TTPs used by BlackByte Ransomware Targeting Critical Infrastructure

By Huseyin Can YUCEEL

Published: 2022-02-21 · Archived: 2026-04-05 14:02:49 UTC

On February 15th, 2022, the FBI and US Secret Service issued a joint advisory on BlackByte ransomware and its indicators of compromise (IOCs). According to the alert, BlackByte ransomware attacks on critical US infrastructures are on the rise. In this blog, we explained TTPs used by the BlackByte ransomware group in detail.

Test your security controls against BlackByte Ransomware NOW!

BlackByte Ransomware Group

BlackByte operates as a Ransomware-as-a-Service group and began its campaign in July 2021. Since then, it has targeted U.S. organizations in critical infrastructure sectors, including government, finance, and food and agriculture. The group also breached the San Francisco 49ers and published portions of the team's confidential data as proof of the attack.

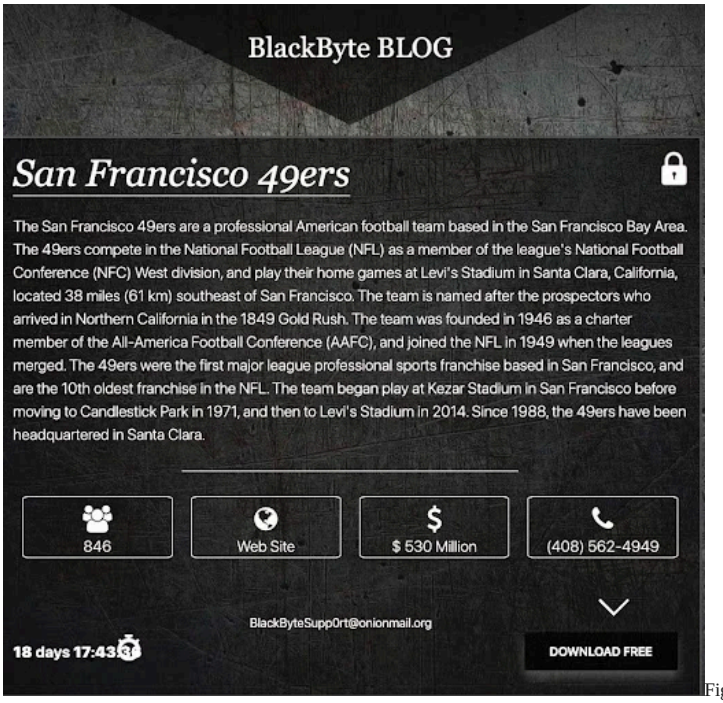

Figure 1: Ransom note of BlackByte for SF49ers[1]

Joint cybersecurity advisory from FBI and US Secret Service warns organizations that beware of the IOCs of BlackByte ransomware attacks and take necessary precautions as the number of attacks is expected to increase.

What is BlackByte Ransomware?

BlackByte ransomware is the collective name of the ransomware variants from the BlackByte RaaS group. The ransomware was first reported back in July 2021. It exploits ProxyShell vulnerabilities found in Microsoft Exchange Server for initial access. The patch for these vulnerabilities is available. However, unpatched systems are falling victim to these ransomware attacks. Check out our blog post and learn how to prevent the exploitation of ProxyShell vulnerabilities.

The ransomware does not attack the infected systems if the language setting is Russian or the languages of former Soviet republics. This behavior is similar to some other ransomware threat groups, as explained in our previous ransomware blog, LockBit 2.0.

BlackByte ransomware variants only use symmetric encryption. In their earlier ransomware variants, The BlackByte threat group distributed the encryption key to every victim from their command and control (C2) server in a .png file. Since the same encryption key is used for every victim, Trustwave was able to devise a global decryptor [2]. After the release of the global decryptor, the ransomware group stopped delivering the encryption key from the C2 server and changed the key. Although the decryptor might not work in some cases, it is worth a try as it does not harm already encrypted files.

After encrypting the victim files, BlackByte ransomware appends the .blackbyte extension. The ransomware leaves the same ransom note in all encrypted directories, and the ransom note includes a .onion link that instructs the victim how to pay the ransom and receive the decryption key. Also, the ransom note claims that the ransomware has exfiltrated data from its victims to scare its victims to pay the ransom.

How Picus Helps Simulate BlackByte Ransomware?

Using the Picus Continuous Security Validation Platform, you can test your security controls against the BlackByte ransomware. We advise you to simulate BlackByte ransomware attacks and determine whether your security controls can prevent them or not. Picus Threat Library includes the following threats to simulate BlackByte ransomware.

Threat Name
BlackByte Ransomware .EXE File Download (1-variant)
BlackByte Ransomware Scenario

Test your security controls against BlackByte Ransomware in minutes!

MITRE ATT&CK Techniques Used by the BlackByte Ransomware

Reconnaissance

- **T1595.002 Active Scanning: Vulnerability Scanning**

The Blackbyte ransomware group exploits several vulnerabilities in the Microsoft Exchange Server. The ransomware threat actors scan the network of their targets and check whether the network has CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 vulnerabilities.

Initial Access

- **T1190 Exploit Public Facing Application**

BlackByte ransomware threat actors exploit ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) found in Microsoft Exchange Server to gain initial access to the target network. Using ProxyShell vulnerabilities, the BlackByte RaaS group drops a webshell with the .aspx extension.

CVE Number	CVSS Score	Vulnerability
CVE-2021-34473	9.8 (Critical)	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-34523	9.8 (Critical)	Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2021-31207	7.2 (High)	Microsoft Exchange Server Security Feature Bypass Vulnerability
Directories where webshell might be located		
Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946		
inetpub\wwwroot\aspnet_client		
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth		

Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium

Execution

- **T1053.005 Scheduled Task/Job: Scheduled Task**

BlackByte ransomware utilizes Scheduled Tasks to launch its executable and print ransom notes using the printers in the victim's network.

Scheduled Tasks used by BlackByte	Description
complex.exe -single <SHA256_hash>	The ransomware executable is named "complex.exe". The purpose of the hash value is unknown; it might be the identifier of the victim.
cmd.exe /c for /l %x in (1,1,75) do start wordpad.exe /p C:\Users\tree.dll.	This command attempts to open tree.dll in Wordpad 75 times and then prints the contents. tree.dll contains the ransom note.

- **T1059.001 Command and Scripting Interpreter: PowerShell**
- **T1059.003 Command and Scripting Interpreter: Windows Command Shell**

The BlackByte threat group uses PowerShell and Windows Command Shell to execute its malicious commands.

Persistence

- **T1505.003 Server Software Component: Web Shell**

BlackByte ransomware abuses MSExchangeMailboxReplication.exe to place a webshell to establish a solid foothold in the victim's network.

Privilege Escalation

- **T1112 Modify Registry**

BlackByte ransomware modifies registries to elevate privileges.

Commands used to modify the registry	Description
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f	Escalate local privilege
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLinkedConnections /t REG_DWORD /d 1 /f	Enable OS to share network connections between different privilege levels

reg add HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v LongPathsEnabled /t REG_DWORD /d 1 /f	Enable long path values for file paths, names, and namespaces to ensure encryption of all file names and paths

Defense Evasion

- **T1027.002 Obfuscated Files or Information: Software Packing**

The BlackByte threat group uses obfuscation to make malware analysis difficult.

- **T1055 Process Injection**

BlackByte ransomware injects a Cobalt Strike beacon into wuauclt.exe.

- **T1070.004 Indicator Removal on Host: File Deletion**

BlackByte ransomware group deletes its executable after encryption to limit chances of analysis.

- **T1562.001 Impair Defenses or Modify Tools**

BlackByte ransomware stops Windows Defender by using an obfuscated PowerShell command. It also deletes a scheduled task for Raccine, a tool used to prevent ransomware attacks.

Commands used for defense evasion	Description
powershell -command "$x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('VwBpA'+'G4ARAB'+'lAGYA'+'ZQB'+'uAG'+'QA'));Stop-Service -Name $x;Set-Service -StartupType Disabled $x"	Stop Windows Defender from executing on Startup
schtasks.exe /DELETE /TN "\"Raccine Rules Updater\"" /F	Delete scheduled task for Raccine Rules Updater.

- **T1562.004 Impair Defenses: Disable or Modify System Firewall**

BlackByte threat actors change firewall rules to discover other assets in the victim's network.

Commands used for defense evasion	Description
netsh advfirewall firewall set rule "group=\"Network Discovery\"" new enable=Yes	Enable network discovery
netsh advfirewall firewall set rule "group=\"File and Printer Sharing\"" new enable=Yes	Enable file and printer sharing

Credential Access

- **T1003 OS Credential Dumping**

BlackByte group uses Cobalt Strike to dump credentials and access service accounts in the victim network.

Discovery

- **T1012 Query Registry**

BlackByte ransomware checks the language settings by querying the related registries.

- **T1016 System Network Configuration Discovery**
- **T1018 Remote System Discovery**

BlackByte uses the following commands to discover other assets in the victim's network.

Commands used for discovery	Description
net.exe view	Display a list of domains, computers, or resources that are being shared
arp.exe -a	Display the current ARP cache tables for all interface

Lateral Movement

- **T1021.002 Remote Services: SMB/Windows Admin Shares**

BlackByte ransomware creates SMB shares to distribute AnyDesk, a remote desktop application, to other assets in the victim's network using Cobalt Strike.

Collection

- **T1560.001 Archive Collected Data: Archive via Utility**

BlackByte compresses the victim's file before exfiltration.

Command and Control (C2)

- **T1105 Ingress Tool Transfer**

The BlackByte group transfers a Cobalt Strike beacon to the victim using the webshell they placed. After the beacon is placed, they transfer the AnyDesk application.

Exfiltration

- **T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage**

BlackByte ransomware sends victim's compressed files to anonymous file-sharing services such as anonymfiles.com and file.io.

Impact

- **T1486 Data Encrypted for Impact**

BlackByte uses symmetric key encryption to encrypt the victim's files. Check out our blog post to learn more detail on this MITRE ATT&CK technique.

- **T1490 Inhibit System Recovery**

BlackByte ransomware resizes and deletes volume shadow copies to prevent file recovery using built-in recovery services.

Commands used for Inhibit System Recovery	Description
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded	Resize volume shadow copy sizes
powershell.exe $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgBfAFMAaABhAGQAb	Delete volume shadow copies Decoded command:

wB3AGMAbwBwAHkAIAB8AC'+'AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkA'+'F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA==''));Invoke-Expression $x	Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

Indicators of Compromise (IOCs)

Command and Control Server IPs:
185.93.6.31
45.9.148.114

MD5 Hashes		
4d2da36174633565f3dd5ed6dc5033c4	cd7034692d8f29f9146deb3641de7986	d63a7756bfdcd2be6c755bf288a92c8b
eed7357ab8d2fe31ea3dbcf3f9b7ec74	695e343b81a7b0208cbae33e11f7044c	296c51eb03e70808304b5f0e050f4f94
0c7b8da133799dd72d0dbe3ea012031e	a77899602387665cddb6a0f021184a2b	1473c91e9c0588f92928bed0ebf5e0f4
28b791746c97c0c04dcbfe0954e7173b	52b8ae74406e2f52fd81c8458647acd8	1785f4058c78ae3dd030808212ae3b04
b8e24e6436f6bed17757d011780e87b9	8dfa48e56fc3a6a2272771e708cdb4d2	4ce0bdd2d4303bf77611b8b34c7d2883
c010d1326689b95a3d8106f75003427c	ae6fbc60ba9c0f3a0fef72aeffcd3dc7	405cb8b1e55bb2a50f2ef3e7c2b28496
11e35160fc4efabd0a3bd7a7c6afc91b	659b77f88288b4874b5abe41ed36380d	151c6f04aeff0e00c54929f25328f6f7
959a7df5c465fcd963a641d87c18a565	5f40e1859053b70df9c0753d327f2cee	df7befc8cdc3c5434ef27cc669fb1e4b
51f2cf541f004d3c1fa8b0f94c89914a	d9e94f076d175ace80f211ea298fa46e	8320d9ec2eab7f5ff49186b2e630a15f
cea6be26d81a8ff3db0d9da666cd0f8f	31f818372fa07d1fd158c91510b6a077	d9e94f076d175ace80f211ea298fa46e
a9cf6dce244ad9afd8ca92820b9c11b9	7139415fecd716bec6d38d2004176f5d	c13bf39e2f8bf49c9754de7fb1396a33
ad29212716d0b074d976ad7e33b8f35f	d4aa276a7fbe8dcd858174eeacbb26ce	58e8043876f2f302fbc98d00c270778b
d2a15e76a4bfa7eb007a07fc8738edfb	e46bfbdf1031ea5a383040d0aa598d45	

MD5	SHA-1	SHA-256
5c0a549ae45d9abe54ab662e53c484e2	f3574a47570cccebb1c502287e21218277ffc589	e837f252af30cc222a1bce815e609a7354e1f9c814baefbb

9344afc63753cd5e2ee0ff9aed43dc56	ee1fa399ace734c33b77c62b6fb010219580448f	1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a22
e2eb5b57a8765856be897b4f6dadca18	c90f32fd0fd4eefe752b7b3f7ebfbc7bd9092b16	91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130

Reference

[1] D. Goodin, “Hacking group is on a tear, hitting US critical infrastructure and SF 49ers,” *Ars Technica*, Feb. 14, 2022. [Online]. Available: https://arstechnica.com/information-technology/2022/02/hacking-group-is-on-a-tear-hitting-us-critical-infrastructure-and-sf-49ers/

[2] SpiderLabs, “GitHub - SpiderLabs/BlackByteDecryptor,” *GitHub*. [Online]. Available: https://github.com/SpiderLabs/BlackByteDecryptor

---