SUBEX

Babuk Ransomware

Date: **20/04/2020**

Shyava Tripathi

Babuk, the first enterprise ransomware variant of 2021, contrived by TrendMicro in January, has resuscitated and is targeting and entrapping organizations with its Look-Lock-Leak extortion campaign. With a beefed-up fancy website, elaborate ransom notes & a reputation-building PR campaign, the threat actors behind Babuk are employing new tacks in the hope that it will persuade more victims to pay the ransom.

A public relations campaign on Babuk's recently refashioned website rolled out the news that the threat actors were back with an improved & repaired version of their decryptor tool.

▪ DEVELOPMENTS IN BABUK'S WEBSITE

The ransom note dropped by the latest variant of Babuk contains two onion links; one of them is used as Babuk's public blog, while the other is used to guide the victims about ransom amounts, payments & the file recovery process.

- hxxp://wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd.onion/
- hxxp://tsu2dpiiv4zjzfyq73eibemit2qyrimbbb6lhpm6n5ihgallom5lhdyd.onion/<ID>

- Babuk's Public Blog

The new blog website rebrands the ransomware as 'Babuk' instead of 'Babyk (Figure 1)'.

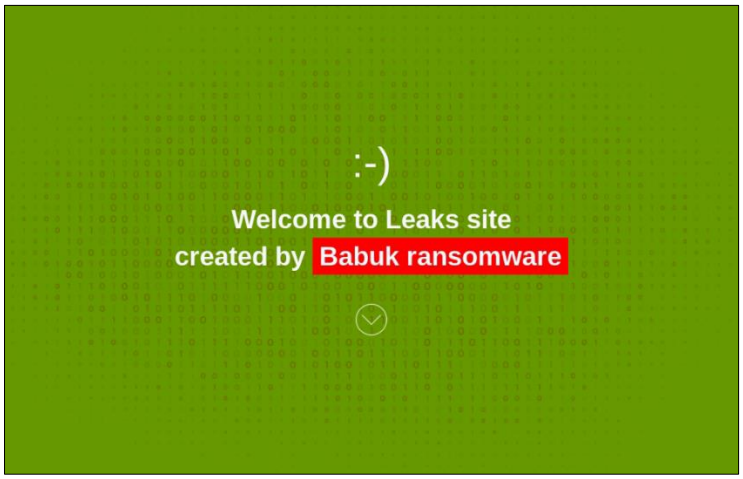


Figure 1: 'Babyk' rebranded to 'Babuk'

The previous version of the website stated that the group does not 'audit' non-profit/charitable foundations except the ones supporting LGBT & Black Lives Matter causes, however, the group seems to have dropped these bigoted views as the vamped-up website now reads no exceptions on non-profit charitable organizations (Figure 2).

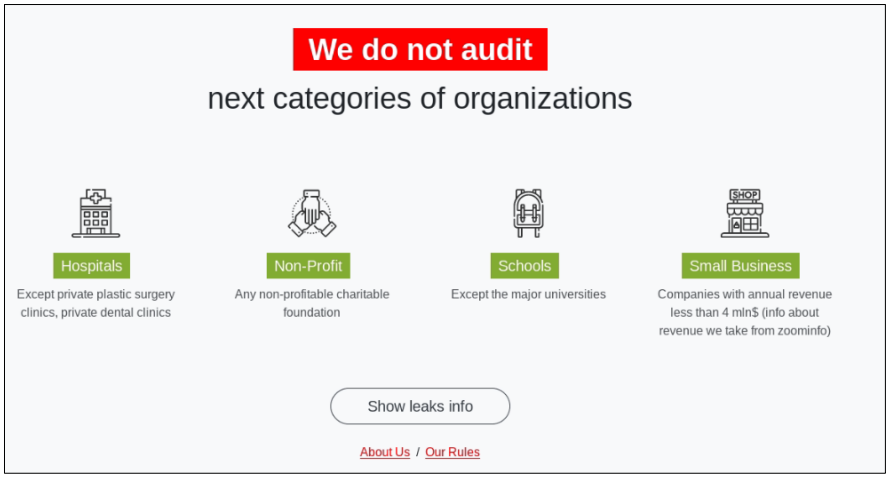
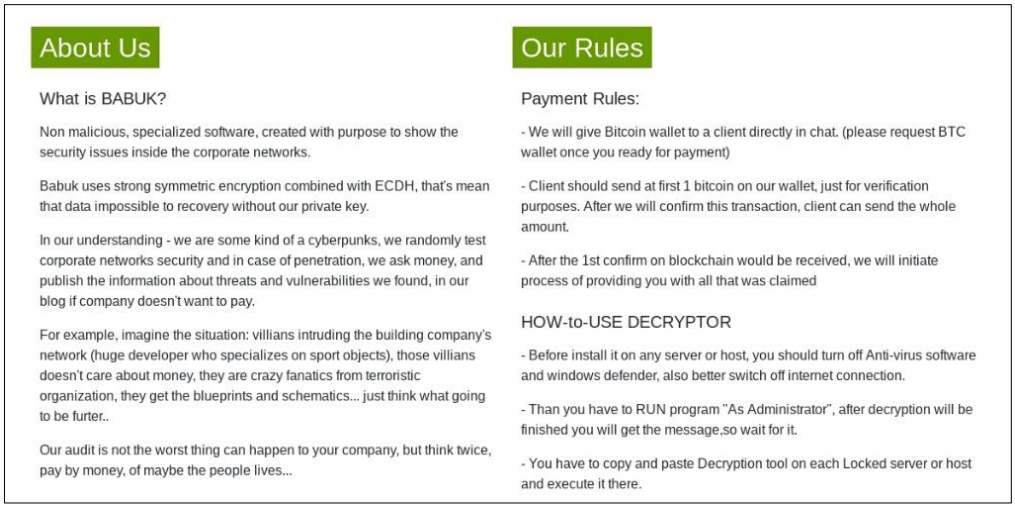


Figure 2: Exceptions of targeting NGOs supporting BLM & LGBT removed

Even though the encryption routine in the latest encountered Babuk sample is the same as the version 4 variants seen before, the details about the encryption & hashing algorithm utilised by the ransomware (mentioned as a custom SHA256 & ChaCha8 in the previous versions of the website) have also been stripped off to conceal the workflow of the encryption (Figure 3). The note now only discloses that strong symmetric encryption combined with ECDH is milked by the malware which makes data recovery impossible without the attacker's private key.



About Us

What is BABUK?

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

Babuk uses strong symmetric encryption combined with ECDH, that's mean that data impossible to recovery without our private key.

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

For example, imagine the situation: villians intruding the building company's network (huge developer who specializes on sport objects), those villians doesn't care about money, they are crazy fanatics from terroristic organization, they get the blueprints and schematics... just think what going to be furter..

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

Our Rules

Payment Rules:

- 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.

- After the 1st confirm on blockchain would be received, we will initiate process of providing you with all that was claimed

HOW-to-USE DECRYPTOR

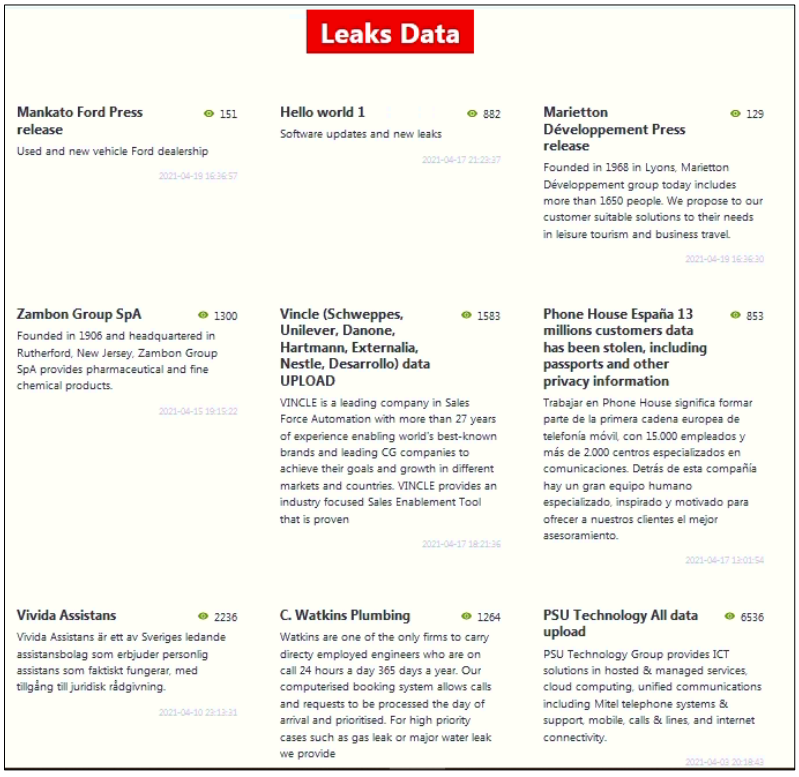
- Before install it on any server or host, you should turn off Anti-virus software and windows defender, also better switch off internet connection.

- Than you have to RUN program "As Administrator", after decryption will be finished you will get the message,so wait for it.

- You have to copy and paste Decryption tool on each Locked server or host and execute it there.

Figure 3: Encryption & Hashing details stripped from the note

The site also lists the recent organizations entrapped by Babuk and contains images of identifiable data collected from the organizations to establish the legitimacy of claims. The 'Leaks data' list has been updated multiple times in the past week with organizations operating in diverse sectors of healthcare, digital services, tourism, mechanical technology & business technology (Figure 4).



Leaks Data

Mankato Ford Press release — 151

Used and new vehicle Ford dealership

2021-04-19 16:36:57

Hello world 1 — 882

Software updates and new leaks

2021-04-17 21:23:37

Marietton Développement Press release — 129

Founded in 1968 in Lyons, Marietton Développement group today includes more than 1650 people. We propose to our customer suitable solutions to their needs in leisure tourism and business travel.

2021-04-19 16:36:30

Zambon Group SpA — 1300

Founded in 1906 and headquartered in Rutherford, New Jersey, Zambon Group SpA provides pharmaceutical and fine chemical products.

2021-04-15 19:15:22

Vincle (Schweppes, Unilever, Danone, Hartmann, Externalia, Nestle, Desarrollo) data UPLOAD — 1583

VINCLE is a leading company in Sales Force Automation with more than 27 years of experience enabling world's best-known brands and leading CG companies to achieve their goals and growth in different markets and countries. VINCLE provides an industry focused Sales Enablement Tool that is proven

2021-04-17 18:21:36

Phone House España 13 millions customers data has been stolen, including passports and other privacy information — 853

Trabajar en Phone House significa formar parte de la primera cadena europea de telefonía móvil, con 15.000 empleados y más de 2.000 centros especializados en comunicaciones. Detrás de esta compañía hay un gran equipo humano especializado, inspirado y motivado para ofrecer a nuestros clientes el mejor asesoramiento.

2021-04-17 13:01:54

Vivida Assistans — 2236

Vivida Assistans är ett av Sveriges ledande assistansbolag som erbjuder personlig assistans som faktiskt fungerar, med tillgång till juridisk rådgivning.

2021-04-10 23:12:31

C. Watkins Plumbing — 1264

Watkins are one of the only firms to carry directy employed engineers who are on call 24 hours a day 365 days a year. Our computerised booking system allows calls and requests to be processed the day of arrival and prioritised. For high priority cases such as gas leak or major water leak we provide

PSU Technology All data upload — 6536

PSU Technology Group provides ICT solutions in hosted & managed services, cloud computing, unified communications including Mitel telephone systems & support, mobile, calls & lines, and internet connectivity.

2021-04-03 20:18:43

Figure 4: Data leaks & information of entrapped organizations

Interestingly, the threat actors have also launched a public relations campaign on Saturday (April 17th) under the title of 'Hello world 1 - Software updates & new leaks'. The note is addressed to journalists & announced that the bug found in the Babuk's decryptor had been mitigated & their tool improved (Figure 5). The group publicized their Serco data breach and claims to have received ransom from the company for procurement of their data. They also claim to have entrapped the Zambon pharmaceutical group, having acquired 10TBs of their data, however, the organization has not confirmed that it has lost any data. Following rules & making anonymous payments are some recommendations made by the threat actors to prevent data leakage.

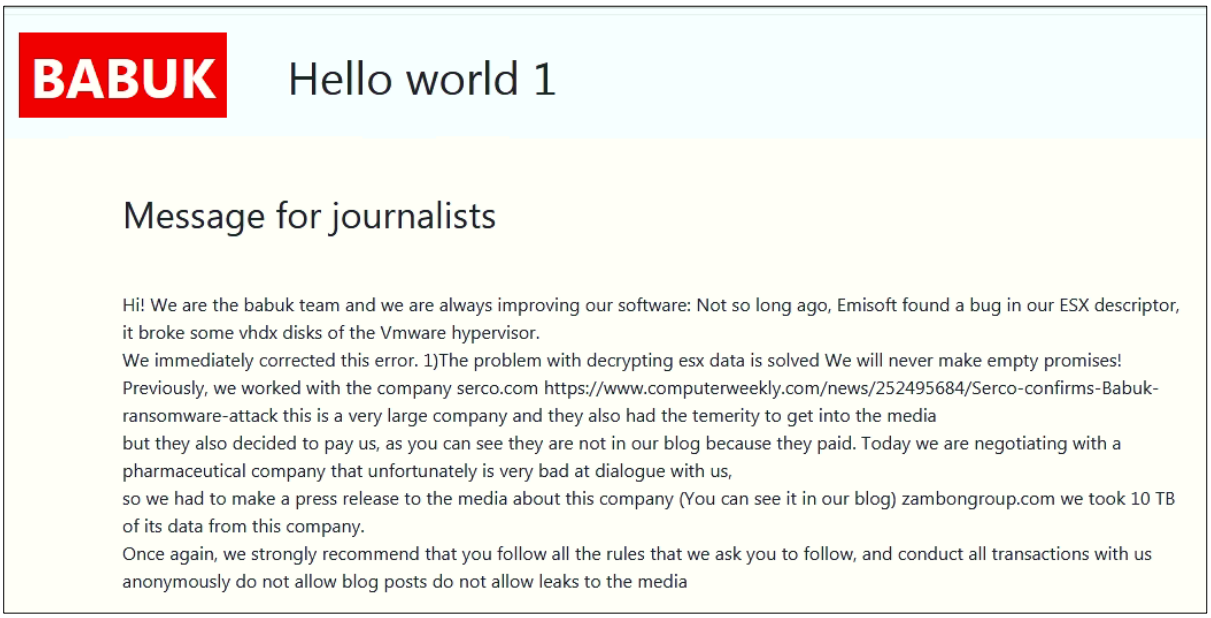


Figure 5: 'Hello World 1' note addressed to journalists

- Babuk's File Encryption/Recovery Website

The file recovery website, when opened, announces the message 'Your network has been encrypted by Babuk Ransomware' (Figure 6). Upon scrolling further, the victim is notified about the infection, the encryption of their sensitive files & the ransom amount one needs to pay to procure their leaked data. In our simulated environment, the ransom demanded was 6000000 USD or 106.27416 BTC (Figure 7).

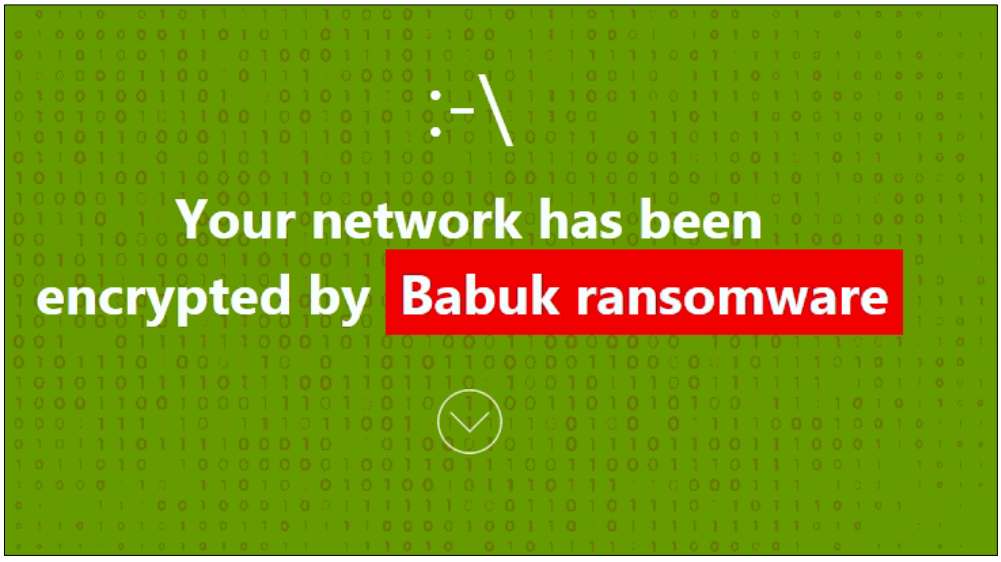


Figure 6: Landing page of Encryption/Recovery website

Figure 7: Infection details & ransom demands

More details about creating a bitcoin wallet, buying the necessary amount of bitcoins for the ransom, and obtaining the decryptor can be found on the website (Figure 8). Chat support has also been added to the website which can be used by the victims to obtain the attacker's bitcoin wallet details as well as getting a single file decrypted for free. The chat support contains some template messages that can be seen upon opening the support chat link (Figure 9).

Figure 8: Bitcoin wallet & Bitcoin procurement details

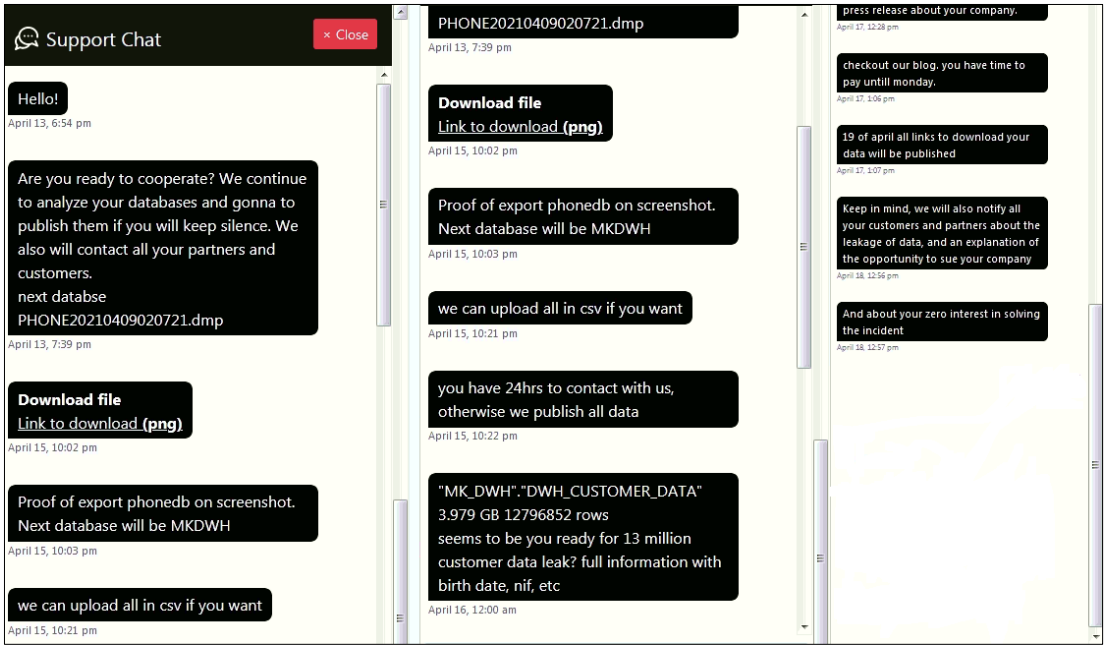


Figure 9: Chat Support available on Babuk's website

▪ TECHNICAL OVERVIEW

The latest variant of Babuk Ransomware collected by Subex Secure's honeypot is analysed below.

- PE File Overview

The malware is a 32-bit executable file and is not obfuscated by any packer.

MD5	b8e5bd86046b596d8cf43843f433bb5d
SHA – 256	bb31f235e86b0fda185e6580ef5327f80d6a6c754f78499e8647de5e229769cc
Size	79.00 KB (80896 bytes)
File Type	Win32 EXE
Architecture	Intel 80386 32-bit
Creation Time	2021-03-23 19:22:40

- Capabilities

1. Terminates Backup Programs, Database Utilities & Security Softwares

As is often the case with typical ransomware, Babuk enumerates the list & status of currently running processes & services. It then matches them against a hardcoded list of common applications, backup programs, database utilities & endpoint security solutions (Table 1). If found, the services are terminated using the "QueryServiceStatusEx," "OpenServiceA," "EnumDependentServicesA,", "CloseServiceHandle" & "GetLastError" are used (Figure 10). Processes are enumerated, matched & terminated using "CreateToolhelp32Snapshot," "lstrcmpw", "OpenProcess, "TerminateProcess." & "CloseHandle" (Figure 11).

```
.text:004047C0 loc_4047C0:                             ; CODE XREF: sub_404770+45↑j
.text:004047C0                 cmp     [ebp+var_10], 2Ch ; ','
.text:004047C4                 jnb     loc_404999
.text:004047CA                 push    2Ch ; ','       ; dwDesiredAccess
.text:004047CC                 mov     ecx, [ebp+var_10]
.text:004047CF                 mov     edx, lpServiceName[ecx*4]
.text:004047D6                 push    edx             ; lpServiceName
.text:004047D7                 mov     eax, [ebp+hSCManager]
.text:004047DA                 push    eax             ; hSCManager
.text:004047DB                 call    ds:OpenServiceA
.text:004047E1                 mov     [ebp+hService], eax
.text:004047E4                 cmp     [ebp+hService], 0
.text:004047E8                 jz      loc_404994
.text:004047EE                 lea     ecx, [ebp+pcbBytesNeeded]
.text:004047F1                 push    ecx             ; pcbBytesNeeded
.text:004047F2                 push    24h ; '$'       ; cbBufSize
.text:004047F4                 lea     edx, [ebp+Buffer]
.text:004047F7                 push    edx             ; lpBuffer
.text:004047F8                 push    0               ; InfoLevel
.text:004047FA                 mov     eax, [ebp+hService]
.text:004047FD                 push    eax             ; hService
.text:004047FE                 call    ds:QueryServiceStatusEx
.text:00404804                 test    eax, eax
.text:00404806                 jz      loc_40498A
.text:0040480C                 cmp     [ebp+var_44], 1
.text:00404810                 jz      loc_40498A
.text:00404816                 cmp     [ebp+var_44]
.text:0040481A                 jz      loc_40498A
.text:00404820                 lea     ecx, [ebp+Se
.text:00404823                 push    ecx
.text:00404824                 lea     edx, [ebp+pcl
.text:00404827                 push    edx
.text:00404828                 push    0
.text:0040482A                 mov     eax, [ebp+lp
.text:0040482D                 push    eax
.text:0040482E                 push    1
.text:00404830                 mov     ecx, [ebp+hService]
.text:00404833                 push    ecx             ; hService
.text:00404834                 call    ds:EnumDependentServicesA
.text:0040483A                 test    eax, eax
.text:0040483C                 jnz     loc_40492C
.text:00404842                 call    ds:GetLastError

; ---------------------------------------------------------------------------

loc_40498A:                                            ; CODE XREF: sub_404770+96↑j
                                                       ; sub_404770+A0↑j ...
                        mov     eax, [ebp+hService]
                        push    eax             ; hSCObject
                        call    ds:CloseServiceHandle

loc_404994:                                            ; CODE XREF: sub_404770+78↑j
                        jmp     loc_4047B7
```

Figure 10: Backup, Security Endpoint & Server Services Terminated

```
.text:004049FE loc_4049FE:                             ; CODE XREF: sub_4049B0+43↑j
.text:004049FE                 cmp     [ebp+var_4], 1Fh
.text:00404A02                 jnb     short loc_404A54
.text:00404A04                 lea     eax, [ebp+pe.szExeFile]
.text:00404A0A                 push    eax             ; lpString2
.text:00404A0B                 mov     ecx, [ebp+var_4]
.text:00404A0E                 mov     edx, lpString1[ecx*4]
.text:00404A15                 push    edx             ; lpString1
.text:00404A16                 call    ds:lstrcmpW
.text:00404A1C                 test    eax, eax
.text:00404A1E                 jnz     short loc_404A52
.text:00404A20                 mov     eax, [ebp+pe.th32ProcessID]
.text:00404A26                 push    eax             ; dwProcessId
.text:00404A27                 push    0               ; bInheritHandle
.text:00404A29                 push    1               ; dwDesiredAccess
.text:00404A2B                 call    ds:OpenProcess
.text:00404A31                 mov     [ebp+hProcess], eax
.text:00404A34                 cmp     [ebp+hProcess], 0
.text:00404A38                 jz      short loc_404A50
.text:00404A3A                 push    9               ; uExitCode
.text:00404A3C                 mov     ecx, [ebp+hProcess]
.text:00404A3F                 push    ecx             ; hProcess
.text:00404A40                 call    ds:TerminateProcess
.text:00404A46                 mov     edx, [ebp+hProcess]
.text:00404A49                 push    edx             ; hObject
.text:00404A4A                 call    ds:CloseHandle
.text:00404A50
.text:00404A50 loc_404A50:                             ; CODE XREF: sub_4049B0+88↑j
.text:00404A50                 jmp     short loc_404A54
```

Figure 11: Backup, Security Endpoint & Server Processes Terminated

2. Mutex Creation

A mutual exclusion object is created by the ransomware to check if an instance of the malware has been executed before (Figure 12).

Mutex Value: 'DoYouWantToHaveSexWithCuongDong'

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
1	9:58:27.620 PM	2	SETUPAPI.dll	CreateMutexW (NULL, FALSE, NULL)	0x000001d4		0.0000035
2	9:58:27.620 PM	2	SETUPAPI.dll	CreateMutexW (NULL, FALSE, NULL)	0x000001dc		0.0000023
3	9:58:27.636 PM	1	urlmon.dll	CreateMutexA (NULL, FALSE, "Local\ZonesCounterMutex")	0x0000024c		0.0000079
4	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x0000024c)	TRUE		0.0000015
5	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x0000024c)	TRUE		0.0000015
6	9:58:27.636 PM	1	urlmon.dll	CreateMutexA (NULL, FALSE, "Local\ZoneAttributeCacheCounterMutex")	0x0000026c		0.0000082
7	9:58:27.636 PM	1	urlmon.dll	CreateMutexA (NULL, FALSE, "Local\ZonesCacheCounterMutex")	0x00000280		0.0000056
8	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x0000024c)	TRUE		0.0000015
9	9:58:27.636 PM	1	urlmon.dll	CreateMutexA (NULL, FALSE, "Local\ZoneAttributeCacheCounterMutex")	0x00000284		0.0000065
10	9:58:27.636 PM	1	urlmon.dll	CreateMutexA (NULL, FALSE, "Local\ZonesLockedCacheCounterMutex")	0x00000294		0.0000053
11	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x0000024c)	TRUE		0.0000015
12	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x00000280)	TRUE		0.0000015
13	9:58:27.636 PM	1	urlmon.dll	ReleaseMutex (0x00000280)	TRUE		0.0000012
14	9:58:28.214 PM	1	bb31f235e86b0fda...	OpenMutexA (MUTEX_ALL_ACCESS, FALSE, "DoYouWantToHaveSexWithCu...	NULL	2 = The system cannot ...	0.0000067
15	9:58:28.214 PM	1	bb31f235e86b0fda...	CreateMutexA (NULL, FALSE, "DoYouWantToHaveSexWithCuongDong")	0x00000350		0.0000088

Pre-Call Value	Post-Call Value
NULL	NULL
FALSE	FALSE
0x01033c60 "DoYouWantToHaveSe...	0x01033c60 "DoYouWantToHaveSe...
	0x00000350

Hex Buffer: 32 bytes (Post-Call)

```
0000  44 6f 59 6f 75 57 61 6e 74 54 6f 48 61 76 65 53 65 78 57 69 74 6
001a  67 44 6f 6e 67 00
```

Figure 12: Babuk's Mutex Creation

3. Deleting Shadow Copies & Emptying Recycle Bin

Babuk deletes the volume shadow copies (Figure 13) using the 'ShellExecuteW' function and empties the recycle bin (Figure 14) of the victim machine using the 'SHEmptyRecycleBinA' function to inhibit any possibility of data recovery.

```
loc_404713:                             ; CODE XREF: sub_4046D0+14↑j
                                        ; sub_4046D0+3A↑j
                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    sub_404AD0
                test    eax, eax
                jz      short loc_404764
                push    offset aKernel32Dll_0 ; "kernel32.dll"
                call    ds:LoadLibraryA
                mov     [ebp+var_14], eax
                push    offset aWow64revertwow ; "Wow64RevertWow64FsRedirection"
                mov     edx, [ebp+var_14]
                push    edx             ; hModule
                call    ds:GetProcAddress
                mov     [ebp+var_C], eax
                cmp     [ebp+var_C], 0
                jz      short loc_404764
                mov     eax, [ebp+var_8]
                push    eax
                call    [ebp+var_C]

; const WCHAR Parameters
Parameters:                             ; DATA XREF: sub_4046D0+47↓o
                text "UTF-16LE", '/c vssadmin.exe delete shadows /all /quiet',0
```

Figure 13: Babuk deletes Volume Shadow Copies

```
loc_40AC54:                             ; CODE XREF: start+6B↑j
                call    sub_404770
                call    sub_4049B0
                call    sub_4046D0
                push    7               ; dwFlags
                push    0               ; pszRootPath
                push    0               ; hwnd
                call    ds:SHEmptyRecycleBinA
                lea     ecx, [ebp+SystemInfo]
                push    ecx             ; lpSystemInfo
                call    ds:GetSystemInfo
                mov     edx, [ebp+SystemInfo.dwNumberOfProcessors]
                mov     [ebp+var_5C], edx
                mov     eax, [ebp+var_5C]
                shl     eax, 2
                mov     [ebp+var_54], eax
                mov     ecx, [ebp+var_54]
                shr     ecx, 1
                mov     [ebp+nCount], ecx
                imul    edx, [ebp+var_54], 6
                push    edx             ; lInitialCount
                push    offset unk_4141FC ; int
                call    sub_412E50
                add     esp, 8
                imul    eax, [ebp+nCount], 3
                push    eax             ; lInitialCount
                push    offset unk_41422C ; int
                call    sub_412E50
                add     esp, 8
```

Figure 14: Babuk empties Recycle Bin

4. Encryption Process

Upon gathering potential sources of data for encryption, the ransomware firsts check if the files have already been encrypted based on the appended file extension.

The files are encrypted using two algorithms, ChaCha which is based on the Salsa20 algorithm that is symmetric and Elliptic-curve Diffie-Hellman (ECDH) for key generation & protection. The "CryptGenRandom" function is used to randomly generate the 32 Bit key & the nonce along with 'CryptAcquireContextW' & each file is encrypted with a separate key (Figure 15).

Once encrypted, the extension '.babyk' is appended to all files using the 'SetFileAttributesW', 'lstrlenW', 'lstrcpyW', 'lstrcatW' & 'MoveFileExW' functions (Figure 16). The ransomware excludes important system files from encryption to protect the victim machine from crashing. The files are excluded from encryption using a hardcoded list of sensitive system files (Table 2). If a match is found, the crucial system file is left unencrypted.

1	10:21:22.967 PM	1	bb31f235e86b0fda...	CryptAcquireContextW (0x0034f8ac, NULL, NULL, PROV_RSA_AES, CRYPT_V...	TRUE
2	10:21:22.967 PM	1	rsaenh.dll	SystemFunction036 (0x0034f4bc, 48)	TRUE
3	10:21:22.975 PM	1	RPCRT4.dll	SystemFunction036 (0x0034f620, 256)	TRUE
4	10:21:22.975 PM	1	RPCRT4.dll	SystemFunction036 (0x0034f640, 256)	TRUE
5	10:21:22.991 PM	1	RPCRT4.dll	SystemFunction036 (0x0034f4a4, 256)	TRUE
6	10:21:22.991 PM	1	RPCRT4.dll	SystemFunction036 (0x0034f4c4, 256)	TRUE
7	10:21:23.006 PM	1	RPCRT4.dll	SystemFunction036 (0x0034e0c4, 256)	TRUE
8	10:21:23.006 PM	1	ole32.dll	CryptAcquireContextW (0x0034e0c4, NULL, "Microsoft Strong Cryptograp...	TRUE
9	10:21:23.006 PM	1	ole32.dll	CryptGenRandom (0x0079e510, 16, 0x0034e0f8)	TRUE
10	10:21:23.006 PM	1	RPCRT4.dll	SystemFunction036 (0x0034dc58, 256)	TRUE
11	10:21:23.100 PM	2	RPCRT4.dll	SystemFunction036 (0x0332fa5c, 256)	TRUE
12	10:21:23.100 PM	2	ole32.dll	CryptGenRandom (0x0079e510, 16, 0x0332eda8)	TRUE
13	10:21:23.100 PM	2	rsaenh.dll	SystemFunction036 (0x0332eb04, 48)	TRUE
14	10:21:23.100 PM	2	RPCRT4.dll	SystemFunction036 (0x0332e908, 256)	TRUE
15	10:21:23.108 PM	10	bb31f235e86b0fda...	CryptGenRandom (0x00771d58, 32, 0x046efbfc)	TRUE
16	10:21:23.108 PM	10	rsaenh.dll	SystemFunction036 (0x046ecdb0, 48)	TRUE
17	10:21:23.108 PM	13	bb31f235e86b0fda...	CryptGenRandom (0x00771d58, 32, 0x0452f874)	TRUE

Parameters: CryptAcquireContextW (Advapi32.dll)

#	Type	Name	Pre-Call Value	Post-Call Value
1	HCRYPTPROV*	phProv	0x0034f8ac = NULL	0x0034f8ac = 0x00771d58
2	LPCTSTR	pszContainer	NULL	NULL
3	LPCTSTR	pszProvider	NULL	NULL
4	DWORD	dwProvType	PROV_RSA_AES	PROV_RSA_AES
5	DWORD	dwFlags	CRYPT_VERIFYCONTEXT	CRYPT_VERIFYCONTEXT

Figure 15: Part of Encryption using 'CryptAcquireContextW' and 'CryptGenRandom'

```
xt:004097A8                mov     [ebp+var_128], 20676E6Fh
xt:004097B2                mov     [ebp+var_124], 6B6F6F6Ch
xt:004097BC                mov     [ebp+var_120], 696C2073h
xt:004097C6                mov     [ebp+var_11C], 6820656Bh
xt:004097D0                mov     [ebp+var_118], 6420746Fh
xt:004097DA                mov     [ebp+var_114], 2121676Fh
xt:004097E4                push    80h ; '€'       ; dwFileAttributes
xt:004097E9                mov     ecx, [ebp+lpFileName]
xt:004097EC                push    ecx             ; lpFileName
xt:004097ED                call    ds:SetFileAttributesW
xt:004097F3                mov     edx, [ebp+lpFileName]
xt:004097F6                push    edx             ; lpString
xt:004097F7                call    ds:lstrlenW
xt:004097FD                lea     eax, [eax+eax+0Eh]
xt:00409801                push    eax
xt:00409802                call    sub_412E00
xt:00409807                add     esp, 4
xt:0040980A                mov     [ebp+lpString1], eax
xt:0040980D                cmp     [ebp+lpString1], 0
xt:00409811                jz      loc_40A2BE
xt:00409817                mov     ecx, [ebp+lpFileName]
xt:0040981A                push    ecx             ; lpString2
xt:0040981B                mov     edx, [ebp+lpString1]
xt:0040981E                push    edx             ; lpString1
xt:0040981F                call    ds:lstrcpyW
xt:00409825                push    offset String2  ; ".babyk"
xt:0040982A                mov     eax, [ebp+lpString1]
xt:0040982D                push    eax             ; lpString1
xt:0040982E                call    ds:lstrcatW
xt:00409834                push    9               ; dwFlags
xt:00409836                mov     ecx, [ebp+lpString1]
xt:00409839                push    ecx             ; lpNewFileName
xt:0040983A                mov     edx, [ebp+lpFileName]
xt:0040983D                push    edx             ; lpExistingFileName
xt:0040983E                call    ds:MoveFileExW
xt:00409844                test    eax, eax
xt:00409846                jz      loc_40A22F
```

Figure 16: '.babyk' extension appended to encrypted files

Additionally, a ransom note containing details about the infection, threat actor group, onion website links & payments (Figure 17) is added to every directory containing encrypted files. The ransom note advises users to not upload any malware sample on VirusTotal. It also threatens the victim to not involve law enforcement or publicly announce the data leak as failing to do so may lead to increased ransom or other serious consequences.

############## [babuk ransomware greetings you] ##############

Introduction

Congratulations! If you see this note, your company've been randomly chosen for security audit and your company haven't passed it.
Unfortunately your servers are encrypted, backups are encrtypted too or deleted.
Our enctyption algorythms are strong and it's impossible to decrypt your stuff without our help.
Only one method to restore all your network and systems is - to buy our universal decryption software.
Follow simple steps that discribed down below and your data will be saved.
In case you ignore this situation, the consequences could me much serious, than you can imagine.

Guarantees

The hack and system encryption wasn't compromised by your competitors or any other 3rd party, this is just and only our initiative and only thing we interested is profit.
Accurding the previous sentence We are very much value of 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 guarantee full support and help through the all decryption process.
As the proof of our abilities and honesty, we can decrypt few small files for free, check the link provided and ask any questions.

Data leakage

We have copied some quantity of data from your servers.
Check those proofs and estimate the seriousness of consequences which can occur in case you ignore us:
http://wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd.onion/blog/<Victim_Specific_ID>
This link is private and only you can see it.
Use tor browser to open link.
Ignoring the interaction with us brings you the publishing your data in our public blog
http://wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd.onion/

Contact
----

1) Download tor browser: https://www.torproject.org/download/
2) Open it
3) Follow this link in tor browser: http://tsu2dpiiv4zjzfyq73eibemit2qyrimbbb6lhpm6n5ihgallom5lhdyd.onion/<Victim_Specific_ID>

*** 6 simple steps do minimize harm from ransomware.**

Thousands of companies around the world are struggling on ransomware these days, and the most of companies are making the same mistakes again and again. Let's figure out how to minimize harm and do not be a dumb and pathetic donkey which will make fun for journalists and so on..
1. If you see small fella malicious .exe file never load it to virustotal.com or any other virus researching website.
Otherwise the info about the hack is not a secret anymore. The fact that your company is under ransomware attack is already known by filthy predators data security agents who will post in their pity twitters the fresh known news "OMG ANOTHER RANSOMWARE NOW IT'S "Your company name LLC!!!!! We are all gonna die aaaaaa halp"

2. No any public announcements about the hack or data leakage. And do not applicate to law enforcement.
If you commit this actions, more serious consequences can occur and you pay much more than a ransom amount. Law structures like GDPR in this case can oblige you to pay huge fine.

3. As soon as you see your network compromised, follow the link inside any note and follow instructions.

4. Calm your employees.
Explain them that this is a drill. And you test your network security systems.

5. If you decide to hire the data recovery company, obligate them to do not inform anyone and any third party about details of the attack.
We strongly do not recommend to cooperate with data recovery company, because they do absolutely nothing that you can do by yourself and take money for it. all communications with hackers could be conducted by your it department indipendently without any extra payments.

6. Do not try to decrypt your data via 3rd party software.
Most of ransomware use strong encryption algorthm and you can harm your files by using 3rd party decryption software.

Figure 17: Babuk's Ransom Note

- **MITRE ATTACK MATRIX**

TACTIC	ID	NAME
DISCOVERY	T1083	File and directory discovery
	T1082	System Information Discovery
	T1057	Process Discovery
	T1135	Network Share Discovery
	T1518.001	Security Software Discovery
EXECUTION	T1129	Shared Modules
	T1106	Native API
IMPACT	T1490	Inhibit System Recovery
PERSISTENCE	T1547.001	Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder
PRIVILEGE ESCALATION	T1055	Process Injection
DEFENCE EVASION	T1070.004	File Deletion
	T1112	Modify Registry
	T1562.001	Impair Defences: Disable or Modify Tools
	T1497	Virtualization or Sandbox Evasion
	T1140	Deobfuscate/Decode Files or Information

SUBEX SECURE PROTECTION
Subex Secure detects Babuk Ransomware as 'SS_Gen_Babuk_PE_A' and 'SS_Gen_Babuk_PE_B'.

OUR HONEYPOT NETWORK
This report has been prepared from threat intelligence gathered by our honeypot network. This honeypot network is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing Centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research Centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analysed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for

purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.

Table - I

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	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

Table 1: Processes & Services Terminated

Table - II

Boot	Windows	Windows.old
TorBrowser	InternetExplorer	Google
Opera	OperaSoftware	Mozilla
MozillaFirefox	$Recycle.Bin	ProgramData
AllUsers	autorun.inf	boot.ini
bootfont.bin	bootsect.bak	bootmgr
bootmgr.efi	bootmgfw.efi	desktop.ini
iconcache.db	ntldr	ntuser.dat
ntuser.dat.log	ntuser.ini	thumbs.db
ProgramFiles	AppData	ProgramFiles(x86)

Table 2: Sensitive files excluded from the Encryption Process