cybersecurity
associates

Babuk Locker Ransomware

Threat Hunting Report

Dated: 8th January 2021

By Zachary Goggins

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

Babuk Locker Ransomware

Threat Hunting Report

Executive Summary

The purpose of this report is to document the current form and methodologies used by the Babuk Locker Ransomware. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the lifecycle of the Babuk Locker Ransomware and how it operates, with supporting evidence and recommendations to mitigate the emerging threat. The report also includes a list of identified indicators of compromise and references where the information within this report was identified from.

Summary

At the start of 2021, a new ransomware strain called Babuk Locker was launched that targets corporate victims. It has amassed a small list of victims and they range from a medical testing products manufacturer to an air conditioning and heating company. It is not yet clear on whether a specific industry is being targeted but one of the victims have agreed to pay a ransom fee at $85,000. The data which will be published online if a ransom is not paid and instead of publishing the stolen data on their own dedicated leak site, it is instead posted on a hacking forum.

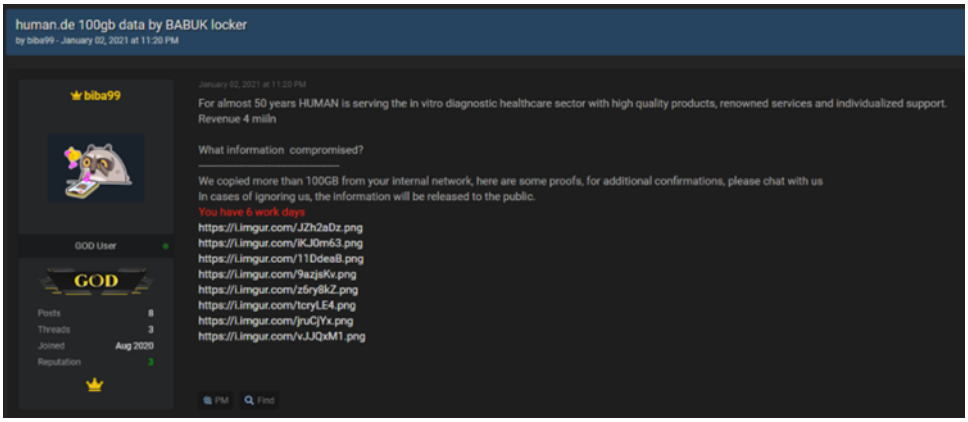


Figure 1: RaidForums Babuk Leak

Babuk will utilize multi-threading encryption and the Windows Restart Manager, which is similar to Conti and REvil. It will also search for shadow copies and other backup files to delete them from the infected device, this is similar to Ryuk. Researcher Chuong Dong points out that 'Babuk is not obfuscated at all, and it's a pretty standard ransomware', however attackers have found success with Babuk's use of the Elliptic-curve Diffie-Hellman algorithm. The ransomware group are using one private key for each sample and has so far copromised several victims.

Elliptic-curve Diffie-Hellman Algorithm

ECDH is a key agreement protocol that allows two parties that each have an elliptic-curve public/private key pair, to establish a shared secret.

The shared secret can be directly used as a key, or to retrieve another key. Either Key can then be used to encrypt communications by using a symmetric-key cipher.

This is a variant of the Diffie-Hellman protocol that uses elliptic-curve cryptography.

Tactics, Techniques, Procedures

Tactics, Techniques, and Procedures (TTP) describes an approach of analysing an APT's operation or can be used as means of profiling a certain threat actor.

Tactics is meant to outline the way an adversary chooses to carry out his attack from the beginning till the end. Technological approach of achieving intermediate results during the campaign is described by Techniques the attacker uses. Lastly, the organizational approach of the attack is defined by procedures which are used by the threat actor.

In order to understand and fight the enemy one has to understand the Tactics, Techniques and Procedures (TTP) the attacker uses. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages. Identifying the Techniques used during an attack allows to identify an organisation's blind spots and implement countermeasures in advance. Finally, the analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

TTPs that are described within this research are based of the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.

Phase 1: Initial Access: Phishing

Researchers have pointed out that the ransomware will arrive in the form of a 32-bit .EXE file that lacks obfuscation, however it is not yet clear on how Babuk reaches its victims. One researcher Dong reports that it likely arrives on systems through phishing campaigns, which is similar to other ransomware groups. The malicious actors use one private key for each Babuk sample, meaning that they mainly target large corporations. The executables that have been analysed by researchers show that each executable is specifically customised for each victim. This includes a hardcoded extension; a ransom note and a Tor victim URL.

Phase 2: Persistence: Kill Processes and Services

Processes:

Once the target has been infected, Babuk contains a hard-coded list of processes and services to be closed before encryption begins. Babuk looks to close 31 processes and these can be found in the Indicators of Compromise section. The ransomware looks to examine all of the processes that run of the system by using calls to CreateToolhelp32Snapshot, Process32firstW and Process32NextW, it can then loop through and look for processes that need to be closed. Once these processes have been found, Babuk will call TerminateProcess to terminate it.

Services:

Before a service is terminated, Babuk will call EnumDependentServicesA, this retrieves the name and status of each service that depends on a specified service. The ransomware then calls ControlService and uses the control code SERVICE_CONTROL_STOP, this stops the retrieved services before terminating the main service. The system-monitoring services that are shutdown include BackupExecVSSProvider, YooBackup and BackupExecDiveciMediaService.

A list of closed processes and services can be found in the Indicators of Compromise section.

Cyber Kill-Chain

The cyber kill chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

Phase 3: Lateral Movement: Delete and Encrypt

Babuk uses techniques like multi-threading encryption, which is similar to Conti, and it also abuses the Windows Restart Manager which is similar to REvil. This terminates any process that is using files and ensures that nothing prevents Babuk from opening and encrypting data. To achieve this, calls are made through RmStartSession, RmRegisterResources and RmGetList to retrieve a list of processes that are using a specified file. According to Dong, Babuk will look to call TerminateProcess if the process is not a critical process or explorer.exe.

Before and after encryption occurs, Babuk will attempt to delete shadow copies of files. In order to disable file system redirection, it will call Wow64DisableWow64FsRedirection, then ShellExecuteW is called so that the following command can be executed: cmd.exe /c vssadmin.exe delete shadows /all /quiet. Once the shadow copies have been deleted, the ransomware will check if the system is running under a 64-bit processor. If this is the case, then Wow64RevertWow64FsRedirection is called, this will enable file system redirection again.

For encryption, Babuk uses two ChaCha8 keys which are generated from 4 random buffers. These buffers are generated from RtlGenRandom. The file encryption comprises two different types: small file encryption and large file encryption. At around 41MB, small files are mapped entirely and encrypted with ChaCha8 two times. The process is different for large files, as they are first divided into three large regions and only the first 10MB of each region is encrypted.

The second ChaCha8 key gets encrypted by the first key, the encrypted second key is then used to encrypt the first key. The encrypted first key is treated as the ECDH private key for the local machine. After this, a local ECDH public key is generated from the private key, which then generates a shared secret by using the local private key and the author's public key which is hard coded. To decrypt files, the local public key is stored in the APPDATA folder under the file ecdh_pub_k.bin. The ECDH's mechanism allows the ransomware author to generate a shared secret from their own private key and the victim's public key, which is used for file decryption.

A recursion method is used in order to traverse and encrypt files. Calls are made to FindFirstFileW and FindNextFileW, this will look for files and sub-directories in each directory. After a directory has been encountered, calls are made recursively to the function: main_encrypt. It is possible that Babuk may not encrypt every single folder in the drive to save time, as it only goes down 16 layers deep. Once a file has been encountered, it will check for the file name 'How To Restore Your Files.txt' or if the file extension is '__NIST_K571__', so that that the ransomware will avoid encrypting the ransom note or encrypted files.

On the victim machine, to encrypt remote drives Babuk will call WNetGetConnectionW. This retrieves the names of network resources that are associated with those drives and then pass them to the encrypting thread. If the

correct parameters are given on the machine's LAN, it will also encrypt network shares. Using the aforementioned method, a call is made to WNetOpenEnumW to traverse through remote folders on the network and encrypt files. This is how Babuk spreads across the network.

Conclusion

Overall, Babuk is a new strain of ransomware that started at the beginning of 2021and this arrives as ransomware attacks continue to rise, with a 350% increase since 2018. It has a very strong encryption scheme, and it utilizes the Elliptic-curve Diffie-Hellman algorithm which has proven effective in attacking companies. This complex encryption scheme is to ensure that the victim cannot recover their files, but the attacker can easily generate the shared secret that is needed for decryption.

Advice

The IOC's identified within this report are monitored by our SIEM solution, BorderPoint, if a host were to demonstrate any of the characteristics CSA would ensure to alarm you. It is imperative that there is a backup strategy in place that is tested and that it also covers worst-case scenarios. CSA recommends:

- Regular Backups must be kept offline; this is the only way to protect against a determined threat actor.
- Regularly test backups for their integrity and if they can be recovered. Scan backups for registry persistence.
- Critical data should be written on WORMs (Write Once Read Many). This write protection ensures that the data cannot be tampered with once it is written to the device.
- Disable all macros, except those that are digitally signed.
- Implement filters at the email gateway. Filter out emails with known malspam indicators and block suspicious IP addresses at the firewall.
- Educate and train employees on social engineering and phishing. (this is a common infection method for malware and ransomware, training employees in this area can reduce the risk of a compromise though emails).
- Adhere to the Principle of Least Privilege (PLP), ensure that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated admins.
- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- If there is not a policy regarding suspicious emails, consider creating one and specify that all suspicious emails should be reported to the security and/or IT departments. Using CSA's tool AppGuard will prevent interaction with the system space.

Indicators of Compromise

Domain Names:

Http[:]//babukq4e2p4wu4iq[.]onion/login[.]php?

Services:

This is a list of services to be closed:

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, PDVFSService, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUpdateSvc

Processes:

This is a list of processes to be closed:

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, sqbcoreservice.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

Hashes:

MD5:

- E10713A4A5F635767DCD54D609BED977
- DD7F88A68A76ACC0BE9EB0515D54A82A
- E25E078255B56B47897AC96A7842DE92

SHA1:

- 320D799BEEF673A98481757B2FF7E3463CE67916
- CA205A28B8DBD74C60FDEAF522804D5A2A45DD0B
- 21FEBFB36DA69C8A611A9EAEE5CC826CFD5684D7

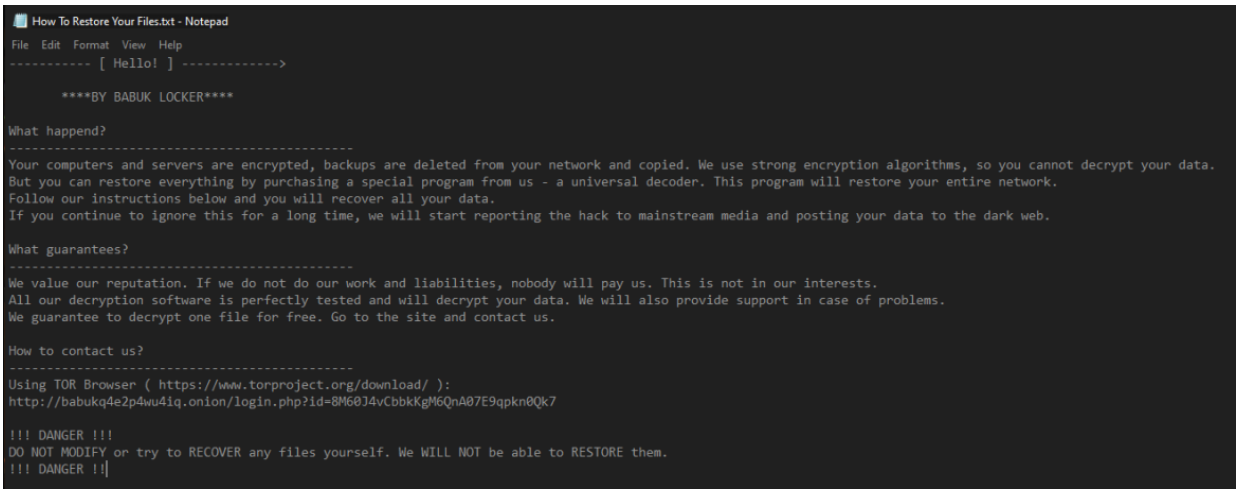
SHA256:

- 8203C2F00ECD3AE960CB3247A7D7BFB35E55C38939607C85DBDB5C92F0495FA9
- 1B9412CA5E9DEB29AEAA37BE05AE8D0A8A636C12FDFF8C17032AA017F6075C02

- 30FCFF7ADD11EA6685A233C8CE1FC30ABE67044630524A6EB363573A4A9F88B8

Ransom Note:

- How To Restore Your Files.txt



Hardcoded Extension (Appended to each encrypted file):

- __NIST_K571__

Commands:

- -lanfirst (Same as no parameter given, encrypts locally)
- -lansecond (Encrypting network shares after encrypting locally)
- -nolan (Same as no parameter given, encrypts locally)
- cmd.exe /c vssadmin.exe delete shadows /all /quiet

References

- https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/?&web_view=true
- https://threatpost.com/ransomware-babuk-locker-large-corporations/162836/?utm_source=dlvr.it&utm_medium=linkedin
- https://siliconangle.com/2021/01/05/babuk-locker-emerges-first-new-form-ransomware-2021/
- http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/
- https://www.securityweek.com/researchers-warn-new-ransomware-targeting-enterprise-networks
- https://sensorstechforum.com/babuk-locker-2021-ransomware/
- https://theopensecurity.com/forum/thread/1207-new-year-new-ransomware-babuk-locker-targets-large-corporations/#
- https://www.pcrisk.com/internet-threat-news/19813-babuk-ransomware-makes-new-year-entrance
- https://cisomag.eccouncil.org/new-year-brings-new-ransomware-strain-babuk-locker/
- https://gbhackers.com/babuk-locker-emerges-as-new-enterprise-ransomware-of-2021/