ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL: https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_apwtYT6OYs
Full analysis: https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248
Verdict: Malicious activity
Threats: Remcos

Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month.

Analysis date: June 29, 2023 at 18:52:04
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: rat remcos keylogger
Indicators:
MD5: F227B42BC5D29AC82A82C40B6325B9E3
SHA1: E5AA130B362D68AD2010540C0DE6BE3372DA3375
SHA256: B24023DF44B0A1074B5DBB86AE6DA16FA4C10918C5C21E0100C4812CAE056C49
SSDEEP: 3:N8SP3u2NAaBrC20ZrVvhG0NZT2n:2Sm2BB+2oxvcSin

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)

Hotfixes

- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Maintenance Service (83.0.0.7621)
- Mozilla Maintenance Service (83.0.0.7621)
- Notepad++ (32-bit x86) (7.9.1)
- Notepad++ (32-bit x86) (7.9.1)
- Opera 12.15 (12.15.1748)
- Opera 12.15 (12.15.1748)
- Skype version 8.29 (8.29)
- Skype version 8.29 (8.29)
- VLC media player (3.0.11)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- WinRAR 5.91 (32-bit) (5.91.0)

Behavior activities

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Writes files like Keylogger logs
- csc.exe (PID: 3824)

Checks Windows Trust Settings
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Executable content was dropped or overwritten
- procexp.exe (PID: 3476)

INFO

The process uses the downloaded file
- chrome.exe (PID: 2064)
- chrome.exe (PID: 2356)
- chrome.exe (PID: 1140)
- WinRAR.exe (PID: 1944)
- chrome.exe (PID: 3868)
- WinRAR.exe (PID: 3092)
- chrome.exe (PID: 2880)

Application launched itself
- chrome.exe (PID: 3140)

Manual execution by a user
- WinRAR.exe (PID: 1944)
- Autoruns.exe (PID: 4056)
- WinRAR.exe (PID: 3092)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

The process checks LSA protection
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- procexp.exe (PID: 3476)

Checks supported languages
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- csc.exe (PID: 2076)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- csc.exe (PID: 2240)
- csc.exe (PID: 148)
- procexp.exe (PID: 3476)

Reads product name
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)
- procexp.exe (PID: 3476)

Reads the machine GUID from the registry
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- procexp.exe (PID: 3476)

Reads the computer name
- Autoruns.exe (PID: 4056)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- csc.exe (PID: 3824)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)
- procexp.exe (PID: 3476)

Reads Environment values
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)
- procexp.exe (PID: 3476)

Create files in a temporary directory
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads Microsoft Office registry keys
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Creates files or folders in the user directory
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

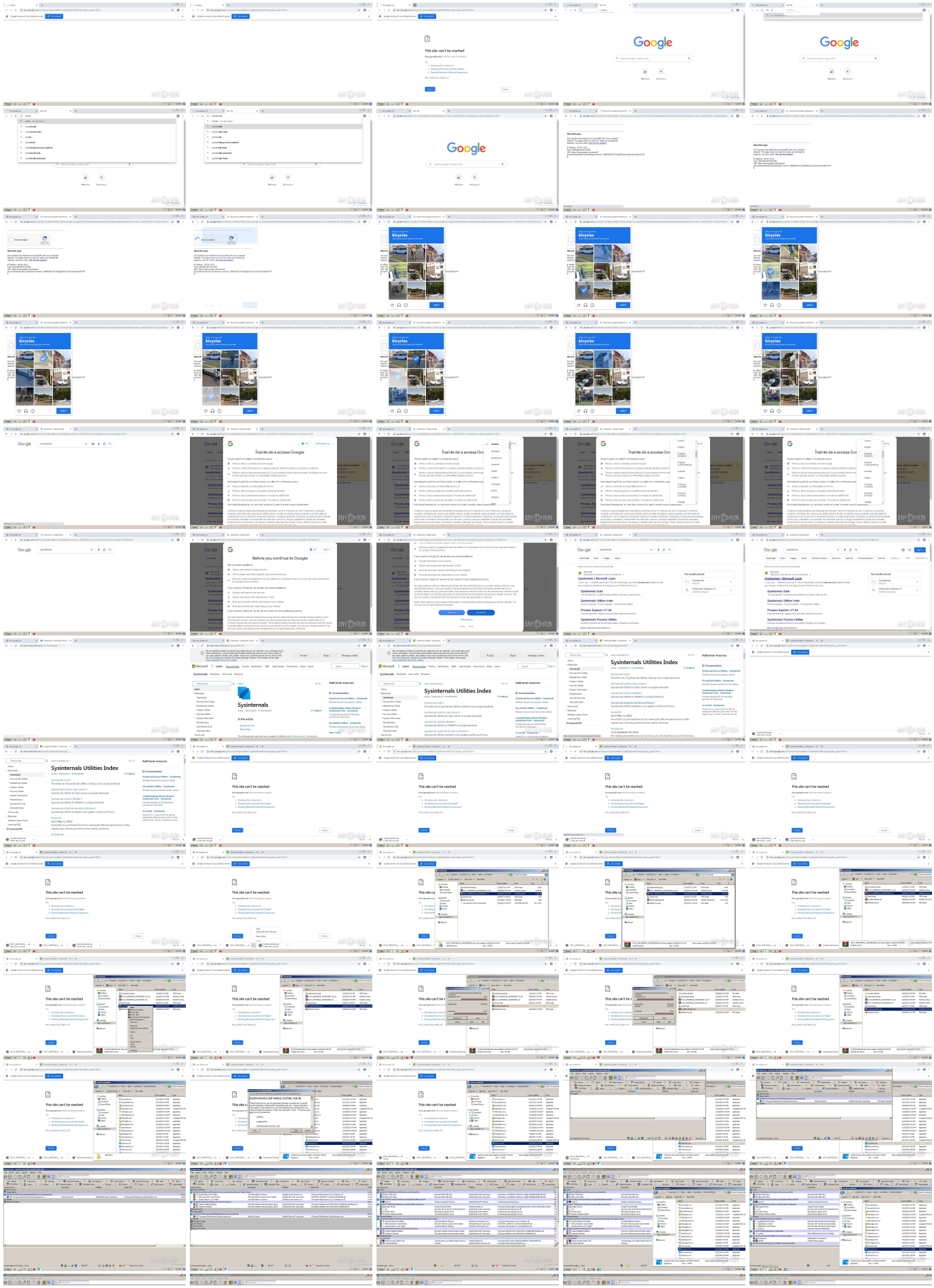
Checks proxy server information

• csc.exe (PID: 3824)

Creates files in the program directory

• csc.exe (PID: 3824)

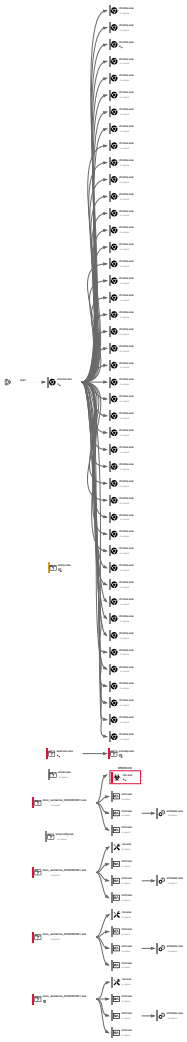
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
138	74	7	1

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
3140	"C:\Program Files\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --disable-background-networking "https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_apwtYT6OYs"	C:\Program Files\Google\Chrome\Application\chrome.exe		explorer.exe

Information

User: admin **Company:** Google LLC

Integrity Level: MEDIUM **Description:** WinRAR archiver
Exit code: 0 **Version:** 5.91.0

3536 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=1800 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

4056 "C:\Users\admin\Downloads\SysinternalsSuite\Autoruns.exe" C:\Users\admin\Downloads\SysinternalsSuite\Autoruns.exe ↪ explorer.exe

Information
User: admin **Company:** Sysinternals - www.sysinternals.com
Integrity Level: MEDIUM **Description:** Autostart program viewer
Version: 14.10

3508 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --disable-gpu-compositing --lang=en-US --extension-process --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=35 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2816 /prefetch:1 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

2676 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=1252 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

3868 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2588 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: MEDIUM **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

3656 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=3476 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

3824 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=3548 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe — chrome.exe

Information
User: admin **Company:** Google LLC
Integrity Level: LOW **Description:** Google Chrome
Exit code: 0 **Version:** 86.0.4240.198

3092 "C:\Program Files\WinRAR\WinRAR.exe" x -iext -ow -ver -- "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001.t C:\Program Files\WinRAR\WinRAR.exe — explorer.exe

ar"
C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\

Information

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

2028	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=1000 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	Company:	Google LLC
Integrity Level:	LOW	Description:	Google Chrome
Exit code:	0	Version:	86.0.4240.198

4040	"C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe"	C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe	—	explorer.exe

Information

User:	admin	Company:	Adobe Systems Incorporated
Integrity Level:	MEDIUM	Description:	Adobe Acrobat
Exit code:	4294967295	Version:	23.1.20174.0

3824	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe	☣ ↪	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Visual C# Command Line Compiler
Version:	4.0.30319.34209 built by: FX452RTMGDR		

2032	"cmd" /c mkdir "C:\Users\admin\AppData\Roaming\AppData"	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3604	"cmd" /c schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3428	"cmd" /c copy "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" "C:\Users\admin\AppData\Roaming\AppData\AppData.exe"	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1796	schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f	C:\Windows\System32\schtasks.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

1156	"C:\Program Files\Windows Media Player\wmpnscfg.exe"	C:\Program Files\Windows Media Player\wmpnscfg.exe	—	explorer.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Media Player Network Sharing Service Configuration Application
Exit code:	0	Version:	12.0.7600.16385 (win7_rtm.090713-1255)

4004	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=576 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	Company:	Google LLC
Integrity Level:	LOW	Description:	Google Chrome
Exit code:	0	Version:	86.0.4240.198

3912	"C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe"	C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe	—	explorer.exe

Information

User:	admin	Company:	Adobe Systems Incorporated
Integrity Level:	MEDIUM	Description:	Adobe Acrobat
Exit code:	4294967295	Version:	23.1.20174.0

2076	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Visual C# Command Line Compiler
Exit code:	2	Version:	4.0.30319.34209 built by: FX452RTMGDR

2900	"cmd" /c mkdir "C:\Users\admin\AppData\Roaming\AppData"	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	1	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3200	"cmd" /c schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

4020	"cmd" /c copy "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" "C:\Users\admin\AppData\Roaming\AppData\AppData.exe"	C:\Windows\System32\cmd.exe	—	DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2580	schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f	C:\Windows\System32\schtasks.exe	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

3608	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=2064 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	Company:	Google LLC
Integrity Level:	LOW	Description:	Google Chrome
Exit code:	0	Version:	86.0.4240.198

3484	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --disable-gpu-compositing --lang=en-US --extension-process --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=43 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1844 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	Company:	Google LLC
Integrity Level:	LOW	Description:	Google Chrome
Exit code:	0	Version:	86.0.4240.198

2880 "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1124,9283558914914597617,309495182446768953,131072 --enable-features=PasswordImport --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1760 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrome.exe – chrome.exe

Information

User:	admin	Company:	Google LLC
Integrity Level:	MEDIUM	Description:	Google Chrome
Exit code:	0	Version:	86.0.4240.198

2432 "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe – explorer.exe

Information

User:	admin	Company:	Adobe Systems Incorporated
Integrity Level:	MEDIUM	Description:	Adobe Acrobat
Exit code:	4294967295	Version:	23.1.20174.0

2240 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Visual C# Command Line Compiler
Exit code:	2	Version:	4.0.30319.34209 built by: FX452RTMGDR

1464 "cmd" /c mkdir "C:\Users\admin\AppData\Roaming\AppData" C:\Windows\System32\cmd.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	1	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2628 "cmd" /c schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f C:\Windows\System32\cmd.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2616 "cmd" /c copy "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" "C:\Users\admin\AppData\Roaming\AppData\AppData.exe" C:\Windows\System32\cmd.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Command Processor
Exit code:	0	Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2572 schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f C:\Windows\System32\schtasks.exe – cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

312 "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe explorer.exe

Information

User:	admin	Company:	Adobe Systems Incorporated
Integrity Level:	HIGH	Description:	Adobe Acrobat
Exit code:	4294967295	Version:	23.1.20174.0

148 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	HIGH	Description:	Visual C# Command Line Compiler
Exit code:	2	Version:	4.0.30319.34209 built by: FX452RTMGDR

3556 "cmd" /c mkdir "C:\Users\admin\AppData\Roaming\AppData" C:\Windows\System32\cmd.exe – DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Command Processor
Exit code:	1	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

2960 "cmd" /c schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f — C:\Windows\System32\cmd.exe — DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1300 "cmd" /c copy "C:\Users\admin\Downloads\DOCX_SENTENCIA_20230003001\DOCX_SENTENCIA_20230003001.exe" "C:\Users\admin\AppData\Roaming\AppData\AppData.exe" — C:\Windows\System32\cmd.exe — DOCX_SENTENCIA_20230003001.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1956 schtasks /create /sc minute /mo 10 /tn "Nano" /tr "'C:\Users\admin\AppData\Roaming\AppData\AppData.exe'" /f — C:\Windows\System32\schtasks.exe — cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Manages scheduled tasks
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3476 C:\Users\admin\Downloads\SysinternalsSuite\procexp.exe — C:\Users\admin\Downloads\SysinternalsSuite\procexp.exe — Autoruns.exe

Information

User:	admin	**Company:**	Sysinternals - www.sysinternals.com
Integrity Level:	MEDIUM	**Description:**	Sysinternals Process Explorer
Version:	17.04		

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
36	82	36	4

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	—	—	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	6.12 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	7.64 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	8.00 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	10.1 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	20.7 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/npdzcmzjb74ekinqef76xb4uai_2970/jflookgnkcckhobaglndicnbbgbonegd_2970_all_ggypvlfi3qjqa6xkwprvpwrzkq.crx3	US	binary	5.94 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zlfhpj3roq46nymxtbz4zq_2022.10.19.1145/ggkkehgbnfjpeggfpleeakpidbkibbmn_2022.10.19.1145_all_ac7cecrzrmfngskhgmtk6zmhfjoa.crx3	US	binary	5.94 Kb	whitelisted

852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zlfhpj3roq46nymxtbz4zq_2022.10.19.1145/ggkkehgbnfjpeggfpleeakpidbkibbmn_2022.10.19.1145_all_ac7cecrzrmfngskhgmtk6zmhfjoa.crx3	US	binary	10.2 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/j2hxfei2occ5siitujtlwgp6xi_3/ojhpjlocmbogdgmfpkhlaaeamibhnphh_3_all_gplutbkdljxxbjolk3siq7kive.crx3	US	binary	10.2 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/j2hxfei2occ5siitujtlwgp6xi_3/ojhpjlocmbogdgmfpkhlaaeamibhnphh_3_all_gplutbkdljxxbjolk3siq7kive.crx3	US	binary	143 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/j2hxfei2occ5siitujtlwgp6xi_3/ojhpjlocmbogdgmfpkhlaaeamibhnphh_3_all_gplutbkdljxxbjolk3siq7kive.crx3	US	binary	362 Kb	whitelisted
852	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/j2hxfei2occ5siitujtlwgp6xi_3/ojhpjlocmbogdgmfpkhlaaeamibhnphh_3_all_gplutbkdljxxbjolk3siq7kive.crx3	US	binary	352 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvMjg0QUFYSnN4MFUtaEQwNDZqVGRkVkFmZw/1.0.6.0_aemomkdncapdnfajjbbcbdebjljbpmpj.crx	US	binary	352 Kb	whitelisted
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvMjg0QUFYSnN4MFUtaEQwNDZqVGRkVkFmZw/1.0.6.0_aemomkdncapdnfajjbbcbdebjljbpmpj.crx	US	crx	9.28 Kb	whitelisted
4056	Autoruns.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?19db4957a89bb5fc	US	compressed	4.70 Kb	whitelisted
4056	Autoruns.exe	GET	200	2.16.241.14:80	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl	unknown	binary	767 b	whitelisted
4056	Autoruns.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Windows%20Verification%20PCA(1).crl	NL	binary	532 b	whitelisted
4056	Autoruns.exe	GET	200	2.16.241.14:80	http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl	unknown	binary	519 b	whitelisted
4056	Autoruns.exe	GET	200	2.16.241.14:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	binary	824 b	whitelisted
4056	Autoruns.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/MicWinProPCA2011_2011-10-19.crl	NL	binary	564 b	whitelisted
4056	Autoruns.exe	GET	200	2.16.241.14:80	http://crl.microsoft.com/pki/crl/products/MicTimStaPCA_2010-07-01.crl	unknown	binary	555 b	whitelisted
4056	Autoruns.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?bf245ae736ae7fbc	US	compressed	62.3 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERyWQYP_A_4/aapLKTSZ439A-0g3nqJr3Q	US	crx	9.28 Kb	whitelisted
4056	Autoruns.exe	GET	200	2.16.241.14:80	http://crl.microsoft.com/pki/crl/products/WinPCA.crl	unknown	binary	530 b	whitelisted
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/hzmeswvvl5uqwcdylzsxu63nma_8083/hfnkpimlhhgieaddgfemjhofmfblmnib_8083_all_n4c6lsdsg5dj4ob6xecmihbhem.crx3	US	crx	25.7 Kb	whitelisted
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERyWQYP_A_4/aapLKTSZ439A-0g3nqJr3Q	US	crx	3.72 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/hzmeswvvl5uqwcdylzsxu63nma_8083/hfnkpimlhhgieaddgfemjhofmfblmnib_8083_all_n4c6lsdsg5dj4ob6xecmihbhem.crx3	US	crx	3.72 Kb	whitelisted
4056	Autoruns.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/certs/Microsoft%20Development%20Root%20Certificate%20Authority%202014.crt	NL	binary	1.51 Kb	whitelisted
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvODJiQUFYYVJaZ0k5di1hUFlXS1prX2xDZw/1.0.0.13_llkgjffcdpffmhiakmfcdcblohccpfmo.crx	US	crx	2.81 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/cxpsjblnoxgjoqggdsbvujtof4_58/khaoiebndkojlmppeemjhbpbandiljpe_58_win_advr4ucepztwtigvw3fduftsvbeq.crx3	US	crx	2.81 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvODJiQUFYYVJaZ0k5di1hUFlXS1prX2xDZw/1.0.0.13_llkgjffcdpffmhiakmfcdcblohccpfmo.crx	US	binary	25.7 Kb	whitelisted
3824	csc.exe	GET	200	178.237.33.50:80	http://geoplugin.net/json.gp	NL	binary	963 b	suspicious
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/n3xmszuzmcp4pxq3qhmant63nm_9.45.0/gcmjkmgdlgnkkcocmoeiminaijmmjnii_9.45.0_all_ecp3yewcq3fuvht5wyi7t7s37y.crx3	US	crx	35.5 Kb	whitelisted
852	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/n3xmszuzmcp4pxq3qhmant63nm_9.45.0/gcmjkmgdlgnkkcocmoeiminaijmmjnii_9.45.0_all_ecp3yewcq3fuvht5wyi7t7s37y.crx3	US	crx	5.46 Kb	whitelisted
852	svchost.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/cxpsjblnoxgjoqggdsbvujtof4_58/khaoiebndkojlmppeemjhbpbandiljpe_58_win_advr4ucepztwtigvw3fduftsvbeq.crx3	US	binary	5.46 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	—	—	whitelisted
2624	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
1076	svchost.exe	224.0.0.252:5355	—	—	—	unknown
3140	chrome.exe	239.255.255.250:1900	—	—	—	whitelisted
3440	chrome.exe	172.217.18.14:443	clients2.google.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.186.77:443	accounts.google.com	GOOGLE	US	suspicious
3440	chrome.exe	216.58.212.142:443	docs.google.com	GOOGLE	US	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
3440	chrome.exe	142.250.185.193:443	clients2.googleusercontent.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.186.35:443	ssl.gstatic.com	GOOGLE	US	whitelisted
3140	chrome.exe	224.0.0.251:5353	—	—	—	unknown
3440	chrome.exe	142.250.185.225:443	lh5.googleusercontent.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.185.227:80	www.gstatic.com	GOOGLE	US	whitelisted
3440	chrome.exe	172.217.18.4:443	www.google.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.181.238:443	encrypted-tbn0.gstatic.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.185.138:443	fonts.googleapis.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.186.67:443	fonts.gstatic.com	GOOGLE	US	whitelisted
3440	chrome.exe	172.217.18.10:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.185.227:443	www.gstatic.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.186.42:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
852	svchost.exe	34.104.35.123:80	edgedl.me.gvt1.com	GOOGLE	US	whitelisted
3440	chrome.exe	13.107.246.45:443	wcpstatic.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	malicious
3440	chrome.exe	142.250.186.46:443	play.google.com	GOOGLE	US	whitelisted
3440	chrome.exe	104.102.48.120:443	learn.microsoft.com	AKAMAI-AS	DE	suspicious
3440	chrome.exe	142.250.185.195:443	update.googleapis.com	GOOGLE	US	whitelisted
3440	chrome.exe	142.250.74.206:443	apis.google.com	GOOGLE	US	whitelisted
3440	chrome.exe	13.107.246.61:443	js.monitor.azure.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
3440	chrome.exe	172.217.16.202:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
3440	chrome.exe	40.79.141.153:443	browser.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	suspicious
3440	chrome.exe	54.171.207.236:443	mscom.demdex.net	AMAZON-02	IE	unknown
4056	Autoruns.exe	2.16.241.14:80	crl.microsoft.com	Akamai International B.V.	DE	suspicious
3440	chrome.exe	152.199.19.160:443	download.sysinternals.com	EDGECAST	US	whitelisted
4056	Autoruns.exe	209.197.3.8:80	ctldl.windowsupdate.com	STACKPATH-CDN	US	whitelisted
4056	Autoruns.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	suspicious
3440	chrome.exe	142.250.184.206:443	docs.google.com	GOOGLE	US	whitelisted
3824	csc.exe	178.237.33.50:80	geoplugin.net	Schuberg Philis B.V.	NL	suspicious
3440	chrome.exe	142.250.185.238:443	clients1.google.com	GOOGLE	US	whitelisted
3824	csc.exe	181.141.7.178:7770	ginebra.con-ip.com	EPM Telecomunicaciones S.A. E.S.P.	CO	suspicious

DNS requests

Domain	IP	Reputation
clients2.google.com	172.217.18.14	whitelisted
accounts.google.com	142.250.186.77	shared

docs.google.com	216.58.212.142 142.250.184.206	shared
clients2.googleusercontent.com	142.250.185.193	whitelisted
ssl.gstatic.com	142.250.186.35	whitelisted
www.gstatic.com	142.250.185.227	whitelisted
www.google.com	172.217.18.4	whitelisted
encrypted-tbn0.gstatic.com	142.250.181.238	whitelisted
lh5.googleusercontent.com	142.250.185.225	whitelisted
fonts.googleapis.com	142.250.185.138	whitelisted
content-autofill.googleapis.com	142.250.186.42 172.217.18.10 172.217.16.202 142.250.186.170 216.58.212.170 172.217.23.106 142.250.185.74 142.250.185.106 142.250.185.138 142.250.185.170 142.250.185.202 142.250.185.234 142.250.186.74 142.250.186.106 142.250.181.234 142.250.184.202	whitelisted
fonts.gstatic.com	142.250.186.67	whitelisted
update.googleapis.com	142.250.185.195	whitelisted
edgedl.me.gvt1.com	34.104.35.123	whitelisted
consent.google.com	142.250.181.238	shared
apis.google.com	142.250.74.206	whitelisted
learn.microsoft.com	104.102.48.120	whitelisted
js.monitor.azure.com	13.107.246.61 13.107.213.61	whitelisted
wcpstatic.microsoft.com	13.107.246.45 13.107.213.45	whitelisted
play.google.com	142.250.186.46	whitelisted
mscom.demdex.net	54.171.207.236 34.246.32.5 54.217.20.142 52.215.85.23 52.209.47.64 52.19.115.14 52.49.138.0 52.211.126.31	whitelisted
microsoftmscompoc.tt.omtrdc.net	66.235.152.107 66.235.152.143 66.235.152.113 66.235.152.152 66.235.152.115 66.235.152.126	whitelisted
target.microsoft.com	66.235.152.115 66.235.152.152 66.235.152.143 66.235.152.126 66.235.152.107 66.235.152.113	whitelisted
safebrowsing.googleapis.com	172.217.16.202	whitelisted
browser.events.data.microsoft.com	40.79.141.153	whitelisted
download.sysinternals.com	152.199.19.160	whitelisted
clients1.google.com	142.250.185.238	whitelisted
doc-0s-3c-docs.googleusercontent.com	142.250.185.225	whitelisted
drive.google.com	142.250.186.46	shared

sb-ssl.google.com	142.250.184.206	whitelisted
ctldl.windowsupdate.com	209.197.3.8	whitelisted
crl.microsoft.com	2.16.241.14 2.16.241.19	whitelisted
www.microsoft.com	95.101.149.131	whitelisted
ginebra.con-ip.com	181.141.7.178	suspicious
geoplugin.net	178.237.33.50	suspicious

Threats

PID	Process	Class	Message
1076	svchost.exe	Potentially Bad Traffic	ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)
3824	csc.exe	Malware Command and Control Activity Detected	ET JA3 Hash - Remcos 3.x TLS Connection
–	–	A Network Trojan was detected	REMOTE [ANY.RUN] REMCOS JA3 Hash

Debug output strings

No debug info

General Info

URL: https://docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgtAG_apwtYT6OYs

Full analysis: https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248

Verdict: Malicious activity

Threats: **Remcos**

Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month.

Analysis date: June 29, 2023, 16:52:04

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: rat remcos keylogger

Indicators:

MD5: F227B42BC5D29AC82A82C40B6325B9E3

SHA1: E5AA130B362D68AD2010540C0DE6BE3372DA3375

SHA256: B24023DF44B0A1074B5DBB86AE6DA16FA4C10918C5C21E0100C4812CAE056C49

SSDEEP: 3:N8SP3u2NAaBrC20ZrVvhG0NZT2n:2Sm2BB+2oxvcSin

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)

Hotfixes