

Technical Analysis of Babuk Ransomware

By Alexandre Mundo, Thibault Seret,
Thomas Rocchia, and John Fokker



Table of Contents

4	Summary of Findings
5	Infection Map
5	Underground
7	Underground Observations
8	Update for Unix Machines
9	Technical Details
14	Vasa Locker: v1 Before the v1?
16	Conclusion
16	Additional Resources
17	Coverage
17	MITRE ATT&CK Techniques
18	IOCs
19	Services List
19	Process List
19	Mutexes
19	YARA Rule
23	McAfee ATR

Authors

This report was researched and written by:

- Alexandre Mundo
- Thibault Seret
- Thomas Roccia
- John Fokker

[Subscribe to receive threat information.](#)

Introduction

Babuk ransomware is a new ransomware threat discovered in 2021 that attacked at least five big enterprises, with one already paying the criminals \$85,000 after negotiations. This ransomware, as other variants, is deployed in the network of enterprises that the criminals carefully target and compromise. This modus operandi is known as the *Big-Game hunting strategy*.

The group behind Babuk has also adopted the same strategies as other ransomware groups and has leaked the stolen data.

The sample analyzed in this report has the following hash:

8203c2f0ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9.

This hash is related to version 1 of Babuk. It comes as an executable of 32 bits compiled in Visual C/C++ and has a small size of 30kb. This initial version is neither protected nor obfuscated.

In this report, McAfee® Advanced Threat Research (ATR) provides a deep insight of this new ransomware variant called Babuk.

Connect With Us



Technical Analysis of Babuk Ransomware

Summary of Findings

- Babuk ransomware is a new ransomware family originally detected at the beginning of 2021.
- Its operators adopted the same operating methods as other ransomware families and leaked the stolen data.
- Babuk's codebase and artefacts are highly similar to Vasa Locker's.
- Babuk advertises on both English-speaking and Russian-speaking forums.
- The individuals behind Babuk ransomware have explicitly expressed themselves negatively against the BlackLivesMatter (BLM) and LGBT communities.
- At least five companies have been breached as of January 15, 2021.
- The ransomware supports command line operation and embeds three different built-in commands used to spread itself and encrypt network resources.
- It checks the services and processes running so it can kill a predefined list and avoid detection.
- There are no local language checks, in contrast to other ransomware gangs that normally spare devices in certain countries.
- The limited diffusion of the ransomware may indicate that those behind it are not working within an organized group or with other partners.
- The most recent variant has been spotted packed (see the 'Additional Resources' section).

Connect With Us



REPORT

Infection Map

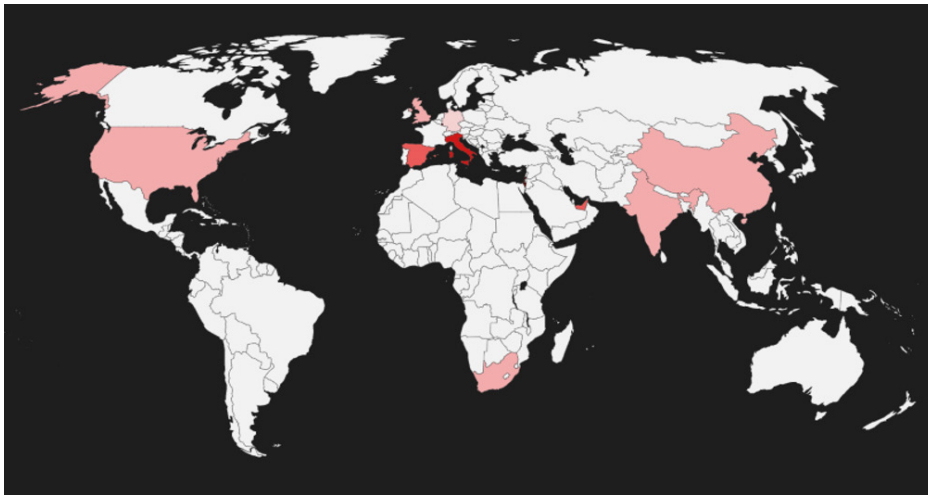


Figure 1. Infection map.

Underground

Babuk actors have been very verbose on an underground forum. The following screenshot shows a post where the authors advertised their leaks and their new support website.

A screenshot of a forum post on a dark-themed website. The post is titled "Babuk for press" and is by user "biba99". The post content includes a greeting, a description of BABUK as non-malicious specialized software, and a list of organizations that are not audited. The user profile for "GOD" is visible on the left side of the post.

Babuk for press
by biba99 - January 05, 2021 at 09:41 PM

January 05, 2021 at 09:41 PM. This post was last modified: January 05, 2021 at 09:49 PM by biba99. Edited 2 times in total.

Hello World! we are a team of babak, this post is for the press, also all entries will be duplicated in our blog, we express our great studying our product, this helps us to become even better

What is BABUK?

Non malicious, specialized software, created with purpose to show the security issues inside the corporate networks.

Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie-Hellman (ECDH) key generation to encrypt files

What issues are we talking about and why we are not a criminals?

In our understanding - we are some kind of a cyberpunks, we randomly test corporate networks security and in case of penetration threats and vulnerabilities we found, in our blog if company doesn't want to pay.

For example, imagine the situation: a hacker intruding the building company's network (huge developer who specializes on sports crazy fanatics from a terrorist organization, they get the blueprints and schematics... just think what going to be further...)

Our audit is not the worst thing that can happen to your company, but think twice, pay by money, or maybe the people lives...

Who is in the whitelist?

We do not audit next categories of organizations:

- *Hospitals (except private plastic surgery clinics, private dental clinics)
- *Any non-profitable charitable foundation (except the foundations who help LGBT and BLM)
- *Schools (except the major universities)
- *Companies with annual revenue less than 4 million\$ (info about revenue we take from zoominfo)

PM Find

A screenshot of a forum post titled "bocagroup.com by BABUK ransom 2gb all leaked". The post includes a table with columns for Display Name, Alias, Primary SMTP Address, and PW. The user profile for "GOD" is visible on the left side of the post.

bocagroup.com by BABUK ransom 2gb all leaked
by biba99 - January 11, 2021 at 03:29 PM

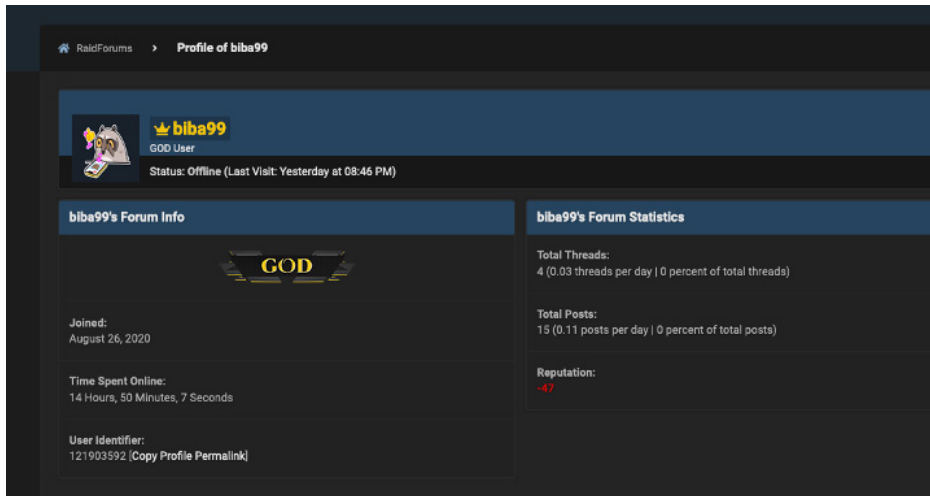
As America's premier elevator and escalator consulting company, BOCA Group is the partner of choice for the biggest and best-known building owners and developers.

Revenue: \$22 Million

Display Name	Alias	Primary SMTP Address	PW
Aaron Ruffins	aaron.ruffins	Aaron.Ruffins@bocagroup.com	Ar556677@01
Alejandrina Gallardo	Alejandrina.gallardo	Alejandrina.Gallardo@bocagroup.com	Ag5456@01
Alex Menendez	Alex.Menendez	Alex.Menendez@bocagroup.com	Am6789@01
Andrew Joseph	Andrew.joseph	Andrew.Joseph@bocagroup.com	Aj5454@01
Atif Chaudhry	Atif.Chaudhry	Atif.Chaudhry@bocagroup.com	Ac98765@01
AtlantichR	AtlantichR	AtlantichR@bocagroup.com	HRsupport4u
Bernadette Wernon	Bernadette.Wernon	Bernadette.Wernon@bocagroup.com	Bw0135@01

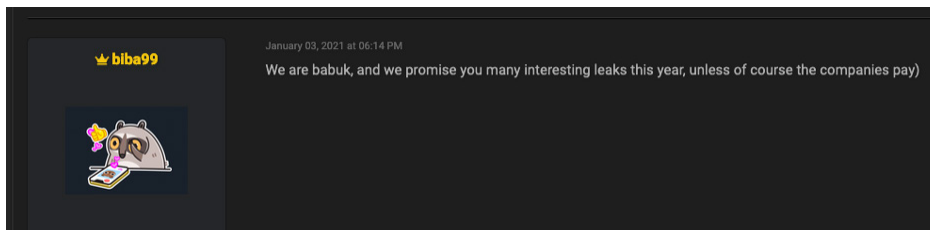
REPORT

As seen in the screenshot below, the persona with the username “Biba99,” created on August 26, 2020, has been active on the forum. All of Biba99’s posts are in the English language.



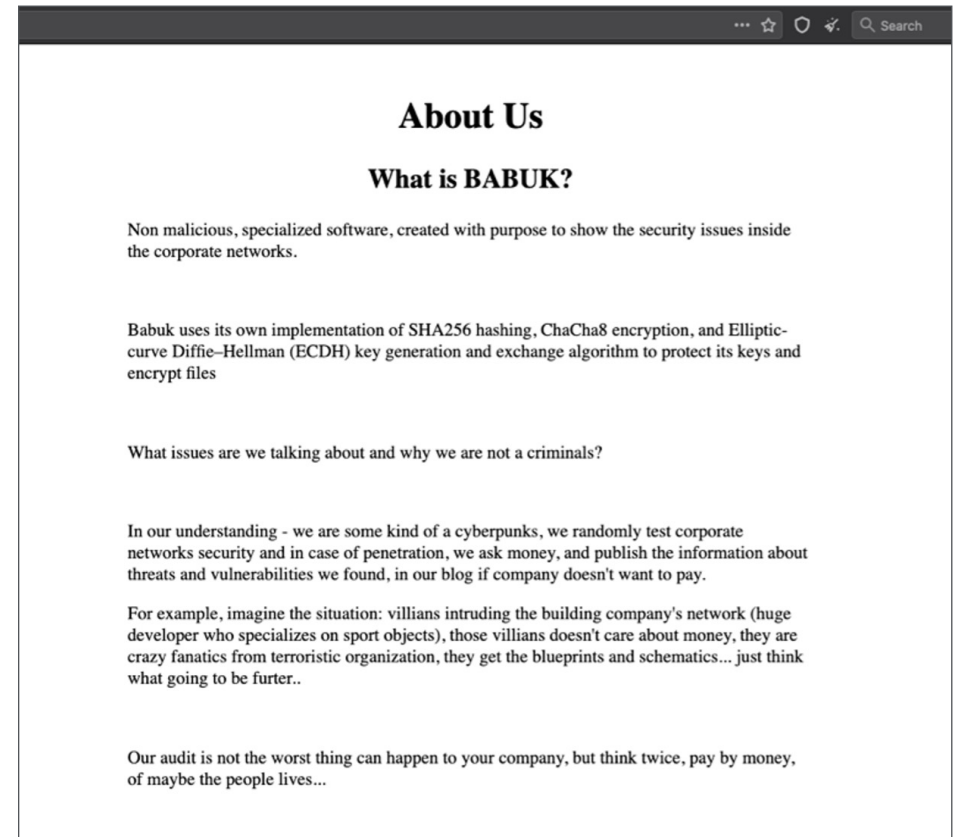
Published evidence suggests the group breached companies in the transport, healthcare, plastic, electronics, and agricultural sectors.

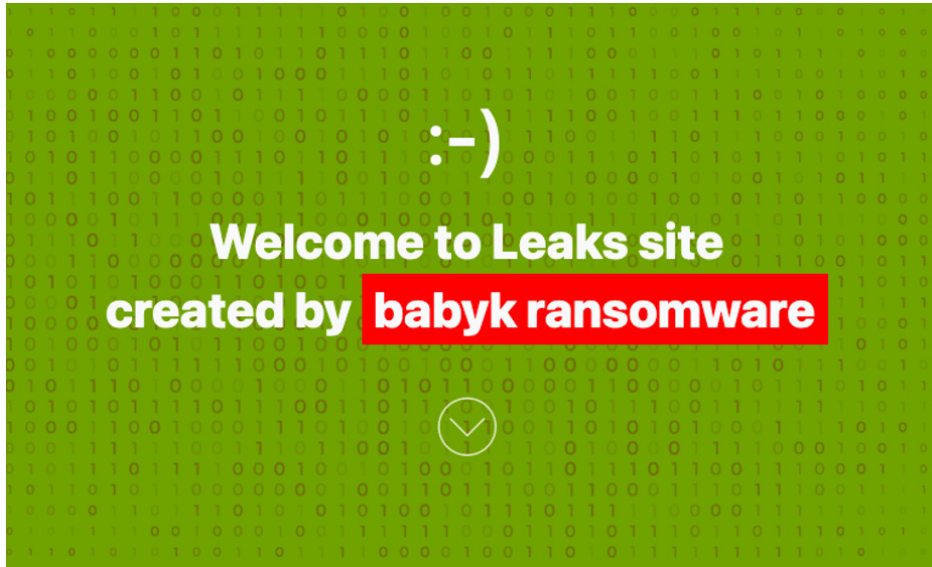
However, only two companies so far have had their data published by those behind the Babuk ransomware. This may indicate that the other victims decided to pay the ransom to avoid having their data leaked. The Babuk operators have indicated they may have breached several other companies.



Two websites are currently accessible; one is used to release the stolen data while the other is used as a support website:

- <http://gtmx56k4hutn3ikv.onion>
- <http://babukq4e2p4wu4iq.onion>



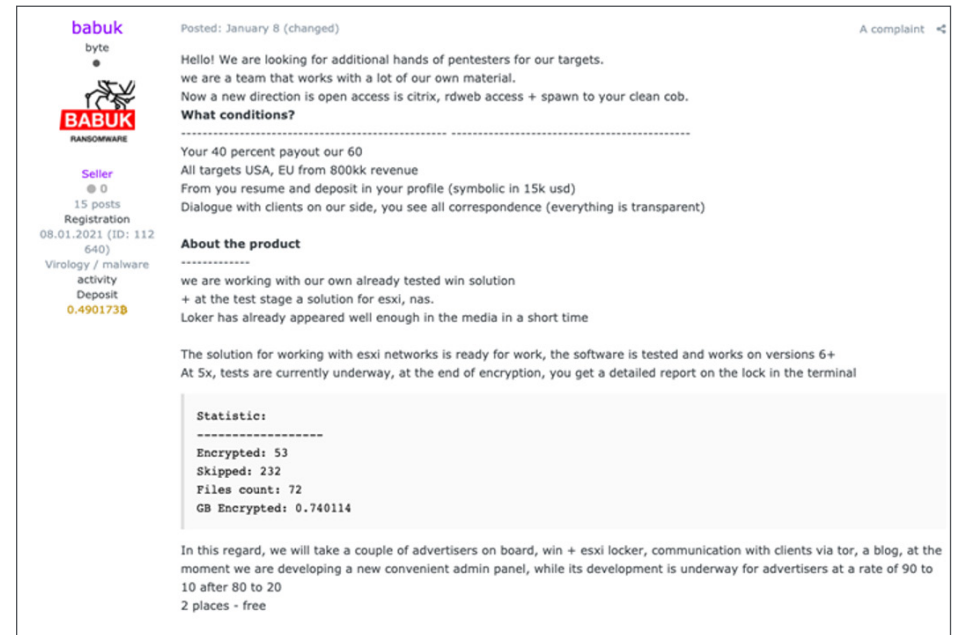


Interestingly, in the new version of the website, the malware developers changed the name from Babuk to Babyk. In Russian, the Cyrillic letter Y sounds similar to the Latin letter U.

It is interesting to note that the Babuk authors are making efforts to gain legitimacy on underground forums, either to advertise for future stolen data or to find potential new partners.

Underground Observations

The team behind Babuk first gained attention by advertising its activity on an English-speaking forum. Initially this was a bit out of the ordinary, since most major ransomware families prominently advertise and communicate on the Russian-speaking forums, though it was not long before we noticed Babuk activity on them too. Below is a screenshot of an affiliate recruitment advertisement, machine translated from Russian.



The advertisements on the Russian-speaking forums were more geared towards affiliate recruitment and details on technical improvements of their malware, whereas the English-speaking forum advertisements were more focused on victim announcements.

REPORT

As mentioned earlier, Babuk's posts are quite verbose. In its initial introductory message, Babuk states that it does not attack (whitelist) hospitals, non-profits, schools, or companies with less than a certain amount of revenue.

Who is in the whitelist?

We do not audit next categories of organizations:

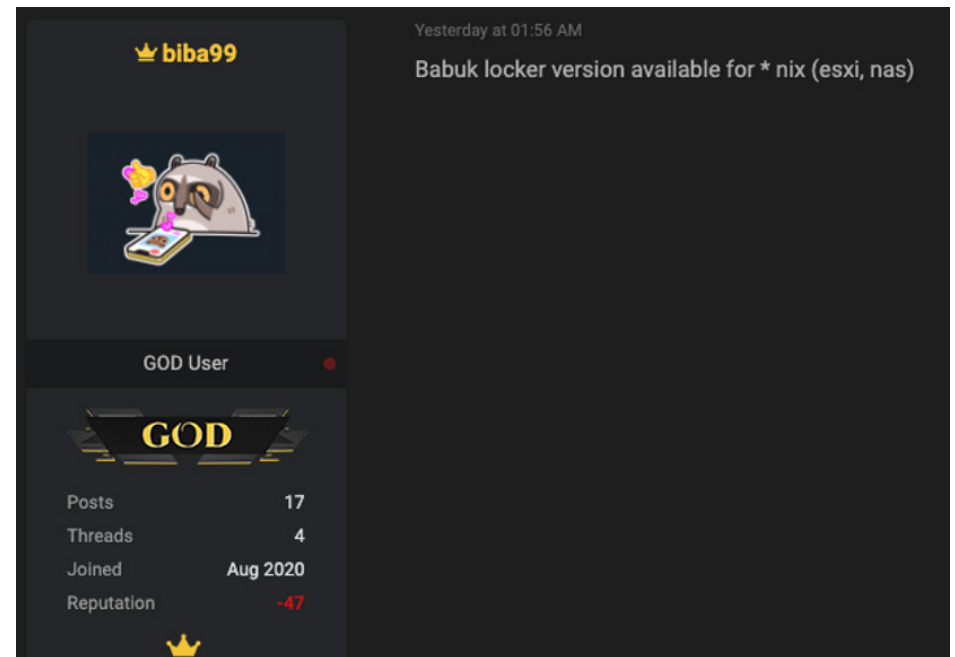
- *Hospitals (except private plastic surgery clinics, private dental clinics)
- *Any non-profitable charitable foundation (except the foundations who help LGBT and BLM)
- *Schools (except the major universities)
- *Companies with annual revenue less than 4 mln\$ (info about revenue we take from zoominfo)

However, what stands out is the explicit mention that it does attack organizations that support the LGBTQ or BlackLivesMatter causes. We have not observed this explicit mentioning before and believe, with a medium level of confidence, that this might be an indication that the criminals behind Babuk are from a social climate where LGBTQ and equality are not supported.

The explicit mentioning of the business intelligence tool ZoomInfo confirms our belief that ransomware criminals not only use the breached access to their victim's network to determine a ransom amount, but also rely on such tools to determine the net worth of an organization.

Update for Unix Machines

In a recent post we observed a new comment from the Babuk authors, which suggests they have prepared a Unix variant of the ransomware, to target NAS, ESXi servers or any other Unix system.



This message shows that Babuk authors are enforcing their relationship with potential partners or customers and extending their capabilities to other systems. We are actively monitoring this threat to detect future versions of the ransomware.

REPORT

Technical Details

The compiled timestamp is December 30, 2020. The sample was compiled without support for operating systems prior to Windows Vista. This is the first version released by the Babuk actors.

More information about the sample can be seen in the following table:

Name	8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9
Size	31232 bytes
File-Type	EXE
SHA 256	8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9
Compile time	30 December 2020 (seems legit)

The malware is a 32-bit executable (".EXE").

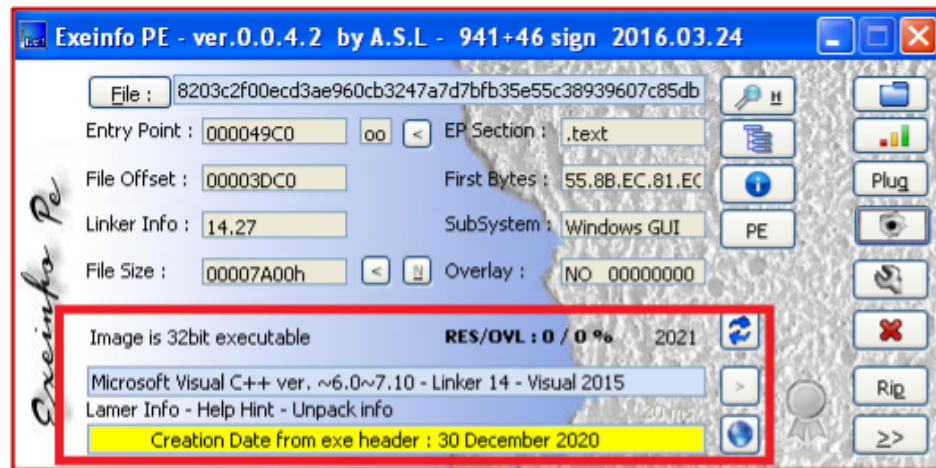


Figure 2. Information about the sample.

The malware is not protected in any way and does not use any packer.

The first action is a check for the arguments provided in the command line, using the function "GetCommandLineA." This is done later with a custom function to get the buffer of arguments prepared.

```
push    ebp
mov     ebp, esp
sub     esp, 278h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     [ebp+LocalVarLanMode], 0 ; default mode is lansecond
mov     [ebp+LocalVarNumberOfArgumentsCommandLine], 0
lea     eax, [ebp+LocalVarNumberOfArgumentsCommandLine]
push    eax ; int
call   ds:GetCommandLineA
push    eax ; lpString
call   BabukGetCommandLineArgumentsInLocalBufferFunction
add     esp, 8
mov     [ebp+LocalPointerToBufferOfArgumentsCommandLine], eax
cmp     [ebp+LocalVarNumberOfArgumentsCommandLine], 1
jle     _se_shutdown_parameters
mov     [ebp+LocalVarArgumentsCommandLineCounter], 1
jmp     short _check_if_need_check_arguments_and_check_lan_first
```

Figure 3. Get command line and arguments.

If no argument is passed, the malware has a mode to encrypt the network by default, but the following arguments can be added in the command line:

- lanfirst
- lansecond
- nolan

- The switch "-lanfirst" forces the mode of behavior to be "1"
- "-lansecond" forces the mode of behavior to be "0" (default value)
- "-nolan" forces the mode of behavior to be "-1"

REPORT

```

_check_if_need_check_arguments_and_check_lan_first: ; CODE XREF: start+50fj
mov     edx, [ebp+LocalVarArgumentsCommandLineCounter]
cmp     edx, [ebp+LocalVarNumberOFArgumentsCommandLine]
jge     _se_shutdown_parameters
push   offset aLanFirst ; "-lanfirst"
mov     eax, 4
shl     eax, 8
mov     ecx, [ebp+LocalPointerToBufferOFArgumentsCommandLine]
mov     edx, [ecx+eax]
push   edx ; lpString1
call   ds:IstrcmpA ; in this case the check is sensitive
test   eax, eax
jnz    short _check_lan_second_string
mov     [ebp+LocalVarLanMode], 1 ; set var to 1 if is the lanfirst string
jmp    short _prepare_to_check_arguments_command_line
;-----
```

Figure 4. Check arguments.

These command line options allow the malware to be very flexible, encrypting the mounted folder before or after the local disk. This support to use arguments gives the operators an easy way to encrypt the network resources.

At this point, we can note a programming mistake. The malware checks all arguments in the command line for these three switches and overrides the behavior mode based on the last valid argument. The malware developers do not use a “break” instruction to finish the argument loop when they get a valid argument, wasting time.

For example, “malware.exe -lanfirst -nolan” prevents the malware from encrypting the network as “-nolan” overrides the behavior mode of “-lanfirst.”

The next action is changing its shutdown level, setting this level to 0 with the function “SetProcessShutdownParameters.” This behavior is not very common in ransomware, but this forces the operating system to show a warning message at shutdown/reboot time, saying the malware process cannot be closed. The user is forced to reboot or shutdown the machine manually.

```

;-----
_se_shutdown_parameters: ; CODE XREF: start+4A7j
; start+777j
push   0 ; dwFlags
push   0 ; dwLevel
call   ds:SetProcessShutdownParameters
;-----
```

Figure 5. Set shutdown level as critical process.

The next action is enumerating all services in the system and stopping all of those which exist in a hardcoded list in the malware.

To perform this action, the ransomware gets the Service Control Manager using the function “OpenSCManagerA” and, with this handle, enumerates all services in the system.

```

sub     esp, 94h
mov     eax, __security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
push   esi
push   edi
mov     [ebp+lpServices], 0
call   ds:GetTickCount
mov     [ebp+LocalVarTimeTick], eax ; save time tick to later check w
mov     [ebp+var_70], 30000 ; 5 seconds
push   0F003Fh ; dwDesiredAccess
push   0 ; lpDatabaseName
push   0 ; lpMachineName
call   ds:OpenSCManagerA ; open sc manager |
mov     [ebp+hSCManager], eax
cmp     [ebp+hSCManager], 0
jz     _exit
mov     [ebp+LocalVarServicesCounter], 0 ; set counter var to 0
jmp    short _check_counter
;-----
```

Figure 6. Get Service Control Manager.

REPORT

The malware checks the status of the service if it is running. If this is the case, it receives the list of services that depend on it and stops them.

```
cmp [ebp+LocalVarServicesCounter], 44
jnb _close_service_manager_handler
push 44 ; dwDesiredAccess
mov ecx, [ebp+LocalVarServicesCounter]
mov edx, lpServiceName[ecx*4] ; using the counter access to the s
push edx ; lpServiceName
mov eax, [ebp+hSCManager]
push eax ; hSCManager
call ds:OpenServiceA
mov [ebp+hService], eax
cmp [ebp+hService], 0
jz _prepare_to_update_counter
lea ecx, [ebp+pcbBytesNeeded]
push ecx ; pcbBytesNeeded
push 24h ; cbBufSize
lea edx, [ebp+Buffer]
push edx ; lpBuffer
push 0 ; InfoLevel
mov eax, [ebp+hService]
push eax ; hService
call ds:QueryServiceStatusEx ; query service status |
test eax, eax
jz _close_service_handler
```

Figure 7. Get service to stop.

For these actions, the functions "QueryServiceStatusEx," "OpenServiceA," "EnumDependentServicesA," and "ControlService" are used. The list of the services closed can be read in the IOC part of this report.

The next action is checking the processes running in the victim system and closing them if they have a name within a hardcoded list in the malware.

```
push ebp
mov ebp, esp
sub esp, 240h
mov eax, ___security_cookie
xor eax, ebp
mov [ebp+var_4], eax
push 0 ; th32ProcessID
push 0Fh ; dwFlags
call CreateToolhelp32Snapshot
mov [ebp+hSnapshot], eax
mov [ebp+pe.dwSize], 22Ch ; important set the size of th
lea eax, [ebp+pe]
push eax ; lppe
mov ecx, [ebp+hSnapshot]
push ecx ; hSnapshot
call Process32FirstW
mov [ebp+LocalVarExistNextProcess], eax
```

Figure 8. Get processes list in the victim machine.

For this, the malware uses the functions "CreateToolhelp32Snapshot," "Process32FirstW," "Process32NextW," "OpenProcess," and "TerminateProcess."

```
jnz short _prepare_to_update_counter
mov eax, [ebp+pe.th32ProcessID]
push eax ; dwProcessID
push 0 ; bInheritHandle
push 1 ; dwDesiredAccess
call ds:OpenProcess
mov [ebp+hProcess], eax
cmp [ebp+hProcess], 0
jz short _prepare_get_next_process
push 9 ; uExitCode
mov ecx, [ebp+hProcess]
push ecx ; hProcess
call ds:TerminateProcess |
mov edx, [ebp+hProcess]
push edx ; hObject
call ds:CloseHandle
```

Figure 9. Open the process and terminate it.

REPORT

The next action is destroying the shadow volumes of the victim machine. It checks if the operating system is 64-bit or 32-bit using the function "IsWow64Process" in a dynamic call (as it does not exist in 32-bit operating systems) and removes the file system redirection to destroy the volumes.

```
sub     esp, 10h
mov     eax, __security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     [ebp+LocalVarPreviousStateFsRedirection], 0 ; set var to 0
call    BabukGetIsWow64ProcessAndCallItToDetectOSPlatformFunction
test    eax, eax
jz     short _delete_shadow_volumes
push   offset LibFileName ; "kernel32.dll"
call   ds:LoadLibrary@
mov     [ebp+hModule], eax
push   offset ProcName ; "Wow64DisableWow64FsRedirection"
mov     eax, [ebp+hModule]
push   eax
call   ds:GetProcAddress
mov     [ebp+LocalVarWow64DisableWow64FsRedirectionFunctionAddress], eax
cnp    [ebp+LocalVarWow64DisableWow64FsRedirectionFunctionAddress], 0 ; check against null
jz     short _delete_shadow_volumes
lea    ecx, [ebp+LocalVarPreviousStateFsRedirection]
push   ecx
call   [ebp+LocalVarWow64DisableWow64FsRedirectionFunctionAddress] ; dynamic call to Wow64Disa
```

Figure 10. Check operating system version.

To destroy the volume, it uses the native command "vssadmin.exe" with "ShellExecuteW."

```
_delete_shadow_volumes: ; CODE XREF: BabukGetOSPlatformAndRemoveFsRedirectionIfC
; BabukGetOSPlatformAndRemoveFsRedirectionIfCanAndDelete
push   0 ; nShowCmd
push   0 ; lpDirectory
push   offset Parameters ; "/c vssadmin.exe delete shadows /all /qu"...
push   offset File ; "cmd.exe"
push   offset Operation ; "open"
push   0 ; hwnd
call   ds:ShellExecuteW
call   BabukGetIsWow64ProcessAndCallItToDetectOSPlatformFunction |
test   eax, eax
jz     short _manage_securiy_cookie
push   offset aKernel32_dll_1 ; "kernel32.dll"
```

Figure 11. Destroy the shadow volumes.

The malware performs this action twice, first at the time of running, then after encrypting all files.

Babuk checks its behavior mode and encrypts the files in the network resources, using the functions "WNetOpenEnumW" and "WNetEnumResourceW."

```
push   13h ; dwUsage
push   0 ; dwType
push   2 ; dwScope
call   WNetOpenEnumW
test   eax, eax
jnz    _exit
mov    edx, [ebp+BufferSize]
push   edx
call   BabukEnterCriticalSectionAndReserveMemoryAndLeaveSectionFunction
add    esp, 4
mov    [ebp+lpNetResource], eax
cnp    [ebp+lpNetResource], 0
jz     _close_wt_enum

_loop_enumerate_resources: ; CODE XREF: BabukNetworkEnumerateTargetsAndCryptTh
lea    eax, [ebp+BufferSize]
push   eax ; lpBufferSize
mov    ecx, [ebp+lpNetResource]
push   ecx ; lpBuffer
lea    edx, [ebp+cCount]
push   edx ; lpCount
mov    eax, [ebp+hEnum]
push   eax ; hEnum
call   WNetEnumResourceW
```

Figure 12. Enumerate network resources.

In the encryption code, the developers made a slight mistake where they create a number of threads based on double the value of CPU cores on the victim machine. However, they later instantiate only one thread per logic disk to encrypt. This means that the encryption process is slow, as it depends on the number of disks, which is most likely lower than the number of processors.

Files are enumerated in the typical way for ransomware, but Babuk has a curious check that other ransoms do not have; it only encrypts a maximum of 16 folders deep, meaning that if one folder has 17 or more subfolders, the 17th and onward are ignored. This is probably to speed up the encryption process.

REPORT

```
push eax ; lpString?
mov ecx, [ebp+lpString1]
push ecx ; lpString1
call ds:lstrecatW
mov edx, [ebp+FindFileData.dwFileAttributes]
and edx, 14h ; check if is folder
jz short _check_if_ransom_note_name
cmp [ebp+ArgumentSecondNumberOfLevelsOffolders], 15 ; check if is 16 levels down in folders (maximum crypt
ja short _prepare_get_next_file ; if is 16 or more avoid enter in more deep folders and check the next fil
mov eax, [ebp+ArgumentSecondNumberOfLevelsOffolders]
add eax, 1 ; the number
push eax ; ArgumentSecondNumberOfLevelsOffolders
mov ecx, [ebp+lpString1]
push ecx ; lpString?
```

Figure 13. Check level of folder encryption.

The encryption process uses the ChaCha algorithm and protects the key and nonce with ECDH (Elliptic Curves). The key and nonce are generated randomly with the function "RltGenRandom." The private and public keys for ECDH are generated as such so that these keys are secure, finally using a public ECDH hardcoded in the malware to get the final key that is used to protect the ChaCha keys.

Only the malware developers can get this information as they have the private key to decrypt these keys. Babuk saves the public key generated on the disk in a file called "ecdh_pub_k.bin." (NB: Version 2 of Babuk is not using this file anymore.)

The files and folders to encrypt are checked with a typical hardcoded list with blacklisted names. After checking if the name is valid to encrypt, it checks whether the file has the ransom note name. In this case, it fetches the size of the target file.

```
push eax ; lpBuffer
push offset Name ; "APPDATA"
call ds:GetEnvironmentVariableW
push offset aEcdh_pub_k_bin ; "\\ecdh_pub_k.bin"
lea ecx, [ebp+Buffer]
push ecx ; lpString1
call ds:lstrcatW
mov [ebp+NumberOfBytesWritten], 0
push 0 ; hTemplateFile
push 80h ; dwFlagsAndAttributes
push 1 ; dwCreationDisposition
push 0 ; lpSecurityAttributes
push 1 ; dwShareMode
push 40000000h ; dwDesiredAccess
lea edx, [ebp+Buffer]
push edx ; lpFileName
call ds:CreateFileW
mov [ebp+hFile], eax
cnp [ebp+hFile], 0FFFFFFFh ; INVALID_HANDLE_VALUE
```

Figure 14. Save public key on disk.

If the size is less than 41,943,040 bytes, it encrypts it directly. If the size is larger, it will split it into three parts.

Like other ransomware variants, Babuk uses the Windows cache to write the files using "MapViewOfFile." This allows the malware to be faster and bypass some security programs.

```
jz _check_if_need_crypt_file_flag
lea edx, [ebp+FileSize]
push edx ; lpFileSize
mov eax, [ebp+hFile]
push eax ; hFile
call ds:GetFileSizeEx ; get file size
push 0 ; lpName
push 0 ; dwMaximumSizeLow
push 0 ; dwMaximumSizeHigh
push 4 ; flProtect
push 0 ; lpFileMappingAttributes
mov ecx, [ebp+hFile]
push ecx ; hFile
call ds:CreateFileMappingA ; map file in memory to crypt more quickly and au
mov [ebp+hFileMappingObject], eax
cnp [ebp+hFileMappingObject], 0
jz _flush_file_buffers
```

Figure 15. Map files to hasten the encryption process.

REPORT

Previously encrypted files have a new extension, “_NIST_K571_,” appended to them. The malware avoids all files that have this extension.

```
mov [ebp+lpString1], eax
cmp [ebp+lpString1], 0
jz short _prepare_to_exit
mov eax, [ebp+lpFileName]
push eax ; lpString2
mov ecx, [ebp+lpString1]
push ecx ; lpString1
call ds:IstrcpyW
push offset String2 ; “_NIST_K571_”
mov edx, [ebp+lpString1]
push edx ; lpString1
call ds:IstreatW
push 9 ; dwFlags
mov eax, [ebp+lpString1]
push eax ; lpNewFileName
mov ecx, [ebp+lpFileName]
push ecx ; lpExistingFileName
call ds:MoveFileExW ; set the ransom extension to mark it as encrypted
mov edx, [ebp+lpString1]
```

Figure 16. Add the extension hardcoded as encrypted file.

After encrypting all files in the folder, the malware drops a ransom note with the hardcoded name of the victim. This may indicate that only one sample per target is prepared. The ransomware note name is “How to Restore Your Files.txt.”

```
push ecx ; lpString1
call ds:IstrcpyW
push offset aHowToRestore_0 ; “\How To Restore Your Files.txt”
mov eax, [ebp+lpString1]
push eax ; lpString1
call ds:IstreatW ; join to the unit path the name of the ransomware note
push 0 ; hTemplateFile
push 0 ; dwFlagsAndAttributes
push 1 ; dwCreationDisposition
push 0 ; lpSecurityAttributes
push 1 ; dwShareMode
push 40000000h ; dwDesiredAccess
mov ecx, [ebp+lpString1]
push ecx ; lpFileName
call ds:CreateFileW ; create ransomware note file
mov [ebp+hFile], eax
cmp [ebp+hFile], 0FFFFFFFFh ; INVALID_HANDLE_VALUE
jz short release_memory
```

Figure 17. Create ransomware note.

Another curious thing about Babuk is that before starting the encryption process, it deletes the contents of the Recycle Bin using the function “SHEmptyRecycleBinA.”

```
call BabukGetOSPlatformAndRemoveFsRedirectionIfCanAndDeleteShadowVolumesAndReenab
push 7 ; dwFlags
push 0 ; pszRootPath - all recycle bins in the system
push 0 ; hwnd
call ds:SHEmptyRecycleBinA ; empty recycle bin in all units in the system
lea eax, [ebp+SystemInfo]
push eax ; lpSystemInfo
call ds:GetSystemInfo ; get number of cores of the cpu
mov ecx, [ebp+SystemInfo.dwNumberOfProcessors]
shl ecx, 1 ; mul by 2
```

Figure 18. Empty all recycle bins in the system.

Vasa Locker: v1 Before the v1?

Looking into Babuk’s history gives us insights into the team’s past activity. By doing this research, we can potentially determine the duration of the development process of the malware. We discovered a sample with a lot of similarities named “Vasa Locker” on VirusTotal:

Name	malware.exe_
Size	28160 bytes
File-Type	EXE
SHA 256	06d370217abec9468bc22c30ba3be72b8de1a7459f9e927656dcf2613a314bf6
Compile time	30 November 2020

By briefly looking at the information, we can see that the sample was compiled one month before the first release of Babuk v1.

REPORT

Vasa Locker has a lot of similarities with Babuk v1:

- Ransom notes look quite similar.

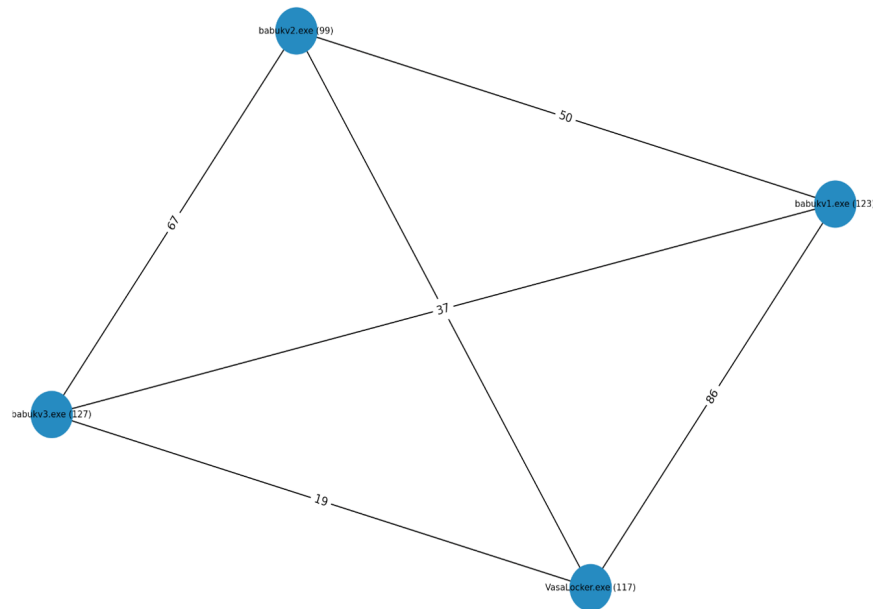
```
****BY BABUK LOCKER****
What happend
-----
Your computers and servers are encrypted, backups are deleted from your network and copied. We use strong encryption algorithms, so you cannot
decrypt your data.
But you can restore everything by purchasing a special program from us - a universal decoder. This program will restore your entire network.
Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting your data to the dark web.
What guarantees
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.
How to contact us
Using TOR Browser ( https://www.torproject.org/download/ ):
```

```
*****BY VASA LOCKER*****
What happend
-----
Your computers and servers are encrypted, backups are deleted from your network and copied. We use strong encryption algorithms, so you cannot
decrypt your data.
But you can restore everything by purchasing a special program from us - a universal decoder. This program will restore your entire network.
Follow our instructions below and you will recover all your data.
If you continue to ignore this for a long time, we will start reporting the hack to mainstream media and posting your data to the dark web.
What guarantees
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.
How to contact us
```

- In Vasa Locker's ransom note, victims are asked to contact the actor by using the mail `babukrip@protonmail.ch`.
- The extension added to encrypted files is the same for both samples `"__NIST_K571__"`.
- The same cryptographic method is used by both samples.
- The process kill list is the same.
- The directories list is the same.

REPORT

By analyzing code similarities between Vasa Locker and the first version of Babuk, we can see that around 86% of the code is shared:



Conclusion

Babuk ransomware is a new threat that first appeared in January 2021. The team is gaining more visibility by advertising on underground forums.

The encryption function does not differ much from other ransomware. An important point to note is the fact that no language blacklist is embedded in the malware.

The codebase itself and artefacts dropped, like the ransom notes, are highly similar to what was previously observed in Vasa Locker activities. There is a clear connection between the two variants, and probably between the teams, if indeed they are not one and the same.

What stands out with Babuk is the racial and anti-LGBTQ statements in its advertisements.

We believe that the team started this business very recently, with limited ransomware coding experience besides a potential Vasa Locker connection, as the code appears to embed several bugs and has been delivered without any obfuscation. However, the encryption algorithm used remains solid. Since we began this write up, a new variant was discovered, improving some of the mechanisms mentioned in this analysis. Additionally, a packed version of Babuk has also been found.

McAfee ATR is actively monitoring this threat and will update accordingly.

Additional Resources

- <https://sebdraiven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62>
- <http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/>
- <https://www.bleepingcomputer.com/news/security/babyk-ransomware-wont-hit-charities-unless-they-support-lgbt-blm/>

REPORT

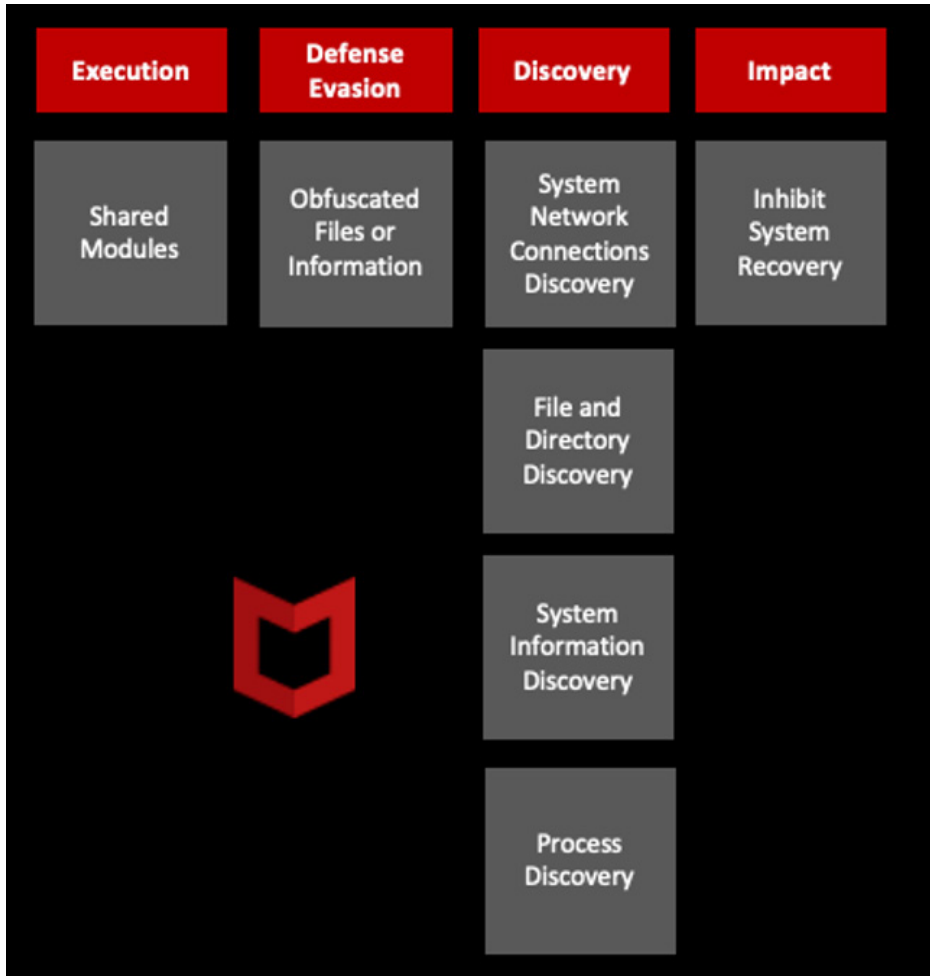
Coverage

We cover this malware with the name Ransom!Babuk<hash>.

MITRE ATT&CK Techniques

Tactic	Technique	Observable	IOCs
Defense Evasion	Obfuscated Files or Information (T1027)	Use ChaCha algorithm and protect the key and nonce with ECDH. The key and nonce are generated randomly.	Function: "RtlGenRandom"
Discovery	File and Directory Discovery (T1083)	Enumerates files on the system.	Functions: "FindFirstFile" "FindNextFile" "FindClose"
	System Information Discovery (T1082)	Enumerates disk volumes on the system, get disk information, query service status.	Functions: "FindFirstVolume" "FindNextVolume" "FindVolumeClose" "GetDriveType" "GetVolumePathNamesForVolumeName" "GetLogicalDrives" "QueryServiceStatusEx"
	Process Discovery (T1057)	Enumerates processes on the system.	Functions: "CreateToolhelp32Snapshot" "Process32First" "Process32Next"
	System Network Connections Discovery (T1049)	Babuk encrypts the files in the network resource.	Functions: "WNetOpenEnumW" "WNetEnumResourceW"
Execution	Shared Modules (T1129)	Link function at runtime.	Functions: "LoadLibrary" "GetProcAddress" "GetModuleHandle"
Impact	Inhibit System Recovery (T1490)	Delete the shadow volumes.	Command: "vssadmin.exe" Function: "ShellExecuteW"

REPORT



IOCs

550771bbf8a3e5625d6ec76d70ed86f6e443f07ce80f-f73e47f8249ddd72a8cf

704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f-945c85f4320

8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f-0495fa9

30fcff7add11ea6685a233c8ce1fc30abe67044630524a6e-b363573a4a9f88b8

1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff-8c17032aa017f6075c02

8140004ff3cf4923c928708505754497e48d26d822a95d63bd-2ed54e14f19766

c5167053129bd4a5542cfef9e739b0443e22e184cb4c0b57c049b448f-030cf15

bc4066c3b8d2bb4af593ced9905d1c9c78fff5b10ab8dbed7f-45da913fb2d748

3dda3ee9164d6815a18a2c23651a53c35d52e3a5ad375001ec-824cf532c202e6

391cfcd153881743556f76de7bbca5b19857f8b69a6f6f6dfde6fd9b-06c17f5e

REPORT

Services List

```
vss, sql, svc$, memtas, mepocs, sophos, veeam, backup,
GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr, DefWatch, ccEvtMgr,
ccSetMgr, SavRoam, RTVscan, QBFCService, QBIDPService,
Intuit.QuickBooks.FCS, QBCFMonitorService, YooBackup,
YooIT, zhudongfangyu, sophos, stc_raw_agent, VSNAPVSS,
VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc,
veeam, PDMFSService, BackupExecVSSProvider, BackupExecA-
gentAccelerator, BackupExecAgentBrowser,
BackupExecDiveciMediaService, BackupExecJobEngine,
BackupExecManagementService, BackupExecRPCService,
AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUupdateSvc,
```

Process List

```
sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe,
agntsvc.exe, isqlplussvc.exe,
xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe,
encsvc.exe, firefox.exe, tbirdconfig.exe,
mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreser-
vice.exe, excel.exe, infopath.exe, msaccess.exe,
mspub.exe, onenote.exe, outlook.exe, powerpnt.exe,
steam.exe, thebat.exe, thunderbird.exe,
visio.exe, winword.exe, wordpad.exe, notepad.exe
```

Mutexes

```
\Sessions\1\BaseNamedObjects\babuk_v2
\Sessions\1\BaseNamedObjects\babuk_v3
\Sessions\1\BaseNamedObjects\DoYouWantToHaveSexWith-
CoungDong
```

YARA Rule

```
rule Ransom_Babuk {
    meta:
        description = "Rule to detect Babuk Locker
unpacked"
        author = "McAfee ATR"
        date = "2021-01-19"
        hash = "e10713a4a5f635767dcd54d609bed977"
        rule_version = "v1.1"
        malware_family = "Ransom:Win/Babuk"
        malware_type = "Ransom"
        mitre_attack = "T1027, T1083, T1057, T1082,
T1129, T1490, T1543.003"
```

REPORT

```
strings:
```

```
  $s1 = "How To Restore Your Files.txt" fullword ascii
```

```
  $s2 = "delete shadows /all /quiet" fullword wide
```

```
  $pattern1 = {4DE88914818B55F483C2018955F4C645FE00EB600FB645FD85C074128B4DF0034DF8C601008B55F883C2018955F-  
8C645FD00C645FE01EB3CC645FD010FB645FE85C074188B4DF0034DF88B55F48B45E8890C908B4DF483C101894DF48B55F-  
00355F88A45FF88028B4DF8}
```

```
  $pattern2 = {FFFF83C040398578FFFFFF7D398B8D78FFFFFF3B4D1C7C02EB2C8B5514039578FFFFFF0FB6028B8D78FFFFFF2B8D74FFF  
FFF0FB6540DBC33C28B4D18038D78FFFFFF8801EBA7E940FFFFFF8B4DFC33CDE8}
```

```
  $pattern3 = {280FBE55FF83FA227506C645FC00EB148B45F00345F88A4DFF88088B55F883C2018955F8E9B50000000FBE45F-  
F8945E48B4DE483E909894DE4837DE41977638B55E4}
```

```
  $pattern4 = {08C7040A65787061B804000000C1E0008B4D08C704016E642033BA04000000D1E28B-  
4508C70410322D6279B9040000006BD1038B4508C704107465206BC745FC0000}
```

```
condition:
```

```
  filesize >= 15KB and filesize <= 80KB and
```

```
  1 of ($s*) and 3 of ($pattern*)
```

```
}
```

REPORT

```
rule RANSOM_Babuk_Packed_Feb2021 {

    meta:

        description = "Rule to detect Babuk Locker packed"
        author = "McAfee ATR"
        date = "2021-02-19"
        hash = "48e0f7d87fe74a2b61c74f0d32e6a8a5"
        rule_version = "v1"
        malware_family = "Ransom:Win/Babuk"
        malware_type = "Ransom"
        mitre_attack = "T1027.005, T1027, T1083, T1082, T1059, T1129"

    strings:

        // First stage

        $first_stagel = { 81 ec 30 04 00 00 68 6c 49 43 00 ff 15 74 20 43 00 a3 60 4e f8 02 b8 db d9 2b 00 ba c5
62 8e 76 b9 35 11 5f 39 eb 09 8d a4 24 00 00 00 00 8b ff 89 14 24 89 4c 24 04 81 04 24 25 10 a3 3b 81 04 24
cf e0 fb 07 81 04 24 35 26 9f 42 81 04 24 65 2b 39 06 81 04 24 3c 37 33 5b 81 44 24 04 48 4f c2 5d 83 e8 01
c7 05 54 4e f8 02 00 00 00 00 75 bf 8b 0d 54 aa 43 00 53 8b 1d 58 20 43 00 55 8b 2d 60 20 43 00 56 81 c1 01
24 0a 00 57 8b 3d 50 20 43 00 89 0d 64 4e f8 02 33 f6 eb 03 8d 49 00 81 f9 fc 00 00 00 75 08 6a 00 ff 15 40
20 43 00 6a 00 ff d7 8b 0d 64 4e f8 02 81 f9 7c 0e 00 00 75 19 6a 00 ff d3 6a 00 6a 00 8d 44 24 48 50 6a
00 6a 00 ff d5 8b 0d 64 4e f8 02 81 fe e5 84 c1 09 7e 0a 81 7c 24 2c 0f 11 00 00 75 12 46 8b c6 99 83 fa 14
7c aa 7f 07 3d 30 c1 cf c7 72 a1 51 6a 00 ff 15 2c 20 43 00 8b 0d 08 a4 43 00 33 f6 a3 f4 31 f8 02 89 0d f4
07 fb 02 39 35 64 4e f8 02 76 10 8b c6 e8 56 e4 ff ff 46 3b 35 64 4e f8 02 72 f0 8b 35 80 20 43 00 bf f0 72
```

REPORT

```
e9 00 8b ff 81 3d 64 4e f8 02 4d 09 00 00 75 04 6a 00 ff d6 83 ef 01 75 eb e8 d6 e3 ff ff e8 11 fe ff ff
e8 0c e4 ff ff 5f 5e 5d 33 c0 5b 81 c4 30 04 00 00 c3 }

$first_stage2 = {81ec3??4????68????????ff????????a3????????b8????????ba????????b9????????eb??8914248
94c240481????????81????????81????????81????????81????????81????????81????????81????????83e801c7????
????????75??8b????????538b????????558b????????5681????????578b????????89????????33f6eb-
??81????????75??6a??ff????????6a??ffd78b????????81????????75??6a??ffd36a??6a??8d442448506a??6a??ffd-
58b????????81????????7e??817c242c0f11????75??468bc69983????7c??7f??3d????????72??516a??ff??????-
????8b????????33f6a3????????89????????39????????76??8bc6e8????????463b????????72??8b????????bf????????8bf
f81????????75??6a??ffd683ef0175??e8????????e8????????e8????????5f5e5d33c05b81c43??4????c3}

$first_stage3 = {81ec3??4????68????????ff????????a3????????b8????????ba??????
??b9????????[2-6]891424894c240481????????81????????81????????81????????81????????-
????81????????81????????83e801c7????????????????[2-
6]8b????????538b????????558b????????5681????????578b????????89????????3
3f6[2-6]81????????[2-6]6a??ff????????6a??ffd78b????????81????????[2-6]6a??ff-
d36a??6a??8d442448506a??6a??ffd58b????????81????????[2-6]817c242c0f11????[2-6]468bc69983????[2-6]
[2-6]3d????????[2-6]516a??ff????????8b????????33f6a3????????89????????39????????[2-6]8b-
c6e8????????463b????????[2-6]8b????????bf????????8bff81????????????[2-6]6a??ffd683ef01[2-6]e8????????e8??
????e8????????5f5e5d33c05b81c43??4????c3}

$first_stage4 = { 81 EC 30 04 00 00 68 6C 49 43 00 FF 15 ?? ?? ?? ?? A3 ?? ?? ?? ?? B8 DB D9 2B 00 BA C5
62 8E 76 B9 35 11 5F 39 EB ?? 8D A4 24 ?? ?? ?? ?? 8B FF 89 14 24 89 4C 24 ?? 81 04 24 25 10 A3 3B 81 04 24
CF E0 FB 07 81 04 24 35 26 9F 42 81 04 24 65 2B 39 06 81 04 24 3C 37 33 5B 81 44 24 ?? 48 4F C2 5D 83 E8 01
C7 05 ?? ?? ?? ?? 00 00 00 00 75 ?? 8B 0D ?? ?? ?? ?? 53 8B 1D ?? ?? ?? ?? 55 8B 2D ?? ?? ?? ?? 56 81 C1 01
24 0A 00 57 8B 3D ?? ?? ?? ?? 89 0D ?? ?? ?? ?? 33 F6 EB ?? 8D 49 ?? 81 F9 FC 00 00 00 75 ?? 6A 00 FF 15 ??
?? ?? ?? 6A 00 FF D7 8B 0D ?? ?? ?? ?? 81 F9 7C 0E 00 00 75 ?? 6A 00 FF D3 6A 00 6A 00 8D 44 24 ?? 50 6A 00
6A 00 FF D5 8B 0D ?? ?? ?? ?? 81 FE E5 84 C1 09 7E ?? 81 7C 24 ?? 0F 11 00 00 75 ?? 46 8B C6 99 83 FA 14 7C
?? 7F ?? 3D 30 C1 CF C7 72 ?? 51 6A 00 FF 15 ?? ?? ?? ?? 8B 0D ?? ?? ?? ?? 33 F6 A3 ?? ?? ?? ?? 89 0D ?? ??
?? ?? 39 35 ?? ?? ?? ?? 76 ?? 8B C6 E8 ?? ?? ?? ?? 46 3B 35 ?? ?? ?? ?? 72 ?? 8B 35 ?? ?? ?? ?? BF F0 72 E9
00 8B FF 81 3D ?? ?? ?? ?? 4D 09 00 00 75 ?? 6A 00 FF D6 83 EF 01 75 ?? E8 ?? ?? ?? ?? E8 ?? ?? ?? ?? E8 ??
?? ?? ?? 5F 5E 5D 33 C0 5B 81 C4 30 04 00 00 C3}
```

```
// Files encryption function

$files_encryption1 = { 8a 46 02 c1 e9 02 88
47 02 83 ee 02 83 ef 02 83 f9 08 72 88 fd f3
a5 fc ff 24 95 20 81 40 00 }

$files_encryption2 = {8a4602c1e90288470283ee0
283ef0283????72??fdf3a5fcff??????????}

$files_encryption3 = { 8A 46 ?? C1 E9 02 88
47 ?? 83 EE 02 83 EF 02 83 F9 08 72 ?? FD F3
A5 FC FF 24 95 ?? ?? ?? ??}

condition:

    filesize <= 300KB and

    any of ($first_stage*) and

    any of ($files_encryption*)

}
```

McAfee ATR

The McAfee Advanced Threat Research Operational Intelligence team operates globally around the clock, keeping watch of the latest cyber campaigns and actively tracking the most impactful cyber threats. Several McAfee products and reports, such as MVISION Insights and APG ATLAS, are fueled with the team's intelligence work. In addition to providing the latest Threat Intelligence to our customers, the team also performs unique quality checks and enriches the incoming data from all of McAfee's sensors in a way that allows customers to hit the ground running and focus on the threats that matter.

[Subscribe to receive our Threat Information.](#)

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com



6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2021 McAfee, LLC. 4711_0221
FEBRUARY 2021