Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:03:07 UTC

Tool: BlackCat

Names	BlackCat ALPHV ALPHVM Noberus
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Palo Alto) The malware itself is coded in the Rust programming language. Though this is not the first piece of malware to use Rust, it is one of the first, if not the first, piece of ransomware to use it. By leveraging this programming language, the malware authors are able to easily compile it against various operating system architectures. Given its numerous native options, Rust is highly customizable, which facilitates the ability to pivot and individualize attacks.
Information	<https://unit42.paloaltonetworks.com/blackcat-ransomware/> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware> <https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/> <https://www.intrinsec.com/alphv-ransomware-gang-analysis/> <https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/> <https://www.varonis.com/blog/alphv-blackcat-ransomware> <https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware> <https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware> <https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html> <https://securelist.com/a-bad-luck-blackcat/106254/> <https://www.darkreading.com/attacks-breaches/blackcat-purveyor-shows-ransomware-operators-have-nine-lives> <https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html>

	<https://www.ic3.gov/Media/News/2022/220420.pdf> <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/> <https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S1068>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat> <https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackcat>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=blackcat-ransomware>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool BlackCat

Changed	Name	Country	Observed	
APT groups				
	ALPHV, BlackCat Gang	[Unknown]	2021-Mar 2024	
	FIN8	[Unknown]	2016-Dec 2022	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b7260119-d178-4d47-9a11-2d32c0d4cd9c