Technical Analysis of Babuk Ransomware

By Alexandre Mundo, Thibault Seret, Thomas Roccia, 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
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:

8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9.

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.
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).
Technical Analysis of Babuk Ransomware

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.
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:

- hxpx://gtmx56k4hutn3ikv.onion
- hxpx://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 Ы 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.
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.

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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>8203c2f00ecd3ae960cb3247a7d7bf35e55c38939607c85dbdb5c92f0495fa9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>31232 bytes</td>
</tr>
<tr>
<td>File-Type</td>
<td>EXE</td>
</tr>
<tr>
<td>SHA 256</td>
<td>8203c2f00ecd3ae960cb3247a7d7bf35e55c38939607c85dbdb5c92f0495fa9</td>
</tr>
<tr>
<td>Compile time</td>
<td>30 December 2020 (seems legit)</td>
</tr>
</tbody>
</table>

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

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.

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”
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.
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.

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.

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

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

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

---

```c
push 13h ; dwUsage
push 0 ; dwFlags
push 2 ; dwScope
call WNetOpenEnumW
test eax, eax
jmp .exit
mov edx, [ebp+BufSize]
push edx
call BabukEnterCriticalSectionAndResumeMemoryAndLeaveCriticalSectionFunction
add esp, 8
mov [ebp+IpNetResource], eax
cmp [ebp+IpNetResource], 0
jz _close_ut_enum

; CODE XREF: BabukGetOSPlatformAndRemoveFsRedirectionIFC
; BabukGetOSPlatformAndRemoveFsRedirectionIFCandDelete
push 0
push 0
; lDirectory
push OFFSET Parameters ; /f vsadmin.exe delete shadows /all /q...
push OFFSET File ; "vsadmin.exe"
push OFFSET Operation ; "delete"
push 0 ; HND
call ShellExecuteW
call BabukGetOSPlatformAndCallItToDetectOSPlatformFunction
lea eax, [ebp+BufferSize]
push eax
add esp, 8
mov [ebp+IpNetResource], eax
cmp eax, [ebp+RequestCount]
jnz .repeat
lea eax, [ebp+Count]
push edx
add esp, 8
mov eax, [ebp+Num]
push eax
add esp, 8
call WNetEnumResourceW

; CODE XREF: BabukNetworkEnumerateTargetsAndCryptThe
lea eax, [ebp+BufferSize]
push eax
add esp, 8
mov ecx, [ebp+IpNetResource]
push ecx
add esp, 8
lea edx, [ebp+Count]
push edx
add esp, 8
mov eax, [ebp+Num]
push eax
add esp, 8
call WNetEnumResourceW
```

---

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

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 ransomwares 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.
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.

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.

Figure 13. Check level of folder encryption.

Figure 14. Save public key on disk.

Figure 15. Map files to hasten the encryption process.
Previously encrypted files have a new extension, “._NIST_K571._,” appended to them. The malware avoids all files that have this extension.

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.”

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

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>malware.exe_</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>28160 bytes</td>
</tr>
<tr>
<td>File-Type</td>
<td>EXE</td>
</tr>
<tr>
<td>SHA 256</td>
<td>06d720217a96ba9486b22c30ba3be72b8de1a7459f9e9527656dcf2613a314bf6</td>
</tr>
<tr>
<td>Compile time</td>
<td>30 November 2020</td>
</tr>
</tbody>
</table>

By briefly looking at the information, we can see that the sample was compiled one month before the first release of Babuk v1.
Vasa Locker has a lot of similarities with Babuk v1:

- Ransom notes look quite similar.

<table>
<thead>
<tr>
<th>What happen</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. 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.</td>
</tr>
</tbody>
</table>

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.
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://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62](https://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62)
- [http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/](http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/)
**Coverage**

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

### MITRE ATT&CK Techniques

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

550771bbf8a3e5625d6ec76d70ed86f6e443f07ce80f-f73e47f8249ddd72a8cf
704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f-945c85f4320
8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f-0495fa9
30fcff7add11ea685a233c8ce1fc30abe67044630524a6e-b363573a4a9f88b8
1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff-8c17032aa0176075c02
8140004ff3cf4923c928708505754497e48d26d822a95d63bd-2ed54e14f19766
c5167053129bd4a5542cfcf9e739b0443e22e184cb4c0b57c049b448f-030cf15
bc4066c3b8d2bb4af593ced9905d1c9c78fff5b10ab8d67df-45da913fb2d748
3dda3ee9164d6815a18a2c23651a53c35d52e3a5ad375001ec-824cf532c202e6
391cfd153881743556f76e7bbca5b19857f8b69a6f6f6dfde6fd9b-06c17f5e
Services List

vss, sql, svc$, memtas, mepocs, sophos, veeam, backup, GxVss, GxBir, GxFWD, GxCVD, GxCIMgr, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, RTVscan, QBFCService, QBIDPService, Intuit.QuickBooks.FCS, QBCMonitorService, YooBackup, YooIT, zhudongfangyu, sophos, stc_raw_agent, VSAPVSS, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, veeam, PDVFSvc, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDivenciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUpsateSvc,

Process List


Mutexes

\Sessions\BaseNamedObjects\babuk_v2
\Sessions\BaseNamedObjects\babuk_v3
\Sessions\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"
strings:

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

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

$pattern1 = {4DE8891481B55F483C2018955F4C645FE0EB600FB645FD85C074128B4DF0034DF8C601008B55F883C2018955F-
8C645FD00C645FE01EB3CC645FD010FB645FE85C074188B4DF0034DF88B55F48B45E8890C908B4DF483C101894DF48B55F-
00355F88A45FF88028B4DF8}

$pattern2 = {FFFF83C040398578FFFFFF7D398B8D78FFFFFF3B4D1C7C02EB2C8B5514039578FFFFFFFF0FB602B8D78FFFFFF2B8D74FF
FFF0FB6540DBC3C2B4D1B038D78FFFFFF8801EBA7E940FFFFFF8B4DFC33CDE8}

$pattern3 = {280FBE55F83FA227506C645FC00EB148B45F00345F88A4DF88088B55F883C2018955F8E9B5000000FBE45F-
F8945E48B4DE483E909894DE4837DE41977638B55E4}

$pattern4 = {08C7040A65787061B804000000C1E0008B4D08C704016E642033BA04000000D1E28B-
4508C70410322D627B9040000006BD1038B4508C704107465206BC745FC0000}

condition:

filesize >= 15KB and filesize <= 80KB and
1 of ($s*) and 3 of ($pattern*)
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 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 26 26 9f 42 81 04 24 26 26 3b 39 06 81 04 24 3c 37 33 5b 81 04 24 04 48 4f c2 5d 83 e8 01 c7 05 54 4e f8 02 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 66 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 00 64 4e f8 02 81 f9 7c 0e 00 00 75 19 6a 00 ff d3 6a 00 6a 00 8d 44 44 44 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 01 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 6f f0 72}
Technical Analysis of Babuk Ransomware

$first_stage2 = (8lec3??4????68????????ff????????a3????????b8????????ba????????b9????????eb??8914248
94c240481?????????81?????????81????????81?????????81?????????81?????????81?e801c7???
????????????75??8b????????53b????????55b????????5681????????578b2????????89????????3f6eb-
??8l????????????75??6a?ff????????6a?ffd78b????????81????????75??6a?ffd36a?6a?8d442448506a?6a?ff-
58b????????81????????????7e??817c242c0f11????75??468bc69983????7c??7f??3d????????72??516a??ff????-
??????b????????33f6a????????89????????39????????76??8bc6e8????????463b????????72??8b?????????bf????????8b
f81????????????75??6a??ffd683ef0175??e8????????e8????????e8????????e8????????5f5e5d33c05b81c43????4????c3)

$first_stage3 = (8lec3??4????68????????ff????????a3????????b8????????ba????????b9????????eb??8914248
94c240481?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81?????????81??
// 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 = {8a4602c1e90288470283ee0283ef0283????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*)
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