

What Is BlackSuit Ransomware & How Could It Impact Your Organization?

 cyberint.com/blog/dark-web/what-is-blacksuit-ransomware-and-how-could-it-impact-your-organization

Adi Bleih

June 28, 2026



Dark Web

Introduction to BlackSuit Ransomware

The BlackSuit ransomware operation surfaced in early April/May 2023. This group engages in multi-faceted extortion, encrypting and exfiltrating data from victims while hosting public data leak sites for those who do not comply with their demands. BlackSuit has notably targeted entities in the healthcare and education sectors, as well as other critical industries. It operates privately, with no public affiliates. BlackSuit's payloads share many technical similarities with Royal ransomware, such as encryption mechanisms and command-line parameters.

Delivery Methods of BlackSuit Ransomware

Infected Email Attachments (Macros): Cybercriminals may disseminate BlackSuit ransomware via email attachments containing malicious links or macros. When users open these attachments or enable macros, they can inadvertently trigger the ransomware's execution on their system.

Torrent Websites: BlackSuit ransomware can be embedded within torrent files, commonly used for file sharing through peer-to-peer networks. Downloading and opening these infected torrent files can lead to ransomware infection.

Malicious Ads (Malvertising): Malvertising involves the use of malicious advertisements to distribute BlackSuit ransomware. Clicking on these ads can redirect users to websites that automatically download and install the ransomware on their systems.

Trojans: BlackSuit ransomware can be delivered through Trojan horses—malicious programs designed to download and install other malware, including ransomware. Trojans can spread via phishing emails, fake software updates, or compromised websites.

BlackSuit supports both Windows and Linux operating systems. The payloads are typically delivered via phishing emails or third-party frameworks like Empire, Metasploit, and Cobalt Strike. Additionally, malicious torrent files have been observed as a delivery vector for this ransomware.

The encryption process of BlackSuit is notably rapid. Upon launch, it quickly processes available files and folders on all accessible volumes after obtaining local logical drive details.

On Windows systems, the ransomware attempts to hinder system recovery by deleting Volume Shadow Copies (VSS) using a hidden shell command that launches VSSADMIN.EXE with the /ALL and /Quiet options.

Ransom notes are placed in all folders containing encrypted files, labeled as “README.BlackSuit.txt” on Windows. On Linux, these notes are slightly different, appearing as “README.blacksuit.txt” with a variation in capitalization.

The Impact of BlackSuit Ransomware

BlackSuit is a private ransomware/extortion group targeting large enterprises as well as small to medium-sized businesses (SMBs) without specific industry discrimination. Similar to Royal ransomware, entities within the Commonwealth of Independent States (CIS) are excluded from their targeting. So far, BlackSuit has primarily attacked organizations in healthcare, education, information technology (IT), government, retail, and manufacturing sectors.

About Check Point Exposure Management

Check Point Exposure Management is an intelligence-led, validation-driven, remediation-first unified platform that helps security teams move quickly and safely from exposure visibility to exposure reduction. Delivered through a single UI, it brings together threat intelligence,

exposure prioritization, Agentic Exposure Validation, and safe remediation so teams can understand risk, prove exploitability, and act from one place.

[Schedule Your Demo Now](#)

BlackSuit Ransomware TTPS

Tactic Name	Technique
Impact	T1490 – Inhibit System Recovery
Impact	T1486 – Data Encrypted for Impact
Discovery	T1083 – File and Directory Discovery
Discovery	T1082 – System Information Discovery
Discovery	T1057 – Process Discovery
Execution	T1059 – Command and Scripting Interpreter
Execution	T1204 – User Execution

BlackSuit Ransomware IOCs

Type	Date Added	Value
SHA-256	2026-06-13	4504db7100a207705efb371d51fd8f8933f73e25bd7f7f64063372ea51b302d2
SHA-256	2026-06-13	06ca930b3531eacf14bc0bdbe2ace2c62912d1bce6e7c31ecf727e8d9f9ed063
SHA-256	2026-01-01	35f3ee553626b2267e4a8f35dce5b40840e5a461f13652bd2659681c31068805
SHA-256	2025-07-04	d3abb9947cbe93297b5064ae2f580c461250a7946672ab58ea8da512e919bbd3

Type	Date Added	Value
SHA-256	2025-05-27	0db187e003c6f976ea511389d22e771e5c94710c6cfc8ea2587812e66be1a52c
SHA-256	2025-05-20	cbd70a7fab661abee699e96bc790f813a553aa9aae80050544cc4137d6842589
SHA-256	2025-05-02	9c48e36b0ea519b37e44f5669da8b1eb59782798f8e8ebb6238441f73dc8102c
SHA-256	2025-04-16	eb12c198fc1b6ec79ea4b457988db4478ee6bc9aca128aa24a85b76a57add459
SHA256	2024-10-05	94200b3b4792c019ebe7bcfd16573fdedf385369e41309d82958568078e90c43
SHA256	2024-07-09	419e88d366b9a9c3ff4e0eca691fbad58919db0079b40e4e9c1711604bd5281d
SHA-256	2024-05-22	90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c
SHA-256	2024-05-22	6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310
SHA-256	2024-05-22	b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c
MD5	2024-05-22	4f813698141cb7144786cdc6f629a92b
MD5	2024-05-22	2902e12f00a185471b619233ee8631f3
MD5	2024-05-22	748de52961d2f182d47e88d736f6c835
SHA-1	2024-05-22	30cc7724be4a09d5bcd9254197af05e9fab76455

Type	Date Added	Value
SHA-1	2024-05-22	69feda9188dbebc2d2efec5926eb2af23ab78c5d
SHA-1	2024-05-22	7e7f666a6839abe1b2cc76176516f54e46a2d453
SHA-256	2024-05-22	1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e