ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	sample-1077.eml
Full analysis:	https://app.any.run/tasks/fa8c1d7b-eaa2-4112-91f1-b2c7ab27cf52
Verdict:	No threats detected
Analysis date:	November 16, 2025 at 20:58:11
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	message/rfc822
File info:	RFC 822 mail, ASCII text, with very long lines (347), with CRLF line terminators
MD5:	1216E237544F77D4F2B967F2D79D051A
SHA1:	2E3107C97055DDDC5166466958D1846F1EE19400
SHA256:	51E70916ED035685DE2DDE3513D8AC831A5BD2098F83E5D3C0FE665D086911DA
SSDEEP:	384:KjYoHI4QMZX+SYJpRo3eqI5HAGIIlOIxII0tIISII2Iu22L:Kj1HI41ZX+SCpRoFI9dIIlOIOI0tIIS2

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

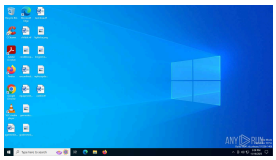
No Malware configuration.

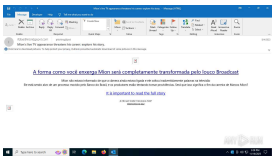
Static information

TRiD

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

Video and screenshots

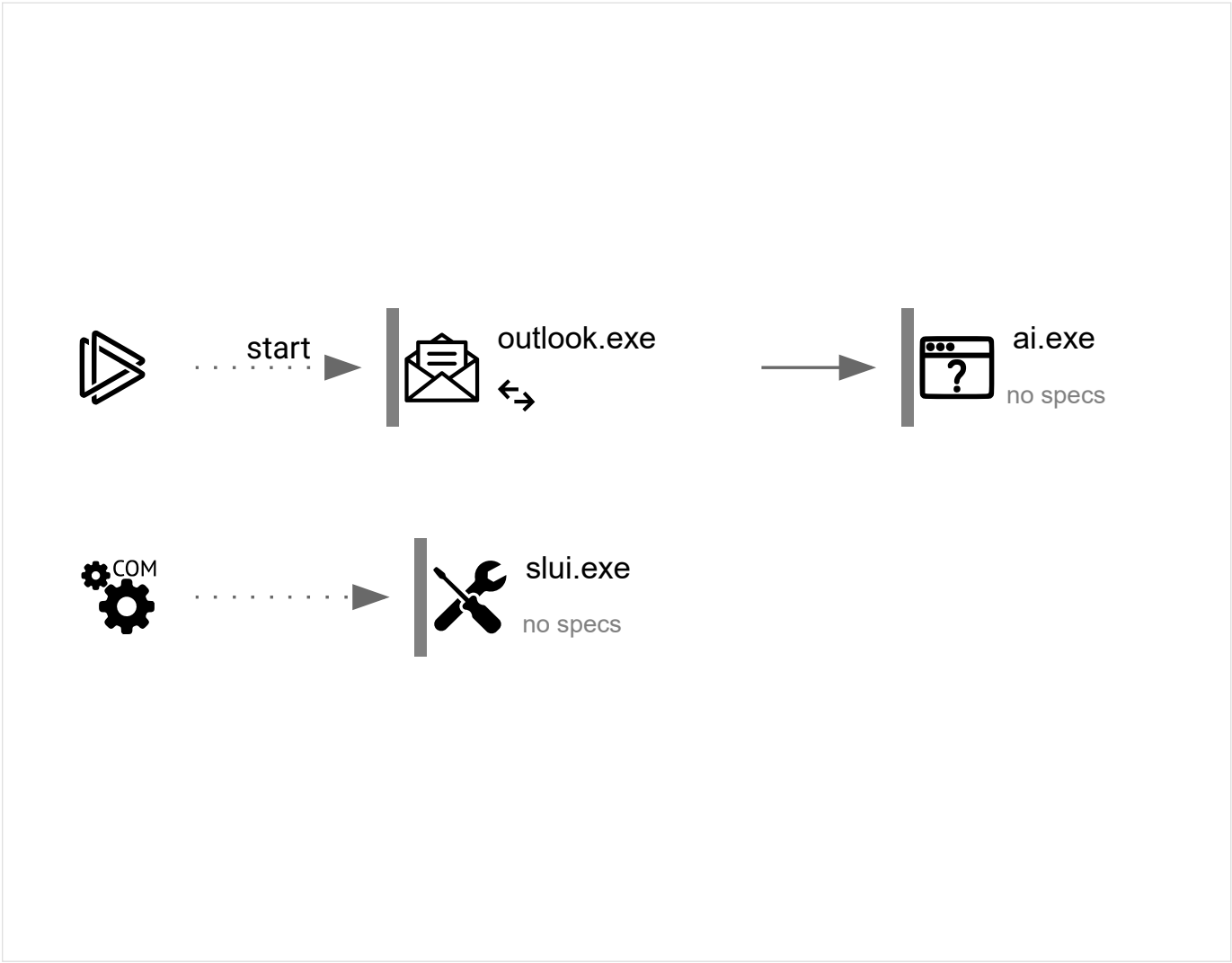




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
152	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
3460	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)		

7424	"C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml C:\Users\admin\AppData\Local\Temp\sample-1077.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		

7964	"C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe" "4E575C64-C873-43E6-A7FC-11B3DF26C4B7" "019244C7-D095-42E7-BD6F-790493EC6CB3" "7424"	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	8	4	0

Dropped files

PID	Process	Filename	Type
7424	OUTLOOK.EXE	C:\Users\admin\Documents\Outlook Files\Outlook1.pst **MD5:** – **SHA256:** –	–
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntitiesUpdated.bin **MD5:** 73F23B92E8DEE0E3B54E985CACFB5FB8 **SHA256:** 098920DE7C0CF03FDA975D14F3941E824CCEFC6F88B8C6B6BFB5A6E42D51B06A	text
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres **MD5:** 987D8D8CC8248D2D8CE57680F4E801EB **SHA256:** CE34455F33F5DE07097DE2EE270FD3919C71A3811F7E2A35B029BE1E79238449	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** 5FA6DBD5FF48810A045CFD2631B254D0 **SHA256:** 394759F34638127A9F8DFFD45AE6D258C3E5F72CAFFBF094663C0B6D4EAF1EE0	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBFE4F7A916411C1E69BDD97BB04 **MD5:** C66B95DA4D7EA4E8213C4FCC26B4A5E2 **SHA256:** 007B55A15C4FAFFE2347F9ECFBE8FE390977195F84921FECD0F40C2873379367	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\45344D15-FB0C-4916-934D-84F7CBB066E5 **MD5:** 4856FB63BBC2EB84451BB849006F91AD **SHA256:** 80DD02E62ACFBAA1B6D61DCFA83AD2620F4DC85BD394F5AE1CE94B634DF6AD47	xml
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$rmalEmail.dotm **MD5:** 70EBD9D0C5854B4ED3738EE37B7E8222 **SHA256:** 9BA26331B113AC7EB8EF2627B4E3A006BB44505696A770177BB5413A9C094099	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A **MD5:** 3496C32EA7810693CF0A66187598BA4B **SHA256:** D429579C04D42E3B15E6254548ACDF9B8D14B1A0E77F114492F8DBE90F3D2BD6	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntities.bin **MD5:** CC90D669144261B198DEAD45AA266572 **SHA256:** 89C701EEFF939A44F28921FD85365ECD87041935DCD0FE0BAF04957DA12C9899	text
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres **MD5:** 7DE31CBC9B43BD8CE1CAE99FD143AC39 **SHA256:** BA5EB8D3A60E2FD3912765B5528B2CF79B9964A71D179744D462E077B8AAD2DA	binary
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TableViewPreviewPrefs_2_A84B69DADD93474782FBA4D2F27D29F5.dat **MD5:** 0E092DB99AEE99FDFF9B5B222C732CFD **SHA256:** D1614AD99ADED9F6F5C1BE7FE7FFA5124BD04A526580DA3818EA8A954E852AA6	xml
7424	OUTLOOK.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres **MD5:** 172F2C2B61B5336DF7358CEFD2B4FA8D **SHA256:** 605EE19B27AE44569892F88F25B38B8C50B114BEBBE71E36EEA65AF38548A075	binary

7424	OUTLOOK.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A	binary
		MD5: E6884396691055AB1143B74258942A9A	**SHA256:** B2797225BF906D1487B2A5FA6C7B6CCD00C685FDF804BA75F6F39BD37625DE40

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
11	33	24	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
4420	svchost.exe	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted
7424	OUTLOOK.EXE	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHI3O1J0%3D	unknown	–	–	whitelisted
2316	svchost.exe	GET	200	95.101.78.32:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
7424	OUTLOOK.EXE	GET	200	23.63.118.230:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIulA%3D	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	95.101.78.32:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	–	–	whitelisted
3356	SIHClient.exe	GET	200	2.16.253.202:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	whitelisted
2316	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5320	RUXIMICS.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
–	–	2.16.204.151:443	www.bing.com	Akamai International B.V.	DE	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
7424	OUTLOOK.EXE	52.109.32.97:443	officeclient.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	GB	whitelisted
7424	OUTLOOK.EXE	52.123.128.14:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7424	OUTLOOK.EXE	52.110.17.11:443	roaming.svc.cloud.microsoft	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7424	OUTLOOK.EXE	23.63.118.230:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
7424	OUTLOOK.EXE	23.32.238.120:443	omex.cdn.office.net	Akamai International B.V.	DE	whitelisted
7424	OUTLOOK.EXE	52.111.243.8:443	messaging.lifecycle.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
7424	OUTLOOK.EXE	4.251.34.91:443	nleditor.osi.office.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4420	svchost.exe	20.190.159.2:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4420	svchost.exe	23.63.118.230:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
2316	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2316	svchost.exe	95.101.78.32:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted

7424	OUTLOOK.EXE	20.189.173.28:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3440	svchost.exe	172.211.123.248:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
5596	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3356	SIHClient.exe	135.232.92.137:443	slscr.update.microsoft.com	LUCENT-CIO	US	whitelisted
3356	SIHClient.exe	2.16.253.202:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
3356	SIHClient.exe	95.101.78.32:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
3356	SIHClient.exe	52.165.164.15:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3356	SIHClient.exe	135.233.95.144:443	slscr.update.microsoft.com	LUCENT-CIO	US	whitelisted
2628	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 20.73.194.208	whitelisted
www.bing.com	2.16.204.151 2.16.204.161 2.16.204.135 2.16.204.152 2.16.204.141 2.16.204.136 2.16.204.159 2.16.204.145 2.16.204.138	whitelisted
google.com	142.250.185.206	whitelisted
officeclient.microsoft.com	52.109.32.97	whitelisted
ecs.office.com	52.123.128.14 52.123.129.14	whitelisted
roaming.svc.cloud.microsoft	52.110.17.11 52.110.17.52 52.110.17.75 52.110.17.32 52.110.17.39 52.110.17.60 52.110.17.68 52.110.17.71	whitelisted
ocsp.digicert.com	23.63.118.230	whitelisted
omex.cdn.office.net	23.32.238.120 2.19.198.58 23.32.238.155 2.19.198.51 2.19.198.40	whitelisted
messaging.lifecycle.office.com	52.111.243.8	whitelisted
nleditor.osi.office.net	4.251.34.91	whitelisted
login.live.com	20.190.159.2 40.126.31.128 40.126.31.2 40.126.31.67 20.190.159.68 20.190.159.129 40.126.31.0 20.190.159.130	whitelisted
crl.microsoft.com	95.101.78.32 95.101.78.42	whitelisted
self.events.data.microsoft.com	20.189.173.28	whitelisted
client.wns.windows.com	172.211.123.248	whitelisted
slscr.update.microsoft.com	135.232.92.137 135.233.95.144	whitelisted
www.microsoft.com	2.16.253.202	whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15	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
© 2017-2025 ANY.RUN LLC. ALL RIGHTS RESERVED