

**∨** US

 $\otimes$ 

కి Client login



Cyber Security ▶ Research Blog

# Shining the Light on Black Basta

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 docume ransomware during a r encryption.

A summary of the findir

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

# **Black Basta**

Black Basta are a ranso year. As is popular with from the network befor Blog" or "Basta News" T victims can use to cont ransomware executable

### 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

Accept all cookies

Reject all cookies

### **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**

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

s occurring in April this ta is first exfiltrated on the "Black Basta and one which the nich is dropped by the

loying Black Basta

file which performs the

# Black Ba

# Off

# **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:



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 🔟

# Discovery

DisableRealtimeMoni

PARSING COMPLETED

DWORD:1

A text file in the C:Wind list of internal IP addres target when deploying

# Command

Qakbot was the primary also observed using Co

# **Impact**

Prior to the deploymen modified configurations

An encoded PowerShel

### **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**

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

ers and from there nines.

ers, both contained a

list of IP addresses to

The threat actor was

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

# **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 I

The Mutex 'dsajdhas.0' this sample it is expected

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

These result in the dele

# Wallpaper i

Following deletion of th sample is saved as 'dlak

### This website makes use of cookies.

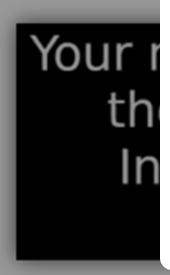
This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share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

h the Mutex is static in

currently analysed en below in Figure 2.



### **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

### 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:

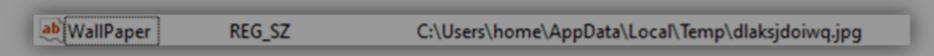
C:\Users\{Username}\AppData\Local\Temp

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.

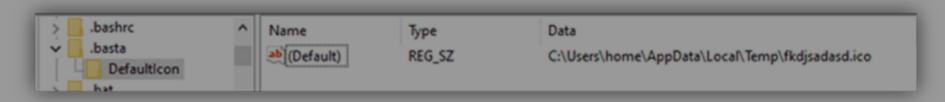


Figure 5 Desktop wallpaper image

### **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

# \*readme.txtFile Edit Form Your data and The data will You can conto https://aazs Your company

### 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

ne ransom site kyd.onion/

900

Off

### **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.

# **Exclusions**

In an attempt to avoid eitself, several exclusions files listed below.

### **Analytical Cookies**

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

nachine or Black Basta ensions, folders and

### 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.

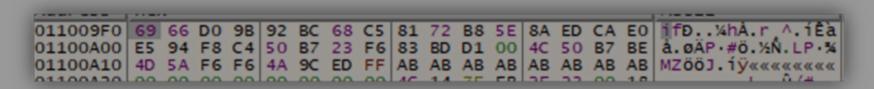


Figure 7 Random generation output

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

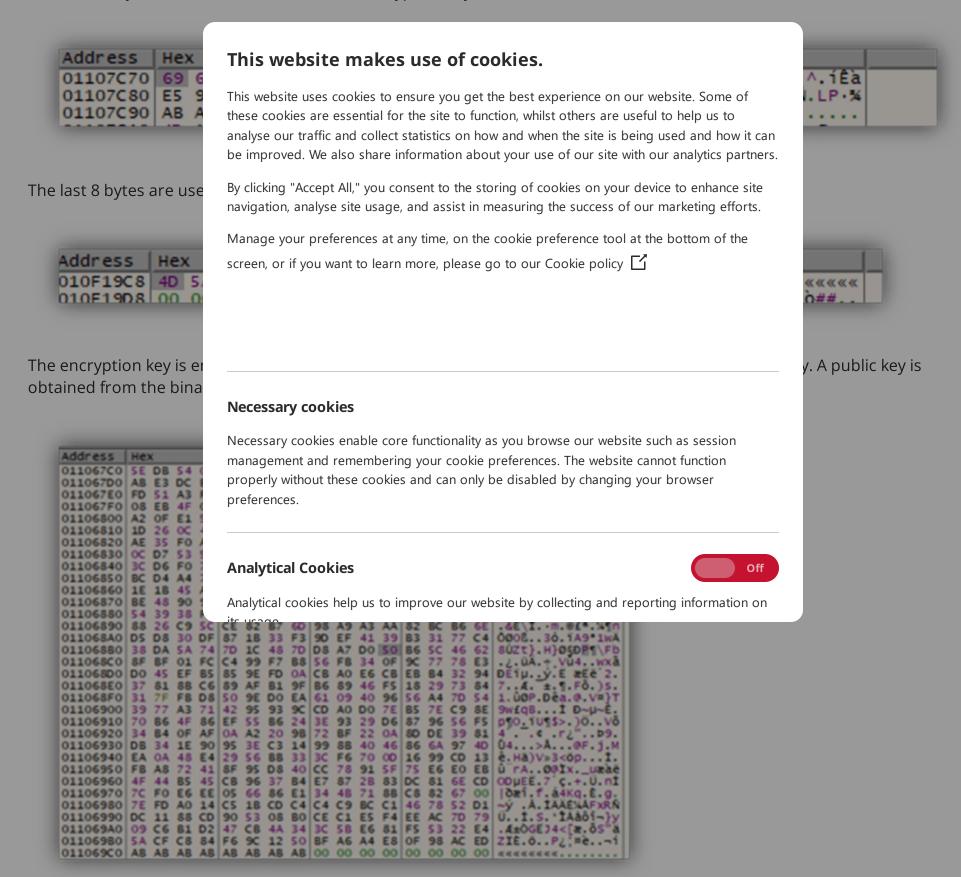


Figure 10 Encrypted encryption key

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
                                                            CÉ 0. †7 * "1 × • OUrh
                                                            ) €D-$ . . - "xåa . "C .
00000010
          29 80 44 AC A7 0B 7F 97 93 78 E5 61
                                              OF
                                                 93
                                                            4sA *** 1$UfW. (k-t
00000020
         34 73 C1 91 AA 22 EE 24 FC 83 57 18 28 6B 96 86
          D2 DE 67 10 46 45 9E D5 B1
                                     2D FC 39
                                                            OÞg.FEŽO±-ü9$%~Ü
00000040
                BA OE 00 B4 09 CD 21 B8 01
                                           4C
                                              CD 21 54 68
                                                            ..°..'.I!..LI!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61
                                                 6E 6E 6F
                                                            is program canno
         74 20 62 65 20 72 75 6E 20 69 6E 20 44
00000060
                                                 4 F
                                                     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.=
                                                            Ûi.=Yň.=1î.=Oň.=
00000090 DB ED 03 3D 59 F1 0D 3D 31 EE 04 3D 4F F1 0D 3D
0000000A0 B1 EE 00 3D 59 F1 0D 3D B0 EE 09 3D 59
                                                 F1 0D 3D
                                                            ±1.=Yñ.=°1.=Yñ.=
                                              00 00 00 00
000000B0
          52 69 63 68 58 F1 OD 3D 00 00 00
                                                            RichXň.=....
000000C0 4C 2D E5 0A 14 07 D2 35 91 25 AC 99
                                                            L-á...05 \%-12...
000000D0 C7 A9 6C 72 68 F6 34 A6 B5 69 48 00 4F C5 B9 07
                                                            Ç@lrhö4;uiH.OA1.
                                                            [.Y@@o#..E."se.p
000000E0 5B 03 9F 40 A9 F5 23 01 07 C8 19 94 F8 EA 1B 70
000000F0 28 56 41 BE 49 FB 84 03 5E 28 F1 03 04 C1 D4 25
                                                            (VA%Iû,.^(ñ..ÁŐ%
```

Figure 11 Example encrypted file

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

### 00000000 4D 5 00000010 B8 0 This website makes use of cookies. 00 0 00000020 00000030 00 0 00000040 0E 1 00000050 69 7 00000060 74 2 00000070 6D 6 00000080 1C 9 00000090 DB E 000000A0 B1 E 52 6 000000B0 00 0 000000C0 000000D0 50 4 00 0 000000E0 000000F0 00 5

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

Finally, the earlier gene decryption purposes.

0005CFF0 00 00 00

0005D000 5E DB 54 0005D010 AB E3 DC 0005D020 FD 51 A3 0005D030 08 E8 4F 0005D040 A2 OF E1

0005D050 1D 26 0C 0005D060 AE 35 FO

0005D070 0C D7 53 0005D080 3C D6 F0

### **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

nich would be used for

0005D090 BC D4 A4 71 39 E9 B4 F2 97 28 54 5D 11 BC AF FD 40xq96 0-+T] 4 9

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

0005D0A0 1E 18 45 AD 05 F8 D7 83 FB 17 7A 1E 73 81 4E DA ..E..@-f@.z.s±NO 0005D0B0 BE 48 90 90 84 F4 F6 CB 7E 90 A3 56 ED A9 AC OC NH.œ..óŏE~.£Vi₽~. 0005D0C0 54 39 38 F3 37 EE 6A 60 8E 71 F1 D0 50 D1 CA 02 T986715 ZghbPNE. "42\1, 'm"OE\*, 141n 0005D0D0 88 26 C9 50 CE 82 B7 6D 98 A9 A3 AA 82 B0 B6 6E 0005D0E0 D5 D8 30 DF 87 18 33 F3 9D EF 41 39 B3 31 77 C4 0008:.36.1A9'1WA 0005D0F0 38 DA 5A 74 7D 10 48 7D D8 A7 D0 50 B6 50 46 62 8ÚZt).H)@SDP¶\Fb 0005D100 8F BF 01 FC C4 99 F7 B8 56 FB 34 0F 9C 77 78 E3 .¿.QA-+,VQ4.owxā 0005D110 DO 45 EF 85 85 9E FD OA CB AO E6 CB EB 84 32 94 ĐENH ŽÝ.E æ£ë'2" 0005D120 37 81 88 C6 89 AF 81 9F 86 89 46 F5 18 29 73 84 0005D130 31 7F F8 D8 50 9E D0 EA 61 09 40 96 56 A4 7D 54 7. (Eh ± 24hFo.) 5. 1.GSPžDěa.8-Vm)T 0005D140 39 77 A3 71 42 95 93 90 CD A0 D0 7E B5 7E C9 8E 9wiqB. "@I D-p-22 0005D150 70 B6 4F 86 EF 55 B6 24 3E 93 29 D6 87 96 56 F5 p40+1U40>") 0 = - V8 0005D160 34 84 OF AF OA A2 20 98 72 8F 22 OA 8D DE 39 81 4'.".0 >rt"..b9. 0005D170 D8 34 1E 90 95 3E C3 14 99 88 40 46 86 6A 97 4D 04...>A. \* @Ffj-M 0005D180 EA 0A 48 E4 29 56 BB 33 3C F6 70 0D 16 99 CD 13 0005D190 FB A8 72 41 8F 95 D8 40 CC 78 91 5F 75 E6 E0 EB è.Hä)V≫3<öp..™1. Q"rA. . DSIx'\_umaë 0005D1A0 4F 44 B5 45 CB 96 37 B4 E7 87 2B 83 DC 81 6E CD ODuEE-7'cs+f0.ni 0005D1B0 7C F0 E6 EE 05 66 86 E1 34 4B 71 8B C8 82 67 00 |8mi.ftá4KgcE,g. ~9 .A.IAAELAFXRN 0005D1C0 7E FD A0 14 C5 18 CD C4 C4 C9 BC C1 46 78 52 D1 0005D1D0 DC 11 88 CD 90 53 08 80 CE C1 E5 F4 EE AC 7D 79 U. 1.S. "IÁA61-)y 0005D1E0 09 C6 B1 D2 47 C8 4A 34 3C 58 E6 81 F5 53 22 E4 0005D1F0 5A CF C8 84 F6 9C 12 50 BF A6 A4 E8 0F 98 AC ED . £±0GEJ4<[æ.öS\*ä ZIE"čœ.P¿; #è. ~~i 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.



While the ransom note uncovered a mechanism the ChaCha20 encryption discovered during analysis.

NCC Group Incident Retriage and analysis, al.

### 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

alysis has not ed earlier, recovery of in the encryption was

ncident handling,

### **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.

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

### **Analytical Cookies**

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

ite us





Terms and Conditions

uccdlont

**Privacy Policy** 

Contact Us

Technical Assurance

Consulting & Implementation

**Managed Services** 

Incident Response

Threat Intelligence

Get in Touch

+1-(415)-268-9300

24/7 Incident Response Hotline

Off

+1-(855)-684-1212 or cirt@nccgroup.com

© NCC Group 2024. All rights reserved.

### 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**



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