Recorded Future®
Sandbox

Malware Analysis Report

2025-10-25 17:39

Sample ID	251025-v6srqagr8t
Target	prefs-1.js
SHA256	08f2f0a58ca7701d46634eaff0c021511a0f249e4e3ba292f3d435834cf0bc1c
Tags	execution persistence

score

3/10

Table of Contents

Part 1. Analysis Overview

score

3/10

SHA256
08f2f0a58ca7701d46634eaff0c021511a0f249e4e3ba292f3d435834cf0bc1c

Threat Level: Likely benign

The file prefs-1.js was found to be: Likely benign.

Malicious Activity Summary

execution persistence

Command and Scripting Interpreter: JavaScript

Uses Task Scheduler COM API

Checks processor information in registry

Modifies registry class

Suspicious use of SendNotifyMessage

Suspicious use of SetWindowsHookEx

Suspicious use of AdjustPrivilegeToken

Suspicious use of FindShellTrayWindow

Suspicious use of WriteProcessMemory

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043		
Resource Development TA0042		
Initial Access TA0001		
Execution **TA0002**	Command and Scripting In… T1059 JavaScript T1059.007	
Persistence TA0003		
Privilege Escalation TA0004		
Defense Evasion TA0005		
Credential Access TA0006		
Discovery **TA0007**	Query Registry T1012	System Information Disco… T1082
Lateral Movement TA0008		
Collection TA0009		
Command and Control TA0011		
Exfiltration TA0010		
Impact TA0040		

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-25 17:36

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:36	2025-10-25 17:39	win10v2004-20251016-en	149s	150s

4. 2. Command Line

```
wscript.exe C:\Users\Admin\AppData\Local\Temp\prefs-1.js
```

4. 3. Signatures

Command and Scripting Interpreter: JavaScript

execution

Checks processor information in registry

Description	Indicator	Process	Target
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\Update Revision	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\VendorIdentifier	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\Update Signature	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\Update Revision	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\Update Signature	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\VendorIdentifier	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~Mhz	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\Local Settings	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\Local Settings	C:\Windows\system32\OpenWith.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Suspicious use of FindShellTrayWindow

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Suspicious use of SendNotifyMessage

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
N/A	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Description	Indicator	Process	Target
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1300 wrote to memory of 5956	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Description	Indicator	Process	Target
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 1116	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5956 wrote to memory of 3676	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Uses Task Scheduler COM API

persistence

4. 4. Processes

C:\Windows\system32\wscript.exe

```
wscript.exe C:\Users\Admin\AppData\Local\Temp\prefs-1.js
```

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

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

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

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

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -prefsHandle 1988 -prefsLen 27099
-prefMapHandle 1468 -prefMapSize 270279 -ipcHandle 2060 -initialChannelId {e02c9a70-706a-4f81-b580-02f456f50859} -parentPid
5956 -crashReporter "\\.\pipe\gecko-crash-server-pipe.5956" -appDir "C:\Program Files\Mozilla Firefox\browser" - 1 gpu
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -prefsHandle 2456 -prefsLen 27135
-prefMapHandle 2460 -prefMapSize 270279 -ipcHandle 2476 -initialChannelId {a3ff4856-8d27-42cc-ab3f-5f84e1843e0e} -parentPid
5956 -crashReporter "\\.\pipe\gecko-crash-server-pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla
Firefox\browser" - 2 socket
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 3816 -prefsLen 27325 -prefMapHandle
3820 -prefMapSize 270279 -jsInitHandle 3824 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 3832 -
initialChannelId {39d3eb2e-c472-4c90-b4e6-cc1f96744c99} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 3 tab
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -prefsHandle 4028 -prefsLen 27325
-prefMapHandle 4032 -prefMapSize 270279 -ipcHandle 4136 -initialChannelId {2f403dd6-6802-4ee0-b788-259aab623748} -parentPid
5956 -crashReporter "\\.\pipe\gecko-crash-server-pipe.5956" -appDir "C:\Program Files\Mozilla Firefox\browser" - 4 rdd
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 4484 -prefsLen 34824 -prefMapHandle
4488 -prefMapSize 270279 -jsInitHandle 4492 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 4500 -
initialChannelId {2f533632-3358-419c-a4a9-3ba554dcdfba} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 5 tab
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -sandboxingKind 0 -prefsHandle
4748 -prefsLen 35012 -prefMapHandle 4756 -prefMapSize 270279 -ipcHandle 4732 -initialChannelId
{56b93fc7-7ddd-4b97-9932-629fe0fc4fe6} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-pipe.5956" -
win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 6 utility
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 5072 -prefsLen 32900 -prefMapHandle
4400 -prefMapSize 270279 -jsInitHandle 5164 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5176 -
initialChannelId {672a4625-2b45-442d-992a-47a104fe0db1} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 7 tab
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 4676 -prefsLen 32900 -prefMapHandle
4372 -prefMapSize 270279 -jsInitHandle 4784 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 2932 -
initialChannelId {5bdd7e20-c157-4ac4-9964-0611d168a3b6} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 8 tab
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 5472 -prefsLen 32900 -prefMapHandle
5476 -prefMapSize 270279 -jsInitHandle 5480 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 4784 -
initialChannelId {5d8cfbe8-914d-4939-bc04-332cf973ac32} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 9 tab
```

C:\Windows\system32\OpenWith.exe

```
C:\Windows\system32\OpenWith.exe -Embedding
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url "C:\Users\Admin\AppData\Local\Temp\prefs-1.js"
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url C:\Users\Admin\AppData\Local\Temp\prefs-1.js
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 2748 -prefsLen 35081 -prefMapHandle
4360 -prefMapSize 270279 -jsInitHandle 4364 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5524 -
initialChannelId {ef2c9c32-273b-4c7a-9d02-4dcadbabfb6f} -parentPid 5956 -crashReporter "\\.\pipe\gecko-crash-server-
pipe.5956" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 10 tab
```

4. 5. Network

Country	Destination	Domain	Proto
GB	92.123.128.139:443	www.bing.com	tcp
US	8.8.8.8:53	tse1.mm.bing.net	udp
US	150.171.28.10:443	tse1.mm.bing.net	tcp
US	150.171.28.10:443	tse1.mm.bing.net	tcp
US	150.171.28.10:443	tse1.mm.bing.net	tcp
US	150.171.28.10:443	tse1.mm.bing.net	tcp
US	8.8.8.8:53	c.pki.goog	udp
GB	142.250.129.94:80	c.pki.goog	tcp
N/A	127.0.0.1:49913		tcp
US	8.8.8.8:53	mozilla.map.fastly.net	udp
US	8.8.8.8:53	mozilla.map.fastly.net	udp
US	8.8.8.8:53	spocs.getpocket.com	udp
US	8.8.8.8:53	mc.prod.ads.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	merino.services.mozilla.com	udp
US	8.8.8.8:53	mc.prod.ads.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	content-signature-chains.prod.autograph.services.mozaws.net	udp
US	8.8.8.8:53	content-signature-chains.prod.autograph.services.mozaws.net	udp
US	8.8.8.8:53	example.org	udp
US	8.8.8.8:53	ipv4only.arpa	udp
US	34.107.221.82:80	detectportal.firefox.com	tcp
US	8.8.8.8:53	prod.detectportal.prod.cloudops.mozgcp.net	udp
US	8.8.8.8:53	prod.detectportal.prod.cloudops.mozgcp.net	udp
N/A	127.0.0.1:49921		tcp
US	8.8.8.8:53	location.services.mozilla.com	udp
US	8.8.8.8:53	mozilla.map.fastly.net	udp
US	35.190.72.216:443	location.services.mozilla.com	tcp
US	8.8.8.8:53	prod.classify-client.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	prod.classify-client.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	archive.mozilla.org	udp
US	151.101.67.19:443	archive.mozilla.org	tcp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
US	8.8.8.8:53	ciscobinary.openh264.org	udp
US	35.190.72.216:443	prod.classify-client.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
DE	18.66.248.93:443	ciscobinary.openh264.org	tcp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp
US	34.104.35.123:443	edgedl.me.gvt1.com	tcp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp

4. 6. Files

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\05a8e782-31d1-4b68-91bf-bc7dc65a2fc1

MD5	2fe4fd32ec41d44451a259a73e32cc29
SHA1	1dfce385fa7c5cb720f37db040a12cabc7ad6ad6
SHA256	c7fffa120e7a7db9e90644ca9b4aefbb9924342460b17e758b5cb11f56e220cf
SHA512	46f77ebb28c5dd2c3b08b6786a24d8815f0002bd3fb1614105c98d32768bd4b99aeca3ddcd548ae27fa8589708043c089c0588676042220165fd50dc51ecf24a

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\db\data.safe.tmp

MD5	dc718e8603e31607f76593c73bf45492
SHA1	afdfd234ddee289b8dd87236f91c3b8f0911bbe3
SHA256	8c73e6e586db474fe2bf4a6412fe518281d31892a419c6595b1ea597ea364b7b
SHA512	a3c2e8f61d0b6b648866009cb04085df0353fc4ed8fd7422c9a5c8ab0801f0213e349c6b4ea05885756a7174e400a2b1d51f0b8b5822514f5f134c05cfc6857a

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\901629b3-4faa-4594-a636-c8a8a3bc1e32

MD5	137ea5c898e942f7073aa187fd3861ff
SHA1	72f419a45974590b92425e73931f514b49a454b1
SHA256	383804a9509ab2489f4af63a0413738d1e99a82f9016707d2cd6cd43d80e51ef
SHA512	0bd51691b28d9b0917ab24fd1a7f1ac450bbec7e119f60e5e897fc5413f0cc0d19e585d416af3c980b45437dc6f60fef25ba675af593cb5576b80e4f164e41aa

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\1e1bb166-1e2d-422c-9d6d-4c89e8e5edb4

MD5	d758352cc7138aadad23305f9b924687
SHA1	bdb890e15c7c705c4b070f69525c744eb198b96e
SHA256	30ac084e953065b14b782d1b6d2d0b083b5419ad031dc14e5f6f4eb5f2c2ed3c
SHA512	45afa6f5892b263105386d72973180482041e8effe65fc17e7fdc5583e472de8d921b3b349e72d58428c561d4e8359f76de41864930911af6577b312177c90f5

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\2d5a1fb6-f7b4-4b4b-a839-ef3d12432cba

MD5	e99b6e253446b1ffac8be1d4120c9466
SHA1	6bf5c62530d39276d22953f91152665615a857c4
SHA256	bb59e1e4a851a0e93fd1074ad35f78429ab64bfa4cc456369a9939010aa45cfc
SHA512	c66c521b1bdc1c2685adff498bb2734b4fa20a8a3ee983aa42ea60b917fcaa1535058bd4036958a1cfc262238be850eeab8e9a624ad6849f386bef575551b91c

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\9ce337be-bb26-4d18-9303-476ac2b940d8

MD5	759195d114f3e31cab6c151bcc7539e1
SHA1	76a511939ce1a73816814326598773b250b76829
SHA256	169cd8bf2a5b68d2dd225b4ab820a412097425e6ae7113e6d3710c981a4c37c5
SHA512	3a6c289ca743d3bd1a644a0f0089346dcb248925b5f39dbbd9909441394cc0c4d535e16cbeb613c904467fff25115317e6584892674c49b156a8859d1eb0e0d3

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\35eb48fa-8c86-45ce-8243-f28f5c73fef7

MD5	1775cc2535376a98f8d709ad2edb4bb5
SHA1	76b5f39783f6e468dd1de6f5ecf07ea760884fe3
SHA256	7c506058f09dd17fb49ab02da56171faae39dab49382c25fcc8a0258c00399f2
SHA512	51b9a55078186c33bdb7b318e08932285072f27fb810fa1e3aeaf45a1ec40b8ac237098a2132fcbf49b0b4e11accbcb0e2fd6502a3b13e900b6b6c6d7617ad1e

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\events\events

MD5	92d428b61413d1017ca251f1a3c36987
SHA1	7e5259bf4e59fee00046846c27c78dadd7fec0c7
SHA256	ffa12a3d5c1f6f0c7efc5e4e237e49e09d79d17e21c2794d1549bace05e26ee2
SHA512	7551607f9fffedc78be38748932e48dc4c92a3ea4ccc60858b3eefc42fe42191433f67169a9dbf503d201bc41cb54f6da4323d8564eeba6cd73014596a8c8e19

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\db\data.safe.tmp

MD5	bc60225d21517db9f7bde1e3f28273e7
SHA1	2d340ab447b9b52597d3a912d41bac43efb0f074
SHA256	b2be111143a71eb3c7527274e3c090ba6eb3d7ea648fa5b7e5408c476659ae4c
SHA512	ab38d2a1b7b79b66e9622787758219964884 63b6d22cd03ce394e67d0ededde9c37dba203b78896be658003f097e45f3742ce024824249be3cb80652a9348d5e

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\db\data.safe.tmp

MD5	a8ab9cb870574c518ecce25516f5d9b4
SHA1	9b7d2f0d972a1da1da70dbb3361a003a87ad46bd
SHA256	91c58527c1a268290c3d1106c0962832a9777474ded01fa12165b6727c919d4d
SHA512	529b460a492f8ff5043403ade9cdd00adc4cb1498f96275493723fe8955b05737c16c60df99f72c28cd0c594fd4ca829f1fefd63ef0412baec9fbb06d3285e24

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\prefs.js

MD5	e6e5a80f79c5ae2ae91896b3613493b3
SHA1	ddc4cf5ea904c333f8842b4612cc3103c5e2f4a1
SHA256	689551b5ffb3189b99128b6a861a04ddff80d4fe46d89320c5b74e7a528cedce
SHA512	96def9dc724efc71a2391c4e7b7bf7a830ea11031e623cdd111f42c80d1ac779e939aae8427441a11b0ef841279c3073440b9d1b7b934789fcf65bce64bbf4dc

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\prefs-1.js

MD5	212167d2d703a4d079896a984dbae059
SHA1	16b3010260859b75cf727cb59344b5e45acf4c0e
SHA256	c61f78f1d190ab666037c18b1dc285fddf2c91bac298db036acd012a501e737c
SHA512	46f67d8b923375758ad963d848c3fea63e19e8720fa1738b687cdfba1a7361f2e6df170430e6f9f159a106d96dbfc007eaf3dfea9cbbb5ce0f6c6035000ae658

C:\Users\Admin\AppData\Local\Mozilla\Firefox\Profiles\1akhe1kg.default-release\startupCache\webext.sc.lz4

MD5	b52f9bccfa158e695f8ac67e2f9ee9bb
SHA1	aa5d68f2b3aa44c2e98da7d25fb3331cc0d2e8a8
SHA256	a6dfb299ee445fc8d1c01b0d00400d0711fa0a7213dcbed122336f9dccb65438
SHA512	cd36559b310eb019fab3e26b37ec94531eb725aa2eafab5f7d70e81238c03cd071d0efe0f129aab8f0ea2f4d6b6a1bbe79bcbd48e3be0cc7f6aad83873ca97c0

C:\Users\Admin\AppData\Local\Temp\tmpaddon

MD5	25e8156b7f7ca8dad999ee2b93a32b71
SHA1	db587e9e9559b433cee57435cb97a83963659430
SHA256	ddf3ba4e25a622276755133e0cce5605b83719c7cab3546e09acbfed00d6a986
SHA512	1211b2fa997ba13ff926aec58b6b35a81d7fe108b0caa8f4d6369d0a37f8481373b78a4b201651243adde9e2b2699ce929482a46226ff6299b0a0e40fe2ddc56

C:\Users\Admin\AppData\Local\Mozilla\Firefox\Profiles\1akhe1kg.default-release\cache2\entries\577120C5183923526312DC856F6825FC1C7D072F

MD5	cc4d00d17eaeae4cd94917983ecdbdb1
SHA1	e0888c7ce22398de8e414b2d704f96a3d544ab03
SHA256	4616bba8cecd2fc7bfca0e04a54a70cfbec711de6772bfd848b63f84576f459c
SHA512	59f2e437e7f4f770cddd5c0b95db7c8b559f745134806e6a661d52ceae8b65e5cc83d2abc2461f45904262451b264f9e652ec67bb125d07f722faadef63a0900

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\extensions.json

MD5	db57b8c5bef863f0c0daef69608e35a7
SHA1	b3d898cc862b68c61b43333b8b88aee7dc589570
SHA256	8b575dbf600fd1c2b9a10a9a088256e497a936f8f40bfcab41b31051538c1400
SHA512	a4aaa74cc314a7a2d602dc16cf6ee0ed7a30d4bf2afedfabcf9aca49d46db49210c102f0c9d7d7a66159f6872d3042381bf869cba3a6942a2c2c0234f5dfde29

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\prefs-1.js

MD5	00abf11fd47cf68da3cabeaeda32af7e
SHA1	54a18a209ec153b3f708d28e5ec16ca61ee51055
SHA256	3a3ad904be6222c73f7e1ae56c5594bfce7679c938c100666e1bf72d1ac59045
SHA512	7b825471c3e3290d4692f482a86e205525a9998d7b298f30aef86d33d7824e8eabcbbba1cb7ec9b733c5b9be23fe2731b41492ac2f1e404cb07c0cbc0435dda3

C:\Users\Admin\AppData\Local\Temp\tmpaddon

MD5	e690f995973164fe425f76589b1be2d9
SHA1	e947c4dad203aab37a003194dddc7980c74fa712
SHA256	87862f4bc8559fbe578389a9501dc01c4c585edb4bb03b238493327296d60171
SHA512	77991110c1d195616e936d27151d02e4d957be6c20a4f3b3511567868b5ddffc6abbfdc668d17672f5d681f12b20237c7905f9b0daaa6d71dcdac4b38f2448b2

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\gmp-gmpopenh264\2.6.0\gmpopenh264.info

MD5	ae29912407dfadf0d683982d4fb57293
SHA1	0542053f5a6ce07dc206f69230109be4a5e25775
SHA256	fe7686a6281f0ab519c32c788ce0da0d01640425018dcffcfcb81105757f6fe6
SHA512	6f9083152c02f93a900cb69b1ce879e0c0d69453f1046280ca549a0301ae7925facdda6329f7ccb61726addee78ba2fffc5ba3491a185f139f3155716caf0a8d

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\gmp-gmpopenh264\2.6.0\gmpopenh264.dll

MD5	626073e8dcf656ac4130e3283c51cbba
SHA1	7e3197e5792e34a67bfef9727ce1dd7dc151284c
SHA256	37c005a7789747b412d6c0a6a4c30d15732da3d857b4f94b744be1a67231b651
SHA512	eebdeef5e47aeadfeebdbab8625f4ec91e15c4c4e4db4be91ea41be4a3da1e1afeed305f6470e5d6b2a31c41cbfb5548b35a15fccd7896d3fde7cdf402d7a339

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\sessionstore-backups\recovery.baklz4

MD5	39aeb173da7141b87822c6f25903ccfd
SHA1	03c06b05fa6b3b7804603c1800ce33fa2431e883
SHA256	89556545e71386d0aa78c68e6f61a4e238968a94bfee26a418234f08ba4b0983
SHA512	25777c054ae7309dbfe3b46ee7fc3c59f67f42348b7433a40b2fc3d984c2d380c30b6a189b2186bb5a94cf5f70a163abb92d764005d783517e395c7cdc470dd5

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\db\data.safe.tmp

MD5	13d99dc06a50745e3be87e02b796a146
SHA1	4b3e74e13f0e78a14e5fd5e3285d9d0c0f9936e0
SHA256	f2d78eb9d29df03e534b1354279078381f9c5ce51cc60cf5e707b03272a07baa
SHA512	b1fa81ade87bb72195cb6ad3309945d94a745749211ad17ba179f78d66afe2424884de1a4b4100e59f59f576b8bec83f5b1b098d58ca0a7244ba590e8c58f6c9

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\gmp-widevinecdm\4.10.2891.0\manifest.json

MD5	32aeacedce82bafbcba8d1ade9e88d5a
SHA1	a9b4858d2ae0b6595705634fd024f7e076426a24
SHA256	4ed3c6389f6f7cd94db5cd0f870c34a296fc0de3b1e707fccf01645b455790ce
SHA512	67dfe5632188714ec87f3c79dbe217a0ae4dfb784f3fac63affd20fef8b8ef1978c28b3bf7955f3daaf3004ac5316b1ffa964683b0676841bab4274c325c6e2b

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\gmp-widevinecdm\4.10.2891.0\widevinecdm.dll

MD5	1b32d1ec35a7ead1671efc0782b7edf0
SHA1	8e3274b9f2938ff2252ed74779dd6322c601a0c8
SHA256	3ed0dec36754402707c2ae4fbfa887fe3089945f6f7c1a8a3e6c1e64ad1c2648
SHA512	ab452caa2a529b5bf3874c291f1ffb2a30d9ea43dae5df6a6995dde4bc3506648c749317f0d8e94c31214e62f18f855d933b6d0b6b44634b01e058d3c5fcb499

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\sessionstore-backups\recovery.baklz4

MD5	bb887097f41b9fc80962386292339f1a
SHA1	5e576a85603aadc1feb313c14a9e053c04aec6c5
SHA256	1b958d93534dc0b25bc567c800fcb13a2d2b49bdc54a8811c640ac4bfef17528
SHA512	f01635f129eebc45a76935333578e1f0de9cc78b2df37651f6570091d737b0856b5a7db081684a8e63cb48647966e142a932e3112fe24e620c5471e477d6aef5

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\sessionstore-backups\recovery.baklz4

MD5	2967f8c3f0749d97ea4395dae1f04bb9
SHA1	e227c27fef3c54af3adc94e67df467c7d307dcb7
SHA256	323ff797c4470b57898598ed8ed65d39016c2ef6bfd289f12a02bc4df6336eac
SHA512	f5b1af18ea06e26f4eaae3e30362ca17654595eb9286daf45f807201928896edd1da7ea62b3d9a048b8ae34ba7564c190d5e077416ee7524a460587e599cb456

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite

MD5	e4ae48133835b76e88f7f6f47b255ccc
SHA1	4f33ea0f9945c59c1c8758e66e161bf3ee48fde7
SHA256	c72d9628d2c6d1af8f665230215ded8b26c50d129feb1e6c4f0ae16a7381f863
SHA512	7777b6af5d3a3fc715059b417e1a2507e473ca226e66cfe00cd259943b6c018c24b5f8f6f53d43655ca61fb5c665ca818b363c689bd87a08310691eb7a188bf6

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:36	2025-10-25 17:39	win11-20251015-en	149s	103s

5. 2. Command Line

```
wscript.exe C:\Users\Admin\AppData\Local\Temp\prefs-1.js
```

5. 3. Signatures

> **Command and Scripting Interpreter: JavaScript**
>
> execution

5. 4. Processes

C:\Windows\system32\wscript.exe

```
wscript.exe C:\Users\Admin\AppData\Local\Temp\prefs-1.js
```

5. 5. Network

5. 6. Files

N/A