BlackCat (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:06:02 UTC

BlackCat

aka: ALPHV, Noberus

Actor(s): Alpha Spider, RansomHub, Vanilla Tempest

VTCollection

ALPHV, also known as BlackCat or Noberus, is a ransomware family that is deployed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports execution on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. ALPHV is marketed as ALPHV on cybercrime forums, but is commonly called BlackCat by security researchers due to an icon of a black cat appearing on its leak site. ALPHV has been observed being deployed in ransomware attacks since November 18, 2021.

ALPHV can be configured to encrypt files using either the AES or ChaCha20 algorithms. In order to maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and stop virtual machines on ESXi servers. ALPHV can self-propagate by using PsExec to remote execute itself on other hosts on the local network.

References

2025-12-30 · US Department of Justice ·
Two Americans Plead Guilty to Targeting Multiple U.S. Victims Using ALPHV BlackCat Ransomware
BlackCat BlackCat

2025-11-03 · Breached Company · Breached Company
When the Defenders Become the Attackers: Cybersecurity Experts Indicted for BlackCat Ransomware Operations
BlackCat BlackCat

2025-07-31 · Intrinsec · CTI Intrinsec
Shadow syndicate infrastructure illumination
AMOS BlackCat Cactus Cicada3301 Clop LockBit PLAY RansomHub Royal Ransom Silence

2025-05-06 · Mandiant · Mandiant
Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines
BlackCat DragonForce RansomHub

2025-05-06 · Mandiant · Mandiant
Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines
BlackCat DragonForce RansomHub

2024-10-30 · EclecticIQ · EclecticIQ Threat Research Team
Inside Intelligence Center: LUNAR SPIDER Enabling Ransomware Attacks on Financial Sector with Brute Ratel C4 and Latrodectus
BlackCat Brute Ratel C4 Latrodectus

2024-09-30 · The DFIR Report · The DFIR Report
Nitrogen Campaign Drops Sliver and Ends With BlackCat Ransomware
BlackCat Nitrogen Loader Sliver

2024-06-05 · S-RM · David Broom, Gavin Hull
Exmatter malware levels up: S-RM observes new variant with simultaneous remote code execution and data targeting
BlackCat BlackMatter Conti ExMatter LockBit REvil Ryuk

2024-04-24 · SentinelOne · Jim Walter
Ransomware Evolution | How Cheated Affiliates Are Recycling Victim Data for Profit
BlackCat RansomHub RansomHub

2024-02-29 · CrowdStrike · Jean-Philippe Teissier
The Anatomy of an ALPHA SPIDER Ransomware Attack
BlackCat Alpha Spider

2024-02-22 · Sekoia · Livia Tibirna, Pierre-Antoine D., Quentin Bourgue, Threat & Detection Research Team
Scattered Spider laying new eggs
BlackCat

2023-12-13 · cocomelonc · cocomelonc
Malware in the wild book
AsyncRAT Babuk BlackCat BlackLotus Carbanak HelloKitty Paradise Stealc WinDealer

2023-12-03 · Twitter (@vxunderground) · VX-Underground
Tweet about ALPHV group compromising Tipalti to pressure its clients.
BlackCat BlackCat

2023-11-16 · The Register · Connor Jones
BlackCat plays with malvertising traps to lure corporate victims
BlackCat

2023-11-16 · CISA · CISA
Scattered Spider
Ave Maria BlackCat Raccoon Vidar

2023-10-30 · eSentire · eSentire
Nitrogen Campaign 2.0: Reloads with Enhanced Capabilities Leading to ALPHV/BlackCat Ransomware
BlackCat Nitrogen Loader

2023-10-25 · Microsoft · Microsoft Incident Response, Microsoft Threat Intelligence
Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction
BlackCat BlackCat Lumma Stealer

2023-09-12 · · ANSSI · ANSSI
FIN12: A Cybercriminal Group with Multiple Ransomware
BlackCat Cobalt Strike Conti Hive MimiKatz Nokoyawa Ransomware PLAY Royal Ransom Ryuk SystemBC

2023-08-17 · Trellix · Phelix Oluoch
Scattered Spider: The Modus Operandi
BlackCat POORTRY

2023-07-18 · Symantec · Threat Hunter Team
FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware
BlackCat Unidentified 103 (FIN8)

2023-07-13 · MSSP Lab · cocomelonc
Malware analysis report: BlackCat ransomware
BlackCat BlackCat

2023-06-10 · The DFIR Report · The DFIR Report
IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment
BlackCat Cobalt Strike IcedID

2023-06-01 · Infinitum IT · Kerime Gencay
BlackCat Ransomware Analysis Report (Paywall)
BlackCat

2023-05-30 · IBM Security · IBM Security X-Force Team
BlackCat (ALPHV) ransomware levels up for stealth, speed and exfiltration
BlackCat BlackCat

2023-05-22 · Trend Micro · Bahaa Yamany, Mahmoud Zohdy, Mohamed Fahmy, Sherif Magdy
BlackCat Ransomware Deploys New Signed Kernel Driver
BlackCat

2023-04-19 · Bleeping Computer · Bill Toulas
March 2023 broke ransomware attack records with 459 incidents
Clop WhiteRabbit BianLian Black Basta BlackCat LockBit Medusa PLAY Royal Ransom

2023-04-18 · Mandiant · Mandiant
M-Trends 2023
QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate

2023-04-03 · Mandiant · Eduardo Mattos, JASON DEYALSINGH, Nick Richard, NICK SMITH, Tyler McLellan
ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access
LaZagne BlackCat MimiKatz

2023-03-30 · United States District Court (Eastern District of New York) · Fortra, HEALTH-ISAC, Microsoft
Cracked Cobalt Strike (1:23-cv-02447)
Black Basta BlackCat LockBit RagnarLocker LockBit Black Basta BlackCat Cobalt Strike Cuba Emotet LockBit Mount Locker PLAY QakBot RagnarLocker Royal Ransom Zloader

2023-03-21 · Github (rivitna) · Andrey Zhdanov
BlackCat v3 Decryptor Scripts
BlackCat BlackCat

2022-11-09 · Netskope · Gustavo Palazolo
BlackCat Ransomware: Tactics and Techniques From a Targeted Attack
BlackCat ExMatter

2022-10-25 · Microsoft · Microsoft Security Threat Intelligence
DEV-0832 (Vice Society) opportunistic ransomware campaigns impacting US education sector
BlackCat Mount Locker PortStarter Zeppelin Vanilla Tempest

2022-10-10 · RiskIQ · Microsoft Threat Intelligence Center (MSTIC)
DEV-0832 Leverages Commodity Tools in Opportunistic Ransomware Campaigns
BlackCat Mount Locker SystemBC Zeppelin

2022-09-22 · ComputerWeekly · Alex Scroxton
ALPHV/BlackCat ransomware family becoming more dangerous
BlackCat BlackCat FIN7

2022-09-22 · Broadcom · Symantec Threat Hunter Team
Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics
BlackCat BlackMatter DarkSide

2022-09-08 · Sentinel LABS · Aleksandar Milenkoski, Jim Walter
Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection
AgendaCrypt Black Basta BlackCat PLAY

2022-09-06 · SecurityScorecard · Vlad Pasca
TTPs Associated With a New Version of the BlackCat Ransomware
BlackCat

2022-08-22 · Microsoft · Microsoft
Extortion Economics - Ransomware's new business model
BlackCat Conti Hive REvil AgendaCrypt Black Basta BlackCat Brute Ratel C4 Cobalt Strike Conti Hive Mount Locker Nokoyawa Ransomware REvil Ryuk

2022-08-11 · SecurityScorecard · Robert Ames
The Increase in Ransomware Attacks on Local Governments
BlackCat BlackCat Cobalt Strike LockBit

2022-07-18 · SecurityScorecard · Vlad Pasca
A Deep Dive Into ALPHV/BlackCat Ransomware
BlackCat

2022-07-14 · Sophos · Andrew Brandt, Andy French, Bill Kearney, Elida Leite, Harinder Bhathal, Lee Kirkpatrick, Peter Mackenzie, Robert Weiland, Sergio Bestulic
BlackCat ransomware attacks not merely a byproduct of bad luck
BlackCat BlackCat

2022-06-29 · Group-IB · Andrey Zhdanov, Oleg Skulkin
Fat Cats - An analysis of the BlackCat ransomware affiliate program
BlackCat BlackCat

2022-06-23 · Kaspersky · Danila Nasonov, Natalya Shornikova, Nikita Nazarov, Vasily Davydov, Vladislav Burtsev
The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs (Download Form)
BlackByte BlackCat Clop Conti Hive LockBit Mespinoza RagnarLocker

2022-06-23 · Kaspersky · Danila Nasonov, Natalya Shornikova, Nikita Nazarov, Vasily Davydov, Vladislav Burtsev
The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs
Conti Hive BlackByte BlackCat Clop LockBit Mespinoza Ragnarok

2022-06-13 · Microsoft · Microsoft Threat Intelligence
The many lives of BlackCat ransomware
BlackCat Velvet Tempest

2022-06-13 · Microsoft · Microsoft 365 Defender Threat Intelligence Team
The many lives of BlackCat ransomware
BlackCat

2022-06-07 · AdvIntel · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy
BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive
BlackCat BlackCat Cobalt Strike

2022-06-01 · Jorge Testa · Jorge Testa
Killing The Bear - Alphv
BlackCat BlackCat

2022-05-23 · Trend Micro · Trend Micro Research
LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022 (PDF)
BlackCat Conti LockBit

2022-05-23 · Trend Micro · Matsugaya Shingo
LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022
BlackCat Conti LockBit

2022-05-20 · AdvIntel · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy
DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape
AvosLocker Black Basta BlackByte BlackCat Conti HelloKitty Hive

2022-05-09 · Microsoft Security · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
Griffon BazarBackdoor BlackCat BlackMatter Blister Gozi LockBit Pandora Rook SystemBC TrickBot

2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT

2022-04-29 · The Record · Jonathan Greig
German wind farm operator confirms cybersecurity incident
Black Basta BlackCat

2022-04-27 · · ANSSI · ANSSI
LE GROUPE CYBERCRIMINEL FIN7
Bateleur BELLHOP Griffon SQLRat POWERSOURCE Andromeda BABYMETAL BlackCat BlackMatter BOOSTWRITE Carbanak Cobalt Strike DNSMessenger Dridex DRIFTPIN Gameover P2P MimiKatz Murofet Qadars Ranbyus SocksBot

2022-04-19 · FBI · FBI
FBI Flash CU-000167-MW: BlackCat/ALPHV Ransomware Indicators of Compromise
BlackCat

2022-04-18 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy
Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group
AvosLocker BazarBackdoor BlackByte BlackCat Cobalt Strike HelloKitty Hive Karakurt

2022-04-18 · Trend Micro · Leandro Froes, Lucas Silva
An Investigation of the BlackCat Ransomware via Trend Micro Vision One
BlackCat

2022-04-08 · The Hacker News · Ravie Lakshmanan
Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity
BlackCat BlackMatter BlackCat BlackMatter

2022-04-07 · Kaspersky · GReAT
A Bad Luck BlackCat
BlackCat

2022-04-07 · Kaspersky · GReAT
A Bad Luck BlackCat
BlackCat BlackCat

2022-03-23 · CrowdStrike · Falcon OverWatch Team
Falcon OverWatch Threat Hunting Contributes to Seamless Protection Against Novel BlackCat Attack
BlackCat

2022-03-17 · Cisco · Caitlin Huey, Tiago Pereira
From BlackMatter to BlackCat: Analyzing two attacks from one affiliate
BlackCat BlackMatter BlackCat BlackMatter

2022-03-16 · Symantec · Symantec Threat Hunter Team
The Ransomware Threat Landscape: What to Expect in 2022
AvosLocker BlackCat BlackMatter Conti DarkSide DoppelPaymer Emotet Hive Karma Mespinoza Nemty Squirrelwaffle VegaLocker WastedLocker Yanluowang Zeppelin

2022-03-01 · Cybereason · Ohav Peri, Tom Fakterman
Cybereason vs. BlackCat Ransomware
BlackCat

2022-02-08 · Trellix · Arnab Roy
BlackCat Ransomware as a Service - The Cat is certainly out of the bag!
BlackCat BlackCat

2022-02-02 · ZDNet · Jonathan Greig
BlackCat ransomware implicated in attack on German oil companies
BlackCat BlackCat

2022-01-28 · KrebsOnSecurity · Brian Krebs
Who Wrote the ALPHV/BlackCat Ransomware Strain?

BlackCat BlackCat

2022-01-27 · Palo Alto Networks Unit 42 · Alex Hinchliffe, Amanda Tanner, Doel Santos

Threat Assessment: BlackCat Ransomware

BlackCat

2022-01-26 · Intrinsec · Intrinsec

ALPHV ransomware gang analysis

BlackCat BlackCat

2022-01-26 · Intrinsec · Intrinsec

ALPHV ransomware gang analysis

BlackCat LockBit

2022-01-26 · Varonis · Jason Hill

ALPHV (BlackCat) Ransomware

BlackCat

2022-01-18 · SentinelOne · Jim Walter

BlackCat Ransomware | Highly-Configurable, Rust-Driven RaaS On The Prowl For Victims

BlackCat

2021-12-16 · Symantec · Threat Hunter Team

Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware

BlackCat

2021-12-10 · Medium s2wlab · S2W TALON

BlackCat: New Rust based ransomware borrowing BlackMatter's configuration

BlackCat BlackMatter

2021-12-10 · Dissecting Malware · Marius Genheimer

BlackCatConf - Static Configuration Extractor for BlackCat Ransomware

BlackCat

2021-12-01 · · ID Ransomware · Andrew Ivanov

BlackCat Ransomware

BlackCat

Yara Rules

▶ [TLP:WHITE] win_blackcat_auto (20251219 | Detects win.blackcat.)

Download all Yara Rules
