ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	windows.storage.dll
Full analysis:	https://app.any.run/tasks/e70d2f58-b32a-4fb7-8836-de4def184cee
Verdict:	Malicious activity
Analysis date:	November 22, 2025 at 18:34:07
OS:	Windows 10 Professional (build: 19044, 64 bit)
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32+ executable (DLL) (console) x86-64, for MS Windows, 8 sections
MD5:	9A10131F6F32EF5356304EF6B754A9E3
SHA1:	33AB5DF5531C32270494913EA876A1C1BEC30CAC
SHA256:	A2B0C3C0BE9F99AEEC4310739915DDF8D09463566DA5506FA30A0776DEF6770C
SSDEEP:	196608:UKCnlF92sSjZUhFhg4N3Ze3qQQVfBsEkFD/:U/c

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)
- FileZilla 3.65.0 (3.65.0)
- 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)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)

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 (16.0.15928.20198)
- 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	SUSPICIOUS	INFO
The DLL Hijacking • regsvr32.exe (PID: 7368)	**Process drops legitimate windows executable** • regsvr32.exe (PID: 7368)	**The sample compiled with english language support** • regsvr32.exe (PID: 7368)

Malware configuration

No Malware configuration.

Static information

TRiD

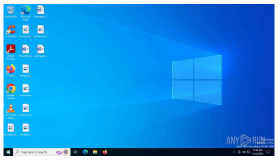
.exe	|	Win64 Executable (generic) (87.3)
.exe	|	Generic Win/DOS Executable (6.3)
.exe	|	DOS Executable Generic (6.3)

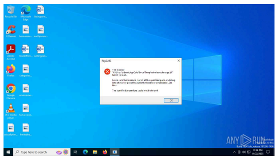
EXIF

EXE

MachineType:	AMD AMD64
TimeStamp:	2086:03:19 03:23:16+00:00
ImageFileCharacteristics:	Executable, Large address aware, DLL
PEType:	PE32+
LinkerVersion:	14.38
CodeSize:	6606848
InitializedDataSize:	2158592
UninitializedDataSize:	-
EntryPoint:	0x361ce0
OSVersion:	10
ImageVersion:	10
SubsystemVersion:	10
Subsystem:	Windows command line
FileVersionNumber:	10.0.26100.7171
ProductVersionNumber:	10.0.26100.7171
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Windows NT 32-bit
ObjectFileType:	Dynamic link library
FileSubtype:	-
LanguageCode:	English (U.S.)
CharacterSet:	Unicode
CompanyName:	Microsoft Corporation
FileDescription:	Microsoft WinRT Storage API
FileVersion:	10.0.26100.7171 (WinBuild.160101.0800)
InternalName:	Windows.Storage
LegalCopyright:	© Microsoft Corporation. All rights reserved.
OriginalFileName:	Windows.Storage.dll
ProductName:	Microsoft® Windows® Operating System
ProductVersion:	10.0.26100.7171

Video and screenshots



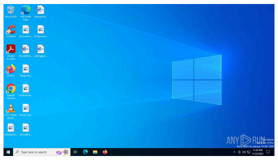


RegSvr32

The module "C:\Users\admin\AppData\Local\Temp\windows.storage.dll" failed to load.

Make sure the binary is stored at the specified path or debug it to check for problems with the binary or dependent .DLL files.

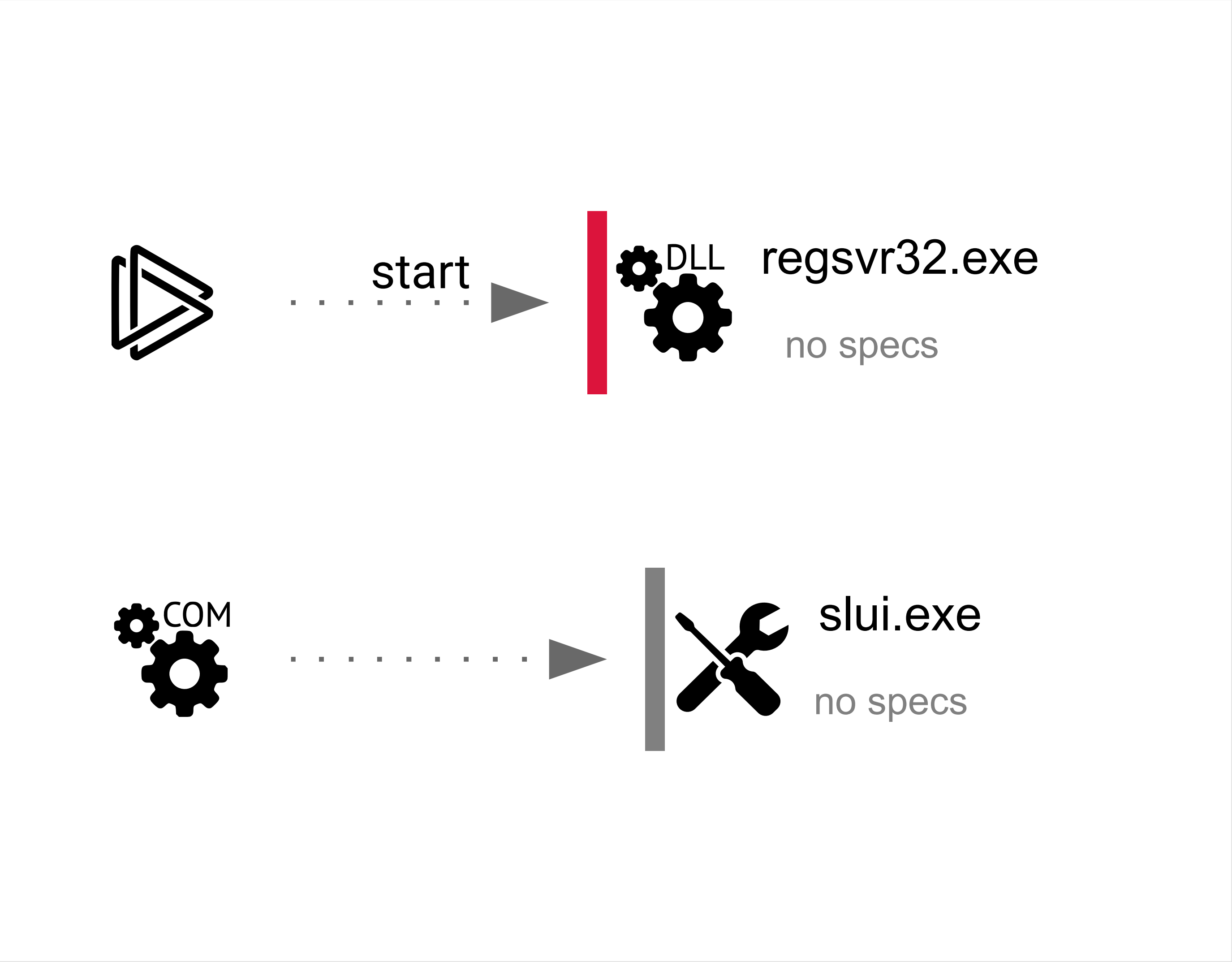
The specified procedure could not be found.



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
145	2	1	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
4804	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)		

7368	"C:\WINDOWS\System32\regsvr32.exe" C:\Users\admin\AppData\Local\Temp\windows.storage.dll	C:\Windows\System32\regsvr32.exe	—	explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft(C) Register Server
Exit code:	3	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

Registry activity

Total events	Read events	Write events	Delete events
0	0	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	0	0

Dropped files

No data

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
9	30	15	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6884	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
5596	MoUsoCoreWorker.exe	GET	200	2.16.164.49:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.16.164.49:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7984	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2348	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
6884	svchost.exe	40.126.31.3:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5596	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
—	—	2.16.204.135:443	www.bing.com	Akamai International B.V.	DE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
6884	svchost.exe	40.126.31.2:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5596	MoUsoCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6884	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
5596	MoUsoCoreWorker.exe	2.16.164.49:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
4328	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3440	svchost.exe	172.211.123.250:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
2348	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5524	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2348	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7984	SIHClient.exe	74.178.76.128:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7984	SIHClient.exe	2.23.181.156:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
7984	SIHClient.exe	2.16.164.49:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
7984	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4324	slui.exe	4.154.185.43:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 4.231.128.59 51.104.136.2	whitelisted
login.live.com	40.126.31.3 40.126.31.2 20.190.159.23 20.190.159.68 40.126.31.129 40.126.31.71 20.190.159.131 40.126.31.131	whitelisted
www.bing.com	2.16.204.135 2.16.204.160 2.16.204.138 2.16.204.161 2.16.204.148 2.16.204.158 2.16.204.155	whitelisted
google.com	142.250.186.78	whitelisted
ocsp.digicert.com	184.30.131.245	whitelisted
crl.microsoft.com	2.16.164.49 2.16.164.120	whitelisted
client.wns.windows.com	172.211.123.250	whitelisted
slscr.update.microsoft.com	74.178.76.128	whitelisted
www.microsoft.com	2.23.181.156	whitelisted
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted

activation-v2.sls.microsoft.com	4.154.185.43	whitelisted

Threats

PID	Process	Class	Message
—	—	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Debug output strings

No debug info

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN