ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	ransomware_c2.exe
Full analysis:	https://app.any.run/tasks/dd0c2176-3c2e-423c-b2cc-a22ea5523fbc
Verdict:	No threats detected
Analysis date:	June 20, 2025 at 09:57:15
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32+ executable (console) x86-64, for MS Windows, 20 sections
MD5:	D45BA3248CBDC0952D2A691F6727A97F
SHA1:	AE46FC37B831F60B3670DDFA8BA77DEC31843872
SHA256:	DC40D6F0CB069D6B89BA4742D4601FBB8186330168FB53111797932DF5488972
SSDEEP:	49152:TfPia9S211gfamovYeg9bL+UX2jj315hBDqqmj+foQ:zL1Kw15hBDqqmj+foQ

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

No malicious indicators.

SUSPICIOUS

No suspicious indicators.

INFO

Checks supported languages
- ransomware_c2.exe (PID: 3832)

Checks proxy server information
- slui.exe (PID: 3724)

Reads the software policy settings
- slui.exe (PID: 3724)

Reads the computer name
- ransomware_c2.exe (PID: 3832)

Malware configuration

No Malware configuration.

Static information

TRiD

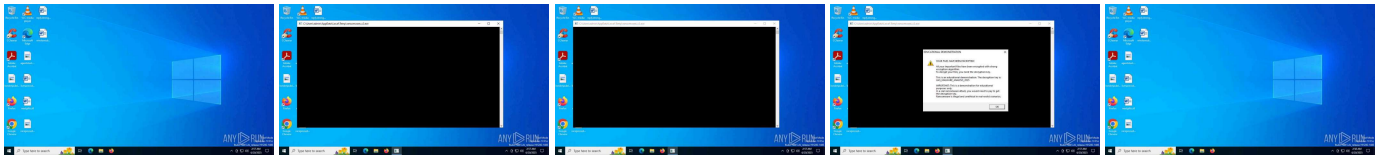
.exe | Win64 Executable (generic) (87.3)
.exe | Generic Win/DOS Executable (6.3)
.exe | DOS Executable Generic (6.3)

EXIF

EXE

MachineType:	AMD AMD64
TimeStamp:	2025:06:18 14:59:58+00:00
ImageFileCharacteristics:	Executable, No line numbers, Large address aware
PEType:	PE32+
LinkerVersion:	2.43
CodeSize:	979456
InitializedDataSize:	1217024
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
139	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
3724	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)

3832	"C:\Users\admin\AppData\Local\Temp\ransomware_c2.exe"	C:\Users\admin\AppData\Local\Temp\ransomware_c2.exe	–	explorer.exe

Information

User: admin Integrity Level: MEDIUM
Exit code: 0

6584 \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1 C:\Windows\System32\conhost.exe – ransomware_c2.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
647	647	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
3832	ransomware_c2.exe	C:\RansomwareTest\RANSOM_NOTE.txt MD5: C63EA992ABFBBFF54B06592E9779E7F5 SHA256: 89082C628AE1C3080FB2F3A429E8A8BA8296AE83C78D56B35F4AACCD41470959	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	24	18	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1268	svchost.exe	GET	200	23.53.40.176:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
1268	svchost.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
6936	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
6936	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted
2940	svchost.exe	GET	200	2.23.197.184:80	http://x1.c.lencr.org/	unknown	–	–	whitelisted
4168	svchost.exe	GET	200	2.17.190.73:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	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
2324	RUXIMICS.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

4	System	192.168.100.255:138	–	–	–	whitelisted
1268	svchost.exe	23.53.40.176:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
1268	svchost.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6936	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6936	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6936	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4168	svchost.exe	20.190.159.129:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4168	svchost.exe	2.17.190.73:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
2336	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
4120	slui.exe	40.91.76.224:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2940	svchost.exe	2.23.197.184:80	x1.c.lencr.org	CW Vodafone Group PLC	GB	whitelisted
3724	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	51.124.78.146	whitelisted
google.com	216.58.206.78	whitelisted
crl.microsoft.com	23.53.40.176 23.53.40.178	whitelisted
www.microsoft.com	23.35.229.160	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted
login.live.com	20.190.159.129 40.126.31.131 20.190.159.131 20.190.159.75 20.190.159.73 40.126.31.73 20.190.159.0 40.126.31.0	whitelisted
ocsp.digicert.com	2.17.190.73	whitelisted
client.wns.windows.com	172.211.123.249	whitelisted
activation-v2.sls.microsoft.com	40.91.76.224 20.83.72.98	whitelisted
x1.c.lencr.org	2.23.197.184	whitelisted
self.events.data.microsoft.com	51.116.246.105	whitelisted

Threats

No threats detected

Debug output strings

No debug info