

January 28, 2021

Industry Security Bulletin

Babuk Ransomware

EXECUTIVE SUMMARY

Babuk, also known as 'Babuk Locker', 'Babyk' and initially 'Vasa Locker', is a ransomware threat utilizing big-game hunter tactics to 'steal, encrypt and leak' victim data in an attempt to extort payments of reportedly up to USD 85,000 in Bitcoin (BTC).

As is often the case with threats of this nature, victims are likely determined by the ease at which they can be compromised combined with the likelihood of making payment. As such, Babuk's leak website states that the group will not target hospitals, non-profit charities or schools as well as avoiding organizations with an annual revenue of less than USD4 million. That being said, private clinics and major universities are considered 'fair game' along with charitable foundations 'who help LGBT and BLM' causes, the latter likely demonstrating the bigoted views of the threat actor.

Seemingly consistent with the above, identifiable victims thus far include organizations operating in the digital services, engineering and healthcare sectors that have operations in Germany, Hong Kong, Sweden and the United States. Anecdotal data also suggests that malware samples have appearing in other Asian, European and North American countries although this may be as a consequence of increased security researcher activity rather than active compromises.

Whilst not much is known about how the victims were initially compromised, similar ransomware campaigns have previously taken advantage of infrastructure vulnerabilities, such as exploits found in remote desktop protocol (RDP) and virtual private network (VPN) hosts, or utilized stolen credentials to gain initial access.

Based on observations throughout January, Babuk appears to be an actively developed threat, likely set to be further fuelled by profits made from their nefarious campaigns.

Demonstrating the active development, the threat actor identity 'biba99' posted a message on 'RaidForums' (Figure 1), an online forum popular with cybercriminals, suggesting that a '*nix' version is being made available that could target NAS devices and VMware ESXi virtualization hosts alongside the already supported Windows hosts.

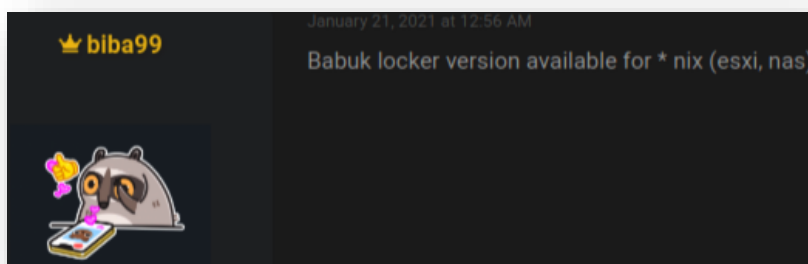


Figure 1 - Babuk Threat Actor Identity 'biba99' post on RaidForums (Jan 21, 2021)

Given the steady stream of victims and the active development thus far in 2021, Babuk could easily rise to be yet another infamous and credible targeted ransomware threat to organizations across multiple industries worldwide.

INITIAL COMPROMISE

Given the nature of this threat, and based on behaviours of other big-game hunter ransomware groups in their targeted attacks, the initial infection vector likely involves the compromise of some account, host or service rather than the ransomware payload being delivered by a broader technique such as an unsolicited malicious email (malspam).

As such, exploitation of vulnerabilities in internet-facing hosts or the compromise of account credentials, potentially following a phishing phase, could allow the threat actors to gain access to the target network.

Once this initial access has been achieved, an element of reconnaissance is almost certainly performed in order to both move laterally within the victim network as well as identifying potential valuable data and hosts.

Subsequently, and prior to the encryption phase, the threat actor is seemingly exfiltrating sensitive data such as documents and financial records related to company confidential matters as well as customer and employee financial and personal data.

The nature of this exfiltration will require forensic analysis of a victim and, as such, no detail has been published or shared thus far. That being said, typical methods could include data transfer to some command and control (C2) infrastructure or even the use of legitimate cloud services.

Having stolen this data, victims that fail to comply with the ransom demands may find that their data is made publicly available (Figure 2) on Babuk's 'Leak Site' (Figure 3) hosted on Tor.

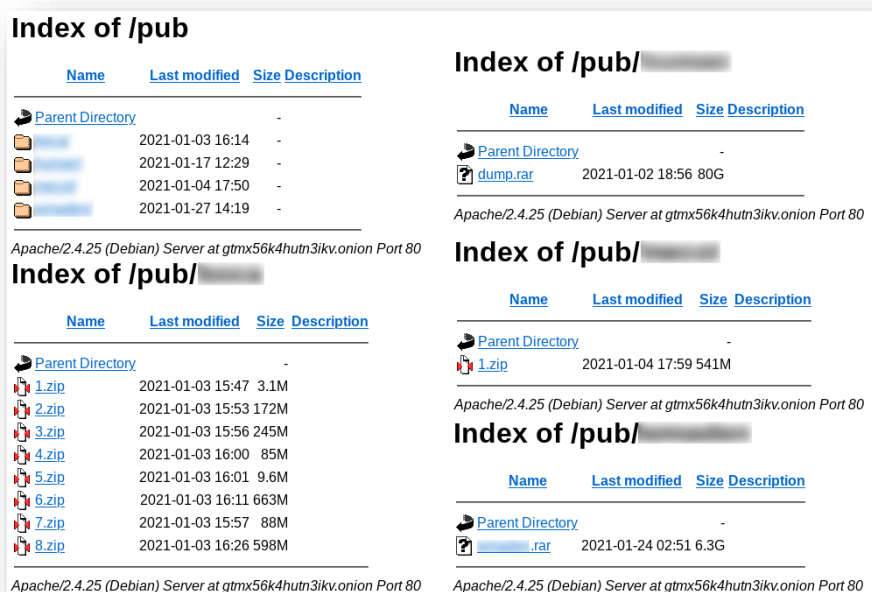


Figure 2 - Babuk Leak Site 'Victim Data Directories'

[ABOUT US](#) | [RULES](#)

Home Page of Leaks site

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)**

XXXXXXXXXX GmbH & Co. KG views: 1354 Published: 2021-01-24 03:28:55
XXXXXXXXXX 100gb data by BABUK locker views: 2662 Published: 2021-01-17 12:38:24
Official request to XXXXXXXXXX views: 2779 Published: 2021-01-15 01:44:08
XXXXXXXXXX.com views: 3045 Published: 2021-01-14 21:38:37

Figure 3 - Babuk Leak Site 'Home Page'

ENCRYPTION PROCESS

Notably, based on the ransomware payload samples observed thus far, it appears that each Babuk instance is victim-specific and includes one private encryption key specific to the victim. As such, it is clear that Babuk have tailored their campaigns toward 'big game' victims, allowing key generation to be easily managed, rather than indiscriminately targeting individuals.

Presumably after the threat actor has identified a suitable target host and exfiltrated sensitive data from it for use in the extortion phase, the Babuk payload is delivered and can be executed using command line arguments to determine if network shares will be encrypted along with local drives.

PREPARATION

Upon execution, Babuk follows the typical ransomware process of first attempting to terminate services and processes related to common applications, backup programs, endpoint security solutions and server software (Figures 4 & 5), for reference a list of these is provided in Appendix A.

```
OpenServiceA (hSCManager=0x459120, lpServiceName="AcronisAgent", dwDesiredAccess=0x2c) returned 0x0
OpenServiceA (hSCManager=0x459120, lpServiceName="CASAD2DWebSvc", dwDesiredAccess=0x2c) returned 0x0
OpenServiceA (hSCManager=0x459120, lpServiceName="CAARCUUpdateSvc", dwDesiredAccess=0x2c) returned 0x0
CloseServiceHandle (hSCObject=0x459120) returned 1
```

Figure 4 - Example Service Termination

```
Process32NextW (in: hSnapshot=0x124, lppe=0x14f760 | out: lppe=0x14f760*(dwSize=0x22c, cntUsage=0x0,
th32ProcessID=0x83c, th32DefaultHeapID=0x0, th32ModuleID=0x0, cntThreads=0x2,
th32ParentProcessID=0x454, pcPriClassBase=8, dwFlags=0x0, szExeFile="outlook.exe")) returned 1
TerminateProcess (hProcess=0x120, uExitCode=0x9) returned 1
CloseHandle (hObject=0x120) returned 1
```

Figure 5 - Example Process Termination

In addition to evading detection during the encryption process and complicating recovery efforts, terminating these processes and services ensures that open files are closed in preparation for being overwritten with encrypted data.

Again, utilizing a common ransomware technique, Windows shadow copies are deleted, in yet another step to thwart recovery, through the execution of the Volume Shadow Copy command line administration utility:

- "C:\\Windows\\System32\\cmd.exe" /c vssadmin.exe delete shadows /all /quiet

Finally in the preparation stage, the 'Recycle Bin' is emptied (Figure 6) presumably to ensure that no data can be recovered from it.

```
SHEmptyRecycleBinA (hwnd=0x0, pszRootPath=0x0, dwFlags=0x7) returned 0x8000ffff
```

Figure 6 - Windows 'Recycle Bin' Emptied

ENCRYPTION PHASE

As is to be expected, the ransomware first determines the disk type (fixed, network, optical, RAM or removable) using a list of drive letters before enumerating the available volumes and logical drives (Figure 7) to determine potential sources of data for encryption.

```
GetDriveTypeW (lpRootPathName="N:\\") returned 0x1
GetDriveTypeW (lpRootPathName="M:\\") returned 0x1
[...]
FindFirstVolumeW (in: lpszVolumeName=0x49bc50, cchBufferLength=0x8000 | out: lpszVolumeName="\\\\?
\\Volume{<GUID>}\\") returned 0x4764d0
GetVolumePathNamesForVolumeNameW (in: lpszVolumeName="\\\\?\\Volume{<GUID>}\\",
lpszVolumePathNames=0x14f784, cchBufferLength=0x78, lpcchReturnLength=0x14f780 | out:
lpszVolumePathNames=0x14f784, lpcchReturnLength=0x14f780) returned 1
lstrlenW (lpString="C:\\") returned 3
[...]
GetLogicalDrives () returned 0x4
```

Figure 7 - Drive and Volume Enumeration

Having obtained the list of potential data locations, a directory traversal process compares each directory and filename against a 'safe' list (Figure 8) to ensure that critical system files are not encrypted to allow the victim host to remain operational with internet access.

```
lstrcmpiW (lpString1="Boot", lpString2="ProgramData") returned -1
lstrcmpiW (lpString1="Boot", lpString2="All Users") returned 1
lstrcmpiW (lpString1="Boot", lpString2="autorun.inf") returned 1
lstrcmpiW (lpString1="Boot", lpString2="boot.ini") returned -1
```

Figure 8 - Directory/Filename 'Safe' List Comparison

Specifically, directories related to installed applications, the operating system and web browsers are excluded from the encryption process:

- \$Recycle.Bin, All Users, Google, Internet Explorer, Mozilla, Mozilla Firefox, Opera, Opera Software, ProgramData, Program Files (x86), Program Files, Tor Browser, Windows, Windows.old

In addition to the following core files also being excluded from the encryption process:

- autorun.inf, boot.ini, bootfont.bin, bootmgfw.efi, bootmgr, bootmgr.efi, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db

Once a file candidate for encryption is encountered, Babuk checks to confirm that it has not already been encrypted based on the appended file extension of `.__NIST_K571__` (v3) or `.babyk` (v4). Additionally, any existing ransom note named `How To Restore Your Files.txt` is also skipped.

Subsequently, assuming the file is to be encrypted, the Babuk file extension is appended and the file is opened ready to be overwritten with encrypted data (Figure 9).

```
MoveFileExW (lpExistingFileName="\\\\?\\C:\\EXAMPLE\\DOCUMENT.DOC" (normalized:
"c:\\EXAMPLE\\DOCUMENT.DOC"), lpNewFileName="\\\\?\\C:\\EXAMPLE\\DOCUMENT.DOC.babyk" (normalized:
"c:\\EXAMPLE\\DOCUMENT.DOC.babyk"), dwFlags=0x9) returned 1
CreateFileW (lpFileName="\\\\?\\C:\\EXAMPLE\\DOCUMENT.DOC.babyk" (normalized: "c:\\EXAMPLE\\DOCUMENT.
DOC.babyk"), dwDesiredAccess=0xc0000000, dwShareMode=0x1, lpSecurityAttributes=0x0,
dwCreationDisposition=0x3, dwFlagsAndAttributes=0x80, hTemplateFile=0x0) returned 0x2f8
```

Figure 9 - Babuk File Extension Append & Preparation

To ensure that the file can be overwritten without encountering errors due to it being in use by another process, and in addition to the earlier process and service termination, the Windows Restart Manager appears to be utilized (Figure 10).

```
RmStartSession () returned 0x0
RmRegisterResources () returned 0x0
RmGetList () returned 0x0
RmEndSession () returned 0x0
```

Figure 10 - Observed Windows Restart Manager Function Calls

The Windows Restart Manager was initially introduced to eliminate or reduce the number of restarts required during legitimate installations or updates and has seemingly been adopted by some ransomware threats for nefarious purposes. Specifically, the Restart Manager performs the following steps that provide obvious benefits to a malicious file manipulation process:

- **RmStartSession** - Starts the Restart Manager session;
- **RmRegisterResources** - Registers resources, in this case the targeted filename;
- **RmGetList** - Determine which processes or services are using the registered resource (file);
- **RmShutdown** - Shuts down any identified process or service using the registered resource;
- **RmRestart** - Restarts any identified process or service after the file modification;
- **RmEndSession** - Closes the Restart Manager session.

Utilizing the ChaCha8 stream cipher for encryption and Elliptic-curve Diffie-Hellman (ECDH) for key generation (Figure 11), the targeted file is encrypted and, in the absence of gaining access to the private key or paying the ransom to receive the decryption utility, decryption will likely be incredibly difficult.

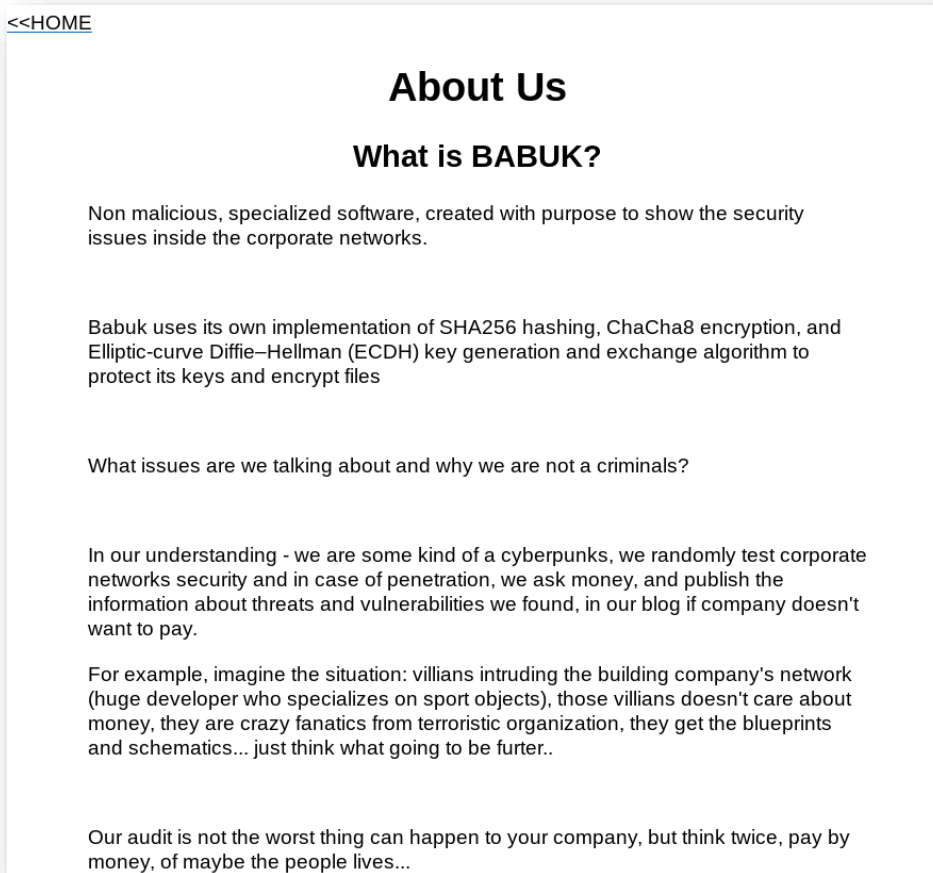


Figure 11 - Babuk 'About' Page

For reference, those interested in an expanded explanation of the Babuk encryption routine are encouraged to read the personal blog article authored by Chuong Dong [1], an independent security researcher, which details key generation, a 'mediocre' multithreading approach and the approach to files larger than 41MB which are reportedly split into three regions with only the first 10MB being encrypted.

Further complicating decryption efforts, Babuk v3 was reportedly observed in January 2021 as implementing a faulty public key generation routine that would prevent even the threat actor from successfully recovering data. This issue was since resolved in version 4, along with other subtle changes including the introduction of the **.babyk** file extension and a new mutual exclusion object (mutex) abusing the security researcher Chuong Dong.

Once files within a directory have been encrypted, a text file named **How To Restore Your Files.txt** is created (Figure 12) and contains the ransom note that is displayed at the conclusion of the ransomware process.

```
CreateFileW (lpFileName="\\\\?\\C:\\EXAMPLE\\How To Restore Your Files.txt" (normalized:
"c:\\EXAMPLE\\how to restore your files.txt"), dwDesiredAccess=0x40000000, dwShareMode=0x1,
lpSecurityAttributes=0x0, dwCreationDisposition=0x1, dwFlagsAndAttributes=0x0, hTemplateFile=0x0)
returned 0x328
WriteFile (in: hFile=0x328, lpBuffer=0x12d1888*, nNumberOfBytesToWrite=0x699,
lpNumberOfBytesWritten=0x14eab8, lpOverlapped=0x0 | out: lpBuffer=0x12d1888*,
lpNumberOfBytesWritten=0x14eab8*=0x699, lpOverlapped=0x0) returned 1
CloseHandle (hObject=0x328) returned 1
```

Figure 12 - Ransom Note Creation

Finally, the encryption key utilized by Babuk is saved to **%appdata%\ecdh_pub_k.bin** and will be required by the victim should they contact the threat actor to pay the ransom and obtain the decryption utility.

EXTORTION

Victims infected by Babuk will, on conclusion of the encryption phase, be presented with a text file containing the ransom note (Appendix B) that instructs them to contact the threat actor via a Tor hidden service (Figure 13) using a link that includes a unique victim identifier.

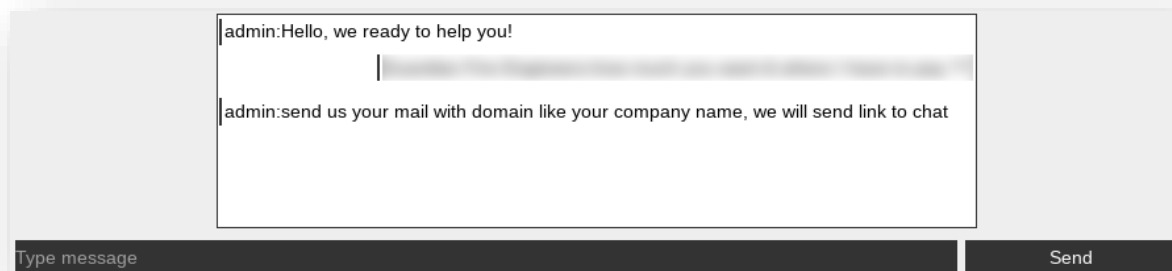


Figure 13 - Babuk Contact Site (Tor Hidden Service)

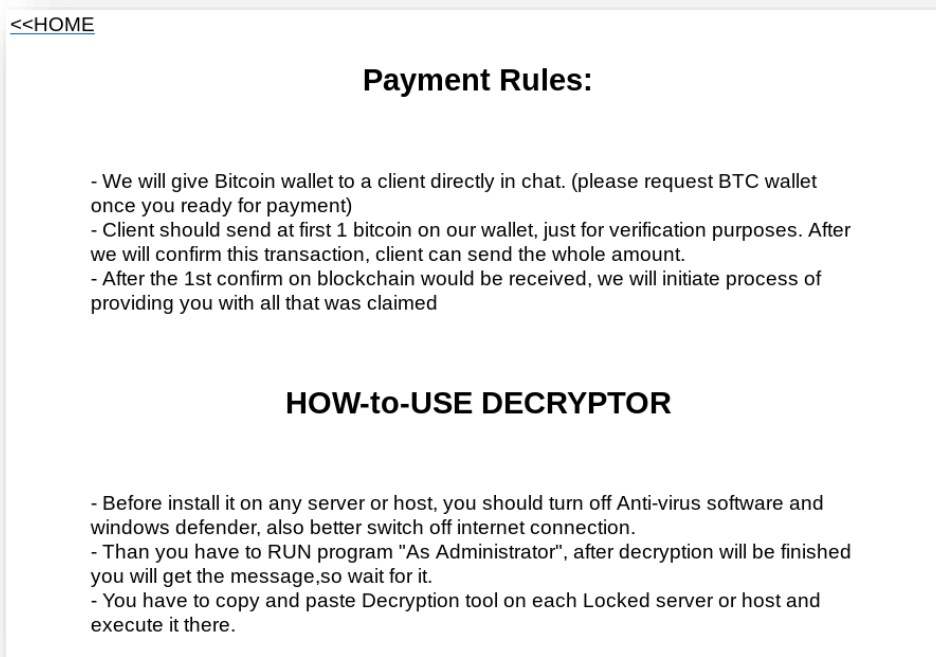
Based on observed interactions with previous victims, the threat actor may first seek to determine if the contact is a 'recovery company' and if the victim has ransomware insurance, likely in an attempt to extort a higher ransom payment if either of these is the case.

The victim, having responded to these initial questions, will likely then be prompted to share 4-5 encrypted files, of no more than 10MB in size, along with the corresponding `%appdata%\ecdh_pub_k.bin` file from an infected host. The threat actor will then decrypted these files as proof of their capabilities and presumably seek payment to decrypt the remaining data.

Those failing to contact the threat actor, or meet their demands, will likely in the first instance find themselves 'named and shamed' on the threat actor's leak site along with a deadline for compliance.

Failure to meet the threat actor's demands at this stage will, based on what has been observed thus far, result in the stolen data being leaked via this Tor hidden service.

As is to be expected in ransomware attacks of this nature, the threat actor requests that payment is made using Bitcoin and provides basic instructions for the use of their decryption utility (Figure 14).



The image shows a screenshot of a document with a white background and a thin blue border. At the top left, there is a link labeled '<<HOME'. The document is divided into two main sections. The first section is titled 'Payment Rules:' in bold black text. Below this title, there are three bullet points: '- We will give Bitcoin wallet to a client directly in chat. (please request BTC wallet once you ready for payment)', '- Client should send at first 1 bitcoin on our wallet, just for verification purposes. After we will confirm this transaction, client can send the whole amount.', and '- After the 1st confirm on blockchain would be received, we will initiate process of providing you with all that was claimed'. The second section is titled 'HOW-to-USE DECRYPTOR' in bold black text. Below this title, there are three bullet points: '- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.', '- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.', and '- You have to copy and paste Decryption tool on each Locked server or host and execute it there.'

Figure 14 - Babuk Payment Terms and Decryption Utility Instructions

Recommendations

- Business continuity and disaster recovery planning remain an important consideration when it comes to being prepared for ransomware worst-case scenarios.
- Ransomware threats of this nature often exploit known vulnerabilities, as such, robust patch management procedures should be enforced to ensure exposed infrastructure is secured.
- Employee security awareness training can help end-users identify suspicious communications and stop many common attack vectors.
- Practice least privilege to limit the impact of credential compromise and contain threats through segregation and limited access.
- Continuous monitoring of endpoint security events, and unusual behaviours such as excessive file operations, can provide an early indication of compromise.
- Given the data theft element of these ransomware campaigns, data sensitive data should be adequately secure, such as through the use of encryption or additional controls in accordance with any legal or regulatory requirements.
- Application permit and deny lists can detect and prevent the execution of unauthorized or unknown executables to harden operating systems against attack.
- Limiting access to administrative and system management tools, such as those abused by ransomware threats, can prevent misuse by threat actors.
- Network segregation, creating separate logical segments for assets that share a similar risk profile and limiting communications between them allows attacks to be contained and provides another layer of damage limitation.
- Wherever possible, organizations should seek to remediate a ransomware attack rather than making ransom payments which serve only to perpetuate the problem and fund threat developments.
- Consideration should be given to the use of an isolation approach, such as provided by Microsoft Defender Application Guard [2], to help protect users from untrusted Office documents and when browsing untrusted websites.

INDICATORS OF COMPROMISE

Whilst it Babuk payloads will likely differ between victims, the following observed indicators of compromise (IOC) may prove useful to defenders further investigating this threat.

URLS

- Contact site: `hxxp://babukq4e2p4wu4iq.onion/login.php?id=<VICTIM_IDENTIFIER>`
- Leak site: `hxxp://gtmx56k4hutn3ikv.onion`

VERSION 4

- `ef326291febe84d6b39d2e5cea7e99a02407892729d688c27dcc444a2ae0b544`
- `3dda3ee9164d6815a18a2c23651a53c35d52e3a5ad375001ec824cf532c202e6`

VERSION 3

- `1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02`
- `30fcff7add11ea6685a233c8ce1fc30abe67044630524a6eb363573a4a9f88b8`
- `550771bbf8a3e5625d6ec76d70ed86f6e443f07ce80ff73e47f8249ddd72a8cf`
- `8140004ff3cf4923c928708505754497e48d26d822a95d63bd2ed54e14f19766`
- `704a0fa7de19564bc743fb68aa0652e38bf86e8ab694bc079b15f945c85f4320`
- `8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9`
- `a f c f 2 6 5 a 1 d c d 9 e a b 5 a a b 2 7 0 d 4 8 a a 5 6 1 e 4 d d e b 7 1 c 0 5 e 3 2 c 8 5 7 d 3 b 8 0 9 b b 6 4 c 0 4 3 0`
- `c5167053129bd4a5542cfef9e739b0443e22e184cb4c0b57c049b448f030cf15`

MUTEX

- `babuk_v3`
- `DoYouWantToHaveSexWithCoungDong`

ENCRYPTED FILE EXTENSIONS

- `.__NIST_K571__`
- `.babyk`

DROPPED FILES

- `How To Restore Your Files.txt`
- `%appdata%\ecd_h_pub_k.bin`
- `DECR.TXT` (Early 'Vasa Locker' version)

MITRE ATT&CK

Technique	Tactic
T1001 - Data Obfuscation	Command & Control
T1005 - Data from Local System	Collection
T1007 - System Service Discovery	Discovery
T1012 - Query Registry	Discovery
T1018 - Remote System Discovery	Discovery
T1036 - Masquerading	Defense Evasion
T1055 - Process Injection	Defense Evasion, Privilege Escalation
T1055.012 - Process Injection: Process Hollowing	Defense Evasion, Privilege Escalation
T1057 - Process Discovery	Discovery
T1067 - Bootkit	Persistence
T1070.004 - File Deletion	Defense Evasion
T1081 - Credentials in Files	Credential Access
T1082 - System Information Discovery	Discovery
T1083 - File and Directory Discovery	Discovery
T1090 - Proxy	Command & Control
T1091 - Replication Through Removable Media	Initial Access, Lateral Movement
T1105 - Ingress Tool Transfer	Command & Control
T1107 - File Deletion	Defense Evasion
T1119 - Automated Collection	Collection
T1120 - Peripheral Device Discovery	Discovery
T1135 - Network Share Discovery	Discovery
T1143 - Hidden Window	Defense Evasion
T1486 - Data Encrypted for Impact	Impact
T1490 - Inhibit System Recovery	Impact
T1497 - Virtualization/Sandbox Evasion	Defense Evasion, Discovery
T1518.001 - Security Software Discovery	Discovery
T1547.001 - Registry Run Keys / Startup Folder	Persistence, Privilege Escalation

APPENDIX A - PROCESS/SERVICE TERMINATION

Processes and services associated with the following application, data backup and endpoint security names are terminated by Babuk during its execution along with any service containing the string `svc$`:

APPLICATIONS

- Intuit QuickBooks: `Intuit.QuickBooks.FCS`, `QBFCMonitorService`, `QBFCService`, `QBIDPService`
- Microsoft Office: `excel.exe`, `infopath.exe`, `msaccess.exe`, `mspub.exe`, `onenote.exe`, `outlook.exe`, `powerpnt.exe`, `visio.exe`, `winword.exe`
- Microsoft Windows: `notepad.exe`, `wordpad.exe`
- Mozilla Firefox: `firefox.exe`
- Mozilla Thunderbird: `tbirdconfig.exe`, `thunderbird.exe`
- Ritlabs The Bat!: `thebat.exe`
- Valve Steam: `steam.exe`

BACKUP SOFTWARE

- Acronis: `AcronisAgent`, `AcrSch2Svc`
- Arcserve: `CAARCUUpdateSvc`, `CASAD2DWebSvc`
- Commvault: `GxBldr`, `GxCIMgr`, `GxCVD`, `GxFWD`, `GxVss`
- IBM vSnap: `VSnap`
- Microsoft Volume Shadow Copy Service: `vss`, `VSSProvider`
- Redgate SQL Backup: `sqbcoreservice.exe`
- STC Raw Backup Agent: `stc_raw_agent`
- Veeam: `veeam`, `VeeamDeploymentService`, `VeeamNFSSvc`, `VeeamTransportSvc`
- Veritas: `BackupExecAgentAccelerator`, `BackupExecAgentBrowser`, `BackupExecDiveciMediaService`, `BackupExecJobEngine`, `BackupExecManagementService`, `BackupExecRPCService`, `BackupExecVSSProvider`, `PDFSService`
- YooBackup: `YooBackup`, `YooIT`

ENDPOINT SECURITY

- 360 Safe Guard: `zhudongfangyu`
- Norton/Symantec Antivirus: `ccEvtMgr`, `ccSetMgr`, `DefWatch`, `RTVscan`, `SavRoam`
- Panda Security (or NTI BackUp): `agntsvc.exe`
- Sophos: `sophos`

SERVERS

- Citrix MetaFrame: `encsvc.exe`
- MailEnable: `mementas`, `mepocs`
- Microsoft SQL Server: `sqlsvc`, `sql.exe`
- Oracle: `isqlplussvc.exe`, `mydesktopqos.exe`, `mydesktopservice.exe`, `ocautoupds.exe`, `ocomm.exe`, `oracle.exe`, `ocssd.exe`, `dbnmp.exe`, `synctime.exe`, `xfssvcon.exe`
- Sybase SQL Anywhere: `dbeng50.exe`

APPENDIX B - RANSOM NOTE EXAMPLES

VERSION 3

```
1. ----- [ Hello, <VICTIM_ORGANIZATION> ] ----->
2.
3.      ****BY BABUK LOCKER****
4.
5.
6.
7. What happend?
8. -----
9. 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.
10. But you can restore everything by purchasing a special program from us -
    a universal decoder. This program will restore your entire network.
11. Follow our instructions below and you will recover all your data.
12. 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.
13.
14. What guarantees?
15. -----
16. We value our reputation. If we do not do our work and liabilities,
    nobody will pay us. This is not in our interests.
17. All our decryption software is perfectly tested and will decrypt your
    data. We will also provide support in case of problems.
18. We guarantee to decrypt one file for free. Go to the site and contact
    us.
19.
20. What information compromised?
21. -----
22. We copied more than <STOLEN_DATA_VOLUME> from your internal network,
    here are some proofs, for additional confirmations, please chat with us
23. In cases of ignoring us, the information will be released to the public.
24. <IMGUR_IMAGE_LINKS>
25.
26. How to contact us?
27. -----
28. Using TOR Browser ( hxxps://www.torproject.org/download/ ):
29. hxxp://babukq4e2p4wu4iq.onion/login.php?id=<VICTIM_IDENTIFIER>
30.
31.
32. !!! DANGER !!!
33. DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able
    to RESTORE them.
34. !!! DANGER !!
```

VERSION 4

```
1. ##### [ babyk ransomware ] #####
2.
3. * What happend?
4. -----
5. Your computers and servers are encrypted, backups are deleted from your
   network and copied.
6. We use strong encryption algorithms, so you cannot decrypt your data
   without us.
7. But you can restore everything by purchasing a special program from us - a
   universal decoder.
8. This program will restore your entire network. Follow our instructions
   below and you will recover all your data.
9. If you continue to ignore this for a long time, we will start reporting
   the hack to mainstream media and posting
10. your data to the dark web.
11.
12.
13. * What guarantees?
14. -----
15. We value our reputation. If we do not do our work and liabilities,
   nobody will pay us. This is not in our interests.
16. All our decryption software is perfectly tested and will decrypt your
   data. We will also provide support in case of problems.
17. We guarantee to decrypt one file for free. Go to the site and contact
   us.
18.
19.
20. * What information compromised?
21. -----
22. We copied many data from your internal network,
23. here are some proofs (private link):
   http://gtmx56k4hutn3ikv.onion/?<VICTIM_IDENTIFIER>
24.
25. For additional confirmations, please chat with us/
26. In cases of ignoring us, the information will be released to the public
   in blog http://gtmx56k4hutn3ikv.onion/
27.
28.
29. * How to contact us?
30. -----
31. 1) Download for browser: https://www.torproject.org/download/
32. 2) Open it
33. 3) Follow this link in tor browser:
   http://babukq4e2p4wu4iq.onion/login.php?id=<VICTIM_IDENTIFIER>
```

REFERENCES

- <http://chuongdong.com/reverse-engineering/2021/01/03/BabukRansomware/>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview>