ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name: Malware Sample.zip

Full analysis: https://app.any.run/tasks/e4e8b7a4-ce7a-4eb5-974a-87fe165f4f18

Verdict: Malicious activity

Threats:

Agent Tesla

Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.

Agent Tesla

Agent Tesla ist eine Spyware, die Informationen über die Aktionen ihrer Opfer sammelt, indem sie Tastatureingaben und Benutzerinteraktionen aufzeichnet. Sie wird auf der speziellen Website, auf der diese Malware verkauft wird, fälschlicherweise als legitime Software vermarktet.

Stealer

Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Analysis date: November 19, 2025 at 13:33:01

OS: Windows 10 Professional (build: 19044, 64 bit)

Tags: arch-exec | auto | agenttesla | stealer | ultravnc | rmm-tool | telegram | exfiltration | ims-api | generic

Indicators:

MIME: application/zip

File info: Zip archive data, at least v5.1 to extract, compression method=AES Encrypted

MD5: 2A97B23E53F0F7A1FCC61708FCCCB60E

SHA1: F090707EB7495A2028F979D5380499ADC37CE4D9

SHA256: 5C174B93F5159C1E9AB27FC8D24EA5DD7D40A0A16071DDB944CE04E0DE482F4D

SSDEEP: 24576:rx2plG9QS9OyVH3t+AhedkXwpzRma41AAl5eh0ROmxKDEnF7Rkxeey3Jnrzmuq:rx2plG9QS9OyVH3t+PdAwpzRdwAAl5ed

Software environment set and analysis options

Launch configuration

Task duration:	180 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	120 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)

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

- 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)
- 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)
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

Behavior activities

MALICIOUS

AGENTTESLA has been found (auto)
- WinRAR.exe (PID: 7328)
- WinRAR.exe (PID: 7768)

Steals credentials from Web Browsers
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

AGENTTESLA has been detected (YARA)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Actions looks like stealing of personal data
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

SUSPICIOUS

Application launched itself
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 7176)

Possible usage of Discord/Telegram API has been detected (YARA)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

The process connected to a server suspected of theft
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Process communicates with Telegram (possibly using it as an attacker's C2 server)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

INFO

Executable content was dropped or overwritten
- WinRAR.exe (PID: 7768)

Manual execution by a user
- WinRAR.exe (PID: 7768)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 7176)

Checks supported languages
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 7176)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Reads the computer name
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 7176)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Reads the machine GUID from the registry
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 7176)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

ULTRAVNC has been detected
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Disables trace logs
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Reads the software policy settings
- slui.exe (PID: 2716)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Checks proxy server information
- slui.exe (PID: 2716)
- c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe (PID: 5948)

Malware configuration

ims-api

(PID) Process	(5948) c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe
Telegram-Tokens (1)	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig
Telegram-Info-Links	
8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig	
Get info about bot	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getMe
Get incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getUpdates
Get webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getWebhookInfo
Delete webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook
Drop incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook?drop_pending_updates=true
Telegram-Tokens (1)	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig

Telegram-Info-Links	
8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig	
Get info about bot	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getMe
Get incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getUpdates
Get webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getWebhookInfo
Delete webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook
Drop incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook?drop_pending_updates=true
Telegram-Requests	
Token	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig
End-Point	sendDocument
Args	
Telegram-Responses	
ok	true
result	
message_id	1768
from	
id	8354849493
is_bot	true
first_name	Sesko
username	Seskou_bot
chat	
id	7594376976
first_name	Lookoloko
last_name	Chester
type	private
date	1763534054
document	
file_name	admin-DESKTOP-JGLLJLD 2025-11-19 06-34-13.html
mime_type	application/octet-stream
file_id	BQACAgQAAxkDAAIG6GkdZOZQPTVaRAN9A4VG8ORr7BylAAKGGwACosPoUGDv4pgzSLpYNgQ
file_unique_id	AgADhhsAAqLD6FA
file_size	417
caption	New PW Recovered! Time: 11/19/2025 06:34:12 User Name: admin/DESKTOP-JGLLJLD OSFullName: Microsoft Windows 10 Pro CPU: AMD Ryzen 5 3500 6-Core Processor RAM: 6138.36 MB

Static information

TRiD

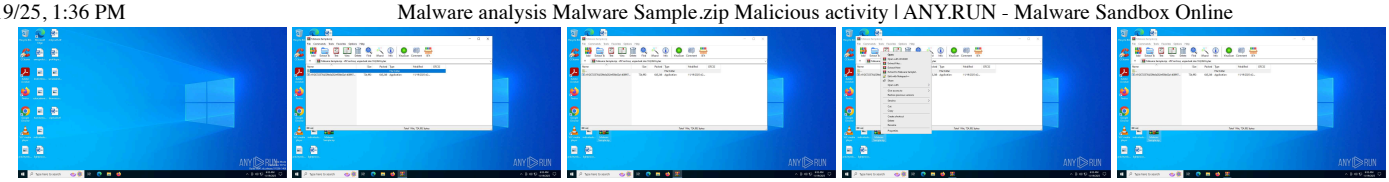
.zip | ZIP compressed archive (100)

EXIF

ZIP

ZipRequiredVersion:	51
ZipBitFlag:	0x0003
ZipCompression:	Unknown (99)
ZipModifyDate:	2025:11:19 04:20:52
ZipCRC:	0x05585b41
ZipCompressedSize:	643246
ZipUncompressedSize:	724992
ZipFileName:	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe

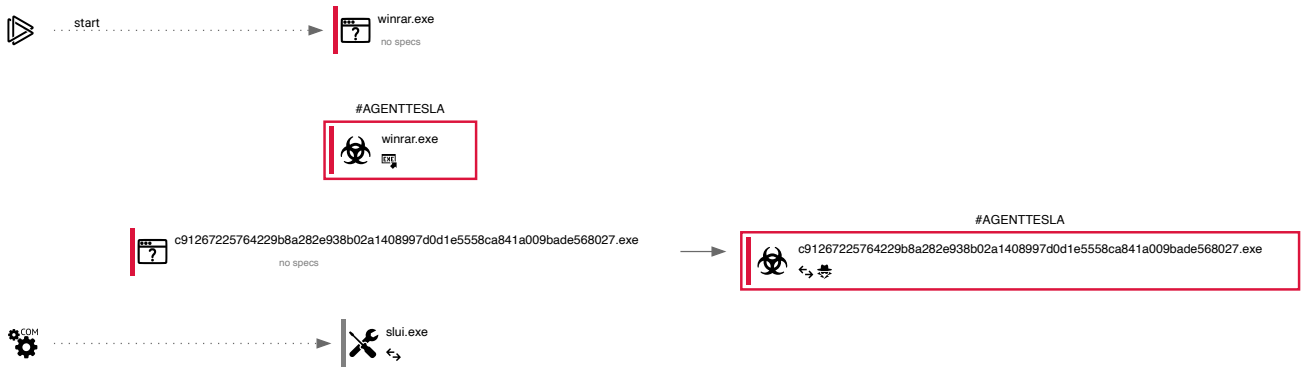
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
153	5	4	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
2716	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)

5948	"C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe"	C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:		Version:	0.0.0.0

Malware configuration ims-api

ims-api

(PID) Process	(5948) c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe
Telegram-Tokens (1)	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig
Telegram-Info-Links	
8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig	
Get info about bot	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getMe
Get incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getUpdates
Get webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getWebhookInfo
Delete webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook
Drop incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook?drop_pending_updates=true

(PID) Process	(5948) c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe
Telegram-Tokens (1)	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig
Telegram-Info-Links	
8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig	
Get info about bot	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getMe
Get incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getUpdates
Get webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/getWebhookInfo
Delete webhook	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook
Drop incoming updates	https://api.telegram.org/bot8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig/deleteWebhook?drop_pending_updates=true
Telegram-Requests	
Token	8354849493:AAF-o67GHd1slu0e-6aslvzWO3nrSq8l0ig
End-Point	sendDocument
Args	
Telegram-Responses	
ok	true
result	
message_id	1768
from	
id	8354849493
is_bot	true
first_name	Sesko
username	Seskou_bot
chat	
id	7594376976
first_name	Lookoloko
last_name	Chester
type	private
date	1763534054
document	
file_name	admin-DESKTOP-JGLLJLD 2025-11-19 06-34-13.html
mime_type	application/octet-stream
file_id	BQACAgQAAxkDAAIG6GkdZOZQPTVaRAN9A4VG8ORr7ByIAAKGGwACosPoUGDv4pgzSLpYNgQ

file_unique_id	AgADhhsAAqLD6FA
file_size	417
caption	New PW Recovered! Time: 11/19/2025 06:34:12 User Name: admin/DESKTOP-JGLLJLD OSFullName: Microsoft Windows 10 Pro CPU: AMD Ryzen 5 3500 6-Core Processor RAM: 6138.36 MB

7176	"C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe"	C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	–	explorer.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:		Exit code:	0
Version:	0.0.0.0		

7328	"C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\admin\Desktop\Malware Sample.zip"	C:\Program Files\WinRAR\WinRAR.exe	–	explorer.exe

Information

User:	admin	Company:	Alexander Roshal
Integrity Level:	MEDIUM	Description:	WinRAR archiver
Version:	5.91.0		

7768	"C:\Program Files\WinRAR\WinRAR.exe" x -iext -ow -ver -- "C:\Users\admin\Desktop\Malware Sample.zip" C:\Users\admin\Desktop\	C:\Program Files\WinRAR\WinRAR.exe		explorer.exe

Information

User:	admin	Company:	Alexander Roshal
Integrity Level:	MEDIUM	Description:	WinRAR archiver
Exit code:	0	Version:	5.91.0

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
1	0	0	0

Dropped files

PID	Process	Filename	Type
7768	WinRAR.exe	C:\Users\admin\Desktop\c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe MD5: 5C22381FF243C8B3FC6984842168F2C7 SHA256: C91267225764229B8A282E938B02A1408997D0D1E5558CA841A009BADE568027	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
10	45	23	7

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
8108	SIHClient.exe	GET	200	95.101.78.42:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–	whitelisted
2900	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted

8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
8108	SIHClient.exe	GET	200	2.19.217.218:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	unknown	—	—	whitelisted
7088	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
6456	svchost.exe	GET	200	104.77.160.85:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
6456	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
5596	MoUsoCoreWorker.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3448	RUXIMICS.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7088	SearchApp.exe	95.100.146.26:443	www.bing.com	Akamai International B.V.	CZ	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
2900	svchost.exe	40.126.32.74:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2900	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
6456	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6456	svchost.exe	104.77.160.85:80	crl.microsoft.com	Akamai International B.V.	GB	whitelisted
3440	svchost.exe	172.211.123.250:443	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
6456	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
8108	SIHClient.exe	20.165.94.63:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
8108	SIHClient.exe	2.19.217.218:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
8108	SIHClient.exe	95.101.78.42:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
8108	SIHClient.exe	20.3.187.198:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2784	slui.exe	4.154.185.43:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7088	SearchApp.exe	2.16.204.158:443	www.bing.com	Akamai International B.V.	DE	whitelisted
7088	SearchApp.exe	2.16.204.160:443	www.bing.com	Akamai International B.V.	DE	whitelisted
7088	SearchApp.exe	204.79.197.222:443	fp.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7088	SearchApp.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	149.154.167.220:443	api.telegram.org	Telegram Messenger Inc	GB	whitelisted
2716	slui.exe	4.154.185.43:443	activation-v2.sls.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

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 40.127.240.158 20.73.194.208	whitelisted
google.com	142.250.185.142	whitelisted
www.bing.com	95.100.146.26 95.100.146.34	whitelisted

	95.100.146.32 95.100.146.8 95.100.146.25 95.100.146.27 95.100.146.24 95.100.146.16 95.100.146.40 2.16.204.160 2.16.204.134 2.16.204.158 2.16.204.155 2.16.204.135 2.16.204.141 2.16.204.161 2.16.204.148 2.16.204.138	
login.live.com	40.126.32.74 20.190.160.65 20.190.160.132 20.190.160.128 20.190.160.130 40.126.32.136 40.126.32.72 20.190.160.5	whitelisted
ocsp.digicert.com	184.30.131.245	whitelisted
crl.microsoft.com	104.77.160.85 104.77.160.74 95.101.78.42 95.101.78.32	whitelisted
client.wns.windows.com	172.211.123.250 172.211.123.248	whitelisted
slscr.update.microsoft.com	20.165.94.63	whitelisted
www.microsoft.com	2.19.217.218	whitelisted
fe3cr.delivery.mp.microsoft.com	20.3.187.198	whitelisted
activation-v2.sls.microsoft.com	4.154.185.43	whitelisted
th.bing.com	2.16.204.158 2.16.204.134 2.16.204.148 2.16.204.146 2.16.204.160 2.16.204.149 2.16.204.135	whitelisted
fp.msedge.net	204.79.197.222	whitelisted
api.telegram.org	149.154.167.220	whitelisted
nexusrules.officeapps.live.com	52.111.229.43	whitelisted

Threats

PID	Process	Class	Message
–	–	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
2276	svchost.exe	Misc activity	ET HUNTING Telegram API Domain in DNS Lookup
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Misc activity	ET HUNTING Observed Telegram API Domain (api .telegram .org in TLS SNI)
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Misc activity	ET HUNTING Telegram API Certificate Observed
5948	c91267225764229b8a282e938b02a1408997d0d1e5558ca841a009bade568027.exe	Successful Credential Theft Detected	STEALER [ANY.RUN] Attempt to exfiltrate via Telegram
–	–	Misc activity	SUSPICIOUS [ANY.RUN] Sent Host Name in HTTP POST Body
–	–	Malware Command and Control Activity Detected	STEALER [ANY.RUN] AgentTesla Telegram Exfiltration

Debug output strings

No debug info