



## Informazioni generali

|                    |   |
|--------------------|---|
| URL:               | https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe  |
| Analisi completa:  | <a href="https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281">https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281</a> |
| Verdetto:          | Attività dannosa  |
| Data di analisi:   | 25 agosto 2024 alle 22:38:59  |
| Sistema operativo: | Windows 10 Professional (build: 19045, 64 bit)  |
| Tag:               | github netreattore  |
| Indicatori:        |   |
| MD5:               | 00B5E91B42712471CDFBDB37B715670C  |
| SHA1:              | D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2  |
| SHA256:            | 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0  |
| SSDEEP:            | 3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa   |

### Set di ambienti software e opzioni di analisi

## Configurazione di avvio

|                              |             |                           |        |                               |                        |
|------------------------------|-------------|---------------------------|--------|-------------------------------|------------------------|
| Durata dell'attività:        | 300 secondi | Opzione Evasione Pesante: |        | Geolocalizzazione della rete: | spento                 |
| Tempo aggiuntivo utilizzato: | 240 secondi | Proxy MITM:               | spento | Riservatezza:                 | Presentazione pubblica |
| Opzione Fakenet:             | spento      | Percorso via Tor:         | spento | Autoconferma dell'UAC:        | SU                     |
| Rete:                        | SU          |                           |        |                               |                        |

### Preimpostazione software

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office professionale 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - it-it (16.0.16026.20146)
- Strumenti di integrità di Microsoft Update (3.74.0.0)
- Microsoft Visual C++ 2013 ridistribuibile (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Runtime aggiuntivo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Runtime minimo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 runtime minimo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 runtime minimo - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Servizio di manutenzione Mozilla (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

### Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

## Attività comportamentali

| MALIZIOSO                  | SOSPETTOSO   | INFORMAZIONI  |
|----------------------------|--|---|
| Nessun indicatore dannoso. | <div>Il processo elimina l'eseguibile legittimo di Windows<ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul></div> <div>Utilizza TIMEOUT.EXE per ritardare l'esecuzione<ul style="list-style-type: none"><li>• cmd.exe (PID: 7520)</li><li>• cmd.exe (PID: 7876)</li></ul></div> <div>Avvia CMD.EXE per l'esecuzione dei comandi<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Controlla le impostazioni di attendibilità di Windows<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Legge le impostazioni di sicurezza di Internet Explorer<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Esegue l'applicazione che si blocca<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Si collega a una porta insolita<ul style="list-style-type: none"><li>• InstallUtil.exe (PID: 5152)</li></ul></div> <div>L'applicazione si è avviata da sola<ul style="list-style-type: none"><li>• Muadnrd.exe (PID: 7824)</li></ul></div> | <div>L'applicazione si è avviata da sola<ul style="list-style-type: none"><li>• firefox.exe (PID: 6552)</li><li>• firefox.exe (PID: 6596)</li></ul></div> <div>Legge le chiavi del registro di Microsoft Office<ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul></div> <div>Il contenuto eseguibile è stato eliminato o sovrascritto<ul style="list-style-type: none"><li>• firefox.exe (PID: 6596)</li></ul></div> <div>Legge il nome del computer<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul></div> <div>Legge il GUID della macchina dal registro<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul></div> <div>Legge i valori dell'ambiente<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Controlla le lingue supportate<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• Muadnrd.exe (PID: 7248)</li></ul></div> <div>Disabilita i log di traccia<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• Muadnrd.exe (PID: 7824)</li></ul></div> <div>Controlla le informazioni del server proxy<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• WerFault.exe (PID: 1356)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• WerFault.exe (PID: 7584)</li></ul></div> <div>Legge le impostazioni dei criteri software<ul style="list-style-type: none"><li>• Jvczfhe.exe (PID: 7492)</li><li>• WerFault.exe (PID: 1356)</li><li>• Muadnrd.exe (PID: 7824)</li><li>• WerFault.exe (PID: 7584)</li></ul></div> <div>Crea file o cartelle nella directory utente<ul style="list-style-type: none"><li>• WerFault.exe (PID: 1356)</li><li>• WerFault.exe (PID: 7584)</li></ul></div> <div>È stato rilevato il protettore del reattore .NET<ul style="list-style-type: none"><li>• InstallUtil.exe (PID: 5152)</li><li>• Muadnrd.exe (PID: 7248)</li></ul></div> |

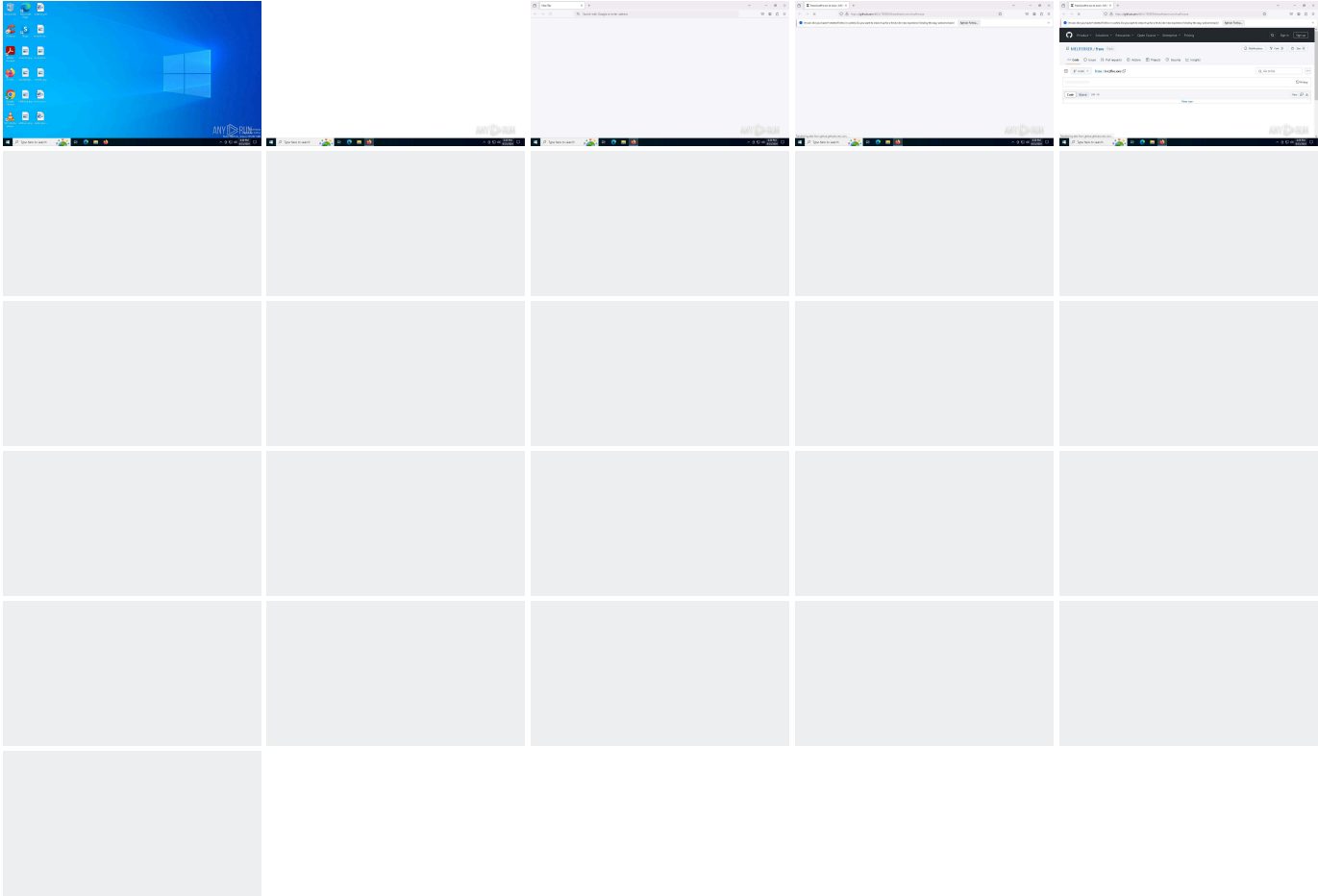
## Configurazione del malware

Nessuna configurazione malware.

## Informazioni statiche

Nessun dato.

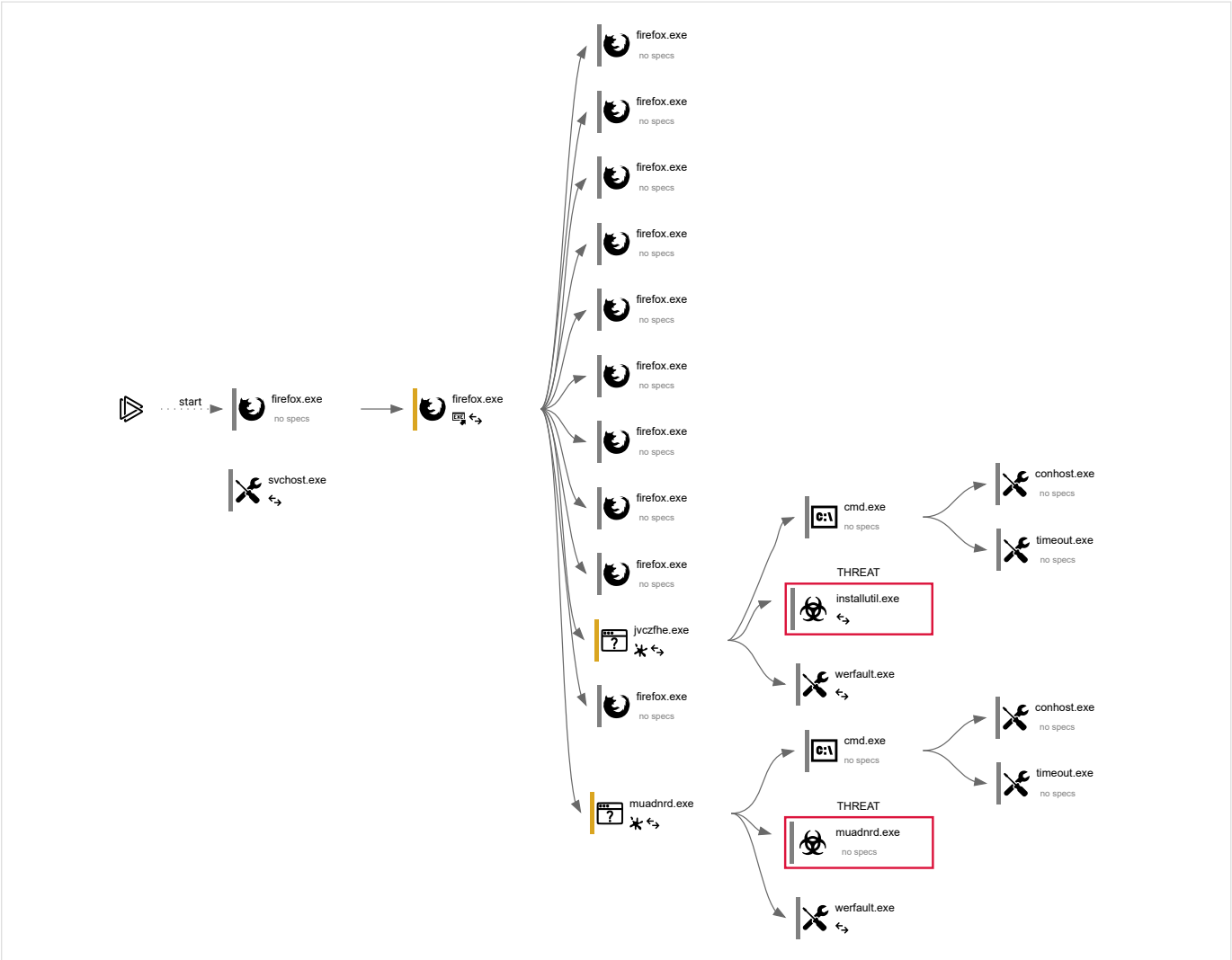
## Video e screenshot



Processi

|                 |                     |                  |                   |
|-----------------|---------------------|------------------|-------------------|
| Processi totali | Processi monitorati | Processi dannosi | Processi sospetti |
| 155             | 25                  | 0                | 3                 |

Grafico del comportamento



| Descrizione delle specifiche           |  |  |  |
|--|--|--|--|
| Program did not start                  | Low-level access to the HDD                  | Process was added to the startup                 | Debug information is available         |
| Probably Tor was used                  | Behavior similar to spam                     | Task has injected processes                      | Executable file was dropped            |
| Known threat                           | RAM overrun                                  | Network attacks were detected                    | Integrity level elevation              |
| Connects to the network                | CPU overrun                                  | Process starts the services                      | System was rebooted                    |
| Task contains several apps running     | Application downloaded the executable file   | Actions similar to stealing personal data        | Task has apps ended with an error      |
| File is detected by antivirus software | Inspected object has suspicious PE structure | Behavior similar to exploiting the vulnerability | Task contains an error or was rebooted |
| The process has the malware config     |  |  |  |

Informazioni sul processo

| PID                   | Comando   | Sentiero                         | Indicatori                             | Processo padre |
|-----------------------|---|----------------------------------|--|----------------|
| 1356                  | C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676 | C:\Windows\SysWOW64\WerFault.exe |  | Jvczfhe.exe    |
| Informazioni          |   |                                  |  |                |
| Utente:               | amministratore                                      | Azienda:                         | Microsoft Corporation                  |                |
| Livello di integrità: | MEDIO   | Descrizione:                     | Segnalazione problemi di Windows       |                |
| Codice di uscita:     | 0   | Versione:                        | 10.0.19041.3996 (WinBuild.160101.0800) |                |

|                       |  |                                 |                                     |             |
|-----------------------|--|---------------------------------|-------------------------------------|-------------|
| 2256                  | C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache | C:\Windows\System32\svchost.exe |                                     | servizi.exe |
| Informazioni          |  |                                 |                                     |             |
| Utente:               | SERVIZIO DI RETE   | Azienda:                        | Microsoft Corporation               |             |
| Livello di integrità: | SISTEMA  | Descrizione:                    | Processo host per i servizi Windows |             |
| Versione:             | 10.0.19041.1 (WinBuild.160101.0800)                              |                                 |                                     |             |

|                       |   |   |  |             |
|-----------------------|---|---|--|-------------|
| 5152                  | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" | C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe |  | Jvczfhe.exe |
| Informazioni          |   |   |  |             |
| Utente:               | amministratore  | Azienda:  | Microsoft Corporation                      |             |
| Livello di integrità: | MEDIO   | Descrizione:  | Utilità di installazione di .NET Framework |             |
| Versione:             | 4.8.9037.0 creato da: NET481REL1                                |   |  |             |

|                       |   |  |                     |             |
|-----------------------|---|--|---------------------|-------------|
| 6340                  | "C:\Programmi\Mozilla Firefox\firefox.exe" -contentproc --channel=5380 -childID 4 -isForBrowser -prefsHandle 5516 -prefMapHandle 5508 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Programmi\Mozilla Firefox\browser" - {fac3d9db-bdd5-4087-af19-991bcb39f3fc} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55d90 tab | C:\Programmi\Mozilla Firefox\firefox.exe | —                   | firefox.exe |
| Informazioni          |   |  |                     |             |
| Utente:               | amministratore  | Azienda:                                 | Mozilla Corporation |             |
| Livello di integrità: | BASSO   | Descrizione:                             | Firefox             |             |
| Versione:             | 123.0   |  |                     |             |


|                       |   |  |                     |             |
|-----------------------|---|--|---------------------|-------------|
| 6360                  | "C:\Programmi\Mozilla Firefox\firefox.exe" -contentproc --channel=5512 -childID 5 -isForBrowser -prefsHandle 5668 -prefMapHandle 5672 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Programmi\Mozilla Firefox\browser" - {87081c36-df2a-495c-8aa3-1f1d82c27099} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4bf3d90 tab | C:\Programmi\Mozilla Firefox\firefox.exe | —                   | firefox.exe |
| Informazioni          |   |  |                     |             |
| Utente:               | amministratore  | Azienda:                                 | Mozilla Corporation |             |
| Livello di integrità: | BASSO   | Descrizione:                             | Firefox             |             |
| Versione:             | 123.0   |  |                     |             |

|                       |   |  |                     |             |
|-----------------------|---|--|---------------------|-------------|
| 6368                  | "C:\Programmi\Mozilla Firefox\firefox.exe" -contentproc --channel=4976 -parentBuildID 20240213221259 -sandboxingKind 0 -prefsHandle 4800 -prefMapHandle 4804 -prefsLen 36339 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Programmi\Mozilla Firefox\browser" - {9f234b1e-a7f5-459b-a776-445e6f7f5cf6} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c46eeb10 utilità | C:\Programmi\Mozilla Firefox\firefox.exe | —                   | firefox.exe |
| Informazioni          |   |  |                     |             |
| Utente:               | amministratore  | Azienda:                                 | Mozilla Corporation |             |
| Livello di integrità: | BASSO   | Descrizione:                             | Firefox             |             |
| Versione:             | 123.0   |  |                     |             |

|                  |   |  |                     |             |
|------------------|---|--|---------------------|-------------|
| 6384             | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5228 -childID 3 -isForBrowser -prefsHandle 5224 -prefMapHandle 5220 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {341d20e2-0ffc-4ced-87ee-4738a3c45fef} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55690 tab | C:\Program Files\Mozilla Firefox\firefox.exe | —                   | firefox.exe |
| Information      |   |  |                     |             |
| User:            | admin   | Company:                                     | Mozilla Corporation |             |
| Integrity Level: | LOW   | Description:                                 | Firefox             |             |
| Version:         | 123.0   |  |                     |             |

|                  |   |  |                     |             |
|------------------|---|--|---------------------|-------------|
| 6456             | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5916 -childID 6 -isForBrowser -prefsHandle 5908 -prefMapHandle 4672 -prefsLen 34713 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {18cad704-8b2b-4301-9d29-a6d45994eac7} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b65310 tab | C:\Program Files\Mozilla Firefox\firefox.exe | —                   | firefox.exe |
| Information      |   |  |                     |             |
| User:            | admin   | Company:                                     | Mozilla Corporation |             |
| Integrity Level: | LOW   | Description:                                 | Firefox             |             |
| Version:         | 123.0   |  |                     |             |

|             |   |  |   |              |
|-------------|---|--|---|--------------|
| 6552        | "C:\Program Files\Mozilla Firefox\firefox.exe" "https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe" | C:\Program Files\Mozilla Firefox\firefox.exe | — | explorer.exe |
| Information |   |  |   |              |

|      |  |  |
|------|--|--|
|      | <div>User:adminCompany:Mozilla CorporationIntegrity Level:MEDIUMDescription:FirefoxExit code:0Version:123.0</div>  |  |
| 6596 | <div>"C:\Program Files\Mozilla Firefox\firefox.exe"<br/><a href="https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe">https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe</a></div> <div>C:\Program Files\Mozilla Firefox\firefox.exe</div> <div></div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Mozilla CorporationIntegrity Level:MEDIUMDescription:FirefoxVersion:123.0</div></div>   |  |
| 6680 | <div>"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4480 -childID 2 -isForBrowser -prefsHandle 4472 -prefMapHandle 4412 -prefsLen 36263 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {a5653cc5-bef6-4bd7-a916-64d6d56bffd5} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c161e850 tab</div> <div>C:\Program Files\Mozilla Firefox\firefox.exe</div> <div>—</div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Mozilla CorporationIntegrity Level:LOWDescription:FirefoxVersion:123.0</div></div> |  |
| 6744 | <div>"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=1824 -parentBuildID 20240213221259 -prefsHandle 1752 -prefMapHandle 1732 -prefsLen 30537 -prefMapSize 244343 -appDir "C:\Program Files\Mozilla Firefox\browser" - {cb10680d-0044-4e6b-8433-6e05fa363c18} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256ba9c2b10 gpu</div> <div>C:\Program Files\Mozilla Firefox\firefox.exe</div> <div>—</div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Mozilla CorporationIntegrity Level:LOWDescription:FirefoxVersion:123.0</div></div>   |  |
| 6816 | <div>"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=2208 -parentBuildID 20240213221259 -prefsHandle 2192 -prefMapHandle 2188 -prefsLen 30537 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {9a337de7-7563-44b0-ad05-1393e51c0827} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256aec7f510 socket</div> <div>C:\Program Files\Mozilla Firefox\firefox.exe</div> <div>—</div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Mozilla CorporationIntegrity Level:LOWDescription:FirefoxVersion:123.0</div></div>  |  |
| 7048 | <div>"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=3028 -childID 1 -isForBrowser -prefsHandle 2880 -prefMapHandle 3020 -prefsLen 26706 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {72307e83-1a5f-44ea-b997-a72e8f677a2c} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0670bd0 tab</div> <div>C:\Program Files\Mozilla Firefox\firefox.exe</div> <div>—</div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Mozilla CorporationIntegrity Level:LOWDescription:FirefoxVersion:123.0</div></div> |  |
| 7248 | <div>"C:\Users\admin\Downloads\Muadnrd.exe"</div> <div>C:\Users\admin\Downloads\Muadnrd.exe</div> <div></div> <div>Muadnrd.exe</div> <div>Information<div>User:adminCompany:Microsoft CorporationIntegrity Level:MEDIUMDescription:Microsoft EdgeExit code:0Version:126.0.2592.113</div></div>  |  |
| 7492 | <div>"C:\Users\admin\Downloads\Jvczfhe.exe"</div> <div>C:\Users\admin\Downloads\Jvczfhe.exe</div> <div></div> <div>firefox.exe</div> <div>Information<div>User:adminCompany:Microsoft CorporationIntegrity Level:MEDIUMDescription:Microsoft EdgeExit code:3762504530Version:126.0.2592.113</div></div>   |  |
| 7520 | <div>"cmd" /c timeout 21 &amp; exit</div> <div>C:\Windows\SysWOW64\cmd.exe</div> <div>—</div> <div>Jvczfhe.exe</div> <div>Information</div>  |  |

|  |  |  |   |         |
|--|--|--|---|---------|
| 7528   | User: admin<br>Integrity Level: MEDIUM | Company: Microsoft Corporation<br>Description: Windows Command Processor | — | cmd.exe |
| Information  |  |  |   |         |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0   |  |  |   |         |
| Company: Microsoft Corporation<br>Description: Console Window Host<br>Version: 10.0.19041.1 (WinBuild.160101.0800) |  |  |   |         |

|  |            |                                 |   |         |
|--|------------|---------------------------------|---|---------|
| 7572   | timeout 21 | C:\Windows\SysWOW64\timeout.exe | — | cmd.exe |
| Information  |            |                                 |   |         |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0   |            |                                 |   |         |
| Company: Microsoft Corporation<br>Description: timeout - pauses command processing<br>Version: 10.0.19041.1 (WinBuild.160101.0800) |            |                                 |   |         |

|   |   |                                  |   |             |
|---|---|----------------------------------|---|-------------|
| 7584  | C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7824 -s 2888 | C:\Windows\SysWOW64\WerFault.exe | ↔ | Muadnrd.exe |
| Information   |   |                                  |   |             |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0  |   |                                  |   |             |
| Company: Microsoft Corporation<br>Description: Windows Problem Reporting<br>Version: 10.0.19041.3996 (WinBuild.160101.0800) |   |                                  |   |             |

|   |   |  |   |             |
|---|---|--|---|-------------|
| 7756  | "C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=7340 -childID 7 -isForBrowser -prefsHandle 6280 -prefMapHandle 6436 -prefsLen 32132 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {6f311190-77cd-4ee9-97c4-08357a8cf697} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0a96150 tab | C:\Program Files\Mozilla Firefox\firefox.exe | — | firefox.exe |
| Information   |   |  |   |             |
| User: admin<br>Integrity Level: LOW<br>Version: 123.0 |   |  |   |             |
| Company: Mozilla Corporation<br>Description: Firefox  |   |  |   |             |

|  |  |                                      |     |             |
|--|--|--------------------------------------|-----|-------------|
| 7824   | "C:\Users\admin\Downloads\Muadnrd.exe" | C:\Users\admin\Downloads\Muadnrd.exe | ✱ ↔ | firefox.exe |
| Information  |  |                                      |     |             |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 3762504530                          |  |                                      |     |             |
| Company: Microsoft Corporation<br>Description: Microsoft Edge<br>Version: 126.0.2592.113 |  |                                      |     |             |

|  |  |                                 |   |         |
|--|--|---------------------------------|---|---------|
| 7860   | ??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1 | C:\Windows\System32\conhost.exe | — | cmd.exe |
| Information  |  |                                 |   |         |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0   |  |                                 |   |         |
| Company: Microsoft Corporation<br>Description: Console Window Host<br>Version: 10.0.19041.1 (WinBuild.160101.0800) |  |                                 |   |         |

|   |                            |                             |   |             |
|---|----------------------------|-----------------------------|---|-------------|
| 7876  | "cmd" /c timeout 21 & exit | C:\Windows\SysWOW64\cmd.exe | — | Muadnrd.exe |
| Information   |                            |                             |   |             |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0  |                            |                             |   |             |
| Company: Microsoft Corporation<br>Description: Windows Command Processor<br>Version: 10.0.19041.3636 (WinBuild.160101.0800) |                            |                             |   |             |

|  |            |                                 |   |         |
|--|------------|---------------------------------|---|---------|
| 7968   | timeout 21 | C:\Windows\SysWOW64\timeout.exe | — | cmd.exe |
| Information  |            |                                 |   |         |
| User: admin<br>Integrity Level: MEDIUM<br>Exit code: 0   |            |                                 |   |         |
| Company: Microsoft Corporation<br>Description: timeout - pauses command processing<br>Version: 10.0.19041.1 (WinBuild.160101.0800) |            |                                 |   |         |

## Registry activity

|              |             |              |               |
|--------------|-------------|--------------|---------------|
| Total events | Read events | Write events | Delete events |
| 35 308       | 35 167      | 140          | 1             |

### Modification events

|                                   |   |
|-----------------------------------|---|
| (PID) Process: (6552) firefox.exe | Key: HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher    |
| Operation: write                  | Name: C:\Program Files\Mozilla Firefox\firefox.exe\Launcher |
| Value: 84B995F900000000           |   |

|  |   |
|--|---|
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 63DA97F900000000                | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Browser                              |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Progress             |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Progress             |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> delete value<br><b>Value:</b>                          | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Installer\308046B0AF4A39CB<br><b>Name:</b> installer.taskbarpin.win10.enabled                              |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Telemetry                            |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\DIIIPrefetchExperiment<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe                        |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Theme                |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Enabled              |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent<br><b>Name:</b> C:\Program Files\Mozilla Firefox\DisableTelemetry                    |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent<br><b>Name:</b> C:\Program Files\Mozilla Firefox\DisableDefaultBrowserAgent          |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent<br><b>Name:</b> C:\Program Files\Mozilla Firefox\SetDefaultBrowserUserChoice         |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> E84455D32EF7DA01                | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent<br><b>Name:</b> C:\Program Files\Mozilla Firefox\AppLastRunTime                      |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 4                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\ScreenX              |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 4                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\ScreenY              |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1168                            | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Width                |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 651                             | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Height               |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Maximized            |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 2                               | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\Flags                |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 00000000000F03F                 | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\CssToDevPixelScaling |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 000000E0EE966A40000001C221D9040 | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\UrlbarCSSSpan        |



|   |   |
|---|---|
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 00000000000000000000000000000000   | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\SearchbarCSSSpan |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0000000000805C40000000E0EEF6694000000202231904000000FCFFA79140   | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\SpringsCSSSpan   |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap<br><b>Name:</b> ProxyBypass                                 |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap<br><b>Name:</b> IntranetName                                |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 1  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap<br><b>Name:</b> UNCAsIntranet                               |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap<br><b>Name:</b> AutoDetect                                  |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 6024B221EA3A6910A2DC08002B30309D0A01000BD0E0C47735D584D9CEDE91E22E2328277010000011402000000000C00000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000 | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer<br><b>Name:</b> SlowContextMenuEntries                                       |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0000002011A96A4000000C8BB158F40  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\UrlbarCSSSpan    |
| <b>(PID) Process:</b> (6596) firefox.exe<br><b>Operation:</b> write<br><b>Value:</b> 0000000000805C40000002011096A4000000C0BB3D8F40000000400189140  | <b>Key:</b> HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings<br><b>Name:</b> C:\Program Files\Mozilla Firefox\firefox.exe\SpringsCSSSpan   |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing<br><b>Name:</b> EnableConsoleTracing  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> EnableFileTracing                                      |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> EnableAutoFileTracing                                  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> EnableConsoleTracing                                   |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b>  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> FileTracingMask  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b>  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> ConsoleTracingMask                                     |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 1048576  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> MaxFileSize  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> %windir%\tracing   | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32<br><b>Name:</b> FileDirectory  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS<br><b>Name:</b> EnableFileTracing                                      |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write<br><b>Value:</b> 0  | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS<br><b>Name:</b> EnableAutoFileTracing                                  |
| <b>(PID) Process:</b> (7492) Jvczfhe.exe<br><b>Operation:</b> write   | <b>Key:</b> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS<br><b>Name:</b> EnableConsoleTracing                                   |

|   |                     |       |  |
|---|---------------------|-------|--|
| Value: 0  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS   |
| Operation:  | write               | Name: | FileTracingMask  |
| Value:  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS   |
| Operation:  | write               | Name: | ConsoleTracingMask   |
| Value:  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS   |
| Operation:  | write               | Name: | MaxFileSize  |
| Value: 1048576  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS   |
| Operation:  | write               | Name: | FileDirectory  |
| Value: %windir%\tracing   |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap                              |
| Operation:  | write               | Name: | ProxyBypass  |
| Value: 1  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap                              |
| Operation:  | write               | Name: | IntranetName   |
| Value: 1  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap                              |
| Operation:  | write               | Name: | UNCasIntranet  |
| Value: 1  |                     |       |  |
| (PID) Process:  | (7492) Jvczfhe.exe  | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap                              |
| Operation:  | write               | Name: | AutoDetect   |
| Value: 0  |                     |       |  |
| (PID) Process:  | (1356) WerFault.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Property                                     |
| Operation:  | write               | Name: | 00180010F429971D   |
| Value: 0100000010000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B20000000002000000000106600000001000020000000CC6B875C440CBAAEA58C5BED8611E39AA9829013E4B8AC51D0D9F7163EADF0000000000E80000000020000200000000BE26AF426085AF609742DB1A14612244C8BCC3E0EDE09C59A27330B31E6E2E9800000000B3BE81583AE43F56559EF36DEAFC074326B67E4667C7B38DFDF2D00FEFB0DAFFB6ED08C7C337A635133822E53A45D8BF87E2E838C0E75D68C7ABE181C36B22668FEEA0C6662B412EA28B9FBBAC304069F4755109ABD70078DB56841A9E3D50ACDF8312B7407568A8EB09E45CD710B4CFB2B5804DE8C31792DF1D88EDD9A04FA00000000BFEAE620CE76ADB5C5AB194CB9B71310F2C4899DC791B2152EE28D52ABE9B061C9591BBB2EE89C5DECE5ED9BD34A1D5EE5BC76A4B2B4A909F6ECDDAA7A113C97B   |                     |       |  |
| (PID) Process:  | (1356) WerFault.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363} |
| Operation:  | write               | Name: | DeviceTicket   |
| Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000200000000001066000000010000200000001DA1D6B12A5EC90F4F9706980DE59F73C4560375DA4FCB70C232F07F2BC4C6C600000000E80000000020000200000007FB8CEDD17CB5141B2B0ADB40F9A7502AA36C37603876555ECDA09F3C20551CD2008000044D2B2E46D6008C27AF6793632853D6B08A92601DE7F4CB111286C54A126EB6E2E501C833903775A205AB65F6ADEDA8ED2D78FA5A121722DEB8668C3EDCCCE49C7D5AE173D74D78837B54F0695FBB85FB0D1F625E4CA36C36991A60D6F08F3D6251B3F6679949B81F095A284E0D6C69D9123B2B4CB87D90CEA6FFE12EEDBD34C802FCF34B179A21FBAC23D500BC74ECC6E324991082ED59DB24D28D930B18C06F4DB8206E0F8CDBB64EB839B213167D15D2FD06FF3F6BE4E21C5243F96F26FA08EFD84FD97D4793BE950B2008AB346677AEF90B56B32D6E41EAC8C1315AFCCE9B7A69B0B606A0225D3487A5DC700F92ABB26C990CCE027B75B7944984859C796A7B4F5DC2F877970B0F1BFA6B979EE8ED60E0202719B3A45C5FA4FA2C305BC34F6B141F3A6D5664888CD6CC52FF89351D4B521062D792D2E756CECCC2753E7416737CC2076B1C6E2B09FB279F243C2FE8AADB602C896AA74D2C1167A18C4D710776A0ED92462E570C2A107ABDDCCCE906B643254858B87E2C1B4B15115CA3C4A959BA12A095B4D4D2D6E73ECACAD3325F8EB085D1AC05EAB140C420254102BE0E2127FFFA9ADAF9350670D13FAFC59493CAD4F61D4ACBF29E8D9CAF1C0D75CA0C69EDC04239CD12BAD8531FF11824E7B3D922F68C01B1976DF59A0B01C9A89DC66CBE9E33F2017AA52BB21246AB3BE41BB9DBDFD55E7CE77732340B94796942841625190340C5A58FF3ECC4C506112762D8DA058510ED0DE2821E2A291448ED097BD0870F1016E107AE388904A2008BC001C875C2F4C7499016BDBD6A93611B7AFEB82670E32F4D49D5DF32978201C9D6FAA84C494079B15236219F0FD905999F36376437384E799336F97BDE8FC2D103191C0B5C57FD8DE5C0A39FBC071009BDCF49A3C6B903909A66860E25AD470D9CD6A3A34955EF862DE96DC6B128A5AA8B68FFD32DE44E4E5915D80154928D5E2BE8F8B537B2513320F750D1A4A52417631BBABFFC7C7BA5100EFC567D638F22F697B98F2C248710DC90C0DB12316374F9B099D2C56F2C0E56521255ADC845EFB38BD03AFD6DD40C2ED9A9BE486238D0DA2FEEB8FD0550A1F5A4DD179003D91823EEF2C42E43A9A8A0E3D45956CC0D7F2E8BC67DDC901A06D7A46FBE3C7D77DF7268E902CA491585AEBDC677B656B5E46B19832A013F72BCB31EC8DD7056B5DAE89020DA19E54F9801349DEFBABA37AF2CEEC282B912A05F6391A5B45F94F112602B510845023B3B9A77C6A03F5B626E519B3CC6B8B6E6686BA1CF251A065571E28E59C8E5E7DA080050600181BE32C1E109ED5B3AD8A420B40243AA0218E213BE660636F24F41E1BE9A9B91E449E4FA30ADA307A0FCC0AA09C5743E9E160D8991B3AFFB6762BABE8A653F85EB5E9F39EA49B2CF458D3AB68555096B6C80669DDDB75F135272F71C2A02BDD6DB36282979C77AB8710C279C831E9E8610BF9A3E76733BC5D2D13B38C7C7995B9FC8222598FCC4F1910CDF9989E8CB1165F97C805DCDD0656B8BF3B04AAB40733A99293B3B2C7F4819F913C66F451EA4B7B08BDA8340230C13351652A185D6C6C6BEE1FEE2403DB202051F7197F738DD4D1A250AD09332B20C7EE810EA0F909B3BDF2AAE69CADAE1B7824987D7F936FC8D31BE5B5188C38BA9FC21829CF14F81765D3DE4F994F7879DB0D4919C4A3C314713D4BDD78BDBDDE7EFCB0FE85740D49466B7E4B846F37F8AC800B2217D80E2505E0D0E076A0E8A90B770A6CDDF5AC3A4E0746B0D3B23F511D2FAE902C9BB2122681EAD3E32174520F31656DD145B95B94C89CE08B98E3066BC633273A367920D6D0E0FD3A90DDC094466935C04E0B625BBA4A38AA4DCD5C210DF94C85916D36E63F1192378475D018C0394A3A68CCBAD9095841340D9959F54110AE1D3B812CCAC80D790E185818A618083727EEDAEA5B7BF7546FD14396B36646EB73B618321F64F790795E727A0F72BF0E8E084B7FC8BF7C46D2706FCFF547593B49515568E03E4C7DC4B117B369E9896723582B326C884ED12670B0C3B36F360A08D8A9CCF9C60A5E72FA8F8F34207A0C8C99B318961E4079BE1B60E155DB0E807F627FAA76BF38BF057A6FF9900DD8DB585BB68576F35A9D2B4D7F2CE5F301E34F84DCBF9EA972D4B91729C4D059AB49765707DFFA2FC69CD8C56E4BBA83068A0A047490977B6A7C7973E2385FA4FA847E0F646920B220F170543E695FEE9BA2FE3231C8AFCAC48CDA5E399EE83D5584DEE5344E48C1AE983871583C6685F62A3565C582498DBD30C84C2AD3157348FB26AAE61022D505D4817B0A1E409B012DB100947C1AD21219EDC8BADEDBE8EE50409EF82BB0BB53D08D9D319DD5956AB5772516099A1096B21EBCE3F6F0C78A6F3E0D0397D6E6C3E00EB9B89A0D3B28B9D6967A61B596CADCC5375EC0CC6146A615E325C13B0CA4E62CC658D470125C73410B0DA679FF4F69D96F10B99443F086C3A06CD43D6A1897725029E975933127E0EE3179B93BA952511AC871EB42F53A326FDAE2059C8753BA7023DC689B41AE67B8D1B1250B54928D267F99637CF57A24A80CA9A7E50DFCDF47C40943FC8FE0CCE635E368AD664F6F03F38CA4FD5D264E6AC80942640EC34202B7D63F00C82B16A6F000975DEDC3BF3114DF549EEF147E9D0D8E2399F7912C2D6B42DF618951113289F83EBAF7632F809E2D86E69A73448BF85C9E276F0237B994928849E1EBA5621E7B578C84D0C48B8388A04192C36C3A243B055896625C43C729A6729676FF5BB4079E4BB561817F324C6F4E7EE2CC7F908F7CB8EF1AD3CADD7DCED5AE9F8252F4E7E2187F31311695DF35A2D27C86E9A727AE8817A04D98507B949090573597EA82CECA38ED848FAD4CE9A41F48765F3AE6084AAD8874DE6FBE78043AB20B0D448B879549C80595BC040000000404819C25DD32F1C35983ACDE8BF3028A338DE6C1D59AC77738FB8DC2DD1F223F676CF6FBDDCFB701B20E1070A8F8C12CC99AC3A2F9CDEA110A5A3C00BB0C049 |                     |       |  |
| (PID) Process:  | (1356) WerFault.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363} |
| Operation:  | write               | Name: | Deviceld   |
| Value: 00180010F429971D   |                     |       |  |
| (PID) Process:  | (1356) WerFault.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363} |
| Operation:  | write               | Name: | ApplicationFlags   |
| Value: 1  |                     |       |  |
| (PID) Process:  | (7824) Muadnrd.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32   |
| Operation:  | write               | Name: | EnableFileTracing  |
| Value: 0  |                     |       |  |
| (PID) Process:  | (7824) Muadnrd.exe  | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32   |
| Operation:  | write               | Name: | EnableAutoFileTracing  |

|                         |                    |       |   |
|-------------------------|--------------------|-------|---|
| Value: 0                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32            |
| Operation:              | write              | Name: | EnableConsoleTracing  |
| Value: 0                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32            |
| Operation:              | write              | Name: | FileTracingMask   |
| Value:                  |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32            |
| Operation:              | write              | Name: | ConsoleTracingMask  |
| Value:                  |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32            |
| Operation:              | write              | Name: | MaxFileSize   |
| Value: 1048576          |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32            |
| Operation:              | write              | Name: | FileDirectory   |
| Value: %windir%\tracing |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | EnableFileTracing   |
| Value: 0                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | EnableAutoFileTracing   |
| Value: 0                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | EnableConsoleTracing  |
| Value: 0                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | FileTracingMask   |
| Value:                  |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | ConsoleTracingMask  |
| Value:                  |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | MaxFileSize   |
| Value: 1048576          |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS            |
| Operation:              | write              | Name: | FileDirectory   |
| Value: %windir%\tracing |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation:              | write              | Name: | ProxyBypass   |
| Value: 1                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation:              | write              | Name: | IntranetName  |
| Value: 1                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation:              | write              | Name: | UNCAsIntranet   |
| Value: 1                |                    |       |   |
| (PID) Process:          | (7824) Muadnrd.exe | Key:  | HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap |
| Operation:              | write              | Name: | AutoDetect  |
| Value: 0                |                    |       |   |

## Files activity

|                  |                  |            |               |
|------------------|------------------|------------|---------------|
| Executable files | Suspicious files | Text files | Unknown types |
| 6                | 190              | 40         | 5             |

### Dropped files

| PID  | Process     | Filename   | Type   |
|------|-------------|--|--------|
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-current.bin | binary |

|      |             |   |  |  |
|------|-------------|---|--|--|
|      |             | MD5: 297E88D7CEB26E549254EC875649F4EB   | SHA256: 8B75D4FB1845BAA0612288D11F6B65E6A36B140C54A72CC13DF390FD7C95702  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite          | —  |  |
|      |             | MD5: —  | SHA256: —  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json.tmp  | binary   |  |
|      |             | MD5: EA8B62857DFDBD3D0BE7D7E4A954EC9A   | SHA256: 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json  | binary   |  |
|      |             | MD5: EA8B62857DFDBD3D0BE7D7E4A954EC9A   | SHA256: 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3561288849sdhlie.sqlite-shm               | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-shm   | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-shm      | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs.js   | text   |  |
|      |             | MD5: 41C3031A19C68F7EBCEA0C4B077A2078   | SHA256: 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\SiteSecurityServiceState.bin   | binary   |  |
|      |             | MD5: 47DD2A463052776C50BF3B020C45FF9  | SHA256: 0731CDA042482C8A43AB9A8E0BAD8938D1D12892640EF963AFBFB05D40582351 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.bin                                   | dbf  |  |
|      |             | MD5: EF90022DF0735160DD056C0E6670E915   | SHA256: 2B663C0B462A437C8DE3D9B95EE157AE181249B78BD6F7BD73F7EB6D9E03F87  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\AlternateServices.bin  | binary   |  |
|      |             | MD5: BD1F8541EE6955620BA2745F31D0EBBC   | SHA256: 1938768BA2E4E560644DBA7C371966C04A2015959AAA0698292F62C678C2F17  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.tmp                                   | dbf  |  |
|      |             | MD5: EF90022DF0735160DD056C0E6670E915   | SHA256: 2B663C0B462A437C8DE3D9B95EE157AE181249B78BD6F7BD73F7EB6D9E03F87  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm              | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db   | sqlite   |  |
|      |             | MD5: B993525C060FE5A22B9747AC239529A8   | SHA256: E9396152C2F9A52ABAB898F259D45C181003CEBE88BB54DE2A4C65402B6B859F |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-shm       | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db-journal   | binary   |  |
|      |             | MD5: 0F5D3BD22808C0A5A90A80E398828F84   | SHA256: 3F6A5CE958BF096926459059C3222D354042D0123B8E08A4973FC9C6B358B7A1 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite-journal   | binary   |  |
|      |             | MD5: 413E2331DE4FE9BC426A8DD5BA855C3A   | SHA256: B017CF1CB55A148D29EA3B0A47A7A38AF056A95C8C601C4C894CA31C2A8CA80A |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-wal      | binary   |  |
|      |             | MD5: 119835D3E2EAA9C0899A5CB90A7E82E  | SHA256: 46E506DB1FBB13A316ECA333F7BBB3AE09C3A09EC0A1DEADDCF35283AAEF233  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs-1.js   | text   |  |
|      |             | MD5: 41C3031A19C68F7EBCEA0C4B077A2078   | SHA256: 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2823318777ntouromlalnodry-naod.sqlite-shm | binary   |  |
|      |             | MD5: B7C14EC6110FA820CA6B65F5AEC85911   | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4.tmp  | jsonlz4  |  |
|      |             | MD5: 7EEF2C12470FD025856EC9A89CA300BE   | SHA256: B2B6A2DFE42C8680CCED019981FDA3A84410120924161940CE460AC0C0A45834 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-wal  | binary   |  |
|      |             | MD5: F3E9E277A5E098BD3BA2EF5CFB4D767F   | SHA256: CE1D2806161C4AE89E46FB5F8C54860DAE64403D6EC6B86CB19A2AE8B816EAB  |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json  | binary   |  |
|      |             | MD5: 6F59D26E61E282B46AF0CF4386C0172F   | SHA256: D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4  | jsonlz4  |  |
|      |             | MD5: 7EEF2C12470FD025856EC9A89CA300BE   | SHA256: B2B6A2DFE42C8680CCED019981FDA3A84410120924161940CE460AC0C0A45834 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4.tmp   | binary   |  |
|      |             | MD5: E08EC08F038834A799C9F2F95F0A7ECD   | SHA256: 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974 |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite-journal   | binary   |  |
|      |             | MD5: D68E8A062869338F6DBC42005285E463   | SHA256: 0F3A6FA7BB4FA468B0C3882CC88DB989C6262CF9EAE4D683BDE59B03BA152AAC |  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4   | binary   |  |
|      |             | MD5: E08EC08F038834A799C9F2F95F0A7ECD   | SHA256: 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974 |  |

|      |             |  |   |
|------|-------------|--|---|
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json.tmp                                     | binary  |
|      |             | MD5: 6F59D26E61E282B46AF0CF4386C0172F  | SHA256: D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json.tmp                         | binary  |
|      |             | MD5: 5125D172D031232D9F8A809258BE53A3  | SHA256: E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.vlpset                  | binary  |
|      |             | MD5: 1074F10F2FB691DD5996FCCED30B5CB5  | SHA256: 9051E2BBD3AD850B7353CF15FE5EDA284FAE8DC6555660E5762CE65ECE50D345  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.sbstore                 | binary  |
|      |             | MD5: C9A39524AA5346ADDA89995267EB6EEC  | SHA256: C2766B2303A07F8F6620303C94DB549F589073FB609EA3C28135923614B92722  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.sbstore          | binary  |
|      |             | MD5: DD0458514C9A922B45DA6A8BEBE47320  | SHA256: D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.vlpset           | binary  |
|      |             | MD5: DE0D88480C24350C59E1E9A3583DE0D1  | SHA256: 01BA9F0B913E04ED10BD7166796483DD4F72005F249D6EE68B12117BE4B5D3C7  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json                             | binary  |
|      |             | MD5: 5125D172D031232D9F8A809258BE53A3  | SHA256: E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.vlpset    | binary  |
|      |             | MD5: 42959B02F1CEEC2316BCF528B3682DF6  | SHA256: A4AA73B23B2D55C428BF7BB62BE731D4AA391D7A22D54586A7ADD1DE8856221F  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.vlpset           | binary  |
|      |             | MD5: 74008AA6F606067615E16B233A6808D2  | SHA256: 5F5DCBDC2BBD909BCB355E6320E2FFA53CE61421C788CB3631F99B7FA472C24   |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.sbstore   | binary  |
|      |             | MD5: 85F5DC8F04559E256822D2C8C7A7167E  | SHA256: 860A6637305E4E5DE4ED5C86DC9A704189A5F55A2865DDFC44518562F12CF8CA  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.sbstore          | binary  |
|      |             | MD5: 40ACCF6B4CBF993EB8DAAA09B2AC6508  | SHA256: 282E12F46E25AA8CEB7227E837772B3B0DD3694F21BD156157B2A23D44A565E9  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.sbstore           | binary  |
|      |             | MD5: F92AB98A911930D5CDD4B0104AAE171D  | SHA256: 3E82D8159C57E04D8A9BAEBDBD72362B08F7EFDBBADAFBDA996173ACFC0C23B6E |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.vlpset            | binary  |
|      |             | MD5: 52A01C93009ED9DF37776CD44897A165  | SHA256: FC64A6418FB19DB437A16C2F7DDC4B5DD071F02D7EF19CC0C1FD2C34BAD4ADC   |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.vlpset          | binary  |
|      |             | MD5: 40165280FF1345B5241EC2A9D1DA2AF0  | SHA256: F80BDD5341D8B1EE946E344E258EF2D35C3C0BB6B13EB7B3E6A77467DFA8B97F  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.vlpset  | binary  |
|      |             | MD5: 9AA2F992F7B0A8A39A2016958EEBF14C  | SHA256: 7F49C1E0EE79DB93724B95C0184640E79A99FA3E7C1D91D13B21954E2E7B94D2  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.sbstore         | binary  |
|      |             | MD5: B9556D03AFF392142AD5691D2F867310  | SHA256: CFD3909B41C1EE3C8CB8B7D2B1378065E7D3B543FFF1F2FB7A4F25C5FF41722C  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.sbstore       | binary  |
|      |             | MD5: 0C0CACE6CB13270CC067680F0C49A5D4  | SHA256: 5F10F5155717403B1D2A18802DA0C1E55D44C40F655D971D9112C654519E7617B |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.sbstore | binary  |
|      |             | MD5: 8B4FF284E845A5465890EEBCE0CAA62   | SHA256: ACBAEC57934E402DE520C0FE376E68A41ED294365497C9220BA33A099F676C47  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.sbstore               | binary  |
|      |             | MD5: 9F6B331AA1E070DCFEE473E76CE56C3   | SHA256: 7DBBEA2DD387EEB85E1F56E02FC9989ACDE570CD43BFEF2C2A827093BA87DA6D  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.vlpset                | binary  |
|      |             | MD5: 130B9AC2BEEC5ADA274561105D81AE36  | SHA256: 7D99FEC08182A5B95D18D1569EDAA2C60C2AAFBD15A56D8882F22F3B395E6460  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.vlpset             | —   |
|      |             | MD5: —   | SHA256: —   |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.vlpset        | binary  |
|      |             | MD5: 355BBE8195ACF89687747D60085C5B30  | SHA256: BFC7F5B2CD28113650477CF2FB36F039682F679644659C66F445C25707CC9DE8  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.sbstore             | binary  |
|      |             | MD5: AD3D0BC4B7B38A5FBE0DA2CDCE8A0245  | SHA256: 3ABF8081360EB366F4DD3B98ACFFAF73C5A990CD19C3D45E100B7F3968EA34    |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.sbstore        | binary  |
|      |             | MD5: 22698B4CF784BBAE2D583F00491D43D   | SHA256: 3849563088AE0677D61702A1310FDE2DE5DD846D53037222D3EFE012197BF5    |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.vlpset              | binary  |
|      |             | MD5: DA94AE10143DE265746AE28DE00B1E0   | SHA256: B567D813342D76D81C51CAEB07646E70546FBA1E3BE68580FBC9982E58FB08A   |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.sbstore              | binary  |
|      |             | MD5: D5D6B4D59B4AE4E2DE4B40D0DA083571  | SHA256: 000E3A78C72A210CA3B5417A3CDD294FBCE2A31661601C9D594C75CF2800571C  |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.vlpset               | binary  |
|      |             | MD5: C2994D388F8780C87D35C352D9582985  | SHA256: 7ED09F7D2BD632F70077A4AE42BD2F3FB654B03CD72652F51678B0C7D027F25   |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.sbstore         | binary  |
|      |             | MD5: DD0458514C9A922B45DA6A8BEBE47320  | SHA256: D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761  |



|      |             |   |        |
|------|-------------|---|--------|
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.vlpset<br>MD5: 7194B6BFF691A056852A51E2E06CE8FE<br>SHA256: CBE2DC6ABFE25BEAD60F4DFAF419FC0F441FF8A8DD4A2FEBF5553BE1CBD90C49                    | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.vlpset<br>MD5: 0C0D67875BD75A0227C02DD8529BA01A<br>SHA256: 614BE0169EC36E67223EB9645A98DA66DBFDE5DFBB89BB064F428AAEABDD9D97                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.sbstore<br>MD5: DE11B7D1A2807D760720D2BAFC9243FC<br>SHA256: F2FC25733FF62CB1CAE712299B9128E6E4D3BFFA6CD810773F0114E6E8D75008                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.metadata<br>MD5: 82E9807B2462B11303A5223234CF3E41<br>SHA256: 673B56A5F4085B2F52F29AE2112E8F65230DE3010CF625D1A27D303E790EB827             | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.vlpset<br>MD5: C0E1AC752CB716038A8245AA68AF4C1F<br>SHA256: E448D98C433F007A572960B5A956B474528893020773110D6921767BECDF3837                    | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.metadata<br>MD5: D706F661CA72A80ABFFCDC4FED3C4DDB<br>SHA256: 1A5D3A3CA49DF4383BD2161A80B9C55B135BAC4161098E2438AAE1D8BDB40F02                 | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.vlpset<br>MD5: C543F008A2E02F4D4F095EAA94722B36<br>SHA256: 1363B9298E63DAD9E5FE8AED4DBDEB20415DE153B27A8C6AC8F552293B324D30                     | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.vlpset<br>MD5: 9819E8BA5957767C478A506CFCE1D9EF<br>SHA256: BC071CF03DF184C5F23EA47AFC8C75F40A9651BB35E9B296840E854D39C5AAD0                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.metadata<br>MD5: BBF7EF2E4A3CA89407D6D4225590A924<br>SHA256: 0D49E29744875E37BB5FC2CFB0A32E30A801037BFF7DB25E4649F131937CF054                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.vlpset<br>MD5: CF3989ADA19750F5BBD46BC8ADAFFB7A<br>SHA256: C9C80D8B5B9464FD22E1C8B84BB80792FCFE69FA56F52F7B491E7FC6DA6C8F4                | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.metadata<br>MD5: DA219EC22F607466BA385F3C98E884D8<br>SHA256: 2CD522E385FD6D09152431644EFBE440C4E1D3657C1607FCBB3891F8A411663                      | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\metadata-v2-tmp<br>MD5: 04C97972673908F5ED4BDC2CAB464AAD<br>SHA256: 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97                        | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto-1.vlpset<br>MD5: —<br>SHA256: —   | —      |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\metadata-v2<br>MD5: 04C97972673908F5ED4BDC2CAB464AAD<br>SHA256: 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97                            | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.sbstore<br>MD5: 00A7316960DD8B059CCF78D4378F256C<br>SHA256: B949AB0D5C3F97B1C8D75A43A8C5C0718F820B60C0C3417824DC2B7832D69EB8                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.metadata<br>MD5: 2A2D9C6ADE9C03E0377BBDE841673FC<br>SHA256: DF47EC2EC4BBAD6638D668A7233D070704F9EF2583D8B37AFDAAE8500C651536                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.vlpset<br>MD5: 94DD091E0A4A2C61EFE13A77E2F0FC9<br>SHA256: CEB94C82C2A8B35DBBF12532548ED1D5402A656473983F146325E9639AA1077C                     | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.sbstore<br>MD5: 519BEB1B01FC355BB388F1F75BE997FD<br>SHA256: FFE2D3077B81AE6F51B220C1C661B276C823FA67DAD1D64FC5F17249FC54BDC0                     | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite-journal<br>MD5: C91DE383C9FCA9AC5C0AA314673F6255<br>SHA256: 762FD03672E3D942F80CAEBFEA1928B60530B7FB95E937B242B5C9B8C2AAB99A                 | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.vlpset<br>MD5: FCC9C2C9B611A3264B68EBE180EB4248<br>SHA256: 6ECD378A537EEFE350B45CFA353741383F407D99D776BF23155A7825DC5DD2BC                      | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.sbstore<br>MD5: 79F921E7A69AAD95115C030A2218875B<br>SHA256: DAFBD8D4E15E55D11E90199D295D69C42189A79D4EA2806B880515FEADA36CD                         | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite<br>MD5: 2852B0CBBA9B0BB004851F3421E0B81C<br>SHA256: CC0489E48450A25DAF1C2114EB820BB096AD7EBBC93EF25E253A37DCDDA2120                          | sqlite |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.vlpset<br>MD5: 1CB5A03C23989B1DDFBD4C5C03204D12<br>SHA256: 191BBF1BB3E1263CC9F962753E9B93698AF50B91A314BDBB92FB58FE51B6AF1                     | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.vlpset<br>MD5: DF26E6FB795248D4D43138A4D346656C<br>SHA256: 3B40F92474BEDB798EDFCD86C919C5BEE014AE80F0703AE6CCDED704629DDD4E                         | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.sbstore<br>MD5: 7BBA9B83F0F213C5A723209D4C9962CE<br>SHA256: E1B8E7DEB0F34EEB6BF4D10E47E734A1FE829C365DF360B98646D7E11F2DD4C7 | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.vlpset<br>MD5: 8AC8A05028631170937EDA4CF0E0A35A<br>SHA256: 456AB2C0E4117D62DC529362EB22C725D410098868442729ADE5E4FF0822E78   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\webappsstore.sqlite-shm<br>MD5: B7C14EC6110FA820CA6B65F5AEC85911<br>SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-new.bin<br>MD5: —<br>SHA256: —  | —      |

|      |             |  |        |
|------|-------------|--|--------|
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache.bin<br>MD5: —<br>SHA256: —   | —      |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linked-digest256.sbstore<br>MD5: 9275B832091D9E3BFE50898A3BE022B5<br>SHA256: 38C52A5435B625083000A05448B9B95E033F7B352377510DF668CEE749DE5803E   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\usage<br>MD5: 58DBA7ED5C9C7CA9F184BBA375F1660F<br>SHA256: 280BD2D0DDAFD903B35A21DD24F7DFAA6EDCF218BAD02765273A54F949CE2936                                | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linked-digest256.vlpset<br>MD5: 5F93E0F827909390D257EBB27C77F392<br>SHA256: 5BCB684F3EE3B2EC2F4945655FBEF281C487399D6BF90451647DB1761715D4C8     | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.sbstore<br>MD5: F130C472E963FF3CEED251C65964B927<br>SHA256: E5D2A5BBE8AA43751EF7F7BC3A817A0963D56272A4C9B6055E60929606186CE2   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.vlpset<br>MD5: B50CF628E0082A7840D84D0CBE1CAD48<br>SHA256: 544DF79BCEF9DC8E082021E342C2A1B12CD0B8BDAF3687E0F23785406EDF33AE    | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.sbstore<br>MD5: BE7D2765DEF13D5A252CC963F62E9DEC<br>SHA256: 06EEE65E89C04B4E84A983437D9D98295DC2FE629A306244AACD7D2A787E5BCD          | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto-1.vlpset<br>MD5: 471E976917D93E066A2836D07189E46D<br>SHA256: D124C902BAAB7044693C31369885B9915683718C10F31A9DE5A446732C066F5D                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto-1.vlpset<br>MD5: 472D24AA36ABE086BE12D6567B7B82E1<br>SHA256: 0E8F4F9FACF1D6B813E944E1DC093A4DFB48AB12E2AA798E02064EF022B07870                    | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-new.bin<br>MD5: DFA790E6BFEBADC616EEF9D430FF8222<br>SHA256: 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2  | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache.bin<br>MD5: DFA790E6BFEBADC616EEF9D430FF8222<br>SHA256: 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2  | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto-1.vlpset<br>MD5: C787F2747806B00C76CDBE040C93F98A<br>SHA256: 2264A14B2545F13F8322AF37F352093105978D0BDD9AC9DDFB388802E4E7D50B                  | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.sbstore<br>MD5: 51D0037241FD968870F54ACE34821097<br>SHA256: C0D2FF4A77D7B1383AF6534B54B0BC3E5DC9248447246D77BACC07D645587DE1                      | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.vlpset<br>MD5: E64E488BEF398EE7185004BC761DD23C<br>SHA256: 7EEE6F6E100DE281737D6F861771B464BD8FA49780B1BD2C1577E02F0C40B35E           | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite-journal<br>MD5: DDFAOB238218E11A9B4BB24CAE34D60E<br>SHA256: 43A6F1E480E674D66E86EE8BCD7C8A57EB5668505C7FD7ECD83A598876216CE4   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\ldb\2918063365piupsah.sqlite-wal<br>MD5: —<br>SHA256: —  | —      |
| 6596 | firefox.exe | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\ldb\1657114595AmcateirvtiSty.sqlite-wal<br>MD5: —<br>SHA256: —   | —      |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.vlpset<br>MD5: AC3767913E46AC546879E57694B8BABA<br>SHA256: F4DD01915D2ECE9FAA5D5475568C7D44A1B82B6E36A8B2BA96AA52AB54DA99ED                       | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child-new.bin<br>MD5: FC15FBC5EA781C717736043BD6A44C93<br>SHA256: A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA                                       | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.vlpset<br>MD5: 93879DA58B8AC3B3B58DCC6DD86D47EC<br>SHA256: 08EA6E59EF882642C30441E0FAB4B6BC0A76B98BE273C540B065AB87F8BE1A97                        | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child.bin<br>MD5: FC15FBC5EA781C717736043BD6A44C93<br>SHA256: A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.sbstore<br>MD5: 03E14BE9BC0A656037A3B5942A546B9C<br>SHA256: 6B768A57493C00B1AE0DA8677C98B99EFB668D1D2BFC7BC3856BA3DCAEE73E6                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.vlpset<br>MD5: C0E1AC752CB716038A8245AA68AF4C1F<br>SHA256: E448D98C433F007A572960B5A956B474528893020773110D6921767BECDF3837                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.sbstore<br>MD5: BBB8F6725E298CF77AAD7FA594F40D87<br>SHA256: E1FE68E203733D0E1B5078B97632D9844C6E021AD78247BFE07AF8F81FA3B6A7                  | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.vlpset<br>MD5: 41FAE052DA51D99364071F405C6C003E<br>SHA256: 32FD3723664E71D8B405FF333C9140DC5CD221B7D20572255A41609A95001DB6                   | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.sbstore<br>MD5: 9AEA09B15A3BB43D85144D3BD1AC7F75<br>SHA256: B880EBD4346DD9EA9EECD9D83B82F85493C4BC4EBEE50C07F6BCFA29D9C8D4E7                       | binary |
| 6596 | firefox.exe | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.sbstore<br>MD5: B4229CDB076DF64F59A6EF909CD8A66<br>SHA256: 485B156B4C5756577A36D077CD74D1AA62FCBB3158F45C31BEA4C64B02D443FB | binary |

|      |              |   |   |            |
|------|--------------|---|---|------------|
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.vlpset<br>MD5: 0371AFCD63B61B5C80CC06ACFE66ED2   | SHA256: FD64F028F01825E02F54E36E8A4B3597BA335974907106D6D147927DED1D961A  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.sbstore<br>MD5: 2CBCC17325808925E52D4DA835FE498B | SHA256: 0E1911A712C9CDE4E411312E8F347C8B3560B19A2B93876D153EFACA52F486A5  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.vlpset<br>MD5: D0DE50C7B2BFE8240FEB389CD09E4E25  | SHA256: 4E25C5110096EE842CFAAE27485CE8994B03E7A00BFEE17458101A209EB3D98   | binary     |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\OOD5yt-b.exe.part<br>MD5: 5EC4256E6A2367502A8058F4BC8F4ECC   | SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BDFD2DBDECED86AA9B2   | executable |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.sbstore<br>MD5: 563B1CF89B324A8E37A899F001A340B0  | SHA256: 2142ECFACC145FE44095F8677BB3CCF021C2DD600C4627F1548B4F1E1C550DC9  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.vlpset<br>MD5: 0E74BACAB7B2923E25B62F282EDD71F    | SHA256: 34D4586E12D08DD3171BC8A383EFD600926BE0F9F826D8362C61FB660DEA1B1   | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite<br>MD5: BA2A9081BD1D04E47C24B92588DA3038                | SHA256: FE95386724215C856F371614219653F672B20B6E2677FFA9C033F92DB1BFED71  | sqlite     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE<br>MD5: FB64A9EBEDF48D3895381D5B7D80743D   | SHA256: EA21D495930AD76F267A33A0F593DBFC7EA75E457CAE49A29DAAD8BD920F42    | binary     |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\Jvczfhe.exe<br>MD5: 5EC4256E6A2367502A8058F4BC8F4ECC   | SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BDFD2DBDECED86AA9B2   | executable |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\Jvczfhe.exe:Zone.Identifier<br>MD5: DCE5191790621B5E424478CA69C47F55   | SHA256: 86A3E68762720ABE870D1396794850220935115D3CCC8BB134FFA521244E3EF8  | text       |
| 6596 | firefox.exe  | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C0018BB1B5834735BFA60CD063B31956<br>MD5: 732CFEB76B91C4D13978A008B8C666ED7   | SHA256: 9FA89FC0A1DA813E6DD8B93904C1FCFA6546CFBE70747FF8468DDD14D2552DBD2 | der        |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.baklz4<br>MD5: A01DA38618B46EA1BC6DDF8CA11634E4  | SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5  | jsonlz4    |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\previous.jsonlz4<br>MD5: 7B0DB853EFD8FCCFD078A91DE1B732CD                                       | SHA256: 72A40CD1C262925FE79A68A7F57042773FB1F23E3F815C24E89426A29957E89   | binary     |
| 1356 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Jvczfhe.exe_e8f4a47beb21929faaf5bbbc7cb947adda294c9_7cb78550_5641ad1f-f35-4b34-8a69-19f8a8163939\Report.wer<br>MD5: —                     | SHA256: —   | —          |
| 1356 | WerFault.exe | C:\Users\admin\AppData\Local\CrashDumps\Jvczfhe.exe.7492.dmp<br>MD5: —  | SHA256: —   | —          |
| 6596 | firefox.exe  | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C0018BB1B5834735BFA60CD063B31956<br>MD5: 06DDBFFCBB38D5FD21F4036E9D92EC2  | SHA256: E071C5DA2B1BDE45851423554AA4BFED3F488CFC4C597A9DF0A01B131AB7AFE0  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4.tmp<br>MD5: A01DA38618B46EA1BC6DDF8CA11634E4                                   | SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5  | jsonlz4    |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4<br>MD5: A01DA38618B46EA1BC6DDF8CA11634E4                                       | SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5  | jsonlz4    |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.files\2<br>MD5: D2AE97B1490CC258D04CF702943AABA6              | SHA256: EE70E50E8C808399C10883D9EA525638DCCF93570B6D855C7586CD15142EDDEC  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json.tmp<br>MD5: 9121DAD27A71AA06B34E22B3247AC3C2   | SHA256: 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.bin<br>MD5: B818374634D95221DEB007E6C1DB1FB7  | SHA256: 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.tmp<br>MD5: B818374634D95221DEB007E6C1DB1FB7  | SHA256: 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll.tmp<br>MD5: 842039753BF41FA5E11B3A1383061A87                                   | SHA256: D88DD3BFC4A558BB943FCAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C   | executable |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info.tmp<br>MD5: 2A461E9EB87FD1955CEA740A3444EE7A                                  | SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC  | text       |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll<br>MD5: 842039753BF41FA5E11B3A1383061A87                                       | SHA256: D88DD3BFC4A558BB943FCAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C   | executable |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json<br>MD5: 9121DAD27A71AA06B34E22B3247AC3C2   | SHA256: 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json.tmp<br>MD5: 6A6ECF6080A1AF8963BD69766AC7E44D  | SHA256: 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7  | binary     |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json<br>MD5: —   | SHA256: —   | binary     |



|      |              |  |  |            |
|------|--------------|--|--|------------|
|      |              | MD5: 6A6ECF6080A1AF8963BD67966AC7E44D  | SHA256: 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info  |  | text       |
|      |              | MD5: 2A461E9EB87FD1955CEA740A3444EE7A  | SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Temp\tmpaddon   |  | compressed |
|      |              | MD5: 09372174E83DBBF696EE732FD2E875BB  | SHA256: C32EFAC2FAF4B9878FB8917C5E71D89FF40DE580C4F52F62E11C6CFAB55167F  |            |
| 1356 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1B6.tmp.xml  |  | xml        |
|      |              | MD5: 737222720E097336E5D12487D43E1890  | SHA256: B5085F683C5AC51872E2C99D400C4E71B5B76427574CA1A1174FE0FE895254F  |            |
| 1356 | WerFault.exe | C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\21253908F3CB05D51B1C2DA8B681A785   |  | binary     |
|      |              | MD5: 82C30E45BF5F93A5DB1D5E47F913053B  | SHA256: 2C6BBFF9207065E8800C4AF0CB2748818ABB3CFFC0D6D518FE17F76A232F8967 |            |
| 1356 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFF.tmp.dmp   |  | binary     |
|      |              | MD5: C0E9448BABAD46120AF409E3D13582CB  | SHA256: B41D7B362ED06B68EC9F259AA83B820396DAA50F36EDF0CCDB4E70AD91ABBD75 |            |
| 1356 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WERB177.tmp.WERInternalMetadata.xml  |  | xml        |
|      |              | MD5: DC4CB05F4E9CE6445F414D263FAE3174  | SHA256: E7F6B8755BAF770E61006D6C9844E09D026878445C3C95F5F3C36C0FBE15286A |            |
| 7584 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Muadnrd.exe_dd9d47dfcaa2177d1190b55ee6f3574cf671f90_4600b98d_c0351b42-4a4c-4b9d-bdbe-a700399d2592\Report.wer |  | —          |
|      |              | MD5: —   | SHA256: —  |            |
| 7584 | WerFault.exe | C:\Users\admin\AppData\Local\CrashDumps\Muadnrd.exe.7824.dmp   |  | —          |
|      |              | MD5: —   | SHA256: —  |            |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\xtorOyHX.exe.part   |  | executable |
|      |              | MD5: 9773175646F2942573BB40551B142A99  | SHA256: B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4.tmp   |  | jsonlz4    |
|      |              | MD5: A6338865EB252D0EF8FCF11FA9AF3F0D  | SHA256: 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4   |  | binary     |
|      |              | MD5: A6338865EB252D0EF8FCF11FA9AF3F0D  | SHA256: 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\session-state.json  |  | binary     |
|      |              | MD5: 7AE136DBC9D972F5B344C42BC468D250  | SHA256: E484553062E15D23A99ED613E21593E9EA3B492806C7E58614E901AC3EC78575 |            |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\Muadnrd.exe.Zone.Identifier   |  | text       |
|      |              | MD5: DCE5191790621B5E424478CA69C47F55  | SHA256: 86A3E68762720ABE870D1396794850220935115D3CCC8BB134FFA521244E3EF8 |            |
| 6596 | firefox.exe  | C:\Users\admin\Downloads\Muadnrd.exe   |  | executable |
|      |              | MD5: 9773175646F2942573BB40551B142A99  | SHA256: B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms~RF13ba1c.TMP   |  | binary     |
|      |              | MD5: 2D72BD10DFB5071E03E48FD977CF5800  | SHA256: 8D7E1049FA26CA1CE3F1ABCC627F0E5AF693D3C791D62872320C360AA6E98D83 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\901A5L0GJXRA5ELANF4V.temp   |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02  | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF13ba4b.TMP   |  | binary     |
|      |              | MD5: A745A87D904244F96B205DD66BA8AD95  | SHA256: E6603B79CF37A0C059B14E1BEBB0277323DFD4B57EEF3B4567417308CB24546C |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms  |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02  | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\rPDIkse4D7V1E6pAjMfUwMOH06SrtemO4GCIWXN4xjU=.ico                            |  | image      |
|      |              | MD5: 6B120367FA9E50D6F91F30601EE58BB3  | SHA256: 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PN5BI8GYQV2728PG9PLV.temp   |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02  | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms  |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02  | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 7584 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WER8665.tmp.dmp  |  | binary     |
|      |              | MD5: 394B3E4971EF4CC959394FA5412F9D75  | SHA256: AE2527D5682A558469189B95620D0B109B073EDD3175D1C41067A08217F75287 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping.tmp  |  | binary     |
|      |              | MD5: 1AA7FA53118748F72035DD5B174D228D  | SHA256: 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\4zihmJyKsj3_uEUSHbD8Te4dekBCaj7n+9q6HH9dZs=.ico                             |  | image      |
|      |              | MD5: 6B120367FA9E50D6F91F30601EE58BB3  | SHA256: 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-wal   |  | binary     |
|      |              | MD5: 93CEBE93AC7602CB9837707C323076E7  | SHA256: 66E2F6CDF7FCEBADFADAC924BDC033528046CF9BDB586A33548E499372F3792D |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NM9BC1I0Q52BK02U77CN.temp   |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02  | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 7584 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WER8761.tmp.xml  |  | xml        |
|      |              | MD5: 90DB48E0CCFB5E6070D4E3226E5C62F   | SHA256: C590E9240CE4B285EFD6659C8D316E5DFF00FCCBADAFB44B71DCB7E316276AB  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping  |  | tss        |

|      |              |   |  |            |
|------|--------------|---|--|------------|
|      |              | MD5: 1AA7FA53118748F72035DD5B174D228D   | SHA256: 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-shm  |  | binary     |
|      |              | MD5: 885F6E89E582997D4F0201085F9C9E2E   | SHA256: 8540D5F07FE075B726A4D466C4FC7B540C30BFB90B2FE3366A348C37EE759EB3 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite   |  | sqlite     |
|      |              | MD5: 9FEB3178D08C74728B501EFBE503141A   | SHA256: D163FC004C74F1723153227392C15978AA4EC36BD7CA66C33E03AEA22C200615 |            |
| 7584 | WerFault.exe | C:\ProgramData\Microsoft\Windows\WER\Temp\WER8740.tmp.WERInternalMetadata.xml   |  | xml        |
|      |              | MD5: E9553BB3BC52242581D148E7FA13EA3A   | SHA256: 152E61F41D80497410469F77812A9BEC7909421779F0D65E6F0814F2478781A8 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-shm  |  | binary     |
|      |              | MD5: D434AC3F132B538B6CB37868CB0A7910   | SHA256: 64068F00FB106029D807BCD37CD9F5102DE442BD4FE3520AF3FF616A45A99899 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\moz-extension+++5851050a-91b8-4af2-8e73-aa77522a1aee*userContextId=4294967295\idb\3647222921wleabcEoxlt-eengsairo.sqlite-shm |  | binary     |
|      |              | MD5: B7C14EC6110FA820CA6B65FAEC85911  | SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B854938EB  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF1595e1.TMP  |  | binary     |
|      |              | MD5: 3B4F6A134652F65F9D64721C63771B02   | SHA256: D9BC51759106B078EF9E8D4D9ED3A3C470429183EACDBE6BB559CC64FB858E0  |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-wal   |  | sqlite-wal |
|      |              | MD5: 0CEFD0A569CA50E00FB85F5987BF0465   | SHA256: D90AD9719B1E9B57964213622C038274D825D3394A739D245EA39E9394023780 |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite   |  | binary     |
|      |              | MD5: 391FA7DCD5DF3F07D4BD42397ABA3D9F   | SHA256: 18FA18B374F3B77471C5115CB7827209C18894609BD1055FACD4BA9986C514DE |            |
| 6596 | firefox.exe  | C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite   |  | binary     |
|      |              | MD5: F8D9E13C59BB94FA0F0A881AA3F2EC40   | SHA256: E1C84814C8DA68EDCB96919FB8AF360110E7F0BBB137E9B2F06AD72C90FFBD1B |            |

## Network activity

|                  |                     |              |         |
|------------------|---------------------|--------------|---------|
| HTTP(S) requests | TCP/UDP connections | DNS requests | Threats |
| 31               | 99                  | 161          | 19      |

### HTTP requests

| PID  | Process       | Method | HTTP Code | IP                | URL  | CN      | Type | Size | Reputation  |
|------|---------------|--------|-----------|-------------------|--|---------|------|------|-------------|
| 6596 | firefox.exe   | GET    | 200       | 34.107.221.82:80  | http://detectportal.firefox.com/canonical.html   | unknown | —    | —    | whitelisted |
| 6596 | firefox.exe   | GET    | 200       | 34.107.221.82:80  | http://detectportal.firefox.com/success.txt?ipv4   | unknown | —    | —    | whitelisted |
| 6596 | firefox.exe   | POST   | 200       | 172.64.149.23:80  | http://ocsp.sectigo.com/   | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.69:80   | http://r11.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.69:80   | http://r11.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 142.250.186.67:80 | http://o.pki.goog/wr2  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.81:80   | http://r10.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.81:80   | http://r10.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 142.250.186.67:80 | http://o.pki.goog/wr2  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.81:80   | http://r10.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.69:80   | http://r11.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.74:80   | http://r11.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 172.64.149.23:80  | http://ocsp.sectigo.com/   | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 192.229.221.95:80 | http://ocsp.digicert.com/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 192.229.221.95:80 | http://ocsp.digicert.com/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.81:80   | http://r10.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 184.24.77.81:80   | http://r10.o.lencr.org/  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 142.250.186.67:80 | http://o.pki.goog/wr2  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | POST   | 200       | 142.250.186.67:80 | http://o.pki.goog/wr2  | unknown | —    | —    | —           |
| 6596 | firefox.exe   | GET    | 200       | 23.35.229.160:80  | http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl  | unknown | —    | —    | whitelisted |
| 2268 | svchost.exe   | GET    | 200       | 192.229.221.95:80 | http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGuABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPIGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D | unknown | —    | —    | whitelisted |
| 7816 | SIHClient.exe | GET    | 200       | 23.35.229.160:80  | http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl                                      | unknown | —    | —    | whitelisted |
| 7816 | SIHClient.exe | GET    | 200       | 23.35.229.160:80  | http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20   | unknown | —    | —    | whitelisted |

|      |             |      |     |                   |   |         |   |   |                              |
|------|-------------|------|-----|-------------------|---|---------|---|---|------------------------------|
| 6596 | firefox.exe | POST | 200 | 184.24.77.69:80   | http://r11.o.lencr.org/<br>lIndata%20Secure%20Server%20CA%202.1.crl                         | unknown | — | — | —                            |
| 6596 | firefox.exe | POST | 200 | 192.229.221.95:80 | http://ocsp.digicert.com/   | unknown | — | — | —                            |
| 6596 | firefox.exe | POST | 200 | 184.24.77.81:80   | http://r10.o.lencr.org/   | unknown | — | — | —                            |
| 6596 | firefox.exe | POST | 200 | 184.24.77.74:80   | http://r11.o.lencr.org/   | unknown | — | — | —                            |
| 6596 | firefox.exe | POST | 200 | 184.24.77.81:80   | http://r10.o.lencr.org/   | unknown | — | — | —                            |
| 6596 | firefox.exe | GET  | 200 | 23.53.40.162:80   | http://ciscobinary.openh264.org/openh264-win64-31c4d2e4a037526fd30d4e5c39f60885986cf865.zip | unknown | — | — | <button>whitelisted</button> |
| 6596 | firefox.exe | GET  | 200 | 34.107.221.82:80  | http://detectportal.firefox.com/canonical.html  | unknown | — | — | <button>whitelisted</button> |
| 6596 | firefox.exe | GET  | 200 | 34.107.221.82:80  | http://detectportal.firefox.com/success.txt?ipv4  | unknown | — | — | <button>whitelisted</button> |

Connections

| PID  | Process             | IP                  | Domain   | ASN                         | CN | Reputation                   |
|------|---------------------|---------------------|--|-----------------------------|----|------------------------------|
| 1920 | svchost.exe         | 40.127.240.158:443  | settings-win.data.microsoft.com                | MICROSOFT-CORP-MSN-AS-BLOCK | IE | <button>unknown</button>     |
| 1048 | RUXIMICS.exe        | 40.127.240.158:443  | settings-win.data.microsoft.com                | MICROSOFT-CORP-MSN-AS-BLOCK | IE | <button>unknown</button>     |
| 2120 | MoUsocoreWorker.exe | 40.127.240.158:443  | settings-win.data.microsoft.com                | MICROSOFT-CORP-MSN-AS-BLOCK | IE | <button>unknown</button>     |
| 4    | System              | 192.168.100.255:138 | —  | —                           | —  | <button>whitelisted</button> |
| 6596 | firefox.exe         | 140.82.121.3:443    | github.com                                     | GITHUB                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 34.107.221.82:80    | detectportal.firefox.com                       | GOOGLE                      | US | <button>whitelisted</button> |
| 6596 | firefox.exe         | 34.117.188.166:443  | contile.services.mozilla.com                   | GOOGLE-CLOUD-PLATFORM       | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 172.64.149.23:80    | ocsp.sectigo.com                               | CLOUDFLARENET               | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 184.24.77.69:80     | r11.o.lencr.org                                | Akamai International B.V.   | DE | <button>unknown</button>     |
| 6596 | firefox.exe         | 142.250.186.138:443 | safebrowsing.googleapis.com                    | —                           | —  | <button>whitelisted</button> |
| 6596 | firefox.exe         | 34.107.243.93:443   | push.services.mozilla.com                      | GOOGLE                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 184.24.77.74:80     | r11.o.lencr.org                                | Akamai International B.V.   | DE | <button>unknown</button>     |
| 6596 | firefox.exe         | 142.250.186.67:80   | o.pki.goog                                     | GOOGLE                      | US | <button>whitelisted</button> |
| 6596 | firefox.exe         | 34.160.144.191:443  | content-signature-2.cdn.mozilla.net            | GOOGLE                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 184.24.77.81:80     | r10.o.lencr.org                                | Akamai International B.V.   | DE | <button>unknown</button>     |
| 6596 | firefox.exe         | 34.149.100.209:443  | firefox.settings.services.mozilla.com          | GOOGLE                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 185.199.109.154:443 | github.githubassets.com                        | FASTLY                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 185.199.108.133:443 | avatars.githubusercontent.com                  | FASTLY                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 34.36.165.17:443    | tiles-cdn.prod.ads.prod.webservices.mozgcp.net | GOOGLE-CLOUD-PLATFORM       | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 140.82.114.21:443   | collector.github.com                           | GITHUB                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 140.82.121.6:443    | api.github.com                                 | GITHUB                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 192.229.221.95:80   | ocsp.digicert.com                              | EDGECAST                    | US | <button>whitelisted</button> |
| 1920 | svchost.exe         | 51.124.78.146:443   | settings-win.data.microsoft.com                | MICROSOFT-CORP-MSN-AS-BLOCK | NL | <button>whitelisted</button> |
| 3260 | svchost.exe         | 40.115.3.253:443    | client.wns.windows.com                         | MICROSOFT-CORP-MSN-AS-BLOCK | NL | <button>whitelisted</button> |
| 6596 | firefox.exe         | 54.71.162.254:443   | shavar.services.mozilla.com                    | AMAZON-02                   | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 34.120.158.37:443   | tracking-protection.cdn.mozilla.net            | GOOGLE-CLOUD-PLATFORM       | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 185.199.110.133:443 | avatars.githubusercontent.com                  | FASTLY                      | US | <button>unknown</button>     |
| 6596 | firefox.exe         | 142.250.74.206:443  | sb-ssl.google.com                              | GOOGLE                      | US | <button>whitelisted</button> |
| 6596 | firefox.exe         | 23.35.229.160:80    | www.microsoft.com                              | AKAMAI-AS                   | DE | <button>whitelisted</button> |
| 2268 | svchost.exe         | 20.190.159.0:443    | login.live.com                                 | MICROSOFT-CORP-MSN-AS-BLOCK | IE | <button>unknown</button>     |
| 2268 | svchost.exe         | 192.229.221.95:80   | ocsp.digicert.com                              | EDGECAST                    | US | <button>whitelisted</button> |
| 7816 | SIHClient.exe       | 40.127.169.103:443  | slscr.update.microsoft.com                     | MICROSOFT-CORP-MSN-AS-BLOCK | IE | <button>unknown</button>     |
| 7816 | SIHClient.exe       | 23.35.229.160:80    | www.microsoft.com                              | AKAMAI-AS                   | DE | <button>whitelisted</button> |

|      |                 |                      |  |                             |    |             |
|------|-----------------|----------------------|--|-----------------------------|----|-------------|
| 7816 | SIHClient.exe   | 20.166.126.56:443    | fe3cr.delivery.mp.microsoft.com              | MICROSOFT-CORP-MSN-AS-BLOCK | IE | unknown     |
| 6596 | firefox.exe     | 35.201.103.21:443    | normandy.cdn.mozilla.net                     | GOOGLE                      | US | unknown     |
| 6596 | firefox.exe     | 35.244.181.201:443   | star-mini.c10r.facebook.com                  | GOOGLE                      | US | unknown     |
| 6596 | firefox.exe     | 35.190.72.216:443    | location.services.mozilla.com                | GOOGLE                      | US | unknown     |
| 6596 | firefox.exe     | 34.98.75.36:443      | classify-client.services.mozilla.com         | GOOGLE                      | US | unknown     |
| 6596 | firefox.exe     | 34.117.121.53:443    | firefox-settings-attachments.cdn.mozilla.net | GOOGLE-CLOUD-PLATFORM       | US | unknown     |
| 7492 | Jvczfhe.exe     | 185.199.110.133:443  | avatars.githubusercontent.com                | FASTLY                      | US | unknown     |
| 3888 | svchost.exe     | 239.255.255.250:1900 | —  | —                           | —  | whitelisted |
| 6596 | firefox.exe     | 23.53.40.162:80      | ciscobinary.openh264.org                     | Akamai International B.V.   | DE | unknown     |
| 5152 | InstallUtil.exe | 91.92.253.47:7702    | egehgdhjbhjtire.duckdns.org                  | —                           | BG | unknown     |
| 1356 | WerFault.exe    | 104.208.16.94:443    | watson.events.data.microsoft.com             | MICROSOFT-CORP-MSN-AS-BLOCK | US | unknown     |
| 6596 | firefox.exe     | 140.82.112.21:443    | collector.github.com                         | GITHUB                      | US | unknown     |
| 7824 | Muadnrd.exe     | 185.199.110.133:443  | avatars.githubusercontent.com                | FASTLY                      | US | unknown     |
| 7584 | WerFault.exe    | 20.42.65.92:443      | watson.events.data.microsoft.com             | MICROSOFT-CORP-MSN-AS-BLOCK | US | unknown     |

DNS requests

| Domain                                     | IP  | Reputation  |
|--|---|-------------|
| settings-win.data.microsoft.com            | 40.127.240.158<br>51.124.78.146   | whitelisted |
| google.com                                 | 142.250.185.238   | whitelisted |
| github.com                                 | 140.82.121.3  | shared      |
| detectportal.firefox.com                   | 34.107.221.82   | whitelisted |
| prod.detectportal.prod.cloudops.mozgcp.net | 34.107.221.82<br>2600:1901:0:38d7::   | whitelisted |
| example.org                                | 93.184.215.14   | whitelisted |
| ipv4only.arpa                              | 192.0.0.170<br>192.0.0.171  | whitelisted |
| contile.services.mozilla.com               | 34.117.188.166  | whitelisted |
| spocs.getpocket.com                        | 34.117.188.166  | whitelisted |
| prod.ads.prod.webservices.mozgcp.net       | 34.117.188.166  | unknown     |
| ocsp.sectigo.com                           | 172.64.149.23<br>104.18.38.233  | whitelisted |
| r11.o.lencr.org                            | 184.24.77.69<br>184.24.77.61<br>184.24.77.75<br>184.24.77.65<br>184.24.77.71<br>184.24.77.48<br>184.24.77.45<br>184.24.77.74<br>184.24.77.76<br>184.24.77.56  | whitelisted |
| ocsp.comodoca.com.cdn.cloudflare.net       | 172.64.149.23<br>104.18.38.233<br>2606:4700:4400::ac40:9517<br>2606:4700:4400::6812:26e9  | whitelisted |
| a1887.dscq.akamai.net                      | 184.24.77.69<br>184.24.77.61<br>184.24.77.75<br>184.24.77.65<br>184.24.77.71<br>184.24.77.48<br>184.24.77.45<br>184.24.77.74<br>2a02:26f0:3500:e::1732:8355<br>2a02:26f0:3500:e::1732:8352<br>2a02:26f0:3500:e::1732:8344<br>184.24.77.76<br>184.24.77.56 | whitelisted |

|   |   |             |
|---|---|-------------|
|   | 2a02:26f0:3500:e::1732:8348<br>2a02:26f0:3500:e::1732:835b  |             |
| content-signature-2.cdn.mozilla.net                       | 34.160.144.191  | whitelisted |
| prod.content-signature-chains.prod.webservices.mozgcp.net | 34.160.144.191<br>2600:1901:0:92a9::  | whitelisted |
| push.services.mozilla.com                                 | 34.107.243.93   | whitelisted |
| safebrowsing.googleapis.com                               | 142.250.186.138<br>2a00:1450:4001:806::200a   | whitelisted |
| r10.o.lencr.org   | 184.24.77.81<br>184.24.77.69<br>184.24.77.56<br>184.24.77.79<br>184.24.77.71<br>184.24.77.75<br>184.24.77.48<br>184.24.77.67  | whitelisted |
| firefox.settings.services.mozilla.com                     | 34.149.100.209  | whitelisted |
| prod.remote-settings.prod.webservices.mozgcp.net          | 34.149.100.209  | whitelisted |
| o.pki.goog  | 142.250.186.67  | whitelisted |
| pki-goog.l.google.com                                     | 142.250.186.67<br>2a00:1450:4001:828::2003  | whitelisted |
| github.githubassets.com                                   | 185.199.109.154<br>185.199.108.154<br>185.199.111.154<br>185.199.110.154  | whitelisted |
| avatars.githubusercontent.com                             | 185.199.108.133<br>185.199.111.133<br>185.199.109.133<br>185.199.110.133<br>2606:50c0:8000::154<br>2606:50c0:8001::154<br>2606:50c0:8003::154<br>2606:50c0:8002::154  | whitelisted |
| tiles-cdn.prod.ads.prod.webservices.mozgcp.net            | 34.36.165.17<br>2600:1901:0:8e3f::  | unknown     |
| collector.github.com                                      | 140.82.114.21<br>140.82.112.21  | whitelisted |
| glb-db52c2cf8be544.github.com                             | 140.82.114.21<br>140.82.112.21  | whitelisted |
| api.github.com  | 140.82.121.6  | whitelisted |
| ocsp.digicert.com   | 192.229.221.95  | whitelisted |
| fp2e7a.wpc.phicdn.net                                     | 192.229.221.95<br>2606:2800:233:fa02:67b:9ff6:6107:833  | whitelisted |
| www.amazon.de   | 52.222.239.71   | whitelisted |
| www.youtube.com   | 172.217.16.206<br>142.250.186.142<br>142.250.184.206<br>216.58.206.78<br>172.217.23.110<br>142.250.186.174<br>172.217.18.14<br>142.250.185.174<br>142.250.186.46<br>216.58.206.46<br>142.250.185.110<br>142.250.185.142<br>142.250.185.78<br>172.217.18.110<br>142.250.184.238<br>142.250.186.110 | whitelisted |
| www.facebook.com  | 157.240.252.35  | whitelisted |
| partnerprogramm.otto.de                                   | 54.37.171.144   | whitelisted |
| www.ebay.de   | 23.206.209.88<br>2.16.97.102  | whitelisted |
| www.wikipedia.org   | 185.15.59.224   | whitelisted |
| www.reddit.com  | 151.101.65.140<br>151.101.1.140   | whitelisted |

|                                     |  |             |
|-------------------------------------|--|-------------|
|                                     | 151.101.129.140<br>151.101.193.140   |             |
| star-mini.c10r.facebook.com         | 157.240.252.35<br>35.244.181.201<br>2a03:2880:f177:83:face:b00c:0:25de   | whitelisted |
| dyna.wikimedia.org                  | 185.15.59.224<br>2a02:ec80:300:ed1a::1   | whitelisted |
| reddit.map.fastly.net               | 151.101.65.140<br>151.101.1.140<br>151.101.129.140<br>151.101.193.140  | whitelisted |
| e11847.a.akamaiedge.net             | 23.206.209.88<br>2.16.97.102   | whitelisted |
| djvbdz1obemzo.cloudfront.net        | 52.222.239.71<br>2600:9000:223e:7e00:e:13a1:b914:2321<br>2600:9000:223e:ae00:e:13a1:b914:2321<br>2600:9000:223e:5400:e:13a1:b914:2321<br>2600:9000:223e:4000:e:13a1:b914:2321<br>2600:9000:223e:6c00:e:13a1:b914:2321<br>2600:9000:223e:f800:e:13a1:b914:2321<br>2600:9000:223e:1400:e:13a1:b914:2321<br>2600:9000:223e:c000:e:13a1:b914:2321<br>2600:9000:223e:a200:e:13a1:b914:2321<br>2600:9000:223e:c200:e:13a1:b914:2321<br>2600:9000:223e:8c00:e:13a1:b914:2321<br>2600:9000:223e:9200:e:13a1:b914:2321<br>2600:9000:223e:9800:e:13a1:b914:2321<br>2600:9000:223e:3a00:e:13a1:b914:2321<br>2600:9000:223e:c00:e:13a1:b914:2321<br>2600:9000:223e:e000:e:13a1:b914:2321 | whitelisted |
| youtube-ui.l.google.com             | 172.217.16.206<br>142.250.186.142<br>142.250.184.206<br>216.58.206.78<br>172.217.23.110<br>142.250.186.174<br>172.217.18.14<br>142.250.185.174<br>142.250.186.46<br>216.58.206.46<br>142.250.185.110<br>142.250.185.142<br>142.250.185.78<br>172.217.18.110<br>142.250.184.238<br>142.250.186.110<br>2a00:1450:4001:827::200e<br>2a00:1450:4001:81d::200e<br>2a00:1450:4001:80b::200e<br>2a00:1450:4001:829::200e  | whitelisted |
| client.wns.windows.com              | 40.115.3.253   | whitelisted |
| shavar.services.mozilla.com         | 54.71.162.254<br>44.226.249.47<br>44.239.24.213  | whitelisted |
| shavar.prod.mozaws.net              | 54.71.162.254<br>44.226.249.47<br>44.239.24.213  | whitelisted |
| tracking-protection.cdn.mozilla.net | 34.120.158.37  | whitelisted |
| tracking-protection.prod.mozaws.net | 34.120.158.37  | whitelisted |
| raw.githubusercontent.com           | 185.199.110.133<br>185.199.109.133<br>185.199.108.133<br>185.199.111.133<br>2606:50c0:8002::154<br>2606:50c0:8003::154<br>2606:50c0:8001::154<br>2606:50c0:8000::154   | shared      |
| sb-ssl.google.com                   | 142.250.74.206   | whitelisted |
| sb-ssl.l.google.com                 | 142.250.74.206<br>2a00:1450:4001:803::200e   | whitelisted |
| www.microsoft.com                   | 23.35.229.160  | whitelisted |
| login.live.com                      | 20.190.159.0<br>20.190.159.2<br>20.190.159.23  | whitelisted |

|  |  |             |
|--|--|-------------|
|  | 40.126.31.73<br>20.190.159.71<br>40.126.31.69<br>20.190.159.68<br>20.190.159.75        |             |
| slscr.update.microsoft.com                                   | 40.127.169.103   | whitelisted |
| fe3cr.delivery.mp.microsoft.com                              | 20.166.126.56  | whitelisted |
| normandy.cdn.mozilla.net                                     | 35.201.103.21  | whitelisted |
| normandy-cdn.services.mozilla.com                            | 35.201.103.21  | whitelisted |
| aus5.mozilla.org   | 35.244.181.201   | whitelisted |
| prod.balrog.prod.cloudops.mozgcp.net                         | 35.244.181.201   | whitelisted |
| location.services.mozilla.com                                | 35.190.72.216  | whitelisted |
| prod.classify-client.prod.webservices.mozgcp.net             | 35.190.72.216  | unknown     |
| classify-client.services.mozilla.com                         | 34.98.75.36  | whitelisted |
| prod-classifyclient.normandy.prod.cloudops.mozgcp.net        | 34.98.75.36  | whitelisted |
| firefox-settings-attachments.cdn.mozilla.net                 | 34.117.121.53  | whitelisted |
| attachments.prod.remote-settings.prod.webservices.mozgcp.net | 34.117.121.53  | whitelisted |
| nexusrules.officeapps.live.com                               | 52.111.227.11  | whitelisted |
| ciscobinary.openh264.org                                     | 23.53.40.162<br>23.53.40.129   | whitelisted |
| a19.dscg10.akamai.net  | 23.53.40.162<br>23.53.40.129<br>2a02:26f0:3100::1735:2881<br>2a02:26f0:3100::1735:28a2 | whitelisted |
| egehgdehjbhtre.duckdns.org                                   | 91.92.253.47   | unknown     |
| watson.events.data.microsoft.com                             | 104.208.16.94<br>20.42.65.92   | whitelisted |
| dns.msftncsi.com   | 131.107.255.255  | whitelisted |

Threats

| PID | Process | Class                              | Message  |
|-----|---------|------------------------------------|--|
| —   | —       | Not Suspicious Traffic             | INFO [ANY.RUN] Attempting to access raw user content on GitHub |
| —   | —       | Not Suspicious Traffic             | INFO [ANY.RUN] Attempting to access raw user content on GitHub |
| —   | —       | Not Suspicious Traffic             | INFO [ANY.RUN] Attempting to access raw user content on GitHub |
| —   | —       | Traffico potenzialmente pericoloso | Query ET INFO DYNAMIC_DNS a un dominio *.duckdns .org          |
| —   | —       | Traffico potenzialmente pericoloso | Query ET INFO DYNAMIC_DNS a un dominio *.duckdns .org          |
| —   | —       | Traffico potenzialmente pericoloso | Query ET INFO DYNAMIC_DNS a un dominio *.duckdns .org          |
| —   | —       | Attività varie                     | ET INFO DYNAMIC_DNS Query al dominio *.duckdns.                |
| —   | —       | Attività varie                     | ET INFO DYNAMIC_DNS Query al dominio *.duckdns.                |
| —   | —       | Attività varie                     | ET INFO DYNAMIC_DNS Query al dominio *.duckdns.                |
| —   | —       | Traffico potenzialmente pericoloso | Query ET INFO DYNAMIC_DNS a un dominio *.duckdns .org          |
| —   | —       | Misc activity                      | ET INFO DYNAMIC_DNS Query to *.duckdns. Domain                 |
| —   | —       | Potentially Bad Traffic            | ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain           |
| —   | —       | Potentially Bad Traffic            | ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain           |
| —   | —       | Misc activity                      | ET INFO DYNAMIC_DNS Query to *.duckdns. Domain                 |
| —   | —       | Misc activity                      | ET INFO DYNAMIC_DNS Query to *.duckdns. Domain                 |
| —   | —       | Potentially Bad Traffic            | ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain           |
| —   | —       | Misc activity                      | ET INFO DYNAMIC_DNS Query to *.duckdns. Domain                 |
| —   | —       | Potentially Bad Traffic            | ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain           |
| —   | —       | Misc activity                      | ET INFO DYNAMIC_DNS Query to *.duckdns. Domain                 |

## Stringhe di output di debug

---

Nessuna informazione di debug



Servizio interattivo di ricerca malware ANY.RUN

© 2017-2025 ANY.RUN LLC. TUTTI I DIRITTI RISERVATI