ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL: https://crypto-whales.io

Full analysis: https://app.any.run/tasks/934be0c2-66d4-46ec-b001-0e294ab80341

Verdict: Malicious activity

Threats:

Loader

A loader is malicious software that infiltrates devices to deliver malicious payloads. This malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans or stealers. Criminals usually deliver loaders through phishing emails and links by relying on social engineering to trick users into downloading and running their executables. Loaders employ advanced evasion and persistence tactics to avoid detection.

Lumma

Lumma is an information stealer, developed using the C programming language. It is offered for sale as a malware-as-a-service, with several plans available. It usually targets cryptocurrency wallets, login credentials, and other sensitive information on a compromised system. The malicious software regularly gets updates that improve and expand its functionality, making it a serious stealer threat.

Stealc

Stealc is a stealer malware that targets victims' sensitive data, which it exfiltrates from browsers, messaging apps, and other software. The malware is equipped with advanced features, including fingerprinting, control panel, evasion mechanisms, string obfuscation, etc. Stealc establishes persistence and communicates with its C2 server through HTTP POST requests.

Stealc

Stealc ist eine Stealer-Malware, die es auf die sensiblen Daten der Opfer abgesehen hat, die sie aus Browsern, Messaging-Apps und anderer Software exfiltriert. Die Malware ist mit fortschrittlichen Funktionen ausgestattet, darunter Fingerprinting, Bedienfeld, Umgehungsmechanismen, String-Verschleierung usw. Stealc stellt eine Persistenz her und kommuniziert mit seinem C2-Server über HTTP-POST-Anfragen.

Stealer

Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Analysis date: August 13, 2024 at 15:40:37

OS: Windows 10 Professional (build: 19045, 64 bit)

Tags: loader lumma stealer antivm stealc

Indicators:

MD5: 8FEBEAE3452C5CD2A82DCCD906D85DE2

SHA1: D1437A0BB6AE76C339E0CDDF18083254EC265185

SHA256: DCB0230AD9B0BEF4B0DB4EEA684D35D08F11605937C4B1BD7D1D384472C0F761

SSDEEP: 3:N8KuOYn:2Kon

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	240 seconds	**MITM proxy:**	off	**Privacy:**	Public submission
Fakenet option:	off	**Route via Tor:**	off	**Autoconfirmation of UAC:**	on
Network:	on				

Software preset

- 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)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (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 профессиональный 2019 - ru-ru (16.0.16026.20146)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional 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
- MSPaint FoD Package

- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (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)
- 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)
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Behavior activities

MALICIOUS

Adds path to the Windows Defender exclusion list
- Install_x64.exe (PID: 3904)

LUMMA has been detected (YARA)
- 1.exe (PID: 4772)

Stealers network behavior
- BitLockerToGo.exe (PID: 2476)
- BitLockerToGo.exe (PID: 6280)

Actions looks like stealing of personal data
- BitLockerToGo.exe (PID: 2476)
- BitLockerToGo.exe (PID: 6280)

SUSPICIOUS

Executable content was dropped or overwritten
- Install_x64.exe (PID: 3904)
- BitLockerToGo.exe (PID: 6280)

Process drops legitimate windows executable
- Install_x64.exe (PID: 3904)
- BitLockerToGo.exe (PID: 6280)

The process drops C-runtime libraries
- Install_x64.exe (PID: 3904)
- BitLockerToGo.exe (PID: 6280)

Drops the executable file immediately after the start

INFO

Creates files in the program directory
- Install_x64.exe (PID: 3904)
- BitLockerToGo.exe (PID: 6280)

Checks supported languages
- Install_x64.exe (PID: 3904)
- 1.exe (PID: 4772)
- 2.exe (PID: 5372)
- BitLockerToGo.exe (PID: 2476)
- BitLockerToGo.exe (PID: 6280)
- 3.exe (PID: 1656)

The process uses the downloaded file

LUMMA has been detected (SURICATA)
• BitLockerToGo.exe (PID: 2476)

STEALC has been detected (SURICATA)
• BitLockerToGo.exe (PID: 6280)

Connects to the CnC server
• BitLockerToGo.exe (PID: 6280)

Steals credentials from Web Browsers
• BitLockerToGo.exe (PID: 6280)

• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 6280)

The process creates files with name similar to system file names
• Install_x64.exe (PID: 3904)

Reads security settings of Internet Explorer
• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 6280)

Process requests binary or script from the Internet
• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 6280)

Script adds exclusion path to Windows Defender
• Install_x64.exe (PID: 3904)

Potential Corporate **Privacy** Violation
• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 6280)

Starts POWERSHELL.EXE for commands execution
• Install_x64.exe (PID: 3904)

Searches for installed software
• BitLockerToGo.exe (PID: 2476)
• BitLockerToGo.exe (PID: 6280)

Windows Defender mutex has been found
• BitLockerToGo.exe (PID: 6280)

There is functionality for VM detection (antiVM strings)
• 2.exe (PID: 5372)

The process drops Mozilla's DLL files
• BitLockerToGo.exe (PID: 6280)

Connects to the server without a host name
• BitLockerToGo.exe (PID: 6280)

Contacting a server suspected of hosting an CnC
• BitLockerToGo.exe (PID: 6280)

• chrome.exe (PID: 2360)
• chrome.exe (PID: 6328)

Reads Microsoft Office registry keys
• chrome.exe (PID: 6328)

Executable content was dropped or overwritten
• chrome.exe (PID: 6328)
• chrome.exe (PID: 7124)

Create files in a temporary directory
• Install_x64.exe (PID: 3904)
• 2.exe (PID: 5372)
• 3.exe (PID: 1656)

Application launched itself
• chrome.exe (PID: 6328)

Script raised an exception (POWERSHELL)
• powershell.exe (PID: 7000)

Checks if a key exists in the options dictionary (POWERSHELL)
• powershell.exe (PID: 7000)

Checks proxy server information
• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 6280)

Reads the computer name
• Install_x64.exe (PID: 3904)
• BitLockerToGo.exe (PID: 2476)
• BitLockerToGo.exe (PID: 6280)

Reads the software policy settings
• BitLockerToGo.exe (PID: 2476)

Creates files or folders in the user directory
• BitLockerToGo.exe (PID: 6280)

Reads Environment values
• BitLockerToGo.exe (PID: 6280)

Reads product name
• BitLockerToGo.exe (PID: 6280)

Reads CPU info
• BitLockerToGo.exe (PID: 6280)

Malware configuration

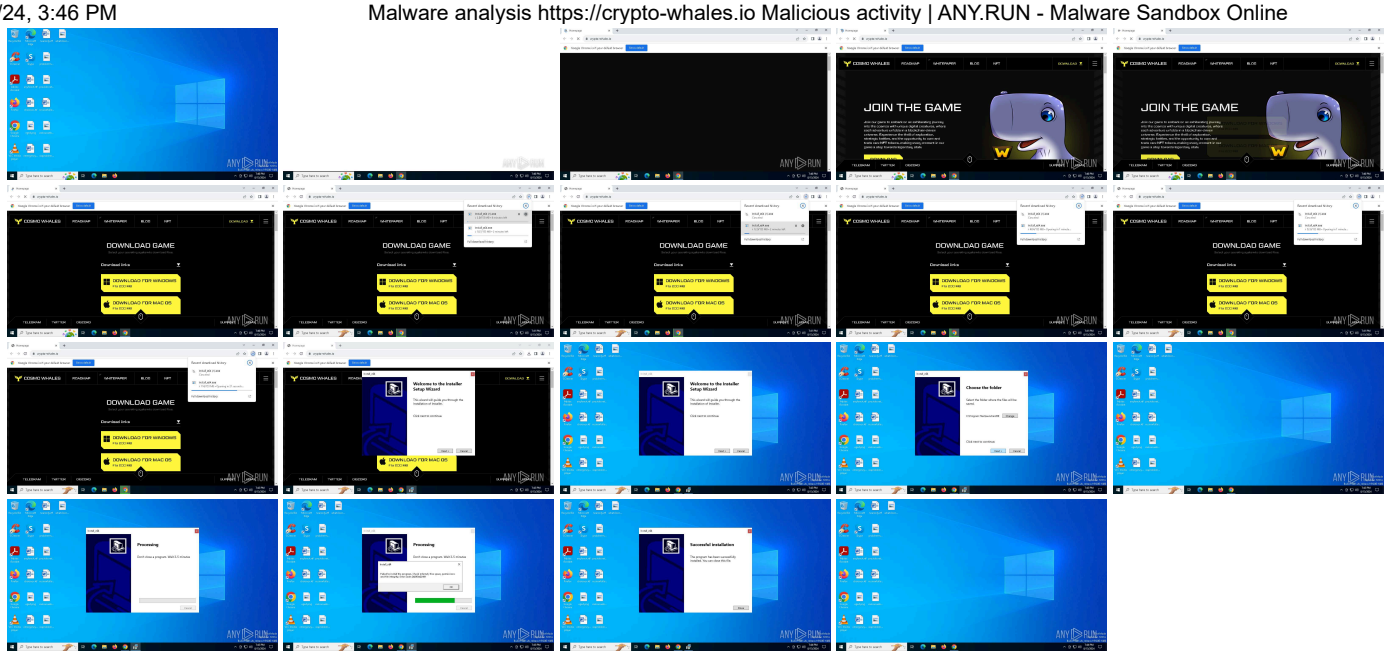
Lumma

(PID) Process	(4772) 1.exe
C2 (9)	deallerospfosu.shop
	writerospzm.shop
	celebratioopz.shop
	mennyudosirso.shop
	complaintsipzzx.shop
	languagedscie.shop
	bassizcellskz.shop
	quialitsuzoxm.shop
	samledwwekspzxp.shop

Static information

No data.

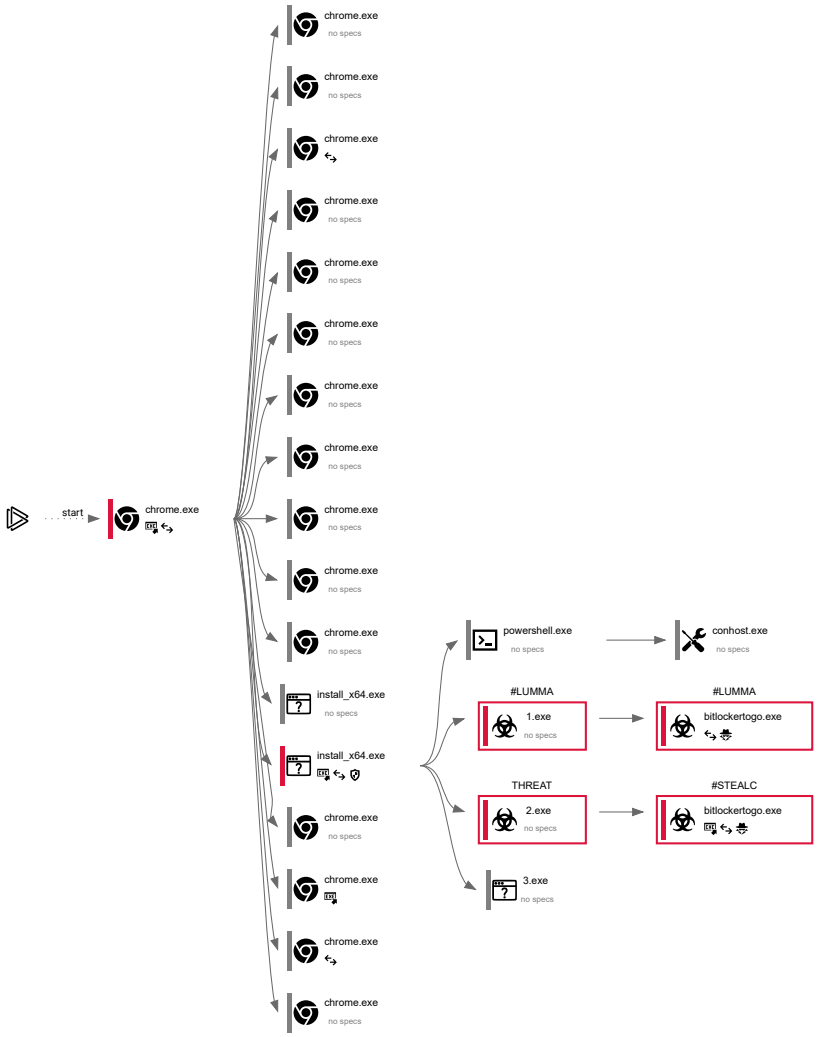
Video and screenshots


JOIN THE GAME
DOWNLOAD GAME
Welcome to the Installer Setup Wizard
Choose the folder
Processing
Successful installation

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
164	25	6	0

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
6328	"C:\Program Files\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --disable-background-networking --	C:\Program Files\Google\Chrome\Application\chrome.exe		explorer.exe

disable-features=OptimizationGuideModelDownloading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://crypto-whales.io"

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	122.0.6261.70		

6456 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=122.0.6261.70 --initial-client-data=0x220,0x224,0x228,0x1fc,0x22c,0x7fffd645dc40,0x7fffd645dc4c,0x7fffd645dc58 — C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	122.0.6261.70		

6588 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgABAMAAAAAAAAAAAAAAAAAABgAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1932 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:2 — C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	122.0.6261.70		

6600 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=1384 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:3 — C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	122.0.6261.70

6620 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=2236 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8 — C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	122.0.6261.70		

6728 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=3032 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1 — C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome

Version: 122.0.6261.70

6756	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=3148 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Version: 122.0.6261.70

6708	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5020 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User: admin **Company:** Google LLC
Integrity Level: MEDIUM **Description:** Google Chrome
Exit code: 0 **Version:** 122.0.6261.70

3188	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5104 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 122.0.6261.70

2536	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5108 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 122.0.6261.70

3864	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5232 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 122.0.6261.70

2360	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5368 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHint	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

s,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	122.0.6261.70

2872 "C:\Users\admin\Downloads\Install_x64.exe" C:\Users\admin\Downloads\Install_x64.exe — chrome.exe

Information

User:	admin	**Company:**	Install_x64
Integrity Level:	MEDIUM	**Description:**	Install_x64
Exit code:	3221226540	**Version:**	1.0.0.0

3904 "C:\Users\admin\Downloads\Install_x64.exe" C:\Users\admin\Downloads\Install_x64.exe chrome.exe

Information

User:	admin	**Company:**	Install_x64
Integrity Level:	HIGH	**Description:**	Install_x64
Exit code:	0	**Version:**	1.0.0.0

7000 "powershell.exe" Add-MpPreference -ExclusionPath 'C:/' C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — Install_x64.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows PowerShell
Exit code:	1	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

3036 \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1 C:\Windows\System32\conhost.exe — powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

6232 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=5140 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.19041.3636 --no-appcompat-clear --gpu-preferences=WAAAAAAAAADoABAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAABEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=4568 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	122.0.6261.70

4772 "C:\Program Files\launcher289\1.exe" C:\Program Files\launcher289\1.exe Install_x64.exe

Information

User:	admin	**Company:**	Vidar Audio
Integrity Level:	HIGH	**Description:**	Vidar Audio RAIDEN 1.0.0
Exit code:	666	**Version:**	1.0.0

Malware configuration Lumma

Lumma

(PID) Process	(4772) 1.exe
C2 (9)	deallerospfosu.shop
	writerospzm.shop
	celebratioopz.shop
	mennyudosirso.shop
	complaintsipzzx.shop

	languagedscie.shop
	bassizcellskz.shop
	quialitsuzoxm.shop
	samledwwekspzxp.shop

7124	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5368 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe		chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	122.0.6261.70

5372	"C:\Program Files\launcher289\2.exe"	C:\Program Files\launcher289\2.exe		Install_x64.exe

Information

User:	admin	**Company:**	NCH Software
Integrity Level:	HIGH	**Description:**	Express Burn Disc Burning Software
Exit code:	666	**Version:**	12.00+

2476	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe		1.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	BitLocker To Go Reader
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7112	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5668 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:3	C:\Program Files\Google\Chrome\Application\chrome.exe		chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	122.0.6261.70		

7004	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=5372 --field-trial-handle=1936,i,8163975433772719385,13751584378607153761, 262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	122.0.6261.70

6280	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe	C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe		2.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	BitLocker To Go Reader
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

1656	"C:\Program Files\launcher289\3.exe"	C:\Program Files\launcher289\3.exe	—	Install_x64.exe

Information

User:	admin	**Company:**	Ashampoo GmbH & Co. KG
Integrity Level:	HIGH	**Description:**	Ashampoo Music Studio 2023 Setup

Version: 1.10.0

Registry activity

Total events	Read events	Write events	Delete events
26 472	26 161	305	6

Modification events

(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operation:	write	**Name:**	failed_count
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	2		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:			
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:	01000000		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	1		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	dr
Value:	1		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\StabilityMetrics
Operation:	write	**Name:**	user_experience_metrics.stability.exited_cleanly
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome
Operation:	write	**Name:**	UsageStatsInSample
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
Operation:	write	**Name:**	usagestats
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	metricsid
Value:			
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	metricsid_installdate
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	metricsid_enableddate
Value:	0		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	lastrun
Value:	13368051646140425		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation:	write	**Name:**	C1I
Value:	1		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation:	write	**Name:**	C2I
Value:	1		
(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C

Operation: write **Name:** C7I
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: write **Name:** C1S
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: write **Name:** C7S
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\PTimes
Operation: write **Name:** C
Value: A8DF8DE6B8EDDA01

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\RLZs
Operation: write **Name:** C1
Value: 1C1GCEB_enDE1123DE1123

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\RLZs
Operation: write **Name:** C2
Value: 1C2GCEB_enDE1123

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\RLZs
Operation: write **Name:** C7
Value: 1C7GCEB_enDE1123

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C1F
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C1I
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C2I
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C7I
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C1S
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\Events\C
Operation: delete value **Name:** C7S
Value:

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\StatefulEvents\C
Operation: write **Name:** C1F
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\StatefulEvents\C
Operation: write **Name:** C1I
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\StatefulEvents\C
Operation: write **Name:** C2I
Value: 1

(PID) Process: (6328) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Common\Rlz\StatefulEvents\C
Operation: write **Name:** C7I
Value: 1

(PID) Process: (2360) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2360) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process:	(2360) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	UNCAsIntranet
Value:	1		

(PID) Process:	(2360) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value:	0		

(PID) Process:	(2360) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories64\{56FFCC30-D398-11D0-B2AE-00A0C908FA49}\Enum
Operation:	write	**Name:**	Implementing
Value:	1C00000001000000E807080002000D0013002A001A00D101010000001E768127E028094199FEB9D127C57AFE		

(PID) Process:	(2360) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
Operation:	write	**Name:**	{2781761E-28E0-4109-99FE-B9D127C57AFE} {56FFCC30-D398-11D0-B2AE-00A0C908FA49} 0xFFFF
Value:	0100000000000000006315DFECB8EDDA01		

(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	ProxyBypass
Value:	1		

(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	IntranetName
Value:	1		

(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	UNCAsIntranet
Value:	1		

(PID) Process:	(6328) chrome.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value:	0		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-462
Value:	Afghanistan Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-461
Value:	Afghanistan Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-222
Value:	Alaskan Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-221
Value:	Alaskan Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2392
Value:	Aleutian Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2391
Value:	Aleutian Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2162
Value:	Altai Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2161
Value:	Altai Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-392
Value:	Arab Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-391
Value:	Arab Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-442

Value: Arabian Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-441
Value: Arabian Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-402
Value: Arabic Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-401
Value: Arabic Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-842
Value: Argentina Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-841
Value: Argentina Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2182
Value: Astrakhan Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2181
Value: Astrakhan Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-82
Value: Atlantic Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-81
Value: Atlantic Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-652
Value: AUS Central Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-651
Value: AUS Central Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2492
Value: Aus Central W. Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2491
Value: Aus Central W. Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-672
Value: AUS Eastern Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-671
Value: AUS Eastern Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-449
Value: Azerbaijan Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-448
Value: Azerbaijan Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-12
Value: Azores Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E

Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-11
Value: Azores Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1662
Value: Bahia Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1661
Value: Bahia Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1022
Value: Bangladesh Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1021
Value: Bangladesh Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1972
Value: Belarus Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1971
Value: Belarus Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2612
Value: Bougainville Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2611
Value: Bougainville Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-142
Value: Canada Central Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-141
Value: Canada Central Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2002
Value: Cabo Verde Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2001
Value: Cabo Verde Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-452
Value: Caucasus Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-451
Value: Caucasus Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-662
Value: Cen. Australia Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-661
Value: Cen. Australia Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-152
Value: Central America Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-151
Value: Central America Daylight Time

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-512
Value:	Central Asia Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-511
Value:	Central Asia Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-105
Value:	Central Brazilian Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-104
Value:	Central Brazilian Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-282
Value:	Central Europe Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-281
Value:	Central Europe Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-292
Value:	Central European Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-291
Value:	Central European Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-722
Value:	Central Pacific Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-721
Value:	Central Pacific Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-162
Value:	Central Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-161
Value:	Central Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-172
Value:	Central Standard Time (Mexico)		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-171
Value:	Central Daylight Time (Mexico)		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2532
Value:	Chatham Islands Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2531
Value:	Chatham Islands Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-572
Value:	China Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-571
Value:	China Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2432

Value: Cuba Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2431
Value: Cuba Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-252
Value: Dateline Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-251
Value: Dateline Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-412
Value: E. Africa Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-411
Value: E. Africa Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-682
Value: E. Australia Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-681
Value: E. Australia Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-332
Value: E. Europe Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-331
Value: E. Europe Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-42
Value: E. South America Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-41
Value: E. South America Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2372
Value: Easter Island Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2371
Value: Easter Island Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-112
Value: Eastern Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-111
Value: Eastern Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2042
Value: Eastern Standard Time (Mexico)

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2041
Value: Eastern Daylight Time (Mexico)

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-342
Value: Egypt Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E

Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-341
Value: Egypt Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1842
Value: Russia TZ 4 Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1841
Value: Russia TZ 4 Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-732
Value: Fiji Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-731
Value: Fiji Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-352
Value: FLE Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-351
Value: FLE Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-435
Value: Georgian Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-434
Value: Georgian Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-262
Value: GMT Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-261
Value: GMT Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-52
Value: Greenland Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-51
Value: Greenland Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-272
Value: Greenwich Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-271
Value: Greenwich Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-362
Value: GTB Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-361
Value: GTB Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2342
Value: Haiti Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2341
Value: Haiti Daylight Time

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-232
Value:	Hawaiian Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-231
Value:	Hawaiian Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-492
Value:	India Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-491
Value:	India Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-432
Value:	Iran Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-431
Value:	Iran Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-372
Value:	Jerusalem Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-371
Value:	Jerusalem Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-335
Value:	Jordan Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-334
Value:	Jordan Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1822
Value:	Russia TZ 1 Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1821
Value:	Russia TZ 1 Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-982
Value:	Kamchatka Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-981
Value:	Kamchatka Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-622
Value:	Korea Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-621
Value:	Korea Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1722
Value:	Libya Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1721
Value:	Libya Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1802

Value: Line Islands Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1801
Value: Line Islands Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2512
Value: Lord Howe Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2511
Value: Lord Howe Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1472
Value: Magadan Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1471
Value: Magadan Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2872
Value: Magallanes Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2871
Value: Magallanes Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2412
Value: Marquesas Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2411
Value: Marquesas Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-912
Value: Mauritius Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-911
Value: Mauritius Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-32
Value: Mid-Atlantic Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-31
Value: Mid-Atlantic Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-365
Value: Middle East Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-364
Value: Middle East Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-772
Value: Montevideo Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-771
Value: Montevideo Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-892
Value: Morocco Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E

Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-891
Value: Morocco Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-192
Value: Mountain Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-191
Value: Mountain Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-182
Value: Mountain Standard Time (Mexico)

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-181
Value: Mountain Daylight Time (Mexico)

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-542
Value: Myanmar Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-541
Value: Myanmar Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2792
Value: Novosibirsk Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2791
Value: Novosibirsk Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-385
Value: Namibia Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-384
Value: Namibia Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-502
Value: Nepal Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-501
Value: Nepal Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-742
Value: New Zealand Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-741
Value: New Zealand Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-72
Value: Newfoundland Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-71
Value: Newfoundland Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2632
Value: Norfolk Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2631
Value: Norfolk Daylight Time

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1872
Value:	Russia TZ 7 Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1871
Value:	Russia TZ 7 Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1862
Value:	Russia TZ 6 Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1861
Value:	Russia TZ 6 Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2062
Value:	North Korea Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2061
Value:	North Korea Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2772
Value:	Omsk Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2771
Value:	Omsk Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-92
Value:	Pacific SA Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-91
Value:	Pacific SA Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-212
Value:	Pacific Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-211
Value:	Pacific Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-215
Value:	Pacific Standard Time (Mexico)		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-214
Value:	Pacific Daylight Time (Mexico)		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-872
Value:	Pakistan Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-871
Value:	Pakistan Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-962
Value:	Paraguay Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-961
Value:	Paraguay Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-3052

Value: Qyzylorda Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-3051
Value: Qyzylorda Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-302
Value: Romance Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-301
Value: Romance Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1912
Value: Russia TZ 10 Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1911
Value: Russia TZ 10 Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1932
Value: Russia TZ 11 Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1931
Value: Russia TZ 11 Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1892
Value: Russia TZ 3 Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1891
Value: Russia TZ 3 Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1832
Value: Russia TZ 2 Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1831
Value: Russia TZ 2 Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-832
Value: SA Eastern Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-831
Value: SA Eastern Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-122
Value: SA Pacific Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-121
Value: SA Pacific Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-792
Value: SA Western Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-791
Value: SA Western Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2452
Value: Saint Pierre Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E

Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2451
Value: Saint Pierre Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2322
Value: Sakhalin Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2321
Value: Sakhalin Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-242
Value: Samoa Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-241
Value: Samoa Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2942
Value: Sao Tome Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2941
Value: Sao Tome Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2842
Value: Saratov Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2841
Value: Saratov Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-562
Value: SE Asia Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-561
Value: SE Asia Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-592
Value: Malay Peninsula Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-591
Value: Malay Peninsula Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-382
Value: South Africa Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-381
Value: South Africa Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-3142
Value: South Sudan Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-3141
Value: South Sudan Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-532
Value: Sri Lanka Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-531
Value: Sri Lanka Daylight Time

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2892
Value:	Sudan Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2891
Value:	Sudan Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1412
Value:	Syria Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1411
Value:	Syria Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-602
Value:	Taipei Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-601
Value:	Taipei Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-692
Value:	Tasmania Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-691
Value:	Tasmania Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2592
Value:	Tocantins Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2591
Value:	Tocantins Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-632
Value:	Tokyo Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-631
Value:	Tokyo Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2752
Value:	Tomsk Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2751
Value:	Tomsk Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-752
Value:	Tonga Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-751
Value:	Tonga Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2142
Value:	Transbaikal Standard Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-2141
Value:	Transbaikal Daylight Time		

(PID) Process:	(4772) 1.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation:	write	**Name:**	C:\WINDOWS\system32\,@tzres.dll,-1502

Value: Turkey Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1501
Value: Turkey Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2572
Value: Turks and Caicos Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-2571
Value: Turks and Caicos Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1042
Value: Ulaanbaatar Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-1041
Value: Ulaanbaatar Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-132
Value: US Eastern Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-131
Value: US Eastern Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-202
Value: US Mountain Standard Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-201
Value: US Mountain Daylight Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-932
Value: Coordinated Universal Time

(PID) Process: (4772) 1.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3c\52C64B7E
Operation: write **Name:** C:\WINDOWS\system32\,@tzres.dll,-931
Value: Coordinated Universal Time

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (6280) BitLockerToGo.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (6280) BitLockerToGo.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
469	173	30	8

Dropped files

PID	Process	Filename	Type
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\PersistentOriginTrials\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\parcel_tracking_db\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\commerce_subscription_db\LOG.old~RFe5e77.TMP **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\commerce_subscription_db\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\chrome_cart_db\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\coupon_db\LOG.old~RFe5e96.TMP **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\coupon_db\LOG.old **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old **MD5:** 19D1A06251A8678F85D8DE5BFAB83807 **SHA256:** AA6E55DCF84CDAF0BD3F913E7B837F65500E9B71A5A7AA773D02FFBC18C7FF01	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** F96D0EF8D63094D714514A441F8CD3FB **SHA256:** 2083625CA1E32D366F0B664D9B87B591791EF2EA2B770F4FA6ABE13FECA01196	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\4dc0d938-c717-4c26-ac69-35d2e5dca941.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** 723783C35EAEEE1492EDB30847AE6750 **SHA256:** C29323F784CF873BF34992E7A2B4630B19641BF42980109E31D5AF2D487DF6F8	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** 668BAE5C0A00EF466FA52102A122346C **SHA256:** A366BA8B2FD21BB25B17C6AC8A2C07428AEE94E6EA8CB14E204E4F77F61E2D40	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Variations **MD5:** 961E3604F228B0D10541EBF921500C86 **SHA256:** F7B24F2EB3D5EB0550527490395D2F61C3D2FE74BB9CB345197DAD81B58B5FED	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Version **MD5:** FCE53E052E5CF7C20819320F374DEA88 **SHA256:** CD95DE277E746E92CC2C53D9FC92A8F6F0C3EDFB7F1AD9A4E9259F927065BC89	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RFe5e96.TMP **MD5:** 139F545948FC1F10256A27E3C2CEF062 **SHA256:** 9399CC6F9C335015E086DB37208B1816A7831221A005B04AC83C4F86CC04230D	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat **MD5:** FC81892AC822DCBB09441D3B58B47125 **SHA256:** FB077C966296D02D50CCBF7F761D2A3311A206A784A7496F331C2B0D6AD205C8	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RFe5e67.TMP **MD5:** 8F45965291AB2DA10EEB049FB6E917C6 **SHA256:** 8A0DE526945B27CDBBD87357C85FDDD37B572370F894CB0A5AC533FD465D2166	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old~RFe5fa0.TMP **MD5:** 602C51DB8380F8CD0A961D9A46AF1186 **SHA256:** 84F716E38017F52138A76222524A3152DB8D3A7FBE30E94067458568B14DC36D	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old~RFe5f52.TMP **MD5:** 390E3C6EDCE7036BB6F52670DC24ABAD **SHA256:** D6F1B47CD05A8E1FAD989DEEC22ED67EA9A013C2DE0CCAFD68A539F69BD0DD70	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old~RFe5fb0.TMP **MD5:** 4320BE33704F77FF4DF4921358D2C50C **SHA256:** 8FDF7387C47EB272670EFF935D71492F03EAFAA55A8B22C05658BB0F1AC472EE	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb~RFe609a.TMP **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old **MD5:** A95974F48FC4A0E16E9D7729D7874157 **SHA256:** 926422473F59B7759EA8EB2064FD6DF9D00A88B548DEF1D5C3E08860357C03A2	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old	text

		MD5: DF81465C6FD3C271021EFEF60DC3C105	**SHA256:** C3099E8B290EC2DB598E8516BE5D963729363E0FB6D8C3F89131F9B747CDDA7F
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old	text
		MD5: 4B26172585D38A3DD6697E274D0608AC	**SHA256:** 85899A7AF1BD1939EA8264009EC427930FC5C092C8C3193984D6391526319268
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\248fa1ff-e570-4136-bc2e-3649c8056aab.tmp	flc
		MD5: 3433CCF3E03FC35B634CD0627833B0AD	**SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RFe5fb0.TMP	text
		MD5: 13D19AD173F46FFCD5871A3309D723EF	**SHA256:** F74346A518C9CA378DE81E9459ACB62FE0B1B6CE4CD9F190D0729A40B75B46F3
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RFe5fcf.TMP	text
		MD5: 86E6BAA91A6F56387D777804EC3DE437	**SHA256:** BB32752B143D45A6914D496141D263991B7AA04ADD153D8BD8C736DE282A2A1A
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RFe9546.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RFe9556.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RFe9556.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RFe9556.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RFe9650.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb	flc
		MD5: 3433CCF3E03FC35B634CD0627833B0AD	**SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RFe9650.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old	—
		MD5: —	**SHA256:** —
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Trust Tokens	sqlite
		MD5: 767A7DB34589653629C0D4299AA9EB7A	**SHA256:** 78A4734F08B47286A3736C88C6FC481F76BD2B1A46E29D0920939F088CE899FD
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RFe875c.TMP	binary
		MD5: 501106C8FFCBFE805C6EF3727B140B3F	**SHA256:** F63D1CF4F3F3287B792F20CA269EC790C7CCCB99DB9E083E633194716FC36E58
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RFe9650.TMP	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\Downloads\Unconfirmed 203390.crdownload	executable
		MD5: BEC3D8F190227C1D133C2D0CD36986B6	**SHA256:** A8DEA7A90CDCE4B3832C83B7D916D23D830A26BC7AA348339DAF57D517372DD2
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences	binary
		MD5: BBCB671C1F9D23B6146008D3E6A319B7	**SHA256:** 251315EBC6D0559BEC3BACF84C7A0C499C41CC38F98B041AF256269B7D2728A5
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\6cec00c8-fe35-4a5f-9619-51df2ccd11e4.tmp	binary
		MD5: BBCB671C1F9D23B6146008D3E6A319B7	**SHA256:** 251315EBC6D0559BEC3BACF84C7A0C499C41CC38F98B041AF256269B7D2728A5
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFe8577.TMP	binary
		MD5: E4129B94C2087C5DC93A5CBEBAE43E4E	**SHA256:** 5EFFB0299F4E0EA6DAD1B30234ECF8140810CEB74C40E11457A1CBAE8E93F0AA
6328	chrome.exe	C:\Users\admin\Downloads\dd74f9bb-f708-4aba-aa93-273eacbb8e92.tmp	executable
		MD5: BEC3D8F190227C1D133C2D0CD36986B6	**SHA256:** A8DEA7A90CDCE4B3832C83B7D916D23D830A26BC7AA348339DAF57D517372DD2
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\387ad389-9d55-452b-833a-cb177f31a255.tmp	binary
		MD5: 724510293CCF119A402FBF0FF0801679	**SHA256:** 6113B23A27F8454A26104F68B1C52ECC16B463997BC61874C2760E667B74FA47
6328	chrome.exe	C:\Users\admin\Downloads\Unconfirmed 820254.crdownload	executable

		MD5: 39B0D8690D0DCB429578D0AF74F1BBC0 **SHA256:** ADAF1F0BD0EAB0E0B691B07920249EAF24FEFF0B76F1E35E5032D2519B8C71AB	
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity **MD5:** 724510293CCF119A402FBF0FF0801679 **SHA256:** 6113B23A27F8454A26104F68B1C52ECC16B463997BC61874C2760E667B74FA47	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State **MD5:** 23C7C3F46599EF4741D494C1E72653EE **SHA256:** E8C686D299F5E3A469FB64BCBDA6625AE8DC17FB80419B1350FF1AA60EAC139C	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\621eb459-c90f-48c1-98bd-f8c1425c0bb3.tmp **MD5:** 23C7C3F46599EF4741D494C1E72653EE **SHA256:** E8C686D299F5E3A469FB64BCBDA6625AE8DC17FB80419B1350FF1AA60EAC139C	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Browser **MD5:** DE9EF0C5BCC012A3A1131988DEE272D8 **SHA256:** 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590	binary
6328	chrome.exe	C:\Users\admin\Downloads\912ce535-7a5d-4687-8dbf-c2b863581dc9.tmp **MD5:** 39B0D8690D0DCB429578D0AF74F1BBC0 **SHA256:** ADAF1F0BD0EAB0E0B691B07920249EAF24FEFF0B76F1E35E5032D2519B8C71AB	executable
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RFe8539.TMP **MD5:** 6EF6D4132727E4F700645C341C4BEEE2 **SHA256:** 5164FDFC5C55D1BE643CF646E2E89C32191344D969632C8AED72922AE31D06C2	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old **MD5:** 87F4E464F4EE3D5C7DA6FA24D1F52629 **SHA256:** F12400B717EF912F6A80A009E3CE2723854F8B057F066C2DD6FDF370657FBE55	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old~RFe9650.TMP **MD5:** 2BB5E5996BF5B9092AFEF1DB178D92D2 **SHA256:** 4F42BBC1849F98F282D3B12B63D6C7DFDCD037101229496BE326ABEEC1845302	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFead04.TMP **MD5:** BBCB671C1F9D23B6146008D3E6A319B7 **SHA256:** 251315EBC6D0559BEC3BACF84C7A0C499C41CC38F98B041AF256269B7D2728A5	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\979118c8-0913-4ad2-82cf-01217ccb1b29.tmp **MD5:** 5C3ACFBBE2816424E2EED4E0236777E1 **SHA256:** 140E534BD5855E7B668DFCF910D10872758602DE817D975705189F0BB659D785	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\BrowserMetrics-spare.pma **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFefb63.TMP **MD5:** CD1671BEF6FA995948885CBC7D570B31 **SHA256:** D528B41FC7D6D6CA49B84EBE1EC76D633AAFAED23DD4B84AE8F283FC952F7B37	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFf267a.TMP **MD5:** D64B91945B510A0C072518FD7B4B1495 **SHA256:** 676B3B48D2B6B20B86D34AC2214DB62AADAF56A75A38F1156AD9C37B220AD13B	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFed434.TMP **MD5:** 5C3ACFBBE2816424E2EED4E0236777E1 **SHA256:** 140E534BD5855E7B668DFCF910D10872758602DE817D975705189F0BB659D785	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\f4e62737-18cd-466d-95de-c949e40f67be.tmp **MD5:** D64B91945B510A0C072518FD7B4B1495 **SHA256:** 676B3B48D2B6B20B86D34AC2214DB62AADAF56A75A38F1156AD9C37B220AD13B	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\365a32f8-04ae-49d6-ba65-4de0784ae6ce.tmp **MD5:** 26514D83CF5C1890B25F239B98324A2A **SHA256:** 8233DCAB646C14A548EB84910C0F0AED523CAED4F7752ACA80759BC93C70AF1A	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\d7213747-fd3d-4782-a170-e6da198c2a9f.tmp **MD5:** D8A03F0CC78EDBCCABAAC0F34F050999 **SHA256:** 48177C61ED2F6766E5584EB1B02BFE989357C5DADC22C51C2E845DE06B9C251A	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFf4da9.TMP **MD5:** 26514D83CF5C1890B25F239B98324A2A **SHA256:** 8233DCAB646C14A548EB84910C0F0AED523CAED4F7752ACA80759BC93C70AF1A	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\6afdb063-8e8b-4946-800a-1bd0089a24fd.tmp **MD5:** CD1671BEF6FA995948885CBC7D570B31 **SHA256:** D528B41FC7D6D6CA49B84EBE1EC76D633AAFAED23DD4B84AE8F283FC952F7B37	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFf74c9.TMP **MD5:** D8A03F0CC78EDBCCABAAC0F34F050999 **SHA256:** 48177C61ED2F6766E5584EB1B02BFE989357C5DADC22C51C2E845DE06B9C251A	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RFf717d.TMP **MD5:** 23C7C3F46599EF4741D494C1E72653EE **SHA256:** E8C686D299F5E3A469FB64BCBDA6625AE8DC17FB80419B1350FF1AA60EAC139C	binary
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\a6b2f021-4412-4f0f-837f-fc8ecb10e06c.tmp **MD5:** AE5A83A1F90F5037C67CD3AA22C00968 **SHA256:** 9E11E4A09CCF44A7D08E4302F09CACB620A4125925BF13AE5E4F4847FFF1457E	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\8edea9f5-893c-42a5-9aa2-4eed6945d4fc.tmp **MD5:** 1AC183CAC033BD64637BE985B7414047 **SHA256:** 75613F7BA53C90EF3FAB19DA534B59AF3084E5BF62AF3E008FAEA72533157144	binary
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State **MD5:** AE5A83A1F90F5037C67CD3AA22C00968 **SHA256:** 9E11E4A09CCF44A7D08E4302F09CACB620A4125925BF13AE5E4F4847FFF1457E	binary
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State~RFf74c9.TMP **MD5:** 2FD2C359C7B53A4913670FB1E67BB72A **SHA256:** 0AA23D2246C843E3CD2314DE8DFE237562F7C225BF20F2A0E716828920A1A478	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\1f85e054-16d9-4226-87e0-cb3eff3c102b.tmp **MD5:** 6CF52CAB3715F04DB05D7CAE07668A67 **SHA256:** DF4F7F79BDA7B63AF3BE7A2CE56D723839045013B4E0C972D4929F0B7BE25B72	binary

6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFf9bf8.TMP	binary
		MD5: 1AC183CAC033BD64637BE985B7414047	**SHA256:** 75613F7BA53C90EF3FAB19DA534B59AF3084E5BF62AF3E008FAEA72533157144
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\60591a1d-93de-4571-adc3-fef349ae1e3d.tmp	binary
		MD5: 5DF62DE9514AB7F62DF5F94244A89D0B	**SHA256:** 8668574972BB9E97A802CDB7A970FAEE36EFC3C60D3F6AB50364BCA131699F30
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\eb827f80-a72d-48b9-a770-4440eb7550b2.tmp	binary
		MD5: 7D94C00B1B640391B125A76E8B7EDC18	**SHA256:** 6BA91C240CE6D2B106D1A212AA6BED5618489E43E7AC7C46DDF3CDF37BC6B276
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFfc337.TMP	binary
		MD5: 5DF62DE9514AB7F62DF5F94244A89D0B	**SHA256:** 8668574972BB9E97A802CDB7A970FAEE36EFC3C60D3F6AB50364BCA131699F30
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-uk.hyb	binary
		MD5: 0EC028755F0CD9EBBA41FB7273DE8BAF	**SHA256:** 1C626ABE40D43F6D56A01B5B40305D7C7D6481F616EAC00A3F3AAAACA8388786
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-und-ethi.hyb	binary
		MD5: 4AA9B2C0C9CCDE5140D01DC6502242BB	**SHA256:** 1DE83CB787DFAF53FB7E6E8DB3AAE5008AD24EBDD28BE02031306EA9E9F3E285
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-tk.hyb	binary
		MD5: ED60185B6F455B6F8ED27EAEB73334A9	**SHA256:** 77FDAED29BD842AAA976AB7EF81B617A15C0A2D1EBD1161C1BF26B79A108B5CD
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-te.hyb	binary
		MD5: BF9DF63B3C97DE3BFF99E24EE4BC5F2E	**SHA256:** 516FA9654FA3AEAAB480D40EAF6AD78FC039086BD8EDC144BE3D59525EDCAC29
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-sv.hyb	binary
		MD5: 892598DC59CE71E68ED337ED9FF3ABC1	**SHA256:** 56642AA5A37625FF9D034761D16B034D4BA5BE74090CBD825956BBCE2775ECD1
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-sq.hyb	binary
		MD5: A22D0F39CD83F3A8E251F95C5B12DD31	**SHA256:** BC29C9401CE952414CBAEBC5C8EE1D27C1706C6F77807B5FF713E2124438B3CA
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-sl.hyb	binary
		MD5: A21358DD4506643486F72F7D80D60A5B	**SHA256:** AD746C68562603AC3B15E89DA03C76E081C08E7D9C8D4C9F64763E53D696C77C
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-sk.hyb	binary
		MD5: CEA295E8B4B99F95738727905A9184E2	**SHA256:** 138C5990961DA21993653F54A413DDACB8921D6D70B892B7CA154D6E8AD2028C
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-ru.hyb	binary
		MD5: 4D132AB42E0C8ABD3BA93D8B34BDBEB3	**SHA256:** 336CE2048FFD31B7BCAF435E53BADFAF0579E405042D49ADBC0823F6BE5F9614
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-ta.hyb	binary
		MD5: AB2F6F9696FC7D699356244725E7C778	**SHA256:** 40FDA94856A86F065DE8BAA6184EA63DCDB011EE4CA498A7C1FEE44C99314C67
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-pt.hyb	binary
		MD5: 564FF32DED64C6BFC693F2758A53D68E	**SHA256:** F6FBF1BCB260CC86256FC494F388F7B27D10865FBF8F61517DEE25AF4D58D6E8
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-nn.hyb	binary
		MD5: F2D8FE158D5361FC1D4B794A7255835A	**SHA256:** 5BCBB58EAF65F13F6D039244D942F37C127344E3A0A2E6C32D08236945132809
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-or.hyb	binary
		MD5: 7E265A294303F69AA66C243F5F474463	**SHA256:** 4E9CD302BAFFC4EA3E9652327EA24072EBF37B5C4FC0719292BDAC10AAAD665B
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-mn-cyrl.hyb	binary
		MD5: 07CDA8332B62726883B29290CA35FC89	**SHA256:** 0D2731F16AA2C90FAEC8E63260358CBCCEDE403FAF95E3AF8C66BC2DB0729CA0
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-nl.hyb	binary
		MD5: D3BB05944DE3D0D7186E7E9383805E2C	**SHA256:** 5EBDE398944B461CF940F0520C5A49C0882B6F36F9AC5CDA0538C8C8B44FB7CA
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-nb.hyb	binary
		MD5: 677EDD1A17D50F0BD11783F58725D0E7	**SHA256:** C2771FBB1BFFF7DB5E267DC7A4505A9675C6B98CFE7A8F7AE5686D7A5A2B3DD0
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-mr.hyb	binary
		MD5: 0807CF29FC4C5D7D87C1689EB2E0BAAA	**SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-mul-ethi.hyb	binary
		MD5: B42317960E5DA868A8120CB79A440ABF	**SHA256:** F2FAC1BD069FFE5CD1112D94CC31137ED38A1B161093ECD74C9C1688428B688B
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-pa.hyb	binary
		MD5: 0F27E5BCCC1CD9DDF3EAC020DA27DA57	**SHA256:** 470329D28FAA484F945D78FFEFB176DCB6F2032C753E25BC014106AD24B2C68A
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-ml.hyb	binary
		MD5: 84A0A36EA2C5B3209A3CD40D1043230F	**SHA256:** 90572DB8F49B01EC6A102732CDF14FC3F07D363CBE0D261103E583043164E888
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-it.hyb	binary
		MD5: A4D5EC24D4C5EE745CDCDC019018074F	**SHA256:** F9C027D7FD44B01CD5E1CDF802E20C63560673098AF18BEA0930BA9AF334E0F7
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-ka.hyb	binary
		MD5: AA6C771083158380B2631F01E3F64F20	**SHA256:** 2472271C7955C67E9FDB86D0CD3C5D88F5E598DA4F44B6741284B2BBCB2E4D52
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-lt.hyb	binary

		MD5: 970C2671EAC4FFF6D840DC122E43B7C6	**SHA256:** 6FE2DA26A96834FB9AECBE586D40F728DF0EF676A4F235450054E66841B9E2CA
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-kn.hyb	binary
		MD5: D986AC2E7C75CF3EF929A7A269AE0D5A	**SHA256:** 2B999D0A152F804601AA8F38FF0D3A6E5949977BF1DAA76FA888ACAE21526287
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-lv.hyb	binary
		MD5: 05DFDB7F1EE5744573CCD62AE565B2C7	**SHA256:** 65962CCB5055E4C693E5AC493D6AFFDC810EC168EB2942F5705B7F4E464F9993
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-la.hyb	binary
		MD5: 9AAA47272099A013A4389BC314B7D2ED	**SHA256:** FD4B6F36135CD3B932E350EC2017DFD89D2E36AC226F54E4C8F2E4BC6DB0593D
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-hu.hyb	binary
		MD5: 37B1F197E8DFBAFDAC4597EDCF673E63	**SHA256:** 8B3A16268CC932B226C17FF405B3CFB6EB38A9511A2043D653DC03729EFCEAC1
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-hy.hyb	binary
		MD5: 70EA4451C3A26FD7197A3D2188BE4152	**SHA256:** 9B34DFCA85CB27546829F104F137757EFB274934C1E9D4991F55AD564962A76A
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-hi.hyb	binary
		MD5: 0807CF29FC4C5D7D87C1689EB2E0BAAA	**SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-hr.hyb	binary
		MD5: 1864E47E724BB7F9C052A2840EEE21D9	**SHA256:** D5F066A5657F1D7C39D053956DF204B7926F40D2FE4F69573AF09D909066E26C
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-fr.hyb	binary
		MD5: 092E0A95D6DADA26CA56D2ED558749A3	**SHA256:** 00BD8B2D398D77575DA2BFBBC5EC641AAD7F2A87D4A31186EC169E85A27DE5B7
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-ga.hyb	binary
		MD5: 768032A419E0AE3BD870D591E2173715	**SHA256:** 1E3043F395BFB2A4C43D0480BA2F168ED622881CC3482359CA6E99821E983BE8
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-gl.hyb	binary
		MD5: 1B08FB098D29C30488B8FC3F19DCF8B9	**SHA256:** 89D98EFF14E2CF1C2314EFDF392339E62D7E786F100202A7377BF7B22095A0C5
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-gu.hyb	binary
		MD5: F6DC4E0FB974869D3D9457C582A38690	**SHA256:** AF0EDB67C2219B803C3EB6C1DEE6F2D41A3FE00468A9DA8BE8EF5056D701ABF3
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-eu.hyb	binary
		MD5: E90EA97070CFCFA795FBD807AC300D34	**SHA256:** E2778A4FC7B8F064A32B6A44BC29F10E264D9D6214B8EDB8EBD1F5F6D68E2EB2
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-en-us.hyb	binary
		MD5: B2693233D14890C81D322BEC948549E7	**SHA256:** 03727CD6F4AA71B203C4C74CA6987AC7D87F13037337AC6F4B6996C2A0DC5F8C
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-en-gb.hyb	binary
		MD5: FA3DCB77293A058277CB148A0FF491FA	**SHA256:** AE4B78009D18E849D87458677151EE3AAD1608AD72EC050DFD2421D22E7D031F
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-et.hyb	binary
		MD5: 2AE42AB807286F6EC0FF1876D9536B0B	**SHA256:** 10079C66014DD2E6ABFEF5A018E6553FD5A036AFB96BD2A235440A188F88B15E
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-es.hyb	binary
		MD5: F6BD0377237FCA3C4B7C6A6CB244298B	**SHA256:** 137461792537A2E56A6475E81E2B9AD7A2BDABF1F4738FAE186DCA3022357349
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-el.hyb	binary
		MD5: 746A59E9F9DDA15C0F17C1B72921C85F	**SHA256:** 76AE3454FB0045ADB83094832578AA4749CE4DC694C4EDCF85B419C1E2D9BCD3
6328	chrome.exe	C:\Users\admin\AppData\Local\Temp\4ae64b11-8d54-404b-830d-ce34b97d4433.tmp	—
		MD5: —	**SHA256:** —
6328	chrome.exe	C:\Users\admin\Downloads\Install_x64.exe	—
		MD5: —	**SHA256:** —
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-de-1996.hyb	binary
		MD5: E7A9906B316D478B55BF8EBCBBB1D1C5	**SHA256:** D673805547A0228D2F57A5AD551B8760CFCC521F38C49284ED3976E3515BCA49
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-de-ch-1901.hyb	binary
		MD5: C6773229845710633D3A4D6DD9800FC5	**SHA256:** 8223A912160354E05735522FDB339DC59B353AD5D1E4F4CFA94898DC348E748F
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-cs.hyb	binary
		MD5: E8B1509F86508E807D61216614B3DD58	**SHA256:** 97A4755FE9E653A08969F1933E3DB19C712078B227BD5AA6799093ABC5A0EDC3
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-da.hyb	binary
		MD5: D0E160DCA547EDA390D6CC7C4A1F7AC6	**SHA256:** 86FDFC8DB62CDAA11F615DAD3712DA1F4708294E029A4AAD0FC285D4EA16C4BD
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-de-1901.hyb	binary
		MD5: DD9D0A81D897F88F76C1F6D69FB7483E	**SHA256:** 8C5FA4B29519D17593E923BC6A9A284DF7A6D07FAC42F897110B8FB2E0BAEEF5
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-cu.hyb	binary
		MD5: B4E5921B1DF85BA9F2EBE6CE578915F6	**SHA256:** 2BAEE19D5024FF87DCF3A1B9D0DA1B3AC5A1E506ADEEAD3B96A4DE5395D0290E
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-bg.hyb	binary
		MD5: E8A4F8F5238F9A0FF6968AD8DBA2755F	**SHA256:** 7593F0395081E3EEB2D8516D10746608AFD826CFFD4E7E37D53936993D200A13
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-bn.hyb	binary

		MD5: 8961FDD3DB036DD43002659A4E4A7365 **SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE	
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-cy.hyb **MD5:** B0F32ED7B4B8A068A962D820627B7229 **SHA256:** 4D0569FE2F4B41B3164CF610310E1D996FD2C553CC39DE6062E50F4E033CC207	binary
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-be.hyb **MD5:** 087DE134F3B23A9944AFD711A9667A0B **SHA256:** 25B7CFA039F82AC92990E1789DE40988D490DB9B613852FB24036B38FF87893C	binary
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-as.hyb **MD5:** 8961FDD3DB036DD43002659A4E4A7365 **SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE	binary
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\manifest.json **MD5:** 2617C38BED67A4190FC499142B6F2867 **SHA256:** D571EF33B0E707571F10BB37B99A607D6F43AFE33F53D15B4395B16EF3FDA665	binary
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809_metadata\verified_contents.json **MD5:** 117D173E82B282DECA740475E35C8ECD **SHA256:** 65491B21947D60C87C6358DCF69DF9ACA2B99E8F3B611BD3D559699BBC25000B	ini
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\component_crx_cache\jamhcnnkihinmdlkakkaopbjbbcngflc_1.c52c62a7c50daf7d3f73ec16977cd4b0ea401710807d5dbe3850941dd1b73a70 **MD5:** 2AC309D48A054C8B1D9EA88BAC4DBD6C **SHA256:** C52C62A7C50DAF7D3F73EC16977CD4B0EA4017108O7D5DBE3850941DD1B73A70	binary
3864	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\hyph-af.hyb **MD5:** FFA9DB945F0F0C15B8BBA75A6E064880 **SHA256:** 5487EE44A4CD706D0086522E90C59C76CDF2AC68CE506FD3EAE6054B9220C0CF	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_902239809\manifest.fingerprint **MD5:** 1CAD009F2AEF6C1DD04097A9F2B3EEE6 **SHA256:** 927620C57785DA956D59A04CE06F426DC759373F107F9A46E540B51EDB873A79	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\42a6344b-d8b1-4959-a6ed-e6352b94130e.tmp **MD5:** 0F0084938675686A8DFD9925ABB58431 **SHA256:** 844FC9573476171E7BE9F90C26C6C5C71879FF62B1E59FF7FFE1F72253EA5E4B	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\DownloadMetadata **MD5:** 0F0084938675686A8DFD9925ABB58431 **SHA256:** 844FC9573476171E7BE9F90C26C6C5C71879FF62B1E59FF7FFE1F72253EA5E4B	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RFfea76.TMP **MD5:** 7D94C00B1B640391B125A76E8B7EDC18 **SHA256:** 6BA91C240CE6D2B106D1A212AA6BED5618489E43E7AC7C46DDF3CDF37BC6B276	binary
2360	chrome.exe	C:\Users\admin\Downloads\Install_x64.exe:Zone.Identifier **MD5:** FBCCF14D504B7B2DBCB5A5BDA75BD93B **SHA256:** EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913	text
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\7d323917-e318-4a43-9f09-5d59af12347c.tmp **MD5:** 44048877807940E6D7B9D27CA7F5BCD7 **SHA256:** 60F6CA7671C6F99FD125123F2DDF8A97C62CB63566EEB81ABE86BF368280BBEA	binary
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Install_x64.runtimeconfig.json **MD5:** 6B21A809E6B60333C382DA8A02F506F4 **SHA256:** 91F3378989682462C95A3C2452758B3A334FAC21458998017847C60F1557327F	binary
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Install_x64.dll **MD5:** F14C8004C085B7369699CBE79ECEA7AA **SHA256:** 347F7C0489D17F018041C1B24E8228AC233E39B6B8763EC4BCBE500D9B0923F9	executable
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RFff004.TMP **MD5:** 6CF52CAB3715F04DB05D7CAE07668A67 **SHA256:** DF4F7F79BDA7B63AF3BE7A2CE56D723839045013B4E0C972D4929F0B7BE25B72	binary
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.VisualBasic.Core.dll **MD5:** 870FCB59AEEE9863E56CA36C2B095241 **SHA256:** D5E263DC32565CC37F3FC2AE712CF09AB2B739136580BCBF5D383E2893A71182	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.Win32.Registry.dll **MD5:** F56B573F2160E505AA07D65D5BDA44ED **SHA256:** A7FF9A52D21B172411C40F6441B59204ED629CCDF4DB4603413D6C2C227D326D	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.AppContext.dll **MD5:** D5CE65B0730D2BB628BC722CBCD1835C **SHA256:** 88638516F59E9D316E5DDB7D120D5E24B576AA8A48666E6DC27CF4E302E88858	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.CSharp.dll **MD5:** C4160DC3F6D21FE4DAD88355CCBE39CC **SHA256:** 1A2BE84D4B37453B53E23F664540517E8A548FBEB66D64A64B70E410DF1C5541	executable
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\e8e662f0-2763-46c8-8016-4cdbbc38856e.tmp **MD5:** BC3295FB0DCD6A5F9D88B77D8CE6602C **SHA256:** E3B4D7B3995E06EB6C7C9B3DD4B8C196CA87405D526B095075D0F35801501D4F	binary
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.Win32.Primitives.dll **MD5:** 21264D0E6F5178565F885351EFC839F5 **SHA256:** CCE359FA0E5B74278E9F4B61AD1DE48E9D068DADD6B23907CDF5195F3FA01A25	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Collections.Concurrent.dll **MD5:** 2E48CA7A4217CD449A2D936AC90A9CBA **SHA256:** 481EA24D7CC9CAF499F79AE6D4DE9453F01077F370C90FAB1B5F6BD13C2B6A75	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Collections.Immutable.dll **MD5:** 6C87A81716FE38F30719605FBF22091B **SHA256:** CC5DEAB7E8706E91B7F76BED8B25ABEFA475E12CABBAA30B53B2165CB0B8219A	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Buffers.dll **MD5:** 462DE1685F6F955D1BE2355A4F74236C **SHA256:** E5D7A69A80EC56232D004F2B1D9895557F1214F7126AB3E60A86223B9A65397C	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Collections.Specialized.dll	executable

		MD5: 04D948CB49A01DAEC0577D8459172BEF	**SHA256:** 751D792AF9A2C6046DBED9C4B821F1B68ABE3A1EE66D4EB88551F45756EA3B78
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Collections.dll	executable
		MD5: 7F93948DC4D4883AD21147AB93186571	**SHA256:** E029ECD6BC46E34D1099A10115C94587A62A5F5431F4E99FFC623B37C2F9AFCB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.Annotations.dll	executable
		MD5: 2771E2266C9A75024C198ECC60C66A69	**SHA256:** 04030D3232C8DD307E3BFF0962B4022206A96AE78D289C2BDB4571B67E4D5CF3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Collections.NonGeneric.dll	executable
		MD5: BC0819BD1F85AFC33531E568D17AF8A0	**SHA256:** 0C6AA659CB235C6923777B2D2A8F860C191B19A101FB4DF217C5A44D6979F939
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.Primitives.dll	executable
		MD5: 401EEEDC1A5CD6C9222BB365A0EA03CC	**SHA256:** 01F04AD89194C81A97A5351B5D925C315D06C6D23AC155DCEA4B44FE432B8C40
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.EventBasedAsync.dll	executable
		MD5: 13AFD2C8AD423BF4DC9D2038F78D0C93	**SHA256:** 168EF8A599B37F4B3FFE40A231C93DE7D935689FBEC985F058E99AF71B4260C1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.DataAnnotations.dll	executable
		MD5: 1788B6D282A61A0EB0AE5DF03F79C173	**SHA256:** 153413962F80EFC0A920FD8ADCCD9D9DF20872B49D96BD3EB490A91C55885933
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.TypeConverter.dll	executable
		MD5: E75E07183DE713FAC418E7D47A6C3574	**SHA256:** 6BC3547951A715589EC145F3F1FFE3D2128EF4B50A2C782FCFDA02ED05B01596
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Configuration.dll	executable
		MD5: 2DA1D0912661D3B41C734A1733C4790D	**SHA256:** 1F45E10B44AB7594751C94407EF8001001229708B5D3D3682EFB4C5FE3D4F5B60
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ComponentModel.dll	executable
		MD5: 608B34843B8B7426D1FE3A4AC3719190	**SHA256:** 0C267A782BC30FA269781780438AA84899AF6B4A625027CE613D23268D016385
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Console.dll	executable
		MD5: 576085B4EB90B682B43EA09399895D10	**SHA256:** 638CA89107A0DE374B22A1AC2B3999B57FC2B532FD13920FA5E2F56668E51385
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Data.DataSetExtensions.dll	executable
		MD5: E73780DB7B29019099CEB0D5EA06D724	**SHA256:** 0741DD90B69DE2A166B86771D5E6FA673DF8A994E58A884736A930031FE001D3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Data.Common.dll	executable
		MD5: 435CE7235B064C7C963B85F294B01020	**SHA256:** 7D22666CA82D502E5F0EC59660797AAA6BEC551932B11BB8001799F383372D32
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Core.dll	executable
		MD5: 58D27AE55B491CAF9E0D6F7394B67A62	**SHA256:** 7A843C7CE3DD4CFF0B7C87BC08D69B6419DAF0C8360F80F8F3646266846A7116
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.Contracts.dll	executable
		MD5: E0A4C22B5ADC246E37A89562253DFBDB	**SHA256:** 2DDA4E022C41632FC5445A01C0DBBCEA4A0A04D46E2ECDC21845A459C8DC5D93
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.DiagnosticSource.dll	executable
		MD5: 9AFCBC0A7742E1E8892A31CB9C15AE91	**SHA256:** FCD720774BA1A8BAD281377F9515263CB143AD555FC8B0AA00B634AF1D875B9C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.Debug.dll	executable
		MD5: B39D621E3116CA4FF2BE3C87A44F83D6	**SHA256:** B5E4AD486994C3D06B6D7CB8004E2C512AC86BAA5A05C11A3550CB2F6E3BD84A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.Process.dll	executable
		MD5: E3BB7D4D834CA3E44B971FE7D1180071	**SHA256:** 30C92BCB55EC2A9CAD7DCAB8A46441C5F14B37B02BEC76B71C9F67FE51B2F7A3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.FileVersionInfo.dll	executable
		MD5: 68E128FF02595D03C43F3E05D6099E26	**SHA256:** CF97843EE097E4670F71D0B5301514F772F687E47D1F15181EA6704255444EE8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Data.dll	executable
		MD5: 0CA27BF73AF05E84C3B0739C6C6BF565	**SHA256:** AFEC80B7AE2329273F6697E258C3CED20507A15233717E3C6EF00BA5957C1D90
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.TraceSource.dll	executable
		MD5: 5E3F0257DF80EC5A311D00B560C089E9	**SHA256:** 54B81D872408ADA6764D770F64ACBB38318327DEA4CBE71DEED2A2E387D73B44
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.Tracing.dll	executable
		MD5: A35D64A451FA6B16DBC482BE51CFBA2E	**SHA256:** CCD811CC72CC0E0154D2147A7460E143C077B43D2673D4F240E6C4C578A3B797
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Drawing.Primitives.dll	executable
		MD5: D11BE9AE1015645776ABBBDB9A4A9EB4	**SHA256:** 82D40D9A2DBDD9EE3C1C4A4FE488E8A02C11A5AAFA28CAC11FFF155180DC9263
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.TextWriterTraceListener.dll	executable
		MD5: 6AACAE1B4DD3195D98D95BC936B38F86	**SHA256:** 4A00C5BA2FA14FD8D35D9343EAAB62840D189731158B59612B56D4B7439568FD
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.Tools.dll	executable
		MD5: 6E1930867DAD03C8768D32B0D80726EA	**SHA256:** C66ED0BE5AB86D1B6DE4E65889F633F47B5CA33820153AABFAA13C32A88BF916
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.StackTrace.dll	executable
		MD5: F1CD8127820C029007FE60A75C6F0154	**SHA256:** 164F859FDE31729F27F3DF653572603A514561F462A6552BEFEC4E7C5AE508F1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Dynamic.Runtime.dll	executable
		MD5: 10638DDE7BC9B49A2E12C09891705EF1	**SHA256:** F01BE6A01A52C807398668553F6BDFAD4D5CF9B816D8014A3F1D9AC35CCBF9A8

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Formats.Asn1.dll **MD5:** ED65DEDB5DE12E725A8F32BE4B0435A5 **SHA256:** 5BD95097A7556C18E6D5131EED75EEBC08B7759DE35C7864BAE26BB150F858F8	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Formats.Tar.dll **MD5:** AA001C16B05BEBBE3F7AB2C35C9BD5D8 **SHA256:** B993FE8E62B1B0A92771A75D4DDD6C2FD4EF096D68F63DD893B0F5530FDC6318	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Globalization.Calendars.dll **MD5:** 452F6B5BBD9A2827F8A7FEB033D37050 **SHA256:** D034DB7E65D1042C6B1768AA15B57AD3CB94F4044B599E1A4F3AAAD922C7CB86	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Globalization.Extensions.dll **MD5:** 4E02B9F45C1F5219CD251B38759F81FE **SHA256:** 975E170AD2268CC5BAF05FD6A0A1ADFA54F3F5BB987CFFBA8A85767E090896EF	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Compression.dll **MD5:** 477448FF187ECBCC14B7ECFA6212C487 **SHA256:** 6BB0458F8FE18BA0A5D5616EE564B21B1D6AD15FD2D783482559C29A83CAE4B5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Globalization.dll **MD5:** 8CB78C9370E3037C608B6BB95227585F **SHA256:** 76B800B76CD1A0AFB25A28F414CC7F827089B93EFDDFF421CB7BC611DC988A5B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Compression.Brotli.dll **MD5:** 681A6F2C04E1EE11B2505A95FB76DF2F **SHA256:** 4077CFD7320D34B4218B4F3C172587BF5D1E462C39BA4C636441B06E988292B0	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.FileSystem.AccessControl.dll **MD5:** 77D42CF6C02646EC05034A5A6376E85A **SHA256:** 1243F6664CD37196AA175287555086FDDDE6FCF153B394E4F391353C76A6F6C5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Compression.FileSystem.dll **MD5:** BA39FF78563836AEE95CD317CD7FA874 **SHA256:** 35F5F3D8B0320CD1805D31181E92C9D74462BEE7AE3CF4729ABCFF458583B58A	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Compression.ZipFile.dll **MD5:** 5F15325A4DB1C1896D0878AB97364418 **SHA256:** CAED8AF31826CE8D8734AE6F5393ED02FDD0A615B7DD2F6653E6205B64EE971B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.FileSystem.DriveInfo.dll **MD5:** 45401AC6F66EA00EA909C65018058C84 **SHA256:** CB589C59AAE620837AF5AC739C8F62DAACFA482E46BA82A2AD386AF337E849E4	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.FileSystem.Primitives.dll **MD5:** 404881BBE99A1AA215281515999A5DF9 **SHA256:** 2E7415CFFA141485F98F0DE13A2B598F465BE73DA40B923A022354D535723125	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.FileSystem.dll **MD5:** 1DE2DF794A538D5B4E75953E01B5798C **SHA256:** 68F8D36E0C42A49BFB731CC2BE838EE597E00396A4510367ADC02AAACE879240	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.IsolatedStorage.dll **MD5:** 050CAD22A0B98DDCAF45FF69471C2020 **SHA256:** CEDE9227F0BF828B029034BB98C4BA23E39C505B61821F28FD63101411DF5430	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.FileSystem.Watcher.dll **MD5:** 916B326705DBB90D5AA5881A6DBE7E99 **SHA256:** F1BFCA48C3D9CC77640965822E9D494AAD3D045BCBB395B0A7991EA16A8C0518	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.MemoryMappedFiles.dll **MD5:** 1A6C398B87EE8E6FB302AE92C1676AD0 **SHA256:** 4A99D50C664719B0D95E9EBB0558C5136788988424724FCEA15AE771D0F13648	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Pipes.dll **MD5:** 265DB7F1AC2515B8D25FC2C03369D5B3 **SHA256:** 4F2E711B96F1A67A56923850026CC65A95A965AFA589F3C9FA8ABFC804FC29B3	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.UnmanagedMemoryStream.dll **MD5:** 9895EEE7F66F2B5F59F50E5D12537E79 **SHA256:** B2398AA92050C46F9217B32C8F7F47370CD10A1103B431078F50EEA329F48F8E	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Linq.Expressions.dll **MD5:** 0EE5CA1977E58EC1FB5832A548079D95 **SHA256:** E6E63F71005B12C063C14BBE8A2FF40E12CDBCF3B31D77FF60642828EA400E3D	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.dll **MD5:** FB5E9367BAEF5C9C19C6B61CE2D0CE8A **SHA256:** A35F07B9978ACE211AA66BC7D82F90F96800A2130FC6B67764933E168E1EB80B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Pipes.AccessControl.dll **MD5:** FEB9B9EBE41C00F7EB0A263A6195767E **SHA256:** 84C5D1E654BC961EDCA1FF3543C49083746FFB1C6E28D32AD6F07867FEF631D0	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Linq.Parallel.dll **MD5:** 5B8882A14D340D25265919A64FBCE984 **SHA256:** 0C72CB6FDA97D072C6F57BDFFAC0AFA2D9E4BD7E40A5E108EB4E547738569ECE	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Memory.dll **MD5:** 9EFAD7640F68FB8D3E9D12680BFC883D **SHA256:** 4E1F49E42EC0CA7A55F017E1300DB72CE49D5BC35DA8C30B0EBBC18ADF19AE2C	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Linq.Queryable.dll **MD5:** B6DE16A69D93DC28FE21305DBD14AE99 **SHA256:** D228E3BE8A6A4FD30AFDCF839A7F86727F691845EC0E861D65459D76A5A1FFC4	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Http.dll **MD5:** C15232F41B2AD231273702308D2C3EC4 **SHA256:** 37369A8E2868BFD0838A3F95CEDB64E0AB2E6B0C88E12F2EB3C5C2A9412DD2D3	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Linq.dll **MD5:** E15D9F4FE1C46770EEBAA6DEEE7FC1A3 **SHA256:** D0521B1A0685855E9DC4C119A6F659EEC5DB08E2091CC8A4368572C05B7C82DD	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Http.Json.dll	executable

		MD5: 5019EFE4F7AD9B6D9721EC894BFD0B5E	**SHA256:** 3DEE9D1D82D10FA7B93EC1288FE2940D885AF0CEC992F441A895A7ACF7629041
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.NameResolution.dll	executable
		MD5: 490982C98A2CE92B7D740AB459A45096	**SHA256:** 86BEC69BEED78E7D6C584C8ABE35D043E14DF792FDF753FC1E72B68C294B4CE4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Ping.dll	executable
		MD5: E4FCA84A8CC666F7722B8DC6AE4A9264	**SHA256:** C46512E57E35AD97DD3967EB83EEE9B0503BD380FA91F1986345797589E86779
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Mail.dll	executable
		MD5: AB88C47E87245ED694FD1F888C7C7616	**SHA256:** BA5CC1BB161E1EA4808234B417B3953A238384B648EC6A1812CB668961E5247F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.HttpListener.dll	executable
		MD5: 67C0853749A13E32BE65AA9AB2B8B34C	**SHA256:** F5BC4127E96B4018036B981D513AC91147BDD97FFB9258CCECE4871D977B6873
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.NetworkInformation.dll	executable
		MD5: DC1A73030DDA33232C417CE17412CCAC	**SHA256:** 4411B03E15361E1F02BBD841AEDD7E8E467988DF1D4957808A164A8C5A0EBF7F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Quic.dll	executable
		MD5: 03B1A3FAEABA732C7052B97E23EBC89B	**SHA256:** EFC7AD2A4A4AEEA513F52896515BBF16EA264E2F6D3DD1C627BF3FFA58688059
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Primitives.dll	executable
		MD5: ADCBED0635FD16D1C8195F1215CC18FC	**SHA256:** D5C032D5837D31CC9953603B4E79D696E7B31A8AD3C7DE031E61371EED88B50B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Sockets.dll	executable
		MD5: 12E0E9FCE32F1C6901F0623F8D882D09	**SHA256:** 91F2D6A01E0D7F9418FF2F337BB03ED3C457EDD4DA72164359F2F0FFD1B9573B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Requests.dll	executable
		MD5: A40A51BADC9D36955E002BD1E80CE894	**SHA256:** F6C007EDE0D2AE1E815943091208D7A535CF9804BEA65A0AEBFABDD1DC2544A4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.ServicePoint.dll	executable
		MD5: 62F1E3643E466EC08131DF0A8DF54AA6	**SHA256:** D25E8F923630E9F02A4238ED4D51C899C3C76DB2A15DDE743BBBA8ED2A2FFAA1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.WebClient.dll	executable
		MD5: A11D33A2A5A5E66E3EDB5F62C822C8CC	**SHA256:** CC030B4CF024C7D503C30DA7DE9F84D147EED184A7A5FDA37D52EC8B4C5176F8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.Security.dll	executable
		MD5: B778B48A5104733F4E8CD2D2B6849B65	**SHA256:** AD77B159FA9DAEC4DA1B275DDD279DB392B388F3EFA8000DBE6C04C96C1B8468
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.WebHeaderCollection.dll	executable
		MD5: C0894A83EAEFBD3B837058F5E038C444	**SHA256:** D68DCA599F7A122E4E45B556B242CD85A28257C701F62E041E0D2E86E5DD3C33
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.WebProxy.dll	executable
		MD5: 8445FF12054BCE4042939951E49DE4D0	**SHA256:** 05DF05B12AF54571B6136985B8679CAC9D20B1C3EA75CE6658F62A5812A48177
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.WebSockets.dll	executable
		MD5: FBD16839BC1FE54C349BBA1D439A55A1	**SHA256:** BD1A8072F52F2A7B875D5CBC1A338C4F722F3EDBC4CCF86AE974B124A0724CE5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.WebSockets.Client.dll	executable
		MD5: D16F3EAF7BA1AA1EB4EA654F1362E3BC	**SHA256:** 7F6F10A18F95844083ED6A8F027B9F7FD216F27078B40F7688B490801BDC7DE4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Net.dll	executable
		MD5: BD33DDBDF43397F7FB73E029E9582598	**SHA256:** 1154B41824B21C2913D6DDE144C96883EEC56005227B12AA81560018D5C8C82E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ObjectModel.dll	executable
		MD5: 50DCD9C27D5EE53CFDAEC6DDF7144502	**SHA256:** 1341E79C5E9971B52235648160C63837EAFA59C743B0DF4FDC370C9A1841C4DC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Numerics.dll	executable
		MD5: A9219D44521BE6EDFE126D73991359A0	**SHA256:** 72BEBAF8A0F77C311790C6AD30FB73C9034D8FC3406A0864CB76786B6876C229
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Numerics.Vectors.dll	executable
		MD5: 53735D1F9B7FCBC8A6588FEB56722285	**SHA256:** 2F19CA215ACC036EFB6D8D7CD6D5DE5A1682DDFB6DC42848A4E7CCEF473BFAB1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Private.CoreLib.dll	executable
		MD5: 1D0B5B063750903245A29D8D7A7C123E	**SHA256:** 1387C7FEAACA387376D320C324097E83B3C6AFA263B3E9BB112AAE803ABF925F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Private.Uri.dll	executable
		MD5: 5CAFE651AB785CF22FA7409A583F32E2	**SHA256:** 3EFBDC54E88C94BD3023A811D55DC44C6919573D38986AFB4C17DBF22E019974
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Private.Xml.dll	executable
		MD5: 39591A0F2D3A6224E246A95FB2A8E3F5	**SHA256:** DF641D132420E3D56FC2EDAD7B7563B7F18CCC5BCEC24E7F2958691D48250D9C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Private.Xml.Linq.dll	executable
		MD5: 0BF4E11E9C948FDBF882CD3E24C9C086	**SHA256:** BDEB77BE920A46D5D1C57045C9A2C58BA704207A54AEFF1F0D42A416D88D4B7B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Private.DataContractSerialization.dll	executable
		MD5: 4B2F5924ADC49F9F5581B4DCDB402841	**SHA256:** 51966E26B8DB37A83A952DD045B32D3382A6150308C2D168939C40E2951AFA79
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.DispatchProxy.dll	executable
		MD5: 8D8A0DDD0AAAF9DEB843A73EEDED0C75	**SHA256:** AC4374944621CFD96C59E3281ACF09B826522B5E48D4CD2B1B096B3256ADE37A

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Emit.ILGeneration.dll	executable
		MD5: 03AE78450F073A094587F87A424C4959	**SHA256:** 48179C1B5C4B064CC7EA72094E98DF14775B727116A11F7BB5A03637953A0B6D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Emit.Lightweight.dll	executable
		MD5: F19BE4FE5D995FF9800F3884CF296193	**SHA256:** E8B503F10BCE6D4F5F9CDB68123AC630BF4C3B848EF45B08A59452DF15214970
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Emit.dll	executable
		MD5: 39304370936E781D01DC435EB7D835F9	**SHA256:** 4EEF50A04CC4BDAA7DCFA2C05C140C5BF66FEB4BDDC22C7891B2812B7AF82817
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Metadata.dll	executable
		MD5: DE0739B8C65464F035E5BBF6FDE56F6C	**SHA256:** 38CC2A406D54A93BC2A393D6357715D04E84B5F7C6DB03317CA0D127A7326902
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Primitives.dll	executable
		MD5: 13FA2FC80C7BF2A9C1DECDBD28D4764F	**SHA256:** B7620ADEC4274E057AA9BDFC9A97358AED333863655644556A59ABA5EFA9C3A2
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.Extensions.dll	executable
		MD5: 6220FD8B1F11E06781062EECB4E5B310	**SHA256:** 9F1845A95DCAF296E82405D40152295E163CD79F3E9B66FD893D68B4DB7FD7A9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.TypeExtensions.dll	executable
		MD5: 0786C0D0B0E6FAEE5D2734B601BF1763	**SHA256:** 2CB739A7EB04DC106215821A464A47AF42EF0B9342593D50EAA987BFFBA1A66D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Reflection.dll	executable
		MD5: 581CC9B97F3AD0AB57602217DDDD3DC2	**SHA256:** 2EB054A9ACBC1095B23746054CB45011BD50D0C0A842622984F0C82FB642E9D6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Resources.Reader.dll	executable
		MD5: 4B5E2B46A7DD13A8F15EBA1AA8BEDC91	**SHA256:** A41BE47EFD628FFB7F36AEBB6557B04D4B9C1A0CCBEF70922FA52C560ED7B6A7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Resources.ResourceManager.dll	executable
		MD5: 46B0F119C6C2B8285C6717619ABFEA9D	**SHA256:** 358BF9C1CEF3C350950F91ECB44B44F733A67CFA135A2EBC276D7DCDDBE103BE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.CompilerServices.VisualC.dll	executable
		MD5: 917C110B54BB04D410D951E8BAD13EB1	**SHA256:** CAE6331F3A0769A3E928646BB9205C46945A46D74856E78EDA380771A5F9F79C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Resources.Writer.dll	executable
		MD5: 9F42ECFC125B1132B6371AA29AD7EC4D	**SHA256:** D0825F2E3C392E3EBF2BD325AB074B46C1F199ADEDFD56F6EEC7C8D9AF4EB1BE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.CompilerServices.Unsafe.dll	executable
		MD5: F1470BD6204FE05FB734C9A4E989FA33	**SHA256:** 8581B2B404F0B262CE1A4DDC184E562E0500489F8275C6571929E1A2F4B9C9CE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Extensions.dll	executable
		MD5: 53C3233C3DEC039A6C3555E6D5951712	**SHA256:** F294AB328E80080A321C254DDF1A44DDD0D39ACCC27DFC14F473B3785F26EBB0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Intrinsics.dll	executable
		MD5: 644E11EAAE5B013E812EE02ABBE6C71C	**SHA256:** 5F2A0777B2AFC69F82B2CE24883BD57E4A69002ABA338EDAA7B2E7DE95DCC536
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.InteropServices.JavaScript.dll	executable
		MD5: CCC1BC1EE6FC5452E99F05268B1A9090	**SHA256:** 1DFF8DDA8181ACE7646964C9CCE0DFBFFAFF98FC5800E21A07EECB3E7123473D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.InteropServices.RuntimeInformation.dll	executable
		MD5: F87FAB28A85534358B6BAC2AC3FF184B	**SHA256:** A60B0D811997F2DCFCAB8E03810344A5538337AB8EA85BF824A361B420AC66CD
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Handles.dll	executable
		MD5: E504FE7613E8E6627950AEC23CA6CE95	**SHA256:** 1ECA0949D1F1CD38983FCBA0D42AF41C9F626E524541758DE4BD7CF9C14C4E68
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.InteropServices.dll	executable
		MD5: 71C937014419622A45762973CE1880E9	**SHA256:** 03A99FF7973A904D9EA3BA30FA2D935D53826CF3002F478DC6A1436C04890F79
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Loader.dll	executable
		MD5: 28AAD2BD962B3E58E1A0C513E532382D	**SHA256:** E7AE1A243C52BBD9E898825B54831DDA6E20DA72D3043A852D8BF91C81022540
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Serialization.Primitives.dll	executable
		MD5: 6DAC8EEB56FFE6991993AA2496FCD560	**SHA256:** 82FCBFC3FF931199A78A17CFEE59044E8EE18D39D6E9A9B0178196876A4EE8C0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Serialization.Json.dll	executable
		MD5: C5C641197868222261BE024B60CAD202	**SHA256:** 956D526A3D12474BB94EEFFD344156697C5EDB68D16BDB390D254F9E356DB30F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Serialization.Formatters.dll	executable
		MD5: 297D053EC462BBB028B995DD7C0790B4	**SHA256:** 83DBBD21A081FF62C8F9FD502708A978D68DF3B2808C1236E9C0036391A7870B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Numerics.dll	executable
		MD5: 041A1ED44F9D46A6BD493A1FEB17F2B1	**SHA256:** 603E39AFDAAEA91167596EA169CC7B8C6B66BB358DF48CAC0E47F5AE5DD379B4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Serialization.Xml.dll	executable
		MD5: 9C5D03C5D75CD524ADB97EE81819637F	**SHA256:** F76653974FCCCECF6CA6BD98F7C872D208AA56038DB68E5E5B9B096EE2995626
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Algorithms.dll	executable
		MD5: 186875D68DFAC9C2EF96994658A531D0	**SHA256:** 9708378F0F0D898F79938F512036D73D293F02E337D1437157992ED8F48EE2EA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.Serialization.dll	executable

		MD5: EA68BB82A88E8992E7055158AB746E40	**SHA256:** 6D60614AB110AA1F60D654FD4D79DE9DA05CDA2E9379DC8BC09F11ACDC12B65D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Claims.dll	executable
		MD5: 2369644EA90D550E765FD9EAAF359FCE	**SHA256:** DFBDC284C61278112E6638280AA8FA9EF7CFBA952017D6EEE9F57D64F4783E73
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Runtime.dll	executable
		MD5: E7AFDEA68461D2C79F7E3E5FCE78D69D	**SHA256:** F7395A0F3CD9A4A3CF7E45FCE80578CEAE7B36BFCE2ECC4711115BAF9B26457E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.AccessControl.dll	executable
		MD5: 3A4B1913EE1F61444F2540E81144DE11	**SHA256:** 8D7D5F7A37CFA9E489932F2BF6DCD10AF8E83737E917F2E5F229377C46E39910
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Encoding.dll	executable
		MD5: 249F034DC3FA390DE56C2A8E00726BC6	**SHA256:** F16A7C54D401768551C7D9356F4A2581F1392DF7CD21A29804F5F74CDAB8B378
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.X509Certificates.dll	executable
		MD5: F95E1D94AB9A9ACC9C3CBA217CB4C0E7	**SHA256:** CAAFF5CBF2D9B1343290E00AB65BB3905EBE7D8090EBFC66694D7ABB8FE916E3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.OpenSsl.dll	executable
		MD5: 44F71877352ABFF4FB290A32D1452D91	**SHA256:** D81607DAEC2C20FE6A2659A979AF08DDFACC5FEBE962A371BA56B88B38F9BFFF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Csp.dll	executable
		MD5: 61B9ECC266AA3F27B13477BC18C4AB08	**SHA256:** 598B5610267F87A931A7AC1001858B7B9A76BEAC8CB7A866A021789195285716
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Cng.dll	executable
		MD5: EB258975814C8F289E0603F8518B9A67	**SHA256:** B25E69BE49320A00E72AB5870184F978A2EFC336EE99F56362032555A344C121
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Primitives.dll	executable
		MD5: A49C697D9AAD01139CD774556117D7EA	**SHA256:** DB672656E5117329003D4EF1606F51631100991A612F8254C3769DC5C959178A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Principal.dll	executable
		MD5: 0343B75783E09A254BF1B80544251836	**SHA256:** A59B784878E192EE2E7E6CA1E2F146F1E386DCEC58463C70579D1E72E9306223
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.dll	executable
		MD5: 1294BB8C9E56E7233B08631F010C9881	**SHA256:** 4B52D78FB3BD9B7EF64BBAF8A08510074D1A8FC30D9C715E5D513A47FC8F8103
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Principal.Windows.dll	executable
		MD5: 591356FF3BA7BFAFF32483A69ED4AB94	**SHA256:** FED8C59518DA4C0F3802241FB160D90F779CCD9367F81E7DECF16C37484CC004
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.SecureString.dll	executable
		MD5: 55DE749EC9D6AB029CE7B63F88CFFC39	**SHA256:** D63C0E8AD3B02BDF5B5171345EC9C09A24925F25BDE79EF5661E35B6C5316725
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.RegularExpressions.dll	executable
		MD5: F7321FEFFF246C396DEB077FCC9F00CB	**SHA256:** 745DEAF694820F3EDDD4B4893B3168B21E61811F6307B34933A25EE9AAE667FE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ServiceProcess.dll	executable
		MD5: 382217652980DBA298E8FBB2FFD16B1B	**SHA256:** 007452C3BD57B65A5A3AD959E6D81BF6A5E5C976A82233DEA5837624A0324985
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.Encoding.Extensions.dll	executable
		MD5: 7D3C350F5211F1A046BC0F3B1B58B575	**SHA256:** 5E35E09F5D2190B54596B325B6E676D5429D282B891D6F729C5C57D77257BB9A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.dll	executable
		MD5: B7AC5691E02862CF6C20E7CE60708C9C	**SHA256:** 22E5A0C21E31DF3FE0CBA6867ED8745082F6C6C7D3AE1F32A1B7C84EBFF0770F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.Encoding.CodePages.dll	executable
		MD5: CD4DA6BCA08FBAE5B4262094E3516E35	**SHA256:** F98261ACD716950DACAC46A5028C5490FBF0148114E04F6D35A5ADA4E8245BCF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.Encodings.Web.dll	executable
		MD5: 8B3A4ED8D8C1E0F33ED3F5B1BEFD8CF9	**SHA256:** A5F55BF3597208E3983560928A90D6B084323D9AA60CB5C0CEE19C7D00F3C512
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ServiceModel.Web.dll	executable
		MD5: 13C69268D18B41E5BEE7294371274778	**SHA256:** FC5524188ADC1234697165B60071C7CF31AC641CF5C4C069C32AC8C502ACE26D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.Json.dll	executable
		MD5: 8C0E51A3348EA67FF49D80C7C547831B	**SHA256:** AD4FDB7A1D46DB6F63138D5C2D86613EDED5A001B0AB5B5E2C5C31E74998A924
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Text.Encoding.dll	executable
		MD5: 90813129A282DDD5A3A9F8A5BDD41DC0	**SHA256:** 3FCA11072FFFDA2A256ED6A2A39ED52AC27AF45544AFE680FE7D028A03726FA0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Channels.dll	executable
		MD5: E0D4EE62056078DCFD012CD346C1D2F4	**SHA256:** 889B95A95B10CD5427C5E19A10FA4EE3AAC9C732A67BF5669E9A954B56DC21C0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.ThreadPool.dll	executable
		MD5: 054506E89D9FE39404BF6AA8F45F6020	**SHA256:** 54345FDA384BDF4EDF2A33EABCCDC8B54BC47B9096495880F65A7039919AC1BB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Overlapped.dll	executable
		MD5: 28596F5C8D03C9698A187AA4B0A449FD	**SHA256:** D7C87633B74240B23DF84A9F4966FF30E78B3CE8171CBE06215F7395D96FF5EB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Tasks.dll	executable
		MD5: 2CD5B8B51D54430B1E0FF8011E7F4042	**SHA256:** 18C587A745C8D9B447123221412E8A52DC2116F1FA285A0E2EFA5B3B5B264DC8

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Thread.dll	executable
		MD5: 4EA45D21B81FFF2B0FD2E1A02677CA74	**SHA256:** 5BD03CB8996AE147244A68BD2BA49CC686EF78B2B58603B2269E3E9E3B0CD1C6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Tasks.Extensions.dll	executable
		MD5: 2EB252F95DFBF12E378F3A149BA2A661	**SHA256:** 4D72458768DD6188526499DAB4B14848DFA1F895F77F35240DB3DFDEF9B02BAE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Timer.dll	executable
		MD5: 1549D3617B46983063569B3EFA842F5D	**SHA256:** F672C67E6100662DF892D6ADC6678F427677BFB2587ADBD5C56DB3CA56D38EA4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Tasks.Dataflow.dll	executable
		MD5: AFDFA13015D0B454B4BCE4D4127EB2D3	**SHA256:** 1BDBBD62BC926F93F950D78544D0BDB5D0AE38F52B3E4B148B24D496DF2FD343
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.Tasks.Parallel.dll	executable
		MD5: A0F5736EEA2A28A8DCA22F0D7192D356	**SHA256:** 8DF45275CC4102EF6E81C5E92F7FD8B7126335AC5A601A126805195DFE901ED4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.dll	executable
		MD5: 02852F1DA5541227B8F42942F02115FD	**SHA256:** 8371D18E4F2A962235268B2688DFF1209051E7EE165C037AF6269BF081145D3E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Transactions.dll	executable
		MD5: FD111621321FDF09F7293223F9DBC8F8	**SHA256:** 17E4F2583C81C224432CDA28AA04EBD06CC575F976B64C0ECEEA19CDE200F32F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Transactions.Local.dll	executable
		MD5: 5C920FB993DE2D76F8C9ED35A6D18800	**SHA256:** 344066BC73509C44AC2A79D0786B1916E0EDCD750CC664E9176F6B45309577CC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.ValueTuple.dll	executable
		MD5: 5EED46BBCF21F7C3C3233B78CE2E1B52	**SHA256:** D491DF919B5D29C77092444D5EF00438FB6C4B8D03D96DF30F200C9D19304139
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Web.HttpUtility.dll	executable
		MD5: 3513838B2B083810F85E0F5A9D36A89D	**SHA256:** FD7563BA3685798DD6F47172DD713F7A1C34CBE773E68D69A32ABCA306FFB6BB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.Serialization.dll	executable
		MD5: 42188C3899B7C9F9A9A94E264B188B6C	**SHA256:** 01A40A8A0F1A331B85762C5FD1A75E734FCAD3A2D11566F1D18370985028E1FE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.Linq.dll	executable
		MD5: F2427B8F56C2E363A169D624EC34A9E5	**SHA256:** 888C9836C10267D28B583563D8D4B70257007A5CE418EA1A5E6BD802A6EE0D86
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.XDocument.dll	executable
		MD5: 62BEF2942539234C5E6D78CF9F2F4660	**SHA256:** A61385CBB7424EE05A5616D1208DCE61A7CE9F2AE41C0B12DCE7FB77E4A1ACE5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.ReaderWriter.dll	executable
		MD5: CCF5F608CE09F51E54C81E91D5C603B5	**SHA256:** 3FED3204B82703220B9461BA0E866AA133AE01E89A24CE4AF895403AC01476D1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.dll	executable
		MD5: 25B1E9D1573ECBCA5E4AF4281F9C4913	**SHA256:** 82A0E20FBE98AD47C8541F7B23F5B214DFC6F71C55BDD74BC61F84BCB6D4FD1D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Web.dll	executable
		MD5: FAACB669C30765D474BEDDE3A8205506	**SHA256:** 0C58596E682270A53FDD10084430486160DFE71094DDBF0CD7EE603483CCEBEE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.XPath.XDocument.dll	executable
		MD5: 4DD59B92F871CEFE20D477A416D4FC6C	**SHA256:** 3808F0298E5ABB95C4EC3D8C3171CCF6230EBEE70EB0510A635E8C99E6D59685
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.XPath.dll	executable
		MD5: BDE2D38FA3E14FDA5497052C5E459CA7	**SHA256:** 02DB2ED79ACEEA9F6F33841B9A983BB223EC7CB3AEFD69F7A5DA15A721D37D33
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.dll	executable
		MD5: C1687B847299FC5EEFFF3287A4F91FB0	**SHA256:** 338D92E9948C42CFBF1AD350DC8B632024340076FB5316B99C41AC0424AC9DF1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.XmlSerializer.dll	executable
		MD5: 731B79E153B8012791716CB432769220	**SHA256:** 755596DB1090194B1FC30604734A37253A3E6EA0461493C61910831ADC45E3BF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.XmlDocument.dll	executable
		MD5: A01FB19BE20787FE046871F323051522	**SHA256:** 7ADB6708F2214FCB4E5809C92179E6A7027CFDA76E3755E42FA8F3256F2B3BCE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xml.dll	executable
		MD5: ACE44EC817A18F5B8F43BD637C1F6FB5	**SHA256:** E0BFB789B207BDE418FD0349B308F2441ED88F810D96E9895FEFF4FF3476368A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\netstandard.dll	executable
		MD5: 04288D07B365A387C48C175E11A668B1	**SHA256:** DFE8483CC044C39482070816B1A7A9DB843CC5BEE0B0B1A78649DB105C521516
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\mscorlib.dll	executable
		MD5: DAA820340228F49F31F0FF71BB903730	**SHA256:** EEFF207E786245D3A2F45A78A193EF0B695E076B7D5D17EF61B6785090928C56
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\DirectWriteForwarder.dll	executable
		MD5: 1407596DDB23CE07E5E70758C2904FAB	**SHA256:** 63F48D0A992616CD031B41EA7AFD91007FD7A10EC7FB3369CE6CB7DC354E9942
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.VisualBasic.Forms.dll	executable
		MD5: 0A1B118EFD3B4CE0F0DCF3A38E75DD45	**SHA256:** 4D9A396C329362D31DB2326446B9A9C6B99A1C00EC4AF97FD4A5C4EFD33D32A8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Accessibility.dll	executable

		MD5: 642B9476A24D757D2BE069571983852F	**SHA256:** F5A9B56BC8740BB0C24B1F1FED21EBC74237B75E35D416908165F2AD459F4F95
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.VisualBasic.dll	executable
		MD5: 0BE0631E4E0E48D2DD74CC54D1565D48	**SHA256:** 267CD27039507D7536D8E2FCB79D9E50EFC49D629374C1EE6A079F82C69C8CEB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework-SystemData.dll	executable
		MD5: D470AA168D57FA8FD72A20E92C10DFF2	**SHA256:** 6416FBEE5BE5C1B2E28327866AC3D538833170499ECEB7D9FC3DFFA36ADFF052
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.Win32.SystemEvents.dll	executable
		MD5: 975B5AA408B869DED27644BC3FA7E308	**SHA256:** C12FA5595385653B7E4B8E18B44ADFCA039D6FA68AB82C6C5434767AF9E7C524
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationCore.dll	executable
		MD5: F284398A24062628E557FC5EA47BF5D1	**SHA256:** 41B6B8326D45AF4941DBB08BFDC266515514553B1977324203DD1E526250D704
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework-SystemCore.dll	executable
		MD5: 919B52E55F6DDE86AF4EA338A4D49C46	**SHA256:** 2BE019F1E8D9B30E33A51E1E33ED81A9C68B93E8D8D1C713B74B1B5E82D8C7E2
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.Win32.Registry.AccessControl.dll	executable
		MD5: F58CE98BE0C399DBDBC2036B01D141E4	**SHA256:** 817C9D93411406BC9BD4C2A64041F2C2B36FA88DBAE2F47A648A4556E028A4E6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework-SystemXml.dll	executable
		MD5: 7D5528BBCC4F599DF1112611204C54F6	**SHA256:** 361AC611156192E9F77B7BD9E38BAABCEEB37ACF0D3865C58484F43C2DF32CA0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework-SystemDrawing.dll	executable
		MD5: 7AE81427AA104B6FFAD34748BBD31E3B	**SHA256:** 5CD3C2341587707102B0F3DBFB53F167A305D0331A74C23AE35D1109995B84A0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework-SystemXmlLinq.dll	executable
		MD5: 91AF0723297F184479ADA62168109776	**SHA256:** D156582C3D1C5D242B6505B52797F6924D9DDB71CD54FDEA98A2AF352C9E172D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.Aero.dll	executable
		MD5: 350E256B98C00835B8EB8804BA698B6D	**SHA256:** EB23F7019F39F6AD88BE6C48DC61A4FA13EFBE36C64877EAB48FBFEB72C71284
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.Aero2.dll	executable
		MD5: E4EE2CFF564CE8463001486BCFB29C93	**SHA256:** 2D186859594D7F5F7BE1587E03DD71E047F8F25253A1204C2585A76843B77CCA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.Luna.dll	executable
		MD5: BA0BFC69FBB0BC26FD8036323C3200D1	**SHA256:** F0914F521C141FD6973513162A063ACF7717A89412E6DDD5D1DFFBF3F54A7365
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.Royale.dll	executable
		MD5: 0A06416EFF267C6057DAD8A92EDB1E63	**SHA256:** 0E271ADB58AF9E7598A7B422D910D8B06513D5F2F021002A1944183D87258A34
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.Classic.dll	executable
		MD5: E7DAE4DA1FADFD40F4FF8E7D0435165F	**SHA256:** A5E0C7D917A7F24DC5D1F002307B7D0C6E98EE2788AF5ED21759598A29A40453
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.AeroLite.dll	executable
		MD5: 609D2AB41C17EA7C5B7C83C8DDE007B5	**SHA256:** 5DB34F5A1ECCC90A8402825DAA2A9AC45CD7ECEF42773E37599ADBA8B30C6A89
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationUI.dll	executable
		MD5: EF61EC70327916C7CD17CAB62BC9B74F	**SHA256:** 8C9B81A79650D3D1A17D37F60756A277E7CB85F6CA69BBF613B5291A4D39F6AA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationFramework.dll	executable
		MD5: D4B260A0EAA3A81497CAF581D043877A	**SHA256:** F708D0126CE5A9108E806A361C44709AFF99C901E5491CC3FDC7C0A5761C2A5A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Design.dll	executable
		MD5: 5F1C6E3AD04E8E035AEBFF4C1F706F0B	**SHA256:** AF88FC4A167361EE72273F0A3BA77789A0F076EA9D2DB6D474196003E8495113
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Configuration.ConfigurationManager.dll	executable
		MD5: DD656AAA7844121CC88CA89217C646DC	**SHA256:** 6D1334A46225B13B9B2F5E788FD82FB41EDD99EAA392DE8B28EAEB518BD65F8B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ReachFramework.dll	executable
		MD5: B608BE493E86964DEEC607F9A49F2503	**SHA256:** B6B654318C7F9D106B98DCD99DFFD4737B0D9C34CB95A10DC629476261E1F909
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.PerformanceCounter.dll	executable
		MD5: 252C7970F3AD55769A92BC68EBFF233F	**SHA256:** 1EDA05107276F62FDA38E95FC53C3E86FEFCFE3EB50F36BE06A89E729CA44D61
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.EventLog.Messages.dll	executable
		MD5: 9801EA6567CD6C9831374BEB0CA7B6D3	**SHA256:** 2691CD89AFFE1990B3A624836BA33B81A3CFFA47BE9EC469ADFF698E1632E7F9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Drawing.dll	executable
		MD5: 05F2E50E251EA2D6C0F0119EFB3E8638	**SHA256:** D015184D3825DFDB2CBA7C385B1BE905DB282C3E1F816FA10B8C55D1B46BFD01
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Drawing.Common.dll	executable
		MD5: DAC0E91B53936EF1C230791AEF1E331B	**SHA256:** 9FDC9693FB2E350AF95096293635CD3F6157AC210FE1F111D84E396BADF631D7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Drawing.Design.dll	executable
		MD5: 9B5905A9FCF7EB8514054FF21A8EF2B2	**SHA256:** F66E07CE2EA735C5C6FB0E12B13302B6B2105C1ABB4647E6759B7DB603CA801A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Diagnostics.EventLog.dll	executable
		MD5: 1A04BDE4F2DDB101180C64E4DBF362C4	**SHA256:** CF86D3368E668D8965D5518A56CEC764517ABA06E14ACD5B8D24B846339D1538

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.DirectoryServices.dll MD5: 89E02727ACB317D3775482CB2CFC6EDA SHA256: CC25568D437F5FB61973D5CE0B0AC85CD0513C2AED516414D1353BA74062A0C5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Printing.dll MD5: 85EBE6E05FB7FA6CA60975EBEBE39068 SHA256: 62671B404E6235E7B95ECE3250B8C077DD99A1B47FBBE1AEE996677937EDAC7E	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Resources.Extensions.dll MD5: 16170F7BA4F9FAA98A6C5F68B060704C SHA256: DE7954EF0C33ED429C7B8DCA37D820EF9F7561DFFB6EB43535EE3355F716A02F	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.IO.Packaging.dll MD5: F3BA798C01B05830322932C109779DF6 SHA256: C764030FE52512F04161BF12418AD1BB883BFEAA072A474BA15304A52B3FB143	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Pkcs.dll MD5: 743A6206BB88DA7F0B98F70025DD964B SHA256: 7A6B65710F37A9991BA10B432EFB5B83B3AA92FEB49122F92BEE3D54836ECC83	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Permissions.dll MD5: 69B065A979BFAD69AB8E09B0F92C3F5F SHA256: 01574A3E246F76C96E29EC062CFB71C6E06EE2366D4278F94C422A1D862DF87B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.ProtectedData.dll MD5: B479DBC256A679EF4FBCEFBB525D40D9 SHA256: 734A599594654D9B76CBC87A145B6BFF6A080924B61DC5D5F10AB5213B27FAA3	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Threading.AccessControl.dll MD5: D81AE1370AB972FFB3E25C537D4DF0BD SHA256: F87F8245BD045E6CA419ADA98E0CF470BF44113BE5BF9BCC86ADE9857A1FE915	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Security.Cryptography.Xml.dll MD5: DF3446D3FF6BA1704CC854B375808859 SHA256: 22E90D319A1123C9FC364EF3E45664594B88A22B71F45FDD1B4280515D4A1C85	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Extensions.dll MD5: 9950EFB6A9985675D0196D0076D62682 SHA256: 5D048E765383D1CBFAC7EB35424691E9F9409B2B0FA0D7D032AA5AD1E2A9BC4B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Controls.Ribbon.dll MD5: 269C4D4ED1DAC44C12817340B8B1DC4E SHA256: 33A7E65DBFEE50EE759211D41983C578E52AA03943FBD8D231522F693BF2DCF0	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Forms.Design.dll MD5: 00429BD4E7C227426FA5752EF20DC8D4 SHA256: C1591FB30EEAE9BB64A20BD2138140898B47F69C25B205382A1A2CA147A93073	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Forms.dll MD5: BF0A728D57CE538A3092D6BEE2D6BD20 SHA256: AB9C4C51C27D5E3B221C963B471153E995E89AB9E51D7E34EF7BAB4A495EC9F7	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Forms.Design.Editors.dll MD5: 0F562C950B03344ACCD3D87675E0778C SHA256: 201FD1771DC36D62B005450468507BBDAFD5ECBA80EAACC22F79A1500950BC99	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Forms.Primitives.dll MD5: FC0D34DAD824FFCF0AE764BDBD13A33A SHA256: 2D13049EE36D348716FD593732DD91974D4D298A50BBDF941D41C9B217092234	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Input.Manipulations.dll MD5: B26B481D565CC2BDEC9AFD4A19DF145C SHA256: 7BF232323FF0901602D89A2724E19A8A16E1623B6EAB25DC9E1AF34E9F623912	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\UIAutomationClient.dll MD5: F483C93D43D5F68673C5BB550140AB99 SHA256: B52F4212D5006C28671607EF1F5C4F0DB45889B4AC4D1693FA853AB0A1303773	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Windows.Presentation.dll MD5: 0242874F2D811D6AFCB9D2250E65DEBB SHA256: 500B7C39877C1587F924EC0BB3767146DDB60B1FFBFB72440FB87E75CDB99970	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Xaml.dll MD5: 51D160699F72599258B121E851F5DDCE SHA256: 84A0A304B9652913EE6F66780D5A9A1580BD4FAEB26559A50CC2E1B58BABCB32	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\UIAutomationClientSideProviders.dll MD5: EB52C2ADDAC00A462B5159AF259E298C SHA256: 8356753A0638D335FE846E445B5E9029FAC2E04888CE686C3A1F1C44F7D6AC40	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\UIAutomationTypes.dll MD5: 02D2D572B437E6C62641D7D754CF3045 SHA256: 35220473EE5A10F9A02966F3FCE2BB269D90B8C94B7B8D1072DC87B27E9F6D08	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\UIAutomationProvider.dll MD5: FCD9E2EBAE052F5D60B043CD13C597F7 SHA256: 8690986A2AA44B1668CF8213A5813122FEB19C04B7B4B10A0F7B4D4A21617FCD	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\WindowsBase.dll MD5: 525DFECB94E08CCABDA0C14AEAE56779 SHA256: 05BDC00C08307C1E3D903E16E8325D7938108A7D2F31D607EBE69769FCC7398E	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\WindowsFormsIntegration.dll MD5: 06B4287C6A0F1AE8072579C11ED4D9E0 SHA256: 531FDE9EE6CDE174AE253FB014131A2833DA2715C826B7310F696C5686F7510D	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PenImc_cor3.dll MD5: 387EE0EED91752BA689D7D55D7193CBA SHA256: 10D2A711939AE082FD5D5525E2398234C574B5CDA6E70B23E756F62F4438031A	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\Microsoft.VisualBasic.Forms.resources.dll MD5: 9E69845983A379C87E8857C52FA0BA6D SHA256: 9B43A453BD6E193B4890A1E3CD74B533885562E0FC67C25709A3C5215BF84569	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\wpfgfx_cor3.dll	executable

		MD5: 24EA1814E6701927B9C714E0A4C3C185	**SHA256:** D2EBEDC0004D5E336C6092E417C11C051767C7DCBCB80303F3484FD805E084AE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\D3DCompiler_47_cor3.dll	executable
		MD5: A7349236212B0E5CEC2978F2CFA49A1A	**SHA256:** A05D04A270F68C8C6D6EA2D23BEBF8CD1D5453B26B5442FA54965F90F1C62082
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\PresentationNative_cor3.dll	executable
		MD5: E67DFF697095B778AB6B76229C005811	**SHA256:** E92B997F6F3A10B43D3FDC7743307228AA3B0A43430AF60CCB06EFA154D37E6A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\vcruntime140_cor3.dll	executable
		MD5: D6AC34C46569EFE379B58F9B7BBCB6FC	**SHA256:** CFF0CED8B2193ADFF2C06119F70A037B6B79B6FC6C4A19664D4E42BC1C06A9F6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\PresentationCore.resources.dll	executable
		MD5: 26D37B70BFA07B2A055B82BDA48D52CD	**SHA256:** F23EB0AB972B0BBB8BF449E75AE068BC824E176127DFEC1FD58140E15789ACCF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\PresentationFramework.resources.dll	executable
		MD5: 88CA6F75E5CF6097E0810D7B86A443D2	**SHA256:** EBBC31C22C063D19B944A3B393D16DE2EB212FEAE155CE876854F5E5AB594656
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\PresentationUI.resources.dll	executable
		MD5: D7445A5B4A40801E05CA0F5BEC40FC65	**SHA256:** 69DDE39C633DAB2BA842C354A06081E702A82B47E634811F50F9A5B7797E4AF8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\ReachFramework.resources.dll	executable
		MD5: E5EDE50E22C4F755D7F845FC8276C925	**SHA256:** B091D6C3ABA54741A3A3BB001E5EC143819CC91850D5026A4072FAC76D6074CE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: FDC69F37866ED1E5D4AF6507AAA89731	**SHA256:** 6676AA715E8A766F7A11B68377D27648BD9C44B6E9C9523A6646C8029D69F0E9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\UIAutomationClient.resources.dll	executable
		MD5: 7B65D50E68EB56890B29402696254844	**SHA256:** F5A1F4F3F7E078D82246235940FECA568836C3784CD82016B70A3B12E7009FB3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: FD48DAE9C99C33A4A17796E9C74F2231	**SHA256:** DA25BC1328F7042C02C944D03DFA427479FCAB5A63B798CC91E9BF8208092E35
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Windows.Forms.Design.resources.dll	executable
		MD5: FFEB847FB1ED5B289C549D74E9B5F629	**SHA256:** ED762BB06DB02D2BCC9FF6C8832D05AAB15D53FD27914DCB449C1E41457B178D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 533672E616025B05AD404016A00C1EC3	**SHA256:** D93E45533C6D2691B421D607E64E2C74F1DE2074D1AB1A8E4B8F55337620F363
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\UIAutomationClientSideProviders.resources.dll	executable
		MD5: 66600E939E4AB796A823DEEA310CAB7A	**SHA256:** 860B7DECD7493D9A57041DBD61EAA630E0743DD7B82CF1890A16C98A3B38BD09
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Windows.Forms.resources.dll	executable
		MD5: 8B6C10AD8DA9EB54742612B5E3A82EC6	**SHA256:** A852D050793C3FAC207A87F9A586ADD09F5AC66F5C1E89C0BCBDDE19D4BA4E3C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\UIAutomationProvider.resources.dll	executable
		MD5: 64551036FEB2CB623FF9F241F08DE77C	**SHA256:** CCBB63694107E33B546BE001A9F26C9FDB5302DC51B1109859E0D7F70105ECD0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\UIAutomationTypes.resources.dll	executable
		MD5: 2AA3A11B8FA56202913FD28A3444D5BA	**SHA256:** 145B1DFE2F372B733FBB836459A7A8914990C72EECFD4D8D729FAC636C6A61D9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\System.Xaml.resources.dll	executable
		MD5: 431FD176890E9D9DA2A2C1A38DA33DA5	**SHA256:** 6C8BA1A2390E78AB13F3CE78C2DDDA4F794815E2188FED0D6CF4035AC7209540
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\PresentationCore.resources.dll	executable
		MD5: 9D9C3E23120B2276D61F8E05AB98E709	**SHA256:** 4E22E68D3118A24D0FA3BD2CFCA676D241E531BB6C8A1FBCA354F84A33A910C1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\WindowsBase.resources.dll	executable
		MD5: 4E79711598A6205C1ADAB620844F63DB	**SHA256:** DC453A536F8FCE7CE32A99C2EA24471A335855FBE61A956F785B99B683546907
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\cs\WindowsFormsIntegration.resources.dll	executable
		MD5: 6C4527D2DCC45CA078457F3D601C99B9	**SHA256:** CC9ED41D01BBF9C127C62C3208CC555135DDBCFB23902FB1ECD09B44F66B1550
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\PresentationFramework.resources.dll	executable
		MD5: 2643771C950B09E153A8E73C78C4A065	**SHA256:** 71467890FB0DD965A324C81BDD769EF33D9A45A5355428BB4E49B99FA2084BF8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 2BE14100FD6898814621B999D7A9EC1D	**SHA256:** F95E58B6BA439B09DDA364F2E7498FBED8E2B4193D44149EF8A4C727102AB54E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\PresentationUI.resources.dll	executable
		MD5: 76EA3EB894A09D7894ACB267E177B654	**SHA256:** 3B9306B394326A324337BEEAEAD369B1EB8F9BE123D5207275B755FDD3DF0A9E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\ReachFramework.resources.dll	executable
		MD5: 82E4ABDC5473C623E93C0FEE95CF8BB6	**SHA256:** 173547EE7DEB966B10E340F5EB3D6C1E8ABFC665D2FA985FC769956DFEFB8641
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Windows.Forms.resources.dll	executable
		MD5: D5B4C510309CCB58AC96AF8816998DC1	**SHA256:** 262DC9A71D39E067612F66F330517BB7F531137F273046646F5850C1D30DC9C4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 65E3A036A82F3EBB0577108B570111E0	**SHA256:** B090363C0830BBB28E96659E56E5C409DA98B3E866CE9C97B6371FBD1A835795

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 73C8103115FFC7DF5AD2A092BE67324A	**SHA256:** 0F942F89D3F86858D2F27F6B4093A3FA3A88BF50CC69B4A1156E9E70D3FF467A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 6973BAED5C93DA183FEE6A522DB9C2CE	**SHA256:** F69C40C3D69C52C1D65061AB8D6A14A8B8D615347478796D89BC372AED3B6926
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Xaml.resources.dll	executable
		MD5: 10C8548AA65B7D661F955A499C0D2E04	**SHA256:** FD3BA68057265E25830F729FA48656A70FC8912AEEEE6DC8982EA68516012202
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\System.Windows.Forms.Design.resources.dll	executable
		MD5: 79C16BEE010BEBC3DFCDA970AA4EAFB7	**SHA256:** BFDAE27CD991DE5CDECC5975C2DDDB009CA21AAC1DE24BA8CEF7BF230A9DA208
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\UIAutomationClientSideProviders.resources.dll	executable
		MD5: DC0CC2F36E6740A1FF17FEDCB231B193	**SHA256:** 5B5C11C5F572C04E9F8FC15BA3B778E1A74EED7251E768E0F8BA84CD1BA7AEBA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\UIAutomationClient.resources.dll	executable
		MD5: C9F1248BC4B5B9815FA619C5D4A2B5DD	**SHA256:** D9CD040E6433EC1A46000D745CD1DFD1F9EA2220241651EBBEBEB739ACF51ADD
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\UIAutomationProvider.resources.dll	executable
		MD5: 82BC82195CAF0183079EC461F2082F3F	**SHA256:** C089A59AC32CDA1E39E68D59E92FF1DC7AC7612F80DF5A7F6605E9C7AFFB14F9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\WindowsBase.resources.dll	executable
		MD5: B16F9D1FC0B2CD8309E00DB8BFD63A58	**SHA256:** 16C8B160FF3410446EEB2A0FB4528C9599C7F8DCC9419F3373972895E5C0C6B3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\UIAutomationTypes.resources.dll	executable
		MD5: 8210478371F0426C8E958C68D32BA68A	**SHA256:** 5AFC46BF470B4DCDF404271CEDCFE578674D46BCC5CD379C0CBA6A52C3668B81
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\de\WindowsFormsIntegration.resources.dll	executable
		MD5: AFB0AA44EDA1EBEC234DDBAC84A6C6DF	**SHA256:** BFE1FD9463EF037DEA7569F12739DC2C57FF2F2AC459E365877C644A5D171E94
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\PresentationFramework.resources.dll	executable
		MD5: 2475085E797810667340D0DCE4CAC594	**SHA256:** A1A152D662F11315ACDD33AF56A3E5BA49942F7B116BE746DA8FABAB4B20069F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\PresentationCore.resources.dll	executable
		MD5: FDF08589FDD59D365186A5641E965F41	**SHA256:** 8C2A52E6BB6AB52A25B1ECBC31987F90ED99FC4480F4DE92106A1C3B620CB5C4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: DE6F90532CC227F3C24BDB628E051983	**SHA256:** 5D7B3814F538EC9F1F19B8DF1BF36CBD791893EF5169393E22C97AF24C265AA1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\PresentationUI.resources.dll	executable
		MD5: FB9D7F107458A0A35515CC6FC4FD3029	**SHA256:** 75ECB64B0C9E222168FF1270A522F46FABBB82F50ECCC3BEC14A13ACA0283F5F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 1F2B06F88862E4AB5E01792440007A97	**SHA256:** 951645161C4C10A0D6F3B7A6277C99A38C56304190384483A78A588BB2A44BA4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\ReachFramework.resources.dll	executable
		MD5: CC9E28CFE3F41AECBDFD7BE6EE74029C	**SHA256:** D0D8895A946C53646EF9F536613522516A9A71F5CF293AE7224C6FB7B88AB0C0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 1A961FA867B5107B90FE1B30A54EE26D	**SHA256:** 049E14A2FEAEAB840A5969D4BA3FA3825B42A2D5018C5385EB03336F2BCB0D0F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Windows.Forms.Design.resources.dll	executable
		MD5: 3EC66106F924BA5D1EC743DA90A0A2FD	**SHA256:** 0A87D7324461C34C55AF4612474E13DCC29FE44C5B2B2FFE718988AF8D3A6E3B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Xaml.resources.dll	executable
		MD5: 16BAACF689ED14AA64555B51F268CC0B	**SHA256:** C1A78BDAAA2137CF150130354BCCAD0A904946D5292C6584E0BD31CDD444236C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Windows.Forms.resources.dll	executable
		MD5: 40F20DD25EE8915F78197964705C9266	**SHA256:** 83B027302FB418EFF4BE091BA40D059C0DE6C5382C6740AFACCC2DFFB311011A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 8A5167D72E6B65B7369DC6F023E8EDDA	**SHA256:** 757C0F435EF19CA31DD0C2327EDF0548961C9213C903B5A57C89555D98424C63
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\PresentationFramework.resources.dll	executable
		MD5: 1C7BDA5B411D8D123A74C7FDBECFFE1B	**SHA256:** 3EE283D18CF039C56D7DEE74CE992688521C8F21D836FFAF9CF6B40EEAACEA54
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\UIAutomationProvider.resources.dll	executable
		MD5: 5FB98C2E38E206FFD96B72D5D20BA781	**SHA256:** 1181F3F06176ED29D20D9887BE63F334A36D7C03243C07C721900369D9A2C479
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\WindowsFormsIntegration.resources.dll	executable
		MD5: 4BE9AFB7912438F20755A3AC34E60AB2	**SHA256:** AE992EA475FDCEA47AD65BFF4C19936233B807F656B53C826DA9CB67E93736A6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\PresentationCore.resources.dll	executable
		MD5: 87BCE879A361CF95889817A52378D6F1	**SHA256:** 386A1F45938F666A439F1B6C8CC69F9F12F5EBE5F863F330E5661738C5916DD5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 0337346EE4A43E3CE99FFA173C560F6F	**SHA256:** DAD6DB3C8FBA85BED41A376F7A04B62C6E80D0190E9B3B892A06BD45DF278BEC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\UIAutomationClientSideProviders.resources.dll	executable

		MD5: 9C507FAF5C3BA03AD40E1A36CD10346F	**SHA256:** 85635802618B51938CFD8A87CBA5159058964A8FA2EDEBA150082499B72805CA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\WindowsBase.resources.dll	executable
		MD5: 854496E7D58AAC1D9155DE3A739F1EEA	**SHA256:** 84BB8F9498345DAB648D031DF8FDFA70EB384D5EC6DFDF8C88827E6CFF404471
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\UIAutomationTypes.resources.dll	executable
		MD5: FC456A18973B4034BFAD69B14F4E7393	**SHA256:** B10FC800D32385B4165764D4B02A095E9015FBFA8B358D503068B6AE3EA9E7EA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\es\UIAutomationClient.resources.dll	executable
		MD5: BC803912851D050D8D8DF5450164F33A	**SHA256:** 015DA297685E03FE3A0C44C655DC97431B49DE5A59BF822CF0B72E207E98A252
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\PresentationUI.resources.dll	executable
		MD5: 4856E6465B2A55B6E955439AA823614A	**SHA256:** 8B3DDF03330BF9D477197BC25C881876C6A7E1DBEA3D6F0D8CA5E2949507E96C
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Windows.Forms.Design.resources.dll	executable
		MD5: 0AB5AF52C92EBA8FA7D812F69C63FEB1	**SHA256:** 745ABE1AE4B2257B84ACDF4BCDB20987C67786B89FC5F4D194BD9A0874DE28EF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 2BF31AE92194182B3A3AF6D9F5DE4532	**SHA256:** D17411E3AF5A2003CB61527E768EE8DEE34150C0350F8EEDE2193D9EC212779E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 1A196EE063AB30983A8E3F6CA694CFE0	**SHA256:** 6FA32728A7C4359A565ED96ADA8C8C36D78CFC6A0FA98DAFAF7EFAF690E9A616
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\ReachFramework.resources.dll	executable
		MD5: 083B6644A229B9936D91E2C0B1D0EA29	**SHA256:** 7A28C36B9644693141578DD12F8B3B7D4898C5A62E1AB5F449DC52ED66F83C60
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Windows.Forms.resources.dll	executable
		MD5: EB23794BBF3DE85857F43856494329A5	**SHA256:** DE4D230DE6D48562D695FBF3B3761126FACAFCED66FBED6514016B8E68E89CAD
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 15E225A0E097CB60284F2DAC80E1C9F8	**SHA256:** 3D25D8634C15623FB67A9516E7BAD74BA5D0F8E74067D80ADE437126D976E2B8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\UIAutomationClientSideProviders.resources.dll	executable
		MD5: D2DC39E459824BE85319E18C74F74FBD	**SHA256:** B0D4EA78C3F6B5C9790469D0DFB86850F9EE7BD0A02A533810C4A12617280912
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\UIAutomationProvider.resources.dll	executable
		MD5: A7244068C5B715A15951559A494F1B85	**SHA256:** 38023EF4528745B58671F1F276141BF7374D1E408017F12B29C6AB32291612B6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\UIAutomationClient.resources.dll	executable
		MD5: DCD8D4F1A79F3BA57688A767E0527A2D	**SHA256:** B9671734B0B7376B6EF39CBE8E2F4922A43CEBED4B9CD5F49C9D5954B2752859
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\System.Xaml.resources.dll	executable
		MD5: 1855C00BD7015EFDEFA1E4C38554B772	**SHA256:** A905FD078D1160B10EB9282DC0F51C63076DF32DF2C965EA7C224B27F8EE11BA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\UIAutomationTypes.resources.dll	executable
		MD5: 7E40AFA29C993CD1699631250A6E3EA4	**SHA256:** C5F5E2F71547BA6ECE66C59A75EDE5AC3CBF0EB3B0F9DD3DE2B490D3343FD2A5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\WindowsFormsIntegration.resources.dll	executable
		MD5: 4CDE43F8C742DF5AB97982D415C7E993	**SHA256:** 3906245D41082B803FF767316CD9D2BDDE70225FD576C0783359A3CCD3E0B5AD
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\PresentationCore.resources.dll	executable
		MD5: 15461FED964A5BE396F135B668361898	**SHA256:** 10AC819C6932D63B51C0355F18503A69C2B6DCB21CE5FCDE88AF3E19029D8FD9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 37EAF707F269A6878B18E7AD817904D4	**SHA256:** 9E5F91438DD3FA2779C2E754DF8A09B5A62767E790AA982A367ABFA5ABD89690
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\fr\WindowsBase.resources.dll	executable
		MD5: 37FDAD51D9F32D6CB992283F2ED876F6	**SHA256:** E6651CAD7D96669C39508F2663FCF29398E1C07DD91545A545241728EB10CB21
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\ReachFramework.resources.dll	executable
		MD5: 3AD68E1EDA3891DD9EABDA3315534AEF	**SHA256:** 408746BA26293162A372D6AE5F062A36FF48A541B0C88AA033FC0AA7253290E6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\PresentationFramework.resources.dll	executable
		MD5: 1A8803747F50CC909E87A25E696C9335	**SHA256:** 8F08FF912D9982E4B61033ED463570A16C4CBAEF8498601E70E3CB47ED7C20CF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Windows.Forms.Design.resources.dll	executable
		MD5: 7E1AFF4F280C381FE39E69FB5F6B256B	**SHA256:** BB93E310863069D22B771E76EF9E41A1EF87ACEC668B7A01F1EB456E17AF2883
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: DE7DBBB0CB8FB553ED97E4EB3EF28C5A	**SHA256:** 01B24DD30AC227F4421F80EBFE2CE22F4F0A32B1D7E21EEE161E7455B61680C8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\PresentationUI.resources.dll	executable
		MD5: 8387284ABE6DE4EF53145549BD3BD934	**SHA256:** 289BEF45414C68FE9B97FB5AAF4290224906EFF297608A1241AC20C73427212B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 36B38D0B19A898B449AF76302DF05B46	**SHA256:** 467CB1CC70089AA3B55A5ED7212C58E45AB2932C67A649A9D2E84DEA1BCBBC31
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Xaml.resources.dll	executable
		MD5: 008AEB7B8A7D38B0645CE08ED0E7B570	**SHA256:** EB4E43824ACE7B6C28B72390886076552DBF6473EE186AB5A23F33157863E86A

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Windows.Forms.resources.dll	executable
		MD5: 26047E459B1CA7134E1633816D90A0C2	**SHA256:** EDDC8D3BB06EFFF8308C1AAD6839012B008479EFD7C4A9B4A6B35300F7360665
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\UIAutomationClient.resources.dll	executable
		MD5: EC23B1DF92C2D71486040626D2618827	**SHA256:** 3E4D47DBE35F00B2A555D71FE4E464B755FF2408B0D1815BC71B9FC40763421F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 957E8306F1D7EED19CB4945594989FF1	**SHA256:** 772775584788D0CF2CD6FE5F62332ECF61100430379352746 3FB79740CBB9E40
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\UIAutomationClientSideProviders.resources.dll	executable
		MD5: 0F30C7F772F8EED79474231DEF7FB7A3	**SHA256:** EC6C7B36776937B9FF76CD3DFEDE5619E17191E5B50051636768B2B8817FADAB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\UIAutomationTypes.resources.dll	executable
		MD5: 77E84923ABEBC4C1620F9D61F01621B4	**SHA256:** E2B3358759C6B42692D9C79EF92164604CD30E0BB740DE0353F8674FB0F08972
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\WindowsBase.resources.dll	executable
		MD5: 67F380AECF0B89848EB5127F170C1C77	**SHA256:** BF109C4D6626692EAB88B6CFCDAB2C233F5054FF79CD7769910721F844755008
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\UIAutomationProvider.resources.dll	executable
		MD5: B108AA27D32A821551A1EE4C5887390B	**SHA256:** 1CCED87FA31D8179D3510A38835701BE6C8E51FBD4ACA13059A952E32E4A95E7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\PresentationCore.resources.dll	executable
		MD5: 0C497A3E24C06CE186B77102C9D07039	**SHA256:** 3FB2D3C78EEBF2B4969332CC7DE7C70A7817519D05E3B2188173E4AA5AA290FA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\it\WindowsFormsIntegration.resources.dll	executable
		MD5: 41DFF151FD73AFA016E37C8406EFBDF2	**SHA256:** AA4C63517822145C2FE981B6D7B2157BCC7AD1DFD82743CC31E36C8654724DC9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: E44910981CFFCBAB492473926960FFD4	**SHA256:** BF3C8454ACBC8672CA8E4F61D4C0BFE65533D44F414272A222A0ACF0CB6CE460
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\PresentationUI.resources.dll	executable
		MD5: 0D043475926F2DD1F9AD52D72F939C1B	**SHA256:** DC214B1A2DC5811ADA6DA9C5B728EC85319BB2A29F0A0ADBA8D50B671FBB4934
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 3167E8DF4513B414701B95ADB0419A73	**SHA256:** EA64B056A716798DA5ABD762883839188CC01BBAADC42C3FEE29D940F262D7D0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 1620D24D27F70FAFCF63F77A6A0B212F	**SHA256:** 8B42695F219F29705085E5E031194604C7FDCB8CBE9E123CB1EEE36190AE00EF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\ReachFramework.resources.dll	executable
		MD5: 6F21F165EEA1FDC1567BF39252F5D117	**SHA256:** 13CB9C867EF14D3560074389A81FA3F7B8EA602C8CA5C80F80D44476697A90B5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\WindowsBase.resources.dll	executable
		MD5: 213D0DD1662E057BB04B075107E4C3FA	**SHA256:** 3EA135224CD1286D5D5048417CE40D0A605E607A51EE0A9FDB8544AF7E712D84
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 9EDF8FD25088921B327D7253EF2B94D4	**SHA256:** C09DA36ACF09E6C9E871FA9D4EDB2DFC3F80E02A96FBCEB9B3BE00D6AA320A2B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Windows.Forms.resources.dll	executable
		MD5: 42FE6BE23BF87ADFF713E555749D1442	**SHA256:** 2732D010C5104E1D637A2B7A759A6E3E8686FF5C620A9C03FF87DC9EACE69789
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\PresentationFramework.resources.dll	executable
		MD5: 17BDD30AE4C14C993AAF3515C7B9EB34	**SHA256:** 2C60F94B3ABA41C9E6815AB86F07FE931301713599 38BCDDC14ACBE5A49DABA2
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Windows.Forms.Design.resources.dll	executable
		MD5: 948150A933D7411FE959B27E6F59C087	**SHA256:** 4114457467E51AB95771D943CB277B908613C3FDA96BCEF2645B780B441A6F33
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\UIAutomationProvider.resources.dll	executable
		MD5: 35C35F4FCADBDE8763F272175B859376	**SHA256:** 498E998C29775434ABE91D89D70EB65454A9F157C4FE088191E9F9B68721DA9B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\UIAutomationClientSideProviders.resources.dll	executable
		MD5: B3321E254BD3EE6EB682A16B1AE92DB9	**SHA256:** 16B635964A39EEE0F2A9609316AE31DF7F0991A2513D253EB48677170344B12D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\System.Xaml.resources.dll	executable
		MD5: EA2D40C9C87793E48B5BA124E0697FB6	**SHA256:** E8D8105FBF529B5A4E844AAAA384E75079E564081A1CBD3DF660B472825884F8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\UIAutomationTypes.resources.dll	executable
		MD5: 7AC385B9FD59A91A9AE2C8A72B922A59	**SHA256:** EB5904B89E4150AB5BBF56BF62E4429C024B2D7782A6EA1BADEE4523FFDBC486
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\UIAutomationClient.resources.dll	executable
		MD5: 4C0CAAF1EDC42DC01336D9340AA11B5E	**SHA256:** 599EF3F8CD4CF54111633941DFFD9BDF733D53F2B938144A8E9F3772629AA32B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\PresentationCore.resources.dll	executable
		MD5: EFD19A40BCB3FC4693D37409C418FEA2	**SHA256:** 6E6E7FAA115094A9A2320433E76DE2AB99F557C28C44B40A41A3278883DA4390
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 60F4FD8FAE1AF4D23C7F59D6F12B7887	**SHA256:** 2AC66B7CDB46B69896B3A7533946AAE33D7B51420E73948C21B966AD95823B22
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ja\WindowsFormsIntegration.resources.dll	executable

		MD5: 8EDA5AA3BD5074561F4D3EC170A88FD4	**SHA256:** 882A4079262B14D942443E845F98A43CFC56726C00AA7347269AABC5D7B35D38
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\PresentationUI.resources.dll	executable
		MD5: 5A05F49B17D0DB5BFF4569647B471FA1	**SHA256:** E5E6C42A7DF578806CEC1C9275E6AEEBCC44D7E12490A58CD2AFECC9A01D3799
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\ReachFramework.resources.dll	executable
		MD5: 55C7E98A7D2C4AD7CA1836A850FBD848	**SHA256:** AEE2AD77BBAB29C79F911BBC4FE18015F668BE43DC6F7C1AD7DD714260D30170
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\PresentationFramework.resources.dll	executable
		MD5: 47E4EC6510F7FFF622FF51A3AE6AB9E8	**SHA256:** 1AC78443BACA8F9CC43B4B55F193D7DFA786B3E44F26CD4828104F1BB0701E7F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Windows.Forms.resources.dll	executable
		MD5: 23C2645536C3498149A040388698E048	**SHA256:** 9E8A46487084473FFF2CA595483F94DCDF48369A0E706B3291D47FF41B5F001B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Windows.Forms.Design.resources.dll	executable
		MD5: 40A4039C6C417D070F9513B223CD9E19	**SHA256:** 7C2D9297C4169183DE2080EE60622F1F8D82D02828023950C0ACD76C9F9995B2
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 5AB2EDEA08F5F5869FB2A29CFE62E32D	**SHA256:** E734B2F3B78C16C26BBC1ED509D28A610FAF1C3AEB9E4C4947AF4A76A22A5B97
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Xaml.resources.dll	executable
		MD5: FC25FF87DDE25C1099E90DB0653A81C2	**SHA256:** B3FB43A7E7FAA0EB429253D4E39B9998A0FB0BD27A820F21D8A74C35D46DA3B9
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\UIAutomationClient.resources.dll	executable
		MD5: 5A69EBFB975C17247F2F2CD5AD66284E	**SHA256:** 621B39F34F14CD5AD77E4C5EF476919E226C63FCAB2A2B88A8C7480FADF70510
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\UIAutomationProvider.resources.dll	executable
		MD5: A87E279ADDAB6BE01C3A03C6C997147A	**SHA256:** 14A2C56F9AAC31B83BF5186A38AFC66EA01FFBAAE15052728F48350962C6D7E6
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\UIAutomationClientSideProviders.resources.dll	executable
		MD5: ACE198F429DF12024A59D0C67FBC07B6	**SHA256:** 0A2C583F07D888DC4FDDC0B1472579F895519E3B5FE14C65DDB295409E589634
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 45C6A3694323E801EE06FF478F1F1EEF	**SHA256:** 548EDDA4FB9F62627866B4D06836B4512EFC86819403096E35249B17AA768EF4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\UIAutomationTypes.resources.dll	executable
		MD5: 7236513B74B7C6BE421911B19EB540E1	**SHA256:** 217D2D728570AF6A82BA5AE50BD7538575FD6A8CDAAEDB85A5ABAFCC84C5F12F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 084DA7FC4BBC387731F92F9FCD986726	**SHA256:** 10031185ED970A61C67A66543146DB375FDDD1FD8019A4D33BD4931C87839DC3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\WindowsFormsIntegration.resources.dll	executable
		MD5: 52FA885C1416FCBF4488C687D89BE7A8	**SHA256:** 268D15DD977889BE081D10F1C07CAD89189199BBD5DB734D8BDFA7DADA8E4BED
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 444A5E08B14D876CF51708ADED36CA75	**SHA256:** 9A96609759E31E1905A947ECF39CBD69ED326D3CD487AE32322DABDE143B2F75
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ko\WindowsBase.resources.dll	executable
		MD5: D00FFBE6EC60B2AF1C9888D7445D579E	**SHA256:** 9A49B841FB6B096C5A801AEF70FE30C8C1653DD3A3ACCA6CAD4E1F1A497F9DCC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\PresentationCore.resources.dll	executable
		MD5: 559F3831B34988564289A18A05DC6E9F	**SHA256:** 86E9C0230054F3D39780BE332E3A5112474E2118B3BCD104F2073E7BB22ADEED
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\PresentationFramework.resources.dll	executable
		MD5: D0A4EF9C0C1989411072B0A74C7F87C2	**SHA256:** B2302B1863F29A43EB131F67BEBC745206ECD9E7F977085D4E6C2182E75B0766
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Windows.Forms.Design.resources.dll	executable
		MD5: F06F361AAFA45C50BF302D06AA73F925	**SHA256:** E1387C2E764794F7CFF62C9BC736C47A0DD1E1D4D5C9194B3C9C360195B044B7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: BADA2A9684D4F5C7581E8413EB48FA0F	**SHA256:** AA99E60652C4F07BD363680217A7D0045D859601BA372F5A5871DB277C710B42
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 21626FD8C9B5865DC0DDBB75BD1412B1	**SHA256:** 3246D188D286320975329AB525B6FC5DE34E173FBE8E21329ECF11D560363039
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\ReachFramework.resources.dll	executable
		MD5: 948190FB78AFD740DCEB1F900478EBC4	**SHA256:** 261B79ED6C78AB00E16D2F46C9DD0E99D9F6858ADC899A059B86B495ACFEFA3A
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\PresentationUI.resources.dll	executable
		MD5: D0001A2602CAFB0C0D062F625BC176C5	**SHA256:** 9ACAD58DD8F162E63B87469B02ACC484432DF67528717FF099100D567CD0F4EF
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\UIAutomationClient.resources.dll	executable
		MD5: C687E22F0BB48EEBEF63DA1FE8E0BE69	**SHA256:** A2FF3F352CF46155C052DA22DC244FBF5AE3ABBC7607B42B04A2DDACEE4D05AC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Xaml.resources.dll	executable
		MD5: E546F84178A6F31000B1AC1925142E8C	**SHA256:** 5591A6751055DFE550557788FF3F07880B7027AA67082476A4649E2A30C01BA3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Windows.Forms.resources.dll	executable
		MD5: 12E2B334FD8E8B1142B070CAE21ED1F6	**SHA256:** AE061A67E1E5B502126FBAB7F49362F0631E732DCFEC803D97357D9C1576896B

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\UIAutomationClientSideProviders.resources.dll	executable
		MD5: D9DAA0BAEFE3D8369BF2F41DE6022DE5	**SHA256:** 258D88A8080EF79EED76A947B674CF12C5867AB454AD0F603268D6B374B0CAC5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 76443EE7C1CC43A3E163C1BE6BDD76F6	**SHA256:** 1D1400E793FF4D82FFEC2AB349E46CC8F92C90C80089F3F3E09CD52050C7EEDC
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\UIAutomationProvider.resources.dll	executable
		MD5: D035AF60299C38548125B2F8DB911EFE	**SHA256:** 57C9D8B053B4B087D07698902AB906C4125F31A3A30B022AF8E36DFA5C4AEFDB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\WindowsBase.resources.dll	executable
		MD5: 23AD4BBE3B4094A42343E3DB17FADB0B	**SHA256:** 8B8C00061F12793C1DD10C294ECE9236C703CDF8C2B98690712009234CAB809D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\WindowsFormsIntegration.resources.dll	executable
		MD5: 6DDAA2F18558B3F7FD2FCBA937FF8F1F	**SHA256:** A62BC23CD533D8A79BC280EA2A4869543D5A5DCFC4772778984043C65A3EAA3E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 74CC7C87850D2DD760B2BFCB6D78C0B8	**SHA256:** 8CB3B555A91D0CE6269E846AACCB4EC21FCD7800C33A29B5C8F1DED4DFD69E7F
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pl\UIAutomationTypes.resources.dll	executable
		MD5: ED4993B49FC2C210AA5A9A97D756544A	**SHA256:** 93E4FE1F0D6EE147DD7EB48E1CC271F97FA8880A2D6E0AA82A89C86C669C8EBA
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\PresentationCore.resources.dll	executable
		MD5: 9548494A53C1E56854F55679E244A92C	**SHA256:** 3DF25BBDF4D8151DEC9D0086D142E7F51899E83CDC959E4F8606A83459B3661B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\PresentationUI.resources.dll	executable
		MD5: B7B6D8DC4EDA856829AB9591E2CE1814	**SHA256:** 456B4F38FB0E0CEBDCF4E106F22A1A51226B0DDEF1284DF17AB4A385D612D25B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\PresentationFramework.resources.dll	executable
		MD5: 0A9B787BE3FFFCFA75E6CD13FFF90795	**SHA256:** DBB4451F4D486FF265653928791FA1CE170A75832996229BFD2523322A140BF3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Windows.Controls.Ribbon.resources.dll	executable
		MD5: 13726D4CB2A95ADAA10FE573C84B7A56	**SHA256:** 2537D9BFA4542652A508AE945896F571C2013E06B9635ED626D259BACB4CA1F7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\ReachFramework.resources.dll	executable
		MD5: C5D6E72726C8A337DEB5AEDC4F3FF51B	**SHA256:** 6F2D70330B74515AF05E5313F889E93DF6624CADEA851ABDA60B65A1038CAF4E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 0D75593BB6FEA00D059084E3E3EF2244	**SHA256:** F4B5F73DABAA6E9C5BA5349AB830648022F96FC345B946F438C3ED6D7DFFD0D1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Xaml.resources.dll	executable
		MD5: D8957E87DBF3591CDF2719C82897C2AA	**SHA256:** 84DEB97ED288E2181E2B6B2D7BDE20E972BF80B30D72FE4334EC58FD629F76D1
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Windows.Forms.Design.resources.dll	executable
		MD5: 6BD1266EA6DDE381F8AA19E705EA1E70	**SHA256:** 853558D5E2BB3F367024355CF4A16968247FFA70DEB5830118DD354EFDC9B7C0
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Windows.Forms.resources.dll	executable
		MD5: 2357C68325032F93ED0E6CF948F6F049	**SHA256:** E879B057E3CADA37C6102CD3BBF927163B6623640635E0A2DFA3A308878867E7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: F48D1B42FD31B8E598962D2C6DBAB6E1	**SHA256:** C7EEEF17C68B549DD5EFEE92BB153A9EC70BA7B8EB6337DD08C267548F13D233
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\UIAutomationTypes.resources.dll	executable
		MD5: EF49C50FFDF34AB3F510324D802DC458	**SHA256:** 68FC5DC03F7255B35A5ECBB365A6230A685F15F929F95C1299D899D8279202E8
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\UIAutomationProvider.resources.dll	executable
		MD5: 6D7003DBF50EEF4D1BCE9ED5909A3F00	**SHA256:** 336D376F39BE0DBD183184F2A2CCE40AA54BD014B6453CF6E0F80447F5142707
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\UIAutomationClientSideProviders.resources.dll	executable
		MD5: 369DE95EAEAE706C5182DC944E81D8E1	**SHA256:** E78E4FDBBD3D016B21FF0ABBEFAE17B7990ECE577EC6B55D22B6BAA99B75F8A4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\UIAutomationClient.resources.dll	executable
		MD5: 665A8EFB7AA5EF39BCC7526775A66A07	**SHA256:** B946C11477D26434BB45DF65DB39F08F3596772ED21E81D287E94B302DC22F20
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\WindowsBase.resources.dll	executable
		MD5: CCFCF0E8DBD54D842B5902BBA4DF2A72	**SHA256:** 03B48BB4D55C217DF5FB1882711F2EE668321E3A4AE2DC3FEB6C5AFBAECCD495
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\PresentationFramework.resources.dll	executable
		MD5: 2C79041C4655A51706E0F41AC147033E	**SHA256:** 7DA82BE2DBD380E07ED195B9009610FB69106AF07CD1FCBF689E83A7DFE1D938
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\pt-BR\WindowsFormsIntegration.resources.dll	executable
		MD5: 6BA8FAD97703DA22070F4C91FAF22985	**SHA256:** D4D1319B81EC07221744BAC75DD553A473C2A0A3FEFCBCA4F5B24B0FE96AC344
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\Microsoft.VisualBasic.Forms.resources.dll	executable
		MD5: 1FB00AB0207F0995FE0C6E324BE03729	**SHA256:** 5294E0DA969CDA415A622EC064A6F13425A184BF06DD3B8AADFA1DFA6D3D9B80
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\PresentationCore.resources.dll	executable
		MD5: 2728AFFB0A8B9579F2DEA9E52987EFB7	**SHA256:** 7331320A14186FBF9E935B839B28C48D81FD2A46D537042CAD8AFABB43A0E35D
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\PresentationUI.resources.dll	executable

		MD5: 462A72D69A8D0660CC9145A769BC80D1 **SHA256:** F05576730BA7204E4013B0B3975BA3541251126C3BD319D40999A00A9314E4DD	
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\ReachFramework.resources.dll **MD5:** A988AFD624DA1B4EBE76A836F9DA6F54 **SHA256:** 93AD70DE1C7FF4F6F551260149656786CF79B6ACB5266192A07F2FB9954DF667	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Windows.Forms.Design.resources.dll **MD5:** 05F3D57ED9E54C7B9F0BDE803EF559D6 **SHA256:** DAACA67FA5C7BEC7327021A7DC437ED54B9EB9A67DE31F2A8E6B04F9872BE283	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Windows.Controls.Ribbon.resources.dll **MD5:** 5711C31517B0487427A6D455EBD50998 **SHA256:** D53EEC346CD10C90B511F51711DE06798ED9DA1D55D493AA31C55478CB276F6C	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Windows.Forms.Primitives.resources.dll **MD5:** CA88370B95F74A75ABD7BFD9DC41AC92 **SHA256:** 243224A43A37B80118F1FCEA0A1555D4896684E0702B649ECA924BC437D094ED	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Windows.Forms.resources.dll **MD5:** 83F2139AB609BE6EA8B6028A4633F401 **SHA256:** E5EC09DA0C11BD73AE2DB1B8C1B182B3591119834BFCFEDC29EBB79C9B47D34F	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\UIAutomationClientSideProviders.resources.dll **MD5:** EDA6408749F62EE5DE74CF5783B14CBC **SHA256:** 30F9E69BEF2F50CC5958142332EBCEAC5A346CD1E6D57841E8584C81164C0072	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\UIAutomationClient.resources.dll **MD5:** 8B1E98EC82B72A450AE3CF63E20D7B8D **SHA256:** CE5249028C1D3837B47312D9EEE390CC6311D6A699333B9FCD746C5FCAF39142	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Windows.Input.Manipulations.resources.dll **MD5:** 582BD307C032520A88CF91F92D9477AC **SHA256:** EFB4D1D908057AD0DECFACC378789569C9E4FA489CE737B179D1B8F1C3F7D789	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\System.Xaml.resources.dll **MD5:** BC1125A346812A75880C67ED7A6EF978 **SHA256:** 01FCB6D40665C43FAA83B2423DF8EEC7317A1B66121C3D4F512FE6B5DB77E9F2	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\UIAutomationProvider.resources.dll **MD5:** AE137DD289236DBA459504EDCAFC927B **SHA256:** 2DA40AF59E27D07E5CB1E84AF1A305D3170821C99878AA5A3D40EF027EE48B84	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\UIAutomationTypes.resources.dll **MD5:** 1B575138E1FD2945A48D5D8E497CC1A6 **SHA256:** BA0C2E5E0347A58F95CF1F43C4862D102D2F33467E83DCF3941E989170403427	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\WindowsBase.resources.dll **MD5:** 2C8CE06D92B357DF3FEE8B9E9E76EBDD **SHA256:** 68CADE6026032618A2C22057673B18D9DFCDE78FC7229D4E34153D56758B1728	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\Microsoft.VisualBasic.Forms.resources.dll **MD5:** 9A2448E97DB5B0C19E373EA541597EB5 **SHA256:** A3F368F33E7BED8B9444E60676B0B820CCA3FD1069D2EB0DAD38AA0DD7E337A6	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\ru\WindowsFormsIntegration.resources.dll **MD5:** 0899DCBE43591B77F1C775088C99339A **SHA256:** 0EA5164BE3CC316B2CB48A80086E19F28512A3BC9A2C7C509A1B8DC4D67D14C5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\PresentationCore.resources.dll **MD5:** 9ADF177D7A625B272143E2E91486BD12 **SHA256:** D7F753E5DDE04530CB08900DEB265B96AC32D0FCB5EC5D5638DC3BD97A323586	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\PresentationUI.resources.dll **MD5:** 347101CBE921D31035A5CAABAE3456EA **SHA256:** 72158B8CD44A4007395289F58DFDBB3E68CAAF334A4ACC1BEFD53D953F9F24AA	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\ReachFramework.resources.dll **MD5:** 93FE9E566FE3AAD4365C7F97980C9655 **SHA256:** 8A9D5CA0838B8BF3C8AB2C3CFA68517BB3A9A8AADDFA301018DDD136717903E5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\PresentationFramework.resources.dll **MD5:** D23CF090E4218276D36C56A6BE2DEB2B **SHA256:** AE35ABB082534CED66611917D663EB685588A703829B9D7A49FE78C84AB3D16B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Windows.Controls.Ribbon.resources.dll **MD5:** A7200E30FCA62D0A57B5FB7AC581F252 **SHA256:** 79BBD511964C951D0224B84BBBB59D51D36F737A3A6AD5791E807A58C52CFCFB	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Windows.Input.Manipulations.resources.dll **MD5:** 0AAB6C7ADDEA2F45E30D66A831F6F386 **SHA256:** 46989803F23E33F79CAE517AE451B508E35972F0B9204B2B85E3E23157883A74	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Windows.Forms.Primitives.resources.dll **MD5:** 9736D3282B497A1ADFE254C66D3FEC76 **SHA256:** A535450D0DFF3F4E56FC12D202FE60A431FE0CD8AD5FCB4C33AEFABFF1DEBDAA	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Windows.Forms.resources.dll **MD5:** 439756EA2E8F571C3943AD0A12478156 **SHA256:** 6CA3E603A0711DB4097E8EDC6891E216DC349AC02B7536DD7EC8629E068D1439	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Windows.Forms.Design.resources.dll **MD5:** 54BE351899E95C5EEA3A4CFE748EEACE **SHA256:** F50A58898B8F17D3F1667CE201DCD9649CF237B513C7A8C1874629F30E4DEDD1	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\UIAutomationProvider.resources.dll **MD5:** E5E730315764C31802BED679CD370A22 **SHA256:** 68D151736BC49477E68BDE2DA3FA56FBC48171BCB02EFB5E1897CE5E1C941A5B	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\UIAutomationClientSideProviders.resources.dll **MD5:** 9E4BB959123BFA9EE52110241ECB0A71 **SHA256:** D5D9F45B239C24F173A561CCAD6268A5CA26610FA8DC0F84900320EA15241661	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\System.Xaml.resources.dll **MD5:** 916390889CEA90BBC545D02E17C997AF **SHA256:** 443C60702D46761333B916E37BE16F908BC998D399E4F6DCBFEF2D8A2A1999DA	executable

3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\UIAutomationTypes.resources.dll MD5: 0305B52C7182A2679C606A966A18DC85 SHA256: 657E7DA6C3F1B27CB2C298410D5037899D121260E70B3CD8073C0E3326EBFA6A	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\UIAutomationClient.resources.dll MD5: 5136AB247A59D744416858966D3043AD SHA256: E3B07ACC9D9ABB8F587DB016643A854B390D3D6EF829FE332521D9D89A93AE24	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\WindowsBase.resources.dll MD5: D0B6347E7E1DC7F057E4323CF6A8F6FF SHA256: D2C023FD274F7395503B0AF9FC598FD249E26038BA9A5C7E9A1A082B5443137C	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\PresentationCore.resources.dll MD5: 0C456A18A2EAAF2156F83A3D6BA9C34F SHA256: 758CEC641FC52F54340DDB69CF47D848014FADAC5FFF6CD1DD75EDE8E35F8E07	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\Microsoft.VisualBasic.Forms.resources.dll MD5: D729BFC3B66EE8FECF00F6D54375D6FD SHA256: E498D0F8F32A3E864042546B79AA36DD7761B0C1C07756076CF3434289A8AE84	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\tr\WindowsFormsIntegration.resources.dll MD5: 977F46DDD9BBDD95D488BB8DEED3DC35 SHA256: E1F202E0AC7751961C939781ADF9B39EF8723D478BD577412AB57D080B4A526D	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\ReachFramework.resources.dll MD5: C6BD032675E737D09A2A0E74F079436B SHA256: 3C65550FFAE43303EF1855CB7F5099EABF3A5A179F1218E32B4E5F5694880F05	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\PresentationUI.resources.dll MD5: D51BBFBDA51FA21E35A887387BC10FBD SHA256: B9825150198BC7CF862D5828451D257DE8E1C87A2732FA5ECB1FFEC5A9EB8BC0	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\PresentationFramework.resources.dll MD5: 0414F970153822E79C22A5B25BB75F1E SHA256: A656FCA207C98E13190E7A62AE17F06B15597746B3109110D4505521ADCDDAA5	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Windows.Forms.Design.resources.dll MD5: FC5516256D6AF0F5A3DE579C050DC742 SHA256: 3CCEF7C6C98E48539995ED39B2D0CA8F12A4DA8FF86DED04E17A497ABBC23AD3	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Windows.Controls.Ribbon.resources.dll MD5: 0F60F6533D114AEAE7178A719F6801F8 SHA256: AFE4E475DA313E128A0F9AC0058DE7D8D4DFFEE0F7274A69F07C973AB4FD3681	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Windows.Forms.resources.dll MD5: DCDA8667157FF231B361C06359AC95E9 SHA256: 2E0D930E016B3954EA0EDFCC35FC72A686D08EC1FC566AF482B6D021B6CBC079	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Windows.Forms.Primitives.resources.dll MD5: 545D4A07AAD537440C430D4FFFC92B4E SHA256: 824B1D922A62F819CE9631CAC4730524CE35D66F29A605BD02CAE9B2C34508B8	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Xaml.resources.dll MD5: 1DB0C5CD75C72857EB98975C80296BC2 SHA256: B7CFC2303EE124996956D8EF06EAB33A5B04CB837878AB5FAF7EB995C8C82362	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\System.Windows.Input.Manipulations.resources.dll MD5: DFD96FEA5D241DC00F474B98E2F9E11A SHA256: 14634CC45BD669E6354101CF9ADD56D725D11AD99295EF272F57C1EB2A2148C3	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\UIAutomationClientSideProviders.resources.dll MD5: C27896B362B232958FD9C5A8AD5039E4 SHA256: E2CE7C89310B9DA0C55ECF3DC9D57D500C6F18DD243519F964332932016A8613	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\UIAutomationClient.resources.dll MD5: 06B95D5FBE0C273D65A1E29E072843C6 SHA256: 22FFA22D72EDC4B15FAB376079529F749AE815DC38CF01AEEBCABC698C66D861	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\UIAutomationProvider.resources.dll MD5: EFD13B515C85C2D02632890A8B1B3F94 SHA256: 3A3C5CB5B4E6224DC2DF74DDE0865B8ED83A82D9ADC87FB3DEEEA16286702A11	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\WindowsBase.resources.dll MD5: BFFDB79EDA4AD0A6E6B82899B92F7FF6 SHA256: 3A54252B0C551136DC17FA363BC4232AF6CBA409689DF3DE7207BB2B2DBE3EFD	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\PresentationCore.resources.dll MD5: 3268EA5A10E4077DFC6E8FA399960096 SHA256: C759FE514012E664D6986A71E73A3374D161966F52C396CA9FF9F47429039110	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\Microsoft.VisualBasic.Forms.resources.dll MD5: C756FD404D8BE77D842AA504FE84A9C2 SHA256: 18ABE1D19C524E5395C53E0E846952D359C90911EE8A11FC75AEEE1A0C099343	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\WindowsFormsIntegration.resources.dll MD5: 134AF3B25E5C2D1EBDF011291D87EAAD SHA256: B581610DC121FC8A9EC1609D9B1016F015982CB3650B6521AF20307C18EA16A7	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hans\UIAutomationTypes.resources.dll MD5: 018EBB05DA526B9DCE32DA9381D8D83A SHA256: DA08EBD6B751E72C0EE1F02227535A8F191AA7ECF1C5F3E39947EBD831A52D02	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\PresentationUI.resources.dll MD5: A146610BDB62779C4B21291D4B5875D4 SHA256: 85B0A9BDE2BF9F928917C2B511182D8FC2719792AF41A8551BA76C56E799BB08	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\PresentationFramework.resources.dll MD5: B411345BEE4143EFC5106FD8684B8987 SHA256: FB960DE749AFD11139E529F9AA60BCDA6E340510592B2778A7C261CBD9A0E204	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Windows.Forms.Design.resources.dll MD5: FD01830776780099179B927C1586FC3F SHA256: CC5BE15DDD4E82E4C24F55733C5DC1B8B5BF4D73A31A9CBD536B0ACF83A000F8	executable
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Windows.Controls.Ribbon.resources.dll	executable

		MD5: 967FF109D6A32E6D9945BEB4AB0759F6	**SHA256:** A8C38F15F5D9941A1793E4A0CC7B993385D6E6F8BD040693AB6FE92E8008657E
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Windows.Forms.Primitives.resources.dll	executable
		MD5: 0563F411CDF95EB68E1FC59001D83D90	**SHA256:** 424240B4AC100BA4DB5C81CDFD6761A89A4E495EB99B3F457FDE24E9A5220935
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\ReachFramework.resources.dll	executable
		MD5: EE65180E42373E9843CDA12EC73EE9C2	**SHA256:** 2ABD95DE2644A7CF5353E95EA41121B9E23D57E03322EAE3B0C2BADD8A562CA5
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Windows.Forms.resources.dll	executable
		MD5: 6FF38E76430C930F88C5A280EC4C89FC	**SHA256:** 2B5E583BDD941B5C931AEA81D2F75A34C179A0DD766E5CDEE8861B23572F7995
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Windows.Input.Manipulations.resources.dll	executable
		MD5: 8F86CFB2F3357EE84945FDBFF3B7B66C	**SHA256:** 9829512093111C9B620179C83F5E1AD964213056F1A0D95AA6D88EC43A746643
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\System.Xaml.resources.dll	executable
		MD5: FA4C4C34F81524D5D89D7B763434FFA9	**SHA256:** DF3ABEEA9256D8CC462290E33E9CC558075376E31B2D4A043DF00DE765D5DB6B
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\UIAutomationTypes.resources.dll	executable
		MD5: 3BC06160674C67882E49254BEB001740	**SHA256:** 49945970837B59F4751051C901F276703E6E2EA386C277C3B0147659449F3367
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\UIAutomationClient.resources.dll	executable
		MD5: F8BF393040BC19673264E6FDAC859541	**SHA256:** AF38FFD07F2F25FF34F481E6497F6033E106288C930B797A5D9DEA6B48084ABE
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\UIAutomationClientSideProviders.resources.dll	executable
		MD5: BB9322E8443FB431E29FF8632977D613	**SHA256:** BA402F947CFFFCA9D7A8D4ADDEDC226A39D79DC06F23795BC595CB469F93CC97
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\WindowsFormsIntegration.resources.dll	executable
		MD5: 23451AAD8712FE418E179725ADBDE63A	**SHA256:** C77F313549A095F004574A9E4B0EA60EC16E4B10B59665DD3CC36CE587CCCE88
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\WindowsBase.resources.dll	executable
		MD5: 79FED54EF0245C30B6FE93B873C59F61	**SHA256:** A27227CDFE7900B4707D84BC3CE1620B0F6FC6BD3E03E6729112597FABFF14F4
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\zh-Hant\UIAutomationProvider.resources.dll	executable
		MD5: 685439CFABC0D57316E96369980DA427	**SHA256:** 791D07E816828FCB844BF1AE6A480FDFFBD0C2E9734207996022123B9316AAB3
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.CodeDom.dll	executable
		MD5: B5EBF75D0F19BB80944CD2730B8E376E	**SHA256:** E192FD224D436FB46E15EFAF19ADB8249447F7568AD9D0EE6E2B009D83BFE465
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.WindowsAPICodePack.dll	executable
		MD5: 9531B41519156855A45C46F0B379A784	**SHA256:** 418B5E7A96F9A6105CC6FE45896A9164E79C8849F40BE23A411B5563A8E3A0D0
7000	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_4vjbf0r0.ncn.ps1	text
		MD5: D17FE0A3F47BE24A6453E9EF58C94641	**SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\System.Management.dll	executable
		MD5: 97F595396F7E5930D6D27735450D12F8	**SHA256:** 8D53F4E69B544034A6AB9EA400392D0D4A3C501BC47E2A96350B1393F2698E11
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF1011d4.TMP	binary
		MD5: 44048877807940E6D7B9D27CA7F5BCD7	**SHA256:** 60F6CA7671C6F99FD125123F2DDF8A97C62CB63566EEB81ABE86BF368280BBEA
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\6b061f95-dc0c-4040-a241-3b5fa3ec074a.tmp	binary
		MD5: 08CCD22A7E2DB34BFD68D873731B0AEC	**SHA256:** 37A83B5CFB24B0B7C51EDED757A084B1922CC7AC26E2CD01435B7A59A5E4CEAB
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Microsoft.WindowsAPICodePack.Shell.dll	executable
		MD5: 54FE9A2748C4A0F282D4EC91E3CADC16	**SHA256:** E6FA9D9E34FF3BF63CE782654B14E4B54A3ABD1022C87BC099032C2948157672
7000	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_k4csv2tn.dff.psm1	text
		MD5: D17FE0A3F47BE24A6453E9EF58C94641	**SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
6232	chrome.exe	C:\Users\admin\AppData\Local\D3DSCache\cb00da9ba77862e\F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.val	binary
		MD5: FF9615348BAFAB70A615C61FD851B1AD	**SHA256:** 896AC590C141FE0109068F3A3D4059FD0A888C0202574E3C4326F9FCEC62C38F
6232	chrome.exe	C:\Users\admin\AppData\Local\D3DSCache\cb00da9ba77862e\F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.idx	binary
		MD5: 6F68F3FFB1DADEFC96D1DE1C1D440ACF	**SHA256:** 28D04B9D08D447AC0BE9DD4CB06480E452D106575BDE529E4D6C1F033E4CF4FD
6232	chrome.exe	C:\Users\admin\AppData\Local\D3DSCache\cb00da9ba77862e\F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.lock	text
		MD5: F49655F856ACB8884CC0ACE29216F511	**SHA256:** 7852FCE59C67DDF1D6B8B997EAA1ADFAC004A9F3A91C37295DE9223674011FBA
7000	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	binary
		MD5: 38C430C5B583A28108A48B76FE4F8F5B	**SHA256:** D75F567F3538FC0CBA2ECBE264DB8436DEB005860D0B7DF4FEBF9F48EC4008A7
3904	Install_x64.exe	C:\Users\admin\AppData\Local\Temp\.net\Install_x64\f40\Install_x64.deps.json	binary
		MD5: 7E1114DED3C1C40F5994E8598CFDD79F	**SHA256:** 1202BC2DF4F1614424C6B8CD40EFF251DB6FC0EF1F6CB6F319F2CCB3C7C3A355
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\95e8076d-7216-4caa-a995-c1054484009a.tmp	binary
		MD5: 9E1FC1EA849CD34026EFFA90776410BD	**SHA256:** B30EF24627909B1FFA09FBB834B99D0E5B17446EEF7902C7BF16899860DEF667
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF103942.TMP	binary
		MD5: 08CCD22A7E2DB34BFD68D873731B0AEC	**SHA256:** 37A83B5CFB24B0B7C51EDED757A084B1922CC7AC26E2CD01435B7A59A5E4CEAB

7124	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_825372098\Google.Widevine.CDM.dll **MD5:** 477C17B6448695110B4D227664AA3C48 **SHA256:** CB190E7D1B002A3050705580DD51EBA895A19EB09620BDD48D63085D5D88031E	executable
4772	1.exe	C:\Users\Public\Libraries\efenp.scif **MD5:** — **SHA256:** —	—
4772	1.exe	C:\Users\Public\Libraries\nifaa.scif **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF1060bf.TMP **MD5:** 9E1FC1EA849CD34026EFFA90776410BD **SHA256:** B30EF24627909B1FFA09FBB834B99D0E5B17446EEF7902C7BF16899860DEF667	binary
3904	Install_x64.exe	C:\Program Files\launcher289\1.exe **MD5:** 1D937347C059389683CB1FCDDAFEBB23 **SHA256:** A654FE947C424A7607A195689678177C9D982F1E19D410BA9B064E2DF9E473A6	executable
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\c461fc22-ac04-4d7c-abd5-d308b1b9cea9.tmp **MD5:** 5C731870A27D05C91CC01B05CC61FFD6 **SHA256:** A412841078E3E5CA01889C0041B990524F12E0D2CBAB6480146E05EA6DCB41C3	binary
7124	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_825372098\manifest.json **MD5:** BBC03E9C7C5944E62EFC9C660B7BD2B6 **SHA256:** 6CCE5AD8D496BC5179FA84AF8AFC568EEBA980D8A75058C6380B64FB42298C28	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_825372098\manifest.fingerprint **MD5:** D30A5BBC00F7334EEDE0795D147B2E80 **SHA256:** A08C1BC41DE319392676C7389048D8B1C7424C4B74D2F6466BCF5732B8D86642	text
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Trust Tokens-journal **MD5:** — **SHA256:** —	—
7124	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_825372098_metadata\verified_contents.json **MD5:** 3E839BA4DA1FFCE29A543C5756A19BDF **SHA256:** 43DAA4139D3ED90F4B4635BD4D32346EB8E8528D0D5332052FCDA8F7860DB729	ini
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\component_crx_cache\neifaoindggfcjicffkgpmnlppeffabd_1.c900ba9a2d8318263fd43782ee6fd5fb50bad78bf0eb2c972b5922c458af45ed **MD5:** F265D47475FFD3884329D92DEEFAE504 **SHA256:** C900BA9A2D8318263FD43782EE6FD5FB50BAD78BF0EB2C972B5922C458AF45ED	crx
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Reporting and NEL-journal **MD5:** — **SHA256:** —	—
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies-journal **MD5:** — **SHA256:** —	—
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Safe Browsing Network\Safe Browsing Cookies-journal **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF10884c.TMP **MD5:** 5C731870A27D05C91CC01B05CC61FFD6 **SHA256:** A412841078E3E5CA01889C0041B990524F12E0D2CBAB6480146E05EA6DCB41C3	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\c457bcee-d179-4074-b159-c767fc88d9ee.tmp **MD5:** 5070CFF8E4F11D57C2C9413318C276AA **SHA256:** 007C636BFBABE3EE3D0843EAEF28625076E75677A87BFF9D99BFE28079B9B243	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF108ee4.TMP **MD5:** BC3295FB0DCD6A5F9D88B77D8CE6602C **SHA256:** E3B4D7B3995E06EB6C7C9B3DD4B8C196CA87405D526B095075D0F35801501D4F	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\5af5a5bb-816b-4de9-8468-1a623e7084bc.tmp **MD5:** 0BEA4FB3B7A8EC6CA14AF06586F9CFBC **SHA256:** 84FEBF22239B7098576CC373F3C84A7739D076B58767B2F8358F4948EEF18675	binary
3904	Install_x64.exe	C:\Program Files\launcher289\2.exe **MD5:** C0C765709CBA75C12DAE71EB91EC8B5C **SHA256:** 45E346DD5F5ECA6785F121D07AD418AC1CCBB3F43EB1CDF6A78FA6105759B3F1	executable
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF10af9b.TMP **MD5:** 5070CFF8E4F11D57C2C9413318C276AA **SHA256:** 007C636BFBABE3EE3D0843EAEF28625076E75677A87BFF9D99BFE28079B9B243	binary
5372	2.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1461009999\bin\jsii-runtime.js **MD5:** 98338361DCEF14695445487CE509677B **SHA256:** 4E0C38C4B6DF379F0364A1BDA5097589CC4A614EE1CCBFE04F033580F240D9B7	binary
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\9400fca3-144a-4db5-9f34-2b3082089bbf.tmp **MD5:** 1A49E823FFDCD949B630B1E882BA2B7A **SHA256:** B45D650C420B240A6F5A2C580E0D04DD83BE5D2BBAC4E47DD4F6F05EAB4D6234	binary
5372	2.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1461009999\lib\program.js **MD5:** BF41580C1454743386E48083EF7CDB9C **SHA256:** B4BF248DDDF226E8F1DEFBD12125F5AE683F37C6DF976E31CC4A8B3201EFE80D	text
5372	2.exe	C:\Users\Public\Libraries\fkeme.scif **MD5:** — **SHA256:** —	—
5372	2.exe	C:\Users\Public\Libraries\bddja.scif **MD5:** — **SHA256:** —	—
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\369f8a5b-d0bd-4ee2-bc46-722477c31b79.tmp **MD5:** 8770D55AEDB30D5C6FA27399A2AEA413 **SHA256:** EE09A16F7F745A8A13BA3742BE8969B75D5A721BB993CEF0E5AA3EBE6F1639A1	binary
5372	2.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1461009999\lib\program.js.map **MD5:** E61E1B73BBC2DEFB6419B023D808574E **SHA256:** D812A3EA536DAB15378AAAFA66DB571D9167CFD44E15D7E67637D4F4EFFA9F83	har
2476	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History	binary

		MD5: 819B266C70B0644EB6C8D1339BE5C6AF	**SHA256:** 03ADB51126BE6CB4CA54C526D7E02F198618A5E434B4400297AE4A8447D34A25
2476	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	sqlite
		MD5: 1D47EB743D7CA6AC2EB7AC07958E6EF4	**SHA256:** 69F3F3EBF763DD42DD0D7A7644A0D2B8E7467E9896EAC439F83A9B9CF4877E4B
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF10d6e9.TMP	binary
		MD5: 1A49E823FFDCD949B630B1E882BA2B7A	**SHA256:** B45D650C420B240A6F5A2C580E0D04DD83BE5D2BBAC4E47DD4F6F05EAB4D6234
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Safe Browsing Network\Safe Browsing Cookies	sqlite
		MD5: 9FA24DE927D92E7C48064251398EF4BB	**SHA256:** F4E8CBF5DAEDF183E590286E3A67B579261F48949712E84E2518A70AE2158754
5372	2.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1461009999\bin\jsii-runtime.js.map	binary
		MD5: 8533F6EEC254252FF2E6D39C8ABB8E23	**SHA256:** 0E6E4C477FC20C3A9C782240AFEEDF15697538B64B5D7DAB7BE9891D323DA1CF
6600	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Reporting and NEL	binary
		MD5: 3FBD88B7FF87C7B256F14DA12C7C0C50	**SHA256:** 90A26E95F1C5EFD96A3AE81D2960F049200C9DED76AC76E54DF1FBF36478AE20
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF10fe47.TMP	binary
		MD5: 8770D55AEDB30D5C6FA27399A2AEA413	**SHA256:** EE09A16F7F745A8A13BA3742BE8969B75D5A721BB993CEF0E5AA3EBE6F1639A1
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\c517eab2-beb5-4338-b9ca-fbad7616b5af.tmp	binary
		MD5: B5A10445855948DC4ADBE14029D32D9A	**SHA256:** 25DCB384A382FDE3C3CC016398B908CC440BEF8E534BF6FAD06036EFD12BB650
7004	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_1730915792\Preload Data	binary
		MD5: 95F14FA7CF5F40EFB6AAB13D6F879DD1	**SHA256:** 0CF70EEA2B4DFFA36719B9A7BF9FB2F40A29728029B8D0BF05144C1A297899CE
7004	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_1730915792_metadata\verified_contents.json	ini
		MD5: 88FD348B29FA400D5CD66060D308B489	**SHA256:** 1F88E8A095B087133A71CB66C9964F300514B238ADEF1B620FDDE2F783FE4A0E
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\component_crx_cache\ggkkehgbnfjpeggfpleeakpidbkibbmn_1.d1f1a6954babb7330ef005df1b89dcdcb3d163ad1fed7a6800032ebb5d3b8b70	binary
		MD5: 3D83FE7C6B4D7396BABF7E6E56DFECEA	**SHA256:** D1F1A6954BABB7330EF005DF1B89DCDCB3D163AD1FED7A6800032EBB5D3B8B70
7004	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_1730915792\manifest.json	binary
		MD5: 3F1496F735AC3C3DE4A5C9BEE0B692EE	**SHA256:** 8570AE9D4BDBFA9A76D303DA090476896352EF170C1309E053998CC484BBFD7D
6328	chrome.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping6328_1730915792\manifest.fingerprint	text
		MD5: DFED5DCEAA8B29163DEFE4D94457EE98	**SHA256:** A8B2FB90B813552ACECB88F2D27DC5134FA935AF5171CED8E0797CC0165CC4D2
6280	BitLockerToGo.exe	C:\ProgramData\KEGCBFCBFBKFHIECAFCF	sqlite
		MD5: 29A644B1F0D96166A05602FE27B3F4AD	**SHA256:** BF96902FEB97E990A471492F78EE8386BCF430D66BDAEFDEAFBF912C8CF7CE46
6280	BitLockerToGo.exe	C:\ProgramData\DAKJDHIE	binary
		MD5: F6C33AC5E1032A0873BE7BFC65169287	**SHA256:** D97895CEDED32E33D57BDCACCDBE144E58AA87AF4D2F8855D630286CE30A8D83
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\9c0c567f-4359-4dbb-a005-f6ef8e768bdf.tmp	binary
		MD5: 06456282AFF72210B37C937E80C982DD	**SHA256:** 0A0CAF520FF859044562463278E856DCDCA919D48609014BA684D61409D11E8E
6280	BitLockerToGo.exe	C:\ProgramData\KECBFBAEBKJJJJKFCGCB	binary
		MD5: A45465CDCDC6CB30C8906F3DA4EC114C	**SHA256:** 4412319EF944EBCCA9581CBACB1D4E1DC614C348D1DFC5D2FAAAAD863D300209
6280	BitLockerToGo.exe	C:\ProgramData\GHDAKKJJJKJKECBGCGDAEBAEHI	sqlite
		MD5: 1D47EB743D7CA6AC2EB7AC07958E6EF4	**SHA256:** 69F3F3EBF763DD42DD0D7A7644A0D2B8E7467E9896EAC439F83A9B9CF4877E4B
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF112586.TMP	binary
		MD5: B5A10445855948DC4ADBE14029D32D9A	**SHA256:** 25DCB384A382FDE3C3CC016398B908CC440BEF8E534BF6FAD06036EFD12BB650
6280	BitLockerToGo.exe	C:\ProgramData\AKKKFBGDHJKFHJJJJDGCBKFHJK	sqlite
		MD5: 31EF1E93260AED2FED884531149F5171	**SHA256:** F2E9869285B794BF4B14BBB67CA6E680BC46BE8FD0DA55F4A7745F34E84815B7
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\e1400167-8c1f-4cb7-84e5-17f3416b2282.tmp	binary
		MD5: 446D1F5E696679EB5437ED5D54A17D2D	**SHA256:** B6B0345C6AAF86A07B60880979F6EB39671A12AD34786E8C24A5CFB87850CB4B
6280	BitLockerToGo.exe	C:\ProgramData\freebl3.dll	executable
		MD5: 550686C0EE48C386DFCB40199BD076AC	**SHA256:** EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF113dd1.TMP	binary
		MD5: 0BEA4FB3B7A8EC6CA14AF06586F9CFBC	**SHA256:** 84FEBF22239B7098576CC373F3C84A7739D076B58767B2F8358F4948EEF18675
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\freebl3[1].dll	executable
		MD5: 550686C0EE48C386DFCB40199BD076AC	**SHA256:** EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\msvcp140[1].dll	executable
		MD5: 5FF1FCA37C466D6723EC67BE93B51442	**SHA256:** 5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
6280	BitLockerToGo.exe	C:\ProgramData\msvcp140.dll	executable
		MD5: 5FF1FCA37C466D6723EC67BE93B51442	**SHA256:** 5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\mozglue[1].dll	executable

		MD5: C8FD9BE83BC728CC04BEFFAFC2907FE9	**SHA256:** BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
1656	3.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1370989234\lib\program.js	binary
		MD5: BF41580C1454743386E48083EF7CDB9C	**SHA256:** B4BF248DDDF226E8F1DEFBD12125F5AE683F37C6DF976E31CC4A8B3201EFE80D
6280	BitLockerToGo.exe	C:\ProgramData\EBGIEGCFHCFHIDHIJECAKKKKKJ	—
		MD5: —	**SHA256:** —
6280	BitLockerToGo.exe	C:\ProgramData\mozglue.dll	executable
		MD5: C8FD9BE83BC728CC04BEFFAFC2907FE9	**SHA256:** BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
1656	3.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1370989234\bin\jsii-runtime.js	binary
		MD5: 98338361DCEF14695445487CE509677B	**SHA256:** 4E0C38C4B6DF379F0364A1BDA5097589CC4A614EE1CCBFE04F033580F240D9B7
3904	Install_x64.exe	C:\Program Files\launcher289\3.exe	executable
		MD5: A97A542453AE817A307A0A19596FAF13	**SHA256:** 559A3369D93B7F9A393F61CCDBBF6A121DAE42C520784F07F42A192FBC5BE249
1656	3.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1370989234\lib\program.js.map	har
		MD5: E61E1B73BBC2DEFB6419B023D808574E	**SHA256:** D812A3EA536DAB15378AAAFA66DB571D9167CFD44E15D7E67637D4F4EFFA9F83
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\a8a0749d-0c33-468b-9568-4364e2804882.tmp	binary
		MD5: BE20623D1FE83C71BF45A297A32F1D86	**SHA256:** DAB4639E1A966F64B581719B2ECA8211C3A59060E3CD0DC0846D9EEFAED34B1D
1656	3.exe	C:\Users\Public\Libraries\opmhj.scif	—
		MD5: —	**SHA256:** —
6280	BitLockerToGo.exe	C:\ProgramData\nss3.dll	executable
		MD5: 1CC453CDF74F31E4D913FF9C10ACDDE2	**SHA256:** AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\vcruntime140[1].dll	executable
		MD5: A37EE36B536409056A86F50E67777DD7	**SHA256:** 8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\softokn3[1].dll	executable
		MD5: 4E52D739C324DB8225BD9AB2695F262F	**SHA256:** 74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\KCV3KQBA\nss3[1].dll	executable
		MD5: 1CC453CDF74F31E4D913FF9C10ACDDE2	**SHA256:** AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
6280	BitLockerToGo.exe	C:\ProgramData\vcruntime140.dll	executable
		MD5: A37EE36B536409056A86F50E67777DD7	**SHA256:** 8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
6280	BitLockerToGo.exe	C:\ProgramData\softokn3.dll	executable
		MD5: 4E52D739C324DB8225BD9AB2695F262F	**SHA256:** 74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
1656	3.exe	C:\Users\admin\AppData\Local\Temp\jsii-runtime.1370989234\bin\jsii-runtime.js.map	har
		MD5: 8533F6EEC254252FF2E6D39C8ABB8E23	**SHA256:** 0E6E4C477FC20C3A9C782240AFEEDF15697538B64B5D7DAB7BE9891D323DA1CF
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF114cd5.TMP	binary
		MD5: 06456282AFF72210B37C937E80C982DD	**SHA256:** 0A0CAF520FF859044562463278E856DCDCA919D48609014BA684D61409D11E8E
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-shm	binary
		MD5: B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
6280	BitLockerToGo.exe	C:\ProgramData\JKEHIIJJECFHJKECFHDGIIDBGD	sqlite
		MD5: 19BA68C3ECBCA72C2B90AFADDE745DC6	**SHA256:** 8B3758EE2D2C0A07EE7003F902F0667ABE5D9667941F8617EDA3CDF94C78E7B8
6280	BitLockerToGo.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-shm	binary
		MD5: B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
6280	BitLockerToGo.exe	C:\ProgramData\EGIJKEHCAKFCAKFHDAAA	text
		MD5: 7A97B8DBC4F98D175F958C00F463A52A	**SHA256:** 92074D2ED1AA1FD621287E35DB9EF1AE3DC04777EFAE5F09E7A3B4534C201548
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\00967242-9739-4736-9670-0eb8ad177dd2.tmp	binary
		MD5: 3D8AF6301CAE5BB1AA087B4E38DB0162	**SHA256:** 29DC19D9A3F47E57215F87E77132AE64D4B29BD9D80CD93A554B78938EF3D659
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF119b33.TMP	binary
		MD5: 3D8AF6301CAE5BB1AA087B4E38DB0162	**SHA256:** 29DC19D9A3F47E57215F87E77132AE64D4B29BD9D80CD93A554B78938EF3D659
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF117404.TMP	binary
		MD5: BE20623D1FE83C71BF45A297A32F1D86	**SHA256:** DAB4639E1A966F64B581719B2ECA8211C3A59060E3CD0DC0846D9EEFAED34B1D
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\710c07a3-40fd-4d68-929e-33ab9f20a609.tmp	binary
		MD5: E8C0E41CFD31FA2346594EE276339096	**SHA256:** 498804738367BC753C8F45259E30DA2C9D9297E1A14EF69B255403946FC4CF24
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF11c272.TMP	binary
		MD5: E8C0E41CFD31FA2346594EE276339096	**SHA256:** 498804738367BC753C8F45259E30DA2C9D9297E1A14EF69B255403946FC4CF24
6328	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\3d6e7057-c798-4a80-bcc9-5e5080520a49.tmp	binary
		MD5: 5007E189BCCECE5D77C2512275C155D6	**SHA256:** 200B3732A83F29898C935B1F5D4E8ACC9FBDE750CB58463500F4526AD7BE3290

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
65	70	47	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
5052	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5048	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5336	SearchApp.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	unknown
4436	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
4436	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
2240	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	–	–	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=2&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	–	–	unknown

5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0.2738.0/neifaoindggfcjicffkgpmnlppeffabd_1.0.2738.0_win64_kj4dp5kifwxbdodqls7e5nzhtm.crx3	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=1&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api.php?status=2&wallets=0&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api.php?status=1&wallets=0&av=1	unknown	—	—	unknown
5052	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0.2738.0/neifaoindggfcjicffkgpmnlppeffabd_1.0.2738.0_win64_kj4dp5kifwxbdodqls7e5nzhtm.crx3	unknown	—	—	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0.2738.0/neifaoindggfcjicffkgpmnlppeffabd_1.0.2738.0_win64_kj4dp5kifwxbdodqls7e5nzhtm.crx3	unknown	—	—	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acaldksiunzh56452py2db5mnbpa_120.0.6050.0/jamhcnnkihinmdlkakkaopbjbbcngflc_120.0.6050.0_all_dgzfpknn7v3zslsbhrwu6bt44e.crx3	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.97.3:80	http://firvfirv.com/1.exe	unknown	—	—	unknown
5052	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/imoffpf67hel7kbknqflao2oo4_1.0.2738.0/neifaoindggfcjicffkgpmnlppeffabd_1.0.2738.0_win64_kj4dp5kifwxbdodqls7e5nzhtm.crx3	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=3&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.97.3:80	http://firvfirv.com/2.exe	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api.php?status=5&wallets=0&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api.php?status=4&wallets=0&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=4&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
5052	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/dvn6tjyuqqxdoyobslkdwn7pvi_2024.4.15.1148/ggkkehgbnfjpeggfpleeakpidbkibbmn_2024.4.15.1148_all_ad7h2np2zton5orbcmedhdzcqjqa.crx3	unknown	—	—	unknown
5052	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/dvn6tjyuqqxdoyobslkdwn7pvi_2024.4.15.1148/ggkkehgbnfjpeggfpleeakpidbkibbmn_2024.4.15.1148_all_ad7h2np2zton5orbcmedhdzcqjqa.crx3	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=5&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.97.3:80	http://firvfirv.com/3.exe	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=6&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/freebl3.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/sqlite3.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/mozglue.dll	unknown	—	—	unknown

6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/msvcp140.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/nss3.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/softokn3.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	GET	200	147.45.47.68:80	http://147.45.47.68/7e2127a40594d70e/vcruntime140.dll	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
3904	Install_x64.exe	GET	200	188.114.96.3:80	http://xilloolli.com/api-debug.php?status=7&proc=Intel(R)%20Core(TM)%20i5-6400%20CPU%20@%202.70GHz&av=1	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown
6280	BitLockerToGo.exe	POST	200	147.45.47.68:80	http://147.45.47.68/a8f961c72f0d877c.php	unknown	—	—	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:138	—	—	—	whitelisted
5600	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
5116	RUXIMICS.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2120	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
3888	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
6600	chrome.exe	142.250.110.84:443	accounts.google.com	GOOGLE	US	unknown
6328	chrome.exe	239.255.255.250:1900	—	—	—	whitelisted
6600	chrome.exe	188.114.97.3:443	crypto-whales.io	CLOUDFLARENET	NL	unknown
6600	chrome.exe	151.101.2.137:443	code.jquery.com	FASTLY	US	unknown
6600	chrome.exe	142.250.185.106:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
5600	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6600	chrome.exe	142.250.185.68:443	www.google.com	GOOGLE	US	whitelisted
6600	chrome.exe	95.216.241.251:443	z5dy0w9re.top	Hetzner Online GmbH	FI	unknown
5336	SearchApp.exe	104.126.37.154:443	www.bing.com	Akamai International B.V.	DE	unknown
5336	SearchApp.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3260	svchost.exe	40.115.3.253:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4436	svchost.exe	40.126.32.72:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
4436	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
5048	backgroundTaskHost.exe	20.74.47.205:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	unknown
5048	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4060	backgroundTaskHost.exe	104.126.37.154:443	www.bing.com	Akamai International B.V.	DE	unknown
5336	SearchApp.exe	104.126.37.144:443	www.bing.com	Akamai International B.V.	DE	unknown
6328	chrome.exe	224.0.0.251:5353	—	—	—	unknown

2120	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2240	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2240	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4936	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
4936	SIHClient.exe	52.165.164.15:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6600	chrome.exe	142.250.186.131:443	update.googleapis.com	GOOGLE	US	whitelisted
5052	svchost.exe	34.104.35.123:80	edgedl.me.gvt1.com	GOOGLE	US	whitelisted
6600	chrome.exe	216.58.206.46:443	clients1.google.com	GOOGLE	US	whitelisted
2656	OfficeClickToRun.exe	52.111.229.19:443	nexusrules.officeapps.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6600	chrome.exe	216.58.212.174:443	sb-ssl.google.com	GOOGLE	US	whitelisted
3904	Install_x64.exe	188.114.96.3:80	crypto-whales.io	CLOUDFLARENET	NL	unknown
3904	Install_x64.exe	188.114.97.3:80	crypto-whales.io	CLOUDFLARENET	NL	unknown
2476	BitLockerToGo.exe	104.21.57.45:443	samledwwekspzxp.shop	CLOUDFLARENET	—	unknown
7112	chrome.exe	142.250.185.131:443	update.googleapis.com	GOOGLE	US	whitelisted
6280	BitLockerToGo.exe	147.45.47.68:80	—	OOO FREEnet Group	RU	unknown

DNS requests

Domain	IP	Reputation
google.com	142.250.186.174	whitelisted
crypto-whales.io	188.114.97.3 188.114.96.3	unknown
accounts.google.com	142.250.110.84	whitelisted
code.jquery.com	151.101.2.137 151.101.130.137 151.101.194.137 151.101.66.137	whitelisted
content-autofill.googleapis.com	142.250.185.106 142.250.185.202 142.250.186.138 142.250.186.74 172.217.18.10 172.217.23.106 142.250.184.202 216.58.212.138 142.250.186.170 142.250.185.234 216.58.206.74 142.250.186.42 172.217.16.202 142.250.186.106 216.58.206.42 142.250.185.170	whitelisted
settings-win.data.microsoft.com	4.231.128.59 20.73.194.208 40.127.240.158	whitelisted
www.google.com	142.250.185.68	whitelisted
z5dy0w9re.top	95.216.241.251	unknown
09lbiq6ms.top	95.216.241.251	unknown
www.bing.com	104.126.37.154 104.126.37.162 104.126.37.137 104.126.37.144 104.126.37.152 104.126.37.139 104.126.37.161 104.126.37.147	whitelisted

	104.126.37.160	
ocsp.digicert.com	192.229.221.95	whitelisted
client.wns.windows.com	40.115.3.253	whitelisted
login.live.com	40.126.32.72 40.126.32.133 40.126.32.74 40.126.32.134 40.126.32.136 40.126.32.76 20.190.160.20 40.126.32.68	whitelisted
fd.api.iris.microsoft.com	20.74.47.205	whitelisted
th.bing.com	104.126.37.144 104.126.37.186 104.126.37.128 104.126.37.137 104.126.37.147 104.126.37.179 104.126.37.130 104.126.37.129 104.126.37.139	whitelisted
arc.msn.com	20.223.35.26	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15	whitelisted
update.googleapis.com	142.250.186.131 142.250.185.131	whitelisted
edgedl.me.gvt1.com	34.104.35.123	whitelisted
clients1.google.com	216.58.206.46	whitelisted
nexusrules.officeapps.live.com	52.111.229.19	whitelisted
sb-ssl.google.com	216.58.212.174	whitelisted
xilloolli.com	188.114.96.3 188.114.97.3	unknown
firvfirv.com	188.114.97.3 188.114.96.3	unknown
samledwwekspzxp.shop	104.21.57.45 172.67.189.34	unknown

Threats

PID	Process	Class	Message
6600	chrome.exe	Not Suspicious Traffic	INFO [ANY.RUN] jQuery JavaScript Library Code Loaded (code .jquery .com)
6600	chrome.exe	Not Suspicious Traffic	INFO [ANY.RUN] jQuery JavaScript Library Code Loaded (code .jquery .com)
6600	chrome.exe	Potentially Bad Traffic	ET DNS Query to a *.top domain - Likely Hostile
3904	Install_x64.exe	A Network Trojan was detected	ET MALWARE Single char EXE direct download likely trojan (multiple families)
3904	Install_x64.exe	Misc activity	ET INFO Packed Executable Download
3904	Install_x64.exe	Potential Corporate **Privacy** Violation	ET POLICY PE EXE or DLL Windows file download HTTP
3904	Install_x64.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
3904	Install_x64.exe	A Network Trojan was detected	ET MALWARE Single char EXE direct download likely trojan (multiple families)
2476	BitLockerToGo.exe	A Network Trojan was detected	STEALER [ANY.RUN] Lumma Stealer TLS Connection
3904	Install_x64.exe	A Network Trojan was detected	ET MALWARE Single char EXE direct download likely trojan (multiple families)
6280	BitLockerToGo.exe	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 23
6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	STEALER [ANY.RUN] Stealc HTTP POST Request
6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	ET MALWARE [SEKOIA.IO] Win32/Stealc C2 Check-in
6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	ET MALWARE Win32/Stealc Requesting browsers Config from C2

6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	ET MALWARE Win32/Stealc Requesting plugins Config from C2
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for sqlite3.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	ET MALWARE Win32/Stealc Submitting System Information to C2
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
6280	BitLockerToGo.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for freebl3.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for mozglue.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for nss3.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for softokn3.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	A suspicious filename was detected	ET HUNTING HTTP GET Request for vcruntime140.dll - Possible Infostealer Activity
6280	BitLockerToGo.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
6280	BitLockerToGo.exe	Malware Command and Control Activity Detected	ET MALWARE Win32/Stealc Submitting Screenshot to C2

Debug output strings

No debug info