Recorded Future®
Sandbox

Malware Analysis Report

2025-10-11 15:35

Sample ID	251011-kbpfpszyhy
Target	SearchHoverUnifiedTileModelCache.dat
SHA256	c8d763647dbbb092b3c76cfcb98899ea1c5b3f38059c3e707b1943e588c36118
Tags	persistence

score

3/10

Table of Contents

Part 1. Analysis Overview

Part 2. MITRE ATT&CK

- 2. 1. Enterprise Matrix V16

Part 3. Analysis: static1

- 3. 1. Detonation Overview
- 3. 2. Signatures

Part 4. Analysis: behavioral1

- 4. 1. Detonation Overview
- 4. 2. Command Line
- 4. 3. Signatures
- 4. 4. Processes
- 4. 5. Network
- 4. 6. Files

Part 5. Analysis: behavioral2

- 5. 1. Detonation Overview
- 5. 2. Command Line
- 5. 3. Signatures
- 5. 4. Processes
- 5. 5. Network
- 5. 6. Files

Part 1. Analysis Overview

score

3/10

SHA256
c8d763647dbbb092b3c76cfcb98899ea1c5b3f38059c3e707b1943e588c36118

Threat Level: Likely benign

The file SearchHoverUnifiedTileModelCache.dat was found to be: Likely benign.

Malicious Activity Summary

persistence

Enumerates physical storage devices

Checks processor information in registry

Modifies registry class

Suspicious behavior: GetForegroundWindowSpam

Suspicious use of AdjustPrivilegeToken

Suspicious use of SetWindowsHookEx

Suspicious use of WriteProcessMemory

Uses Task Scheduler COM API

Suspicious use of FindShellTrayWindow

Suspicious use of SendNotifyMessage

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043		
Resource Development TA0042		
Initial Access TA0001		
Execution TA0002		
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
2025-10-11 08:25

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 08:25	2025-10-11 08:26	win10v2004-20250610-en	30s	22s

4. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\SearchHoverUnifiedTileModelCache.dat
```

4. 3. Signatures

Enumerates physical storage devices

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 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 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\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 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 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\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-1-5-21-815616237-4012932787-4224613991-1000_Classes\Local Settings	C:\Windows\system32\cmd.exe	N/A

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\Local Settings	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\dat_auto_file	C:\Windows\system32\OpenWith.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\.dat\ = "dat_auto_file"	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\dat_auto_file\shell\open\command	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\.dat	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\dat_auto_file\shell\open	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\dat_auto_file\shell	C:\Windows\system32\OpenWith.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\dat_auto_file\shell\open\command\ = "\"C:\\Program Files\\Mozilla Firefox\\firefox.exe\" -osint -url \"%1\""	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-815616237-4012932787-4224613991-1000_Classes\Local Settings	C:\Program Files\Mozilla Firefox\firefox.exe	N/A

Suspicious behavior: GetForegroundWindowSpam

Description	Indicator	Process	Target
N/A	N/A	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

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

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

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
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:\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:\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:\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:\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:\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

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 5016 wrote to memory of 4628	N/A	C:\Windows\system32\OpenWith.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 5016 wrote to memory of 4628	N/A	C:\Windows\system32\OpenWith.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Description	Indicator	Process	Target
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4628 wrote to memory of 4524	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 2640	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4524 wrote to memory of 4548	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\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\SearchHoverUnifiedTileModelCache.dat
```

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\SearchHoverUnifiedTileModelCache.dat"
```

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

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

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -prefsHandle 2020 -prefsLen 27099 -
prefMapHandle 2024 -prefMapSize 270279 -ipcHandle 2100 -initialChannelId {02113982-579b-455b-a65a-53f9742929f8} -parentPid
4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -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 2500 -prefsLen 27135 -
prefMapHandle 2504 -prefMapSize 270279 -ipcHandle 2512 -initialChannelId {bd776d13-fcf5-49d9-8386-33f8faa0006f} -parentPid
4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -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 3820 -prefsLen 27276 -prefMapHandle
3824 -prefMapSize 270279 -jsInitHandle 3828 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 3836 -initialChannelId
{36a2b8d7-d571-4aac-b870-49aa7a3e24c5} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -
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 3988 -prefsLen 27276 -
prefMapHandle 3992 -prefMapSize 270279 -ipcHandle 4072 -initialChannelId {b3608e21-a65c-417f-8ebf-a0e43328e2d3} -parentPid
4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -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 2924 -prefsLen 34775 -prefMapHandle
2872 -prefMapSize 270279 -jsInitHandle 2876 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 4460 -initialChannelId
{199869f5-6017-461b-8373-c53ab7fa2106} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -
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 5180
-prefsLen 35012 -prefMapHandle 5204 -prefMapSize 270279 -ipcHandle 5188 -initialChannelId {aafae294-e702-417a-b4d2-
d4a840777cd4} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -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 5440 -prefsLen 32900 -prefMapHandle
5444 -prefMapSize 270279 -jsInitHandle 5448 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5220 -initialChannelId
{66116cce-0806-4b63-ac69-6db366cde484} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -
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 5436 -prefsLen 32952 -prefMapHandle
5576 -prefMapSize 270279 -jsInitHandle 5580 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5584 -initialChannelId
{95fe24c8-cd6e-4427-8ad7-0a1cd590eca2} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -
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 5768 -prefsLen 32952 -prefMapHandle
5764 -prefMapSize 270279 -jsInitHandle 5760 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5756 -initialChannelId
{a9212fc5-7771-4831-982d-d5424de53993} -parentPid 4524 -crashReporter "\\.\pipe\gecko-crash-server-pipe.4524" -
win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 9 tab
```

4. 5. Network

Country	Destination	Domain	Proto
N/A	127.0.0.1:49861		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
US	8.8.8.8:53	mc.prod.ads.prod.webservices.mozgcp.net	udp
US	151.101.129.91:443	merino.services.mozilla.com	tcp
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	127.0.0.1:49869		tcp

4. 6. Files

C:\Users\Admin\Downloads\lWzSk0hs.dat.part

MD5	b3b2ab44637f48f5247f35a48d7d068e
SHA1	ae08f492f3b4c68d83fef94203f3bf099fc18467
SHA256	c8d763647dbbb092b3c76cfcb98899ea1c5b3f38059c3e707b1943e588c36118
SHA512	f8b37c6cfdcf2dad97f9aaa0cfe1d3002e34595a084af8570e68c1add314a4f18c15ca146e88ace939af2318422331faab29be66697a8564c511092fd74ee3db

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\7338faab-40c6-461a-876a-354aacd989e6

MD5	d456f6dc1fe7e996cb84c45e040d49fe
SHA1	fe0fcc25baa317e426fac1e9d3c8b171f237daa4
SHA256	06c9c121b2a5a3009b3852dfd4e7e25e1eb66870fd2f971480b18ee893dd96a7
SHA512	7a254fad4038934b1d42cae33909e8e12e9e8330670442ff36655574f50a9caaaaf90a5d59ced4dbe2f1f5cd76db2811eef1b2a9d7affa3083aab2d414a0282e

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\edc41103-00cb-4325-96a4-87861f955b3f

MD5	c465687cc82e6e37e5a3618d61cdc867
SHA1	7df0ffb7c07ed7577b135eddd7a429f98c380c39
SHA256	f44d8c61a0b19b753b9d22cd6efe38350e72df5df688987335e70b2e3fbc9844
SHA512	03380097749228fec559f7fb07f1a58e8076074da342bd820b1a85609f48858ecb4ab6c40c0c7347bd2fd85d5ef0cb81c52673d5b77f26e820a27a5b856467de

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\a1d8a76c-fa80-49c5-8663-53e01a9d90f4

MD5	f9c12e42e2bb966fc6868a5e54097a8f
SHA1	0de925a4896dec0ec1495d4ce75d1726bfb65f7a
SHA256	4b5f0a771e424aacc160425c48c36794fc66a6335fbaf7499f5008f4b0ebb460
SHA512	b7ee7c411660529429039d5503c45f696420e51fc6ee253b3011912a8493ac0c48bee3b6abf83d4feb38df350c2c71afb1d8420d11f23f7355e1024360d37da5

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\events\events

MD5	05d5b52a164a1a2df26ae12eef9406ec
SHA1	ea215d8646f120276dabba3ebfb471e2f54ab8ec
SHA256	266d0e487cc87260df0b27c31ff59921b5c893ff033b0c0b937ef59b1ec2c56d
SHA512	fb966a18822bee95e36d9676d06b4328a5db54623c6ff08a67022b73649b1a60a1bf927994f2b174be685cce053b6e122bca0e845bed24339476ed3d0ead0242

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\db\data.safe.tmp

MD5	32ccd6e1fa21a082db67211916564aa5
SHA1	f0ac661698b914f8734dd58512d19fb45d51a2ff
SHA256	e6cac6bc5c771a80ec8cdd0df20af7754eff6bce57647ccf13a43621558c37d7
SHA512	c078fd0176449efa662e8fe185e301d59b16e9a74bd083c8fe8c4697164edba1b400e14480a1eb92bbaa3035e3168b46ec747fd15913f4a4274bbe89296e7d29

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\f144d8fc-cf66-4e62-bf05-e4853ed617bf

MD5	46cb58d4b6626f75e06cad7532fcd0b8
SHA1	32f80a1b7ee62b929e277fad56f58c0ea14ff24d
SHA256	b1731fde873b6bc02feba5513e9b7b20a5efba3479113c65e9e9cea5cce859b1
SHA512	bb0ea7871b15e9e212746ac36f54544cbcf95e93e97fe4cdf7e3a9422a645c707d9de0644aabc17cd6ad86f0788b6c4a2e46c510e06b4085ff011809b086ef2e

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\8dc6a224-05e0-42c6-921a-c34972288dfb

MD5	6909dc82920866c423e71b1a9361538d
SHA1	5f0905eabeefdac307511b84e971dacc47a2cab7
SHA256	53701136d936a8a42983cafdd96443919e05b00685c82279001273e89c18cc1d
SHA512	9ebb02950f8702e9f90d4d0ecfde04b28093254ad27f836d57cd8565f5757083c6d3926dec21292b86f8c00e12dd50384592ffac20914fc6b710cb646745c5f1

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\pending_pings\1fb9778d-d27a-4a64-a810-25d512731c03

MD5	2b9c65942b50b5eb4bde1d2a98c42ff9
SHA1	47ef9ddeb3e43a63ff4dee0dce24a29d092866bd
SHA256	7169c0fc4bd8cbf63037541fb08bb1fc38a4bd5ea5cad012fd2c83afefb8caea
SHA512	3831ec5ced5fe410df74a89cb3a626ec5f9e168020c2a9c0dd1e5a80c39c73fe82d9f08a6718a6f35b7f3bbd9d09c846cd72432b1e8957d5646f4de74a94185c

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\datareporting\glean\db\data.safe.tmp

MD5	2748d7abc841a281f39fe7334f7d3b1a
SHA1	b69c0173fd22fef994b27d386a7a7fff684f71ee
SHA256	52a70b638f6fe490ab36ea62bfe6031ef159ea077fbc876212e7644183af7680
SHA512	09caa29986b31f3285cb7ea97ac34517ee6b7b12209b0b5d5fe1ad2d622c09f5166cd7a30939db2e1e4e41d5bf398024523b43d32c3d169fa810b8a59f94480a

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\3yibrljg.default-release\prefs.js

MD5	7a93dfc350ba5083a1b24e5f14919e11
SHA1	25bd1f6744f8362ef8d468f5b5345017280764f3
SHA256	9e68150260a20237c629da4e63d73b4c18f73ed89e333167b10de8fce2f332ce
SHA512	f20c9853c9bd7875b60da7d7c18e75d8c327be9c83e3906268690b2cfc609d83e94277f16c33da657b8b2f2e16eb8b8f190d0313cecd8164d021e422c4c06dfe

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel
2025-10-11 08:25	2025-10-11 08:26	win11-20250619-en	28s

5. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\SearchHoverUnifiedTileModelCache.dat
```

5. 3. Signatures

Enumerates physical storage devices

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-3625340254-1625357543-1797847221-1000_Classes\Local Settings	C:\Windows\system32\cmd.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-3625340254-1625357543-1797847221-1000_Classes\Local Settings	C:\Windows\system32\OpenWith.exe	N/A

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A

5. 4. Processes

C:\Windows\system32\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\SearchHoverUnifiedTileModelCache.dat
```

C:\Windows\system32\OpenWith.exe

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

5. 5. Network

N/A

5. 6. Files

N/A