ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	76fbcfb93293e25b62ae7ea1aa2f72cb.exe
Full analysis:	https://app.any.run/tasks/2a86bce4-8715-4e06-aa5b-5606a4c18d0f
Verdict:	Malicious activity
Threats:	**RedLine** RedLine Stealer is a malicious program that collects users' confidential data from browsers, systems, and installed software. It also infects operating systems with other malware.
Analysis date:	August 22, 2022 at 18:28:32
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan rat redline stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	76FBCFB93293E25B62AE7EA1AA2F72CB
SHA1:	E7974D06F11C52E1AF3FCB2ABEB1A707CFC6AA38
SHA256:	7CA46744C8FB60A69A5236E5DEA109DEA0BA8DCF6578F1A59D89ECFB08E27A76
SSDEEP:	1536:mG6ijoigxUl/btlrK/AgtOUf3NyGLpDliduODv0ujXyyedS+tauIgS6pZ:as7tUf3NXLpDl7O70ujyzdOZ

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

REDLINE was detected
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Steals credentials from Web Browsers
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

REDLINE detected by memory dumps
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Stealing of credential data
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Actions looks like stealing of personal data
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

SUSPICIOUS

Reads the computer name
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Checks supported languages
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Reads Environment values
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Searches for installed software
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

INFO

Reads settings of System Certificates
76fbcfb93293e25b62ae7ea1aa2f72cb.exe (PID: 2176)

Static information

TRiD

.exe | Generic CIL Executable (.NET, Mono, etc.) (55.8)
.exe | Win64 Executable (generic) (21)
.scr | Windows screen saver (9.9)
.dll | Win32 Dynamic Link Library (generic) (5)
.exe | Win32 Executable (generic) (3.4)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2097:08:15 01:34:58+02:00
PEType:	PE32
LinkerVersion:	48
CodeSize:	93184
InitializedDataSize:	2048
UninitializedDataSize:	0

EntryPoint:	0x18ade
OSVersion:	4
ImageVersion:	0
SubsystemVersion:	4
Subsystem:	Windows command line
FileVersionNumber:	0.0.0.0
ProductVersionNumber:	0.0.0.0
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Win32
ObjectFileType:	Executable application
FileSubtype:	0
LanguageCode:	Neutral
CharacterSet:	Unicode
FileDescription:	
FileVersion:	0.0.0.0
InternalName:	Implosions.exe
LegalCopyright:	
OriginalFileName:	Implosions.exe
ProductVersion:	0.0.0.0
AssemblyVersion:	0.0.0.0

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_CUI
Compilation Date:	09-Jul-1961 17:06:42
FileDescription:	
FileVersion:	0.0.0.0
InternalName:	Implosions.exe
LegalCopyright:	
OriginalFilename:	Implosions.exe
ProductVersion:	0.0.0.0
Assembly Version:	0.0.0.0

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:	0x00000080

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	09-Jul-1961 17:06:42
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	0x00002000	0x00016AE4	0x00016C00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	5.90753
.rsrc	0x0001A000	0x000004DE	0x00000600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	3.72394
.reloc	0x0001C000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

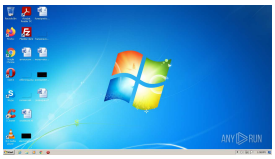
Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.00112	490	UNKNOWN	UNKNOWN	RT_MANIFEST

Imports

mscoree.dll

Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
36	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
2176	"C:\Users\admin\AppData\Local\Temp\76fbcfb93293e25b62ae7ea1aa2f72cb.exe"	C:\Users\admin\AppData\Local\Temp\76fbcfb93293e25b62ae7ea1aa2f72cb.exe		Explorer.EXE

Information

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

Registry activity

Total events	Read events	Write events	Delete events
4 080	4 054	26	0

Modification events

(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	EnableFileTracing
Value:	0		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	EnableConsoleTracing
Value:	0		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	FileTracingMask
Value:			
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	ConsoleTracingMask
Value:			
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	MaxFileSize
Value:	1048576		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASAPI32
Operation:	write	**Name:**	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	EnableFileTracing
Value:	0		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	EnableConsoleTracing
Value:	0		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	FileTracingMask
Value:			
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	ConsoleTracingMask
Value:			
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	MaxFileSize
Value:	1048576		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\76fbcfb93293e25b62ae7ea1aa2f72cb_RASMANCS
Operation:	write	**Name:**	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(2176) 76fbcfb93293e25b62ae7ea1aa2f72cb.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	**Name:**	LanguageList
Value:	en-US		

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	0	24

Dropped files

PID	Process	Filename	Type
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADFA.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE24.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE0F.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE0D.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADD6.tmp **MD5:** B8E63E7225C9F4E0A81371F29D6456D8 **SHA256:** 35A6919CE60EA8E0A44934F8B267BDE2C5A063C2E32F22D34724F168C43150C8	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADE8.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADC5.tmp **MD5:** CC104C4E4E904C3AD7AD5C45FBFA7087 **SHA256:** 321BE844CECC903EF1E7F875B729C96BB3ED0D4986314384CD5944A29A670C9B	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADFD.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADFB.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE26.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE11.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE0E.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADFC.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE22.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE25.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE10.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADC6.tmp **MD5:** CC104C4E4E904C3AD7AD5C45FBFA7087 **SHA256:** 321BE844CECC903EF1E7F875B729C96BB3ED0D4986314384CD5944A29A670C9B	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE23.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADE9.tmp **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpADD7.tmp **MD5:** B8E63E7225C9F4E0A81371F29D6456D8 **SHA256:** 35A6919CE60EA8E0A44934F8B267BDE2C5A063C2E32F22D34724F168C43150C8	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE38.tmp **MD5:** 23D08A78BC908C0B29E9800D3D5614E7 **SHA256:** F6BD7DF5DFAE9FD88811A807DBA14085E00C1B5A6D7CC3D06CC68F6015363D59	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE39.tmp **MD5:** 23D08A78BC908C0B29E9800D3D5614E7 **SHA256:** F6BD7DF5DFAE9FD88811A807DBA14085E00C1B5A6D7CC3D06CC68F6015363D59	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE37.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	C:\Users\admin\AppData\Local\Temp\tmpAE36.tmp **MD5:** 8BB736AB1E4300EF81B27CDBF26D78B0 **SHA256:** 7059AEA2275152A5390580485A2180143879F721C88A4CB0D7702A832751A952	sqlite

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
4	3	1	7

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	POST	200	70.36.108.69:7963	http://70.36.108.69:7963/	US	text	212 b	malicious
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	POST	200	70.36.108.69:7963	http://70.36.108.69:7963/	US	text	147 b	malicious
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	POST	200	70.36.108.69:7963	http://70.36.108.69:7963/	US	text	4.63 Kb	malicious
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	POST	200	70.36.108.69:7963	http://70.36.108.69:7963/	US	text	261 b	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	70.36.108.69:7963	—	Perfect International, Inc	US	malicious
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	104.26.12.31:443	api.ip.sb	Cloudflare Inc	US	suspicious

DNS requests

Domain	IP	Reputation
api.ip.sb	104.26.12.31 104.26.13.31 172.67.75.172	whitelisted

Threats

PID	Process	Class	Message
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	A Network Trojan was detected	AV TROJAN RedLine Stealer Config Download
2176	76fbcfb93293e25b62ae7ea1aa2f72cb.exe	Generic Protocol Command Decode	SURICATA HTTP unable to match response to request

Debug output strings

No debug info