ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL:	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1
Full analysis:	https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a
Verdict:	Suspicious activity
Analysis date:	June 29, 2023 at 18:56:12
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MD5:	7CD193E2B99F15030CA538B924B4498C
SHA1:	07A04D3C4279FFFE62968A4F76133B1AC71B490F
SHA256:	3B9E727C56BFA9A16E5311F8D17472B9DCBE2F1E149FA2924EDA013611076D39
SSDEEP:	3:N8tMCMEd2NMOYVVqJS3ERXM7JUqET+hdSadtSXG2dzKhYMN:21MEgNMOYVlUOadyfjSNWYMN

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)

Hotfixes

- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Maintenance Service (83.0.0.7621)
- Mozilla Maintenance Service (83.0.0.7621)
- Notepad++ (32-bit x86) (7.9.1)
- Notepad++ (32-bit x86) (7.9.1)
- Opera 12.15 (12.15.1748)
- Opera 12.15 (12.15.1748)
- Skype version 8.29 (8.29)
- Skype version 8.29 (8.29)
- VLC media player (3.0.11)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- WinRAR 5.91 (32-bit) (5.91.0)

Behavior activities

MALICIOUS

Bypass execution policy to execute commands
- powershell.exe (PID: 3300)

SUSPICIOUS

The process executes Powershell scripts
- powershell.exe (PID: 2272)

INFO

Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

The process bypasses the loading of PowerShell profile settings
- powershell.exe (PID: 2272)

Reads the Internet Settings
- powershell.exe (PID: 2272)
- powershell.exe (PID: 3300)

Application launched itself
- powershell.exe (PID: 2272)

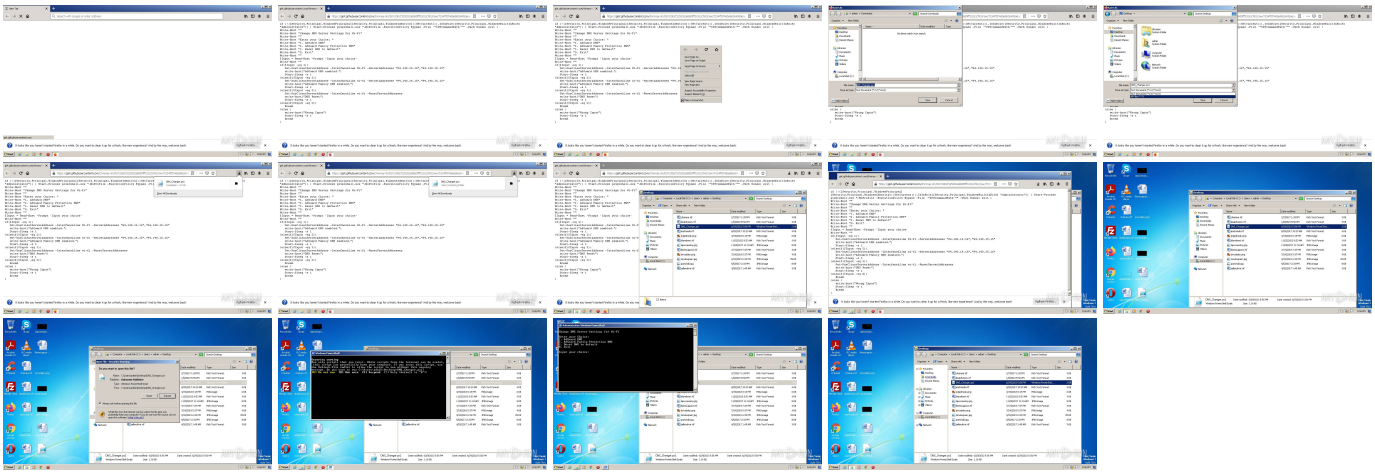
Using PowerShell to operate with local accounts
- powershell.exe (PID: 3300)

Starts POWERSHELL.EXE for commands execution
- powershell.exe (PID: 2272)

The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

Manual execution by a user
- powershell.exe (PID: 2272)

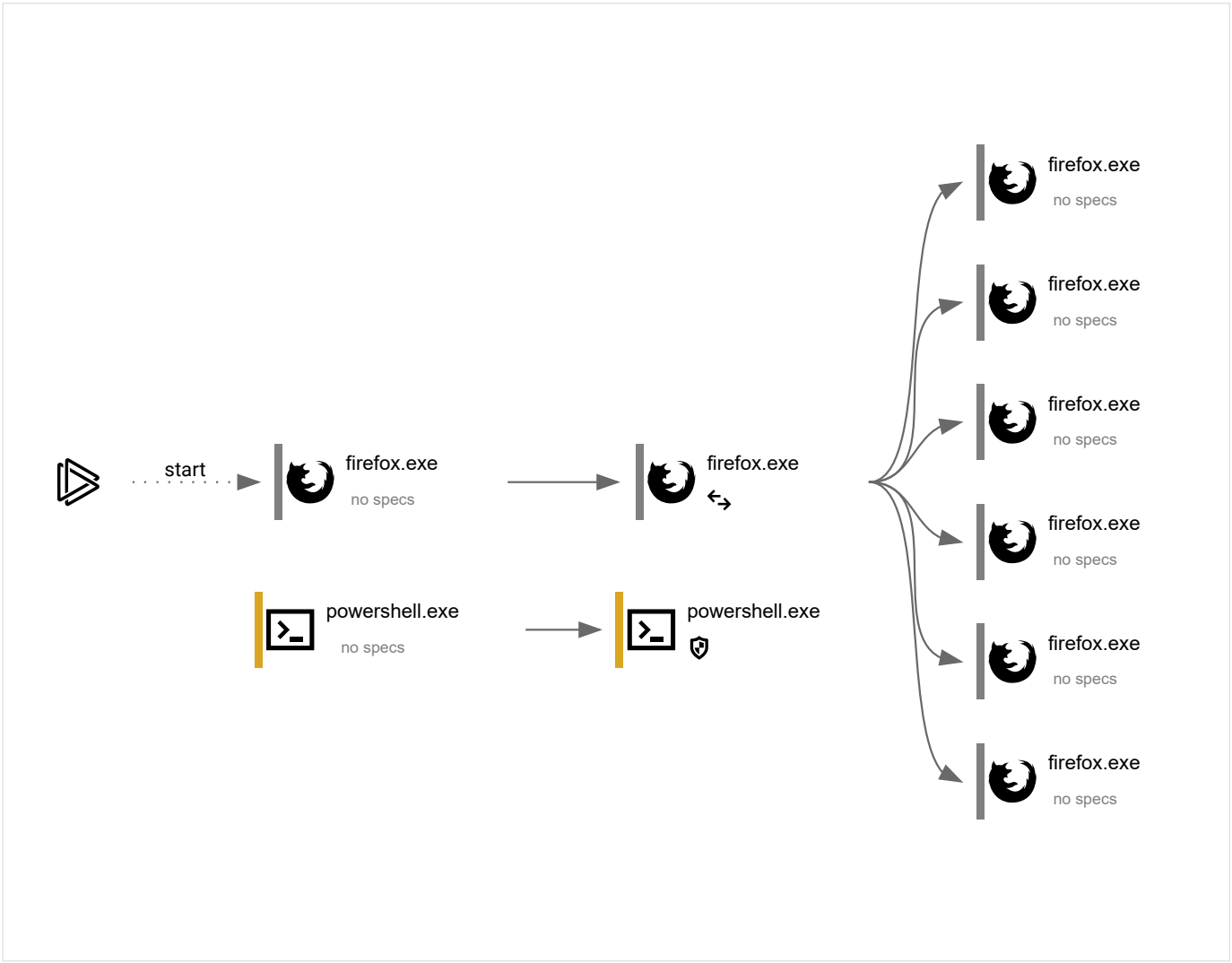
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
54	10	0	2

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
2976	"C:\Program Files\Mozilla Firefox\firefox.exe" "https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1"	C:\Program Files\Mozilla Firefox\firefox.exe	–	explorer.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	MEDIUM	Description:	Firefox

Exit code: 0 Version: 83.0

3384 "C:\Program Files\Mozilla Firefox\firefox.exe" https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1 C:\Program Files\Mozilla Firefox\firefox.exe ↪ firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: MEDIUM Description: Firefox
Exit code: 0 Version: 83.0

1824 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.0.587709683\935443381" -parentBuildID 20201112153044 -prefsHandle 1112 -prefMapHandle 1108 -prefsLen 1 -prefMapSize 238726 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 1196 gpu C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: MEDIUM Description: Firefox
Exit code: 1 Version: 83.0

3772 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.6.910586701\1435467684" -childID 1 -isForBrowser -prefsHandle 4872 -prefMapHandle 4868 -prefsLen 181 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 4884 tab C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: LOW Description: Firefox
Exit code: 0 Version: 83.0

1648 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.13.327271405\1549222807" -childID 2 -isForBrowser -prefsHandle 3764 -prefMapHandle 3896 -prefsLen 6644 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 3256 tab C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: LOW Description: Firefox
Exit code: 0 Version: 83.0

1160 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.20.307103037\2146044254" -childID 3 -isForBrowser -prefsHandle 2100 -prefMapHandle 3080 -prefsLen 7470 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 3924 tab C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: LOW Description: Firefox
Exit code: 0 Version: 83.0

3260 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.21.336355644\1791217740" -childID 4 -isForBrowser -prefsHandle 3336 -prefMapHandle 1904 -prefsLen 7470 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 3544 tab C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: LOW Description: Firefox
Exit code: 0 Version: 83.0

2404 "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3384.34.549990267\825554380" -childID 5 -isForBrowser -prefsHandle 2708 -prefMapHandle 3160 -prefsLen 7536 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3384 "\\.\pipe\gecko-crash-server-pipe.3384" 2712 tab C:\Program Files\Mozilla Firefox\firefox.exe – firefox.exe

Information

User: admin Company: Mozilla Corporation
Integrity Level: LOW Description: Firefox
Exit code: 0 Version: 83.0

2272 "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-file" "C:\Users\admin\Desktop\DNS_Changer.ps1" C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe – explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3300 "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.ex e" -NoProfile -ExecutionPolicy Bypass -File "C:\Users\admin\Desktop\DNS_Changer.ps1" C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
9	22	58	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3384	firefox.exe	POST	200	23.55.163.56:80	http://r3.o.lencr.org/	US	der	503 b	shared
3384	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt	US	text	8 b	whitelisted
3384	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	US	der	471 b	whitelisted
–	–	POST	200	23.55.163.56:80	http://r3.o.lencr.org/	US	der	503 b	shared
3384	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	US	der	313 b	whitelisted
3384	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	US	text	8 b	whitelisted
3384	firefox.exe	POST	200	142.250.186.35:80	http://ocsp.pki.goog/gts1c3	US	binary	472 b	whitelisted
3384	firefox.exe	POST	200	23.55.163.56:80	http://r3.o.lencr.org/	US	der	503 b	shared
–	–	POST	200	23.55.163.56:80	http://r3.o.lencr.org/	US	binary	503 b	shared

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
3384	firefox.exe	34.149.100.209:443	firefox.settings.services.mozilla.com	GOOGLE	US	suspicious
3384	firefox.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3384	firefox.exe	34.107.221.82:80	detectportal.firefox.com	GOOGLE	US	whitelisted
2248	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted
3384	firefox.exe	52.24.231.34:443	location.services.mozilla.com	AMAZON-02	US	unknown
3384	firefox.exe	34.160.144.191:443	content-signature-2.cdn.mozilla.net	GOOGLE	US	suspicious
3384	firefox.exe	142.250.186.35:80	ocsp.pki.goog	GOOGLE	US	whitelisted
3384	firefox.exe	34.117.65.55:443	push.services.mozilla.com	GOOGLE-CLOUD-PLATFORM	US	suspicious
3384	firefox.exe	172.217.16.138:443	safebrowsing.googleapis.com	GOOGLE	US	whitelisted
1076	svchost.exe	224.0.0.252:5355	–	–	–	unknown
3384	firefox.exe	185.199.108.133:443	gist.githubusercontent.com	FASTLY	US	malicious
3384	firefox.exe	140.82.121.4:443	gist.github.com	GITHUB	US	malicious
3384	firefox.exe	23.55.163.56:80	r3.o.lencr.org	Akamai International B.V.	DE	unknown
3384	firefox.exe	34.117.121.53:443	firefox-settings-attachments.cdn.mozilla.net	GOOGLE-CLOUD-PLATFORM	US	unknown
3384	firefox.exe	13.32.121.49:443	snippets.cdn.mozilla.net	AMAZON-02	US	suspicious

DNS requests

Domain	IP	Reputation
detectportal.firefox.com	34.107.221.82	whitelisted
prod.detectportal.prod.cloudops.mozgcp.net	34.107.221.82 2600:1901:0:38d7::	whitelisted
gist.github.com	140.82.121.4	suspicious
github.com	140.82.121.4	shared
firefox.settings.services.mozilla.com	34.149.100.209	whitelisted
prod.remote-settings.prod.webservices.mozgcp.net	34.149.100.209	suspicious
example.org	93.184.216.34	whitelisted
location.services.mozilla.com	52.24.231.34 44.233.10.108 54.244.114.149 52.42.53.182 44.233.226.27 52.34.120.119	whitelisted
ipv4only.arpa	192.0.0.171 192.0.0.170	whitelisted
locprod2-elb-us-west-2.prod.mozaws.net	52.34.120.119 44.233.226.27 52.42.53.182 54.244.114.149 44.233.10.108 52.24.231.34	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
fp2e7a.wpc.phicdn.net	192.229.221.95	whitelisted
r3.o.lencr.org	23.55.163.56 23.55.163.58	shared
a1887.dscq.akamai.net	23.55.163.58 23.55.163.56 2a02:26f0:1700:f::1737:a1a1 2a02:26f0:1700:f::1737:a1a4	whitelisted
gist.githubusercontent.com	185.199.108.133 185.199.111.133 185.199.109.133 185.199.110.133	shared
content-signature-2.cdn.mozilla.net	34.160.144.191	whitelisted
prod.content-signature-chains.prod.webservices.mozgcp.net	34.160.144.191 2600:1901:0:92a9::	whitelisted
safebrowsing.googleapis.com	172.217.16.138 2a00:1450:4001:80f::200a	whitelisted
push.services.mozilla.com	34.117.65.55	whitelisted
ocsp.pki.goog	142.250.186.35	whitelisted
pki-goog.l.google.com	142.250.186.35 2a00:1450:4001:803::2003	whitelisted
autopush.prod.mozaws.net	34.117.65.55	whitelisted
firefox-settings-attachments.cdn.mozilla.net	34.117.121.53	whitelisted
attachments.prod.remote-settings.prod.webservices.mozgcp.net	34.117.121.53	suspicious
snippets.cdn.mozilla.net	13.32.121.49 13.32.121.112 13.32.121.85 13.32.121.15	whitelisted
d228z91au11ukj.cloudfront.net	13.32.121.15 13.32.121.49 13.32.121.112 13.32.121.85	whitelisted
www.facebook.com	157.240.9.35	whitelisted
www.youtube.com	142.250.185.78 142.250.181.238 142.250.186.110	whitelisted

	172.217.16.206 142.250.186.78 142.250.185.142 142.250.185.110 142.250.186.174 142.250.186.142 172.217.16.142 142.250.185.174 142.250.185.206 142.250.185.238 172.217.18.110 172.217.18.14 142.250.186.46	
www.ebay.de	23.206.209.88	whitelisted
youtube-ui.l.google.com	142.250.186.46 142.250.185.78 142.250.181.238 142.250.186.110 172.217.16.206 142.250.186.78 142.250.185.142 142.250.185.110 142.250.186.174 142.250.186.142 172.217.16.142 142.250.185.174 142.250.185.206 142.250.185.238 172.217.18.110 172.217.18.14 2a00:1450:4001:829::200e 2a00:1450:4001:82f::200e 2a00:1450:4001:828::200e 2a00:1450:4001:813::200e	whitelisted
www.wikipedia.org	91.198.174.192	shared
star-mini.c10r.facebook.com	157.240.9.35 2a03:2880:f176:84:face:b00c:0:25de	whitelisted
dyna.wikimedia.org	91.198.174.192 2620:0:862:ed1a::1	whitelisted
www.reddit.com	151.101.1.140 151.101.65.140 151.101.129.140 151.101.193.140	whitelisted
e11847.a.akamaiedge.net	23.206.209.88	whitelisted
reddit.map.fastly.net	151.101.193.140 151.101.129.140 151.101.65.140 151.101.1.140	whitelisted

Threats

No threats detected

Debug output strings

No debug info

General Info

URL:	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1
Full analysis:	https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a
Verdict:	Suspicious activity
Analysis date:	June 29, 2023, 16:56:12
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)