ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	nicoelsoto.pdf
Full analysis:	https://app.any.run/tasks/7d00667b-97b9-4245-8fb6-834f06db746e
Verdict:	No threats detected
Analysis date:	September 23, 2025 at 21:30:07
OS:	Windows 10 Professional (build: 19044, 64 bit)
MIME:	text/plain
File info:	ASCII text, with CRLF line terminators
MD5:	81051BCC2CF1BEDF378224B0A93E2877
SHA1:	BA8AB5A0280B953AA97435FF8946CBCBB2755A27
SHA256:	7EB70257593DA06F682A3DDDA54A9D260D4FC514F645237F5CA74B08F8DA61A6
SSDEEP:	3:y:y

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	60 seconds	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)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)

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 (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.	**Reads security settings of Internet Explorer** • notepad.exe (PID: 4948) **Checks proxy server information** • slui.exe (PID: 4552) **Reads the software policy settings** • slui.exe (PID: 4552)

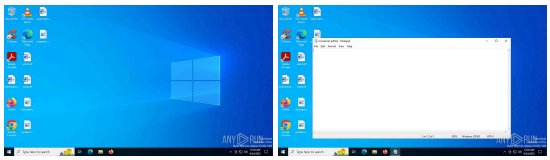
Malware configuration

No Malware configuration.

Static information

No data.

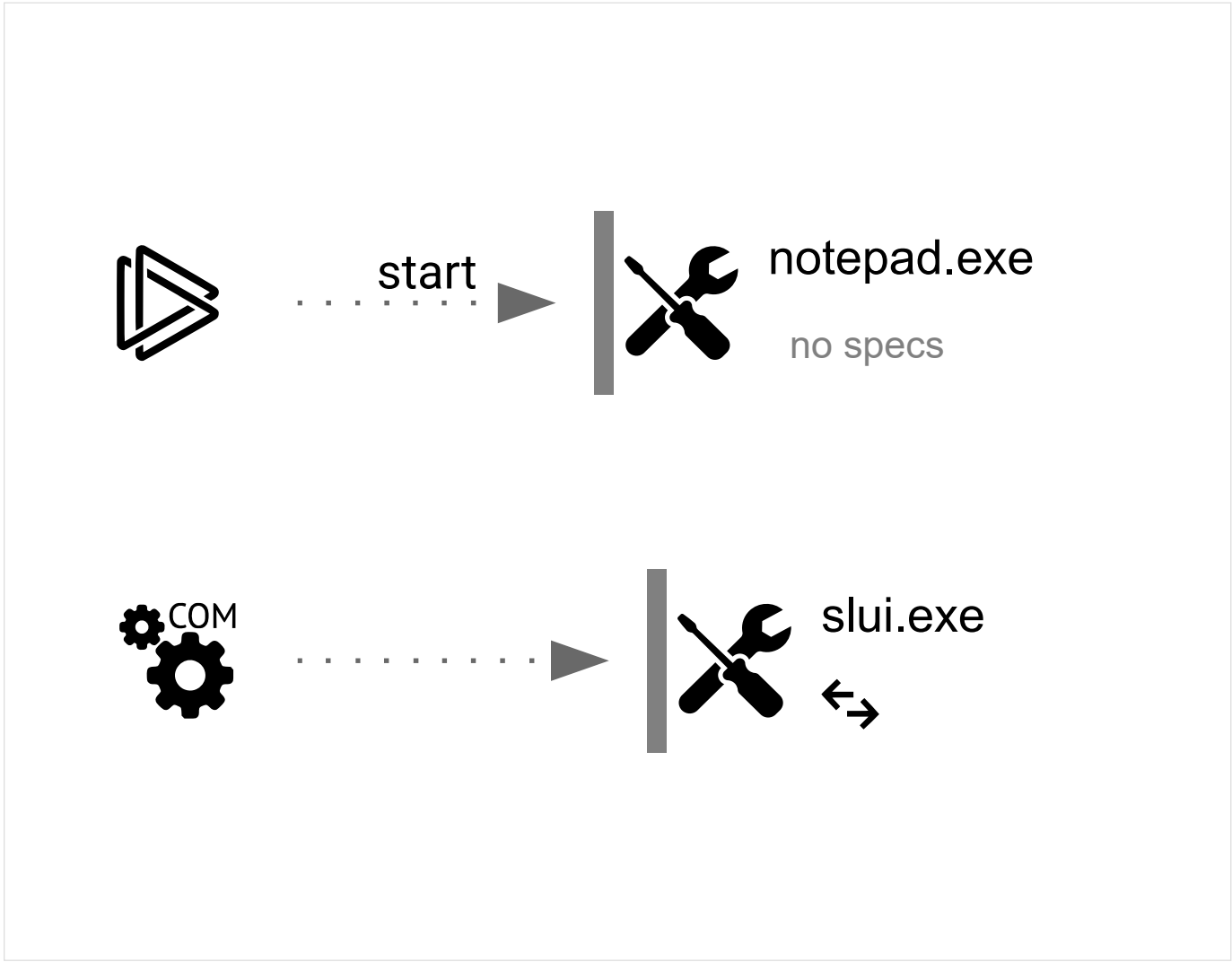
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
137	2	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
4552	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)

4948	"C:\WINDOWS\system32\NOTEPAD.EXE" C:\Users\admin\AppData\Local\Temp\nicoelsoto.pdf.txt	C:\Windows\System32\notepad.exe	–	explorer.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Notepad
Version:	10.0.19041.1 (WinBuild.160101.0800)		

Registry activity

Total events	Read events	Write events	Delete events
3 772	3 772	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
12	28	20	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1580	svchost.exe	GET	200	172.66.2.5:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
6180	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.1.crl	unknown	–	–	whitelisted
6180	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
6180	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.1.crl	unknown	–	–	whitelisted
2940	svchost.exe	GET	200	72.246.169.163:80	http://x1.c.lencr.org/	unknown	–	–	whitelisted
1268	svchost.exe	GET	200	2.16.168.114:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
6180	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
1268	svchost.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
6180	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
6180	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	–	–	whitelisted
6180	SIHClient.exe	GET	200	23.53.41.90:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–	whitelisted
6180	SIHClient.exe	GET	200	2.23.181.156:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation

4	System	192.168.100.255:137	—	—	—	whitelisted
5944	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3572	RUXIMICS.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
1580	svchost.exe	40.126.31.130:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1580	svchost.exe	172.66.2.5:80	ocsp.digicert.com	—	US	whitelisted
1268	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1268	svchost.exe	2.16.168.114:80	crl.microsoft.com	Akamai International B.V.	RU	whitelisted
1268	svchost.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
5944	MoUsoCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6180	SIHClient.exe	74.179.77.204:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6180	SIHClient.exe	2.23.181.156:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6180	SIHClient.exe	23.53.41.90:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
6180	SIHClient.exe	40.69.42.241:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5944	MoUsoCoreWorker.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2336	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
4120	slui.exe	4.154.209.85:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2940	svchost.exe	72.246.169.163:80	x1.c.lencr.org	AKAMAI-AS	DE	whitelisted
4552	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	40.127.240.158 20.73.194.208 4.231.128.59 51.124.78.146	whitelisted
google.com	142.250.181.238	whitelisted
login.live.com	40.126.31.130 40.126.31.131 40.126.31.129 20.190.159.128 20.190.159.4 40.126.31.69 20.190.159.71 20.190.159.73	whitelisted
ocsp.digicert.com	172.66.2.5 162.159.142.9	whitelisted
crl.microsoft.com	2.16.168.114 2.16.168.124 23.53.41.90 23.53.40.178	whitelisted
www.microsoft.com	95.101.149.131 2.23.181.156	whitelisted
slscr.update.microsoft.com	74.179.77.204	whitelisted
fe3cr.delivery.mp.microsoft.com	40.69.42.241	whitelisted
client.wns.windows.com	172.211.123.249	whitelisted
self.events.data.microsoft.com	20.189.173.8	whitelisted
activation-v2.sls.microsoft.com	4.154.209.85	whitelisted
x1.c.lencr.org	72.246.169.163	whitelisted
nexusrules.officeapps.live.com	52.111.229.19	whitelisted

Threats

No threats detected

Debug output strings

No debug info