BlackCat (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:43:32 UTC

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.

2025-12-30 · US Department of Justice · Office of Public Affairs
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 2024-07-02 · Sekoia · Quentin Bourgue
Exposing FakeBat loader: distribution methods and adversary infrastructure
BlackCat Royal Ransom EugenLoader Carbanak Cobalt Strike DICELOADER Gozi IcedID Lumma Stealer NetSupportManager RAT Pikabot RedLine Stealer SectopRAT Sliver SmokeLoader Vidar 2023-12-03 · Twitter (@vxunderground) · VX-Underground
Tweet about ALPHV group compromising Tipalti to pressure its clients.
BlackCat BlackCat 2023-11-16 · CISA · CISA
Scattered Spider
BlackCat Ave Maria Raccoon Vidar 2023-10-25 · Microsoft · Microsoft Incident Response, Microsoft Threat Intelligence
Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction
BlackCat BlackCat Lumma Stealer 2023-07-13 · MSSP Lab · cocomelonc
Malware analysis report: BlackCat ransomware
BlackCat BlackCat 2023-05-30 · IBM Security · IBM Security X-Force Team
BlackCat (ALPHV) ransomware levels up for stealth, speed and exfiltration
BlackCat BlackCat 2023-05-15 · CrowdStrike · CrowdStrike
Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks
BlackCat SystemBC 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 2022-09-28 · vmware · Giovanni Vigna

ESXi-Targeting Ransomware: The Threats That Are After Your Virtual Machines (Part 1)

Avoslocker Babuk Black Basta BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit Luna RansomEXX RedAlert Ransomware REvil 2022-09-22 · ComputerWeekly · Alex Scroxton

ALPHV/BlackCat ransomware family becoming more dangerous

BlackCat BlackCat FIN7 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 2022-07-14 · 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 2022-06-07 · 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 2022-05-11 · Kaspersky · GReAT

New ransomware trends in 2022

BlackCat Conti DEADBOLT DoubleZero LockBit PartyTicket StealBit 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 2022-04-21 · Forescout · Vedere Labs

Analysis of an ALPHV incident

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 BlackCat 2022-03-27 · Bleeping Computer · Lawrence Abrams

Hive ransomware ports its Linux VMware ESXi encryptor to Rust

BlackCat Hive Hive 2022-03-22 · The Register · Jeff Burt

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

BlackCat BlackMatter 2022-03-17 · Cisco · Caitlin Huey, Tiago Pereira

From BlackMatter to BlackCat: Analyzing two attacks from one affiliate

BlackCat BlackMatter BlackCat BlackMatter 2022-02-23 · Emsisoft · Senan Conrad

Ransomware Profile: ALPHV

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 2022-01-26 · Intrinsec · Intrinsec

ALPHV ransomware gang analysis

BlackCat BlackCat 2021-12-21 · Twitter (@sisoma2) · sisoma2

BlackCat Ransomware Linux variant

BlackCat

▶ [TLP:WHITE] elf_blackcat_auto (20251219 | Detects elf.blackcat.)
