/global-it-services-provider-inetum-hit-by-ransomware-attack/>
	Dec 2021	Fashion giant Moncler confirms data breach after ransomware attack <https://www.bleepingcomputer.com/news/security/fashion-giant-moncler-confirms-data-breach-after-ransomware-attack/>

Jan 2022	BlackCat ransomware implicated in attack on German oil companies <https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/>
Jan 2022	String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say <https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say/>
Feb 2022	BlackCat (ALPHV) claims Swissport ransomware attack, leaks data <https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/>
Apr 2022	BlackCat, believed a rebranded version of the BlackMatter or DarkSide ransomware group, has claimed to have successfully targeted several organizations including a popular Nigerian betting platform Bet9ja, three universities - FIU, NCAT State University, AIT-Thailand, and the largest natural gas supplier in Latin America - TGS, in the past few days. <https://www.bankinfosecurity.com/blackcat-attack-on-betting-company-disrupts-service-a-18886>
May 2022	Austrian federal state Carinthia has been hit by the BlackCat ransomware gang, also known as ALPHV, who demanded a $5 million to unlock the encrypted computer systems. <https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-asks-5-million-to-unlock-austrian-state/>
May 2022	Lockbit, Hive, and BlackCat attack automotive supplier in triple ransomware attack <https://news.sophos.com/en-us/2022/08/10/lockbit-hive-and-blackcat-attack-automotive-supplier-in-triple-ransomware-attack/>
Jun 2022	Louisiana authorities investigating ransomware attack on city of Alexandria <https://therecord.media/louisiana-authorities-investigating-ransomware-attack-on-city-of-alexandria/>
Jun 2022	BlackCat Attacks University of Pisa, Demands $4.5M Ransom <https://www.bankinfosecurity.com/blackcat-attacks-university-pisa-demands-45m-ransom-a-19338>
Jun 2022	Ransomware gang creates site for employees to search for their stolen data <https://www.bleepingcomputer.com/news/security/ransomware-gang-creates-site-for-employees-to-search-for-their-stolen-data/>
Jul 2022	BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2,5M in Demands <https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands>
Jul 2022	Bandai Namco confirms hack after ALPHV ransomware data leak threat <https://www.bleepingcomputer.com/news/security/bandai-namco-confirms-hack-after-alphv-ransomware-data-leak-threat/>

Jul 2022	The ALPHV ransomware gang, aka BlackCat, claimed responsibility for a cyberattack against Creos Luxembourg S.A. last week, a natural gas pipeline and electricity network operator in the central European country. <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/>
Aug 2022	Major airline technology provider Accelya attacked by ransomware group <https://therecord.media/major-airline-technology-provider-accelya-attacked-by-ransomware-group/>
Aug 2022	The BlackCat/ALPHV ransomware gang claimed responsibility for an attack that hit the systems of Italy's energy agency Gestore dei Servizi Energetici SpA (GSE) over the weekend. <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/>
Sep 2022	“BlackCat” attempts to up the pressure on Suffolk County; starts to leak data? <https://www.databreaches.net/blackcat-attempts-to-up-the-pressure-on-suffolk-county-starts-to-leak-data/>
Sep 2022	BlackCat said they breached US Department of Defense contractor and went offline <https://cybernews.com/news/blackcat-breached-department-of-defense-contractor-went-offline/>
Oct 2022	ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access <https://www.mandiant.com/resources/blog/alphv-ransomware-backup>
Dec 2022	Colombian energy supplier EPM hit by BlackCat ransomware attack <https://www.bleepingcomputer.com/news/security/colombian-energy-supplier-epm-hit-by-blackcat-ransomware-attack/>
Dec 2022	Toy maker Jakks Pacific reports cyberattack after multiple ransomware groups leak data <https://therecord.media/toy-maker-jakks-pacific-reports-cyberattack-after-multiple-ransomware-groups-post-stolen-data/>
Dec 2022	Ransomware gang cloned victim’s website to leak stolen data <https://www.bleepingcomputer.com/news/security/ransomware-gang-cloned-victim-s-website-to-leak-stolen-data/>
Jan 2023	The BlackCat Ransomware group claims to have hacked SOLAR INDUSTRIES INDIA and to have stolen 2TB of “secret military data.” <https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html>
Jan 2023	BlackCat Adds Indian Missile Fuel Maker to Its Victims List <https://www.bankinfosecurity.com/blackcat-adds-indian-missile-fuel-maker-to-its-victims-list-a-21089>

Feb 2023	Pennsylvania Health System CEO Confirms BlackCat Attack <https://www.bankinfosecurity.com/pennsylvania-health-system-ceo-confirms-blackcat-attack-a-21279>
Feb 2023	Ransomware gang posts breast cancer patients' clinical photographs <https://therecord.media/ransomware-lehigh-valley-alphv-black-cat>
Feb 2023	Reddit hackers threaten to leak data stolen in February breach <https://www.bleepingcomputer.com/news/security/reddit-hackers-threaten-to-leak-data-stolen-in-february-breach/>
Mar 2023	Amazon-owned Ring denies 'ransomware event' following darknet listing <https://therecord.media/ring-denies-ransomware-attack-alphv>
Mar 2023	Indian pharmaceutical giant warns of revenue loss, litigation after ransomware attack <https://therecord.media/sun-pharma-india-ransomware-attack>
Apr 2023	Australian Law Firm Hack Affected 65 Government Agencies <https://www.bankinfosecurity.com/australian-law-firm-hack-affected-65-government-agencies-a-23110>
May 2023	ALPHV gang claims ransomware attack on Constellation Software <https://www.bleepingcomputer.com/news/security/alphv-gang-claims-ransomware-attack-on-constellation-software/>
May 2023	Legal services platform used by SEC, Pentagon investigating ransomware attack claims <https://therecord.media/casepoint-legal-tech-platform-investigating-ransomware-attack-claims-blackcat>
May 2023	Norton Healthcare discloses data breach after May ransomware attack <https://www.bleepingcomputer.com/news/security/norton-healthcare-discloses-data-breach-after-may-ransomware-attack/>
Jun 2023	BlackCat ransomware fails to extort Australian commercial law giant <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-fails-to-extort-australian-commercial-law-giant/>
Jun 2023	Now BlackCat extortionists threaten to leak stolen plastic surgery pics <https://www.theregister.com/2023/06/22/blackcat_ransomware_plastic_surgery_clinic/>
Jun 2023	Bangladesh government website leaks citizens' personal data <https://techcrunch.com/2023/07/07/bangladesh-government-website-leaks-citizens-personal-data/>> <https://www.databreaches.net/almost-everything-you-have-posted-in-your-news-article-about-this-incident-is-a-total-crap-blackcat-to-bangladeshi-news-outlets/>
Jun 2023	AlphV group takes credit for ransomware attack on Georgia county <https://therecord.media/forsyth-county-georgia-ransomware-alphv-post>
Jul 2023	BlackCat, Clop claim ransomware attack on cosmetics maker Estée Lauder <https://therecord.media/blackcat-clop-claim-cyberattack-on-estee-lauder>

Jul 2023	ALPHV ransomware adds data leak API in new extortion strategy <https://www.bleepingcomputer.com/news/security/alphv-ransomware-adds-data-leak-api-in-new-extortion-strategy/>
Jul 2023	Japanese watchmaker Seiko breached by BlackCat ransomware gang <https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/>
Aug 2023	Microsoft: BlackCat's Sphynx ransomware embeds Impacket, RemCom <https://www.bleepingcomputer.com/news/microsoft/microsoft-blackcats-sphynx-ransomware-embeds-impacket-remcom/>
Sep 2023	BlackCat ransomware hits Azure Storage with Sphynx encryptor <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-hits-azure-storage-with-sphynx-encryptor/>
Sep 2023	Alphv group claims the hack of Clarion, a global manufacturer of audio and video equipment for cars <https://securityaffairs.com/151299/data-breach/alphv-ransomware-hacked-clarion.html>
Sep 2023	Product leasing giant warns that sensitive information was stolen during cyberattack <https://therecord.media/product-leasing-giant-progressive-ransomware>
Sep 2023	Large Michigan healthcare provider confirms ransomware attack <https://therecord.media/mclaren-healthcare-ransomware-attack-michigan>
Sep 2023	Motel One discloses data breach following ransomware attack <https://www.bleepingcomputer.com/news/security/motel-one-discloses-data-breach-following-ransomware-attack/>
Oct 2023	McLaren Health Care says data breach impacted 2.2 million people <https://www.bleepingcomputer.com/news/security/mclaren-health-care-says-data-breach-impacted-22-million-people/>
Oct 2023	ALPHV ransomware gang claims attack on Florida circuit court <https://www.bleepingcomputer.com/news/security/alphv-ransomware-gang-claims-attack-on-florida-circuit-court/>
Oct 2023	The Alphv ransomware gang stole 5TB of data from the Morrison Community Hospital <https://securityaffairs.com/152486/cyber-crime/alphv-ransomware-morrison-community-hospital.html>
Oct 2023	BlackCat Climbs the Summit With a New Tactic <https://unit42.paloaltonetworks.com/blackcat-ransomware-releases-new-utility-munchkin/>
Oct 2023	Another small firm suffers a serious ransomware attack: Cadre Services gets mauled by AlphV <https://www.databreaches.net/another-small-firm-suffers-a-serious-ransomware-attack-cadre-services-gets-mauled-by-alphv/>

Oct 2023	BlackCat ransomware claims breach of healthcare giant Henry Schein <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/>
Oct 2023	Advarra hacked, threat actors threatening to leak data <https://www.databreaches.net/exclusive-advarra-hacked-threat-actors-threatening-to-leak-data/>
Nov 2023	AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC <https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/>
Nov 2023	Notorious ransomware gang takes credit for cyberattack on Fidelity National Financial <https://therecord.media/fidelity-national-financial-ransomware-alphv-black-cat>
Nov 2023	The big bad BlackCat tries to bully Hampton-Newport News CSB. Shame on BlackCat. <https://www.databreaches.net/the-big-bad-blackcat-tries-to-bully-hampton-newport-news-csb-shame-on-blackcat/>
Nov 2023	Henry Schein re-encrypted by BlackCat again <https://www.databreaches.net/henry-schein-re-encrypted-by-blackcat-again/>
Nov 2023	HTC Global Services confirms cyberattack after data leaked online <https://www.bleepingcomputer.com/news/security/htc-global-services-confirms-cyberattack-after-data-leaked-online/>
Nov 2023	Trans-Northern Pipelines investigating ALPHV ransomware attack claims <https://www.bleepingcomputer.com/news/security/trans-northern-pipelines-investigating-alphv-ransomware-attack-claims/>
Dec 2023	AlphV claims an attack before even alerting the victim. How will that work out for them? <https://www.databreaches.net/alphv-claims-an-attack-before-even-alerting-the-victim-how-will-that-work-out-for-them/>
Dec 2023	If at first you don’t succeed, screw it up again? <https://www.databreaches.net/if-at-first-you-dont-succeed-screw-it-up-again/>
Dec 2023	AlphV reacts to law enforcement action by allowing affiliates to attack hospitals, critical infrastructure <https://www.databreaches.net/alphv-reacts-to-law-enforcement-action-by-allowing-affiliates-to-attack-hospitals-critical-infrastructure/>
Jan 2024	ALPHV ransomware claims loanDepot, Prudential Financial breaches <https://www.bleepingcomputer.com/news/security/alphv-ransomware-claims-loandepot-prudential-financial-breaches/>
Feb 2024	UnitedHealth subsidiary Optum hack linked to BlackCat ransomware <https://www.bleepingcomputer.com/news/security/unitedhealth-subsidiary-optum-hack-linked-to-blackcat-ransomware/>

	Feb 2024	Hessen Consumer Center says systems encrypted by ransomware <https://www.bleepingcomputer.com/news/security/hessen-consumer-center-says-systems-encrypted-by-ransomware/>
	Mar 2024	BlackCat ransomware shuts down in exit scam, blames the 'feds' <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/> <https://www.bleepingcomputer.com/news/security/blackcat-ransomware-turns-off-servers-amid-claim-they-stole-22-million-ransom/>
Counter operations	Dec 2023	Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant>
	Feb 2024	US offers up to $15 million for tips on ALPHV ransomware gang <https://www.bleepingcomputer.com/news/security/us-offers-up-to-15-million-for-tips-on-alphv-ransomware-gang/>
	Mar 2024	US offers $10 million bounty for info on 'Blackcat' hackers who hit UnitedHealth <https://www.reuters.com/technology/cybersecurity/us-offers-10-million-bounty-info-blackcat-hackers-who-hit-unitedhealth-2024-03-27/>
Information	<https://unit42.paloaltonetworks.com/blackcat-ransomware/> <https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/> <https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/> <https://www.darkreading.com/vulnerabilities-threats/everything-you-need-to-know-about-blackcat-alphav-> <https://securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/> <https://www.trendmicro.com/en_us/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html> <https://www.esentire.com/blog/the-notorious-alphv-blackcat-ransomware-gang-is-attacking-corporations-and-public-entities-using-google-ads-laced-with-malware-warns-esentire> <https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a> <https://www.sygnia.co/blog/blackcat-ransomware/> <https://www.menlosecurity.com/blog/swindled-blackcat-affiliate-wants-money-from-change-healthcare-ransom>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
