ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	Image22077.exe
Full analysis:	https://app.any.run/tasks/27448ce4-d305-4583-979d-877c37a4ac41
Verdict:	Malicious activity
Analysis date:	August 23, 2022 at 16:49:38
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	7246CF1B1777A1422EBCDD9136B5B5D8
SHA1:	0891558FA30B9AD2F2C072572DBEAFE459160959
SHA256:	62119ACDA45CAAFC41D4879BE1B05E208CC29311F337BBC4887B6ED1AA62864A
SSDEEP:	12288:vH/AONru3XDG2dpqeodd+P5HfFrt5YPOMim2BHYT+muaS:PPNwG2j+G5N/HfxaS

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:**	off
Network:	on				

Software preset

Internet Explorer 11.0.9600.19596 KB4534251
Adobe Acrobat Reader DC (20.013.20064)
Adobe Flash Player 32 ActiveX (32.0.0.453)
Adobe Flash Player 32 NPAPI (32.0.0.453)
Adobe Flash Player 32 PPAPI (32.0.0.453)
Adobe Refresh Manager (1.8.0)
CCleaner (5.74)
FileZilla Client 3.51.0 (3.51.0)
Google Chrome (86.0.4240.198)
Google Update Helper (1.3.36.31)
Java 8 Update 271 (8.0.2710.9)
Java Auto Updater (2.8.271.9)
Microsoft .NET Framework 4.5.2 (4.5.51209)
Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Italian) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)

Hotfixes

Client LanguagePack Package
Client Refresh LanguagePack Package
CodecPack Basic Package
Foundation Package
IE Hyphenation Parent Package English
IE Spelling Parent Package English
IE Troubleshooters Package
InternetExplorer Optional Package
InternetExplorer Package TopLevel
KB2479943
KB2491683
KB2506212
KB2506928
KB2532531
KB2533552
KB2533623
KB2534111
KB2545698
KB2547666
KB2552343
KB2560656
KB2564958
KB2574819
KB2579686
KB2585542
KB2604115
KB2620704
KB2621440
KB2631813
KB2639308
KB2640148
KB2653956
KB2654428
KB2656356
KB2660075
KB2667402
KB2676562
KB2685811
KB2685813
KB2685939
KB2690533

Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972
Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461

Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102

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++ 2019 X86 Additional 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 Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

Steals credentials from Web Browsers
Image22077.exe (PID: 1932)

Actions looks like stealing of personal data
Image22077.exe (PID: 1932)

SUSPICIOUS

Checks supported languages
Image22077.exe (PID: 3456)
Image22077.exe (PID: 1932)

Reads the computer name
Image22077.exe (PID: 3456)
Image22077.exe (PID: 1932)

Application launched itself
Image22077.exe (PID: 3456)

Reads Environment values
Image22077.exe (PID: 1932)

INFO

Checks supported languages
firefox.exe (PID: 2340)
firefox.exe (PID: 2740)
firefox.exe (PID: 2824)
firefox.exe (PID: 3052)
firefox.exe (PID: 3388)
firefox.exe (PID: 2728)
firefox.exe (PID: 968)

Reads the computer name
firefox.exe (PID: 2340)
firefox.exe (PID: 3052)
firefox.exe (PID: 2824)
firefox.exe (PID: 2728)
firefox.exe (PID: 968)
firefox.exe (PID: 3388)

Manual execution by user
firefox.exe (PID: 2740)

Reads CPU info
firefox.exe (PID: 3052)

Application launched itself
firefox.exe (PID: 3052)
firefox.exe (PID: 2740)

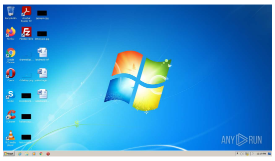
Creates files in the program directory
firefox.exe (PID: 3052)

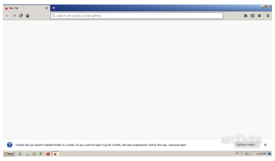
Static information

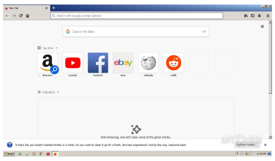
TRiD

.exe	Generic CIL Executable (.NET, Mono, etc.) (56.7)
.exe	Win64 Executable (generic) (21.3)
.scr	Windows screen saver (10.1)
.dll	Win32 Dynamic Link Library (generic) (5)
.exe	Win32 Executable (generic) (3.4)

Video and screenshots



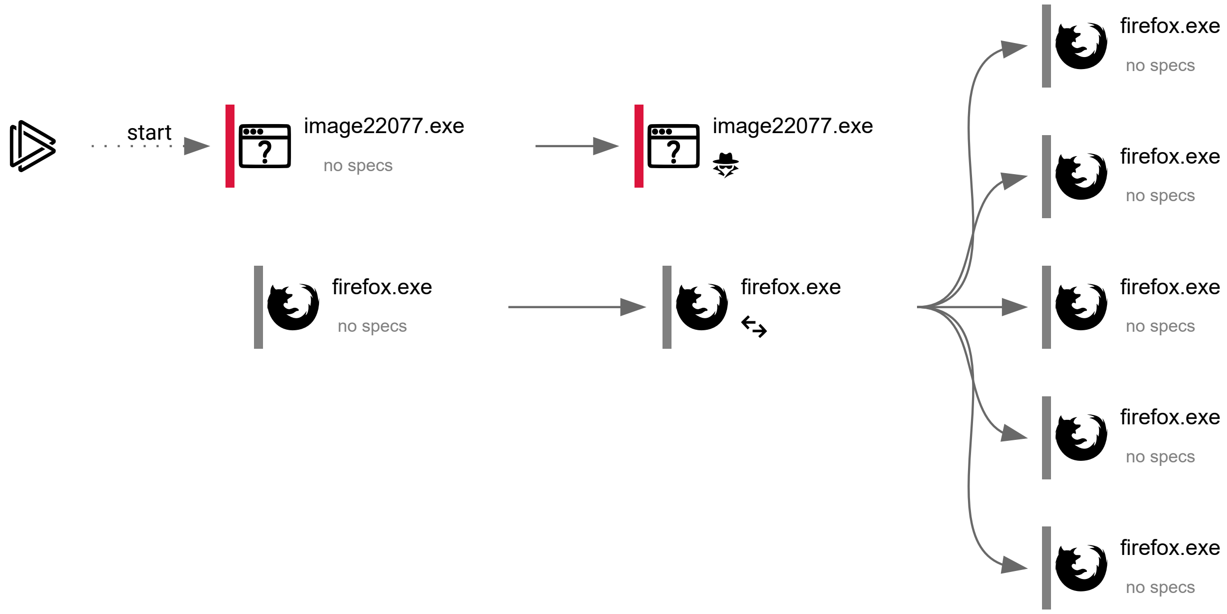




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
43	9	2	0

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
3456	"C:\Users\admin\AppData\Local\Temp\Image22077.exe"	C:\Users\admin\AppData\Local\Temp\Image22077.exe	—	Explorer.EXE

Information

User:	admin	Company:	Никита Юдин
Integrity Level:	MEDIUM	Description:	Tetris
Exit code:	0	Version:	1.0.0.0

2740	"C:\Program Files\Mozilla Firefox\firefox.exe"	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

3052	"C:\Program Files\Mozilla Firefox\firefox.exe"	C:\Program Files\Mozilla Firefox\firefox.exe	⇆	firefox.exe

Information

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

2824	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3052.0.380418825\82104054" -parentBuildID 20201112153044 -prefsHandle 1104 -prefMapHandle 840 -prefsLen 1 -prefMapSize 238726 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3052 "\\.\pipe\gecko-crash-server-pipe.3052" 1200 gpu	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

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

2340	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3052.6.1905282289\1205278492" -childID 1 -isForBrowser -prefsHandle 2476 -prefMapHandle 2472 -prefsLen 245 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3052 "\\.\pipe\gecko-crash-server-pipe.3052" 2488 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

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

3388	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3052.13.673301082\1375437839" -childID 2 -isForBrowser -prefsHandle 3160 -prefMapHandle 3156 -prefsLen 6644 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3052 "\\.\pipe\gecko-crash-server-pipe.3052" 3172 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

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

968	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3052.20.359883539\1555661308" -childID 3 -isForBrowser -prefsHandle 3540 -prefMapHandle 3544 -prefsLen 7470 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3052 "\\.\pipe\gecko-crash-server-pipe.3052" 3576 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

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

2728	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel="3052.21.930674450\1525005480" -childID 4 -isForBrowser -prefsHandle 3584 -prefMapHandle 3264 -prefsLen 7470 -prefMapSize 238726 -parentBuildID 20201112153044 -appdir "C:\Program Files\Mozilla Firefox\browser" - 3052 "\\.\pipe\gecko-crash-server-pipe.3052" 3604 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

1932	"C:\Users\admin\AppData\Local\Temp\Image22077.exe"	C:\Users\admin\AppData\Local\Temp\Image22077.exe	🕵	Image22077.exe

Information

User:	admin	Company:	Никита Юдин
Integrity Level:	MEDIUM	Description:	Tetris
Version:	1.0.0.0		

Registry activity

Total events	Read events	Write events	Delete events
7 344	7 312	32	0

Modification events

(PID) Process: (3456) Image22077.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: ProxyBypass
Value: 1

(PID) Process: (3456) Image22077.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: IntranetName
Value: 1

(PID) Process: (3456) Image22077.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: UNCAsIntranet
Value: 1

(PID) Process: (3456) Image22077.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write Name: AutoDetect
Value: 0

(PID) Process: (2740) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Launcher
Operation: write Name: C:\Program Files\Mozilla Firefox\firefox.exe|Launcher
Value: 65D1593517000000

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Launcher
Operation: write Name: C:\Program Files\Mozilla Firefox\firefox.exe|Browser
Value: 34DB593517000000

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Launcher
Operation: write Name: C:\Program Files\Mozilla Firefox\firefox.exe|Telemetry
Value: 0

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\DllPrefetchExperiment
Operation: write Name: C:\Program Files\Mozilla Firefox\firefox.exe
Value: 0

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent
Operation: write Name: C:\Program Files\Mozilla Firefox|DisableTelemetry
Value: 1

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent
Operation: write Name: C:\Program Files\Mozilla Firefox|DisableDefaultBrowserAgent
Value: 0

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent
Operation: write Name: C:\Program Files\Mozilla Firefox|ServicesSettingsServer
Value: https://firefox.settings.services.mozilla.com/v1

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent
Operation: write Name: C:\Program Files\Mozilla Firefox|SecurityContentSignatureRootHash
Value: 97:E8:BA:9C:F1:2F:B3:DE:53:CC:42:A4:E6:57:7E:D6:4D:F4:93:C2:47:B4:14:FE:A0:36:81:8D:38:23:56:0E

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write Name: ProxyEnable
Value: 0

(PID) Process: (3052) firefox.exe Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write Name: LanguageList
Value: en-US

(PID) Process: (3052) firefox.exe Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write Name: SavedLegacySettings
Value: 460000003B010000090000000000000000000000000000000040000000000000C0E333BBEAB1D301000000000000000000000000010000000200000C0A80164000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	86	30	12

Dropped files

PID	Process	Filename	Type
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\startupCache\scriptCache-current.bin **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-wal **MD5:** A67B0E44801EC45E73B676DD71493D48 **SHA256:** 49404EA3DE7CDB12F079109A8B7F91EC6191A817298CCCAA116F2BD8ED843537	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\sessionCheckpoints.json **MD5:** EA8B62857DFDBD3D0BE7D7E4A954EC9A **SHA256:** 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\cookies.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\2823318777ntouromlalnodry--naod.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\prefs.js **MD5:** 299A2B747C11E4BDA194E563FEA4A699 **SHA256:** 94EE461F62E8B4A0A65471A41E10C8C56722B73C0A019D76ACA7F5BAF109813E	text
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\sessionCheckpoints.json.tmp **MD5:** EA8B62857DFDBD3D0BE7D7E4A954EC9A **SHA256:** 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\1451318868ntouromlalnodry--epcr.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\3561288849sdhlie.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\search.json.mozlz4.tmp **MD5:** B17F8D93B0C43D6B72DC03752C20A2D9 **SHA256:** ADA0F70D374223FB63C2F19471FAB45D986A681E2485692E63F00F5071F19D76	jsonlz4
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Temp\mz_etilqs_Vo6ABlE4H15bRET **MD5:** F8FBADBCC51C994E0565F3CA25D7C825 **SHA256:** E16FC85ED204FE45EA1086A5B4A188F166FF89D0D98468FA02814B924727F6ED	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\prefs-1.js **MD5:** 299A2B747C11E4BDA194E563FEA4A699 **SHA256:** 94EE461F62E8B4A0A65471A41E10C8C56722B73C0A019D76ACA7F5BAF109813E	text
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\startupCache\urlCache-current.bin **MD5:** 994A33896BB41A278A315D0D796422B6 **SHA256:** 54EC50A20FFF8CC016710E49437CF6A11D3FE5EE7B28C185E4A9AAFEE2908B63	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\search.json.mozlz4 **MD5:** B17F8D93B0C43D6B72DC03752C20A2D9 **SHA256:** ADA0F70D374223FB63C2F19471FAB45D986A681E2485692E63F00F5071F19D76	jsonlz4
3052	firefox.exe	C:\Users\admin\AppData\Local\Temp\mz_etilqs_DOSrFe8oQ7T2ay4 **MD5:** AAE6283111FE0E7934E1A26AE05E240F **SHA256:** 8C5A25D46D8AF7B3161FDCA32353E8922C09B55D59DD0268BB9F1420606760F9	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\settings\main\ms-language-packs\asrouter.ftl.tmp **MD5:** C460716B62456449360B23CF5663F275 **SHA256:** 0EC0F16F92D876A9C1140D4C11E2B346A9292984D9A854360E54E99FDCD99CC0	text
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\settings\main\ms-language-packs\asrouter.ftl **MD5:** C460716B62456449360B23CF5663F275 **SHA256:** 0EC0F16F92D876A9C1140D4C11E2B346A9292984D9A854360E54E99FDCD99CC0	text
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-phish-proto.vlpset **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\startupCache\urlCache.bin **MD5:** 2FDBF2FE41902644F9FF9137132F00DD **SHA256:** AA809EC12586D348032C6A26722CC42F326C3B20C5B158BB99C58E1026640A79	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-badbinurl-proto.vlpset **MD5:** D6FE27E6FA4C59AE30F10D3ED3C4E643 **SHA256:** 1E4376B6D787AAF51254B1D04124E5F1734FB0209D3B28096228657E6AEEAAC2	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Temp\mz_etilqs_43DvpqUhkchcUqQ **MD5:** 15F7ADE6CCDD8A9D6CE18804274761F3 **SHA256:** 5F826DB297DE7C618E3156580F27F38E05FA9DC61E73324D39F941E42AD67862	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\broadcast-listeners.json **MD5:** 149301E0C06AC44CB5A653FE701BDEC1 **SHA256:** 98ABD888436CC226B9BFE457AE321D4510BE8DB88AF9EC724633A964EA7A4CBC	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\sessionstore-backups\recovery.jsonlz4 **MD5:** A05B4B4E64A24D6643D3B837E8A2C29E **SHA256:** 8B924689C358E8520093F98D20D97EB7C538B6A49C9AAAF1D660F97A5074E194	jsonlz4

3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\addonStartup.json.lz4.tmp **MD5:** 01DAE35763819EE4C2BD72553B33C337 **SHA256:** 674E499CCF7E955DEFFEB21B94C092DE0A8EA1DD308C426DCF04BC84DBDFA377	jsonlz4
3052	firefox.exe	C:\Users\admin\AppData\Local\Temp\mz_etilqs_aSHoNWVVr0QSSFX **MD5:** F576C781A80E1B8B844C7982AC6DA7EE **SHA256:** EE1DEA409450B25411CBC40CDDDB43815D2BC2159BCE0F011B77106CDED2E727	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Temp\mz_etilqs_3l7FgCoqDwJLV9z **MD5:** BA69B1C0919F17E1A086D4351D487F2B **SHA256:** E9B8785CA65C7EB64FADD2963EF26FBA34FD26C8C59BB5A7756421F68B9B714A	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\addonStartup.json.lz4 **MD5:** 01DAE35763819EE4C2BD72553B33C337 **SHA256:** 674E499CCF7E955DEFFEB21B94C092DE0A8EA1DD308C426DCF04BC84DBDFA377	jsonlz4
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\broadcast-listeners.json.tmp **MD5:** 149301E0C06AC44CB5A653FE701BDEC1 **SHA256:** 98ABD888436CC226B9BFE457AE321D4510BE8DB88AF9EC724633A964EA7A4CBC	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\startupCache\urlCache-new.bin **MD5:** 2FDBF2FE41902644F9FF9137132F00DD **SHA256:** AA809EC12586D348032C6A26722CC42F326C3B20C5B158BB99C58E1026640A79	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-downloadwhite-proto.vlpset **MD5:** EA86E0097B81FDBDEE3F12AC90CA6410 **SHA256:** 6A242B62530E38DDCFD272643F6CC44EDC0208C69DC3022D6CC273F4C7E79AF8	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-badbinurl-proto.metadata **MD5:** 53553242D57214AAA5726A09B05FE7BC **SHA256:** 1BE2B3990B410CA4FB38D1F79019C4018CD8820B69618646C81D22DFCBDDC802	abr
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-downloadwhite-proto.metadata **MD5:** 1EF5E829303A139CE967440E0CDCA10C **SHA256:** 98CE42DEEF51D40269D542F5314BEF2C7468D401AD5D85168BFAB4C0108F75F7	abr
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\sessionstore-backups\recovery.jsonlz4.tmp **MD5:** A05B4B4E64A24D6643D3B837E8A2C29E **SHA256:** 8B924689C358E8520093F98D20D97EB7C538B6A49C9AAAF1D660F97A5074E194	jsonlz4
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.files\1 **MD5:** 9B95765B0E26AF76116A95A966D61354 **SHA256:** 34F969C8E082310785EC4262E2D5B58C919D4DE856FFC64B3467507F83AC9571	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-wal **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-phish-proto-1.vlpset **MD5:** — **SHA256:** —	—
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-unwanted-proto.vlpset **MD5:** 6C7BD66A4404B7128ED3CDB1E071827D **SHA256:** 3C91EC10984682B15DDAC25FFE9E70359FA28B8878AA701E75EB235004445629	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-unwanted-proto.metadata **MD5:** 53553242D57214AAA5726A09B05FE7BC **SHA256:** 1BE2B3990B410CA4FB38D1F79019C4018CD8820B69618646C81D22DFCBDDC802	abr
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-malware-proto.vlpset **MD5:** E4FE13A7FB7B2F22B44B786D234FB402 **SHA256:** 2B22D4F40C144D94634D04421F41F9BD5E99134DD1B901A85247A1E81F22357C	binary
3052	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite **MD5:** B3C509CD1B466A5D04DAC152084ACA0E **SHA256:** 721BE0AA75C831316F4293F47E2A2BB0D0AA01F5561C16F5FCC69F57CC35542D	sqlite
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-phish-proto.metadata **MD5:** 53553242D57214AAA5726A09B05FE7BC **SHA256:** 1BE2B3990B410CA4FB38D1F79019C4018CD8820B69618646C81D22DFCBDDC802	abr
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-malware-proto.metadata **MD5:** 53553242D57214AAA5726A09B05FE7BC **SHA256:** 1BE2B3990B410CA4FB38D1F79019C4018CD8820B69618646C81D22DFCBDDC802	abr
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-unwanted-proto-1.vlpset **MD5:** 2DD7C729BB518F5A096E266D5A20F917 **SHA256:** C36E4D38FCAB6C51C13C819F6EE58A683CB388C207CE501E79E3CAF36B1F0D8E	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-malware-proto-1.vlpset **MD5:** A9EEDCDBA5256662AB4DC00E56931BCD **SHA256:** 309B7D7EE234FAFA71554B902B85BBC5CA6D1738E996F79891F5191E2E6FD8F3	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\mozplugin-block-digest256.vlpset **MD5:** FCC9C2C9B611A3264B68EBE180EB4248 **SHA256:** 6ECD378A537EEFE350B45CFA353741383F407D99D776BF23155A7825DC5DD2BC	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-badbinurl-proto-1.vlpset **MD5:** 2F6913F1573045143DC7C7E32A57AFEC **SHA256:** 81319046F3B08AF5FE3EF941AAF25FC16E825A0E8428BBDC155D643D40B5DB04	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\ads-track-digest256.sbstore **MD5:** A03E51212AD01CFE7EB3A87C8CE51744 **SHA256:** 2328A7569AB3D1E0C8638282E09860C82DB28EDD1C1BE75CAAD91FC7015E966C	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google4\goog-downloadwhite-proto-1.vlpset **MD5:** B0272F5CF9F56F11C856155DC5F40BE1 **SHA256:** 74AB81A1929A8806D559A13140947F076CABA52BF882364C416EF4D8E9B155F4	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\mozplugin-block-digest256.sbstore **MD5:** 519BEB1B01FC355BB388F1F75BE997FD **SHA256:** FFE2D3077B81AE6F51B220C1C661B276C823FA67DAD1D64FC5F17249FC54BDC0	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-track-digest256.sbstore **MD5:** 59D2D3A9FF42621AE974078BCAABD9BC **SHA256:** 7371E8534C31C4BFF73E340413D77C988593A0E559418B0F2A5B34B9C82DDDD2	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\ads-track-digest256.vlpset	binary

		MD5: 38F55098AB1772E8A7B90A05CB33CFAE **SHA256:** FD44A8121E20CF102D8FD79D6EE45D55CCB0D92893907091BB7587ED3B274244	
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-track-digest256.vlpset **MD5:** E1EDDE17E24B61C5B26D7B76BA039463 **SHA256:** C2C4612B7B9545751F37B302EE345ABD0F22170C7CC2497320897B385D508B7F	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\analytics-track-digest256.vlpset **MD5:** 1E1C0442F3FE16B185D5DB74F0E91FCE **SHA256:** 43ACC2D047C7988E9073ECF32AC619DE0D080C45B061D441D1D671D305BB4F08	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\mozstd-trackwhite-digest256.sbstore **MD5:** 92A93E4C81027F5788873296C6E2875B **SHA256:** 4358B8F0AF157CF2EF36A3A8BD152A528D32CFE98A2E0AE66207DBDB1D943EFA	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\content-track-digest256.sbstore **MD5:** 2BE5027A476EFB5FE011AE8257E6B428 **SHA256:** 26D0EF7103DBC0516ADD2DA8029CA43567B98BDA1EF8D8E4CDA42F09AA9A4B36	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\analytics-track-digest256.sbstore **MD5:** AE706ABFAECFD90D67E5C965091E004E **SHA256:** 13CBF8A5389A33A562E6DD10660F68E8964313536A109AA80ACFD8838BF45E73	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\content-track-digest256.vlpset **MD5:** 897401403F6A9BBC2727BF8ACFA8BBAF **SHA256:** 75157865105C44C1220C337AEFF723E7B2E4AEF506CE7DB00E2621D5CEAF45B8	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\mozstd-trackwhite-digest256.vlpset **MD5:** C8663695A49BB5FB5A301D1A7233DB6C **SHA256:** 498D10D381ED91BE12CFF65292813BCCCD676176BCF614534AB7BA0E5536306E	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google-trackwhite-digest256.sbstore **MD5:** FEC9BC354A7EE92C6FEEFE63E6B0FA26 **SHA256:** 258EF8E6994A09FFB54BD0D5AFEC97C13C31F2EEFB7FE90A2A4C487C87817519	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\allow-flashallow-digest256.sbstore **MD5:** DD0458514C9A922B45DA6A8BEBE47320 **SHA256:** D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\allow-flashallow-digest256.vlpset **MD5:** DE0D88480C24350C59E1E9A3583DE0D1 **SHA256:** 01BA9F0B913E04ED10BD7166796483DD4F72005F249D6EE68B12117BE4B5D3C7	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\google-trackwhite-digest256.vlpset **MD5:** E54E5B84194EEE15E64D2A03F1136BB7 **SHA256:** 07707B589BE3DBA3BB0BDAC67760A2B180EA3531E9D7976B73E4C1D8DF9DBB1E	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\block-flash-digest256.vlpset **MD5:** 130B9AC2BEEC5ADA274561105D81AE36 **SHA256:** 7D99FEC08182A5B95D18D1569EDAA2C60C2AAFBD15A56D8882F22F3B395E6460	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\base-fingerprinting-track-digest256.sbstore **MD5:** DAA7ABDB5ED1DBF8877F4028092E32F6 **SHA256:** B8F20B14AD5291B4528DF859129B301F367A9885F417F9807821D5A386352530	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\block-flash-digest256.sbstore **MD5:** 9F6B331AA1E070DCFEED473E76CE56C3 **SHA256:** 7DBBEA2DD387EEB85E1F56E02FC9989ACDE570CD43BFEF2C2A827093BA87DA6D	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\block-flashsubdoc-digest256.vlpset **MD5:** 40165280FF1345B5241EC2A9D1DA2AF0 **SHA256:** F80BDD5341D8B1EE946E344E258EF2D35C3C0BB6B13EB7B3E6A77467DFA8B97F	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-linkedin-digest256.vlpset **MD5:** 3303AA4BCB02D27F1A8B6AFF30C1DD9C **SHA256:** 6F33CCFCF9767B612657242C2819C325CFDF17B8D92224DB588A886F7EC2D26E	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flashsubdoc-digest256.sbstore **MD5:** 22698B4CF784DBBAE2D583F00491D43D **SHA256:** 3849563088AE0677D61702A1310FDE26DE5DDD846D53037222D3EFE012197BF5	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-twitter-digest256.vlpset **MD5:** 35D8FD43D868D7BBA7041362EB8101B3 **SHA256:** 104C2467E4F7BC7CAC0CE0E456D5ABD8C192C2C8C44F7C9A38412A59ABDD1772	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flash-digest256.vlpset **MD5:** C2994D388F8780C87D35C352D9582985 **SHA256:** 7ED09F7D2BD632F70077A4AE4F2BD2F3FB654B03CD72652F51678B0C7D027F25	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-facebook-digest256.sbstore **MD5:** 58FBC7F7687CC8798AEA35B7066EB198 **SHA256:** 3A2035AD8446C71242DAA9EAF3818B87F673D0429E4F5334621905B47A1C3DF5	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\base-cryptomining-track-digest256.sbstore **MD5:** D6C5C2E242DF3EC5FF8E17DD8EE15F73 **SHA256:** F0C6512E42F2732B3AA401F9AB4DF84C0A89C9755968B158796706A48B9F492A	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\block-flashsubdoc-digest256.sbstore **MD5:** B9556D03AFF392142AD5691D2F867310 **SHA256:** CFD3909B41C1EE3CBCB8B7D2B1378065E7D3B543FFF1F2FB7A4F25C5FF41722C	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-twitter-digest256.sbstore **MD5:** 373411CEBF6E3BCB89D8BFA632409BF1 **SHA256:** C1D5B95B18FF02514BDA0EC7865D9468C3A89E5C3BA2EBD3D4284FD8FCD463D4	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-facebook-digest256.vlpset **MD5:** 86B1ACDBF1FC7201D0EB7C85EE75F5AF **SHA256:** A0F4C83316CD66525F663CD72A2DC8BD1B2AA2E40D599B8B6F334D61C5D03098	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flashsubdoc-digest256.vlpset **MD5:** 0C0D67875BD75A0227C02DD8529BA01A **SHA256:** 614BE0169EC36E67223EB9645A98DA66DBFDE5DFBB89BB064F428AAEABDD9D97	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flash-digest256.sbstore **MD5:** D5D6B4D59B4AE4E2DE4B40D0DA083571 **SHA256:** 000E3A78C72A210CA3B5417A3CDD294FBCE2A31661601C9D594C75CF2800571C	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\base-fingerprinting-track-digest256.vlpset **MD5:** FA7667EEED0B53973506278ECE958E62 **SHA256:** 0D55A21E6694FCE19F366F9E5351A02D215D378541DBC38DF68645B63B56D8BF	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\social-tracking-protection-linkedin-	

		digest256.sbstore **MD5:** 3B11B562807FEF504FE671DED4D0E8CE **SHA256:** 9BF05ADC119CDD219347572787A9B7E18308C4465A8F440C34C697B2F5CD479F	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\base-cryptomining-track-digest256.vlpset **MD5:** 7D532B89A987D92DEF1D7AABBAAD62AB **SHA256:** 7CB574BE3E783D6876740DBCA525D868677307A52DDDD67AC84665CCFAAE895E	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flashallow-digest256.sbstore **MD5:** DD0458514C9A922B45DA6A8BEBE47320 **SHA256:** D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	binary
3052	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\qldyz51w.default\safebrowsing-updating\except-flashallow-digest256.vlpset **MD5:** 7194B6BFF691A056852A51E2E06CE8FE **SHA256:** CBE2DC6ABFE25BEAD60F4DFAF419FC0F441FF8A8DD4A2FEBF5553BE1CBD90C49	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	26	59	2

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3052	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt	US	text	8 b	whitelisted
3052	firefox.exe	POST	200	142.250.185.131:80	http://ocsp.pki.goog/gts1c3	US	der	472 b	whitelisted
3052	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	US	text	8 b	whitelisted
3052	firefox.exe	POST	200	93.184.220.29:80	http://ocsp.digicert.com/	US	der	471 b	whitelisted
3052	firefox.exe	POST	200	93.184.220.29:80	http://ocsp.digicert.com/	US	der	471 b	whitelisted
3052	firefox.exe	POST	200	93.184.220.29:80	http://ocsp.digicert.com/	US	der	471 b	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3052	firefox.exe	52.222.214.84:443	firefox.settings.services.mozilla.com	Amazon.com, Inc.	US	suspicious
3052	firefox.exe	34.107.221.82:80	detectportal.firefox.com	—	US	whitelisted
3052	firefox.exe	54.184.13.11:443	location.services.mozilla.com	Amazon.com, Inc.	US	unknown
—	—	34.107.221.82:80	detectportal.firefox.com	—	US	whitelisted
3052	firefox.exe	18.66.139.67:443	content-signature-2.cdn.mozilla.net	Massachusetts Institute of Technology	US	suspicious
3052	firefox.exe	142.250.185.131:80	ocsp.pki.goog	Google Inc.	US	whitelisted
3052	firefox.exe	52.222.236.127:443	firefox-settings-attachments.cdn.mozilla.net	Amazon.com, Inc.	US	unknown
3052	firefox.exe	13.32.121.49:443	snippets.cdn.mozilla.net	Amazon.com, Inc.	US	unknown
3052	firefox.exe	52.36.24.174:443	push.services.mozilla.com	Amazon.com, Inc.	US	unknown
3052	firefox.exe	142.250.186.138:443	safebrowsing.googleapis.com	Google Inc.	US	whitelisted
3052	firefox.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3052	firefox.exe	44.240.237.74:443	shavar.services.mozilla.com	University of California, San Diego	US	unknown
3052	firefox.exe	18.66.97.122:443	tracking-protection.cdn.mozilla.net	Massachusetts Institute of Technology	US	unknown

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
firefox.settings.services.mozilla.com	52.222.214.84 52.222.214.96 52.222.214.105 52.222.214.116	whitelisted
location.services.mozilla.com	54.184.13.11	whitelisted

	34.213.44.137 52.35.17.16 35.162.19.172 35.161.134.0 44.241.228.251	
locprod2-elb-us-west-2.prod.mozaws.net	44.241.228.251 35.161.134.0 35.162.19.172 52.35.17.16 34.213.44.137 54.184.13.11	whitelisted
example.org	93.184.216.34	whitelisted
ipv4only.arpa	192.0.0.171 192.0.0.170	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
cs9.wac.phicdn.net	93.184.220.29	whitelisted
content-signature-2.cdn.mozilla.net	18.66.139.67 18.66.139.17 18.66.139.125 18.66.139.97	whitelisted
d2nxq2uap88usk.cloudfront.net	18.66.139.97 18.66.139.125 18.66.139.17 18.66.139.67 2600:9000:225e:7200:a:da5e:7900:93a1 2600:9000:225e:2200:a:da5e:7900:93a1 2600:9000:225e:6000:a:da5e:7900:93a1 2600:9000:225e:7400:a:da5e:7900:93a1 2600:9000:225e:6400:a:da5e:7900:93a1 2600:9000:225e:ca00:a:da5e:7900:93a1 2600:9000:225e:a000:a:da5e:7900:93a1 2600:9000:225e:4400:a:da5e:7900:93a1	shared
safebrowsing.googleapis.com	142.250.186.138 2a00:1450:4001:82b::200a	whitelisted
push.services.mozilla.com	52.36.24.174	whitelisted
autopush.prod.mozaws.net	52.36.24.174	whitelisted
ocsp.pki.goog	142.250.185.131	whitelisted
pki-goog.l.google.com	142.250.185.131 2a00:1450:4001:829::2003	whitelisted
www.youtube.com	216.58.212.174 172.217.18.110 142.250.74.206 172.217.23.110 216.58.212.142 142.250.185.78 142.250.185.110 142.250.185.142 142.250.185.174 142.250.185.206 142.250.185.238 142.250.186.142 142.250.186.46 142.250.181.238 142.250.186.110 172.217.16.142	whitelisted
www.facebook.com	185.60.216.35	whitelisted
www.ebay.de	104.75.89.144	whitelisted
youtube-ui.l.google.com	172.217.16.142 142.250.186.110 142.250.181.238 142.250.186.46 142.250.186.142 142.250.185.238 142.250.185.206 142.250.185.174 142.250.185.142 142.250.185.110 142.250.185.78 216.58.212.142 172.217.23.110 142.250.74.206 172.217.18.110 216.58.212.174	whitelisted

	2a00:1450:4001:827::200e 2a00:1450:4001:82f::200e 2a00:1450:4001:829::200e 2a00:1450:4001:808::200e	
e11847.a.akamaiedge.net	104.75.89.144	whitelisted
star-mini.c10r.facebook.com	185.60.216.35 2a03:2880:f12d:181:face:b00c:0:25de	whitelisted
www.wikipedia.org	91.198.174.192	shared
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
reddit.map.fastly.net	151.101.193.140 151.101.129.140 151.101.65.140 151.101.1.140	whitelisted
firefox-settings-attachments.cdn.mozilla.net	52.222.236.127 52.222.236.89 52.222.236.38 52.222.236.4	whitelisted
fennec-catalog-cdn.prod.mozaws.net	52.222.236.4 52.222.236.38 52.222.236.89 52.222.236.127	whitelisted
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 13.32.121.85 13.32.121.112 13.32.121.49	whitelisted
shavar.services.mozilla.com	44.240.237.74 44.236.110.253 54.189.93.11 52.11.213.12 52.33.232.236 44.227.235.173	whitelisted
shavar.prod.mozaws.net	44.227.235.173 52.33.232.236 52.11.213.12 54.189.93.11 44.236.110.253 44.240.237.74	whitelisted
tracking-protection.cdn.mozilla.net	18.66.97.122 18.66.97.89 18.66.97.19 18.66.97.117	whitelisted
d1zkz3k4cclnv6.cloudfront.net	18.66.97.117 18.66.97.19 18.66.97.89 18.66.97.122	shared

Threats

PID	Process	Class	Message
3052	firefox.exe	Potentially Bad Traffic	ET INFO Terse Request for .txt - Likely Hostile
3052	firefox.exe	Potentially Bad Traffic	ET INFO Terse Request for .txt - Likely Hostile

Debug output strings

No debug info