ANY ▷ RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	✳ 🖳 🗐 🕱
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:		Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

• Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)

• Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)

• Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)

• VLC media player (3.0.11)

• WinRAR 5.91 (64-bit) (5.91.0)

• Windows PC Health Check (3.6.2204.08001)

Behavior activities

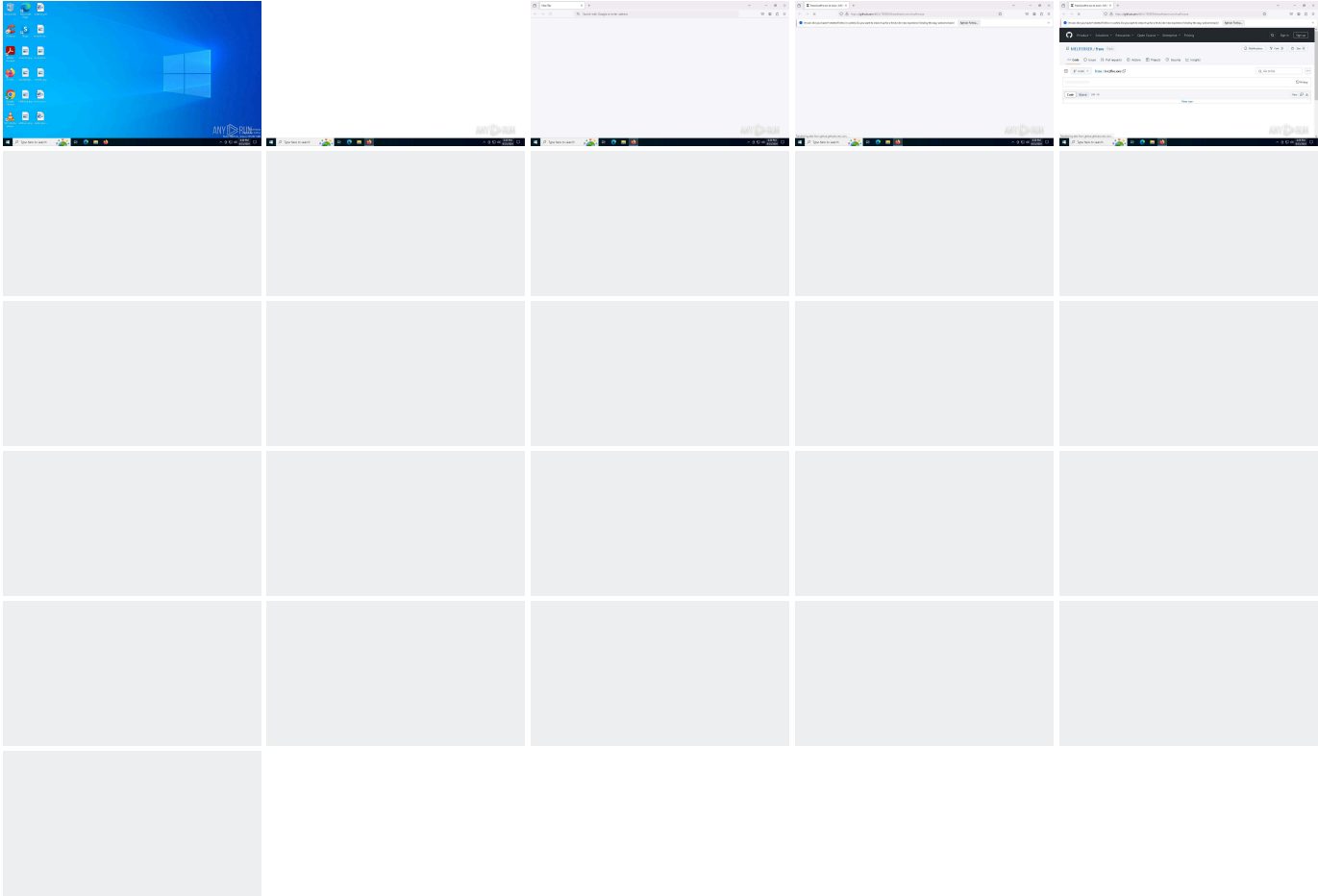| MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	**Uses TIMEOUT.EXE to delay execution**	**Application launched itself**
	• cmd.exe (PID: 7520)	• firefox.exe (PID: 6552)
	• cmd.exe (PID: 7876)	• firefox.exe (PID: 6596)
	Starts CMD.EXE for commands execution	**Executable content was dropped or overwritten**
	• Jvczfhe.exe (PID: 7492)	• firefox.exe (PID: 6596)
	• Muadnrd.exe (PID: 7824)	**Checks supported languages**
	Process drops legitimate windows executable	• Jvczfhe.exe (PID: 7492)
	• firefox.exe (PID: 6596)	• InstallUtil.exe (PID: 5152)
	Reads security settings of Internet Explorer	• Muadnrd.exe (PID: 7824)
	• Jvczfhe.exe (PID: 7492)	• Muadnrd.exe (PID: 7248)
	• Muadnrd.exe (PID: 7824)	**Reads Microsoft Office registry keys**
	Checks Windows Trust Settings	• firefox.exe (PID: 6596)
	• Jvczfhe.exe (PID: 7492)	**Reads the machine GUID from the registry**
	• Muadnrd.exe (PID: 7824)	• Jvczfhe.exe (PID: 7492)
	Executes application which crashes	• InstallUtil.exe (PID: 5152)
	• Jvczfhe.exe (PID: 7492)	• Muadnrd.exe (PID: 7824)
	• Muadnrd.exe (PID: 7824)	• Muadnrd.exe (PID: 7248)
	Connects to unusual port	**Disables trace logs**
	• InstallUtil.exe (PID: 5152)	• Jvczfhe.exe (PID: 7492)
	Application launched itself	• Muadnrd.exe (PID: 7824)
	• Muadnrd.exe (PID: 7824)	**Reads the computer name**
		• Jvczfhe.exe (PID: 7492)
		• InstallUtil.exe (PID: 5152)
		• Muadnrd.exe (PID: 7824)
		• Muadnrd.exe (PID: 7248)
		Reads the software policy settings
		• Jvczfhe.exe (PID: 7492)
		• WerFault.exe (PID: 1356)
		• Muadnrd.exe (PID: 7824)
		• WerFault.exe (PID: 7584)
		Reads Environment values
		• Jvczfhe.exe (PID: 7492)
		• InstallUtil.exe (PID: 5152)
		• Muadnrd.exe (PID: 7824)
		Checks proxy server information
		• Jvczfhe.exe (PID: 7492)
		• WerFault.exe (PID: 1356)
		• Muadnrd.exe (PID: 7824)
		• WerFault.exe (PID: 7584)
		Creates files or folders in the user directory
		• WerFault.exe (PID: 1356)
		• WerFault.exe (PID: 7584)
		.NET Reactor protector has been detected
		• InstallUtil.exe (PID: 5152)
		• Muadnrd.exe (PID: 7248)

Malware configuration

No Malware configuration.
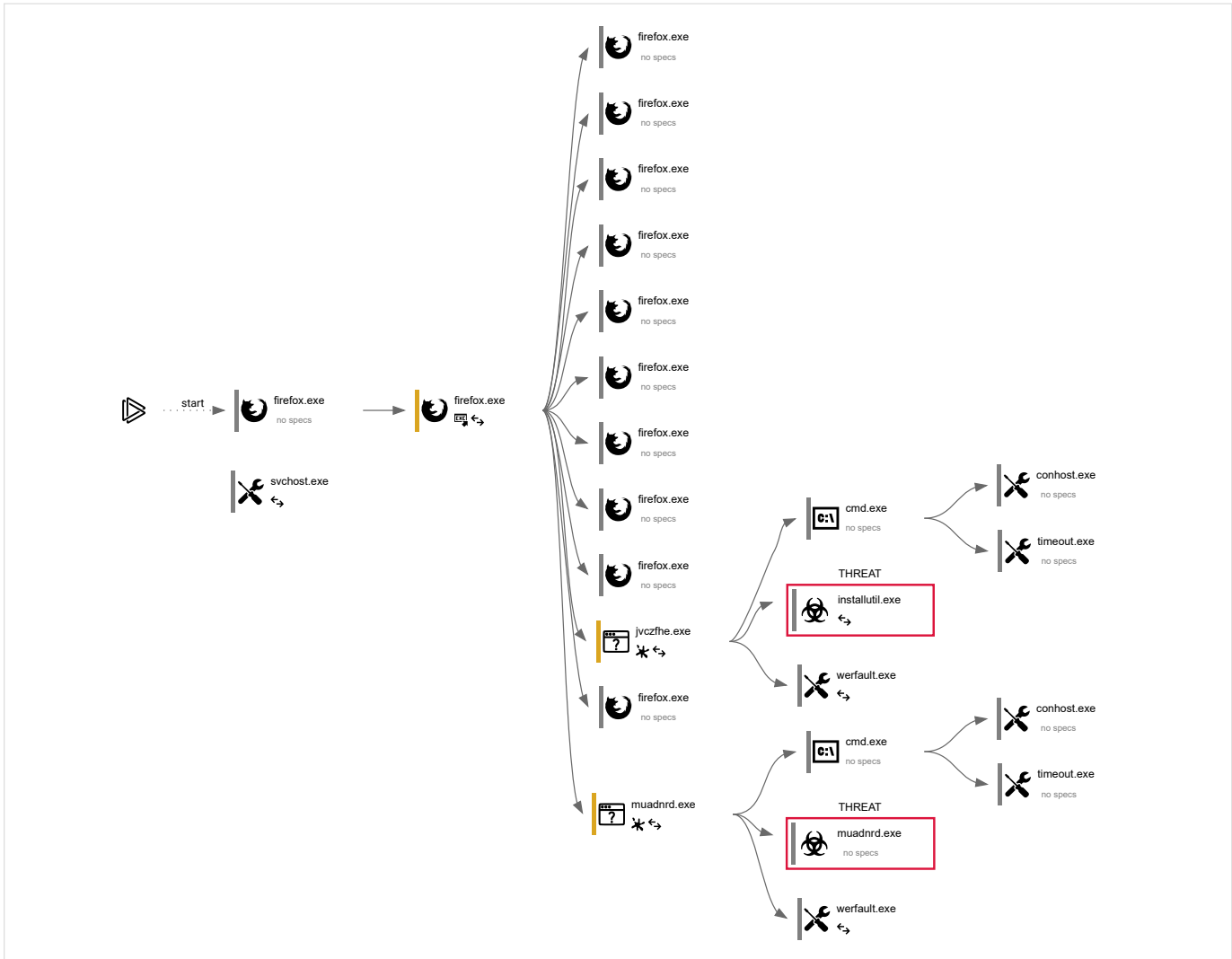
Static information

No data.

Video and screenshots

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
155	25	0	3

Behavior graph

Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
1356	C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676	C:\Windows\SysWOW64\WerFault.exe	↩	Jvczfhe.exe

Information			
User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Problem Reporting
Exit code:	0	Version:	10.0.19041.3996 (WinBuild.160101.0800)

| 2256 | C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache | C:\Windows\System32\svchost.exe | ↩→ | services.exe |

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation	
Integrity Level:	SYSTEM	Description:	Host Process for Windows Services	
Version:	10.0.19041.1 (WinBuild.160101.0800)			

| 5152 | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe | ☣ ↩→ | Jvczfhe.exe |

Information

User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	.NET Framework installation utility	
Version:	4.8.9037.0 built by: NET481REL1			

| 6340 | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5380 -childID 4 -isForBrowser -prefsHandle 5516 -prefMapHandle 5508 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {fac3d9db-bdd5-4087-af19-991bcb39f3fc} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55d90 tab | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |

Information

User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

| 6360 | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5512 -childID 5 -isForBrowser -prefsHandle 5668 -prefMapHandle 5672 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {87081c36-df2a-495c-8aa3-1f1d82c27099} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4bf3d90 tab | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |

Information

User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

| 6368 | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4976 -parentBuildID 20240213221259 -sandboxingKind 0 -prefsHandle 4800 -prefMapHandle 4804 -prefsLen 36339 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {9f234b1e-a7f5-459b-a776-445e6f7f5cf6} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c46eeb10 utility | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |

Information

User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

| 6384 | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5228 -childID 3 -isForBrowser -prefsHandle 5224 -prefMapHandle 5220 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {341d20e2-0ffc-4ced-87ee-4738a3c45fef} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55690 tab | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |

Information

User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

| 6456 | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5916 -childID 6 -isForBrowser -prefsHandle 5908 -prefMapHandle 4672 -prefsLen 34713 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {18cad704-8b2b-4301-9d29-a6d45994eac7} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b65310 tab | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |

Information

User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

| 6552 | "C:\Program Files\Mozilla Firefox\firefox.exe" "https://github.com/MELITERRER/frew/blob/main/Jvczfhe.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:	123.0			

6596   "C:\Program Files\Mozilla Firefox\firefox.exe"   C:\Program Files\Mozilla Firefox\firefox.exe   📖 ↪   firefox.exe
https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	MEDIUM	Description:	Firefox
Version:	123.0		

6680   "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4480 -childID 2 -isForBrowser -prefsHandle 4472 -prefMapHandle 4412 -prefsLen 36263 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {a5653cc5-bef6-4bd7-a916-64d6d56bffd5} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c161e850 tab   C:\Program Files\Mozilla Firefox\firefox.exe   —   firefox.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	LOW	Description:	Firefox
Version:	123.0		

6744   "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=1824 -parentBuildID 20240213221259 -prefsHandle 1752 -prefMapHandle 1732 -prefsLen 30537 -prefMapSize 244343 -appDir "C:\Program Files\Mozilla Firefox\browser" - {cb10680d-0044-4e6b-8433-6e05fa363c18} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256ba9c2b10 gpu   C:\Program Files\Mozilla Firefox\firefox.exe   —   firefox.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	LOW	Description:	Firefox
Version:	123.0		

6816   "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=2208 -parentBuildID 20240213221259 -prefsHandle 2192 -prefMapHandle 2188 -prefsLen 30537 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {9a337de7-7563-44b0-ad05-1393e51c0827} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256aec7f510 socket   C:\Program Files\Mozilla Firefox\firefox.exe   —   firefox.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	LOW	Description:	Firefox
Version:	123.0		

7048   "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=3028 -childID 1 -isForBrowser -prefsHandle 2880 -prefMapHandle 3020 -prefsLen 26706 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {72307e83-1a5f-44ea-b997-a72e8f677a2c} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0670bd0 tab   C:\Program Files\Mozilla Firefox\firefox.exe   —   firefox.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	LOW	Description:	Firefox
Version:	123.0		

7248   "C:\Users\admin\Downloads\Muadnrd.exe"   C:\Users\admin\Downloads\Muadnrd.exe   ☣   Muadnrd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft Edge
Exit code:	0	Version:	126.0.2592.113

7492   "C:\Users\admin\Downloads\Jvczfhe.exe"   C:\Users\admin\Downloads\Jvczfhe.exe   ✳ ↪   firefox.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft Edge
Exit code:	3762504530	Version:	126.0.2592.113

7520   "cmd" /c timeout 21 & exit   C:\Windows\SysWOW64\cmd.exe   —   Jvczfhe.exe

Information

7528	User: \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	admin	Company: C:\Windows\System32\conhost.exe	Microsoft Corporation	—	cmd.exe
	Integrity Level:	MEDIUM	Description:	Windows Command Processor		

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Console Window Host	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

7572	timeout 21		C:\Windows\SysWOW64\timeout.exe	—	cmd.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	timeout - pauses command processing	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

7584	C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7824 -s 2888		C:\Windows\SysWOW64\WerFault.exe	↩	Muadnrd.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Windows Problem Reporting	
Exit code:	0	Version:	10.0.19041.3996 (WinBuild.160101.0800)	

7756	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=7340 -childID 7 -isForBrowser -prefsHandle 6280 -prefMapHandle 6436 -prefsLen 32132 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {6f311190-77cd-4ee9-97c4-08357a8cf697} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0a96150 tab		C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information				
User:	admin	Company:	Mozilla Corporation	
Integrity Level:	LOW	Description:	Firefox	
Version:	123.0			

7824	"C:\Users\admin\Downloads\Muadnrd.exe"		C:\Users\admin\Downloads\Muadnrd.exe	✳ ↩	firefox.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Microsoft Edge	
Exit code:	3762504530	Version:	126.0.2592.113	

7860	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1		C:\Windows\System32\conhost.exe	—	cmd.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Console Window Host	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

7876	"cmd" /c timeout 21 & exit		C:\Windows\SysWOW64\cmd.exe	—	Muadnrd.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Windows Command Processor	
Exit code:	0	Version:	10.0.19041.3636 (WinBuild.160101.0800)	

7968	timeout 21		C:\Windows\SysWOW64\timeout.exe	—	cmd.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	timeout - pauses command processing	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

Registry activity

Total events	Read events	Write events	Delete events
35 308	35 167	140	1

Modification events

(PID) Process:	(6552) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Launcher
Value:	84B995F900000000		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Browser
Value:	63DA97F900000000		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Progress
Value:	0		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Progress
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Installer\308046B0AF4A39CB
Operation:	delete value	Name:	installer.taskbarpin.win10.enabled
Value:			

(PID) Process:	(6596) 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:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\DllPrefetchExperiment
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe
Value:	0		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Theme
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Enabled
Value:	1		

(PID) Process:	(6596) 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:	(6596) 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:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	Name:	C:\Program Files\Mozilla Firefox|SetDefaultBrowserUserChoice
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	Name:	C:\Program Files\Mozilla Firefox|AppLastRunTime
Value:	E84455D32EF7DA01		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|ScreenX
Value:	4		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|ScreenY
Value:	4		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Width
Value:	1168		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Height
Value:	651		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Maximized
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|Flags
Value:	2		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|CssToDevPixelScaling
Value:	000000000000F03F		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|UrlbarCSSSpan
Value:	000000E0EE966A400000001C221D9040		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|SearchbarCSSSpan
Value:	00000000000000000000000000000000		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|SpringsCSSSpan
Value:	0000000000805C40000000E0EEF66940000000202231904000000FCFFA79140		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation:	write	Name:	SlowContextMenuEntries
Value:	6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E23282770100000114020000000000C0000000000000468D0000006078A409B011A54DAFA526D86198A 780390100000A9AD298B2EDA6DE11BA8CA68E55D895936E000000		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|UrlbarCSSSpan
Value:	0000002011A96A40000000C8BB158F40		

(PID) Process:	(6596) firefox.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	Name:	C:\Program Files\Mozilla Firefox\firefox.exe|SpringsCSSSpan
Value:	0000000000805C400000002011096A40000000C0BB3D8F400000000400189140		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	EnableConsoleTracing

Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	ConsoleTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	MaxFileSize
Value:	1048576		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Property
Operation:	write	Name:	00180010F429971D

Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B200000000020000000001066000000010000200000000CCC6B875C440CBAEA
58C5BED8611E39AA9829013E4B8AC51D0D9F7163EADF000000000000E8000000002000200000000BE26AF426085AF609742DB1A14612244C8BCC3E0EDE09C59A27330B31E6E2E9800000
00D3BE81583AE43F56559EF36DEAFC074326B67E4667C7B38DFDF2D00FEFB0DAFFB6ED08C7C33F7A635133822E53A45D8BF87E2E838C0E75D68C7ABE181C36B22668FEEA0C6662B412EA
28B9FBBAC304069F4755109ABD70078DB56B41A9E3D50ACDF8312B7407568A8EB09E45CD710B4CFB2B5804DE8C31792DF1D88EDD9A04FA40000000BFEAE620CE76ADB5C5AB194CB9B7
1310F2C4899DC791B2152EE28D52ABE9B061C9591BBB2EE89C5DCE5ED9BD34A1D5EE5BC76A4B2B4A909FE6CD0AA7A113C97B

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation:	write	Name:	DeviceTicket

Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000200000000010660000000100002000000001DA1D6B12A5EC90F4
F9706980DE59F73C4560375D4FCB70C2320F70F2BC4C6C6000000000E8000000002000200000007FB8CEDD17CB5141B2B0ADB40F9A7502AA36C37603876555ECDA09F3C20551CD20080
00044D2B2E46D6008C27AF67936328535D6B0B492601D7F4CB111286C54A126EB6E2E501C8339307775A205AB65F6ADEDA8ED2D78FA5A121722DEB8668C3EDCCE49C7D5AE173D74D788
37B54F0695FBB85FB0D1F625E4CA36C36991A60D6F08F3D6251B3F6679949B81F095A284E0D6C69D9123B2B4CB87D90CEA6FFE12EEDBD34C802FCF34B179A21FBAC23D500BC74ECC6E3
24991082ED59DB24D28D930B18C06F4DBB206E0F8CDBB64EB839B213167D15D2F0D6FF3F6EDE21C5243F96F26FA08EFDB4FD97D4793BE950B2008AB346677AEF90B56B32D6E41EAC8C13
15AFCE9B7A69B0B606A0225D3487A5DC700F92ABB26C990CCE027B75B7944984859C796A7B4F5DC2F877970B0F1BFA6B979EE8ED60E0202719B3A45C5FA4FA2C305BC34F6B141F3A6D56
64888CD6CC52FF89351D4B521062D792D2E756CECCC2753E7416737CC2076B1C6E2B09FB279F243C2FE8AADB602C896AA74D2C1167A18C4D7107760A0ED92462E570C2A107ABDDCCE9
06B643254858B87E2C1B4B15115CA3C4A959BA12A095B4D4D2D6E73ECACAD3325F8EB085D1AC05EAB140C420254102BE0E2127FFFA9ADAF935D670D13FAEFC59493CAD4F61D4A8CF29E
8D9CAF1C0D75CA0C69EDC04239CD12BAD8531FF11824E7B3D922F68C01B1976DF59A0B01C9AB9DC66CBE9E33F2017AA52BB21246AB3BE41BB9DBFD55E7CE77732340B94796942841625
190340C5A58FF3ECC4C506112762D8DA058510ED0DE2821E2A291448ED097BD0B70F1016E107AE388904A2008BC001C875C2F4C7499016BBDB6A93611B7AFEB82670E32F4D49D5DF3297
8201C9D6FAA84C494079B15236219F0FD905999F363764373B4E799336F97BDE8FC2D103191C0B5C57FD8DE5E9F39EAA9BD2F458D3AB68555096B6C80669DDDB75F135272F71C2A02BDD6DB36282979C77ABB710C
279C831E9E8610BF9A3E76733BC52D21B38C7C7995B9FC8222598FCC4F1910CFD9989E8CB1165F979C805DCDD0656BABF3B04AAB40733A99293B3B3B2C7F4819F913C66F451EA4B7B08
BDA834230C13351652A185D6C6C6BEE1FEE2403DB202051F7F197FEF38DD4D1A250AD09332B20C7EE810EA0F909B3BDF2AAE69CADE1B7824987D7F936FC8D31BE5B5188C38BA9FC2182
9CF14F81765D3DE4F994F7879DB0D4919C4A3C314713D4BDD78BDBDDE7EFCB0FE85740D49466B7EB4864F37F8ACB00B2217D80E2505ED0E076A0E8A90B770A6CDDF5AC3A4E0746B0D3B
23F511D2FAE902C9BB2122681EADE3E2174520F31656DDD145B95B94C89CEE0B98E3066BC633273A367920D6DDE0FD3A90DDC094466935C04E0B625BBAA4A38AA4DCD5C210DF94C8591
6D36E63F1192378475D018C0394A3A68CCBAD9095841340D9959F54110AEE1D3B812CCACB0D790E185818A618083727EEDAEA5B7BF75446FD14396B36646EB73B618321F64F790795E72
7A0F72BF0E8E084B7FC8BF7C46D2706FCCFF547593B49515568E03E4C7DC4B117B369E98967235852B326C884ED12670B0C3B36F360A08D8A9CCF9C60A5E72FA8F8F34207A0C8C99B31B
961E4079BE1B60E155DB0E807F627FAA76BF38BF057A6FF9900DD8DB585BBB68576F35A9D2B4D7F2ECE5F301E34F84DCBF9EA972D4B91729C4D059AB49765707DFFA2FCD69CD8C56E4B
BA843068A0A047490977B6A7C7973E2385FA4FA847E0F646920B220F170543E695FFEE9BA2FE3231C8AFCAC48CDA5E399EE83D5584DEE5344E48C1AE983871583C6685F62A3565C582498
DBD30C84C2AD3157348FFB26AE61022D505D4B17B0A1E409B012DB100947C1AD21219EDC8BADEDBE8EE50409EF82BB0BB53D08D9D319DD5956AB5772516099A1096B21EBCE36F00C78
A6F3E0D0397D6E6C3E00EB9B89A0D3B28B9D6967A61B596CADCD5375EC0CC6146A615E325C13B0C4E62CC658D470125C73410B0DA679FFF4F69D96F10B99443F086C3A06CD43D6A1897
725029E975933127E0EE3179B93B4952511AC871EB42F53A326FDAE2059C8753B47023DC689B41AAE67B8D1B1250B54928D267FF98637CF57A24A80CAA947E50DFCDF47C40943FC8FE0C
CE635E368AD6B64F6F03F38CA4FD5D264E46AEC80942640EC34202B7D63F00C82B16A6F000997D5EDC3BF3114DF549EEF147E90D08E239EF7912C2D6B42DF6198951113289F83EBAF7632
F809E2D86E69A73D48BFBC5C9E276F02379B94928849E1EBA5621E7B578C84DC084B83888A04192C36C3A243B055896625C43C729A6299D76FF5BB4079E4BB561817F324C6F4E7EE2CC7
F908F7CB8EF1AD3CADD7DCED5AEF9F8252F4E7E218F731311695DF35A2D27C86E9A727AE8817A04D98507B94909057359B7EA82ECECA38ED848FAD4CE9A41F48765F3AE6084AADD8874
DE6FBE78043AB20B0D44BB879549C80595BC040000000404819C25DD32F1C35983ACDE8BF3028A338ED6C1D59AC77388FB8DC2DD1F223F676CF6FBDDCFB701B20E1070A8F8C12CC99AC
3A2F9CDEA110A5A3C00BB0C049

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation:	write	Name:	DeviceId
Value:	00180010F429971D		

(PID) Process:	(1356) WerFault.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation:	write	Name:	ApplicationFlags
Value:	1		

(PID) Process:	(7824) Muadnrd.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(7824) Muadnrd.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	Name:	EnableAutoFileTracing

Value: 0			
(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write		**Name:**	EnableConsoleTracing
Value: 0			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write		**Name:**	FileTracingMask
Value:			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write		**Name:**	ConsoleTracingMask
Value:			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write		**Name:**	MaxFileSize
Value: 1048576			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write		**Name:**	FileDirectory
Value: %windir%\tracing			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	EnableFileTracing
Value: 0			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	EnableAutoFileTracing
Value: 0			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	EnableConsoleTracing
Value: 0			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	FileTracingMask
Value:			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	ConsoleTracingMask
Value:			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	MaxFileSize
Value: 1048576			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write		**Name:**	FileDirectory
Value: %windir%\tracing			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write		**Name:**	ProxyBypass
Value: 1			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write		**Name:**	IntranetName
Value: 1			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write		**Name:**	UNCAsIntranet
Value: 1			

(PID) Process: (7824) Muadnrd.exe		**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write		**Name:**	AutoDetect
Value: 0			

Files activity

Executable files	Suspicious files	Text files	Unknown types
6	190	40	5

Dropped files

PID	Process	Filename		Type
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json.tmp		binary

		MD5: EA8B62857DFDBD3D0BE7D7E4A954EC9A	SHA256: 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite- MD5: –	SHA256: –	–
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-current.bin MD5: 297E88D7CEB26E549254EC875649F4EB	SHA256: 8B75D4FB1845BAA06122888D11F6B65E6A36B140C54A72CC13DF390FD7C95702	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json MD5: EA8B62857DFDBD3D0BE7D7E4A954EC9A	SHA256: 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs-1.js MD5: 41C3031A19C68F7EBCEA0C4B077A2078	SHA256: 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873	text
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1451318868ntouromlalnodry--epcr.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2823318777ntouromlalnodry--naod.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs.js MD5: 41C3031A19C68F7EBCEA0C4B077A2078	SHA256: 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873	text
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\SiteSecurityServiceState.bin MD5: 47DDD2A463052776C50BF3B020C45FF9	SHA256: 0731CDA042482C8A43AB9A8E0BAD8938D1D12892640EF963AFBFB05D405B2351	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\AlternateServices.bin MD5: BD1F8541EE6955620BA2745F31D0EBBC	SHA256: 1938768BA2E4E560644DBA7C371966C04A2015959AAAA0698292F62C678C2F17	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db-journal MD5: 0F5D3BD22808C0A5A90A80E398828F84	SHA256: 3F6A5CE958BF096926459059C3222D354042D0123B8E08A4973FC9C6B358B7A1	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3561288849sdhlie.sqlite-shm MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.bin MD5: EF90022DF0735160DD056C0E6670E915	SHA256: 2B663C0B462A437C8DE3D9B95EE157AE181249B78BDD6F7BD73F7EB6D9E03F87	dbf
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.tmp MD5: EF90022DF0735160DD056C0E6670E915	SHA256: 2B663C0B462A437C8DE3D9B95EE157AE181249B78BDD6F7BD73F7EB6D9E03F87	dbf
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db MD5: B993525C060FE5A22B9747AC239529A8	SHA256: E9396152C2F9A52ABAB898F259D45C181003CEBE88BB54DE2A4C65402B6BB59F	sqlite
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite-journal MD5: 413E2331DE4FE9BC426A8DD5BA855C3A	SHA256: B017CF1CB55A148D29EA3B0A47A7A38AF056A95C8C601C4C894CA31C2A8CA80A	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-wal MD5: 119835D3E2EAAA9C0899A5CB90A7E82E	SHA256: 46E506DB1FBB13A316ECA333F7BBB3AE09C3A09EC0A1DEADDCF35283AAE0F233	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.vlpset MD5: DE0D88480C24350C59E1E9A3583DE0D1	SHA256: 01BA9F0B913E04ED10BD7166796483DD4F72005F249D6EE68B12117BE4B5D3C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json MD5: 5125D172D031232D9F8A809258BE53A3	SHA256: E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json MD5: 6F59D26E61E282B46AF0CF4386C0172F	SHA256: D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-wal MD5: F3E9E277A5E098BD3BA2EF5CFB4D767F	SHA256: CE1D2806161C4AE89E46FB5F8C54860DAE64403D6EC6BC86CB19A2AE8B816EAB	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.sbstore MD5: F92AB98A911930D5CDD4B0104AAE171D	SHA256: 3E82D8159C57E04D8A9BAEBDBD72362B08F7EFDBBADAFBDA996173ACF0C23B6E	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite-journal MD5: D68E8A062869338F6DBC42005285E463	SHA256: 0F3A6FA7BB4FA468B0C3882CC88DB989C6262CF9EAE4D683BDE59B03BA152AAC	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4.tmp MD5: 7EEF2C12470FD025856EC9A89CA300BE	SHA256: B2B6A2DFE42C8680CCED019981FDA3A84410120924161940CE460AC0C0A45834	jsonlz4

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4	binary
		MD5: E08EC08F038834A799C9F2F95F0A7ECD	SHA256: 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.sbstore	binary
		MD5: C9A39524AA5346ADDA89995267EB6EEC	SHA256: C2766B2303A07F8F6620303C94DB549F589073FB609EA3C28135923614B92722	

6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json.tmp	binary
		MD5: 6F59D26E61E282B46AF0CF4386C0172F	SHA256: D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.vlpset	binary
		MD5: 42959B02F1CEEC2316BCF528B3682DF6	SHA256: A4AA73B23B2D55C428BF7BB62BE731D4AA391D7A22D54586A7ADD1DE8856221F	

6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4	jsonlz4
		MD5: 7EEF2C12470FD025856EC9A89CA300BE	SHA256: B2B6A2DFE42C8680CCED019981FDA3A844101209241619 40CE460AC0C0A45834	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.vlpset	binary
		MD5: 52A01C93009ED9DF37776CD44897A165	SHA256: FC64A6418FB19DB437A16C2F7DDDC4B5DD071F02D7EF19CC0C1FD2C34BAD4ADC	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4.tmp	binary
		MD5: E08EC08F038834A799C9F2F95F0A7ECD	SHA256: 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.vlpset	binary
		MD5: 1074F10F2FB691DD5996FCCED30B5CB5	SHA256: 9051E2BBD3AD850B7353CF15FE5EDA284FAE8DC6555660E5762CE65ECE50D345	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.sbstore	binary
		MD5: 85F5DC8F04559E256822D2CBC7A7167E	SHA256: 860A6637305E4E5DE4ED5C86DC9A704189A5F55A2865DDFC44518562F12CF8CA	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.sbstore	binary
		MD5: DD0458514C9A922B45DA6A8BEBE47320	SHA256: D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json.tmp	binary
		MD5: 5125D172D031232D9F8A809258BE53A3	SHA256: E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.sbstore	binary
		MD5: 40ACCF6B4CBF993EB8DAAA09B2AC6508	SHA256: 282E12F46E25AA8CEB7227E837772B3B0DD3694F21BD156157B2A23D44A565E9	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.vlpset	binary
		MD5: 74008AA6F606067615E16B233A6808D2	SHA256: 5F5DCBDC2BBD909BCB355E6320E22FFA53CE61421C788CB3631F99B7FA472C24	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.sbstore	binary
		MD5: 8B4FFF284E845A5465890EEBCE0CAA62	SHA256: ACBAEC57934E402DE520C0FE376E68A41ED294365497C9220BA33A099F676C47	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.vlpset	binary
		MD5: DA94AE10143DE265746EAE28DE00B1E0	SHA256: B567D813342D76D81C51CAEB07646E70546FBAC1E3BE68580FBC9982E5BFB08A	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.vlpset	binary
		MD5: 40165280FF1345B5241EC2A9D1DA2AF0	SHA256: F80BDD5341D8B1EE946E344E258EF2D35C3C0BB6B13EB7B3E6A77467DFA8B97F	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.vlpset	binary
		MD5: 7194B6BFF691A056852A51E2E06CE8FE	SHA256: CBE2DC6ABFE25BEAD60F4DFAF419FC0F441FF8A8DD4A2FEBF5553BE1CBD90C49	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.vlpset	binary
		MD5: 130B9AC2BEEC5ADA274561105D81AE36	SHA256: 7D99FEC08182A5B95D18D1569EDAA2C60C2AAFBD15A56D8882F22F3B395E6460	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.sbstore	binary
		MD5: B9556D03AFF392142AD5691D2F867310	SHA256: CFD3909B41C1EE3CBCB8B7D2B1378065E7D3B543FFF1F2FB7A4F25C5FF41722C	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.sbstore	binary
		MD5: D5D6B4D59B4AE4E2DE4B40D0DA083571	SHA256: 000E3A78C72A210CA3B5417A3CDD294FBCE2A31661601C9D594C75CF2800571C	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.vlpset	—
		MD5: —	SHA256: —	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.vlpset	binary
		MD5: C2994D388F8780C87D35C352D9582985	SHA256: 7ED09F7D2BD632F70077A4AE4F2BD2F3FB654B03CD72652F51678B0C7D027F25	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.sbstore	binary
		MD5: AD3D0BC4B7B38A5FBE0DA2CDCE8A0245	SHA256: 3ABF8081360EB366F4DD3B98ACFFAFC73C5A9900CD19C3D45E100B7F3968EA34	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.sbstore	binary
		MD5: DD0458514C9A922B45DA6A8BEBE47320	SHA256: D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.vlpset	binary
		MD5: 0C0D67875BD75A0227C02DD8529BA01A	SHA256: 614BE0169EC36E67223EB9645A98DA66DBFDE5DFBB89BB064F428AAEABDD9D97	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.sbstore	binary
		MD5: 22698B4CF784DBBAE2D583F00491D43D	SHA256: 3849563088AE0677D61702A1310FDE26DE5DDD846D53037222D3EFE012197BF5	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.vlpset	binary
		MD5: 355BBE8195ACF89687747D60085C5B30	SHA256: BFC7F5B2CD28113650477CF2FB36F039682F679644659C66F445C25707CC9DE8	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.sbstore	binary
		MD5: 0C0CACE6CB13270CC067680F0C49A5D4	SHA256: 5F10F5155717403B1D2A18802DA0C1E55D44C40F655D971D9112C46519E7617B	

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.sbstore	binary

		MD5: 9F6B331AA1E070DCFEED473E76CE56C3 SHA256: 7DBBEA2DD387EEB85E1F56E02FC9989ACDE570CD43BFEF2C2A827093BA87DA6D	
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.vlpset MD5: 9AA2F992F7B0A8A39A2016958EEBF14C SHA256: 7F49C1E0EE79DB93724B95C0184640E79A99FA3E7C1D91D13B21954E2E7B94D2	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.sbstore MD5: DE11B7D1A2807D760720D2BAFC9243FC SHA256: F2FC25733FF62CB1CAE712299B9128E6E4D3BFFA6CD810773F0114E6E8D75008	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.metadata MD5: D706F661CA72A80ABFFCDC4FED3C4DDB SHA256: 1A5D3A3CA49DF4383BD2161A80B9C55B135BAC4161098E2438AAE1DBBDB40F02	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.vlpset MD5: C0E1AC752CB716038A8245AA68AF4C1F SHA256: E448D98C433F007A572960B5A956B474528893020773110D6921767BECFD3837	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.vlpset MD5: CF3989ADA19750F5BBD46BC8ADAFFB7A SHA256: C9C80D8B5B9464FD22E1C8B84BB80792FCFE69FA56F52F7B491E7FCB6DA6C8F4	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.metadata MD5: DA219EC22F607466BA385F3C98E884D8 SHA256: 2CD522E385FD6D09152431644EFBE440C4E1D3657C1607FCBB3F891F8A411663	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\.metadata-v2-tmp MD5: 04C97972673908F5ED4BDC2CAB464AAD SHA256: 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.sbstore MD5: 00A73169660DDB059CCF78D4378F256C SHA256: B949AB0D5C3F97B1C8D75A43A8C5C0718F820B60C0C3417824DC2B7832D69EB8	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.metadata MD5: 2A2D9C6ADE9C03E03C77BBDE841673FC SHA256: DF47EC2EC4BBAD6638D668A7233D070704F9EF2583D8B37AFDAAE8500C651536	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.vlpset MD5: FCC9C2C9B611A3264B68EBE180EB4248 SHA256: 6ECD378A537EEFE350B45CFA353741383F407D99D776BF23155A7825DC5DD2BC	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\.metadata-v2 MD5: 04C97972673908F5ED4BDC2CAB464AAD SHA256: 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto-1.vlpset MD5: — SHA256: —	—
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite-journal MD5: C91DE383C9FCA9AC5C0AA314673F6255 SHA256: 762FD03672E3D942F80CAEBFEA1928B60530B7FB95E937B242B5C9B8C2AAB99A	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.metadata MD5: 82E9807B2462B11303A5223234CF3E41 SHA256: 673B56A5F4085B2F52F29AE2112E8F65230DE3010CF625D1A27D303E790EB827	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.vlpset MD5: 9819E8BA5957767C478A506CFCE1D9EF SHA256: BC071CF03DF184C5F23EA47AFC8C75F40A9651BB35E9B296840E854D39C5AAD0	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.vlpset MD5: C543F008A2E02F4D4F095EAA94722B36 SHA256: 1363B9298E63DAD9E5FE8AED4DBDEB20415DE153B27A8C6AC8F552293B324D30	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.vlpset MD5: 94DD091E0A4A2C61EFEE13A77E2F0FC9 SHA256: CEB94C82C2A8B35DBBF12532548ED1D5402A656473983F146325E9639AA1077C	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.sbstore MD5: 519BEB1B01FC355BB388F1F75BE997FD SHA256: FFE2D3077B81AE6F51B220C1C661B276C823FA67DAD1D64FC5F17249FC54BDC0	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.sbstore MD5: 7BBA9B83F0F213C5A723209D4C9962CE SHA256: E1B8E7DEB0F34EEB6BF4D10E47E734A1FE829C365DF360B98646D7E11F2DD4C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.vlpset MD5: 1CB5A03C23989B1DDFBDC45C03204D12 SHA256: 191BBF1BB3E1263CC9F962753E9B9369B8AF50B91A314BDBB92FB58FE51B6AF1	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.sbstore MD5: 79F921E7A69AAD95115C030A2218875B SHA256: DAFBD8D4E15E55D11E90199D295D69C42189A79D4EA2806B880515FEAADA36CD	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.vlpset MD5: DF26E6FB795248D4D43138A4D346656C SHA256: 3B40F92474BEDB798EDFCD86C919C5BEE014AE80F0703AE6CCDED704629DDD4E	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite MD5: 2852B0CBBA9B0BB004851F3421E0B81C SHA256: CC0489E48450A25DAF1C2114EB820BB096AD77EBBC93EF25E253A37DCDD2A120	sqlite
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\usage MD5: 58DBA7ED5C9C7CA9F184BBA375F1660F SHA256: 280BD2D0DDAFD903B35A21DD24F7DFAA6EDCF218BAD02765273A54F949CE2936	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256.sbstore MD5: 9275B832091D9E3BFE50898A3BE022B5 SHA256: 38C52A5435B625083000A054489B95E033F7B352377510DF668CEE749DE5803E	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256.vlpset MD5: 5F93E0F827909390D257EBB27C77F392 SHA256: 5BCB684F3EE3B2EC2F4945655FBEF281C487399D6BF90451647DB1761715D4C8	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.sbstore MD5: F130C472E963FF3CEED251C65964B927 SHA256: E5D2A5BBE8AA43751EF7F7BC3A817A0963D56272A4C9B6055E60929606186CE2	binary

PID	Process	Path	Type
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.vlpset **MD5:** B50CF628E0082A7840D84D0CBE1CAD48 **SHA256:** 544DF79BCEF9DC8E082021E342C2A1B12CD0B8BDAF3687E0F23785406EDF33AE	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-new.bin **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache.bin **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.sbstore **MD5:** BE7D2765DEF13D5A252CC963F62E9DEC **SHA256:** 06EEE65E89C04B4E84A983437D9D98295DC2FE629A306244AACD7D2A787E5BCD	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto-1.vlpset **MD5:** 471E976917D93E066A2836D07189E46D **SHA256:** D124C902BAAB7044693C31369885B9915683718C10F31A9DE5A446732C066F5D	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto-1.vlpset **MD5:** C787F2747806B00C76CDBE040C93F98A **SHA256:** 2264A14B2545F13F8322AF37F352093105978D0BDD9AC9DDFB388802E4E7D50B	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto-1.vlpset **MD5:** 472D24AA36ABE086BE12D6567B7B82E1 **SHA256:** 0E8F4F9FAFC1D6B813E944E1DC093A4DFB48AB12E2AA798E02064EF022B07870	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-new.bin **MD5:** DFA790E6BFEBADC616EEF9D430FF8222 **SHA256:** 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache.bin **MD5:** DFA790E6BFEBADC616EEF9D430FF8222 **SHA256:** 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.sbstore **MD5:** BBB8F6725E298CF77AAD7FA594F40D87 **SHA256:** E1FE68E203733D0E1B5078B97632D9844C6E021AD78247BFE07AF8F81FA3B6A7	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.sbstore **MD5:** 03E14BE9BC0A656037A3B5942A546B9C **SHA256:** 6B768A574930C00B1AE0DA8677C98B99EFB66D81D2BFC7BC3856BA3DCAEE73E6	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.sbstore **MD5:** 51D0037241FD968870F54ACE34821097 **SHA256:** C0D2FF4A77D7B1383AF6534B54B0BC3E5DC9248447246D77BACC07D645587DE1	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.vlpset **MD5:** 41FAE052DA51D99364071F405C6C003E **SHA256:** 32FD3723664E71D8B405FF333C9140DC5CD221B7D20572255A41609A95001DB6	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.vlpset **MD5:** E64E488BEF398EE7185004BC761DD23C **SHA256:** 7EEE6F6E100DE281737D6F861771B464BD8FA49780B1BD2C1577E02F0C40B35E	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite-journal **MD5:** DDFA0B238218E11A9B4BB24CAE34D60E **SHA256:** 43A6F1E480E674D66E86EE8BCD7C8A57EB5668505C7FD7ECD83A598876216CE4	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-wal **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.vlpset **MD5:** AC3767913E46AC546879E57694B8BABA **SHA256:** F4DD01915D2ECEF9AA5D5475568C7D44A1B82B6E36A8B2BA96AA52AB54DA99ED	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child-new.bin **MD5:** FC15FBC5EA781C717736043BD6A44C93 **SHA256:** A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.vlpset **MD5:** C0E1AC752CB716038A8245AA68AF4C1F **SHA256:** E448D98C433F007A572960B5A956B474528893020773110D6921767BECFD3837	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.sbstore **MD5:** 9AEA09B15A3BB43D85144D3BD1AC7F75 **SHA256:** B880EBD4346DD9EA9EECD9D83B82F85493C4CB4EBEE50C07F6BCFA29D9C8D4E7	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child.bin **MD5:** FC15FBC5EA781C717736043BD6A44C93 **SHA256:** A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.vlpset **MD5:** 93879DA58B8AC3B3B58DCC6DD86D47EC **SHA256:** 08EA6E59EF882642C30441E0FAB4B6BC0A76B98BE273C540B065AB87F8BE1A97	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.sbstore **MD5:** 2CBCC17325808925E52D4DA835FE498B **SHA256:** 0E1911A712C9CDE4E411312E8F347C8B3560B19A2B93876D153EFACA52F486A5	binary
6596	firefox.exe	C:\Users\admin\Downloads\Jvczfhe.exe:Zone.Identifier **MD5:** DCE5191790621B5E424478CA69C47F55 **SHA256:** 86A3E68762720ABE870D1396794850220935115D3CCC8BB134FFA521244E3EF8	text
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.vlpset **MD5:** 0371AFCDE63B61B5CB0CC06ACFE66ED2 **SHA256:** FD64F028F01825E02F54E36E8A4B3597BA335974907106D6D147927DED1D961A	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.sbstore **MD5:** B4229CDB076DF6F4F59A6EF909CD8A66 **SHA256:** 485B156B4C5756577A36D077CD74D1AA62FCBB3158F45C31BEA4C64B02D443FB	binary

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.vlpset	binary
		MD5: 0E74BACCAB7B2923E25B62F282EDD71F　　SHA256: 34D4586E12D08DDD3171BC8A383EFD600926BE0F9F826D8362C61FB660DEA1B1	
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.vlpset	binary
		MD5: D0DE50C7B2BFE8240FEB389CD09E4E25　　SHA256: 4E25C5110096EE842CFAAE27485CE8994B03E7A00BFEE174581011A209EB3D98	
6596	firefox.exe	C:\Users\admin\Downloads\OOD5yt-b.exe.part	executable
		MD5: 5EC4256E6A2367502A8058F4BC8F4ECC　　SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BFDF2DDBDECED86AA9B2	
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.sbstore	binary
		MD5: 563B1CF89B324A8E37A899F001A340B0　　SHA256: 2142ECFACC145FE44095F8677BB3CCF021C2DD600C4627F1548B4F1E1C550DC9	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite	sqlite
		MD5: BA2A9081BD1D04E47C24B92588DA3038　　SHA256: FE95386724215C856F371614219653F672B20B6E2677FFA9C033F92DB1BFED71	
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE	binary
		MD5: FB64A9EBEDF48D3895381D5B7D80743D　　SHA256: EA21D495930AD76F267A33A0F593DBF0C7EA75E457FCAE49A29DAAD8BD920F42	
6596	firefox.exe	C:\Users\admin\Downloads\Jvczfhe.exe	executable
		MD5: 5EC4256E6A2367502A8058F4BC8F4ECC　　SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BFDF2DDBDECED86AA9B2	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4.tmp	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4　　SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4　　SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\previous.jsonlz4	binary
		MD5: 7B0DB853EFD8FCCFD078A91DE1B732CD　　SHA256: 72A40CD1C262925FE79A68A7F5704277F3FB1F23E3F815C24E89426A29957E89	
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C0018BB1B5834735BFA60CD063B31956	binary
		MD5: 06DDBFFCBB338D5FD21F4036E9D92EC2　　SHA256: E071C5DA2B1BDE45851423554AA4BFED3F488CFC4C597A9DF0A01B131AB7AFE0	
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C0018BB1B5834735BFA60CD063B31956	der
		MD5: 732CFEB76B91C4D13978A00B8C666ED7　　SHA256: 9FAB9FC0A1DA813E6DDB93904C1FCFA6546CFBE70747FF8468DDD14D2552DBD2	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json.tmp	binary
		MD5: 9121DAD27A71AA06B34E22B3247AC3C2　　SHA256: 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275	
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Jvczfhe.exe_e8f4a47beb21929faaf5bbbc7cb947adda294c9_7cb78550_56 41ad1f-ff35-4b34-8a69-19f8a8163939\Report.wer	—
		MD5: —　　SHA256: —	
1356	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\Jvczfhe.exe.7492.dmp	—
		MD5: —　　SHA256: —	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.baklz4	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4　　SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.bin	binary
		MD5: B818374634D95221DEB007E6C1DB1FB7　　SHA256: 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.tmp	binary
		MD5: B818374634D95221DEB007E6C1DB1FB7　　SHA256: 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json.tmp	binary
		MD5: 6A6ECF6080A1AF8963BD69766AC7E44D　　SHA256: 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info.tmp	text
		MD5: 2A461E9EB87FD1955CEA740A3444EE7A　　SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll.tmp	executable
		MD5: 842039753BF41FA5E11B3A1383061A87　　SHA256: D88DD3BFC4A558BB943F3CAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll	executable
		MD5: 842039753BF41FA5E11B3A1383061A87　　SHA256: D88DD3BFC4A558BB943F3CAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.files\2	binary
		MD5: D2AE97B1490CC258D04CF702943AABA6　　SHA256: EE70E50E8C808399C10883D9EA525638DCCF93570B6D855C7586CD15142EDDEC	
1356	WerFault.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\21253908F3CB05D51B1C2DA8B681A785	binary
		MD5: 82C30E45BF5F93A5DB1D5E47F913053B　　SHA256: 2C6BBFF9207065E8800C4AF0CB2748818ABB3CFFC0D6D518FE17F76A232F8967	
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFEF.tmp.dmp	binary
		MD5: C0E9448BABAD46120AF409E3D13582CB　　SHA256: B41D7B362ED06B68EC9F259AA83B820396DAA50F36EDF0CCDB4E70AD91ABBD75	
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB177.tmp.WERInternalMetadata.xml	xml
		MD5: DC4CB05F4E9CE6445F414D263FAE3174　　SHA256: E7F6B8755BAF770E61006D6C9844E09D026878445C3C95F5F3C36C0FBE15286A	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info	text
		MD5: 2A461E9EB87FD1955CEA740A3444EE7A　　SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC	
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1B6.tmp.xml	xml
		MD5: 737222720E097336E5D12487D43E1890　　SHA256: B5085F683C5AC51872E2C999D400C4E71B5B76427574CA1A1174FE0FE895254F	

PID	Process	Path	Type
6596	firefox.exe	C:\Users\admin\AppData\Local\Temp\tmpaddon **MD5:** 09372174E83DBBF696EE732FD2E875BB **SHA256:** C32EFAC42FAF4B9878FB8917C5E71D89FF40DE580C4F52F62E11C6CFAB55167F	compressed
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json **MD5:** 9121DAD27A71AA06B34E22B3247AC3C2 **SHA256:** 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\session-state.json **MD5:** 7AE136DBC9D972F5B344C42BC468D250 **SHA256:** E484553062E15D23A99ED613E21593E9EA3B492806C7E58614E901AC3EC78575	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json **MD5:** 6A6ECF6080A1AF8963BD69766AC7E44D **SHA256:** 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4.tmp **MD5:** A6338865EB252D0EF8FCF11FA9AF3F0D **SHA256:** 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965	jsonlz4
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.metadata **MD5:** BBF7EF2E4A3CA89407D6D4225590A924 **SHA256:** 0D49E29744875E37B5BFC2CFB0A32E30A801037BFF7DB25E4649F131937CF054	binary
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Muadnrd.exe_dd9d47dfcaa2177d1190b55ee6f3574cf671f90_4600b98d_c0351b42-4a4c-4b9d-bdbe-a700399d2592\Report.wer **MD5:** — **SHA256:** —	—
7584	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\Muadnrd.exe.7824.dmp **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping.tmp **MD5:** 1AA7FA53118748F72035DD5B174D228D **SHA256:** 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping **MD5:** 1AA7FA53118748F72035DD5B174D228D **SHA256:** 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77	tss
6596	firefox.exe	C:\Users\admin\Downloads\xtoROyHX.exe.part **MD5:** 9773175646F2942573BB40551B142A99 **SHA256:** B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0	executable
6596	firefox.exe	C:\Users\admin\Downloads\Muadnrd.exe:Zone.Identifier **MD5:** DCE5191790621B5E424478CA69C47F55 **SHA256:** 86A3E68762720ABE870D1396794850220935115D3CCC8BB134FFA521244E3EF8	text
6596	firefox.exe	C:\Users\admin\Downloads\Muadnrd.exe **MD5:** 9773175646F2942573BB40551B142A99 **SHA256:** B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0	executable
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4 **MD5:** A6338865EB252D0EF8FCF11FA9AF3F0D **SHA256:** 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\901A5L0GJXRA5ELANF4V.temp **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\rPDlkse4D7V1E6pAjMfUwMOHO6SrtemO4GCiWXN4xjU=.ico **MD5:** 6B120367FA9E50D6F91F30601EE58BB3 **SHA256:** 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0	image
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms~RF13ba1c.TMP **MD5:** 2D72BD10DFB5071E03E48FD977CF5800 **SHA256:** 8D7E1049FA26CA1CE3F1ABCC627F0E5AF693D3C791D62872320C360AA6E98D83	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF13ba4b.TMP **MD5:** A745A87D904244F96B205DD66BA8AD95 **SHA256:** E6603B79CF37A0C059B14E1BEBB0277323DFD4B57EEF3B4567417308CB24546C	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PN5BI8GYQV2728PG9PLV.temp **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.vlpset **MD5:** 8AC8A05028631170937EDA4CF0E0A35A **SHA256:** 456AB2C0E4E117D62DC529362EB22C725D410098868442729ADE5E4FF0822E78	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\webappsstore.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8665.tmp.dmp **MD5:** 394B3E4971EF4CC959394FA5412F9D75 **SHA256:** AE2527D5682A558469189B95620D0B109B073EDD3175D1C41067A0821F7F5287	binary
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8740.tmp.WERInternalMetadata.xml **MD5:** E9553BB3BC52242581D148E7FA13EA3A **SHA256:** 152E61F41D80497410469F77812A9BEC7909421779F0D65E6F0814F2478781A8	xml
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8761.tmp.xml **MD5:** 90DB48E0CCFB53E6070D4E3226E5C62F **SHA256:** C590E9240CE4B285EFDF6659C8D316E5DFF00FCCBADAFB44B71DCB7E316276AB	xml
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\4zihmJyKsj3j_uEUShbD8Te4dekBCaj7n+9q6HH9dZs=.ico **MD5:** 6B120367FA9E50D6F91F30601EE58BB3 **SHA256:** 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0	image
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\moz-extension+++5851050a-91b8-4af2-8e73-aa77522a1aee^userContextId=4294967295\idb\3647222921wleabcEoxlt-eengsairo.sqlite-shm	binary

		MD5: B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NM9BC1I0Q52BKO2U77CN.temp		binary
		MD5: 3B4F6A134652F65F9D64721C63771B02	**SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-shm		binary
		MD5: 885F6E89E582997D4F0201085F9C9E2E	**SHA256:** 8540D5F07FE075B726A4D466C4FC7B540C30BFB90B2FE3366A348C37EE759EB3	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-wal		sqlite-wal
		MD5: 0CEF0DA569CA50E00FB85F5987BF0465	**SHA256:** D90AD9719B1E9B57964213622C038274D825D3394A739D245EA39E9394023780	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite		sqlite
		MD5: 9FEB3178D08C74728B501EFBE503141A	**SHA256:** D163FC004C74F1723153227392C15978AA4EC36BD7CA66C33E03AEA22C200615	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-wal		binary
		MD5: 93CEBE93AC7602CB9837707C323076E7	**SHA256:** 66E2F6CDF7FCEBADFADAC924BDC033528046CF9BDB586A3354BE499372F3792D	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF1595e1.TMP		binary
		MD5: 3B4F6A134652F65F9D64721C63771B02	**SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite		binary
		MD5: F8D9E13C59BB94FA0F0A881AA3F2EC40	**SHA256:** E1C84814C8DA68EDCB96919FB8AF360110E7F0BBB137E9B2F06AD72C90FFBD1B	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-shm		binary
		MD5: D434AC3F132B538B6CB37868CB0A7910	**SHA256:** 64068F00FB106029D807BCD37CD9F5102DE442BD4FE3520AF3FF616A45A99899	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite		binary
		MD5: 391FA7DCD5DF3F07D4BD42397ABA3D9F	**SHA256:** 18FA18B374F3B77471C5115CB7827209C18894609BD1055FACD4BA9986C514DE	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
31	99	161	19

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6596	firefox.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	unknown	–	–	whitelisted
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	unknown	–	–	whitelisted
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/canonical.html	unknown	–	–	whitelisted
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.74:80	http://r11.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/	unknown	–	–	–
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	–	–	–
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	–	–	–
2268	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
7816	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	–
7816	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	–	–	–
6596	firefox.exe	GET	200	23.53.40.162:80	http://ciscobinary.openh264.org/openh264-win64-31c4d2e4a037526fd30d4e5c39f60885986cf865.zip	unknown	–	–	whitelisted

6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.74:80	http://r11.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/canonical.html	unknown	–	–	whitelisted
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	unknown	–	–	whitelisted
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	–
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	–
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	–

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1920	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
1048	RUXIMICS.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2120	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4	System	192.168.100.255:138	–	–	–	whitelisted
6596	firefox.exe	140.82.121.3:443	github.com	GITHUB	US	unknown
6596	firefox.exe	34.107.221.82:80	detectportal.firefox.com	GOOGLE	US	whitelisted
6596	firefox.exe	34.117.188.166:443	contile.services.mozilla.com	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	172.64.149.23:80	ocsp.sectigo.com	CLOUDFLARENET	US	unknown
6596	firefox.exe	184.24.77.69:80	r11.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	142.250.186.138:443	safebrowsing.googleapis.com	–	–	whitelisted
6596	firefox.exe	34.107.243.93:443	push.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	184.24.77.74:80	r11.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	142.250.186.67:80	o.pki.goog	GOOGLE	US	whitelisted
6596	firefox.exe	34.160.144.191:443	content-signature-2.cdn.mozilla.net	GOOGLE	US	unknown
6596	firefox.exe	184.24.77.81:80	r10.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	34.149.100.209:443	firefox.settings.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	185.199.109.154:443	github.githubassets.com	FASTLY	US	unknown
6596	firefox.exe	185.199.108.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
6596	firefox.exe	34.36.165.17:443	tiles-cdn.prod.ads.prod.webservices.mozgcp.net	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	140.82.114.21:443	collector.github.com	GITHUB	US	unknown
6596	firefox.exe	140.82.121.6:443	api.github.com	GITHUB	US	unknown
6596	firefox.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
1920	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3260	svchost.exe	40.115.3.253:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6596	firefox.exe	54.71.162.254:443	shavar.services.mozilla.com	AMAZON-02	US	unknown
6596	firefox.exe	34.120.158.37:443	tracking-protection.cdn.mozilla.net	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
6596	firefox.exe	142.250.74.206:443	sb-ssl.google.com	GOOGLE	US	whitelisted
6596	firefox.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
2268	svchost.exe	20.190.159.0:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2268	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
7816	SIHClient.exe	40.127.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
7816	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted

7816	SIHClient.exe	20.166.126.56:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6596	firefox.exe	35.201.103.21:443	normandy.cdn.mozilla.net	GOOGLE	US	unknown
6596	firefox.exe	35.244.181.201:443	star-mini.c10r.facebook.com	GOOGLE	US	unknown
6596	firefox.exe	35.190.72.216:443	location.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	34.98.75.36:443	classify-client.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	34.117.121.53:443	firefox-settings-attachments.cdn.mozilla.net	GOOGLE-CLOUD-PLATFORM	US	unknown
7492	Jvczfhe.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
3888	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
6596	firefox.exe	23.53.40.162:80	ciscobinary.openh264.org	Akamai International B.V.	DE	unknown
5152	InstallUtil.exe	91.92.253.47:7702	egehgdehjbhjtre.duckdns.org	—	BG	unknown
1356	WerFault.exe	104.208.16.94:443	watson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6596	firefox.exe	140.82.112.21:443	collector.github.com	GITHUB	US	unknown
7824	Muadnrd.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
7584	WerFault.exe	20.42.65.92:443	watson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 51.124.78.146	whitelisted
google.com	142.250.185.238	whitelisted
github.com	140.82.121.3	shared
detectportal.firefox.com	34.107.221.82	whitelisted
prod.detectportal.prod.cloudops.mozgcp.net	34.107.221.82 2600:1901:0:38d7::	whitelisted
example.org	93.184.215.14	whitelisted
ipv4only.arpa	192.0.0.170 192.0.0.171	whitelisted
contile.services.mozilla.com	34.117.188.166	whitelisted
spocs.getpocket.com	34.117.188.166	whitelisted
prod.ads.prod.webservices.mozgcp.net	34.117.188.166	unknown
ocsp.sectigo.com	172.64.149.23 104.18.38.233	whitelisted
r11.o.lencr.org	184.24.77.69 184.24.77.61 184.24.77.75 184.24.77.65 184.24.77.71 184.24.77.48 184.24.77.45 184.24.77.74 184.24.77.76 184.24.77.56	whitelisted
ocsp.comodoca.com.cdn.cloudflare.net	172.64.149.23 104.18.38.233 2606:4700:4400::ac40:9517 2606:4700:4400::6812:26e9	whitelisted
a1887.dscq.akamai.net	184.24.77.69 184.24.77.61 184.24.77.75 184.24.77.65 184.24.77.71 184.24.77.48 184.24.77.45 184.24.77.74 2a02:26f0:3500:e::1732:8355 2a02:26f0:3500:e::1732:8352 2a02:26f0:3500:e::1732:8344 184.24.77.76 184.24.77.56	whitelisted

	2a02:26f0:3500:e::1732:8348 2a02:26f0:3500:e::1732:835b	
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
push.services.mozilla.com	34.107.243.93	whitelisted
safebrowsing.googleapis.com	142.250.186.138 2a00:1450:4001:806::200a	whitelisted
r10.o.lencr.org	184.24.77.81 184.24.77.69 184.24.77.56 184.24.77.79 184.24.77.71 184.24.77.75 184.24.77.48 184.24.77.67	whitelisted
firefox.settings.services.mozilla.com	34.149.100.209	whitelisted
prod.remote-settings.prod.webservices.mozgcp.net	34.149.100.209	whitelisted
o.pki.goog	142.250.186.67	whitelisted
pki-goog.l.google.com	142.250.186.67 2a00:1450:4001:828::2003	whitelisted
github.githubassets.com	185.199.109.154 185.199.108.154 185.199.111.154 185.199.110.154	whitelisted
avatars.githubusercontent.com	185.199.108.133 185.199.111.133 185.199.109.133 185.199.110.133 2606:50c0:8000::154 2606:50c0:8001::154 2606:50c0:8003::154 2606:50c0:8002::154	whitelisted
tiles-cdn.prod.ads.prod.webservices.mozgcp.net	34.36.165.17 2600:1901:0:8e3f::	unknown
collector.github.com	140.82.114.21 140.82.112.21	whitelisted
glb-db52c2cf8be544.github.com	140.82.114.21 140.82.112.21	whitelisted
api.github.com	140.82.121.6	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
fp2e7a.wpc.phicdn.net	192.229.221.95 2606:2800:233:fa02:67b:9ff6:6107:833	whitelisted
www.amazon.de	52.222.239.71	whitelisted
www.youtube.com	172.217.16.206 142.250.186.142 142.250.184.206 216.58.206.78 172.217.23.110 142.250.186.174 172.217.18.14 142.250.185.174 142.250.186.46 216.58.206.46 142.250.185.110 142.250.185.142 142.250.185.78 172.217.18.110 142.250.184.238 142.250.186.110	whitelisted
www.facebook.com	157.240.252.35	whitelisted
partnerprogramm.otto.de	54.37.171.144	whitelisted
www.ebay.de	23.206.209.88 2.16.97.102	whitelisted
www.wikipedia.org	185.15.59.224	whitelisted
www.reddit.com	151.101.65.140 151.101.1.140	whitelisted

	151.101.129.140	
	151.101.193.140	
star-mini.c10r.facebook.com	157.240.252.35	whitelisted
	35.244.181.201	
	2a03:2880:f177:83:face:b00c:0:25de	
dyna.wikimedia.org	185.15.59.224	whitelisted
	2a02:ec80:300:ed1a::1	
reddit.map.fastly.net	151.101.65.140	whitelisted
	151.101.1.140	
	151.101.129.140	
	151.101.193.140	
e11847.a.akamaiedge.net	23.206.209.88	whitelisted
	2.16.97.102	
djvbdz1obemzo.cloudfront.net	52.222.239.71	whitelisted
	2600:9000:223e:7e00:e:13a1:b914:2321	
	2600:9000:223e:ae00:e:13a1:b914:2321	
	2600:9000:223e:5400:e:13a1:b914:2321	
	2600:9000:223e:4000:e:13a1:b914:2321	
	2600:9000:223e:6c00:e:13a1:b914:2321	
	2600:9000:223e:f800:e:13a1:b914:2321	
	2600:9000:223e:1400:e:13a1:b914:2321	
	2600:9000:223e:c000:e:13a1:b914:2321	
	2600:9000:223e:a200:e:13a1:b914:2321	
	2600:9000:223e:c200:e:13a1:b914:2321	
	2600:9000:223e:8c00:e:13a1:b914:2321	
	2600:9000:223e:9200:e:13a1:b914:2321	
	2600:9000:223e:9800:e:13a1:b914:2321	
	2600:9000:223e:3a00:e:13a1:b914:2321	
	2600:9000:223e:c00:e:13a1:b914:2321	
	2600:9000:223e:e000:e:13a1:b914:2321	
youtube-ui.l.google.com	172.217.16.206	whitelisted
	142.250.186.142	
	142.250.184.206	
	216.58.206.78	
	172.217.23.110	
	142.250.186.174	
	172.217.18.14	
	142.250.185.174	
	142.250.186.46	
	216.58.206.46	
	142.250.185.110	
	142.250.185.142	
	142.250.185.78	
	172.217.18.110	
	142.250.184.238	
	142.250.186.110	
	2a00:1450:4001:827::200e	
	2a00:1450:4001:81d::200e	
	2a00:1450:4001:80b::200e	
	2a00:1450:4001:829::200e	
client.wns.windows.com	40.115.3.253	whitelisted
shavar.services.mozilla.com	54.71.162.254	whitelisted
	44.226.249.47	
	44.239.24.213	
shavar.prod.mozaws.net	54.71.162.254	whitelisted
	44.226.249.47	
	44.239.24.213	
tracking-protection.cdn.mozilla.net	34.120.158.37	whitelisted
tracking-protection.prod.mozaws.net	34.120.158.37	whitelisted
raw.githubusercontent.com	185.199.110.133	shared
	185.199.109.133	
	185.199.108.133	
	185.199.111.133	
	2606:50c0:8002::154	
	2606:50c0:8003::154	
	2606:50c0:8001::154	
	2606:50c0:8000::154	
sb-ssl.google.com	142.250.74.206	whitelisted
sb-ssl.l.google.com	142.250.74.206	whitelisted
	2a00:1450:4001:803::200e	
www.microsoft.com	23.35.229.160	whitelisted
login.live.com	20.190.159.0	whitelisted
	20.190.159.2	
	20.190.159.23	

	40.126.31.73	
	20.190.159.71	
	40.126.31.69	
	20.190.159.68	
	20.190.159.75	
slscr.update.microsoft.com	40.127.169.103	whitelisted
fe3cr.delivery.mp.microsoft.com	20.166.126.56	whitelisted
normandy.cdn.mozilla.net	35.201.103.21	whitelisted
normandy-cdn.services.mozilla.com	35.201.103.21	whitelisted
aus5.mozilla.org	35.244.181.201	whitelisted
prod.balrog.prod.cloudops.mozgcp.net	35.244.181.201	whitelisted
location.services.mozilla.com	35.190.72.216	whitelisted
prod.classify-client.prod.webservices.mozgcp.net	35.190.72.216	unknown
classify-client.services.mozilla.com	34.98.75.36	whitelisted
prod-classifyclient.normandy.prod.cloudops.mozgcp.net	34.98.75.36	whitelisted
firefox-settings-attachments.cdn.mozilla.net	34.117.121.53	whitelisted
attachments.prod.remote-settings.prod.webservices.mozgcp.net	34.117.121.53	whitelisted
nexusrules.officeapps.live.com	52.111.227.11	whitelisted
ciscobinary.openh264.org	23.53.40.162 23.53.40.129	whitelisted
a19.dscg10.akamai.net	23.53.40.162 23.53.40.129 2a02:26f0:3100::1735:2881 2a02:26f0:3100::1735:28a2	whitelisted
egehgdehjbhjtre.duckdns.org	91.92.253.47	unknown
watson.events.data.microsoft.com	104.208.16.94 20.42.65.92	whitelisted
dns.msftncsi.com	131.107.255.255	whitelisted

Threats

PID	Process	Class	Message
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
–	–	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain

Debug output strings

No debug info

No debug info