Shining the Light on Black Basta

06 June 2022 By RIFT: Research and Intelligence Fusion Team

Research Threat Intelligence Digital Forensics and Incident Response (DFIR)

This research was conducted by **Ross Inman** (@rdi_x64) and **Peter Gurney** from NCC Group Cyber Incident Response Team. You can find more here Incident Response – NCC Group

Summa

tl;dr

This blog post documen loying Black Basta ransomware during a r file which performs the encryption.

A summary of the findi

- Lateral movement thro
- Gathering internal IP ac
- Disabling Windows Def
- Deleting Veeam backup
- Use of WMI to push out
- Technical analysis of th

Black Basta

Black Basta are a ranso s occurring in April this year. As is popular with ta is first exfiltrated from the network befor on the "Black Basta Blog" or "Basta News" T and one which the victims can use to cont hich is dropped by the ransomware executabl

Black Ba

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 \SYSVOL\.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 "HKLMSystemCurrentControlSetControlTerminal 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 "HKLMSystemCurrentControlSetControlTerminal ServerWinStationsRDP-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:SOFTWAREPoliciesMicrosoftWindows 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\M
DisableRealtimeMoni
DWORD:1

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


Discovery

A text file in the C:Windo ers, both contained a list of internal IP addres list of IP addresses to target when deploying t

Command a

Qakbot was the primary . The threat actor was also observed using Co

Impact

Prior to the deploymen ers and from there modified configurations hines.

An encoded PowerShel h, 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:Windowspc_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

- 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.
- 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.
- 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:WindowsPsExec.exe	Filename	PsExec
C:WindowsSYSVOLsysvol.dll	Filename	Qakbot payload
C:WindowsTemplog.info C:WindowsTemplog.dat	Filename	Invoke-TotalExec output log files

Ransomware Technical Analysis

Shadow Copy Deletion

Upon execution, Black B

The Mutex 'dsajdhas.0' gh the Mutex is static in this sample it is expecte

```
C:\Windows\SysNative\vss
C:\WindowsSystem32\vssad
```

These result in the dele

Wallpaper i

Following deletion of th currently analysed sample is saved as 'dlak en below in Figure 2.

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 `HKCUControl PanelDesktopWallpaper`, setting the path to the JPG as seen below in Figure 4.

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.

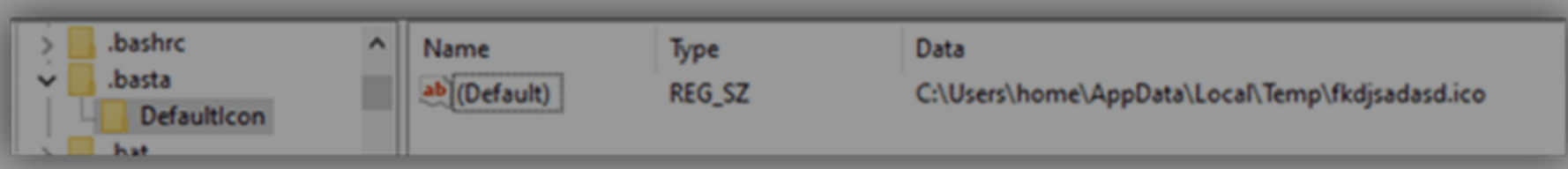
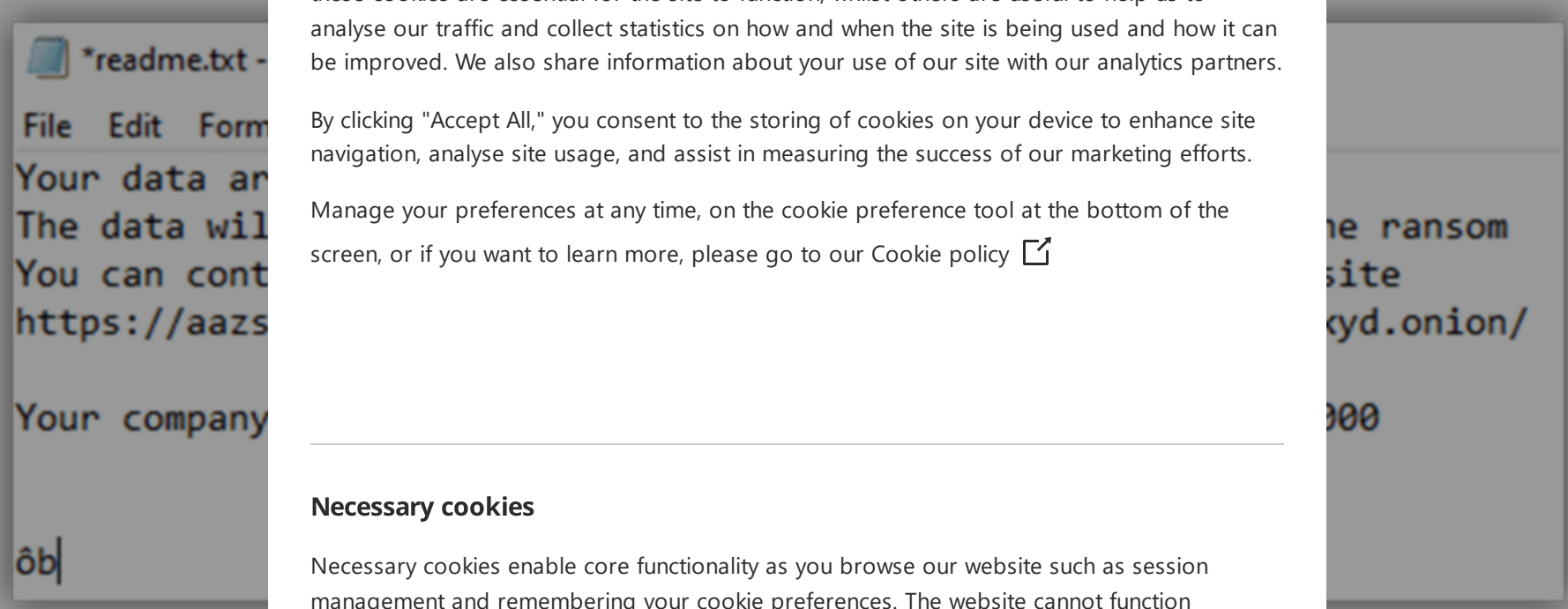


Figure 5 Desktop wallpaper image

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 nego

A company ID is also pr



Exclusions

In an attempt to avoid e machine or Black Basta itself, several exclusions nsions, 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.

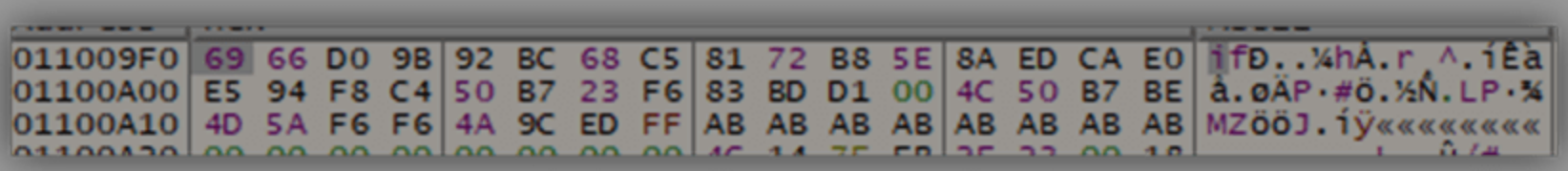
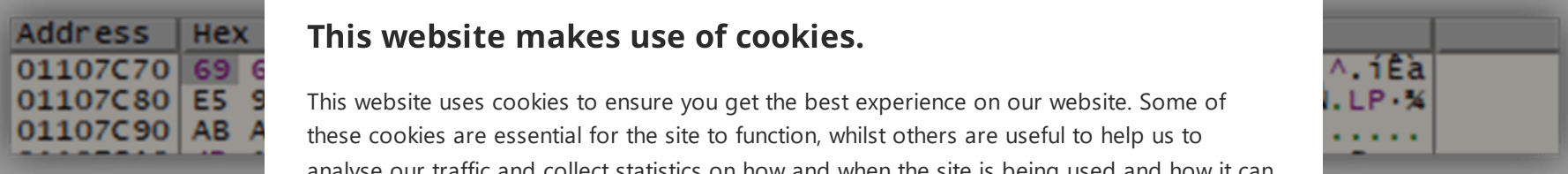
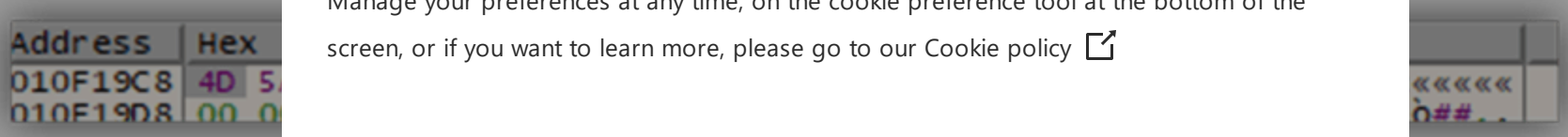


Figure 7 Random generation output

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



The last 8 bytes are use



The encryption key is e y. A public key is obtained from the bina

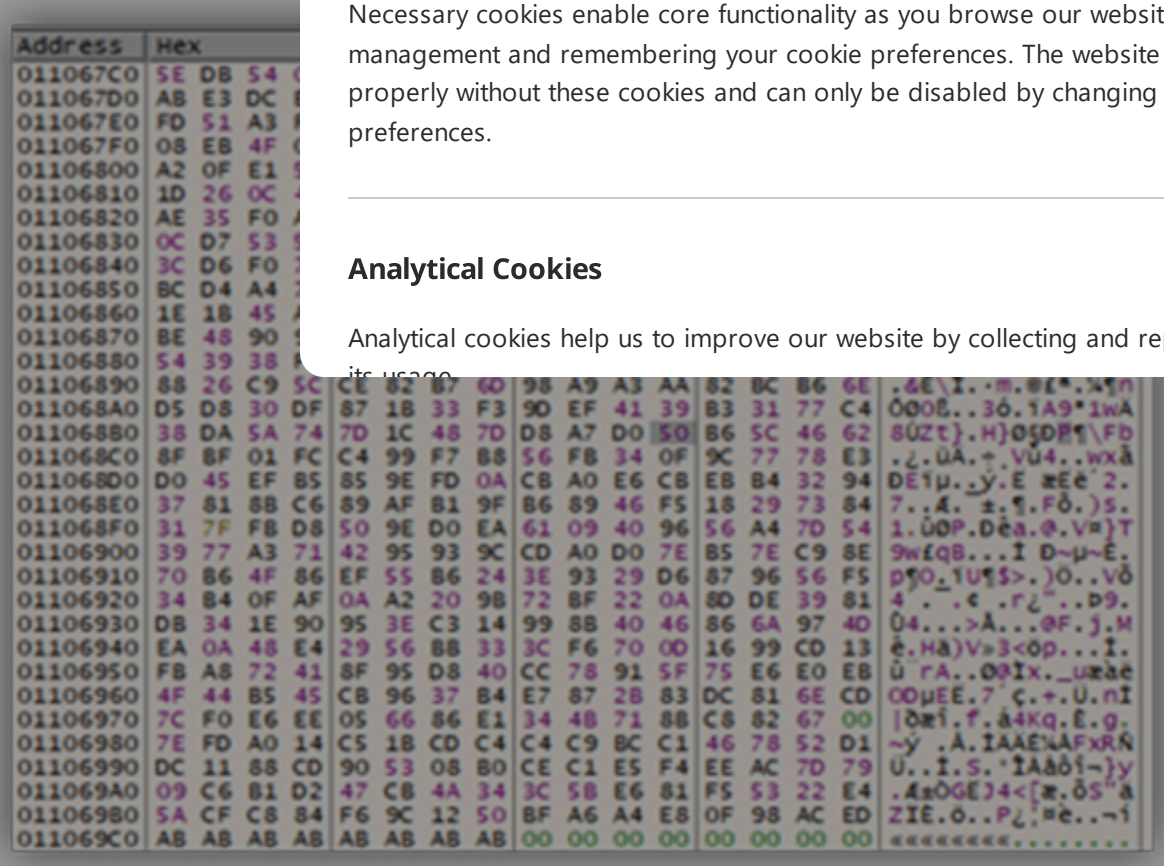


Figure 10 Encrypted encryption key

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.

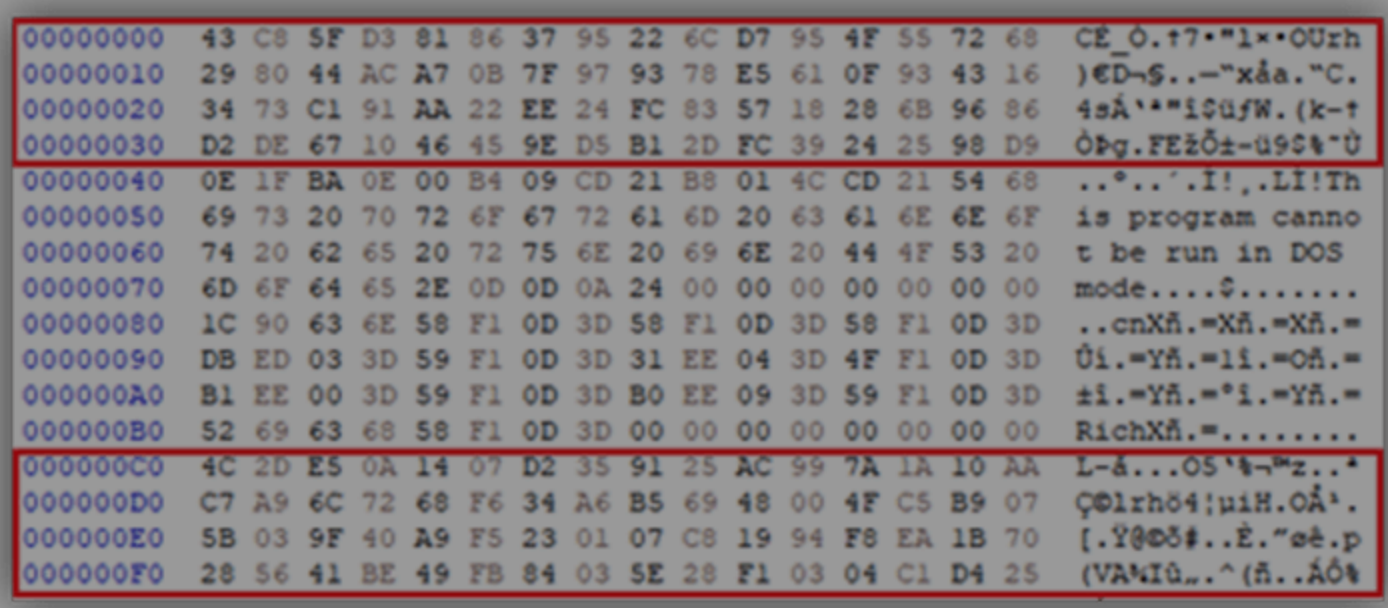
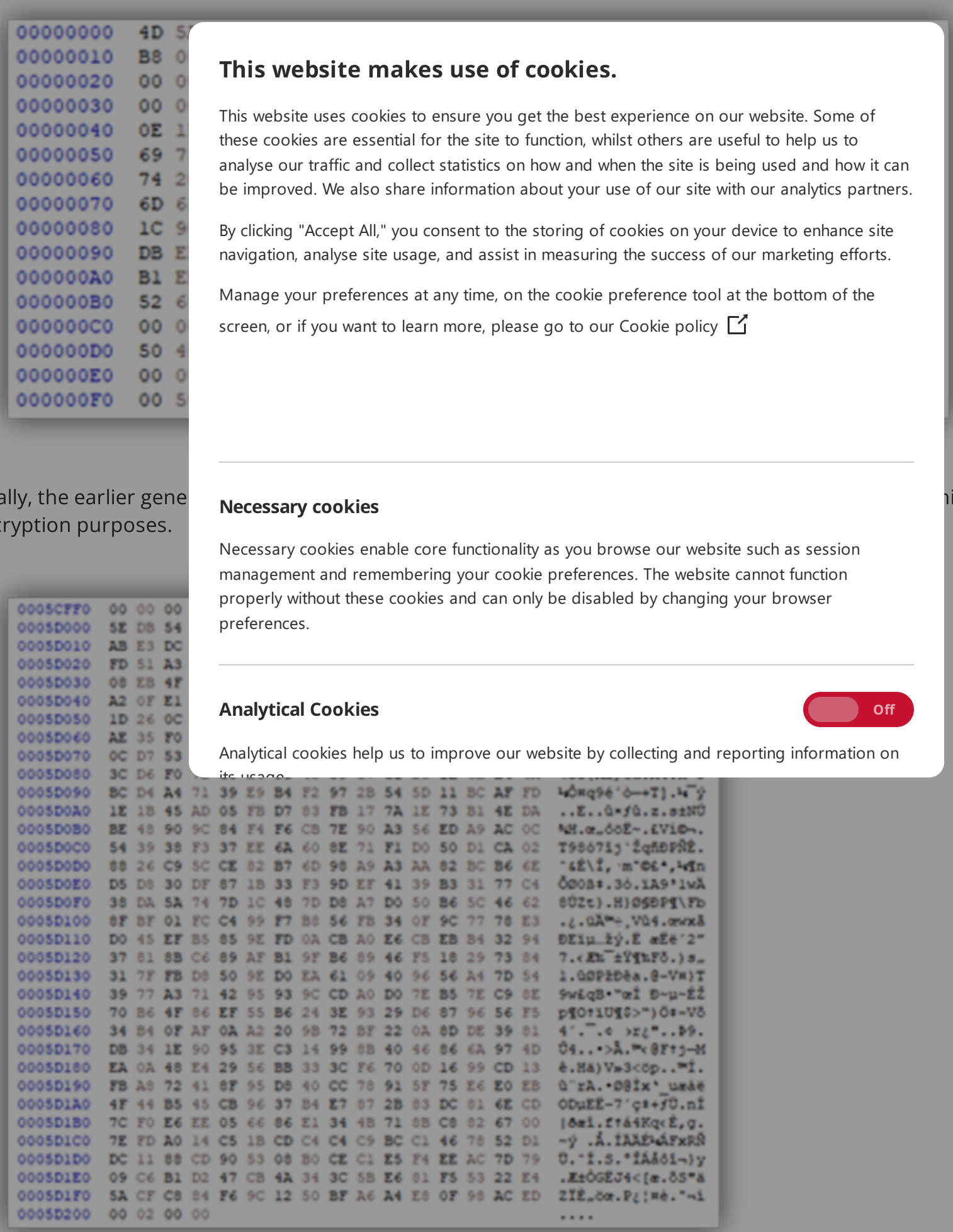


Figure 11 Example encrypted file

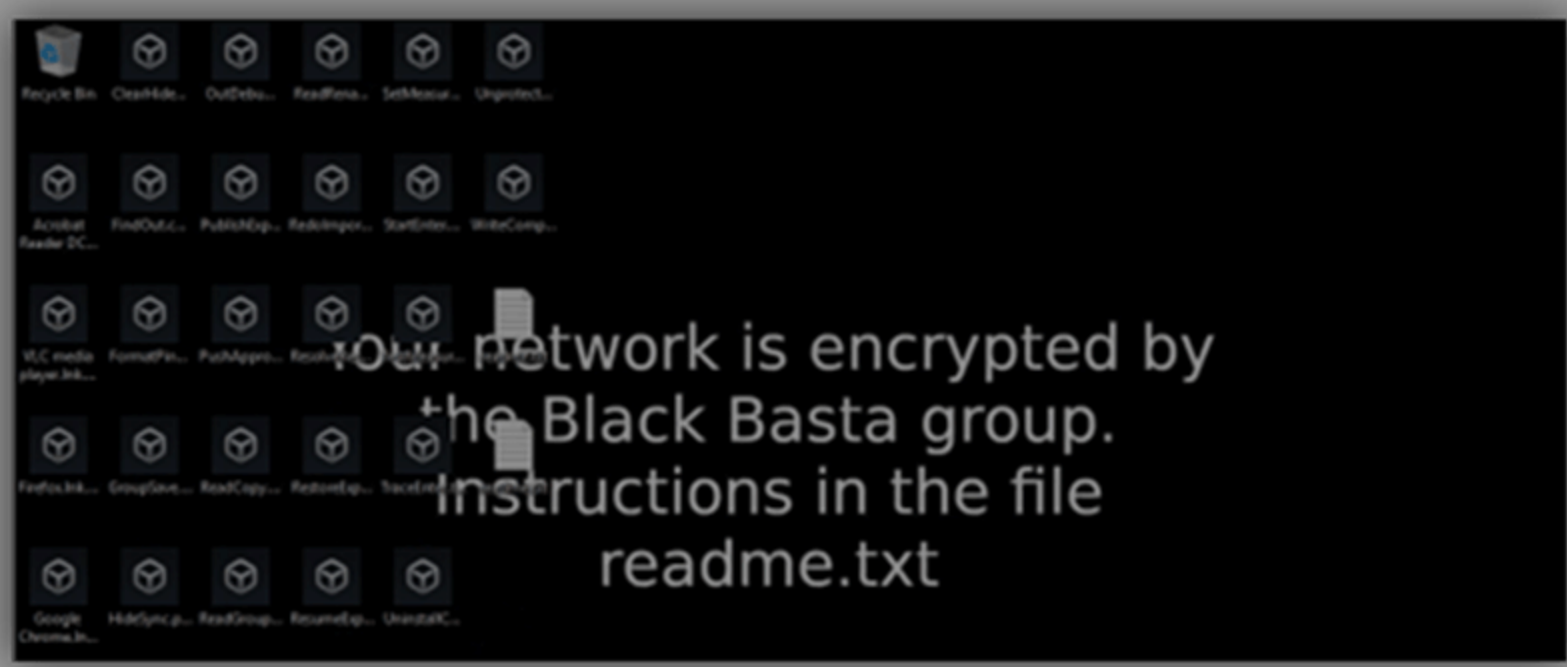
To further demonstrate this, an unencrypted version of the file can be seen below in Figure 12.



Finally, the earlier gene ich would be used for decryption purposes.

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.



While the ransom note alysis has not
uncovered a mechanism ed earlier, recovery of
the ChaCha20 encryptio s in the encryption was
discovered during analy ey.

NCC Group Incident Re ncident handling,
triage and analysis, al

unting capabilities to
ection capabilities to
ity is an arms race
prove their tools and
effective against the
Fox-IT at its core. This
gence into powerful

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.