THREAT PROFILE:

BlackSuit Ransomware

Table of Contents

Executive Summary

First Identified:

2023

Operation style:

Private ransomware operation.

Extortion method:

Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:

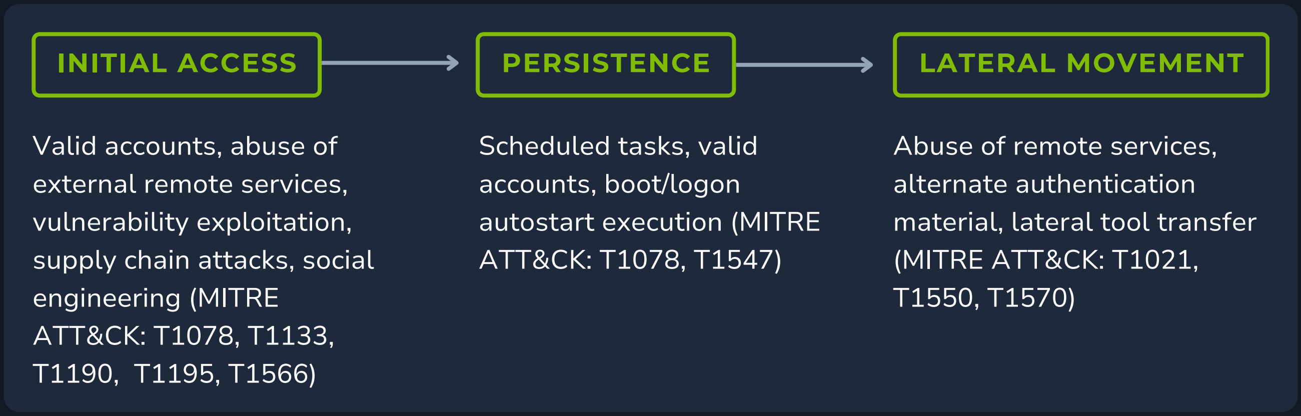
- Industrials (Construction & Engineering)

Most frequently targeted victim HQ region:

- United States, North America

Known Associations:

- Ignoble Scorpius
- Conti Ransomware
- Hermes Ransomware
- Royal Ransomware
- Ryuk Ransomware
- Zeon Ransomware



INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

INITIAL ACCESS

Valid accounts, abuse of external remote services, vulnerability exploitation, supply chain attacks, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1195, T1566)

PERSISTENCE

Scheduled tasks, valid accounts, boot/logon autostart execution (MITRE ATT&CK: T1078, T1547)

LATERAL MOVEMENT

Abuse of remote services, alternate authentication material, lateral tool transfer (MITRE ATT&CK: T1021, T1550, T1570)

Description

Black Suit Ransomware was first discovered in May 2023 and operates in the double extortion method, where victim data is stolen and leaked via a data leak site if the ransom demand is not paid. Black Suit has been assessed to be a likely rebrand of the Royal ransomware operation due to the similarities in their binaries.

Black Suit operators have been reported to often demand between $1 million and $10 million ransom demands from victims.

Black Suit ransomware operators have been observed gaining initial access via social engineering attacks, torrent websites, malicious ads, and deployment via additional malware.

The 32-bit Windows variants of the Black Suit and Royal ransomware variants share a 93.2% similarity in functions, 99.3% similarity in basic blocks, and 98.4% similarity in jumps. Both variants also use OpenSSL's AES for encryption and leverage similar intermittent encryption technique. The Black Suit and Royal Linux ransomware share 98% similarity in function, 99.5% similarity in blocks, and 98.9% similarity in jumps.

Black Suit uses OpenSSL's AES for encryption and uses an intermittent encryption technique to accelerate the encryption process. Black Suit, similar to Royal, prepares the files for encryption by rounding up the file size to the nearest multiple of 16, after which 41 bytes are added. A check is then performed for the file being encrypted to determine if the size is greater than 0x40000h. If the condition is met, it will use the value set using "-percent." The number of bytes to be used for intermittent encryption is then calculated using the same formula found in the Linux version of Royal ransomware. When files are encrypted they are appended with the ".blacksuit" extension.

Black Suit operators have been reported to often demand between $1 million and $10 million from victims.

Similar to Royal, Black Suit is not considered to be a ransomware-as-a-service (RaaS); there are no known affiliates of the Black Suit ransomware operation. Additionally, Royal had been tied to the Conti ransomware operation that ended in 2022; it is widely believed the group splintered into multiple smaller groups and rebranded to evade law enforcement detection.

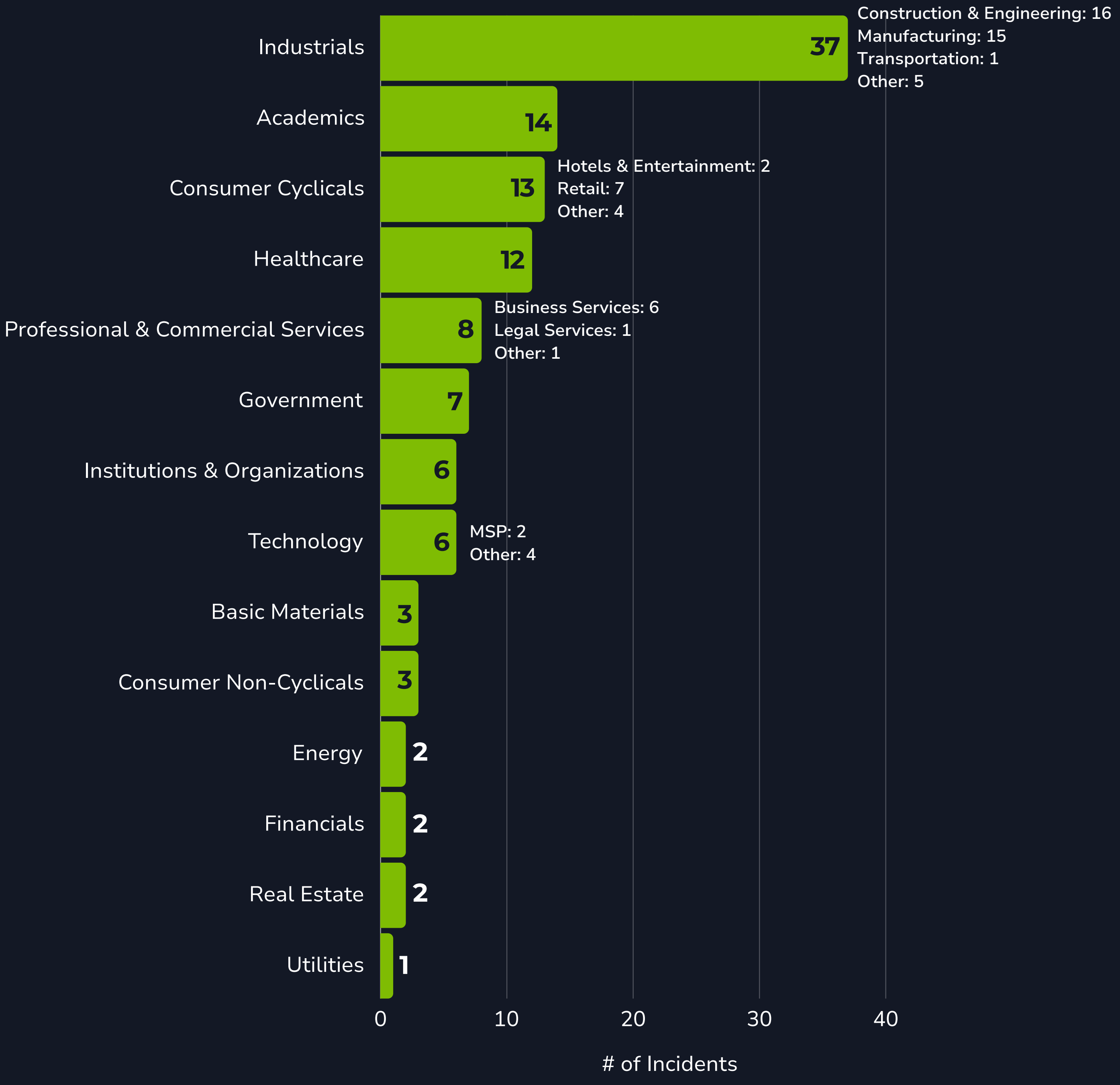
In October 2024, Barracuda researchers reported that the Black Suit operation was likely the sixth generation of the Hermes ransomware. Hermes was first observed being sold on cybercriminal forums in 2016. Hermes was then linked to the Ryuk operation in 2018 based on code similarities. Ryuk was then assessed to operate the Conti Ransomware operation in 2019. Conti operated until 2022 when a Ukrainian researcher with access to Conti resources leaked their operations' information. Zeon Ransomware was then identified in 2022, the Zeon operation rebranded to Royal Ransomware.

In 2023, Royal Ransomware operators were observed testing a new encryptor, Black Suit, which led to the assessment the group was likely going to rebrand. In May 2023, Black Suit was observed with a data leak site and began posting purported victims' data.

This operation highlights the continuous rebranding, shifting, and the long lineage the current day ransomware operations likely have.

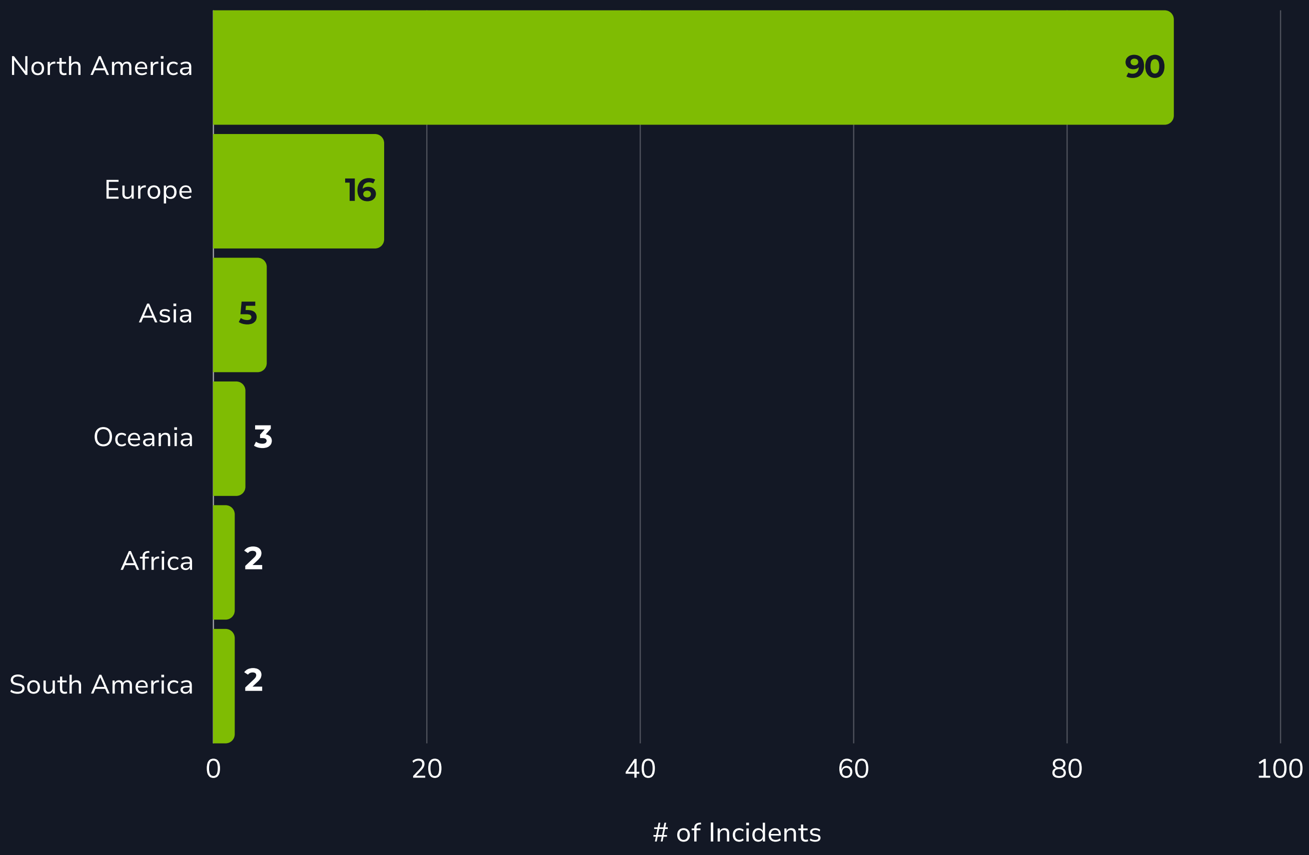
Previous Targets: Black Suit

Previous Industry Targets from 01 Oct 2023 to 30 Sep 2024

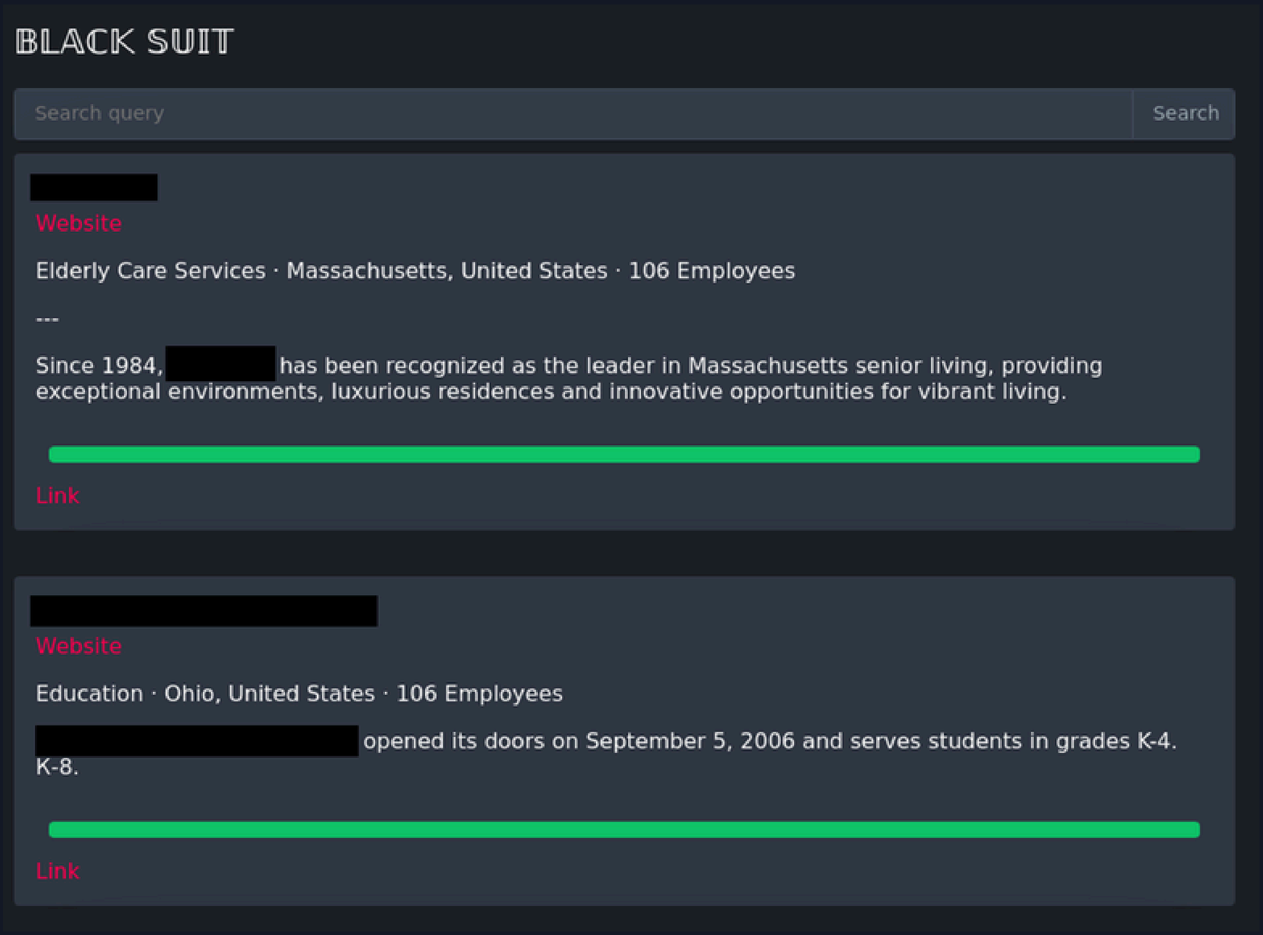


Previous Targets: BlackSuit

Previous Victim HQ Regions from 01 Oct 2023 to 30 Sep 2024



Data Leak Site: Black Suit



BLACK SUIT

[redacted]

Website

Elderly Care Services · Massachusetts, United States · 106 Employees

---

Since 1984, [redacted] has been recognized as the leader in Massachusetts senior living, providing exceptional environments, luxurious residences and innovative opportunities for vibrant living.

Link

[redacted]

Website

Education · Ohio, United States · 106 Employees

[redacted] opened its doors on September 5, 2006 and serves students in grades K-4. K-8.

Link

hxxp://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd[.]onion/

Associations: Black Suit

Ignoble Scorpius

The threat actor reportedly behind the BlackSuit Ransomware operation, tracked by Palo Alto.

Conti Ransomware

Royal is believed to be comprised of former members of the Conti operation, indicating that members of the Black Suit operations are likely former members of the Conti operation.

Hermes Ransomware

Hermes Ransomware was identified in 2016 that was sold on cybercriminal forums for affiliates to use. BlackSuit Ransomware has been assessed to be the 6th ransomware variant in the Hermes evolution.

Royal Ransomware

Black Suit and Royal ransomware variants have significant overlaps in both their Linux and Windows variants, indicating that Black Suit is likely a rebrand of the Royal operation.

Ryuk Ransomware

Ryuk Ransomware was identified in 2018 and was linked to Hermes Ransomware after researchers identified several code similarities.

Zeon Ransomware

Zeon Ransomware was identified in 2022 and was linked to the Conti Ransomware. Zeon was then rebranded to Royal Ransomware in 2023. Researchers have assessed that Royal then rebranded to the current BlackSuit Ransomware operation.

Known Tools: Black Suit

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
Arechclient2	AKA SecTopRAT. A .NET RAT with numerous capabilities. The malware can profile victim systems, steal information such as browser and crypto-wallet data, and launch a hidden secondary desktop to control browser sessions.
Atera Agent	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.
Brute Ratel	A post-exploitation tool that enables operators to deploy agents (badgers) while inside a target environment that enable arbitrary command execution to perform lateral movement, privilege escalation, and establish additional avenues of persistence.
Bublup	An easy to use platform for putting content in the cloud in an organized way. Threat actors have been observed using the platform to exfiltrate data.
Chisel	A fast TCP/UDP tunnel, transported over HTTP, secured via SSH. It can be used to pass through firewalls and to provide a secure endpoint into a victim network.
Cloudflared	A tool used to establish outbound connections (tunnels) between internal resources and Cloudflare’s global network.
cmd	A program used to execute commands on a Windows computer.

Known Tools: Black Suit

Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
ConnectWise	Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.
eHorus	A remote-control software for Windows, Linux, and Mac servers and workstations that has been used to remotely access victim environment.
Get-DataInfo.ps1	A PowerShell script that has been used to enumerate local systems.
GMER	A rootkit detector and remover that has been used to identify and kill processes such as anti-virus and EDR software.
Gootloader	A malware variant that is capable of stealing information and deploying second stage payloads.
LogMeIn	A remote access tool that has been used by malicious threat actors to gain remote access to victim machines.
LSASS	A Windows component that manages user authentication and security policies.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
MobaXterm	An application that provides X-Server capability for the Microsoft Windows OS. It allows applications running in the Unix/Linux environment to display graphical user interfaces on the MS Windows desktop.
NanoDump	A flexible tool that creates a minidump of the LSASS process.
netscan	A utility that scans within a subnet or IP range to check for devices.

Known Tools: Black Suit

Networx	A tool for monitoring network bandwidth, measuring network connection speed, logging incoming and outgoing traffic usage, and more.
nircmd	A command line tool that can be used to manipulate a variety of setting son a computer, modify the registry, add shortcuts, and open the default internet connection.
NirSoft	A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more.
NotePad	A simple text editor for Windows; it creates and edits plain text documents.
nsudo	An open-source tool used to disable AV solutions.
ntdsutil	A command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
OpenSSH	A suite of networking utilities based on the Secure Shell protocol that provides a secure channel over an unsecured network in the client-server architecture.
OpenSSL	A commercial grade open-source toolkit for the TLS protocol and is based on a full-strength general purpose cryptographic library.
PoorTry	A Windows driver that implements process termination and requires a userland utility to initiate the functionality.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerTool	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.
PsExec	A utility tool that allows users to control a computer from a remote location.

Known Tools: Black Suit

PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Rubeus	A C# toolset for raw Kerberos interaction and abuses.
SharpHound	The official data collector for BloodHound; it is written in C# and uses native Windows API functions and LSAP namespace functions to collect data from domain controllers and domain-joined Windows systems.
SharpShares	A tool used to enumerate accessible network shares within a compromised domain.
StoneStop	A Windows userland utility that attempts to terminate processes by creating and loading a malicious driver, POORTRY.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Ursnif	AKA Gozi, Dreambot, Papras, snifula. A malware variant that is capable of stealing and exfiltrating sensitive information and deploying second-stage payloads.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
Windows Restart Manager	A library for reducing required reboots during software updates. The tool is often used by threat actors to support the encryption process and retrieve processes running on the system.
WinRAR	A trialware file archiver utility for Windows devices that can backup data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.

Known Tools: Black Suit

WordPad	A tool included in Microsoft that is a basic work processor, positioned as more advanced that the Notepad text editor by supporting rich text editing.

Observed Black Suit Behaviors: Windows

Execution	COMSPEC% /b /c start /b /min powershell -nop -w hidden –encodedcommand -path: specifies a target directory to encrypt -id: creates the victim ID -ep: percentage of a file that should be encrypted -list: used to specify a text file containing the target directories to encrypt -delete: used to delete itself -network: used to encrypt file shares connected to the system -networkonly: encrypts file shares connected to the system -local: encrypts local system only (observed in older variants) -localonly: encrypts only the local system -disablesafeboot: used to disable safeboot -noprotect: used to disable mutex creation -percent: used to define encryption parameters
Persistence	powershell.exe windowstyle -hidden Command RegCreatekeyExA CoCreateInstance ITaskScheduler NewWorkItem HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Run (Value == socks_powershell)
Privilege Escalation	C:\Windows\system32\cmd.exe /c echo e6b1e5ac4ae > \\.\pipe\612990
Defense Evasion	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server DenyTSConnections cmd /v/c "set f={Malware File Name}&for /l %l in () do if exist !f! (del /f/a "!f!") else (exit)“ "%System%\vssadmin.exe" Delete Shadows /All /Quiet “%System%\bcdedit.exe" /deletevalue {current} safeboot shutdown.exe /r /t 0
Credential Access	AS-REP Roasting ReadProcessMemory

Observed Black Suit Behaviors: Windows

Discovery	C:\Windows\system32\cmd.exe /C nltest /dclist: C:\Winodws\system32\cmd.exe /C systeminfo SharpHound LDAP searches: "(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913))", "(BuildString("(primarygroupid=*)“ C:\Windows\system32\cmd.exe /C C:\Perflogs\adf\adf.bat C:\Windows\system32\cmd.exe /C C:\Perflogs\adf\AdFind.exe C:\Windows\system32\cmd.exe /C C:\Perflogs\start.bat powershell.exe –executionpolicy remotesigned –File .\Get-DataInfo.ps1 method C:\Windows\system32\cmd.exe /C net group "domain admins" /domain C:\Windows\system32\cmd.exe /C nltest /dclist <domainname redacted> nltest /domain_trusts /all_trusts C:\Windows\system32\cmd.exe /C net group "enterprise admins" /domain C:\Windows\system32\cmd.exe /C ping <hostname redacted> C:\Windows\system32\taskmgr.exe /4 C:\Windows\system32\cmd.exe /C All windows Import-Module ActiveDirectory Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingSystem, LastLogonDate, IPv4Address | Export-CSV C:\Users\AllWindows.csv -NoTypeInformation -Encoding UTF8 C:\Windows\system32\cmd.exe /C route print C:\Windows\system32\cmd.exe /C ping http://<IP redacted>/ C:\Windows\system32\mmc.exe C:\Windows\system32\dsa.msc C:\Windows\system32\mmc.exe C:\Windows\System32\gpedit.msc FindFirstFileW() FindNextFileW()
Command and Control	C:\Tools\socks32.exe
Collection	C:\Users\[redacted]\7z.exe a –tzip .\result.zip –mx=9 –aoa .\result*
Impact	C:\Windows\system32\NOTEPAD.EXE C:\Users\123.txt

Observed Black Suit Behaviors: Linux

Execution	"esxcli vm process list > list_" "esxcli vm process kill --type=soft --world-id=%s" "esxcli vm process kill --type=soft --world-id=%s" "esxcli vm process list > PID_list_"
Defense Evasion	"esxcli vm process list > list_” "esxclivm process kill --type=soft --world-id=%s“ "esxcli vm process list > PID_list_"
Impact	N = (X/10)*(Original File Size / 100) then round down to multiples of 16 Where X is the value of “-percent”

MITRE ATT&CK® Mappings: Black Suit

Resource Development	
T1608: Stage Capabilities	.006: SEO Poisoning
T1650: Acquire Access	
Initial Access	
T1078: Valid Account	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Attack	.002: Compromise Software Supply Chain
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link .004: Spearphishing Voice
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution

MITRE ATT&CK® Mappings: Black Suit

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys/Startup Folder
Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1548: Abuse Elevation Control Mechanism	
Defense Evasion	
T1055: Process Injection	
T1070: Indicator Removal	.001: Clear Linux or Mac System Logs
T1112: Modify Registry	
T1218: System Binary Proxy Execution	.010: Regsvr32
T1484: Domain or Tenant Policy Modification	.001: Group Policy Modification
T1562: Impair Defenses	.001: Disable or Modify Tools
T1564: Hide Artifacts	.006: Run Virtual Instance
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .003: NTDS .006: DCSync

MITRE ATT&CK® Mappings: Black Suit

Credential Access	
T1557: Adversary-in-the-Middle	
T1558: Steal or Forge Kerberos Tickets	.001: Golden Ticket .003: Kerberoasting .004: AS-REP Roasting
Discovery	
T1016: System Network Configuration Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares

MITRE ATT&CK® Mappings: Black Suit

Lateral Movement	
T1550: Use Alternate Authentication Material	.002: Pass the Hash
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1119: Automated Collection	
T1560: Archive Collected Data	
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	
T1095: Non-Application Layer Protocol	
T1105: Ingress Tool Transfer	
T1572: Protocol Tunneling	
Exfiltration	
T1048: Exfiltration Over Alternative Protocol	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage

MITRE ATT&CK® Mappings: Black Suit

Impact
T1486: Data Encrypted for Impact
T1489: Service Stop
T1490: Inhibit System Recovery
T1657: Financial Theft

References

- Alzahrani, Abdulaziz (2023, November 11) LinkedIn: “Understanding the BlackSuit Ransomware: A New Threat to Healthcare Cybersecurity.” https://www.linkedin.com/pulse/understanding-blacksuit-ransomware-new-threat-aziz-alzahrani-kkbie
- Barry, Christine (2024, October 29) Barracuda: “BlackSuit ransomware: 8 years, 6 names, 1 cybercrime syndicate.” https://blog.barracuda.com/2024/10/29/blacksuit-ransomware--8-years--6-names--1-cybercrime-syndicate
- Casona, Katherine; Chavez, Ivan Nicole; Gonzalez, Ieriz Nicolle; Bonaobra, Jeffrey Francis (2023, May 31) Trend Micro: “Investigating BlackSuit Ransomware’s Similarities to Royal.” https://www.trendmicro.com/en_za/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
- CISA (2023, November 13) “#StopRansomware: Royal Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
- Cluley, Graham (2023, December 07) TripWire: “BlackSuit ransomware - what you need to know.” https://www.tripwire.com/state-of-security/blacksuit-ransomware-what-you-need-know
- DFIR (2024, August 26) “BlackSuit Ransomware.” https://thedfirreport.com/2024/08/26/blacksuit-ransomware/
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf
- HC3 (2023, November 06) “BlackSuit Ransomware.” https://www.hhs.gov/sites/default/files/blacksuit-ransomware-analyst-note-tlpclear.pdf
- Montini, Heloise (2023, September 07) Salvage Data: “BlackSuit Ransomware: The Complete Guide.” https://www.salvagedata.com/blacksuit-ransomware/
- Roy, Srestha (2024, September 25) Fidelis Security: “Best Practices for Preventing BlackSuit Ransomware Infections.” https://fidelissecurity.com/threatgeek/threat-intelligence/blacksuit-ransomware/
- SentinelOne (2024, January 12) “BlackSuit.” https://www.sentinelone.com/anthology/blacksuit/
- Unit 42 (2024, November 20) “Threat Assessment: Ignoble Scorpius, Distributors of BlackSuit Ransomware.” https://unit42.paloaltonetworks.com/threat-assessment-blacksuit-ransomware-ignoble-scorpius/

Adversary Pursuit Group