ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	sample-100.eml
Full analysis:	https://app.any.run/tasks/f339bd16-ca65-4f5a-bb29-c3ca3e6abb1b
Verdict:	No threats detected
Analysis date:	November 16, 2025 at 19:24:16
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	message/rfc822
File info:	RFC 822 mail, Unicode text, UTF-8 text, with very long lines (396), with CRLF line terminators
MD5:	4DD77CA48BA1C3437713B8DD8B4EFF7E
SHA1:	34096D58535F2C201B15FB577BB9316BE5B8EFE5
SHA256:	9FB2E491E28E6848614AE9539E2F685EE5C75357339505998B91FB9B89B3127E
SSDEEP:	192:I006uT+iv2fXCMzy8tq5a8WTv1IfEKqfWsd313GesvYwHsgOTvfcn+7ejXdG:B0PZz368kv1bQIcn+yxG

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

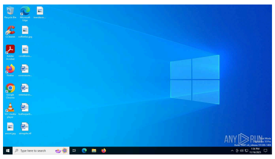
No Malware configuration.

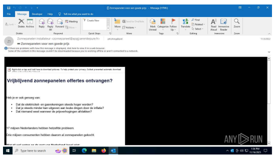
Static information

TRiD

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

Video and screenshots





Zonnepanelen voor een goede prijs - Message (HTML)

Zonnepanelen installateur <zonnepaneel@appjj.serenitepure.fr>

Zonnepanelen voor een goede prijs

Vrijblijvend zonnepanelen offertes ontvangen?

Heb je er ook genoeg van:

- Dat de elektriciteit- en gasrekeningen steeds hoger worden?
- Dat je steeds minder kan uitgeven aan leuke dingen door de inflatie?
- Dat niemand weet wanneer de prijsverhogingen afvlakken?

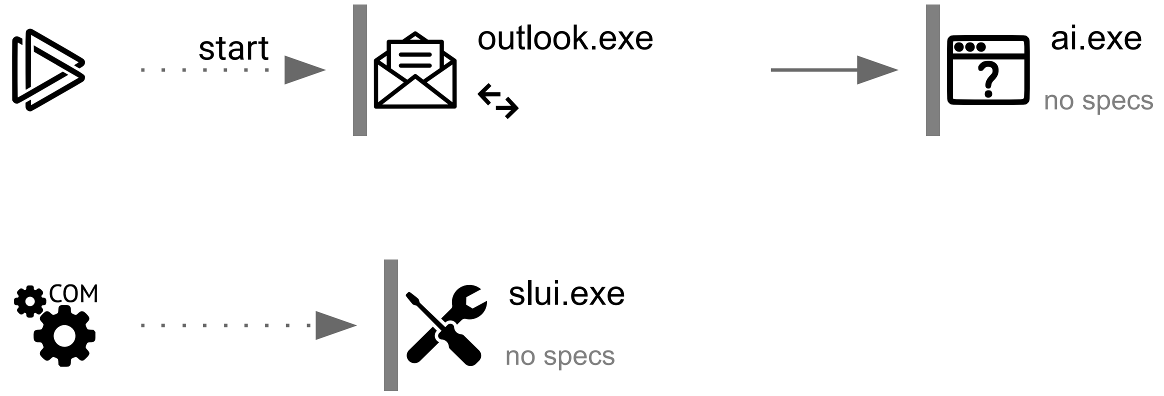
17 miljoen Nederlanders hebben hetzelfde probleem.

Drie miljoen consumenten hebben daarom al zonnepanelen gekocht.

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:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml C:\Users\admin\AppData\Local\Temp\sample-100.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		

5516	"C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe" "F3AAE6D4-F483-41EC-95F8-5B87EB915A3D" "7F8B7E02-2CE3-404E-8373-D3ADCB9F6E22" "2772"	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		

7792	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)		

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	4	0

Dropped files

PID	Process	Filename	Type
2772	OUTLOOK.EXE	C:\Users\admin\Documents\Outlook Files\Outlook1.pst **MD5:** — **SHA256:** —	—
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres **MD5:** D03382AF919D8E028A47065C2A02ABCD **SHA256:** 4D82F96FAB359FDC02F14397AFEB8796ECBCB457BB5992B4BC9D29A7E00B9FEA	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres **MD5:** 44FB6210495B3CDD640B0A1CCFEA280B **SHA256:** 3405FF1754A7DDA7C379609646EC92AD6B67D59AD0AE99DC6825561F0229AC50	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntities.bin **MD5:** CC90D669144261B198DEAD45AA266572 **SHA256:** 89C701EEFF939A44F28921FD85365ECD87041935DCD0FE0BAF04957DA12C9899	text
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntitiesUpdated.bin **MD5:** C8182E810828B5EF8A29FBB43D8F1088 **SHA256:** 38EF21555BBDBC75ACC43857C7A30395384C3A5C32B039E5C23653841C0C34DD	text
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres **MD5:** 355BA75DFCC7A002389BA3CFA8BB4A44 **SHA256:** C04CAAE23B7A409A5E37F6B34F1D5F813550E990D98E70C0A57B7BD9D1DF3022	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$rmalEmail.dotm **MD5:** FEDA863B661A9B4B668136A0401D7C4C **SHA256:** 69450ED772C2B9E17E8A409419CDD481C51A46197337BD59695A2524F248C686	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** C66B95DA4D7EA4E8213C4FCC26B4A5E2 **SHA256:** 007B55A15C4FAFFE2347F9ECFBE8FE390977195F84921FECD0F40C2873379367	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TableViewPreviewPrefs_2_7F6CA4AF0FF9FB4B9A7F3E032CFFDD99.dat **MD5:** 0E092DB99AEE99FDFF9B5B222C732CFD **SHA256:** D1614AD99ADED9F6F5C1BE7FE7FFA5124BD04A526580DA3818EA8A954E852AA6	xml
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\outlook.exe_Rules.xml **MD5:** B8A666F1A403D48066B9AE7F2907661A **SHA256:** FA935E867528B36EB08B73428ABB58B741F79679E6A753A5180A26017CAEFBF8	—
2772	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** 5EC1E6FF823DE42921C50123CFE6475C **SHA256:** 46C3648FD51C60F4A3EFCA837F107F7DD13F1FED6E3A075BEE33961DE816D17D	binary
2772	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Temp\mso27B1.tmp **MD5:** ED3C1C40B68BA4F40DB15529D5443DEC **SHA256:** 039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A	image

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
10	29	20	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6432	svchost.exe	GET	200	95.101.78.32:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
2772	OUTLOOK.EXE	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIulA%3D	unknown	—	—	whitelisted
6076	svchost.exe	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	95.101.78.32:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
7632	SIHClient.exe	GET	200	23.59.18.102:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
5596	MoUsoCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
2852	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6432	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
2772	OUTLOOK.EXE	52.123.128.14:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2772	OUTLOOK.EXE	2.19.198.51:443	omex.cdn.office.net	Akamai International B.V.	DE	whitelisted
2772	OUTLOOK.EXE	52.111.243.8:443	messaging.lifecycle.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6432	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6432	svchost.exe	95.101.78.32:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
2772	OUTLOOK.EXE	51.104.15.252:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	GB	whitelisted
2772	OUTLOOK.EXE	23.63.118.230:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
6076	svchost.exe	20.190.159.128:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6076	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	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7632	SIHClient.exe	74.179.77.204:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7632	SIHClient.exe	23.59.18.102:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
7632	SIHClient.exe	95.101.78.32:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
7632	SIHClient.exe	20.3.187.198:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2636	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	4.231.128.59 20.73.194.208 51.104.136.2	whitelisted
google.com	216.58.212.142	whitelisted
ecs.office.com	52.123.128.14 52.123.129.14	whitelisted
omex.cdn.office.net	2.19.198.51 2.19.198.58 23.32.238.120	whitelisted
messaging.lifecycle.office.com	52.111.243.8	whitelisted
crl.microsoft.com	95.101.78.32 95.101.78.42	whitelisted
self.events.data.microsoft.com	51.104.15.252	whitelisted
ocsp.digicert.com	23.63.118.230	whitelisted
login.live.com	20.190.159.128 40.126.31.130 20.190.159.0 40.126.31.129 40.126.31.2 20.190.159.23 40.126.31.131 20.190.159.4	whitelisted
client.wns.windows.com	172.211.123.250	whitelisted
slscr.update.microsoft.com	74.179.77.204	whitelisted
www.microsoft.com	23.59.18.102	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

ANY.RUN
INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN