Shining the Light on Black Basta

June 6, 2022
Authored by: **Ross Inman** (@rdi_x64) and **Peter Gurney**

Summary

tl;dr

This blog post documents some of the TTPs employed by a threat actor group who were observed deploying Black Basta ransomware during a recent incident response engagement, as well as a breakdown of the executable file which performs the encryption.

A summary of the findings can be found below:

- Lateral movement through use of Qakbot.
- Gathering internal IP addresses of all hosts on the network.
- Disabling Windows Defender.
- Deleting Veeam backups from Hyper-V servers.
- Use of WMI to push out the ransomware.
- Technical analysis of the ransomware executable.

Black Basta

Black Basta are a ransomware group who have recently emerged, with the first public reports of attacks occurring in April this year. As is popular with other ransomware groups, Black Basta uses doubleextortion attacks where data is first exfiltrated from the network before the ransomware is deployed. The threat actor then threatens to leak the data on the “Black Basta Blog” or “Basta News” Tor site. There are two Tor sites used by Black Basta, one which leaks stolen data and one which the victims can use to contact the ransomware operators. The latter site is provided in the ransom note which is dropped by the ransomware executable.

Black Basta TTPs

Lateral Movement

Black Basta was observed using the following methods to laterally move throughout the network after their initial access had been gained:

- PsExec.exe which was created in the C:\Windows\ folder.
- Qakbot was leveraged to remotely create a temporary service on a target host which was configured to execute a Qakbot DLL using regsvr32.exe:
    - `regsvr32.exe -s \\<IP address of compromised Domain Controller>\SYSVOL\<random string>.dll`
- RDP along with the deployment of a batch file called rdp.bat which contained command lines to enable RDP logons. This was used to allow the threat actor to establish remote desktop sessions on compromised hosts, even if RDP was disabled originally:
    - `reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f`
    - `net start MpsSvc`
    - `netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes`
    - `reg add "HKLM\System\CurrentControlSet\Control\Terminal`

Server\WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f

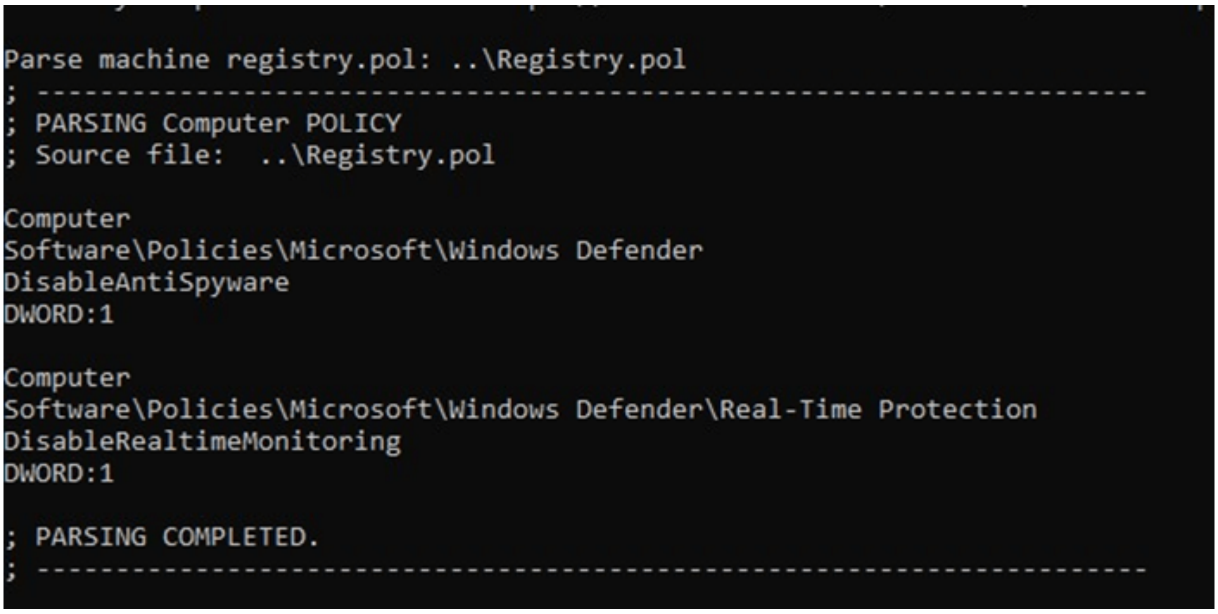
Defense Evasion

During the intrusion, steps were taken by the threat actor in order to prevent interference from anti-virus. The threat actor was observed using two main techniques to disable Windows Defender.

The first used the batch script d.bat which was deployed locally on compromised hosts and executed the following PowerShell commands:

- powershell -ExecutionPolicy Bypass -command "New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender' -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force"
- powershell -ExecutionPolicy Bypass -command "Set-MpPreference -DisableRealtimeMonitoring 1"
- powershell -ExecutionPolicy Bypass Uninstall-WindowsFeature -Name Windows-Defender

The second technique involved creating a GPO (Group Policy Object) on a compromised Domain Controller which would push out the below changes to the Windows Registry of domain-joined hosts:



```
Parse machine registry.pol: ..\Registry.pol
; ----------------------------------------------------------------------
; PARSING Computer POLICY
; Source file:  ..\Registry.pol

Computer
Software\Policies\Microsoft\Windows Defender
DisableAntiSpyware
DWORD:1

Computer
Software\Policies\Microsoft\Windows Defender\Real-Time Protection
DisableRealtimeMonitoring
DWORD:1

; PARSING COMPLETED.
; ----------------------------------------------------------------------
```

Figure 1 Parsed Registry.pol of the created GPO

Discovery

A text file in the C:\Windows\ folder named pc_list.txt was present on two compromised Domain Controllers, both contained a list of internal IP addresses of all the systems on the network. This was to supply the threat actor with a list of IP addresses to target when deploying the ransomware.

Command and Control

Qakbot was the primary method utilised by the threat actor to maintain their presence on the network. The threat actor was also observed using Cobalt Strike beacons during the compromise.

Impact

Prior to the deployment of the ransomware, the threat actor established RDP sessions to Hyper-V servers and from there modified configurations for the Veeam backup jobs and deleted the backups of the hosted virtual machines.

An encoded PowerShell command was observed on one of the compromised Domain Controllers which, when decoded, yielded a script labelled as Invoke-TotalExec that provided the ability to spread and execute files over the network using WMI (Windows Management Instrumentation). The script appears to have been run to push out the ransomware binary to the IP addresses contained within the file C:\Windows\pc_list.txt. Analysis of the script indicates that two log files are created:

- C:\Windows\Temp\log.info – Contains log entries for successful attempts.
- C:\Windows\Temp\log.dat – Contains log entries for unsuccessful attempts.

For the incident investigated by NCC Group CIRT, only the latter log file had data. The log file contained entries relating to failed uploads for all the IP addresses from pc_list.txt, indicating that the threat actor attempted to deploy the ransomware executable across all hosts on the network, however this had failed. Despite this, the ransomware was still deployed to Hyper-V servers and the Domain Controllers.

Recommendations

1. Hypervisors should be isolated by placing them in a separate domain or by adding them to a workgroup to ensure that any compromise in the domain in which the hosted virtual machines reside does not pose any risk to the Hypervisors.
2. Ensure that both online and offline backups are taken and test the backup strategy regularly to identify any weak points that could be exploited by an adversary.
3. Restrict internal RDP and SMB traffic ensuring only hosts that are required to communicate via these protocols are allowed to.

Indicators of Compromise

IOC Value	Indicator Type	Description
23.106.160[.]188	IP Address	Cobalt Strike Command-and-Controller server
eb43350337138f2a77593c79cee1439217d02957	SHA1	Batch script which enabled RDP on the host (rdp.bat)
920fe42b1bd69804080f904f0426ed784a8ebbc2	SHA1	Batch script to disable Windows Defender (d.bat)

C:\Windows\PsExec.exe	Filename	PsExec
C:\Windows\SYSVOL\sysvol\<random string>.dll	Filename	Qakbot payload
C:\Windows\Temp\log.info C:\Windows\Temp\log.dat	Filename	Invoke-TotalExec output log files

Ransomware Technical Analysis

Shadow Copy Deletion

Upon execution, Black Basta performs several operations before launching its encryption activities.

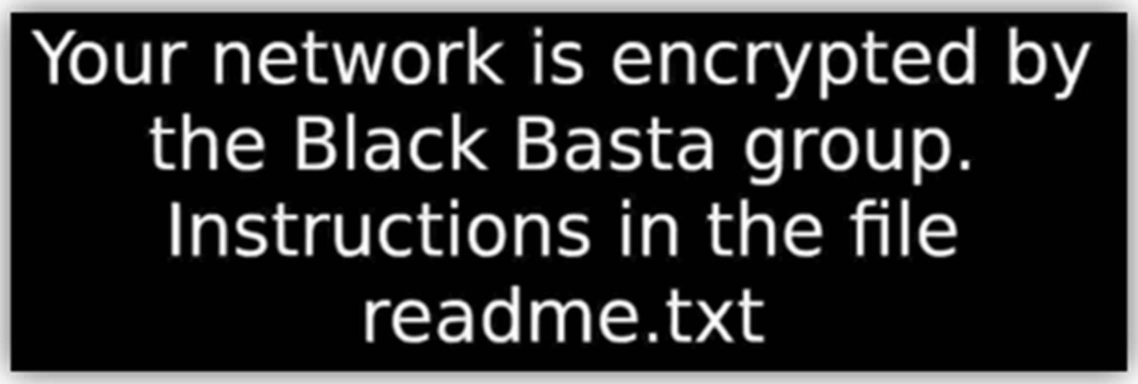
The Mutex ‘dsajdhas.0’ is checked before issuing the two vssadmin.exe commands listed below. Although the Mutex is static in this sample it is expected to change across future samples.

```
C:\\Windows\\SysNative\\vssadmin.exe delete shadows /all /quiet
C:\\Windows\\System32\\vssadmin.exe delete shadows /all /quiet
```

These result in the deletion of shadow copies ensuring they cannot be used for recovery purposes.

Wallpaper icon modification

Following deletion of the shadow copies, two files are obtained from the binary. Firstly, a JPG file in the currently analysed sample is saved as ‘dlaksjdoiwq.jpg’, used as a wallpaper on targeted devices. The image used can be seen below in Figure 2.



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

Figure 2 Desktop wallpaper image

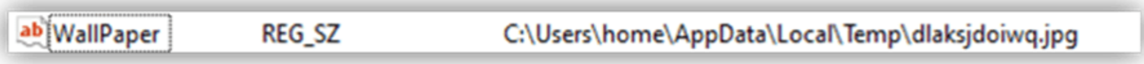
The second dropped file is an icon file obtained from within the binary and used as a default icon for all files with extension. basta. The file is saved in the currently analysed sample with the name fkdjsadasd.ico within the *%Temp% directory, for example:*

```
C:\Users\{Username}\AppData\Local\Temp
```

The icon used can be seen below in Figure 3.

Figure 3 Basta icon

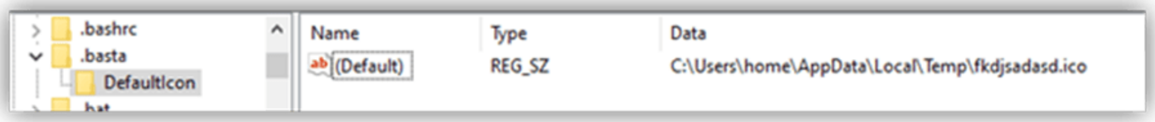
The wallpaper is modified to display the dropped JPG through the registry located at HKCU\Control Panel\Desktop\Wallpaper, setting the path to the JPG as seen below in Figure 4.



```
WallPaper    REG_SZ    C:\Users\home\AppData\Local\Temp\dlaksjdoiwq.jpg
```

Figure 4 String de-obfuscation example

The next operation creates a new registry key with the name .basta under HKEY_CLASSES_ROOT and sets the DefaultIcon subkey to display the dropped .ico file. This results in files given a .basta file extension inheriting the Black Basta logo. The registry key can be seen below in Figure 5.



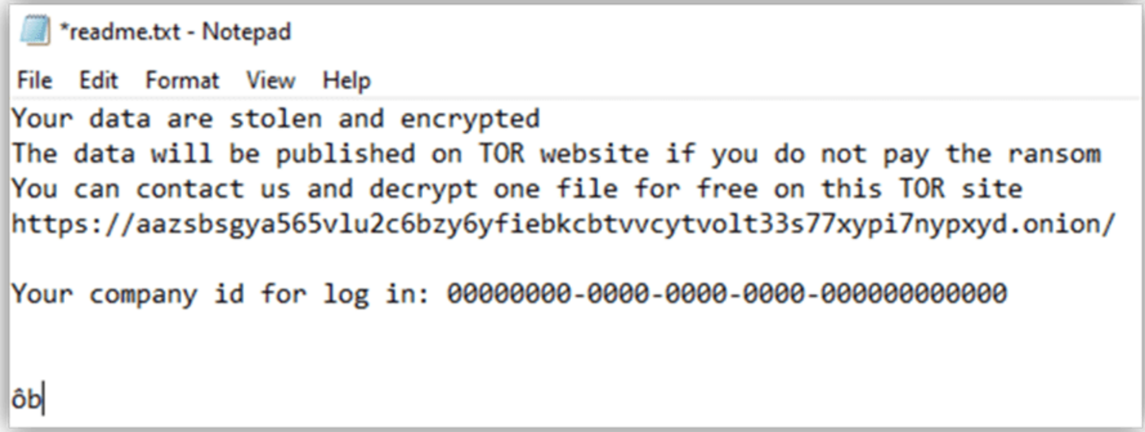
Name	Type	Data
(Default)	REG_SZ	C:\Users\home\AppData\Local\Temp\fkdjsadasd.ico

Figure 5 Desktop wallpaper image

Ransom Note

The ransomware note is stored within the binary and written to a text file named readme.txt, as shown in Figure 6. This file is written to folders throughout the system. The content comprises a standard Black Basta template with a URL to a Tor site where victims can negotiate with operators.

A company ID is also present, which varies between compromises.



```
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
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/

Your company id for log in: 00000000-0000-0000-0000-000000000000


ôb
```

Figure 6 Ransom Note

Exclusions

In an attempt to avoid encrypting files or folders that are likely essential to the operation of the target machine or Black Basta itself, several exclusions are in place that will prevent encrypting specific files. This includes several extensions, folders and files listed below.

Extension exclusions:

- exe
- cmd
- bat
- com
- bat
- basta

File Folder exclusions:

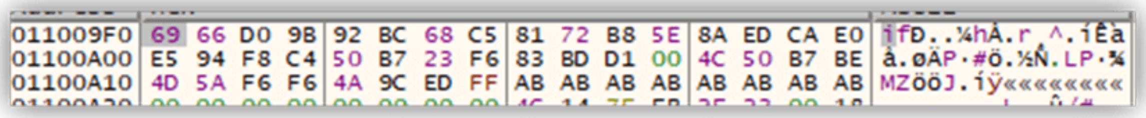
- $Recycle.Bin
- Windows
- Documents and Settings
- Local Settings
- Application Data
- OUT.txt
- Boot
- Readme.txt
- Dlaksjdoiwq.jpg
- NTUSER.DAT
- fkdjsadasd.iso

A copy of the ransom note is placed where an eligible folder is found, and suitable files discovered within the folder are passed for encryption.

Encryption

Several threads are created that are responsible for performing the encryption activity. Each file that is not skipped by the previously mentioned exclusions is encrypted using the ChaCha20 cypher.

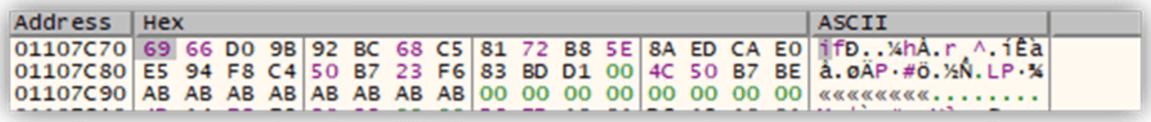
The encryption key is generated using the C++ rand_s function resulting in a random 40-byte hexadecimal output.



```
011009F0  69 66 D0 9B 92 BC 68 C5 81 72 B8 5E 8A ED CA E0  ifÐ..¼hÅ.r¸^.íÊà
01100A00  E5 94 F8 C4 50 B7 23 F6 83 BD D1 00 4C 50 B7 BE  å.øÄP·#ö.½Ñ.LP·¾
01100A10  4D 5A F6 F6 4A 9C ED FF AB AB AB AB AB AB AB AB  MZööJ.íÿ««««««««
```

Figure 7 Random generation output

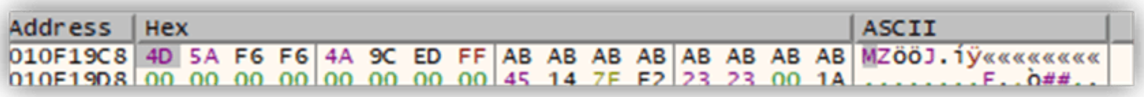
The first 32 bytes are used as the ChaCha20 encryption key.



```
Address   Hex                                              ASCII
01107C70  69 66 D0 9B 92 BC 68 C5 81 72 B8 5E 8A ED CA E0  ifÐ..¼hÅ.r¸^.íÊà
01107C80  E5 94 F8 C4 50 B7 23 F6 83 BD D1 00 4C 50 B7 BE  å.øÄP·#ö.½Ñ.LP·¾
01107C90  AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00  ««««««««........
```

Figure 8 Encryption key

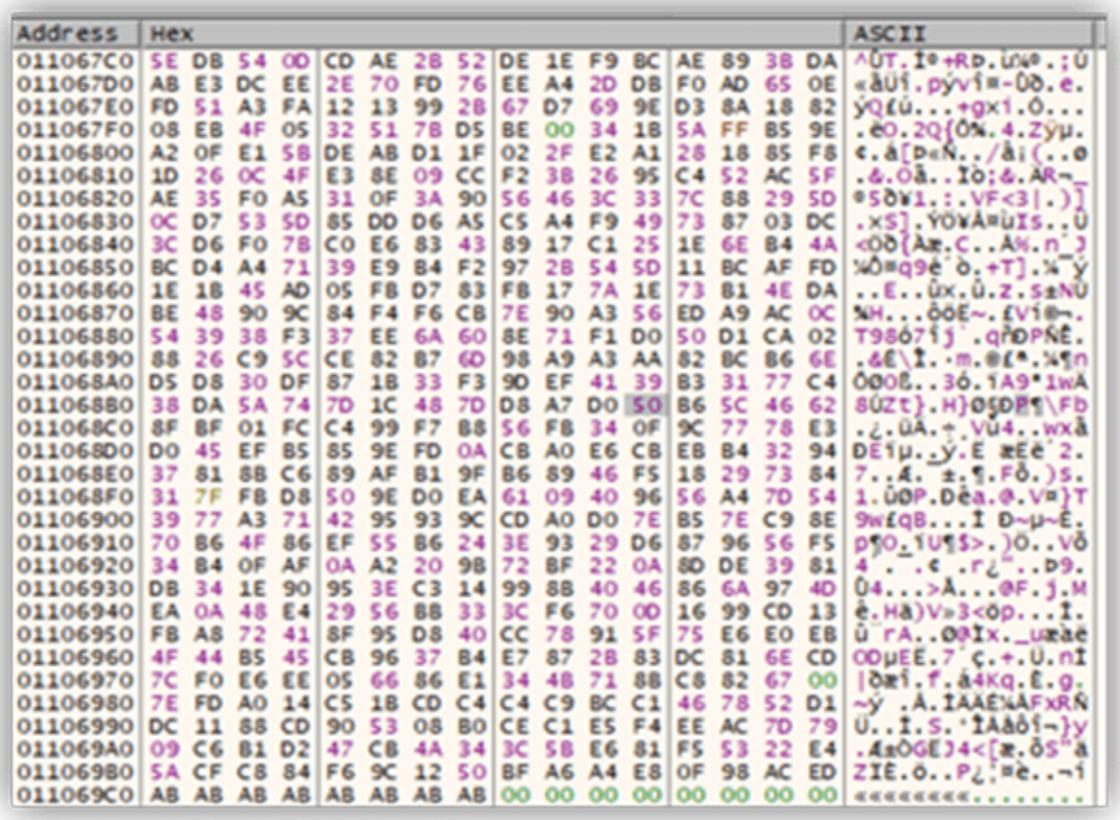
The last 8 bytes are used as the ChaCha20 nonce.



```
Address   Hex                                              ASCII
010F19C8  4D 5A F6 F6 4A 9C ED FF AB AB AB AB AB AB AB AB  MZööJ.íÿ««««««««
```

Figure 9 Nonce

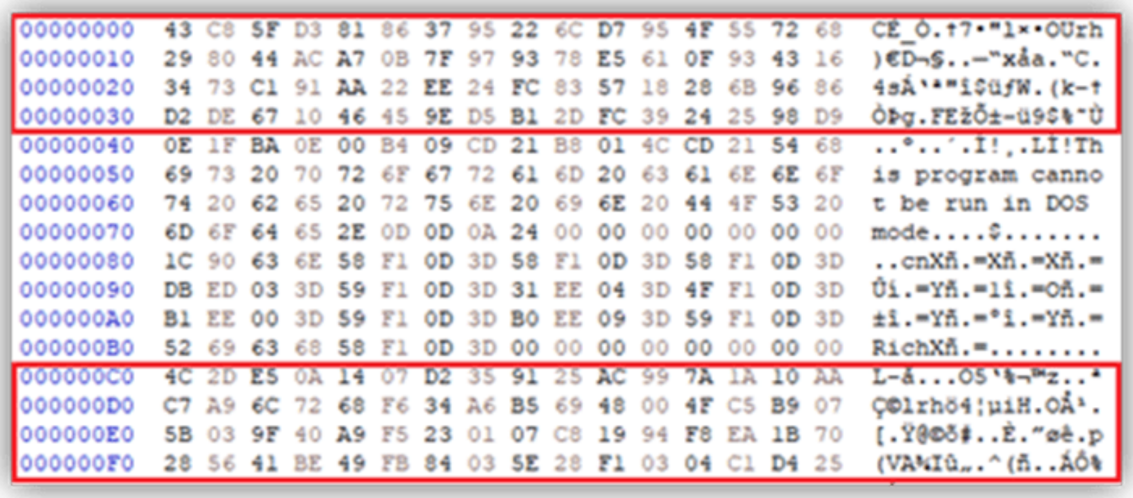
The encryption key is encrypted using an implementation of RSA provided through the Mini GMP library. A public key is obtained from the binary that results in an output similar to the below output in Figure 10.



```
Address   Hex                                                ASCII
011067C0  5E DB 54 0D CD AE 2B 52 DE 1E F9 BC AE 89 3B DA    ^ÛT.Í®+RÞ.ù¼®‰;Ú
011067D0  AB E3 DC EE 2E 70 FD 76 EE A4 2D DB F0 AD 65 0E    «ãÜî.pývî¤-Ûð.e.
011067E0  FD 51 A3 FA 12 13 99 2B 67 D7 69 9E D3 8A 18 82    ýQ£ú...+g×i.Ó...
011067F0  08 EB 4F 05 32 51 7B D5 BE 00 34 1B 5A FF B5 9E    .ëO.2Q{Õ¾.4.Zÿµ.
01106800  A2 0F E1 5B DE AB D1 1F 02 2F E2 A1 28 18 85 F8    ¢.á[Þ«Ñ../â¡(..ø
01106810  1D 26 0C 4F E3 8E 09 CC F2 3B 26 95 C4 52 AC 5F    .&.Oã..Ìò;&.ÄR¬_
01106820  AE 35 F0 A5 31 0F 3A 90 56 46 3C 33 7C 88 29 5D    ®5ð¥1.:.VF<3|.)]
01106830  0C D7 53 5D 85 DD D6 A5 C5 A4 F9 49 73 87 03 DC    .×S].ÝÖ¥Å¤ùIs..Ü
01106840  3C D6 F0 7B C0 E6 83 43 89 17 C1 25 1E 6E B4 4A    <Öð{Àæ.C..Á%.n´J
01106850  BC D4 A4 71 39 E9 B4 F2 97 2B 54 5D 11 BC AF FD    ¼Ô¤q9é´ò.+T].¼¯ý
01106860  1E 1B 45 AD 05 FB D7 83 FB 17 7A 1E 73 B1 4E DA    ..E..û×.û.z.s±NÚ
01106870  BE 48 90 9C 84 F4 F6 CB 7E 90 A3 56 ED A9 AC 0C    ¾H...ôöË~.£Ví©¬.
01106880  54 39 38 F3 37 EE 6A 60 8E 71 F1 D0 50 D1 CA 02    T98ó7îj`.qñÐPÑÊ.
01106890  88 26 C9 5C CE 82 B7 6D 98 A9 A3 AA 82 BC B6 6E    .&É\Î.·m.©£ª.¼¶n
011068A0  D5 D8 30 DF 87 1B 33 F3 9D EF 41 39 B3 31 77 C4    ÕØ0ß..3ó.ïA9³1wÄ
011068B0  38 DA 5A 74 7D 1C 48 7D D8 A7 D0 50 B6 5C 46 62    8ÚZt}.H}Ø§ÐP¶\Fb
011068C0  8F BF 01 FC C4 99 F7 B8 56 FB 34 0F 9C 77 78 E3    .¿.üÄ.÷¸Vû4..wxã
011068D0  D0 45 EF B5 85 9E FD 0A CB A0 E6 CB EB B4 32 94    ÐEïµ..ý.Ë æËë´2.
011068E0  37 81 8B C6 89 AF B1 9F B6 89 46 F5 18 29 73 84    7..Æ.¯±.¶.Fõ.)s.
011068F0  31 7F FB D8 50 9E D0 EA 61 09 40 96 56 A4 7D 54    1.ûØP.Ðêa.@.V¤}T
01106900  39 77 A3 71 42 95 93 9C CD A0 D0 7E B5 7E C9 8E    9w£qB...Í Ð~µ~É.
01106910  70 B6 4F 86 EF 55 B6 24 3E 93 29 D6 87 96 56 F5    p¶O.ïU¶$>.)Ö..Võ
01106920  34 B4 0F AF 0A A2 20 9B 72 BF 22 0A 8D DE 39 81    4´.¯.¢ .r¿"..Þ9.
01106930  DB 34 1E 90 95 3E C3 14 99 8B 40 46 86 6A 97 4D    Û4...>Ã...@F.j.M
01106940  EA 0A 48 E4 29 56 BB 33 3C F6 70 0D 16 99 CD 13    ê.Hä)V»3<öp...Í.
01106950  FB A8 72 41 8F 95 D8 40 CC 78 91 5F 75 E6 E0 EB    û¨rA..Ø@Ìx._uæàë
01106960  4F 44 B5 45 CB 96 37 B4 E7 87 2B 83 DC 81 6E CD    ODµEË.7´ç.+.Ü.nÍ
01106970  7C F0 E6 EE 05 66 86 E1 34 4B 71 8B C8 82 67 00    |ðæî.f.á4Kq.È.g.
01106980  7E FD A0 14 C5 1B CD C4 C4 C9 BC C1 46 78 52 D1    ~ý .Å.ÍÄÄÉ¼ÁFxRÑ
01106990  DC 11 88 CD 90 53 08 B0 CE C1 E5 F4 EE AC 7D 79    Ü..Í.S.°ÎÁåôî¬}y
011069A0  09 C6 B1 D2 47 CB 4A 34 3C 5B E6 81 F5 53 22 E4    .Æ±ÒGËJ4<[æ.õS"ä
011069B0  5A CF C8 84 F6 9C 12 50 BF A6 A4 E8 0F 98 AC ED    ZÏÈ.ö..P¿¦¤è..¬í
011069C0  AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00    ««««««««........
```

Figure 10 Encrypted encryption key

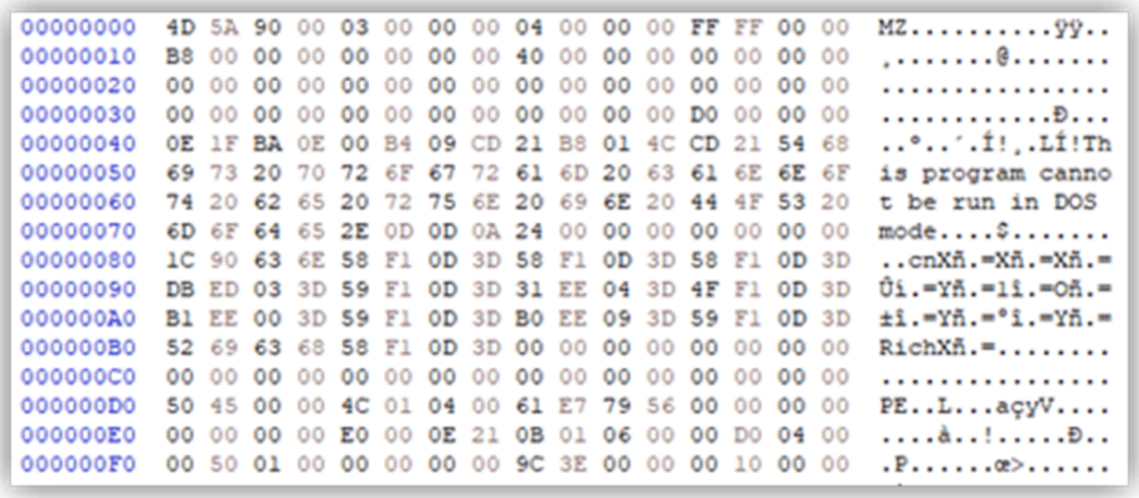
Black Basta, as with many ransomware variants, doesn't encrypt the entire file, instead only partially encrypts the file to increase the speed and efficiency of encryption. Black Basta achieves this by only encrypting 64-byte blocks of a file interspaced by 128-bytes. This can be seen in Figure 11 below, where the first two encrypted data blocks are shown.



```
00000000  43 C8 5F D3 81 86 37 95 22 6C D7 95 4F 55 72 68  CÈ_Ó.†7•"l×•OUrh
00000010  29 80 44 AC A7 0B 7F 97 93 78 E5 61 0F 93 43 16  )€D¬§..—"xåa."C.
00000020  34 73 C1 91 AA 22 EE 24 FC 83 57 18 28 6B 96 86  4sÁ'ª"î$üƒW.(k–†
00000030  D2 DE 67 10 46 45 9E D5 B1 2D FC 39 24 25 98 D9  ÒÞg.FEžÕ±-ü9$%˜Ù
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  1C 90 63 6E 58 F1 0D 3D 58 F1 0D 3D 58 F1 0D 3D  ..cnXñ.=Xñ.=Xñ.=
00000090  DB ED 03 3D 59 F1 0D 3D 31 EE 04 3D 4F F1 0D 3D  Ûí.=Yñ.=1î.=Oñ.=
000000A0  B1 EE 00 3D 59 F1 0D 3D B0 EE 09 3D 59 F1 0D 3D  ±î.=Yñ.=°î.=Yñ.=
000000B0  52 69 63 68 58 F1 0D 3D 00 00 00 00 00 00 00 00  RichXñ.=........
000000C0  4C 2D E5 0A 14 07 D2 35 91 25 AC 99 7A 1A 10 AA  L-å...Ò5'%¬™z..ª
000000D0  C7 A9 6C 72 68 F6 34 A6 B5 69 48 00 4F C5 B9 07  Ç©lrhö4¦µiH.OÅ¹.
000000E0  5B 03 9F 40 A9 F5 23 01 07 C8 19 94 F8 EA 1B 70  [.Ÿ@©õ#..È."øê.p
000000F0  28 56 41 BE 49 FB 84 03 5E 28 F1 03 04 C1 D4 25  (VA¾Iû„.^(ñ..ÁÔ%
```

Figure 11 Example encrypted file

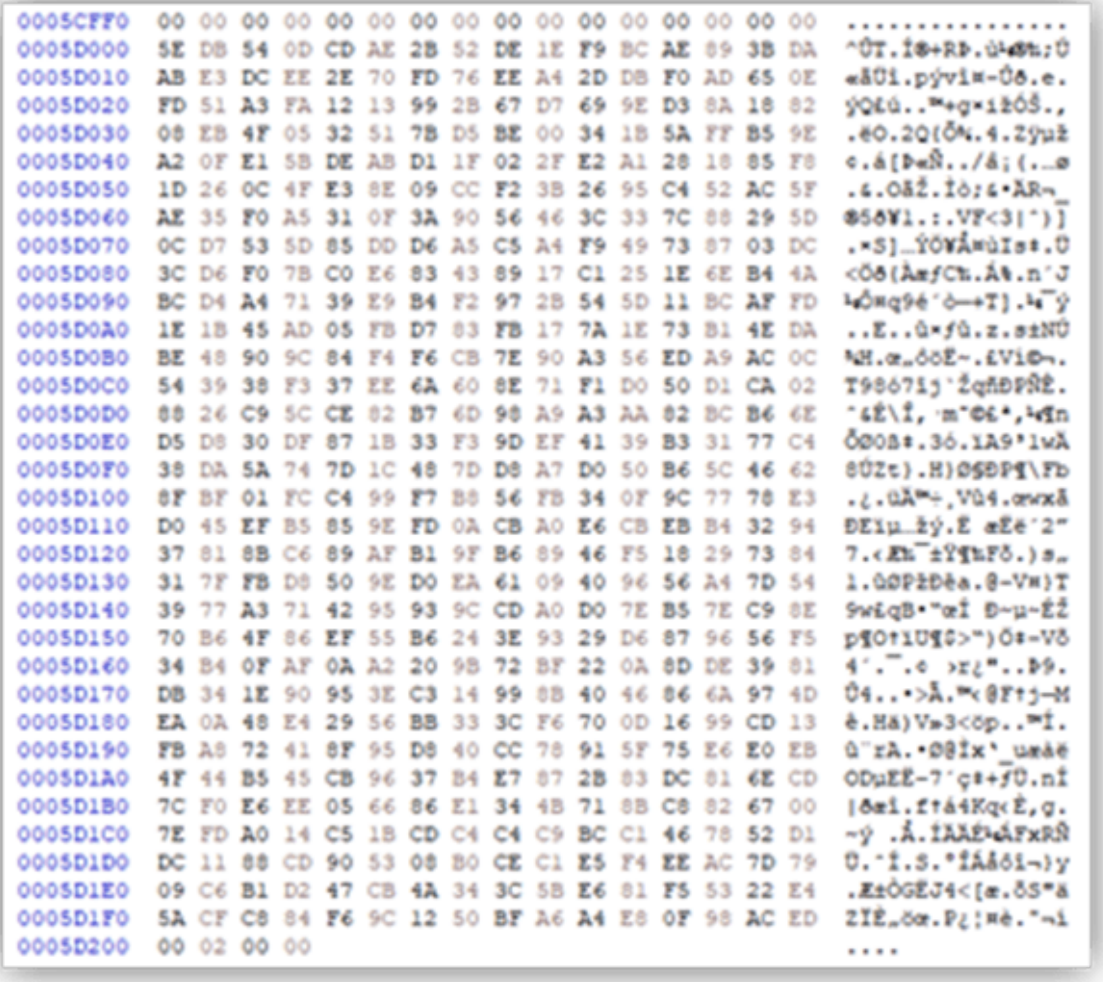
To further demonstrate this, an unencrypted version of the file can be seen below in Figure 12.



```
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 D0 00 00 00  ............Ð...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  1C 90 63 6E 58 F1 0D 3D 58 F1 0D 3D 58 F1 0D 3D  ..cnXñ.=Xñ.=Xñ.=
00000090  DB ED 03 3D 59 F1 0D 3D 31 EE 04 3D 4F F1 0D 3D  Ûí.=Yñ.=1î.=Oñ.=
000000A0  B1 EE 00 3D 59 F1 0D 3D B0 EE 09 3D 59 F1 0D 3D  ±î.=Yñ.=°î.=Yñ.=
000000B0  52 69 63 68 58 F1 0D 3D 00 00 00 00 00 00 00 00  RichXñ.=........
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  50 45 00 00 4C 01 04 00 61 E7 79 56 00 00 00 00  PE..L...açyV....
000000E0  00 00 00 00 E0 00 0E 21 0B 01 06 00 00 D0 04 00  ....à..!.....Ð..
000000F0  00 50 01 00 00 00 00 00 9C 3E 00 00 00 10 00 00  .P......œ>......
```

Figure 12 Example of the unencrypted file

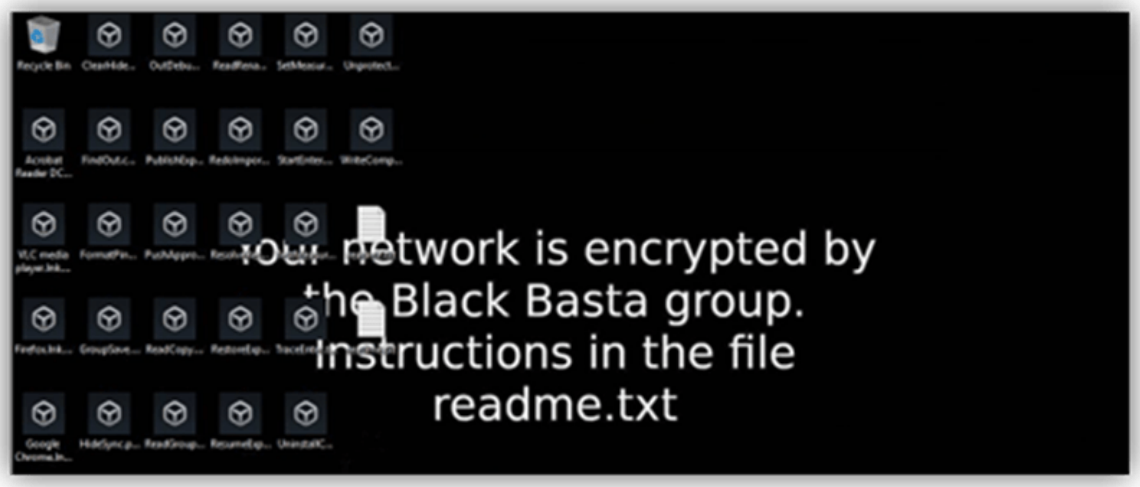
Finally, the earlier generated RSA encrypted key and 0x00020000 are appended to the end of the file, which would be used for decryption purposes.



```
0005CFF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0005D000  5E DB 54 0D CD AE 2B 52 DE 1E F9 BC AE 89 3B DA  ^ÛT.Í®+RÞ.ù¼®‰;Ú
0005D010  AB E3 DC EE 2E 70 FD 76 EE A4 2D DB F0 AD 65 0E  «ãÜî.pývî¤-Ûð.e.
0005D020  FD 51 A3 FA 12 13 99 2B 67 D7 69 9E D3 8A 18 82  ýQ£ú..™+g×ižÓŠ.‚
0005D030  08 EB 4F 05 32 51 7B D5 BE 00 34 1B 5A FF B5 9E  .ëO.2Q{Õ¾.4.Zÿµž
0005D040  A2 0F E1 5B DE AB D1 1F 02 2F E2 A1 28 18 85 F8  ¢.á[Þ«Ñ../â¡(.…ø
0005D050  1D 26 0C 4F E3 8E 09 CC F2 3B 26 95 C4 52 AC 5F  .&.OãŽ.Ìò;&•ÄR¬_
0005D060  AE 35 F0 A5 31 0F 3A 90 56 46 3C 33 7C 88 29 5D  ®5ð¥1.:.VF<3|ˆ)]
0005D070  0C D7 53 5D 85 DD D6 A5 C5 A4 F9 49 73 87 03 DC  .×S]…ÝÖ¥Å¤ùIs‡.Ü
0005D080  3C D6 F0 7B C0 E6 83 43 89 17 C1 25 1E 6E B4 4A  <Öð{ÀæƒC‰.Á%.n´J
0005D090  BC D4 A4 71 39 E9 B4 F2 97 2B 54 5D 11 BC AF FD  ¼Ô¤q9é´ò—+T].¼¯ý
0005D0A0  1E 1B 45 AD 05 FB D7 83 FB 17 7A 1E 73 B1 4E DA  ..E..û×ƒû.z.s±NÚ
0005D0B0  BE 48 90 9C 84 F4 F6 CB 7E 90 A3 56 ED A9 AC 0C  ¾H.œ„ôöË~.£Ví©¬.
0005D0C0  54 39 38 F3 37 EE 6A 60 8E 71 F1 D0 50 D1 CA 02  T98ó7îj`ŽqñÐPÑÊ.
0005D0D0  88 26 C9 5C CE 82 B7 6D 98 A9 A3 AA 82 BC B6 6E  ˆ&É\Î‚·m˜©£ª‚¼¶n
0005D0E0  D5 D8 30 DF 87 1B 33 F3 9D EF 41 39 B3 31 77 C4  ÕØ0ß‡.3ó.ïA9³1wÄ
0005D0F0  38 DA 5A 74 7D 1C 48 7D D8 A7 D0 50 B6 5C 46 62  8ÚZt}.H}Ø§ÐP¶\Fb
0005D100  8F BF 01 FC C4 99 F7 B8 56 FB 34 0F 9C 77 78 E3  .¿.üÄ™÷¸Vû4.œwxã
0005D110  D0 45 EF B5 85 9E FD 0A CB A0 E6 CB EB B4 32 94  ÐEïµ…žý.Ë æËë´2”
0005D120  37 81 8B C6 89 AF B1 9F B6 89 46 F5 18 29 73 84  7.‹Æ‰¯±Ÿ¶‰Fõ.)s„
0005D130  31 7F FB D8 50 9E D0 EA 61 09 40 96 56 A4 7D 54  1.ûØPžÐêa.@–V¤}T
0005D140  39 77 A3 71 42 95 93 9C CD A0 D0 7E B5 7E C9 8E  9w£qB•“œÍ Ð~µ~ÉŽ
0005D150  70 B6 4F 86 EF 55 B6 24 3E 93 29 D6 87 96 56 F5  p¶O†ïU¶$>“)Ö‡–Võ
0005D160  34 B4 0F AF 0A A2 20 9B 72 BF 22 0A 8D DE 39 81  4´.¯.¢ ›r¿"..Þ9.
0005D170  DB 34 1E 90 95 3E C3 14 99 8B 40 46 86 6A 97 4D  Û4..•>Ã.™‹@F†j—M
0005D180  EA 0A 48 E4 29 56 BB 33 3C F6 70 0D 16 99 CD 13  ê.Hä)V»3<öp..™Í.
0005D190  FB A8 72 41 8F 95 D8 40 CC 78 91 5F 75 E6 E0 EB  û¨rA.•Ø@Ìx‘_uæàë
0005D1A0  4F 44 B5 45 CB 96 37 B4 E7 87 2B 83 DC 81 6E CD  ODµEË–7´ç‡+ƒÜ.nÍ
0005D1B0  7C F0 E6 EE 05 66 86 E1 34 4B 71 8B C8 82 67 00  |ðæî.f†á4Kq‹È‚g.
0005D1C0  7E FD A0 14 C5 1B CD C4 C4 C9 BC C1 46 78 52 D1  ~ý .Å.ÍÄÄÉ¼ÁFxRÑ
0005D1D0  DC 11 88 CD 90 53 08 B0 CE C1 E5 F4 EE AC 7D 79  Ü.ˆÍ.S.°ÎÁåôî¬}y
0005D1E0  09 C6 B1 D2 47 CB 4A 34 3C 5B E6 81 F5 53 22 E4  .Æ±ÒGËJ4<[æ.õS"ä
0005D1F0  5A CF C8 84 F6 9C 12 50 BF A6 A4 E8 0F 98 AC ED  ZÏÈ„öœ.P¿¦¤è.˜¬í
0005D200  00 02 00 00                                      ....
```

Figure 13 appended encrypted key and hex

Following successful encryption of a file, its extension is changed to .basta which automatically adjusts its icon to the earlier drop icon file. An example of what a victim would be presented with can be seen below in Figure 14.



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

Figure 14 example post encrypted desktop

While the ransom note threatens victims with the publication of data if the ransom is not met, initial analysis has not uncovered a mechanism for exfiltration. With access to the private key counterpart of the public key used earlier, recovery of the ChaCha20 encryption key by operators should be possible allowing for file decryption. No weakness in the encryption was discovered during analysis that would provide an opportunity for decryption without the private RSA key.