ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	54f62366f7dc3478ce307aae86e6c2df.exe
Full analysis:	https://app.any.run/tasks/0e8977cb-b9ab-4229-a7bc-0c395fb04933
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 12:23:22
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	rat remcos
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	54F62366F7DC3478CE307AAE86E6C2DF
SHA1:	8C95A35C1C79D7479253FF1146F3820ADA8817FC
SHA256:	5608583B4DA5D0628D0F12FA308CC3A2C5A26E4DB1ADEB2D2D1B65EDD1A014F5
SSDEEP:	12288:o49iwr0vI3cQbtWOc7NKM2TgsNxXKG8wHd36Mo66rMgnIv+30gloc0DMrqSwe7xh:o49iwr0vI3cQbtJgsN9KLwHdlI0Q8

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
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)

REMCOS was detected
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
remcos.exe (PID: 3492)

Changes the autorun value in the registry
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
remcos.exe (PID: 3492)

REMCOS detected by memory dumps
remcos.exe (PID: 3492)

SUSPICIOUS

Checks supported languages
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
cmd.exe (PID: 2772)
remcos.exe (PID: 2904)
remcos.exe (PID: 3492)

Reads the computer name
remcos.exe (PID: 2904)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)
remcos.exe (PID: 3492)

Drops a file with a compile date too recent
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)

Executable content was dropped or overwritten
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)

Application launched itself
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 716)
remcos.exe (PID: 2904)

Reads Environment values
54f62366f7dc3478ce307aae86e6c2df.exe (PID: 2164)
remcos.exe (PID: 3492)

INFO

Reads the computer name
PING.EXE (PID: 3064)
schtasks.exe (PID: 2520)
schtasks.exe (PID: 2440)

Checks supported languages
schtasks.exe (PID: 2520)
PING.EXE (PID: 3064)
schtasks.exe (PID: 2440)

Static information

TRiD

.exe		Generic CIL Executable (.NET, Mono, etc.) (56.7)
.exe		Win64 Executable (generic) (21.3)
.scr		Windows screen saver (10.1)
.dll		Win32 Dynamic Link Library (generic) (5)
.exe		Win32 Executable (generic) (3.4)

EXIF

EXE

AssemblyVersion:	3.1.0.2
ProductVersion:	3.1.0.2
ProductName:	Steam CMD
OriginalFileName:	vvrSc.exe
LegalTrademarks:	
LegalCopyright:	CC BY-NC-SA 4.0
InternalName:	vvrSc.exe
FileVersion:	3.1.0.2
FileDescription:	Steam CMD
CompanyName:	
Comments:	Graphical interface for SteamCMD
CharacterSet:	Unicode
LanguageCode:	Neutral
FileSubtype:	0
ObjectFileType:	Executable application
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	3.1.0.2
FileVersionNumber:	3.1.0.2
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0xe439e
UninitializedDataSize:	0
InitializedDataSize:	4096
CodeSize:	926720
LinkerVersion:	80
PEType:	PE32
TimeStamp:	2022:08:16 09:19:03+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	16-Aug-2022 07:19:03
Comments:	Graphical interface for SteamCMD
CompanyName:	
FileDescription:	Steam CMD
FileVersion:	3.1.0.2
InternalName:	vvrSc.exe
LegalCopyright:	CC BY-NC-SA 4.0
LegalTrademarks:	
OriginalFilename:	vvrSc.exe
ProductName:	Steam CMD
ProductVersion:	3.1.0.2
Assembly Version:	3.1.0.2

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

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	16-Aug-2022 07:19:03
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_EXECUTABLE_IMAGE

OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000080

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00002000	0x000E23A4	0x000E2400	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.79794
.rsrc	0x000E6000	0x00000D50	0x00000E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.7684
.reloc	0x000E8000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

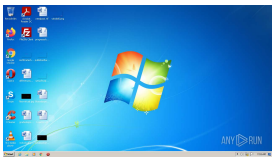
Resources

Title	Entropy	Size	Codepage	Language	Type
1	4.86362	2401	UNKNOWN	UNKNOWN	RT_MANIFEST

Imports

mscoree.dll

Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
44	8	5	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
716	"C:\Users\admin\AppData\Local\Temp\54f62366f7dc3478ce307aae86e6c2df.exe"	C:\Users\admin\AppData\Local\Temp\54f62366f7dc3478ce307aae86e6c2df.exe		Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:	Steam CMD	**Exit code:**	0
Version:	3.1.0.2		

2520	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WSxXBHR" /XML "C:\Users\admin\AppData\Local\Temp\tmpBCD9.tmp"	C:\Windows\System32\schtasks.exe	—	54f62366f7dc3478ce307aae86e6c2df.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)

2164	"{path}"	C:\Users\admin\AppData\Local\Temp\54f62366f7dc3478ce307aae86e6c2df.exe		54f62366f7dc3478ce307aae86e6c2df.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:	Steam CMD	Exit code:	0
Version:	3.1.0.2		

2772	C:\Windows\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\install.bat" "	C:\Windows\system32\cmd.exe	—	54f62366f7dc3478ce307aae86e6c2df.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)

3064	PING 127.0.0.1 -n 2	C:\Windows\system32\PING.EXE	—	cmd.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	TCP/IP Ping Command
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

2904	"C:\Users\admin\AppData\Roaming\remcos\remcos.exe"	C:\Users\admin\AppData\Roaming\remcos\remcos.exe	—	cmd.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:	Steam CMD	Exit code:	0
Version:	3.1.0.2		

2440	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WSxXBHR" /XML "C:\Users\admin\AppData\Local\Temp\tmp630C.tmp"	C:\Windows\System32\schtasks.exe	—	remcos.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	1	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

3492	"{path}"	C:\Users\admin\AppData\Roaming\remcos\remcos.exe		remcos.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:	Steam CMD	Version:	3.1.0.2

Registry activity

Total events	Read events	Write events	Delete events
1 801	1 774	27	0

Modification events

(PID) Process:	(716) 54f62366f7dc3478ce307aae86e6c2df.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(716) 54f62366f7dc3478ce307aae86e6c2df.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(716) 54f62366f7dc3478ce307aae86e6c2df.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet

Value: 1

(PID) Process: (716) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2164) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** remcos
Value: "C:\Users\admin\AppData\Roaming\remcos\remcos.exe"

(PID) Process: (2164) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2164) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2164) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2164) 54f62366f7dc3478ce307aae86e6c2df.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2904) remcos.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2904) remcos.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2904) remcos.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2904) remcos.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3492) remcos.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** remcos
Value: "C:\Users\admin\AppData\Roaming\remcos\remcos.exe"

(PID) Process: (3492) remcos.exe **Key:** HKEY_CURRENT_USER\Software\remcos_ufduenkgsc
Operation: write **Name:** EXEpath
Value: €Ãø Û) e ×¹'(± ∫ª êS Ÿ) s }¬ž¸_ N¥» :ÖXmK ¶C

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	0	4	0

Dropped files

PID	Process	Filename	Type
716	54f62366f7dc3478ce307aae86e6c2df.exe	C:\Users\admin\AppData\Local\Temp\tmpBCD9.tmp **MD5:** BAC802F6C189C389C4A43F994EF6C3F5 **SHA256:** A89C095EEAE487FC43D04E696DBE782AF210095DDE901111718F500D9B5E75D3	xml
3492	remcos.exe	C:\Users\admin\AppData\Roaming\remcos\logs.dat **MD5:** F2C2F3C56C730538E44F428FC90F4BE5 **SHA256:** 11876AD66BAE4825B7CA91B09584EDDE38D15140413BE1CD5799145E2AB922FD	text
2904	remcos.exe	C:\Users\admin\AppData\Local\Temp\tmp630C.tmp **MD5:** BAC802F6C189C389C4A43F994EF6C3F5 **SHA256:** A89C095EEAE487FC43D04E696DBE782AF210095DDE901111718F500D9B5E75D3	xml
2164	54f62366f7dc3478ce307aae86e6c2df.exe	C:\Users\admin\AppData\Roaming\remcos\remcos.exe **MD5:** 54F62366F7DC3478CE307AAE86E6C2DF **SHA256:** 5608583B4DA5D0628D0F12FA308CC3A2C5A26E4DB1ADEB2D2D1B65EDD1A014F5	executable
2164	54f62366f7dc3478ce307aae86	C:\Users\admin\AppData\Local\Temp\install.bat	

	e6c2df.exe			text
		MD5: 4BE8E47D35A08B8B6AD69312F7B4E077	**SHA256:** 428B8E9AF103691C24E02AA1F514D45763C29FD1F83EA77DAB7DEF653545FB60	
716	54f62366f7dc3478ce307aae86e6c2df.exe	C:\Users\admin\AppData\Roaming\WSxXBHR.exe		executable
		MD5: 54F62366F7DC3478CE307AAE86E6C2DF	**SHA256:** 5608583B4DA5D0628D0F12FA308CC3A2C5A26E4DB1ADEB2D2D1B65EDD1A014F5	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	2	1	0

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	194.187.251.163:3573	–	M247 Ltd	BE	malicious

DNS requests

Domain	IP	Reputation
dns.msftncsi.com	131.107.255.255	shared

Threats

No threats detected

Debug output strings

No debug info

ANY RUN INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN
© 2017-2022 ANY.RUN LLC. ALL RIGHTS RESERVED