Recorded Future®
Sandbox

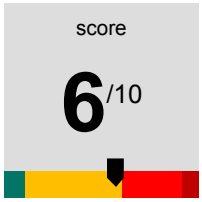
Malware Analysis Report

2025-10-25 17:24

Sample ID	251025-vvtvmssqdt
Target	dafsaData.bin
SHA256	d74d0e429343f5e1b3e0b9437e048917c4343a30cff068739ea898bad8e37ffd
Tags	persistence

Table of Contents

Part 1. Analysis Overview



SHA256
d74d0e429343f5e1b3e0b9437e048917c4343a30cff068739ea898bad8e37ffd

Threat Level: Shows suspicious behavior

The file dafsaData.bin was found to be: Shows suspicious behavior.

Malicious Activity Summary

persistence

- **Drops desktop.ini file(s)**
- **Enumerates physical storage devices**
- **Modifies registry class**
- **Suspicious behavior: AddClipboardFormatListener**
- **Suspicious behavior: GetForegroundWindowSpam**
- **Suspicious use of SetWindowsHookEx**
- **Checks processor information in registry**
- **Suspicious use of AdjustPrivilegeToken**
- **Suspicious use of FindShellTrayWindow**
- **Suspicious use of SendNotifyMessage**
- **Suspicious use of WriteProcessMemory**
- **Uses Task Scheduler COM API**

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
2025-10-25 17:19

3. 2. Signatures

N/A

Part 4. Analysis: behavioral2

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:19	2025-10-25 17:21	win11-20251015-en	149s	103s

4. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\dafsaData.bin
```

4. 3. Signatures

Enumerates physical storage devices

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-1644934582-3155071241-5924616-1000_Classes\Local Settings	C:\Windows\system32\cmd.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1644934582-3155071241-5924616-1000_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

4. 4. Processes

C:\Windows\system32\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\dafsaData.bin
```

C:\Windows\system32\OpenWith.exe

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

4. 5. Network

4. 6. Files

N/A

Part 5. Analysis: behavioral1

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:19	2025-10-25 17:21	win10v2004-20251016-en	148s	148s

5. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\dafsaData.bin
```

5. 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

Enumerates physical storage devices

Checks processor information in registry

Description	Indicator	Process	Target
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\VendorIdentifier	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\VendorIdentifier	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 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\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\ProcessorNameString	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
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 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

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 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\VendorIdentifier	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\~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\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 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\Update Signature	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\.bin	C:\Windows\system32\OpenWith.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\.bin\ = "bin_auto_file"	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\bin_auto_file\shell	C:\Windows\system32\OpenWith.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\bin_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-1-5-21-389786158-2176552546-1679795138-1000_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\cmd.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
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\bin_auto_file	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\bin_auto_file\shell\open	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-389786158-2176552546-1679795138-1000_Classes\bin_auto_file\shell\open\command	C:\Windows\system32\OpenWith.exe	N/A

Suspicious behavior: AddClipboardFormatListener

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A

Suspicious behavior: GetForegroundWindowSpam

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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

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\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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

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\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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

Description	Indicator	Process	Target
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\VideoLAN\VLC\vlc.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 4260 wrote to memory of 3756	N/A	C:\Windows\system32\OpenWith.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 4260 wrote to memory of 3756	N/A	C:\Windows\system32\OpenWith.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3756 wrote to memory of 3552	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Description	Indicator	Process	Target
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 4288	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
PID 3552 wrote to memory of 5376	N/A	C:\Program Files\Mozilla Firefox\firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe

Uses Task Scheduler COM API

persistence

5. 4. Processes

C:\Windows\system32\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\dafsaData.bin
```

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\dafsaData.bin"
```

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

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

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -parentBuildID 20250130195129 -prefsHandle 2008 -prefsLen 27099 -
prefMapHandle 2012 -prefMapSize 270279 -ipcHandle 2100 -initialChannelId {3f24aeaf-1e57-4b92-9152-fc4bcc77bfe7} -parentPid 3552 -
crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 2480 -prefsLen 27135 -
prefMapHandle 2484 -prefMapSize 270279 -ipcHandle 2496 -initialChannelId {31cee4cf-2856-4922-a648-9b18528de6e2} -parentPid 3552 -
crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 3912 -prefsLen 27276 -prefMapHandle 3916 -
prefMapSize 270279 -jsInitHandle 3920 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 3928 -initialChannelId
{77d742ab-5233-4a0e-8dff-7368d4465b80} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 4100 -prefsLen 27276 -
prefMapHandle 4104 -prefMapSize 270279 -ipcHandle 4180 -initialChannelId {ad88eaeb-7f96-4920-aa52-94769978a124} -parentPid 3552 -
crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 2972 -prefsLen 34775 -prefMapHandle 2976 -prefMapSize 270279 -jsInitHandle 2724 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 2720 -initialChannelId {0efe6950-771c-4261-bead-2eab067bf1d6} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 5240 -prefsLen 35012 -prefMapHandle 5248 -prefMapSize 270279 -ipcHandle 5228 -initialChannelId {6376e6d5-62f8-440a-93b4-34bce620ad0b} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 5412 -prefsLen 32900 -prefMapHandle 5424 -prefMapSize 270279 -jsInitHandle 5428 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5440 -initialChannelId {26bf51d6-2148-453b-aea9-1546ce5ee92d} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 5468 -prefsLen 32952 -prefMapHandle 5480 -prefMapSize 270279 -jsInitHandle 5412 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5428 -initialChannelId {8a1dc076-0b56-41cc-bc6b-f9daaad9b38e} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -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 5692 -prefsLen 32952 -prefMapHandle 5644 -prefMapSize 270279 -jsInitHandle 5780 -jsInitLen 253512 -parentBuildID 20250130195129 -ipcHandle 5856 -initialChannelId {19743e60-314f-4428-92d1-cd80fcf4efae} -parentPid 3552 -crashReporter "\\.\pipe\gecko-crash-server-pipe.3552" -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - 9 tab
```

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

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

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

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

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url "C:\Users\Admin\Downloads\dafsaData.bin"
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url C:\Users\Admin\Downloads\dafsaData.bin
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url "C:\Users\Admin\Downloads\dafsaData(1).bin"
```

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

```
"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url C:\Users\Admin\Downloads\dafsaData(1).bin
```

C:\Program Files\VideoLAN\VLC\vlc.exe

```
"C:\Program Files\VideoLAN\VLC\vlc.exe" C:\Users\Admin\Downloads\dafsaData(1).bin
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	g.bing.com	udp
US	150.171.27.10:443	g.bing.com	tcp
US	23.33.40.136:443	www.bing.com	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	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

N/A	127.0.0.1:49848		tcp
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	127.0.0.1:49854		tcp
US	8.8.8.8:53	location.services.mozilla.com	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	8.8.8.8:53	ciscobinary.openh264.org	udp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
US	151.101.67.19:443	mozilla-download.fastly-edge.com	tcp
US	34.104.35.123:443	edgedl.me.gvt1.com	tcp
US	52.85.193.51:443	ciscobinary.openh264.org	tcp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp
US	8.8.8.8:53	mozilla-download.fastly-edge.com	udp
US	8.8.8.8:53	d156sk07toobyl.cloudfront.net	udp
US	8.8.8.8:53	c.pki.goog	udp
US	142.250.80.67:80	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	content-signature-chains.prod.autograph.services.mozaws.net	udp
US	8.8.8.8:53	firefox-settings-attachments.cdn.mozilla.net	udp
US	8.8.8.8:53	mozilla.map.fastly.net	udp

5. 6. Files

C:\Users\Admin\Downloads\9BlpMJeM.bin.part

MD5	64f469698e53d0c828b7f90acd306082
SHA1	bcc041b3849e1b0b4104ffeb46002207eeac54f3
SHA256	d74d0e429343f5e1b3e0b9437e048917c4343a30cff068739ea898bad8e37ffd
SHA512	a8334d1304f2fbd32cfd0ca35c289a45c450746cf3be57170cbbe87b723b1910c2e950a73c1fb82de9dc5ed623166d339a05fec3d78b861a9254dc2cb51fab5f

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\8a205292-d3d4-48ed-87aa-db250e59d5a1

MD5	606a032f261bb8fff679fcf0e26eb893
SHA1	523b60a204bd195bb62e6d3d3c07db5019b63454
SHA256	b0eda593cc947341dd74dc87b8555693596b63ccf3f12bc85fa261af06b1c265
SHA512	1273e52ac986f07e8bc78a5f767df004860d8236c96068119f13e3639b6c79142d3033832a49aebb77c0cab82fdfb51fed1d12d4f54247c0e0c46e4dd04b10e1

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\25643295-fab9-433d-8a3b-062df2ac6c23

MD5	29ee1939f6597c8eef2a9a69b1834e8b
SHA1	b01d1c0dfce02ee1259c67c9d4e142ff62b00798
SHA256	0f1977b87d85213a5a9a41fc7ff2499cc336871b12b61c3784a8096418d605c1
SHA512	03be47244ea61ff12cb7c9e278a0bb1246e80c2865a1100f82e886e4590cf2a34007cf23c3b4b14930a214cc553470e955b94c42bd0422e5bf653dc1c8682a66

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\fc92b58e-8136-4711-8f0f-fc89154774e6

MD5	286ffb2aee7fbea9f4ece5d9787cb2a8
SHA1	fcb3a01ebfed430bdea65a700273bed48bab1451
SHA256	3278f75d935fc0c21bf5907c2c4df5c5fc45afe11e83ddf5136acfe7553d65c8
SHA512	b1c30f4642e41c7f44c89d058ecdb3175b5223fd1875faaa503a1c1f65482848274f414539e4740c1bb50212dd5237103eb5b0f9daa49119462aa207df9a4d66

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

MD5	759c545180efbb4a703c40a6f613b5ee
SHA1	e25dcf1860e03cd9e45c2a89879d0638c29fdf10
SHA256	9265a2add306497730de737010384ff76f261aae5b9a04f121e7e6e0feeca4aa
SHA512	651010deaef4281b8d8dbd5d86b9c4b8abc5f214d216f74abd9f520a8bfa73dc647456c93cecc8fda8fd1c736862e6af7bca4e324f4e971d6fb3c65fc11ff947

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

MD5	e4266acfeadf64afda0e131e2203f8ac
SHA1	aaf880cc5029256a93be08f2517f32956a7ef4eb
SHA256	35410b381d2ab58b927aa776baa1ba246597715139884a420fc64d93d1ad1d29
SHA512	ca32ff20775ee35099a52b762451ca11f9370de8f2534df7e4b7f55c49073d588beaa77b1c260b0c1d0d288e3667a3f93efa2fc96ac3df3609eb758d724c0d1a

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\7faefcb4-b871-44a8-be54-5773d22ddb67

MD5	a65ed18b3b2a50e6dadee4a4460a621f
SHA1	279ef4c629eab75a35507d7a64a22cb178235c6c
SHA256	13c378625bbaccb92ad4a0ed99989c7582e0ef5731cba5c5671da244c959315c
SHA512	3233dd87fb9e912ec85fe54c11a6e2b9c92137d8bf1ef877cf2f316caff4e1dfd97af886e77069e0986d3f8a97f9a330cc6a44be07fc2104f0ea18f3fa544fca

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

MD5	7f94398009e1d173ddc7838173a97129
SHA1	0f91b5e5304256e510dc9650707f1246022cf652
SHA256	dfc29d02e3573eb4c8659a20c635b46144ecfd4e059167c69466efbb8de47443
SHA512	41f3cf4dd6514d210fd4fb713f354dd40d8fc1be9abf2e9da9c89ebc1cff40c8c08fb37dcfe955f413c394af0fdc3eb94b098729d97299339ee724dbfa51debb

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\efbaf3f0-1ca3-4d72-92b3-e39c215c3eeb

MD5	31e19a4bcea824e31d98140eb33b1c14
SHA1	7bfa91953efa9f8e29fa844499cc4056bbbc3ad0
SHA256	5541cfba153cf9e9653f48d21fa59d2e9a66dfa0bfb45bec17b680d901574aa7
SHA512	32f742642779ced26e641745fa6f5964cccd246e78f112b882cf8527b1ebfc24146cded43cfa6ceed0b279b7b115d533c829cee0fb5cf1ea57cfce493d177fa9

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\datareporting\glean\pending_pings\97b8946c-c10d-4adb-8472-324e8b1af758

MD5	d3343cf318b0a8b0333626fdd3702859
SHA1	f0ed10735d49cb867094d37c762a4c9213f94719
SHA256	b5fd4e8e1009add4b570e0182c79a670a5dfebef43520cbbd610b26ff2c242ec
SHA512	64cbc9a209014fc711a391c86e71d4353beeb7088bc6284b1dab732f808e46e4c339064179f8a914dcfaeb147879c4f3e15c5806a5a4e121af2448e62e753aaf

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

MD5	9a7c6d3d1b19318b726b4f4a69917256
SHA1	2ac72e13b6aa562cbd4b420cfb5edadde092944b
SHA256	d35ea90a085dccfcff285aefd209797dc8f1eb4ccaa8c6584774e480cef88145
SHA512	71171871d249a6a8b7f8de6ef8bc09fcda8e70aff3eff6ee6b713c1636e802d5356a9f6f97729c43ba309b2a1adfd175c3a2928f64d55fbf1cd4f5667f27f9d3

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

MD5	a7a264b04ec203bec367eeb7d2a43a47
SHA1	6073ad368d3dcb3c63e824b7cad296db4fa1fb82
SHA256	09623a5e0b79ffb6fe36f5f16455ad139d4612016552a7c1d8c3b9de218d853a
SHA512	e16660658bf67a2a52969b8be13e324afeaa14b683a2b69a99bf39ae6b6546bb07bc3225b4ed49044915aee682bd8240a4db1ecfa6fb081dfe8701624d7d7172

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

MD5	0e5928e06186aa988ee2d9a07b21b4c3
SHA1	5ef7836aefa4fe423e027703e268ac3b1219142f
SHA256	79d568d5cd6b684f8396e9084c7b9fe8989c527485359b481136d878e430ada0
SHA512	3132417f2d3bdba45fea1edd977aa2edec1e0212d0bade1df0240663da91ec84ba04f787a3776954cc948bb99a08d079142254d6b2f28bc98891fa74f50ee66e

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

MD5	25e8156b7f7ca8dad999ee2b93a32b71
SHA1	db587e9e9559b433cee57435cb97a83963659430
SHA256	ddf3ba4e25a622276755133e0cce5605b83719c7cab3546e09acbfed00d6a986
SHA512	1211b2fa997ba13ff926aec58b6b35a81d7fe108b0caa8f4d6369d0a37f8481373b78a4b201651243adde9e2b2699ce929482a46226ff6299b0a0e40fe2ddc56

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

MD5	bb0cf67181e4cfad95f37c76e4681194
SHA1	2e6ca7276bc148a09201f565cf76cf271fc99235
SHA256	d2ef7c709030d727ebfdae1c49cda84188b294eb1d27335d3f247c17b1d4ae0b
SHA512	06b7f2050ba5317bbc43b7ceb275d2b064d3a596f32927a3c463600980cdd96ff6ed280306879347baf37a9181d7bc0e10fc5909228c58366b62c0fbf0a4e54d

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

MD5	ac7a7db6e98723b2c6c45e1c054b9784
SHA1	7e4cf86931b03f04aa0734b64cdab5036d60e94f
SHA256	3a52bbf20307785888e23895028073bfeac6058bd08689a47136520ff23837fc
SHA512	cf8d129bbdc6d0f95a22964f23b5667518794f265aa3515abbb316460b04df1f745b68922e3167953fdc8286e9dc62810579c6f7260c0a24ec8db44d66b203ad

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

MD5	6e018e9d3880b690745ae85da1e62405
SHA1	d0b0c4472024e92c0a6f314a37f9845b63b54247
SHA256	08f2f0a58ca7701d46634eaff0c021511a0f249e4e3ba292f3d435834cf0bc1c
SHA512	97ddedfb0dbc69ffe82815de7197e6acf76301c7b317526e784a2c281e52c51983a8a24744e5bb9d6d511a91f33f167b6c642f7c5150758869564f154daf4caa

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\datareporting\glean\db\data.safe.tmp

MD5	b2f0f9a0e32a8a7f107b26ddff596df2
SHA1	c794dbe8743c6ed5dc7260bd677381959e530d20
SHA256	d6301fc9c45802d6313e7e12a8aad3767edaab1b5012c3d915aeff32420fcc6a
SHA512	ea18d5480fdfd2570f51bf6f27c36333b719ac216537d361f9eea3e53c974b24f7fd7d473417a475c8bd1196f7bdd592ac51a13b7f51c6b99ce388179af7190d

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	2471ae911026ca92d73d129d00cf3ff6
SHA1	29c543aa0f221a3b7d147cc68f46eecfcdc91f31
SHA256	9d04e5a385ae27c9043a85c5056ea0971630cb506124bc53c52c5bc2f56078f2
SHA512	88cde1aef6cb5c5b88bea3554e7ca6d8daff24e8efbc5b543f497461e63b3dcdefbac11f415788efc76195c394f0c7dfe7280fda0a22f7e2d2e800e5a079eaa5

memory/5204-701-0x00007FF630290000-0x00007FF630388000-memory.dmp

memory/5204-702-0x00007FF9D1C80000-0x00007FF9D1CB4000-memory.dmp

memory/5204-708-0x00007FF9D1C00000-0x00007FF9D1C1D000-memory.dmp

memory/5204-707-0x00007FF9D1C20000-0x00007FF9D1C37000-memory.dmp

memory/5204-709-0x00007FF9D1BE0000-0x00007FF9D1BF1000-memory.dmp

memory/5204-714-0x00007FF9D1B20000-0x00007FF9D1B31000-memory.dmp

memory/5204-713-0x00007FF9D1B40000-0x00007FF9D1B58000-memory.dmp

memory/5204-712-0x00007FF9D1B60000-0x00007FF9D1B81000-memory.dmp

memory/5204-711-0x00007FF9D1B90000-0x00007FF9D1BD1000-memory.dmp

memory/5204-710-0x00007FF9D1580000-0x00007FF9D178B000-memory.dmp

memory/5204-703-0x00007FF9D1790000-0x00007FF9D1A46000-memory.dmp

memory/5204-706-0x00007FF9D1C40000-0x00007FF9D1C51000-memory.dmp

memory/5204-705-0x00007FF9D1C60000-0x00007FF9D1C77000-memory.dmp

memory/5204-704-0x00007FF9EB500000-0x00007FF9EB518000-memory.dmp

memory/5204-723-0x00007FF630290000-0x00007FF630388000-memory.dmp

memory/5204-725-0x00007FF9D1790000-0x00007FF9D1A46000-memory.dmp

memory/5204-724-0x00007FF9D1C80000-0x00007FF9D1CB4000-memory.dmp

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

MD5	d6c0b20edb9f867f8fb4d54ed01e3040
SHA1	945cd8de70635aeadef6e748d9e2e6b071a1ec9b
SHA256	e2fd8297033d1691309b2e6290cf8a23815cf05144bd79f65f13d025fadf18d0
SHA512	1bd2d910887617d9b84758e0b831049b073319967170ef084035cc5b8107ff8d5c83cf92a9ec92c1b73c5e664aceb277b3b6324f08374fb8aab137a52e1ad687

C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\1akhe1kg.default-release\sessionstore-backups\recovery.jsonlz4

MD5	0531dbb73e1805fde184e80f091a95b8
SHA1	62f2dc3a6eebae0f3b8f94b17a416bb728f1b50f
SHA256	c00522c3664db45a38d52424a9769c6b9ef3155c2a4a6bd326be3b40a7c32e19
SHA512	d089f945b371051b99ee7d2ce1b2a7691c7615bb520d841752f7151f6787ae68bc3653be635de64d5cc7070c76674437f53d2ccd3f84ae6b4bd063e1ff8711d2

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

MD5	4de765fd7b4d782dadfe1f3eb7866653
SHA1	0462ca99a7635a14cf0bd4e15a5cf241ed888e78
SHA256	c6f7e1df78b079ccc9e81ad2bdb3f406910efd2cced3b929934147bc80ae6211
SHA512	3dd322ce9c2ff40cc8604f8fb4fb17e7177bb2b0a241364bdd19e14817f4f28492aeddc5de094d0813a26ae87964cc7564bfda6aa0acc2d068951b06abc50e8e

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

MD5	dca601b9e8686ec2d70805432b230da3
SHA1	248c623893370f61586940fbb4094d822de1999f
SHA256	d2a39d07f9d4f93c97a49a407ad9ad7c1bd54bc815fc4952f6995c897b2d4b28
SHA512	51115cd027fef6d5f8fc4456e40ffb9b097d733060e5454b3afc3e4a0a915b8c6461e9c9fab0fb1d5bfc8c67cc56ebcd75e82b66f797f030cabba281858058cb

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

MD5	f6d9733cb72c8cd3f4abe17c6bda7a70
SHA1	ca97b157159778de96be15c6b0f948bd6738f7f6
SHA256	8ea41495fed1751b85ccd4d70ead904748d2a02f7b35f85633eff4c78278d843
SHA512	a6c51d95af22e078ba10d14cbb325069adcd66487b8b147389de331b37ec07fe48d1a3fca55c0a9bca9802be0301d698a222eab9f25324e7a7eba057d151df0c