Examining the Black Basta Ransomware's Infection Routine

We analyze the Black Basta ransomware and examine the malicious actor's familiar infection tactics.

By: Ieriz Nicolle Gonzalez, Ivan Nicole Chavez, Katherine Casona, Nathaniel Morales

May 09, 2022

Black Basta, a new ransomware gang, has swiftly risen to prominence in recent weeks after it caused massive breaches to organizations in a short span of time.

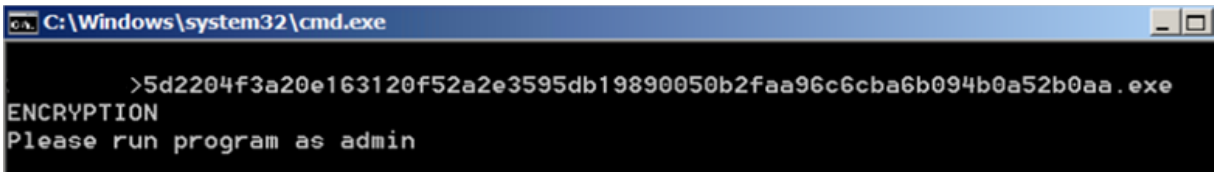
On April 20, 2022, a user named Black Basta posted on underground forums known as XSS.IS and EXPLOIT.IN to advertise that it intends to buy and monetize corporate network access credentials for a share of the profits. The advertisement also specified that it was looking for organizations based in the United States, Canada, United Kingdom, Australia, and New Zealand, which are all English-speaking countries. A report noted that malicious actors acquired stolen credentials from some darknet websites that peddle an enormous amount of exfiltrated data to the underground market.

On April 26, Twitter user PCrisk tweeted about the new Black Basta ransomware that appends the extension .basta and changes the desktop wallpaper.

This blog entry takes a closer look at the Black Basta ransomware and analyzes this newcomer's familiar infection techniques.

The infection routine

Black Basta ransomware needs administrator rights to run. It otherwise displays a command prompt message as shown on Figure 1.

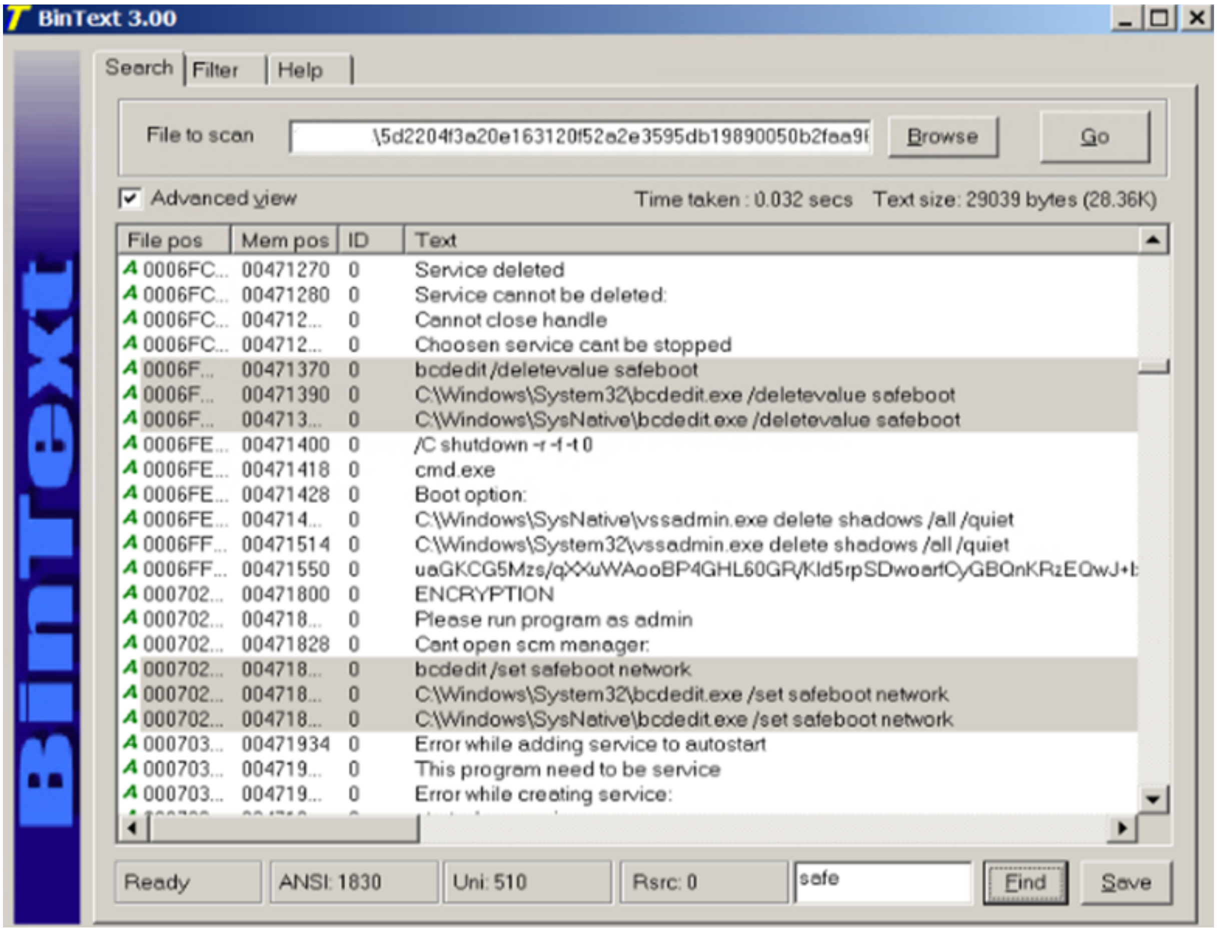


```
        >5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa.exe
ENCRYPTION
Please run program as admin
```

Figure 1. A command prompt is displayed if Black Basta ransomware is not run with administrator rights.

After running the ransomware as administrator, it removes shadow copies, disables Windows recovery and repair, and boots the PC in safe mode.

- C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
- C:\Windows\SysNative\bcdedit.exe /deletevalue safeboot
- C:\Windows\SysNative\bcdedit /set safeboot networkChanges



File to scan: \5d2204f3a20e163120f52a2e3595db19890050b2faa9(

☑ Advanced view

Time taken : 0.032 secs   Text size: 29039 bytes (28.36K)

	File pos	Mem pos	ID	Text
A	0006FC...	00471270	0	Service deleted
A	0006FC...	00471280	0	Service cannot be deleted:
A	0006FC...	004712...	0	Cannot close handle
A	0006FC...	004712...	0	Choosen service cant be stopped
A	0006F...	00471370	0	bcdedit /deletevalue safeboot
A	0006F...	00471390	0	C:\Windows\System32\bcdedit.exe /deletevalue safeboot
A	0006F...	004713...	0	C:\Windows\SysNative\bcdedit.exe /deletevalue safeboot
A	0006FE...	00471400	0	/C shutdown -r -f -t 0
A	0006FE...	00471418	0	cmd.exe
A	0006FE...	00471428	0	Boot option:
A	0006FE...	004714...	0	C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
A	0006FF...	00471514	0	C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
A	0006FF...	00471550	0	uaGKCG5Mzs/qXXuWAooBP4GHL60GR/Kld5rpSDwoarfCyGBQnKRzEQwJ+b
A	000702...	00471800	0	ENCRYPTION
A	000702...	004718...	0	Please run program as admin
A	000702...	00471828	0	Cant open scm manager:
A	000702...	004718...	0	bcdedit /set safeboot network
A	000702...	004718...	0	C:\Windows\System32\bcdedit.exe /set safeboot network
A	000702...	004718...	0	C:\Windows\SysNative\bcdedit.exe /set safeboot network
A	000703...	00471934	0	Error while adding service to autostart
A	000703...	004719...	0	This program need to be service
A	000703...	004719...	0	Error while creating service:

Ready | ANSI: 1830 | Uni: 510 | Rsrc: 0 | safe | Find | Save

Figure 2. Commands such as "C:\Windows\SysNative\bcedit /set

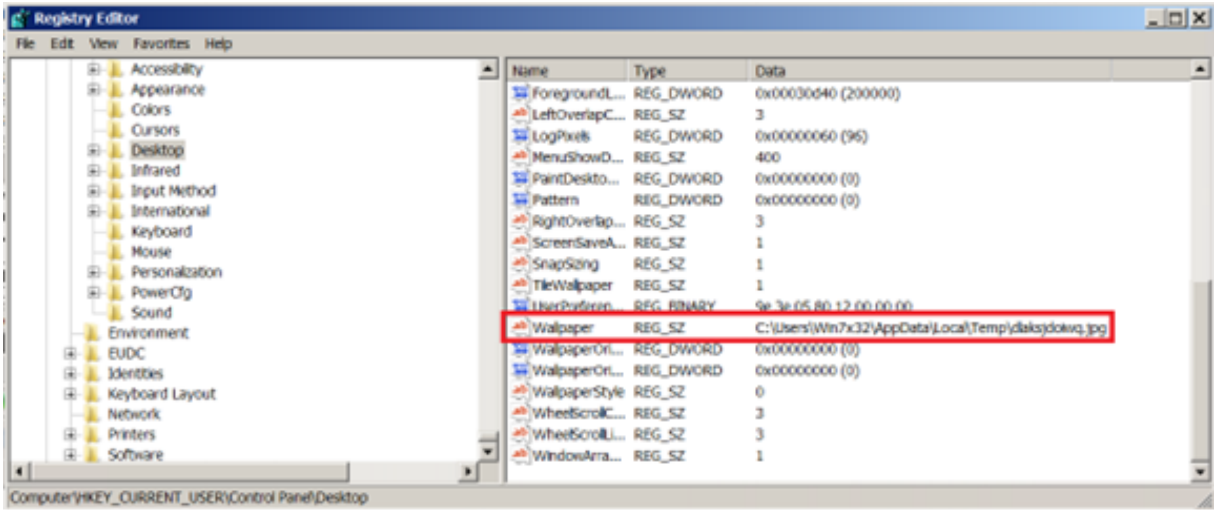
safeboot networkChanges" are embedded in the binary and can be viewed easily.

It also drops the following files, which will be used later when changing the desktop wallpaper and icons for encrypted files:

- %Temp%\fkdjsadasd.ico
- %Temp%\dlaksjdoiwq.jpg

Before booting the infected device into safe mode, it changes the desktop wallpaper by dropping the .jpg file into the %temp% folder and creating the following registry entry:

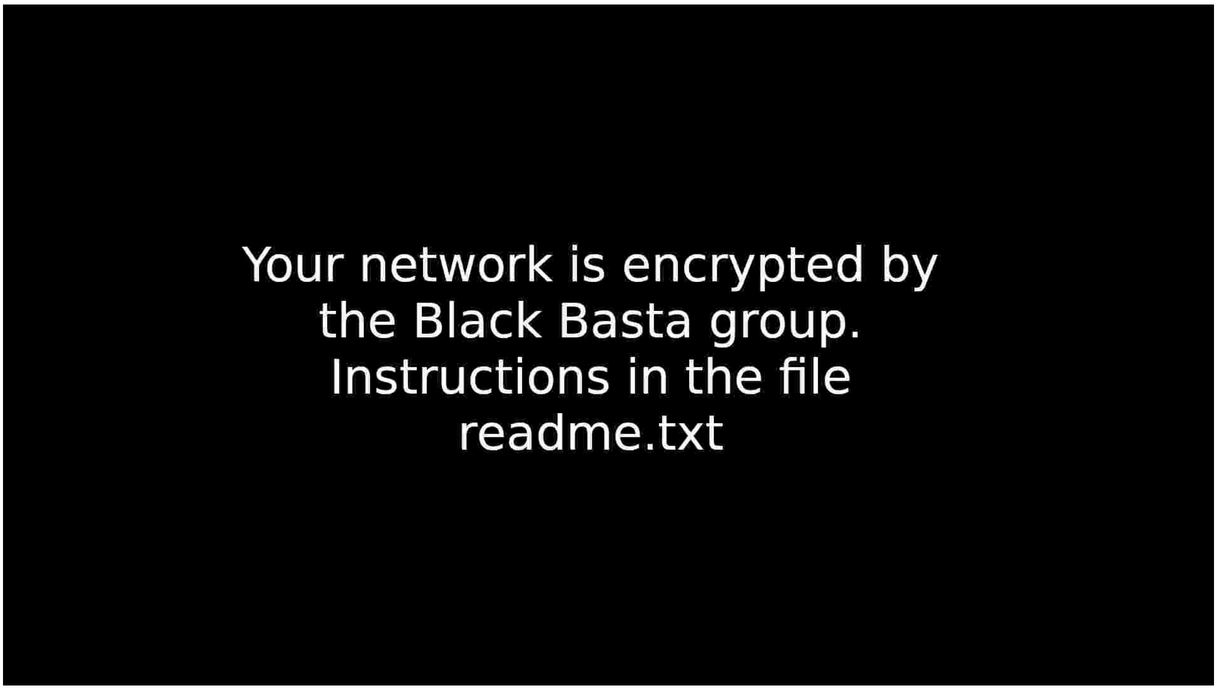
- Key: HKCU\Control Panel\Desktop; Value: Wallpaper; Data:%Temp%\dlaksjdoiwq.jpg;



Name	Type	Data
ForegroundL...	REG_DWORD	0x00030d40 (200000)
LeftOverlapC...	REG_SZ	3
LogPixels	REG_DWORD	0x00000060 (96)
MenuShowD...	REG_SZ	400
PaintDeskto...	REG_DWORD	0x00000000 (0)
Pattern	REG_DWORD	0x00000000 (0)
RightOverlap...	REG_SZ	3
ScreenSaveA...	REG_SZ	1
SnapSizing	REG_SZ	1
TileWallpaper	REG_SZ	1
UserPreferen...	REG_BINARY	9e 3e 05 80 12 00 00 00
Wallpaper	REG_SZ	C:\Users\Win7x32\AppData\Local\Temp\dlaksjdoiwq.jpg
WallpaperOri...	REG_DWORD	0x00000000 (0)
WallpaperOri...	REG_DWORD	0x00000000 (0)
WallpaperStyle	REG_SZ	0
WheelScrollC...	REG_SZ	3
WheelScrollL...	REG_SZ	3
WindowArra...	REG_SZ	1

Computer\HKEY_CURRENT_USER\Control Panel\Desktop

Figure 3. The registry entry created after Black Basta ransomware changes the wallpaper on the infected machine

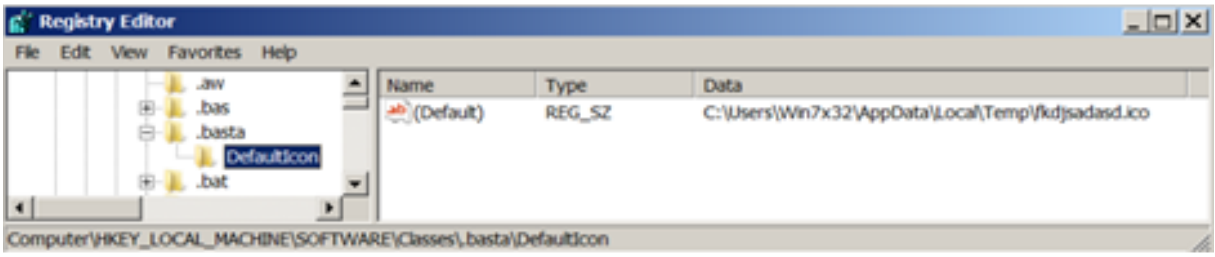


Your network is encrypted by
the Black Basta group.
Instructions in the file
readme.txt

Figure 4. The desktop wallpaper created by the ransomware from the .jpg file dropped in the %temp% folder

After changing the desktop wallpaper, it then adds the following registry keys to change the icon of the encrypted files with the .basta extension:

- HKLM\SOFTWARE\Classes\.basta
- HKLM\SOFTWARE\Classes\.basta\DefaultIcon data: %TEMP%\fkdjsadasd.ico



.aw
.bas
.basta
DefaultIcon
.bat

Name	Type	Data
(Default)	REG_SZ	C:\Users\Win7x32\AppData\Local\Temp\fkdjsadasd.ico

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.basta\DefaultIcon

Figure 5. The registry keys added by the ransomware to change the icon of the files with the .basta extension

The ransomware proceeds to encrypt files while the device is in safe mode, appending all encrypted files with the .basta extension. The ransom note is found in all the folders the ransomware has affected.

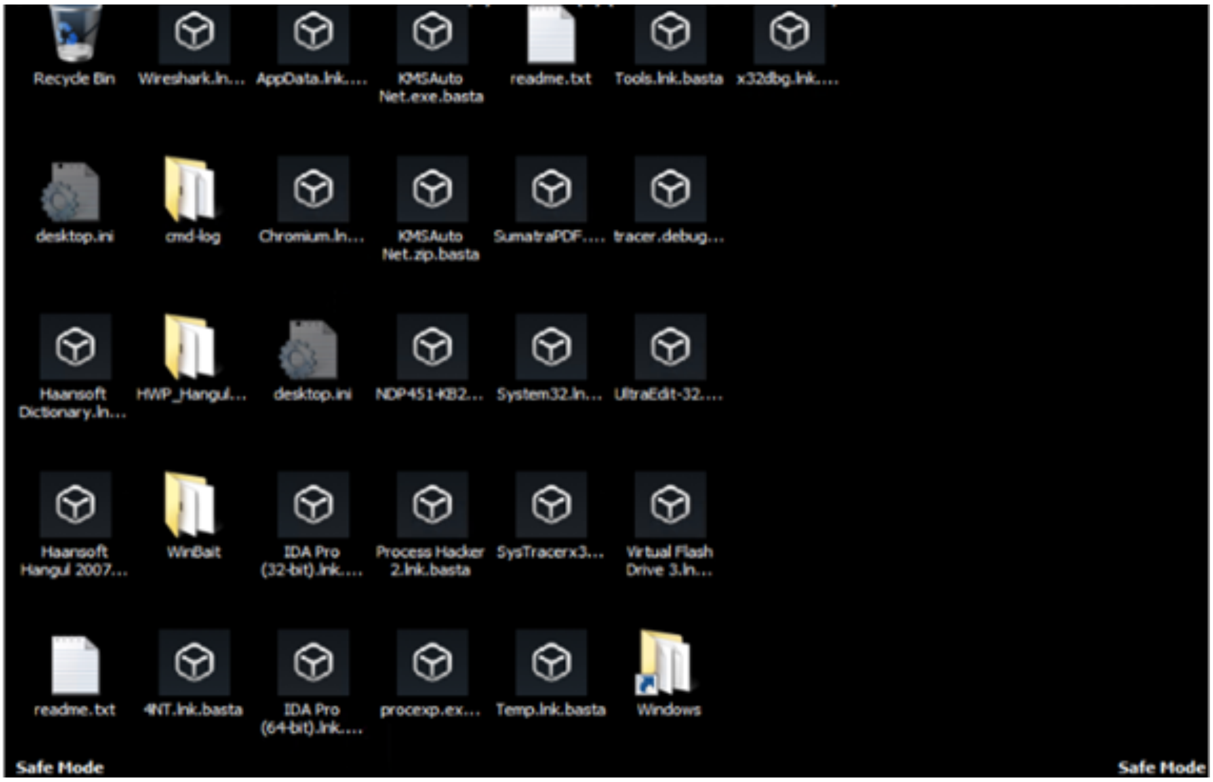
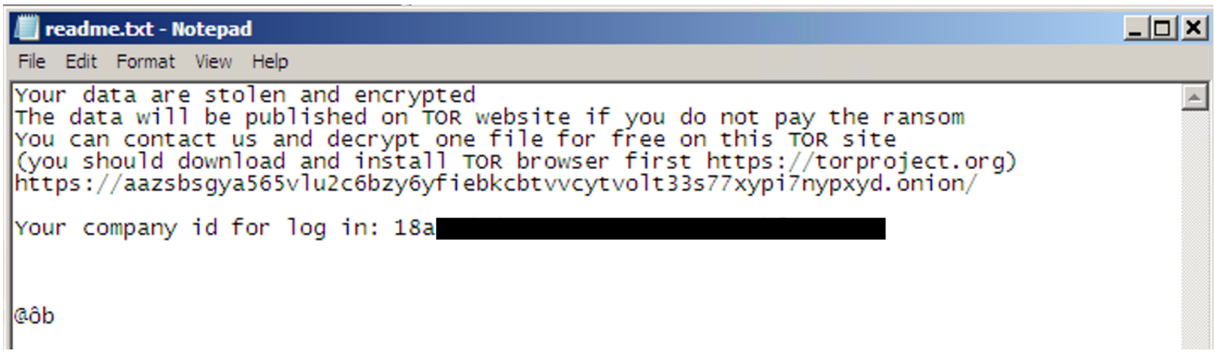


Figure 6. The infected files shown with the .basta extension

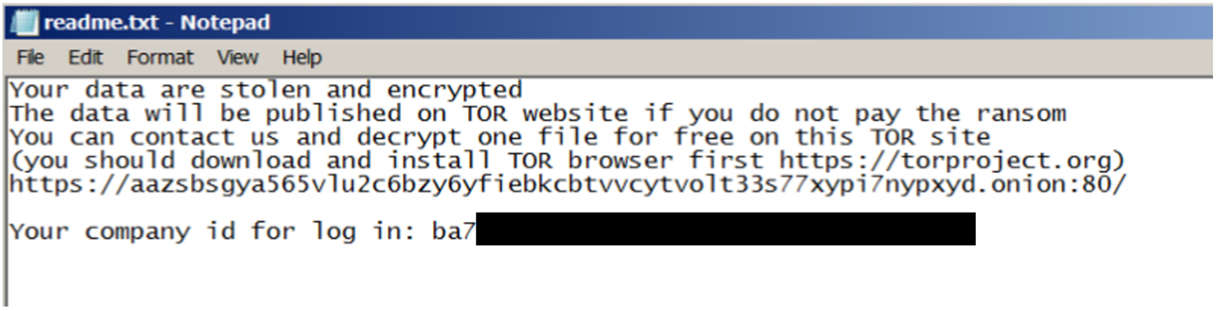
The ransom note indicates the malicious actor’s onion site and a company ID. Despite running the same ransomware (SHA256 hash: 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa) on different virtual machines, the company ID the gang provides is the same across all devices.



```
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/

Your company id for log in: 18a[redacted]


@ôb
```

Figure 7. The ransom note dropped by Black Basta

Using another binary (SHA256 hash: 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a), a different company ID is shown on the ransom note. The files are likewise appended with the .basta extension.



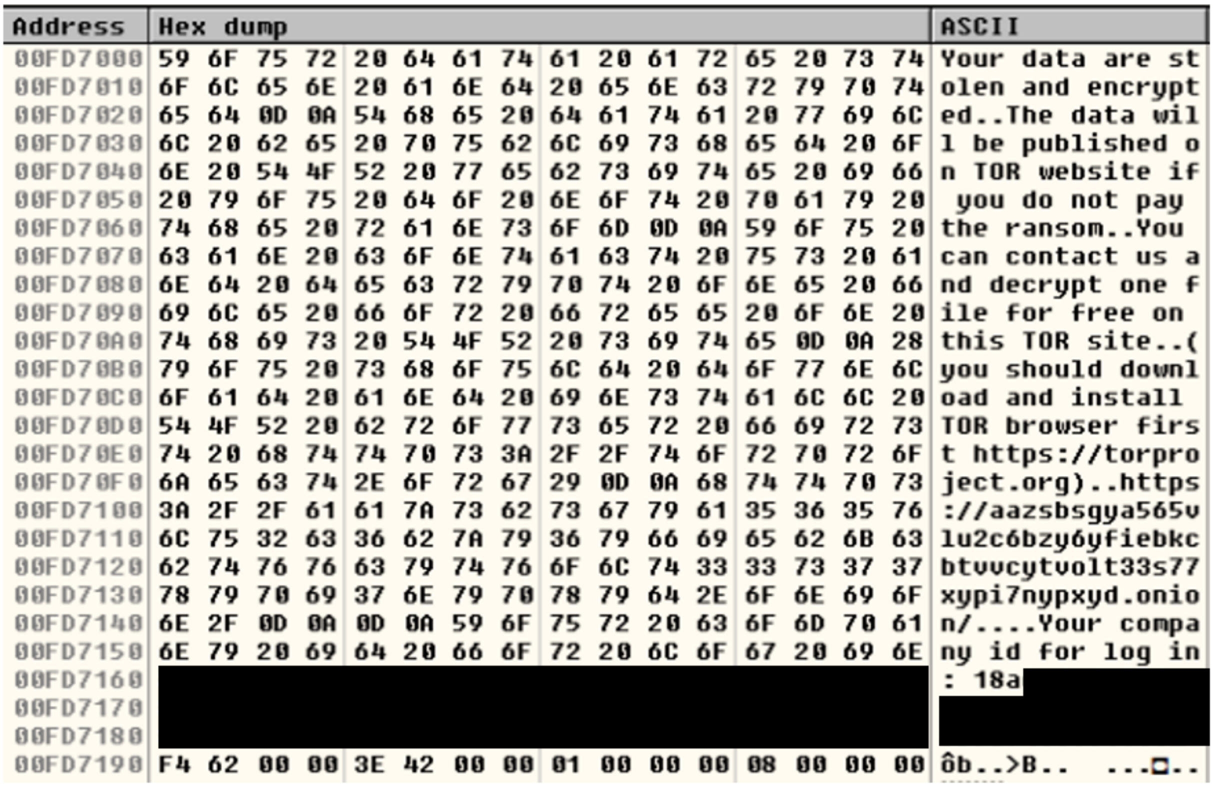
```
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/

Your company id for log in: ba7[redacted]
```

Figure 8. A different company ID is given when another binary is used.

Analyzing the infection routine

Black Basta's recent entry to the cybercrime world suggests that information about their operations is still limited. According to a report, the gang has neither started marketing its operations nor has it begun recruitment of affiliates in underground forums. Based on advertisements they posted before the attacks, the malicious actor likely uses stolen credentials — purchased in darknet websites or underground forums — to get into an organization's system.

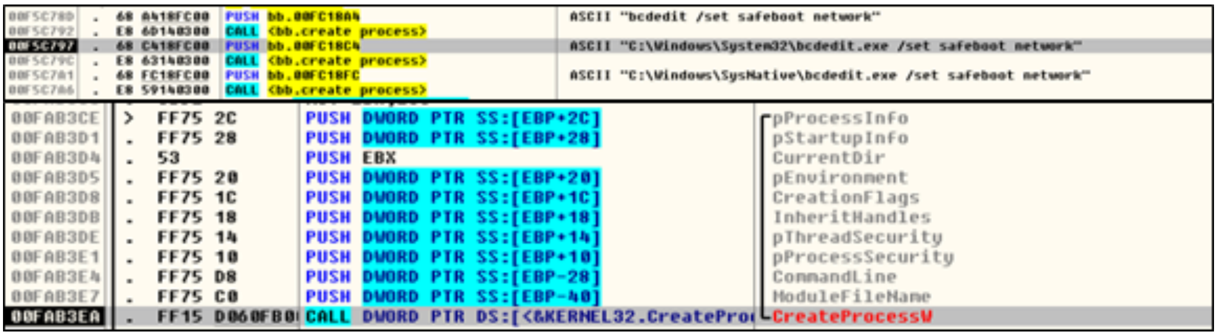
We probed further and found that the company ID written in the ransom note is hardcoded in the binary file.



```
Address  Hex dump                                         ASCII
00FD7000 59 6F 75 72 20 64 61 74 61 20 61 72 65 20 73 74 Your data are st
00FD7010 6F 6C 65 6E 20 61 6E 64 20 65 6E 63 72 79 70 74 olen and encrypt
00FD7020 65 64 0D 0A 54 68 65 20 64 61 74 61 20 77 69 6C ed..The data wil
00FD7030 6C 20 62 65 20 70 75 62 6C 69 73 68 65 64 20 6F l be published o
00FD7040 6E 20 54 4F 52 20 77 65 62 73 69 74 65 20 69 66 n TOR website if
00FD7050 20 79 6F 75 20 64 6F 20 6E 6F 74 20 70 61 79 20  you do not pay
00FD7060 74 68 65 20 72 61 6E 73 6F 6D 0D 0A 59 6F 75 20 the ransom..You
00FD7070 63 61 6E 20 63 6F 6E 74 61 63 74 20 75 73 20 61 can contact us a
00FD7080 6E 64 20 64 65 63 72 79 70 74 20 6F 6E 65 20 66 nd decrypt one f
00FD7090 69 6C 65 20 66 6F 72 20 66 72 65 65 20 6F 6E 20 ile for free on
00FD70A0 74 68 69 73 20 54 4F 52 20 73 69 74 65 0D 0A 28 this TOR site..(
00FD70B0 79 6F 75 20 73 68 6F 75 6C 64 20 64 6F 77 6E 6C you should downl
00FD70C0 6F 61 64 20 61 6E 64 20 69 6E 73 74 61 6C 6C 20 oad and install
00FD70D0 54 4F 52 20 62 72 6F 77 73 65 72 20 66 69 72 73 TOR browser firs
00FD70E0 74 20 68 74 74 70 73 3A 2F 2F 74 6F 72 70 72 6F t https://torpro
00FD70F0 6A 65 63 74 2E 6F 72 67 29 0D 0A 68 74 74 70 73 ject.org)..https
00FD7100 3A 2F 2F 61 61 7A 73 62 73 67 79 61 35 36 35 76 ://aazsbsgya565v
00FD7110 6C 75 32 63 36 62 7A 79 36 79 66 69 65 62 6B 63 lu2c6bzy6yfiebkc
00FD7120 62 74 76 76 63 79 74 76 6F 6C 74 33 33 73 37 37 btvvcytvolt33s77
00FD7130 78 79 70 69 37 6E 79 70 78 79 64 2E 6F 6E 69 6F xypi7nypxyd.onio
00FD7140 6E 2F 0D 0A 0D 0A 59 6F 75 72 20 63 6F 6D 70 61 n/....Your compa
00FD7150 6E 79 20 69 64 20 66 6F 72 20 6C 6F 67 20 69 6E ny id for log in
00FD7160 [redacted]                                       : 18a[redacted]
00FD7170
00FD7180
00FD7190 F4 62 00 00 3E 42 00 00 01 00 00 00 08 00 00 00 ôb..>B..  ...□..
```

Figure 9. The company ID in the ransom note is hardcoded in the binary file.

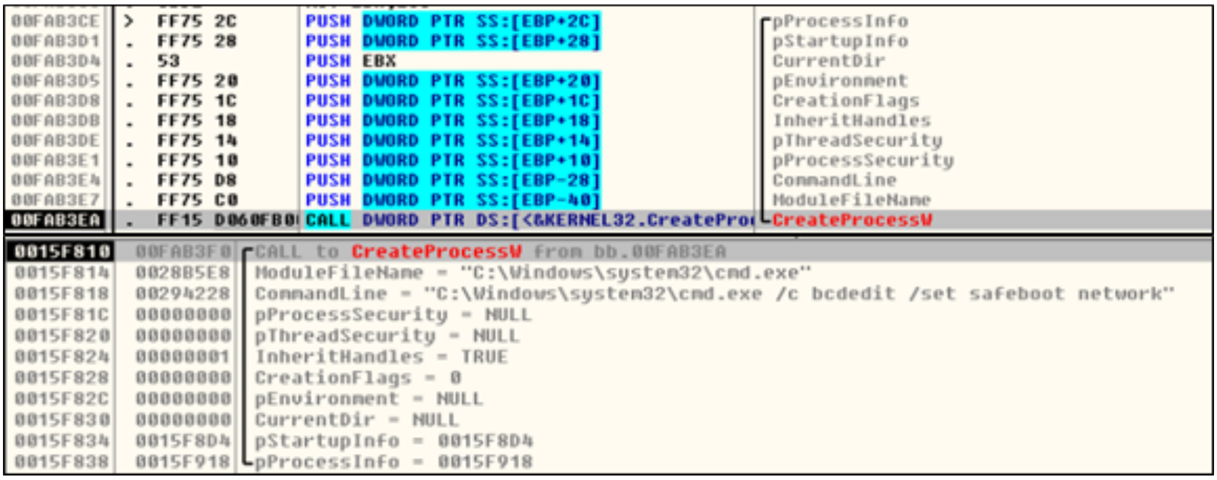
Black Basta attempts to delete shadow copies using vssadmin.exe and boots the device in safe mode using bcdexit.exe from different paths, specifically, %SysNative% and %System32%.



```
00F5C78D  .  68 A418FC00  PUSH bb.00FC18A4          ASCII "bcdedit /set safeboot network"
00F5C792  .  E8 6D140300  CALL <bb.create process>
00F5C797  .  68 C418FC00  PUSH bb.00FC18C4          ASCII "C:\Windows\System32\bcdedit.exe /set safeboot network"
00F5C79C  .  E8 63140300  CALL <bb.create process>
00F5C7A1  .  68 FC18FC00  PUSH bb.00FC18FC          ASCII "C:\Windows\SysNative\bcdedit.exe /set safeboot network"
00F5C7A6  .  E8 59140300  CALL <bb.create process>
```

```
00FAB3CE  >  FF75 2C      PUSH DWORD PTR SS:[EBP+2C]              ┌pProcessInfo
00FAB3D1  .  FF75 28      PUSH DWORD PTR SS:[EBP+28]              │pStartupInfo
00FAB3D4  .  53           PUSH EBX                                │CurrentDir
00FAB3D5  .  FF75 20      PUSH DWORD PTR SS:[EBP+20]              │pEnvironment
00FAB3D8  .  FF75 1C      PUSH DWORD PTR SS:[EBP+1C]              │CreationFlags
00FAB3DB  .  FF75 18      PUSH DWORD PTR SS:[EBP+18]              │InheritHandles
00FAB3DE  .  FF75 14      PUSH DWORD PTR SS:[EBP+14]              │pThreadSecurity
00FAB3E1  .  FF75 10      PUSH DWORD PTR SS:[EBP+10]              │pProcessSecurity
00FAB3E4  .  FF75 D8      PUSH DWORD PTR SS:[EBP-28]              │CommandLine
00FAB3E7  .  FF75 C0      PUSH DWORD PTR SS:[EBP-40]              │ModuleFileName
00FAB3EA  .  FF15 D060FB0 CALL DWORD PTR DS:[<&KERNEL32.CreatePro └CreateProcessW
```

Figure 10. Black Basta's attempts to delete shadow copies using vssadmin.exe

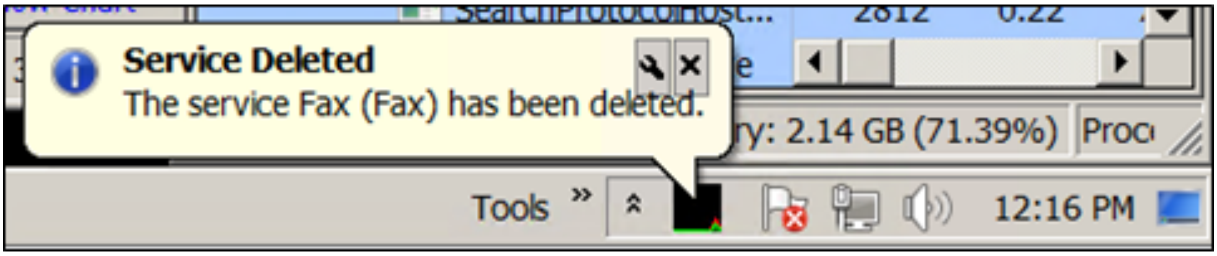


```
00FAB3CE  >  FF75 2C      PUSH DWORD PTR SS:[EBP+2C]              ┌pProcessInfo
00FAB3D1  .  FF75 28      PUSH DWORD PTR SS:[EBP+28]              │pStartupInfo
00FAB3D4  .  53           PUSH EBX                                │CurrentDir
00FAB3D5  .  FF75 20      PUSH DWORD PTR SS:[EBP+20]              │pEnvironment
00FAB3D8  .  FF75 1C      PUSH DWORD PTR SS:[EBP+1C]              │CreationFlags
00FAB3DB  .  FF75 18      PUSH DWORD PTR SS:[EBP+18]              │InheritHandles
00FAB3DE  .  FF75 14      PUSH DWORD PTR SS:[EBP+14]              │pThreadSecurity
00FAB3E1  .  FF75 10      PUSH DWORD PTR SS:[EBP+10]              │pProcessSecurity
00FAB3E4  .  FF75 D8      PUSH DWORD PTR SS:[EBP-28]              │CommandLine
00FAB3E7  .  FF75 C0      PUSH DWORD PTR SS:[EBP-40]              │ModuleFileName
00FAB3EA  .  FF15 D060FB0 CALL DWORD PTR DS:[<&KERNEL32.CreatePro └CreateProcessW
```

```
0015F810   00FAB3F0  ┌CALL to CreateProcessW from bb.00FAB3EA
0015F814   0028B5E8  │ModuleFileName = "C:\Windows\system32\cmd.exe"
0015F818   00294228  │CommandLine = "C:\Windows\system32\cmd.exe /c bcdedit /set safeboot network"
0015F81C   00000000  │pProcessSecurity = NULL
0015F820   00000000  │pThreadSecurity = NULL
0015F824   00000001  │InheritHandles = TRUE
0015F828   00000000  │CreationFlags = 0
0015F82C   00000000  │pEnvironment = NULL
0015F830   00000000  │CurrentDir = NULL
0015F834   0015F8D4  │pStartupInfo = 0015F8D4
0015F838   0015F918  └pProcessInfo = 0015F918
```

Figure 11. Black Basta boots the device in safe mode using bcdexit.exe from different paths, specifically, %SysNative% and %System32%.

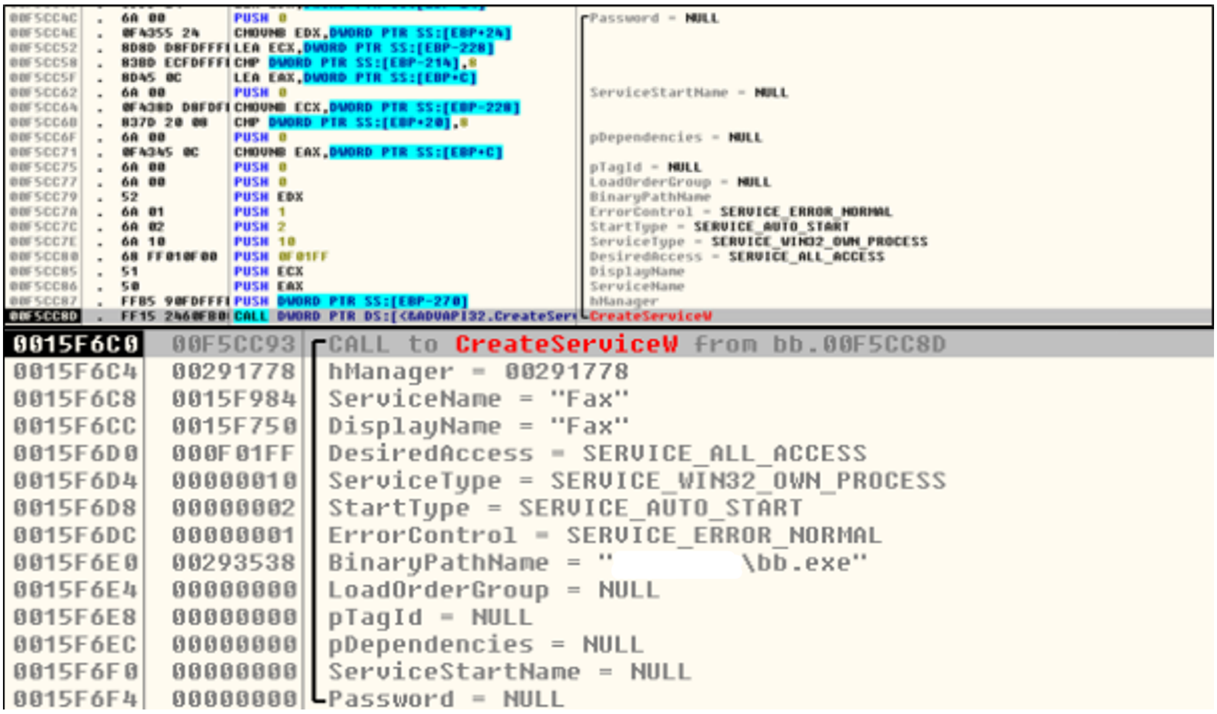
At this stage, the ransomware deletes the service named Fax, and creates a new one with the same name using the malware's path and adds it to the registry for persistence.



Service Deleted

The service Fax (Fax) has been deleted.

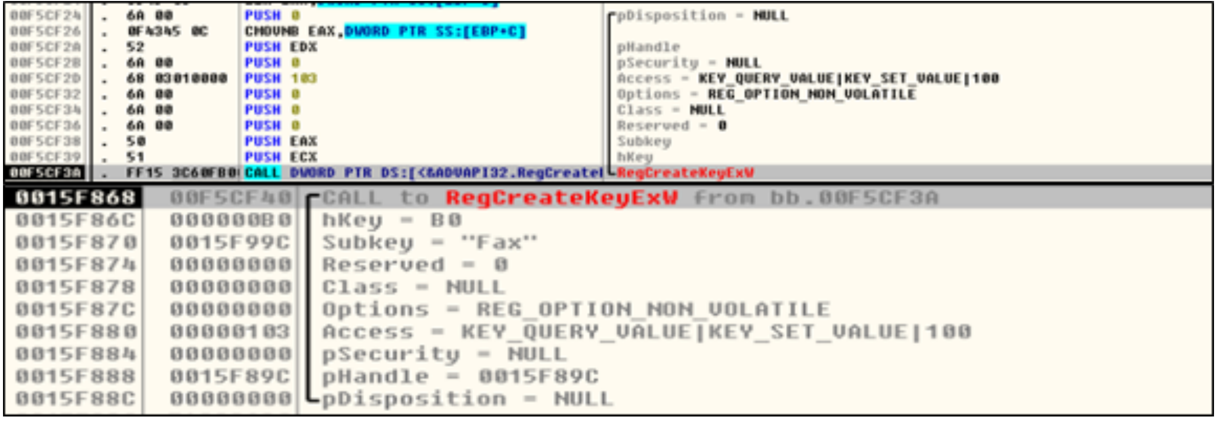
Figure 12. Pop-up notification when the Fax service is deleted



```
00F5CC4C  .  6A 00          PUSH 0                                   ┌Password = NULL
00F5CC4E  .  0F4355 24      CMOVNB EDX,DWORD PTR SS:[EBP+24]         │
00F5CC52  .  8D8D D8FDFFFF  LEA ECX,DWORD PTR SS:[EBP-228]           │
00F5CC58  .  83BD ECFDFFFF  CMP DWORD PTR SS:[EBP-214],8             │
00F5CC5F  .  8D45 0C        LEA EAX,DWORD PTR SS:[EBP+C]             │
00F5CC62  .  6A 00          PUSH 0                                   │ServiceStartName = NULL
00F5CC64  .  0F438D D8FDFF  CMOVNB ECX,DWORD PTR SS:[EBP-228]        │
00F5CC68  .  837D 20 08     CMP DWORD PTR SS:[EBP+20],8              │
00F5CC6F  .  6A 00          PUSH 0                                   │pDependencies = NULL
00F5CC71  .  0F4345 0C      CMOVNB EAX,DWORD PTR SS:[EBP+C]          │
00F5CC75  .  6A 00          PUSH 0                                   │pTagId = NULL
00F5CC77  .  6A 00          PUSH 0                                   │LoadOrderGroup = NULL
00F5CC79  .  52             PUSH EDX                                 │BinaryPathName
00F5CC7A  .  6A 01          PUSH 1                                   │ErrorControl = SERVICE_ERROR_NORMAL
00F5CC7C  .  6A 02          PUSH 2                                   │StartType = SERVICE_AUTO_START
00F5CC7E  .  6A 10          PUSH 10                                  │ServiceType = SERVICE_WIN32_OWN_PROCESS
00F5CC80  .  68 FF010F00    PUSH 0F01FF                              │DesiredAccess = SERVICE_ALL_ACCESS
00F5CC85  .  51             PUSH ECX                                 │DisplayName
00F5CC86  .  50             PUSH EAX                                 │ServiceName
00F5CC87  .  FFB5 90FDFFFF  PUSH DWORD PTR SS:[EBP-270]              │hManager
00F5CC8D  .  FF15 2460FB00  CALL DWORD PTR DS:[<&ADVAPI32.CreateServ └CreateServiceW
```

```
0015F6C0   00F5CC93  ┌CALL to CreateServiceW from bb.00F5CC8D
0015F6C4   00291778  │hManager = 00291778
0015F6C8   0015F984  │ServiceName = "Fax"
0015F6CC   0015F750  │DisplayName = "Fax"
0015F6D0   000F01FF  │DesiredAccess = SERVICE_ALL_ACCESS
0015F6D4   00000010  │ServiceType = SERVICE_WIN32_OWN_PROCESS
0015F6D8   00000002  │StartType = SERVICE_AUTO_START
0015F6DC   00000001  │ErrorControl = SERVICE_ERROR_NORMAL
0015F6E0   00293538  │BinaryPathName = "[redacted]\bb.exe"
0015F6E4   00000000  │LoadOrderGroup = NULL
0015F6E8   00000000  │pTagId = NULL
0015F6EC   00000000  │pDependencies = NULL
0015F6F0   00000000  │ServiceStartName = NULL
0015F6F4   00000000  └Password = NULL
```

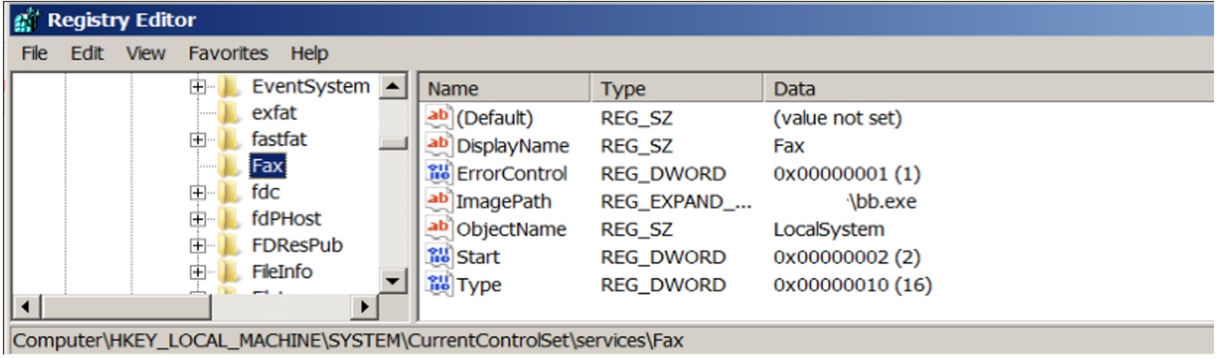
Figure 13. Functions used in creating a new service, also named “Fax,” that uses the file path of the malware as its binary path name



```
00F5CF24  .  6A 00          PUSH 0                                   ┌pDisposition = NULL
00F5CF26  .  0F4345 0C      CMOVNB EAX,DWORD PTR SS:[EBP+C]          │
00F5CF2A  .  52             PUSH EDX                                 │pHandle
00F5CF2B  .  6A 00          PUSH 0                                   │pSecurity = NULL
00F5CF2D  .  68 03010000    PUSH 103                                 │Access = KEY_QUERY_VALUE|KEY_SET_VALUE|100
00F5CF32  .  6A 00          PUSH 0                                   │Options = REG_OPTION_NON_VOLATILE
00F5CF34  .  6A 00          PUSH 0                                   │Class = NULL
00F5CF36  .  6A 00          PUSH 0                                   │Reserved = 0
00F5CF38  .  50             PUSH EAX                                 │Subkey
00F5CF39  .  51             PUSH ECX                                 │hKey
00F5CF3A  .  FF15 3C60FB00  CALL DWORD PTR DS:[<&ADVAPI32.RegCreateK └RegCreateKeyExW
```

```
0015F868   00F5CF40  ┌CALL to RegCreateKeyExW from bb.00F5CF3A
0015F86C   000000B0  │hKey = B0
0015F870   0015F99C  │Subkey = "Fax"
0015F874   00000000  │Reserved = 0
0015F878   00000000  │Class = NULL
0015F87C   00000000  │Options = REG_OPTION_NON_VOLATILE
0015F880   00000103  │Access = KEY_QUERY_VALUE|KEY_SET_VALUE|100
0015F884   00000000  │pSecurity = NULL
0015F888   0015F89C  │pHandle = 0015F89C
0015F88C   00000000  └pDisposition = NULL
```

Figure 14. Functions used when creating a registry key

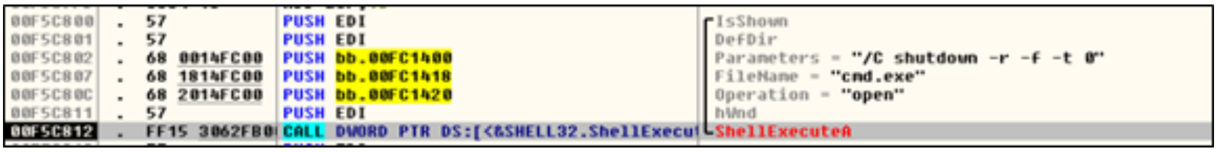


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	Fax
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_...	[redacted]\bb.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Fax

Figure 15. New registry key created for the new “Fax” service that replaces the deleted service

It then uses ShellExecuteA to shut down and restart the victim’s machine.

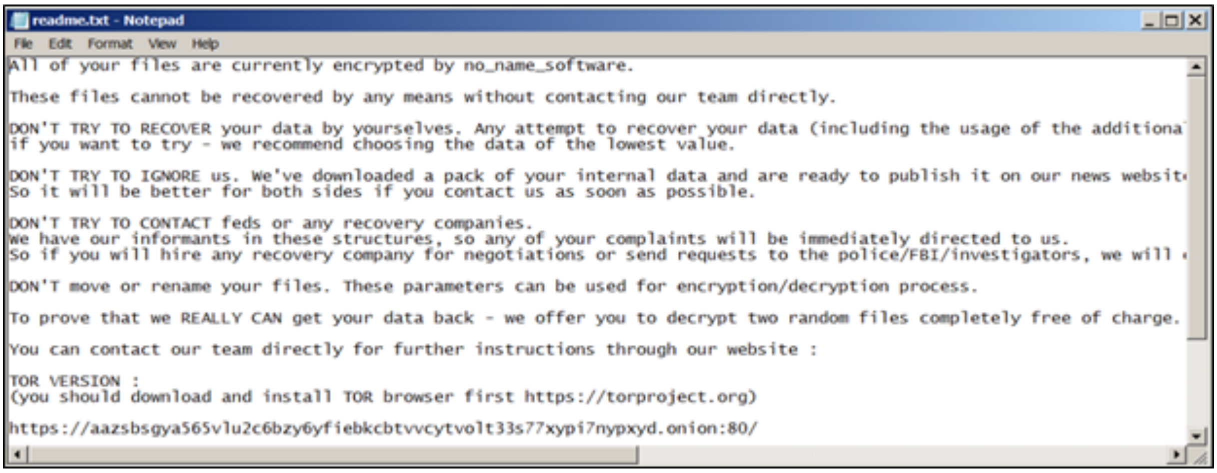


```
00F5C800  .  57              PUSH EDI                                     ┌IsShown
00F5C801  .  57              PUSH EDI                                     │DefDir
00F5C802  .  68 0014FC00     PUSH bb.00FC1400                             │Parameters = "/C shutdown -r -f -t 0"
00F5C807  .  68 1814FC00     PUSH bb.00FC1418                             │FileName = "cmd.exe"
00F5C80C  .  68 2014FC00     PUSH bb.00FC1420                             │Operation = "open"
00F5C811  .  57              PUSH EDI                                     │hWnd
00F5C812  .  FF15 3062FB0    CALL DWORD PTR DS:[<&SHELL32.ShellExecu      └ShellExecuteA
```

Figure 16. Function ShellExecuteA used to shut down and restart the victim's machine

Extortion phase

For a newcomer in the field, Black Basta is quite prolific for having compromised at least a dozen organizations in just a few weeks. The group's first known attack using the Black Basta ransomware occurred in the second week of April 2022. But an earlier sample was also spotted back in February 2022 with the ransomware name "no_name_software," which appends the extension "encrypted" to encrypted files. According to some threat researchers, it appears that Black Basta has been in development since early February 2022.

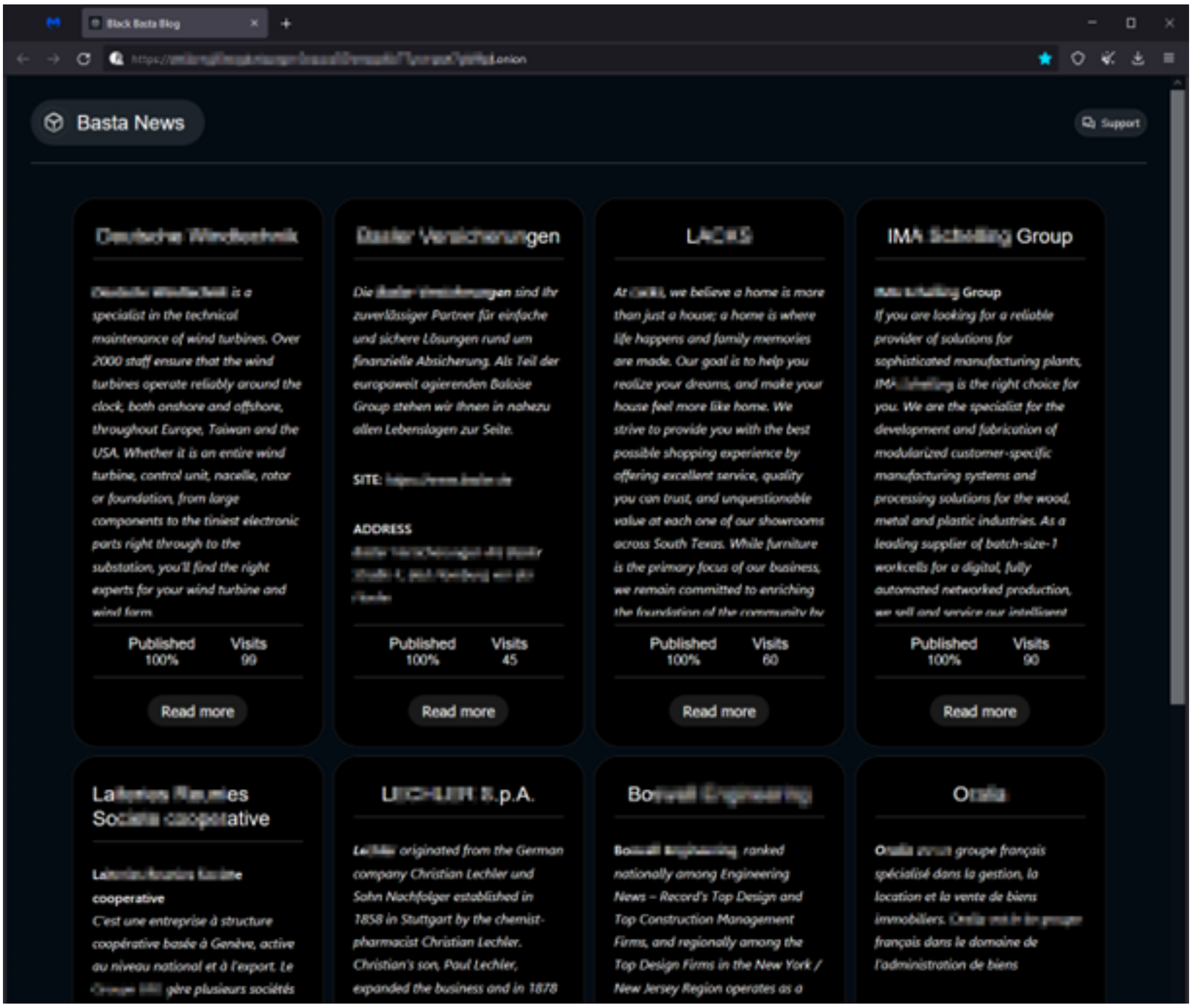


```
All of your files are currently encrypted by no_name_software.

These files cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additiona
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news websit
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will

DON'T move or rename your files. These parameters can be used for encryption/decryption process.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/
```

Figure 17. Ransom note used in an earlier sample

Like other enterprise-focused ransomware operations, Black Basta employs a double extortion scheme that involves exfiltrating confidential data before encryption to threaten victims with public release of the stolen data.

The gang carries out the extortion phase of its attacks on its Tor site, Basta News, which contains a list of all the victims who have not paid the ransom.



Basta News

[redacted]

[redacted] is a specialist in the technical maintenance of wind turbines. Over 2000 staff ensure that the wind turbines operate reliably around the clock, both onshore and offshore, throughout Europe, Taiwan and the USA. Whether it is an entire wind turbine, control unit, nacelle, rotor or foundation, from large components to the tiniest electronic parts right through to the substation, you'll find the right experts for your wind turbine and wind farm.

Published 100% Visits 99

Read more

[redacted]gen

Die [redacted]gen sind Ihr zuverlässiger Partner für einfache und sichere Lösungen rund um finanzielle Absicherung. Als Teil der europaweit agierenden Baloise Group stehen wir Ihnen in nahezu allen Lebenslagen zur Seite.

SITE: [redacted]

ADDRESS
[redacted]

Published 100% Visits 45

Read more

L[redacted]

At [redacted], we believe a home is more than just a house; a home is where life happens and family memories are made. Our goal is to help you realize your dreams, and make your house feel more like home. We strive to provide you with the best possible shopping experience by offering excellent service, quality you can trust, and unquestionable value at each one of our showrooms across South Texas. While furniture is the primary focus of our business, we remain committed to enriching the foundation of the community by

Published 100% Visits 60

Read more

IMA [redacted] Group

[redacted] Group
If you are looking for a reliable provider of solutions for sophisticated manufacturing plants, IMA [redacted] is the right choice for you. We are the specialist for the development and fabrication of modularized customer-specific manufacturing systems and processing solutions for the wood, metal and plastic industries. As a leading supplier of batch-size-1 workcells for a digital, fully automated networked production, we sell and service our intelligent

Published 100% Visits 90

Read more

La[redacted]es So[redacted]ative

La[redacted]e cooperative
C'est une entreprise à structure coopérative basée à Genève, active au niveau national et à l'export. Le [redacted] gère plusieurs sociétés

L[redacted] S.p.A.

Le[redacted] originated from the German company Christian Lechler und Sohn Nachfolger established in 1858 in Stuttgart by the chemist-pharmacist Christian Lechler. Christian's son, Paul Lechler, expanded the business and in 1878

Bo[redacted]

[redacted], ranked nationally among Engineering News – Record's Top Design and Top Construction Management Firms, and regionally among the Top Design Firms in the New York / New Jersey Region operates as a

O[redacted]

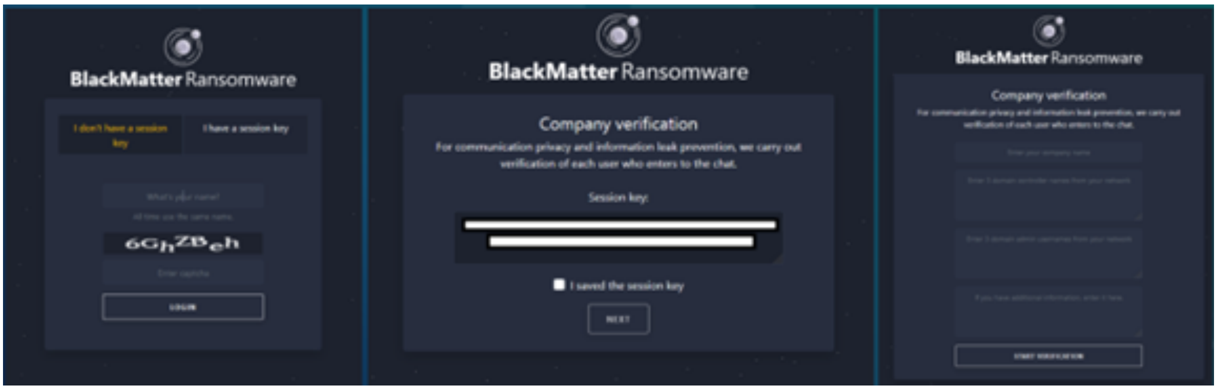
O[redacted] groupe français spécialisé dans la gestion, la location et la vente de biens immobiliers. [redacted] français dans le domaine de l'administration de biens

Figure 18. Black Basta's leak site, retrieved from https://twitter.com/MarceloRivero/status/1519398885193654273

Possible relation to an APT

Security researchers exchanged speculations on Twitter that Black Basta is possibly a rebranding of the Conti ransomware operation. MalwareHunterTeam pointed out many similarities in its leak site, payment site, and negotiation style to those of Conti's. Twitter user Arkbird echoed the same observation. Lawrence Abrams of BleepingComputer also mentioned that the malicious actors behind Black Basta seem like they are exerting a lot of effort to avoid any resemblance to their previous identity.

We have also noticed some similarities between the Black Basta and Black Matter payment sites. Like Black Matter, Black Basta implements user verification on its Tor site. However, the leak site does not implement a session key.



BlackMatter Ransomware

I don't have a session key

I have a session key

What's your name?

All time use the same name.

6GhZBeh

Enter captcha

LOGIN

BlackMatter Ransomware

Company verification

For communication privacy and information leak prevention, we carry out verification of each user who enters to the chat.

Session key:

[redacted]

□ I saved the session key

NEXT

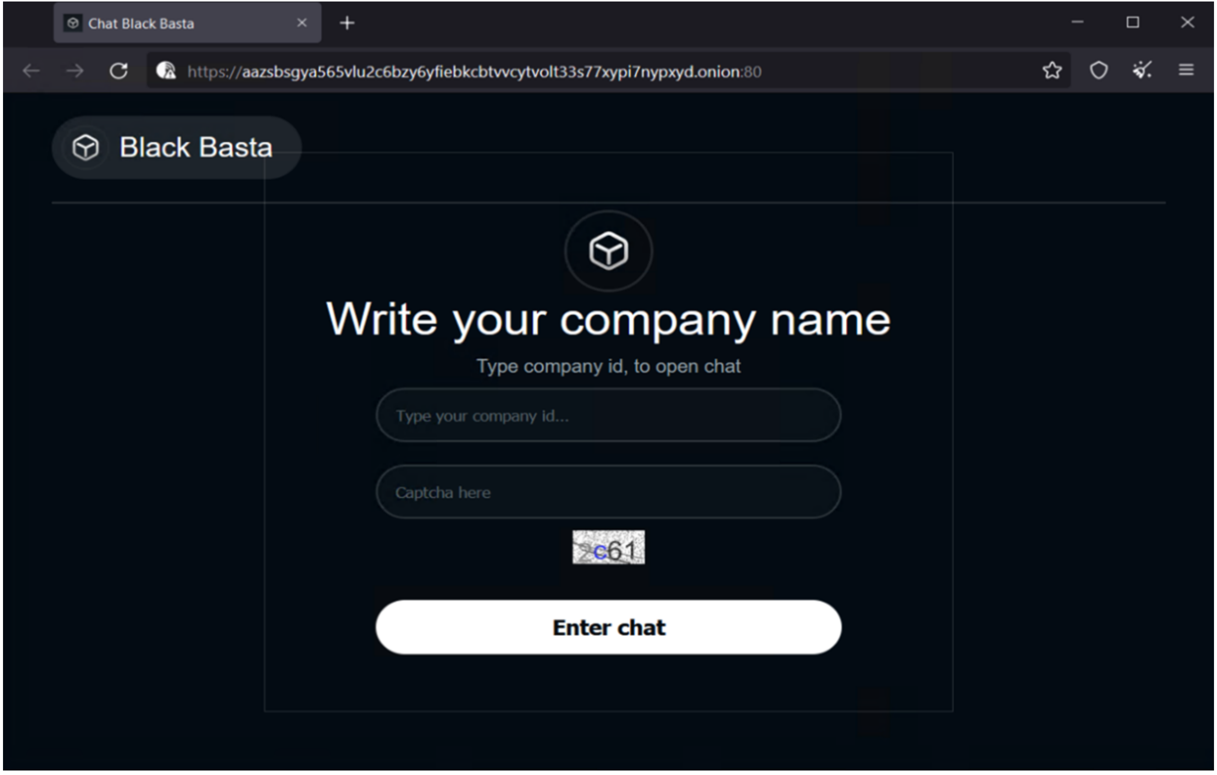
BlackMatter Ransomware

Company verification

For communication privacy and information leak prevention, we carry out verification of each user who enters to the chat.

START VERIFICATION

Figure 19. The Black Matter payment site



Chat Black Basta

https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80

Black Basta

Write your company name

Type company id, to open chat

Type your company id...

Captcha here

2c61

Enter chat

Figure 20. The Black Basta payment site

Insights

The malicious actors could be using a unique binary for each organization that they target. This can be seen from the ransom note that they drop, which is hardcoded in the malware itself. A ransomware typically creates a unique ID for each victim despite being infected by the same executable. Their choice of target organizations also suggests this to be the case. They buy corporate network access credentials in underground markets, which could mean that they do not distribute their malware sporadically. Instead, they use a certain kind of binary or variant for a specific organization.

Recommendations

Threat researchers suggest that the recent attacks by Black Basta can be seen as early manifestations of Conti’s rebranding efforts. True or not, organizations should keep a watchful eye against ransomware threats. An organization’s thorough assessment of its security posture and its implementation of solid cybersecurity defenses give it a better fighting chance against such threats.

To protect systems against similar attacks, organizations can establish security frameworks that allocate resources systematically for establishing a strong defense strategy against ransomware. Here are some best practices that organizations can consider:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Audit event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee’s role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allowlist that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication (MFA)

Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees in security skills
- Conduct red-team exercises and penetration tests

A multilayered approach can help organizations guard possible entry points into their system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior, which can help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.
- Trend Micro Cloud One™ – Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

SHA256	Trend Micro Detection

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	Ransom.Win32.BASTACRYPT.THDBGBB
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a	Ransom.Win32.BASTACRYPT.YXCD2
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	Ransom.Win32.BASTACRYPT.THDBIBB
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Ransom.Win32.BASTACRYPT.YXCD2
a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1	Ransom.Win32.BASTACRYPT.THDBGBB
1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250	Ransom.Win32.BASTACRYPT.YXCD2
2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88	Ransom.Win32.BASTACRYPT.YXCD2.note
f088e6944b2632bb7c93fa3c7ba1707914c05c00f9491e033f78a709d65d7cff	Ransom.Win32.BASTACRYPT.YXCD2.note