

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](#)

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 double-extortion 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.

Bla Late

Black Bas
after thei

- PsExec.e
- Qakbot w
- configure
- regsvr32
- RDP alon
- enable RI
- on comp
- reg add
- "fDenyTs
- net star
- netsh ac
- reg add
- "UserAut

Defe

During th
anti-virus
Defender

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.

network

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

ines to
sessions

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.

cp" /v

Analytical Cookies



ce from

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

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 m
; -----
; PARSI
; Sourc

Comput
Softwar
Disabl
DWORD:1


Comput
Softwar
Disabl
DWORD:1

; PARSI
; -----
```

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

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

Disc

A text file
Controller
was to su
ransomw

Com



omain
rk. This

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 was observed to be executed on a Hyper-V server, likely to the IP address 10.10.10.10, and the results were saved to a file named 'results.txt'.

two log files

- C:\Windows
 - C:\Windows
- For the infected Hyper-V server, the file contained the three log files, the three network servers and

Recc

- Hypervisors workgroup reside dc
- Ensure the identify a
- Restrict i these pro

Indic

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.

IOC Value		
23.106		
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:Windows C:Windows		Output

Rail And Shac

Upon execution of these activities

The Mute Switch is Although

C:\Windows
C:\Windows

These results are for purposes


Wall

Following the investigation in the current devices.

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](#) 

1

below.
5.

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.



JPG file
geted

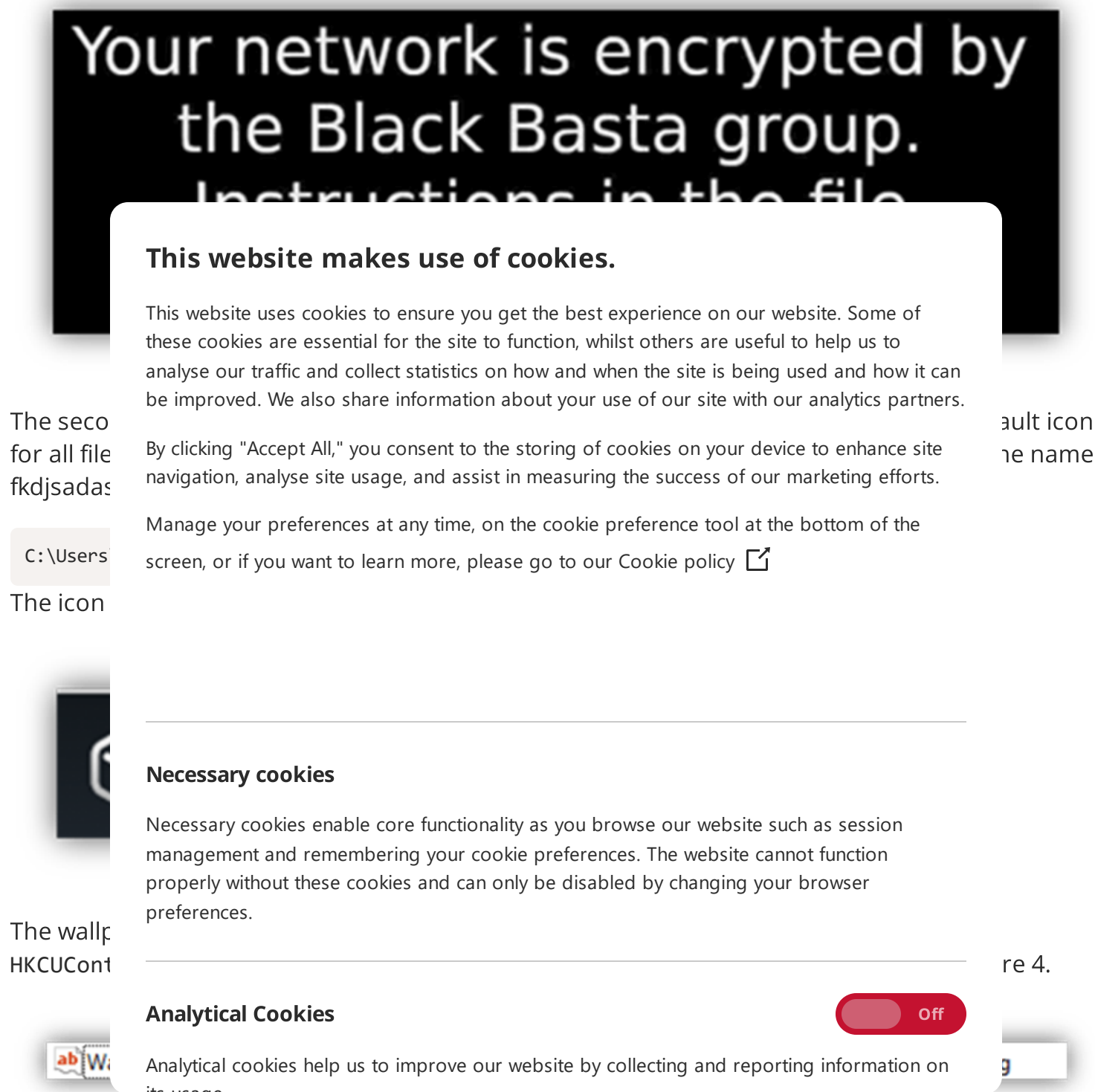


Figure 4 String de-obfuscation example

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.

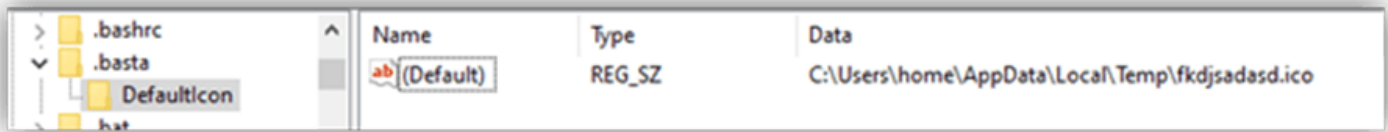


Figure 5 Desktop wallpaper image

Ransom Note

The ransom note is shown in the standard operator interface.

A 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](#)

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 target malicious specific file extensions:

Analytical Cookies

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




of the
typing

Extension exclusions:

- .exe
- .cmd
- .bat
- .com

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

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.

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 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.

Off

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

only
achieves
in

```
00000000 43 C8 5F D3 81 86 37 95 22 6C D7 95 4F 55 72 68 CE 0. +7.*1x.OUrh
00000010 29 80 44 AC A7 0B 7F 97 93 78 E5 61 0F 93 43 16 )eD-S...-xaa."C.
00000020 34 73 C1 91 AA 22 EE 24 FC 83 57 18 28 6B 96 86 4sA'*=i0ufW. (k-t
00000030 D2 DE 67 10 46 45 9E D5 B1 2D FC 39 24 25 98 D9 00g.FEz0+-u90t-U
00000040 0E 1F BA 0E 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
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
```

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.

☐ Off

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 .....
0005D000 5E DB 54 0D CD AE 2B 52 DE 1E F9 BC AE 89 3B DA ^0T.i8+Rb.0+8t;0
0005D010 AB E3 DC EE 2E 70 FD 76 EE A4 2D DB F0 AD 65 0E e&0i.pyvi=-08.e.
0005D020 FD 51 A3 FA 12 13 99 2B 67 D7 69 9E D3 8A 18 82 yQtd.."+q=i20S.,
0005D030 08 EB 4F 05 32 51 7B D5 BE 00 34 1B 5A FF B5 9E .e0.2Q(0%4.2ypu
0005D040 A2 0F E1 5B DE AB D1 1F 02 2F E2 A1 28 18 85 F8 e.&[p=8.../8;(.e
0005D050 1D 26 0C 4F E3 8E 09 CC F2 3B 26 95 C4 52 AC 5F .&.0&2.i0;4*AR=
0005D060 AE 35 F0 A5 31 0F 3A 90 56 46 3C 33 7C 88 29 5D 858Vl.:.VF<3[~)]
0005D070 0C D7 53 5D 85 DD D6 35 C6 34 F6 49 73 87 03 DC .e1 40viamat.e.0
```

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](#) 

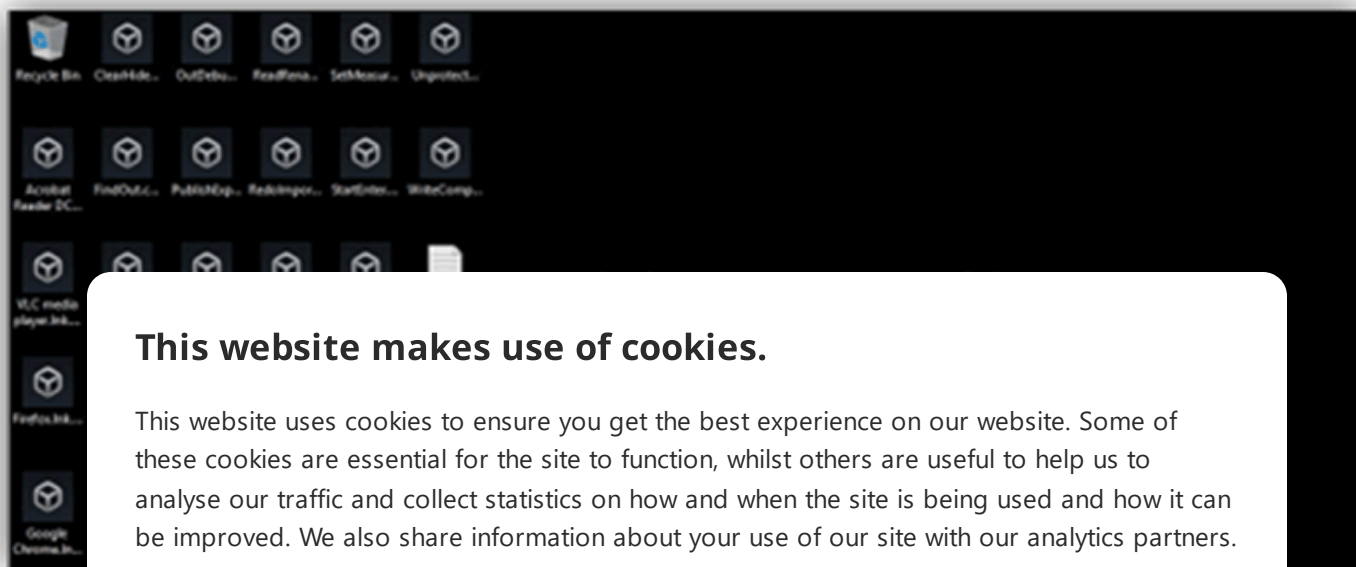
Necessary cookies

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.






While the initial and counterparty should be during ar

NCC Gro through guidance

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](#) 

met,
e key
operators
ered
A key.

you
mediation

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.



e, and
great
abilities
ape.

Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading

cyber threat intelligence into powerful detection strategies.



Terms and

Privacy Policy

Contact Us


Hotline

© NCC Group

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.