ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	sample-1.eml
Full analysis:	https://app.any.run/tasks/607c024c-28a4-49fc-a515-af3c84a91c9f
Verdict:	No threats detected
Analysis date:	November 16, 2025 at 19:08:14
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	message/rfc822
File info:	RFC 822 mail, Unicode text, UTF-8 text, with CRLF line terminators
MD5:	4CA6586577DA9BC304FC0E11CC0A1F53
SHA1:	1A301B3D06A0ABCF7F9B97E4DF076A802331DC99
SHA256:	35EF116A75E5E46E6859B49B60A23B4DDFE5F91D1368E0FC67A16DF698CB96E0
SSDEEP:	192:4v96wuGv7ugYcXerGF3T5r9kfnWPOrzuynp3gag9ip9dFswHCy/9pRgmsZi5TgqP:4v9HjkiqGFrsWGnDQp9O5lpRm4pZabi

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)
- 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)

Hotfixes

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

- Update for Windows 10 for x64-based Systems (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
No malicious indicators.	No suspicious indicators.	No info indicators.

Malware configuration

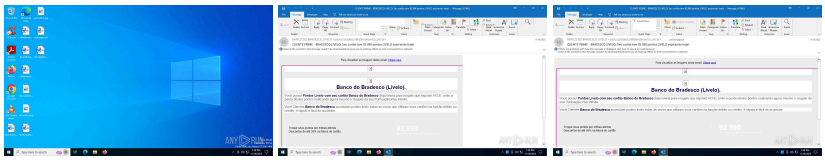
No Malware configuration.

Static information

TRiD

.eml | E-Mail message (Var. 5) (100)

Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
150	3	0	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
2772	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)		

7516	"C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml C:\Users\admin\AppData\Local\Temp\sample-1.eml	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE	↔	explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Outlook
Version:	16.0.16026.20146		

7944	"C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe" "D34C7BB4-6871-4A5B-B168-6FCEBC220515" "4656FB68-672B-4AB7-8464-1B9A8EB0F33B" "7516"	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe	–	OUTLOOK.EXE

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Artificial Intelligence (AI) Host for the Microsoft® Windows® Operating System and Platform x64.
Version:	0.12.2.0		

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	6	3	0

Dropped files

PID	Process	Filename	Type
7516	OUTLOOK.EXE	C:\Users\admin\Documents\Outlook Files\Outlook1.pst **MD5:** – **SHA256:** –	–
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres **MD5:** 54CC5E85AC2971753C8BF173AE26EFC8 **SHA256:** B4DB157DAB428323DE96380A04D138484F8E795DBBF2E45DA42C004C3EFCF63E	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntities.bin **MD5:** CC90D669144261B198DEAD45AA266572 **SHA256:** 89C701EEFF939A44F28921FD85365ECD87041935DCD0FE0BAF04957DA12C9899	text
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres **MD5:** 6648E8540A0EF16861D24DBB756ACE00 **SHA256:** 3E64C92D34520E62236474A2024A73FE291199840B0FFFF37673952EDF4402CB	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntitiesUpdated.bin **MD5:** 3D90EDA2FF5F6FE91E24EA745914CE31 **SHA256:** 5D0D86E0376DB414CEF21752529F29166DB14080448B94C9EA8354F1BEF7C5E0	text
7516	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** C66B95DA4D7EA4E8213C4FCC26B4A5E2 **SHA256:** 007B55A15C4FAFFE2347F9ECFBE8FE390977195F84921FECD0F40C2873379367	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres **MD5:** EBCF38822FEAF9496B54B82C71EC4D6A **SHA256:** E24983E51D8AC0C05C567D81769B2745BBABB73EC7101DE77B8D683D51EB8F0F	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** FB2F6038783A6E5279203E93F493D9E8 **SHA256:** 09C3190E12180ACB596CFFA64C54981A57BB8FE0FD00D55B94676A6BFC37E877	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$rmalEmail.dotm **MD5:** D2A99E0799D16A182902D9D651A2FE3E **SHA256:** B5059964FF28019D41D8360C8B9B9CDFF62185FF5909C7D39BBA201331EC8EE4	binary
7516	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TableViewPreviewPrefs_2_DDE574647E20AA4B8DA5B54C87A829E4.dat **MD5:** 0E092DB99AEE99FDFF9B5B222C732CFD **SHA256:** D1614AD99ADED9F6F5C1BE7FE7FFA5124BD04A526580DA3818EA8A954E852AA6	xml

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats

10 29 21 1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2576	svchost.exe	GET	200	95.101.78.32:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
2620	svchost.exe	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	2.19.126.146:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
7516	OUTLOOK.EXE	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIulA%3D	unknown	—	—	whitelisted
3208	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	—	—	whitelisted
2576	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5596	MoUsoCoreWorker.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4452	RUXIMICS.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
7088	SearchApp.exe	2.16.204.142:443	www.bing.com	Akamai International B.V.	DE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
7516	OUTLOOK.EXE	52.123.129.14:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7516	OUTLOOK.EXE	2.19.198.51:443	omex.cdn.office.net	Akamai International B.V.	DE	whitelisted
7516	OUTLOOK.EXE	52.111.243.8:443	messaging.lifecycle.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2576	svchost.exe	95.101.78.32:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
7516	OUTLOOK.EXE	20.42.65.94:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2620	svchost.exe	40.126.31.130:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7516	OUTLOOK.EXE	23.63.118.230:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
2620	svchost.exe	23.63.118.230:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
3440	svchost.exe	172.211.123.250:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
5596	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5596	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3208	SIHClient.exe	74.178.240.61:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3208	SIHClient.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
3208	SIHClient.exe	2.19.126.146:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
3208	SIHClient.exe	20.3.187.198:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5612	slui.exe	4.154.209.85:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	51.124.78.146 40.127.240.158 51.104.136.2	whitelisted
www.bing.com	2.16.204.142 2.16.204.137 2.16.204.161 2.16.204.146 2.16.204.135 2.16.204.139 2.16.204.138 2.16.204.141 2.16.204.157	whitelisted
google.com	142.250.186.46	whitelisted
ecs.office.com	52.123.129.14 52.123.128.14	whitelisted
omex.cdn.office.net	2.19.198.51 2.19.198.40 2.19.198.58	whitelisted
messaging.lifecycle.office.com	52.111.243.8	whitelisted
crl.microsoft.com	95.101.78.32 95.101.78.42 2.19.126.146 2.19.126.133	whitelisted
self.events.data.microsoft.com	20.42.65.94	whitelisted
login.live.com	40.126.31.130 40.126.31.0 20.190.159.4 20.190.159.73 40.126.31.2 20.190.159.71 20.190.159.130 20.190.159.2	whitelisted
ocsp.digicert.com	23.63.118.230	whitelisted
client.wns.windows.com	172.211.123.250	whitelisted
slscr.update.microsoft.com	74.178.240.61	whitelisted
www.microsoft.com	95.101.149.131	whitelisted
fe3cr.delivery.mp.microsoft.com	20.3.187.198	whitelisted
activation-v2.sls.microsoft.com	4.154.209.85	whitelisted

Threats

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

Debug output strings

No debug info