Recorded Future®
Sandbox

Malware Analysis Report

2025-10-11 16:18

Sample ID	251011-tmxqwsvvft
Target	prefs.js
SHA256	d228bd82adba46065a76849223b549443a7da85be05505b794c36fc82777d591
Tags	execution persistence

score

6/10

Table of Contents

Part 1. Analysis Overview

SHA256
d228bd82adba46065a76849223b549443a7da85be05505b794c36fc82777d591

Threat Level: Shows suspicious behavior

The file prefs.js was found to be: Shows suspicious behavior.

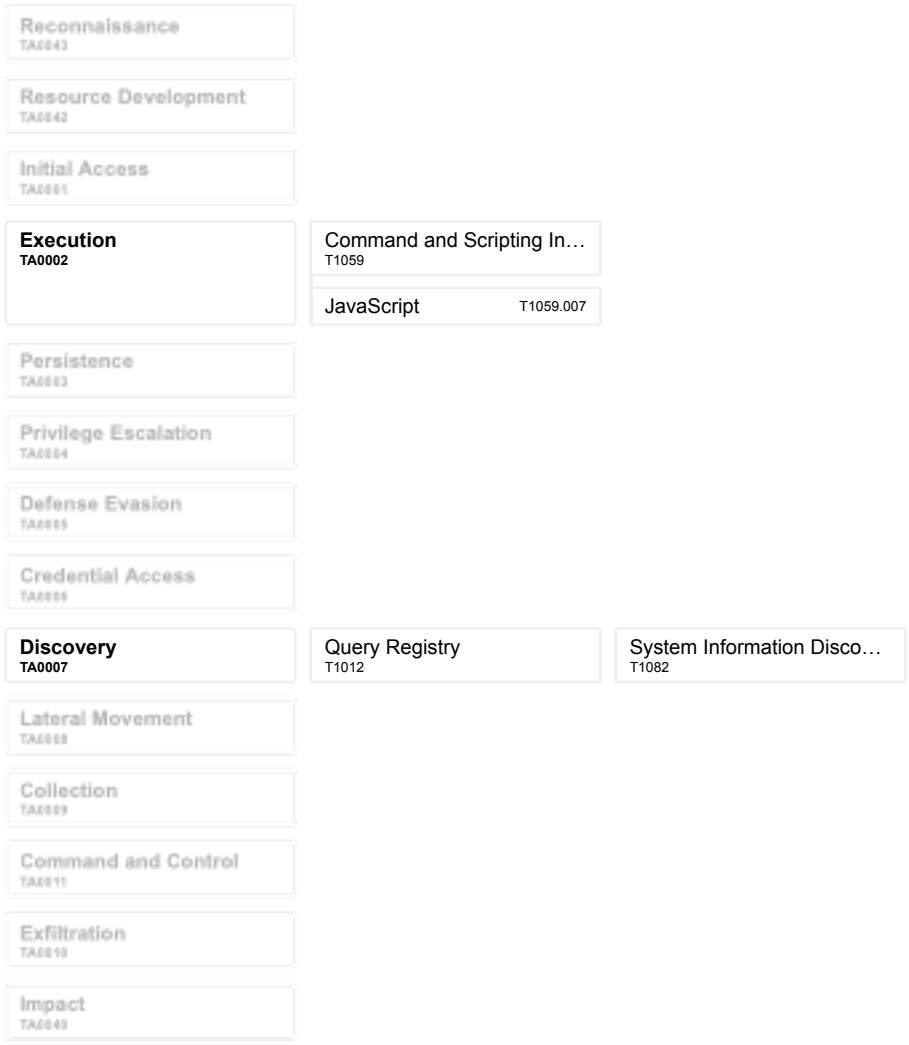
Malicious Activity Summary

execution	persistence

- **Drops desktop.ini file(s)**
- **Command and Scripting Interpreter: JavaScript**
- **Uses Task Scheduler COM API**
- **Checks processor information in registry**
- **Suspicious use of AdjustPrivilegeToken**
- **Suspicious use of SendNotifyMessage**
- **Suspicious use of SetWindowsHookEx**
- **Suspicious use of WriteProcessMemory**
- **Modifies registry class**
- **Suspicious use of FindShellTrayWindow**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16



Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-11 16:11

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-11 16:11	2025-10-11 16:17	win10ltsc2021-20250619-en	329s	327s

4. 2. Command Line

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

4. 3. Signatures

Drops desktop.ini file(s)

Description	Indicator	Process	Target
File opened for modification	C:\Users\Admin\Documents\desktop.ini	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
File opened for modification	C:\Users\Public\desktop.ini	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
File opened for modification	C:\Users\Public\Documents\desktop.ini	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

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\~Mhz	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\~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 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 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\Update Revision	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\ProcessorNameString	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 value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	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

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 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 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 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

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-1916311604-1391214034-3562683274-1000_Classes\Local Settings	C:\Program Files\Mozilla Firefox\firefox.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1916311604-1391214034-3562683274-1000_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
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
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
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 SendNotifyMessage

Description	Indicator	Process	Target

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:\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:\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:\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

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Description	Indicator	Process	Target
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5188 wrote to memory of 1812	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 3860	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 1812 wrote to memory of 4944	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.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 1976 -prefsLen 27100 -prefMapHandle 1980 -prefMapSize 270279 -ipcHandle 2068 -initialChannelId {86dca5d3-4df1-4041-a690-b1e7ae89a72a} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 2444 -prefsLen 27136 -prefMapHandle 2448 -prefMapSize 270279 -ipcHandle 2456 -initialChannelId {192e9fcb-2c8b-4b8f-9c2b-85e1d8d63997} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 3656 -prefsLen 27277 -prefMapHandle 3660 -prefMapSize 270279 -jsInitHandle 3664 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 3668 -initialChannelId {2c36f089-b71c-4e40-a7fc-426a16012775} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 3816 -prefsLen 27277 -prefMapHandle 3820 -prefMapSize 270279 -ipcHandle 3844 -initialChannelId {b34cf247-72a5-4d85-bfef-eb61e0d02853} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 3088 -prefsLen 34776 -prefMapHandle 3112 -prefMapSize 270279 -jsInitHandle 3116 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 4572 -initialChannelId {0e851316-e8cd-425e-85b8-7e648828a7ed} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 2812 -prefsLen 34906 -prefMapHandle 2588 -prefMapSize 270279 -ipcHandle 3280 -initialChannelId {a128af0a-7a67-4b5c-a9fe-e74197f17cad} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 5576 -prefsLen 32845 -prefMapHandle 5580 -prefMapSize 270279 -jsInitHandle 5584 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5588 -initialChannelId {0f62a52c-f26c-4a23-954e-06d047aaa8d5} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 5760 -prefsLen 32845 -prefMapHandle 5764 -prefMapSize 270279 -jsInitHandle 5768 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5736 -initialChannelId {c77aac92-7d81-463d-b95e-e370a7a0261e} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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 5940 -prefsLen 32845 -prefMapHandle 5944 -prefMapSize 270279 -jsInitHandle 5948 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5956 -initialChannelId {4f8470ac-b3ba-428f-ad9b-0ee1bbc06342} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -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\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js"
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -isForBrowser -prefsHandle 15888 -prefsLen 40423 -prefMapHandle 20264 -prefMapSize 270279 -jsInitHandle 20140 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 2940 -initialChannelId {bf33a009-a7a6-4b38-9861-88298e6d0c34} -parentPid 1812 -crashReporter "\\.\pipe\gecko-crash-server-pipe.1812" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 10 tab
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	c.pki.goog	udp
SG	64.233.170.94:80	c.pki.goog	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	merino.services.mozilla.com	udp
N/A	127.0.0.1:49830		tcp
N/A	127.0.0.1:49837		tcp
US	8.8.8.8:53	mc.prod.ads.prod.webservices.mozgcp.net	udp
US	151.101.1.91:443	merino.services.mozilla.com	tcp
US	8.8.8.8:53	content-signature-chains.prod.autograph.services.mozaws.net	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	example.org	udp
US	8.8.8.8:53	ipv4only.arpa	udp
US	8.8.8.8:53	prod.detectportal.prod.cloudops.mozgcp.net	udp
US	34.107.221.82:80	prod.detectportal.prod.cloudops.mozgcp.net	tcp
US	8.8.8.8:53	prod.detectportal.prod.cloudops.mozgcp.net	udp
US	8.8.8.8:53	checkappexec.microsoft.com	udp
JP	40.74.81.198:443	checkappexec.microsoft.com	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	35.190.72.216:443	prod.classify-client.prod.webservices.mozgcp.net	udp
US	8.8.8.8:53	archive.mozilla.org	udp
US	151.101.195.19:443	archive.mozilla.org	tcp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
US	8.8.8.8:53	ciscobinary.openh264.org	udp
US	34.104.35.123:443	edgedl.me.gvt1.com	tcp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp
SG	13.35.238.59:443	d156sk07toobyl.cloudfront.net	tcp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp
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	firefox-settings-attachments.cdn.mozilla.net	udp
US	151.101.1.91:443	firefox-settings-attachments.cdn.mozilla.net	tcp

4. 6. Files

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\c61c30ac-3b7b-4f84-a223-90f7fea36aac

MD5	b5d74c4242f1e7bee7a46e94c574a4ef
SHA1	3310442660437abd78a623f743a1cd697d2c2180
SHA256	87d3ff62bbfcf7a24ecf4cf418aced82995678c3b9dc3761bd8908e84faa9f5e
SHA512	777bb04dcbd492574bb5b4862c6a7a8132af75ca0f42eb08471dc33972464deb95972eaeeed3fa8aacfc52ff9c409abc5968cde813a344385bf7257a14138684

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\db\data.safe.tmp

MD5	221cace68ad9f7033b8d8f9cdd60ba7d
SHA1	df82c63c6419772fe472e53025a2cc6cb84fbf79
SHA256	4696b9e84f55c416b249b1b36ab2df09ceea7600e3b07e923b5e9fb585e4b658
SHA512	c890b5634c10320d926e387e1277cfe8797f5fc58a38cc30a91b190a2b1e186182778eeb96b29b83b89c970b1c92123e494e043b0d847b60299755b0180665cd

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\8020e86c-007e-4b7e-b029-2b9a1faed6b2

MD5	1865d5143bc9f728a08c1c526b7420b1
SHA1	44f697562d1950c1615af40d5ba0e395420bb62c
SHA256	c7c6e5122af8a0b0841673179a2a0c13a8a5d0e73c87c74c492471f2896b58ce
SHA512	b92905180f4db248f8132ab0640c9b9b0c01bc97566180c5e005037b782eb0d54b1f9b774437ec84b682fed720e353d94db338b2d10431b027f94872208ec951

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\fb496ff6-df2d-4864-9443-a2ec5c337efa

MD5	4e307822dc20d77d67923f96fd55f18f
SHA1	fd9b264133e1cfd1e6cd6b9e1611a981a7deab25
SHA256	540f9a30697b7b417fe52000ca7375a017d57fb8ecba0b89f74f922f294b18ed
SHA512	387fbe2fa28e2fd0cc8ddaabe99736b295d3a65c73d4bc76aafadaca5a324141d68bdcaf9c42e2d2695e699a07674ceb04628c5183e4ca3639f8c885bcbf8545

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\90f2f4ea-c8f3-4bcf-bc21-a495195a934f

MD5	16bc352541e75058d1060d86a8e0805b
SHA1	f6d835816cbb336c7e12e86bd2c2126cc9e22786
SHA256	fdb295bb11dae50b20d9520d3785832de211edb8bb7d9d29a665f3d3ccb87747
SHA512	e40038937242e6502d97583f3c88c27eb87491c3075fd63d589d27a2fc5e0aa15b203fda288c4d1695a3ab6f818450227671b1be83c37410d1b407ecd697a1f3

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\e5a4b5dd-e0df-44e3-ac45-8832ebef6018

MD5	32319d3bbd655614afbfa2122d9a411c
SHA1	9f10b37c0d47762fce7f01e8a31e85e759a667cd
SHA256	c8ad931b1f8a11df7713bf001da2435b84310cf2d1c085eb8bddcc4c807dce41
SHA512	77b00f44866b1e512a4adc969c1f242052218bda247a73c65dec1758e752f9d4eecf8a4602badbc5222946cc58ff2da1cc42332b8ded2af87ea7df90249f4fa8

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\events\events

MD5	4257f92c2d190b199ed80064dd394dfd
SHA1	d9f97a7996b61289bd83446f652e8b0c19fb96b8
SHA256	c69da1e72ff56773eaebc2e2919bb648530ce20e36330c9b36cae376de01d880
SHA512	ea70478157c2e1185b6a9ba4e7327022d01933ca451c7646f7ee79dda28e650090b46f3a72bd91de643efdea205d8bdf84ed58e1c3721aedc3529ae7c5373f1c

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\pending_pings\2394f19d-da9e-4415-b448-5f72d5dd7d18

MD5	67071983c8169bf7383893b87cf2bf2c
SHA1	8e2dcb3a34bdfee757ef3127a8d42183db518936
SHA256	49cb99da11145f6728356fb21539ce2dcd5798ace58bcdf0a7ee8a9225476a05
SHA512	c4710c23a6e542537ce94059d0eb95136190a8d976680aa0e6c4e61662238279cc80502197f004d1db846f24408e1c480040b616b4f68010c5cf9ed94db1fd5a

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\db\data.safe.tmp

MD5	d84f41e1a953d7f8f256def05281d7af
SHA1	82c670d81dd8ca28dd37fb44afbba92a4318a210
SHA256	c85fe2c5e8b10af7f7cfcec5f1ad8357f813ab746c5c16b7a475b58cbab43b58
SHA512	7bb93d241eb390668c815ccc195e2a92b7dd25eb4e9ba1a3a684d67ddbc9ec8bef2d46ede40d88deb4bda63820d5781a501d2a32e015b8d483c93df21b164672

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js

MD5	3d5fdc32dd825e16ef830022996a249e
SHA1	cebe466a271f68217d3e9d14b9bc33448c77ff3a
SHA256	94ce23420478911ee356a29fe122efb146682afc55f8a89d98d5aafd4cc28f03
SHA512	885cce7d775d882bd569263da04de992971db348813308a623d1e006f8159617a3391c0b2e5c8a1a7c0c414d64686cfea2638c6e061293b14153bf986aa0ca79

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs-1.js

MD5	8f8f8db920eb3a4b6f06f886def48acc
SHA1	031800b2df7da6e73a947b5d19290857995026fc
SHA256	403146a8f0472b22f99276ce851b1db5121b096661a6d2387f5b04ec5ecd6660
SHA512	e4e5ad69729b7cc031b38576c914833f93068e196dc1ba3e8cbe41ebe4a08f265ed3a62782edfbf30f4b35dc66c6c3381fa9087a83098e95b65d732ace0d49b3

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\sessionstore-backups\recovery.baklz4

MD5	fa248fd568368d462a469589c9bbb2a6
SHA1	e3fbf55089f4756c14375e659f735523b1f22c0a
SHA256	67b32b089ec75f694182d7cee6e13c4221ded77ec6c67cafc6103c2307f690c3
SHA512	947cd18f05f6b60d8479dd917d50f1cfa13a39761f9d8320483224160620e3980fcb2d979d1386a87c9f98a92f424ca1610932caedab2444fd9b84f52e5fee1f

C:\Users\Admin\AppData\Local\Mozilla\Firefox\Profiles\st0i9lle.default-release\cache2\entries\C2717B99982B5EE4C407BE5FD5A3BE0F00D7649C

MD5	ffa813dd133c93c77654ba1d7c5f09e7
SHA1	0b949c17f735303ab449539c40456c41d171a606
SHA256	ef4b491725830af12f5dc21e5b013d0f081fed9cff455b588a91bdcf9dae8e6b
SHA512	af6ee39a767c119b655bb78b75c7eeef999bed642cec0563034f8d9ac0838cbe42587281fbae00cafe50c19651e304cc5d16f98c644c66006931a9ac0c786f61

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js

MD5	1cd06c72b8951f3250ed32db5f8c7a4a
SHA1	a29631653f79f226d692d06d37fdb3094db98119
SHA256	532478cc4d872c50dc9eba773e2e83d6ac380a4dc1de2c5c4fafc7550e8e8a87
SHA512	54094398eaf7cbc41b4f585e71b18cd79bfe00741ce5c30cb2eadc08757d5e2c1eafaf198da3f175cf683380e7127a7eb9ac24cac7fe853d9de729e54a08046b

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js

MD5	2479c96b9d478923c90bd7d44801c65b
SHA1	d23629cf33deb0ccffbcdee2e0ff11c3b34099ef
SHA256	8e19e1e08a678a907df76b34c1a15b4c95782a675dcf3bf2db19e3394d5c037a
SHA512	c9fbfe13aedc3389256bf005b38afa28c4f2b15981325f33e6fe2767a63fb4bd412493b9c602ad8220acaa20b09e24fcdad771b3e6327b50f68a40841b5df658

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

MD5	25e8156b7f7ca8dad999ee2b93a32b71
SHA1	db587e9e9559b433cee57435cb97a83963659430
SHA256	ddf3ba4e25a622276755133e0cce5605b83719c7cab3546e09acbfed00d6a986
SHA512	1211b2fa997ba13ff926aec58b6b35a81d7fe108b0caa8f4d6369d0a37f8481373b78a4b201651243adde9e2b2699ce929482a46226ff6299b0a0e40fe2ddc56

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\datareporting\glean\events\events

MD5	360d9b7d9e5e0f2265641f6e28308a62
SHA1	eb9a869f3daf90fee854ce51b2b1580045a62827
SHA256	ca43b2c84ba202beacd8431886a413aba8eba6bde3d9b2cffab0a89828bb1ce1
SHA512	cc1a9330df45c6275e74b7bcda2665a2178ad74297666689aa4057a49467c0046740ecf5d26a0dd15c57615b84289dc3e705605f5bfce49d880aa3b95470a47b

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\extensions.json

MD5	1dab42888398e243f82bb252ac5c426a
SHA1	2836e78c1ac1c209e287eac229ab92563fe64189
SHA256	e0d0f082565a3c65df6be617eb6766ee0a78f9a2653f6caafa1623dfa1aeee92
SHA512	d322bffa0b7c1bcfc1887d108080f9df7a595e188e2b447727fd256adb167785b339a2a09b1d2a1e7b40fff7d22ee109dc56f81566f2a4c82eeb3bea7d93e308

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

MD5	e690f995973164fe425f76589b1be2d9
SHA1	e947c4dad203aab37a003194dddc7980c74fa712
SHA256	87862f4bc8559fbe578389a9501dc01c4c585edb4bb03b238493327296d60171
SHA512	77991110c1d195616e936d27151d02e4d957be6c20a4f3b3511567868b5ddffc6abbfdc668d17672f5d681f12b20237c7905f9b0daaa6d71dcdac4b38f2448b2

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.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\st0i9lle.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\st0i9lle.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\st0i9lle.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\st0i9lle.default-release\sessionstore-backups\recovery.jsonlz4

MD5	48aaf7c734a2d0b48c4191b65a489a98
SHA1	b6a42f89369b43697cd68041256fed906461b75b
SHA256	d148addb56cfa0d76fe4f427a3e3f309aa03e75572862842da42e7faeff28eb7
SHA512	1d16a34a2d8976103d0351eb47df11ceaf70b58d84f3dd8d5e1cb33dc7b693f381b83bd4ea99f86160d3772190f0a107ddd767ea4abab40b9ef2ad5cf743fce1

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs-1.js

MD5	19e6a8ad63481b950f6067142843f6e0
SHA1	c6d636342d33edb5e9a12e8dfa2ddad468e7a078
SHA256	5bf5be69bc3bc5a6453f5cb10260ebde1b5e28f84e7772ed95429740862fe451
SHA512	e971ab7af3b49dd1d051337c41587ab3b0294f388bcc59d7c7ff0517a5c0dd73f657b40224c5863b9200da42031f91c873234b50c8de0f0de300dad917d7abb0

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite

MD5	0da5456b76cd21560bd42bc784a98045
SHA1	aa8f74778dc1ce9806296dc671c20366f40ab509
SHA256	1f557c1dec7dc03de8f3bed22efbfef2ae27bf0260521726f6caa8b89aa8339c
SHA512	0dd6b0529bdfd5391fc32de188ae22d2ed002ec21c665a34e93fe1e6ecf05b41074734e297ae4fcd9e78718d26b0d50961275782d1f31464476c0efb166a3bf0

C:\Users\Admin\AppData\Local\Temp\1d7541d8-9d89-4fee-8768-322ef645a433.zip

MD5	27a612cab8388ee9579632f193623e9c
SHA1	2a99e329e4406e30ae3cb31320313b2190e6d79b
SHA256	f32681b5175b2b29e0a1f7473960403258fcd13c50c3fdf150365e7e35249c11
SHA512	3ee04df50a16d2ed64a8e585b9f86eb55bee71d8915681650ba7ceaff93eba23ece4a6db6b4072652adbb20c669162bf4471e1666b80b37897841c05c57cd44b

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\prefs.js

MD5	db30bcda81550b9e3699b8e4c48c783c
SHA1	7acda4521549e1c4caa71bb11d948ba567270dca
SHA256	940ac0b64dc56636247ef70e2e0aeddb68d3b9a60d2c00c523da4cadf82d6fe1
SHA512	651f597eb8cc929ae8065ed75595adb798996213275af0c2d6a51f6262b97f79e3c409b22fc2c6285779a126d4dd5397e3923140f78d22e0f5f433d5850f561f

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\sessionstore-backups\recovery.baklz4

MD5	607a9002900539c34dd5b565c4eb4c25
SHA1	985e3803318ab3ba64bd6dadccaa2fbbaf65f774
SHA256	148c42a6087ee35a17574ecffe2cb3dd184ed5ce3589ff76b6ee31c23b3aa835
SHA512	0b6cfe1dca52b36f92c2c13112d776b12f8d146ba5fbfb825b6316055240bab8a1e5eaf04ff13d161913d07aa0ac539dad42b9c3d77f086d6a05202cfe8dde66

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\st0i9lle.default-release\sessionstore-backups\recovery.baklz4

MD5	bc3897eb4e9d44887213ee1297ca8913
SHA1	81e9026dd6e4b5aec90fb1d2a3d7f4c4286d5b1a
SHA256	c5375be1dd48d0eb8ead2b31511a23c68af008eb4655cdd12b632dce91bf6d57
SHA512	e73e19268d4fecbfbb24287e74520ebba7b940f2df3ae7d067731f7a419af7732ce091951fcfca2ea89c73260a3a5457a66129a04d876ace1fb4900708d8c2bc

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-11 16:11	2025-10-11 16:14	win11-20250619-en	149s	132s

5. 2. Command Line

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

5. 5. Network

5. 6. Files

N/A