ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	608d4a6897d2fd5a8b996bdb43e54d5f.exe
Full analysis:	https://app.any.run/tasks/df018312-2941-4f82-8d98-776668df9a20
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:	August 17, 2022 at 12:24:23
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	rat remcos trojan floxif keylogger
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	608D4A6897D2FD5A8B996BDB43E54D5F
SHA1:	7CCE8325BD1ACA05B525910D65FEA90EA18D0B3C
SHA256:	36C153AE3A33E8EB9BADB45FC6C89B2C805BD61F52AD2E2003E1C0107BE6D7D8
SSDEEP:	12288:z0kUVo1voInwnWh77v8FLkrsfZiM5NiBjvrEH7/6:Q3e1voMw/FLk+Z5HErEH7/6

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	none	**MITM proxy:**	off	**Privacy:**	Public submission
Fakenet option:	off	**Route via Tor:**	off	**Autoconfirmation of UAC:**	off
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402
- KB2676562
- KB2685811

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2685939
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)	KB2690533
Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972

Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461
Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178

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 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++ 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 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3156016
KB3159398
KB3161102
KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

Drops executable file immediately after starts
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

REMCOS was detected
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Changes AppInit_DLLs value (autorun option)
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Loads dropped or rewritten executable
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

REMCOS detected by memory dumps
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Connects to CnC server
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

FLOXIF was detected
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

SUSPICIOUS

Checks supported languages
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Executable content was dropped or overwritten
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Reads the computer name
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Drops a file with a compile date too recent
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Reads Environment values
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Writes files like Keylogger logs
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

Creates files in the program directory
608d4a6897d2fd5a8b996bdb43e54d5f.exe (PID: 1300)

INFO

No info indicators.

Static information

TRiD

.exe | Win64 Executable (generic) (76.4)
.exe | Win32 Executable (generic) (12.4)
.exe | Generic Win/DOS Executable (5.5)
.exe | DOS Executable Generic (5.5)

EXIF

EXE

Subsystem:	Windows GUI
SubsystemVersion:	5.1
ImageVersion:	0

OSVersion:	5.1
EntryPoint:	0x31ca9
UninitializedDataSize:	0
InitializedDataSize:	134144
CodeSize:	342528
LinkerVersion:	14
PEType:	PE32
TimeStamp:	2022:08:10 00:59:45+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	09-Aug-2022 22:59:45
Detected languages:	English - United States

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000118

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	7
Time date stamp:	09-Aug-2022 22:59:45
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0005384B	0x00053A00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.6167
.rdata	0x00055000	0x000171F2	0x00017200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.86249
.data	0x0006D000	0x00005C24	0x00000E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	2.96099
.tls	0x00073000	0x00000009	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0.0203931
.gfids	0x00074000	0x00000230	0x00000400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	2.38489
.rsrc	0x00075000	0x00004AD0	0x00004C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	3.98324
.reloc	0x0007A000	0x00003940	0x00003A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.68568

Resources

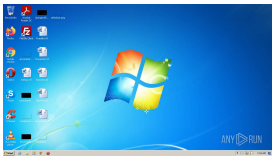
Title	Entropy	Size	Codepage	Language	Type
1	3.38988	1128	Latin 1 / Western European	English - United States	RT_ICON
2	3.25192	2440	Latin 1 / Western European	English - United States	RT_ICON
3	3.13574	4264	Latin 1 / Western European	English - United States	RT_ICON
4	3.3891	9640	Latin 1 / Western European	English - United States	RT_ICON
123	2.62308	62	Latin 1 / Western European	English - United States	RT_GROUP_ICON
SETTINGS	7.8273	1219	Latin 1 / Western European	UNKNOWN	RT_RCDATA

Imports

ADVAPI32.dll
GDI32.dll
KERNEL32.dll
SHELL32.dll

SHLWAPI.dll
USER32.dll
WININET.dll
WINMM.dll
WS2_32.dll
gdiplus.dll
urlmon.dll

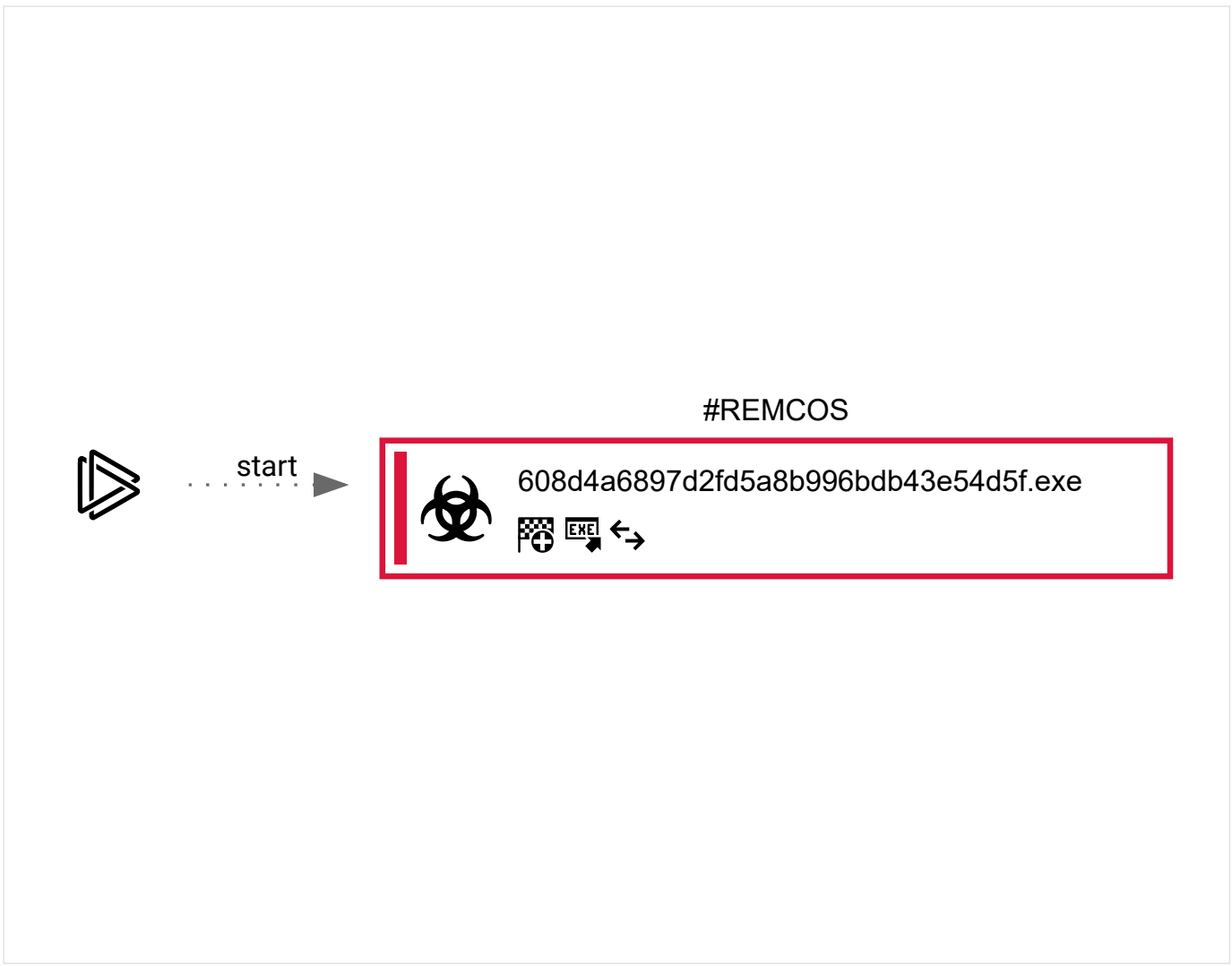
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
37	1	1	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
1300	"C:\Users\admin\AppData\Local\Temp\608d4a6897d2fd5a8b996bdb43e54d5f.exe"	C:\Users\admin\AppData\Local\Temp\608d4a6897d2fd5a8b996bdb43e54d5f.exe		Explorer.EXE

Information

User: admin Integrity Level: MEDIUM

Registry activity

Total events	Read events	Write events	Delete events
612	538	73	1

Modification events

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
Operation: write **Name:** AppInit_DLLs
Value: C:\Users\admin\AppData\Local\Temp\conres.dll

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
Operation: write **Name:** LoadAppInit_DLLs
Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
Operation: write **Name:** RequireSignedAppInit_DLLs
Value: 0

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Remcos-Y8FGJS
Operation: write **Name:** exepath
Value: FC579C6752453F34552CF36CD57AA52B685CFA55C01F1673BF0077FA8B74FDA63F33F5EF2ED06DC8A9E729228818134251A1442A62F6A763871AF0A2D78A03DC5F7167B477D737450E49FC8E535B721A4AF34161EB0A8EDA93902918CEE4EAF7DC3E8818E4C8BC0354277A3587AF3342A5B860D0F863089C2B28D9F1CE36F0B209404D49D572A48A5E1216591B5F

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Remcos-Y8FGJS
Operation: write **Name:** licence
Value: B520B2A2389E533BF3093F8D67DACBD2

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B0100000900000000000000000000000000000000000000040000000000000 0C0E333BBEAB1D301000000000000000000000000000000000100000002000000C0A80164000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionReason

Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 9CAC813C06B2D801

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecision
Value: 0

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadNetworkName
Value: Network 4

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionReason
Value: 1

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 9CAC813C06B2D801

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecision
Value: 0

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDetectedUrl
Value:

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: A44A3D4306B2D801

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: A44A3D4306B2D801

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: delete value **Name:** WpadDetectedUrl
Value:

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 3BE33D4306B2D801

(PID) Process: (1300) 608d4a6897d2fd5a8b996bdb43e54d5f.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 3BE33D4306B2D801

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	2	2	0

Dropped files

PID	Process	Filename	Type
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PO2HN1X2\json[1].json	binary
		MD5: 99C94709040174A54B91AAFBA329BE8D **SHA256:** 3241F6C448D1D5D5AD0AF4D067B46D2FD879B2677C48E3FCD597C1F7F6CFA1E2	
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	C:\Users\admin\AppData\Local\Temp\conres.dll	executable
		MD5: 7574CF2C64F35161AB1292E2F532AABF **SHA256:** DE055A89DE246E629A8694BDE18AF2B1605E4B9B493C7E4AEF669DD67ACF5085	
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	C:\users\admin\appdata\local\temp\conres.dll.000	text
		MD5: 1130C911BF5DB4B8F7CF9B6F4B457623 **SHA256:** EBA08CC8182F379392A97F542B350EA0DBBE5E4009472F35AF20E3D857EAFDF1	

1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	C:\Users\admin\AppData\Roaming\Screenshots\time_20220817_075444.jpg		image
		MD5: 6A90D75317B39327A704C7B714D576A9	**SHA256:** 634284B376E1E263B34488A738E5BEF5A00FFE8F0E16BC77EF77AB1A82714241	
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	C:\ProgramData\remcos\logs.dat		binary
		MD5: D9F366E7F6CE55C0E21B31EE82F777F9	**SHA256:** B31C524703144287773EE9874702C2E9C84D399492E948CA086F513D1D9D9E29	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
7	12	5	7

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	200	178.237.33.50:80	http://geoplugin.net/json.gp	NL	binary	927 b	suspicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	403	104.200.22.130:80	http://www.aieov.com/logo.gif	US	html	175 b	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	403	104.200.22.130:80	http://www.aieov.com/logo.gif	US	html	175 b	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	403	104.200.22.130:80	http://www.aieov.com/logo.gif	US	html	175 b	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	403	104.200.22.130:80	http://www.aieov.com/logo.gif	US	html	175 b	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	403	104.200.23.95:80	http://www.aieov.com/logo.gif	US	html	175 b	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	GET	—	104.200.23.95:80	http://www.aieov.com/logo.gif	US	—	—	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	179.15.24.19:7475	marzo172022.con-ip.com	—	CO	unknown
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	104.200.23.95:80	www.aieov.com	Linode, LLC	US	malicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	178.237.33.50:80	geoplugin.net	Schuberg Philis B.V.	NL	suspicious
1300	608d4a6897d2fd5a8b996bdb43e54d5f.exe	104.200.22.130:80	www.aieov.com	Linode, LLC	US	malicious

DNS requests

Domain	IP	Reputation
marzo172022.con-ip.com	179.15.24.19	malicious
5isohu.com	—	whitelisted
geoplugin.net	178.237.33.50	suspicious
www.aieov.com	104.200.22.130 104.200.23.95	malicious

Threats

PID	Process	Class	Message
—	—	Potentially Bad Traffic	ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)
—	—	Potentially Bad Traffic	ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)

Debug output strings

Debug output strings

No debug info