ANY☑RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	ransomware_x1.exe
Full analysis:	https://app.any.run/tasks/04724325-504d-489e-b808-05b646b74b10
Verdict:	No threats detected
Analysis date:	June 14, 2025 at 20:20:00
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows, 11 sections
MD5:	31F53A501776777FB59EAE993ABB8FD0
SHA1:	973A8A764118942ECF1BA389DC632D63B97F149B
SHA256:	FABF6A48A69C9A7F34B363F90E8298152E93D0CDECD88C028C430E2EE37A284E
SSDEEP:	12288:fdu2nnnnnnnD2AtFEdNlgiOKhNmCEtuKeMlNeaeZl4OkXZfgV2akw1vSuhuHQiFl:f4JKcw1tZin0ByQbiTWqmgdWU/PgCRK

Software environment set and analysis options

Launch configuration

Task duration:	240 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	180 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)

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.	**Checks proxy server information**
		• slui.exe (PID: 2280)
		Checks supported languages
		• ransomware_x1.exe (PID: 3752)
		Reads the computer name
		• ransomware_x1.exe (PID: 3752)
		Reads the software policy settings
		• slui.exe (PID: 2280)

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:	2025:06:14 13:19:34+00:00
ImageFileCharacteristics:	Executable, No line numbers, No symbols, Large address aware, No debug
PEType:	PE32+
LinkerVersion:	2.43
CodeSize:	957440
InitializedDataSize:	1185792
UninitializedDataSize:	3584
EntryPoint:	0x13e0
OSVersion:	4
ImageVersion:	-
SubsystemVersion:	5.2
Subsystem:	Windows command line

Video and screenshots
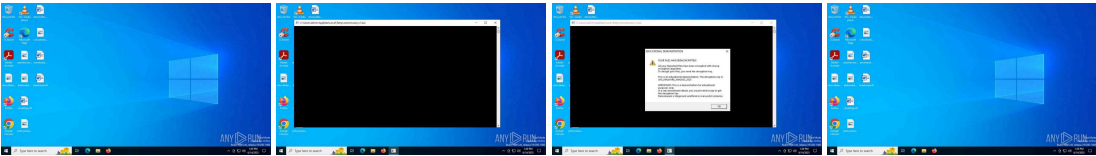
Processes

| Total processes	Monitored processes	Malicious processes	Suspicious processes
141	3	0	0

Behavior graph
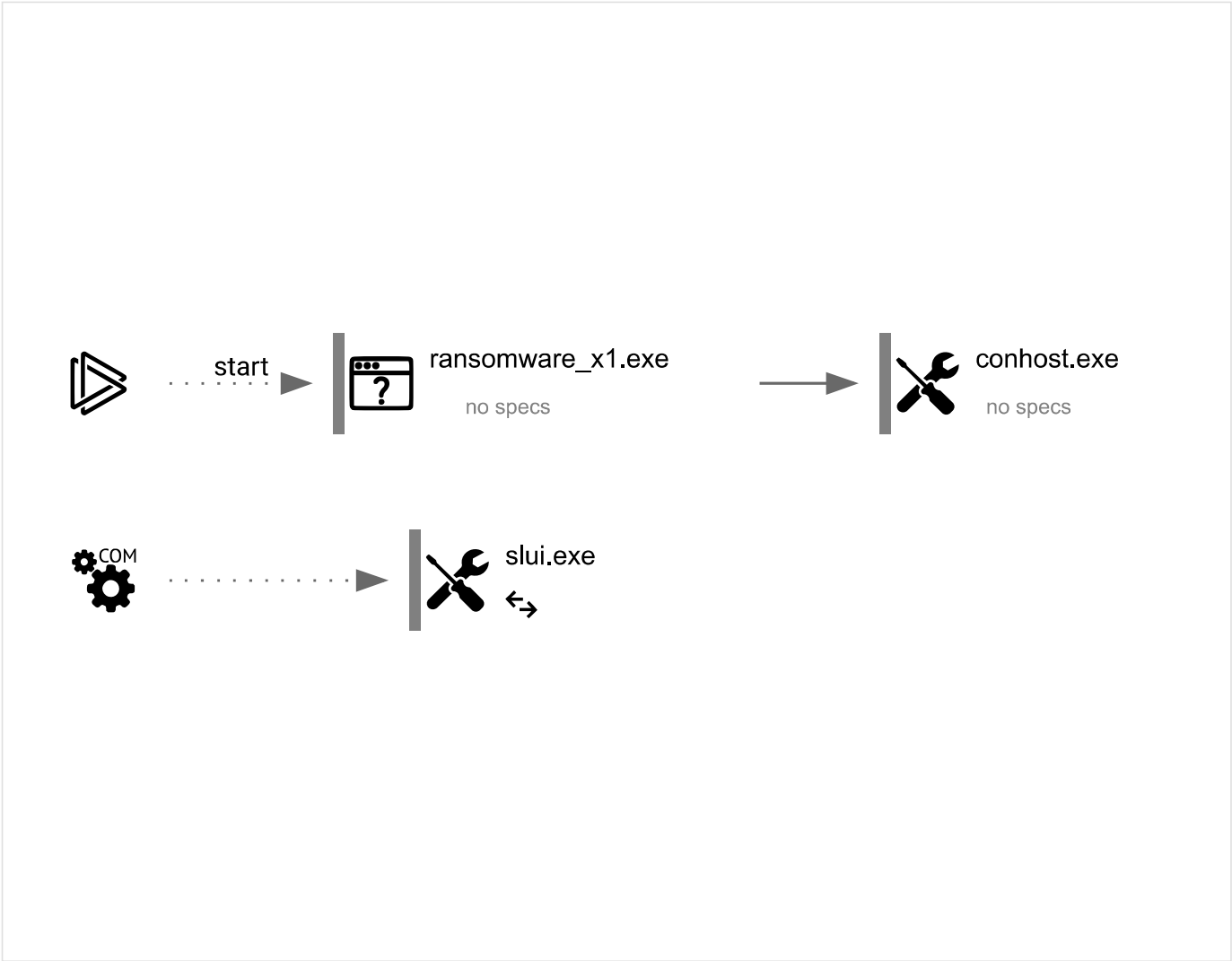
Specs description

Program did not start	Low-level access to the HDD	Process was added to the startup	Debug information is available
Probably Tor was used	Behavior similar to spam	Task has injected processes	Executable file was dropped
Known threat	RAM overrun	Network attacks were detected	Integrity level elevation
Connects to the network	CPU overrun	Process starts the services	System was rebooted
Task contains several apps running	Application downloaded the executable file	Actions similar to stealing personal data	Task has apps ended with an error
File is detected by antivirus software	Inspected object has suspicious PE structure	Behavior similar to exploiting the vulnerability	Task contains an error or was rebooted
The process has the malware config			

Process information

PID	CMD	Path	Indicators	Parent process
2280	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)

PID	CMD	Path		Parent process
3752	"C:\Users\admin\AppData\Local\Temp\ransomware_x1.exe"	C:\Users\admin\AppData\Local\Temp\ransomware_x1.exe	—	explorer.exe

Information				
User:	admin	Integrity Level:	MEDIUM	
Exit code:	0			

3884	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	ransomware_x1.exe

Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Console Window Host	
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)	

Registry activity

Total events	Read events	Write events	Delete events
749	749	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	1	0

Dropped files

PID	Process	Filename	Type
3752	ransomware_x1.exe	C:\RansomwareTest\RANSOM_NOTE.txt	text
		MD5: C63EA992ABFBBFF54B06592E9779E7F5 SHA256: 89082C628AE1C3080FB2F3A429E8A8BA8296AE83C78D56B35F4AACCD41470959	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	26	19	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3768	svchost.exe	GET	200	2.17.190.73:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCG gUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVb RTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3 D	unknown	—	—	whitelisted
1268	svchost.exe	GET	200	23.48.23.143:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut201 1_2011_03_22.crl	unknown	—	—	whitelisted
1268	svchost.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_20 11-10-18.crl	unknown	—	—	whitelisted
2940	svchost.exe	GET	200	23.209.209.135:80	http://x1.c.lencr.org/	unknown	—	—	whitelisted
4768	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20 Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
4768	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20 Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	—	—	whitelisted
5944	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1812	RUXIMICS.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted

4	System	192.168.100.255:138	–	–	–	whitelisted
2336	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
3768	svchost.exe	20.190.160.22:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3768	svchost.exe	2.17.190.73:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
1268	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1268	svchost.exe	23.48.23.143:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
1268	svchost.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
4768	SIHClient.exe	172.202.163.200:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	GB	whitelisted
4768	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
4768	SIHClient.exe	52.165.164.15:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2064	slui.exe	20.83.72.98:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2940	svchost.exe	23.209.209.135:80	x1.c.lencr.org	PT. Telekomunikasi Selular	ID	whitelisted
2280	slui.exe	20.83.72.98:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP		Reputation
settings-win.data.microsoft.com	51.104.136.2 51.124.78.146		whitelisted
google.com	142.250.27.138 142.250.27.100 142.250.27.102 142.250.27.113 142.250.27.101 142.250.27.139		whitelisted
client.wns.windows.com	172.211.123.249		whitelisted
login.live.com	20.190.160.22 20.190.160.4 40.126.32.72 20.190.160.67 20.190.160.65 40.126.32.74 20.190.160.131 40.126.32.138		whitelisted
ocsp.digicert.com	2.17.190.73		whitelisted
crl.microsoft.com	23.48.23.143 23.48.23.156		whitelisted
www.microsoft.com	23.35.229.160		whitelisted
nexusrules.officeapps.live.com	52.111.227.13		whitelisted
slscr.update.microsoft.com	172.202.163.200		whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15		whitelisted
activation-v2.sls.microsoft.com	20.83.72.98		whitelisted
x1.c.lencr.org	23.209.209.135		whitelisted
self.events.data.microsoft.com	52.182.143.215		whitelisted

Threats

No threats detected

Debug output strings

No debug info

ANY RUN
INTERACTIVE MALWARE ANALYSIS