ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	a093c3a1e9dac0ed3259a5e7976897a1.exe
Full analysis:	https://app.any.run/tasks/06dc8d29-3afa-48c9-b773-62c6e8ade20d
Verdict:	Malicious activity
Analysis date:	August 23, 2022 at 15:47:15
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan amadey loader stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	A093C3A1E9DAC0ED3259A5E7976897A1
SHA1:	B489529B88DDDAAE91A2490D76CE1C736B795F42
SHA256:	CDDEBFB93CDDF19DC65C5B2E2BB93B15EC280795A22BED578FC46B83F242837D
SSDEEP:	6144:TEkSnKzlOBYfGTX7+W2AY+WvTzREtd9Ud9HrfelOwVfk:TEkSnSOKfkX3kx4/u9C

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)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 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
- KB2685813
- 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)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398

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)

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

Changes settings of System certificates
wfyoot.exe (PID: 3980)

AMADEY was detected
wfyoot.exe (PID: 3980)

Connects to CnC server
wfyoot.exe (PID: 3980)
rundll32.exe (PID: 3712)

Drops executable file immediately after starts
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)
wfyoot.exe (PID: 3980)

Changes the Startup folder
wfyoot.exe (PID: 3980)

Actions looks like stealing of personal data
rundll32.exe (PID: 3712)

Loads dropped or rewritten executable
rundll32.exe (PID: 3712)

Stealing of credential data
rundll32.exe (PID: 3712)

SUSPICIOUS

Application launched itself
wfyoot.exe (PID: 3980)

Executed via Task Scheduler
wfyoot.exe (PID: 1236)
wfyoot.exe (PID: 3504)

Adds / modifies Windows certificates
wfyoot.exe (PID: 3980)

Checks supported languages
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)
wfyoot.exe (PID: 3980)
wfyoot.exe (PID: 1236)
wfyoot.exe (PID: 3504)

Reads the computer name
wfyoot.exe (PID: 3980)
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)

Executable content was dropped or overwritten
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)
wfyoot.exe (PID: 3980)

Starts itself from another location
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)

Drops a file with a compile date too recent
a093c3a1e9dac0ed3259a5e7976897a1.exe (PID: 3240)
wfyoot.exe (PID: 3980)

INFO

Reads settings of System Certificates
wfyoot.exe (PID: 3980)

Checks supported languages
schtasks.exe (PID: 3768)
rundll32.exe (PID: 3712)

Checks Windows Trust Settings
wfyoot.exe (PID: 3980)

Reads the computer name
schtasks.exe (PID: 3768)
rundll32.exe (PID: 3712)

Static information

TRiD

.exe	|	Win32 Executable MS Visual C++ (generic) (42.2)
.exe	|	Win64 Executable (generic) (37.3)
.dll	|	Win32 Dynamic Link Library (generic) (8.8)
.exe	|	Win32 Executable (generic) (6)
.exe	|	Generic Win/DOS Executable (2.7)

EXIF

EXE

FileSubtype:	0
ObjectFileType:	Unknown (53)
FileOS:	Unknown (0x60484)
FileFlags:	(none)
FileFlagsMask:	0x790c
ProductVersionNumber:	91.0.0.0
FileVersionNumber:	42.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	5.1
ImageVersion:	0
OSVersion:	5.1
EntryPoint:	0x5e3a
UninitializedDataSize:	0
InitializedDataSize:	582144
CodeSize:	65024
LinkerVersion:	10
PEType:	PE32
TimeStamp:	2021:08:19 07:55:45+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	19-Aug-2021 05:55:45
Detected languages:	French - Switzerland Kannada - India (Kannada script)
Debug artifacts:	C:\mezawuhujewicu\dadazubaloyodu-vezerapi40\sije\wexeruzuzat.pdb

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:	0x000000E8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	19-Aug-2021 05:55:45
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0000FC22	0x0000FE00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.4608
.data	0x00011000	0x0007D350	0x0001EE00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.70753
.rsrc	0x0008F000	0x0000F158	0x0000F200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	6.45903

Resources

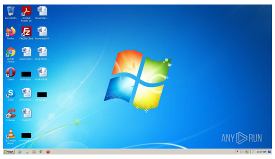
Title	Entropy	Size	Codepage	Language	Type
1	3.4074	408	UNKNOWN	French - Switzerland	RT_VERSION
2	5.58531	2216	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
3	6.20656	1384	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
4	6.39823	9640	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
5	6.58544	4264	UNKNOWN	Kannada - India	RT_ICON

				(Kannada script)	
6	6.59309	2440	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
7	5.93298	1128	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
8	5.3999	3752	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
9	5.82863	2216	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
10	5.91747	1736	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
11	5.89429	1384	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
12	2.31497	34	UNKNOWN	French - Switzerland	RT_GROUP_CURSOR
13	6.00077	4264	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
14	5.92835	2440	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
15	6.00268	1128	UNKNOWN	Kannada - India (Kannada script)	RT_ICON
16	2.21078	816	UNKNOWN	French - Switzerland	RT_CURSOR
17	3.2585	1194	UNKNOWN	French - Switzerland	RT_STRING
18	2.6581	304	UNKNOWN	French - Switzerland	RT_CURSOR
19	2.20327	176	UNKNOWN	French - Switzerland	RT_CURSOR
20	3.30008	1668	UNKNOWN	French - Switzerland	RT_STRING
120	2.83776	104	UNKNOWN	Kannada - India (Kannada script)	RT_GROUP_ICON
130	4.62296	2001	UNKNOWN	French - Switzerland	WOCIYIYAJETAFO
153	2.91481	118	UNKNOWN	Kannada - India (Kannada script)	RT_GROUP_ICON
738	4.64297	1590	UNKNOWN	French - Switzerland	SENUZEMIX
2387	2.33006	34	UNKNOWN	French - Switzerland	RT_GROUP_CURSOR

Imports

ADVAPI32.dll
KERNEL32.dll
USER32.dll

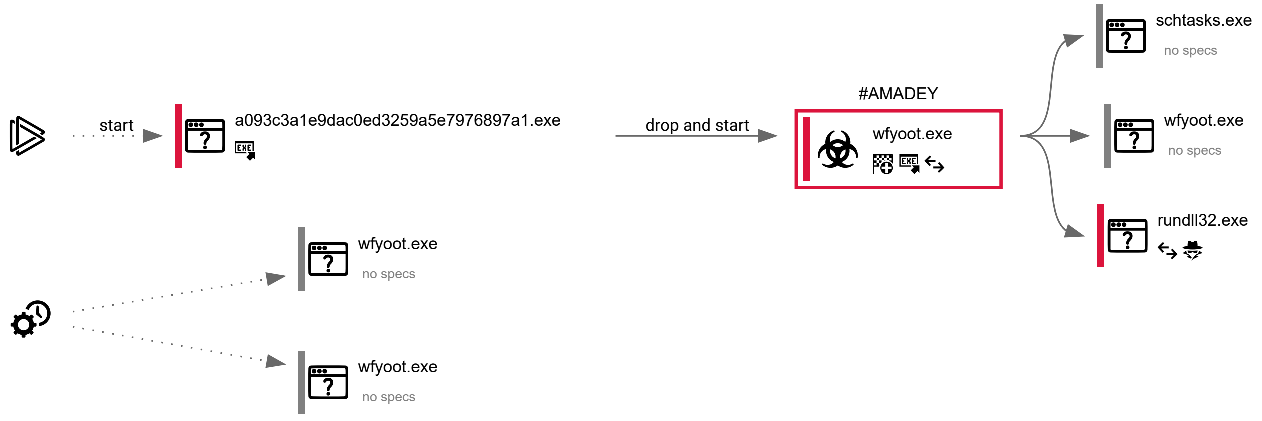
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
40	7	3	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
3240	"C:\Users\admin\AppData\Local\Temp\a093c3a1e9dac0ed3259a5e7976897a1.exe"	C:\Users\admin\AppData\Local\Temp\a093c3a1e9dac0ed3259a5e7976897a1.exe	EXE	Explorer.EXE

Information

User:	admin	Integrity Level:	MEDIUM
Exit code:	0		

3980	"C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe"	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	⇆ ☣	a093c3a1e9dac0ed3259a5e7976897a1.exe

Information

User:	admin	Integrity Level:	MEDIUM

3768	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN wfyoot.exe /TR "C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe" /F	C:\Windows\System32\schtasks.exe	—	wfyoot.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)

1236	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	—	taskeng.exe

Information

User:	admin	Integrity Level:	MEDIUM
Exit code:	0		

1852	"C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe"	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	—	wfyoot.exe

Information

User:	admin	Integrity Level:	MEDIUM

3712	"C:\Windows\System32\rundll32.exe" C:\Users\admin\AppData\Roaming\9034267ed8b4ad\cred.dll, Main	C:\Windows\System32\rundll32.exe	⇆	wfyoot.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows host process (Rundll32)
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

3504	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe	—	taskeng.exe

Information

User:	admin	Integrity Level:	MEDIUM
Exit code:	0		

Registry activity

Total events	Read events	Write events	Delete events
6 976	6 909	64	3

Modification events

(PID) Process:	(3240) a093c3a1e9dac0ed3259a5e7976897a1.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value: 1			
(PID) Process:	(3240) a093c3a1e9dac0ed3259a5e7976897a1.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value: 1			
(PID) Process:	(3240) a093c3a1e9dac0ed3259a5e7976897a1.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value: 1			
(PID) Process:	(3240) a093c3a1e9dac0ed3259a5e7976897a1.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value: 0			
(PID) Process:	(3980) wfyoot.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Operation:	write	Name:	Startup
Value: C:\Users\admin\AppData\Local\Temp\7ce0308eb7\			
(PID) Process:	(3980) wfyoot.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value: 1			

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B0100000900000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000000100000002000000C0A8016400000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000

(PID) Process: (3980) wfyoot.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: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: E0153993D9B6D801

(PID) Process: (3980) wfyoot.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: (3980) wfyoot.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: (3980) wfyoot.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: (3980) wfyoot.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: E0153993D9B6D801

(PID) Process: (3980) wfyoot.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: (3980) wfyoot.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (3980) wfyoot.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8
Operation: write **Name:** Blob
Value: 040000000100000010000000CD2F9E0DA1773E9ED864DA5E370E74E0F000000010000000200000003F0411EDE9C4477057D57E57883B1F205B20CDC0F3263129B1EE0269A2678F63030000
00010000014000000CABD2A79A1076A31F21D253635CB039D4329A5E809000000001000000C000000300A06082B0601050507030110D0000000100000010000000073B6876195F5D18E0485
10422AEF04E314000000010000001400000079B459E67BB6E5E40173800888C81A58F6E99B6E0B0000000100000001A00000049005300520047002000520006F006F007400200058003100000
06200000001000000200000000096BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6190000000100000001000000002FE1F70BB05D7C92335BC5E05B984DA62000
0000010000006F0500003082056B30820353A003020102021100821 0CFB0D240E3594463E0BB63828B00300D06092A864886F70D01010B0500304F310B300906035504061302555331293027060355040A1320496E7465726E65742053656375726974792052657365617263682047726F75703115301306035504031 30C4953524720526F6F74205831301E170D3135303630343131303
433385A170D3335303630343131303433385A304F310B300906035504061302555331293027060355040A1320496E7465726E6574205365637572697479205265736561726368204772 6F757
03115301306035504031 30C4953524720526F6F74205831308202223 00D06092A864886F70D01010105000382020F003082020A0282020100ADE82473F41437F39B9E2B57281C87BEDCB7D
F38908C6E3CE657A078F775C2A2FEF56A6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5DD79DFB3B8FF12F1219A4BC18A8671694A66666C8F7E3C70B
FAD292206F3E4C0E680AEE24B8FB7997E94039FD347977C99482353E838AE4F0A6F832ED149578C8074B6DA2FD0388D7B0370211B75F2303CFA8FAEDDDA63ABEB164FC28E114B7ECF0BE
8FFB5772EF4B27B4AE04C12250C708D0329A0E15324EC13D9EE19BF10B34A8C3F89A36151DEAC870794F46371EC2EE26F5B9881E1895C34796C76EF3B906279E6DBA49A2F26C5D010E10
EDED9108E16FBB7F7A8F7C7E50207988F360895E7E237960D36759EFB0E72B11D9BBC03F94905D881DD05B42AD641E9AC0176950A0FD8DFD5BD121F352F28176CD298C1A80964776E473

```
7BACEAC595E689D7F72D689C50641293E593EDD26F524C911A75AA34C401F46A199B5A73A516E863B9E7D72A712057859ED3E5178150B038F8DD02F05B23E7B4A1C4B730512FCC6EAE05
0137C439374B3CA74E78E1F0108D030D45B7136B407BAC130305C48B7823B98A67D608AA2A32982CCBABD83041BA2830341A1D605F11BC2B6F0A87C863B46A8482A88DC769A76BF1F6A
A53D198FEB38F364DEC82B0D0A28FFF7DBE21542D422D0275DE179FE18E77088AD4EE6D98B3AC6DD27516EFFBC64F533434F0203010001A3423040300E0603551D0F0101FF04040302010
6300F0603551D130101FF040530030101FF301D0603551D0E0416041479B459E67BB6E5E40173800888C81A58F6E99B6E300D06092A864886F70D01010B05000382020100551F58A9BCB2A
850D00CB1D81A6920272908AC61755C8A6EF882E5692FD5F6564BB9B8731059D321977EE74C71FBB2D260AD39A80BEA17215685F1500E59EBCEE059E9BAC915EF869D8F8480F6E4E9919
0DC179B621B45F06695D27C6FC2EA3BEF1FCFCBD6AE27F1A9B0C8AEFD7D7E9AFA2204EBFFD97FEA912B22B1170E8FF28A345B58D8FC01C954B9B826CC8A8833894C2D843C82DFEE9657
05BA2CBBF7C4B7C74E3B82BE31C822737392D1C280A43939103323824C3C9F86B255981DBE29868C229B9EE26B3B573A82704DDC09C789CB0A074D6CE85D8EC9EFCEABC7BBB52B4E45D
64AD026CCE572CA086AA595E315A1F7A4EDC92C5FA5FBFFAC28022EBED77BBBE3717B9016D3075E46537C3707428CD3C4969CD599B52AE0951A8048AE4C3907CECC47A452952BBAB8FB
ADD233537DE51D4D6DD5A1B1C7426FE64027355CA328B7078DE78D3390E7239FFB509C796C46D5B415B3966E7E9B0C963AB8522D3FD65BE1FB08C284FE24A8A389DAAC6AE1182AB1A84
3615BD31FDC3B8D76F22DE88D75DF17336C3D53FB7BCB415FFFDCA2D06138E196B8AC5D8B37D775D533C09911AE9D41C1727584BE0241425F67244894D19B27BE073FB9B84F817451E17
AB7ED9D23E2BEE0D52804133C31039EDD7A6C8FC60718C67FDE478E3F289E0406CFA5543477BDEC899BE91743DF5BDB5FFE8E1E57A2CD409D7E6222DADE1827
```

(PID) Process: (3980) wfyoot.exe
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8
Operation: delete key
Name: (default)
Value:

(PID) Process: (3980) wfyoot.exe
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8
Operation: write
Name: Blob
Value:

```
5C0000000100000004000000001000000F00000001000000200000003F0411EDE9C4477057D57E57883B1F205B20CDC0F3263129B1EE0269A2678F630300000001000000140000000CABD2A
79A1076A31F21D253635CB039D4329A5E80900000001000000000C000000300A06082B0601050507030111D00000000100000001000000073B6876195F5D18E048510422AEF04E31400000001000
0001400000079B459E67BB6E5E40173800888C81A58F6E99B6E0B000000010000001A000000490053005200470020005200200F006F0074002000580031000000620000000100000020000009
6BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6190000000100000010000000002FE1F70BB05D7C92335BC5E05B984DA620000000010000006F050000308205
6B30820353A003020102021100821 0CFB0D240E3594463E0BB63828B00300D06092A864886F70D01010B0500304F310B300906035504061302555331293027060355040A1320496E7465726
E6574205365637572697479205265736561726368204772F757031153013060355040313 0C4953524720526F6F74205831301E170D313530363034313130343385A170D333530363034313
1303433385A304F310B300906035504061302555331293027060355040A1320496E7465726E6574205365637572697479205265736561726368204772F757031153013060355040313 0C495
3524720526F6F742058313 0820222300D06092A864886F70D01010105000382020F003082020A0282020100ADE82473F41437F39B9E2B57281C87BEDCB7DF38908C6E3CE657A078F775C2A
2FEF56A6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5DD79DFB3B8FF12F1219A4BC18A8671694A66666C8F7E3C70BFAD292206F3E4C0E680AEE24B8
FB7997E94039FD347977C99482353E838AE4F0A6F832ED149578C8074B6DA2FD0388D7B0370211B75F2303CFA8FAEDDDA63ABEB164FC28E114B7ECF0BE8FFB5772EF4B27B4AE04C12250
C708D0329A0E15324EC13D9EE19BF10B34A8C3F89A36151DEAC870794F46371EC2EE26F5B9881E1895C34796C76EF3B906279E6DBA49A2F26C5D010E10EDED9108E16FBB7F7A8F7C7E50
207988F360895E7E237960D36759EFB0E72B11D9BBC03F94905D881DD05B42AD641E9AC0176950A0FD8DFD5BD121F352F28176CD298C1A80964776E4737BACEAC595E689D7F72D689C50
641293E593EDD26F524C911A75AA34C401F46A199B5A73A516E863B9E7D72A712057859ED3E5178150B038F8DD02F05B23E7B4A1C4B730512FCC6EAE050137C439374B3CA74E78E1F010
8D030D45B7136B407BAC130305C48B7823B98A67D608AA2A32982CCBABD83041BA2830341A1D605F11BC2B6F0A87C863B46A8482A88DC769A76BF1F6AA53D198FEB38F364DEC82B0D0
A28FFF7DBE21542D422D0275DE179FE18E77088AD4EE6D98B3AC6DD27516EFFBC64F533434F0203010001A3423040300E0603551D0F0101FF040403020106300F0603551D130101FF04053
0030101FF301D0603551D0E0416041479B459E67BB6E5E40173800888C81A58F6E99B6E300D06092A864886F70D01010B05000382020100551F58A9BCB2A850D00CB1D81A6920272908AC
61755C8A6EF882E5692FD5F6564BB9B8731059D321977EE74C71FBB2D260AD39A80BEA17215685F1500E59EBCEE059E9BAC915EF869D8F8480F6E4E99190DC179B621B45F06695D27C6FC
2EA3BEF1FCFCBD6AE27F1A9B0C8AEFD7D7E9AFA2204EBFFD97FEA912B22B1170E8FF28A345B58D8FC01C954B9B826CC8A8833894C2D843C82DFEE965705BA2CBBF7C4B7C74E3B82BE31
C822737392D1C280A43939103323824C3C9F86B255981DBE29868C229B9EE26B3B573A82704DDC09C789CB0A074D6CE85D8EC9EFCEABC7BBB52B4E45D64AD026CCE572CA086AA595E3
15A1F7A4EDC92C5FA5FBFFAC28022EBED77BBBE3717B9016D3075E46537C3707428CD3C4969CD599B52AE0951A8048AE4C3907CECC47A452952BBAB8FBADD233537DE51D4D6DD5A1B1
C7426FE64027355CA328B7078DE78D3390E7239FFB509C796C46D5B415B3966E7E9B0C963AB8522D3FD65BE1FB08C284FE24A8A389DAAC6AE1182AB1A843615BD31FDC3B8D76F22DE88
D75DF17336C3D53FB7BCB415FFFDCA2D06138E196B8AC5D8B37D775D533C09911AE9D41C1727584BE0241425F67244894D19B27BE073FB9B84F817451E17AB7ED9D23E2BEE0D52804133
C31039EDD7A6C8FC60718C67FDE478E3F289E0406CFA5543477BDEC899BE91743DF5BDB5FFE8E1E57A2CD409D7E6222DADE1827
```

(PID) Process: (3980) wfyoot.exe
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8
Operation: write
Name: Blob
Value:

```
5C000000010000000400000000100000190000000100000010000000 2FE1F70BB05D7C92335BC5E05B984DA6620000000100000002000000096BCEC06264976F37460779ACF28C5A7CFE8A3
C0AAE11A8FFCEE05C0BDDF08C60B000000010000001A000000490053005200470020005200200F006F0074002000580031000000140000000100000014000000079B459E67BB6E5E401738008
88C81A58F6E99B6E1D000000010000000100000073B6876195F5D18E048510422AEF04E303000000001000000140000000CABD2A79A1076A31F21D253635CB039D4329A5E80F0000000100000
00200000003F0411EDE9C4477057D57E57883B1F205B20CDC0F3263129B1EE0269A2678F6309000000001000000160000000301406082B0601050507030206082B0601050507030120000000
10000006F0500003082056B30820353A003020102021100821 0CFB0D240E3594463E0BB63828B00300D06092A864886F70D01010B0500304F310B300906035504061302555331293027060 3
55040A1320496E7465726E6574205365637572697479205265736561726368204772F757031153013060355040313 0C4953524720526F6F74205831301E170D31353036303431313034333 38
5A170D333530363034313130343385A304F310B300906035504061302555331293027060355040A1320496E7465726E6574205365637572697479205265736561726368204772F75703115
3013060355040313 0C4953524720526F6F742058313 0820222300D06092A864886F70D01010105000382020F003082020A0282020100ADE82473F41437F39B9E2B57281C87BEDCB7DF3890
8C6E3CE657A078F775C2A2FEF56A6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5DD79DFB3B8FF12F1219A4BC18A8671694A66666C8F7E3C70BFAD29
2206F3E4C0E680AEE24B8FB7997E94039FD347977C99482353E838AE4F0A6F832ED149578C8074B6DA2FD0388D7B0370211B75F2303CFA8FAEDDDA63ABEB164FC28E114B7ECF0BE8FFB5
772EF4B27B4AE04C12250C708D0329A0E15324EC13D9EE19BF10B34A8C3F89A36151DEAC870794F46371EC2EE26F5B9881E1895C34796C76EF3B906279E6DBA49A2F26C5D010E10EDED9
108E16FBB7F7A8F7C7E50207988F360895E7E237960D36759EFB0E72B11D9BBC03F94905D881DD05B42AD641E9AC0176950A0FD8DFD5BD121F352F28176CD298C1A80964776E4737BACE
AC595E689D7F72D689C50641293E593EDD26F524C911A75AA34C401F46A199B5A73A516E863B9E7D72A712057859ED3E5178150B038F8DD02F05B23E7B4A1C4B730512FCC6EAE050137C
439374B3CA74E78E1F0108D030D45B7136B407BAC130305C48B7823B98A67D608AA2A32982CCBABD83041BA2830341A1D605F11BC2B6F0A87C863B46A8482A88DC769A76BF1F6AA53D1
98FEB38F364DEC82B0D0A28FFF7DBE21542D422D0275DE179FE18E77088AD4EE6D98B3AC6DD27516EFFBC64F533434F0203010001A3423040300E0603551D0F0101FF040403020106300F
0603551D130101FF040530030101FF301D0603551D0E0416041479B459E67BB6E5E40173800888C81A58F6E99B6E300D06092A864886F70D01010B05000382020100551F58A9BCB2A850D0
0CB1D81A6920272908AC61755C8A6EF882E5692FD5F6564BB9B8731059D321977EE74C71FBB2D260AD39A80BEA17215685F1500E59EBCEE059E9BAC915EF869D8F8480F6E4E99190DC17
9B621B45F06695D27C6FC2EA3BEF1FCFCBD6AE27F1A9B0C8AEFD7D7E9AFA2204EBFFD97FEA912B22B1170E8FF28A345B58D8FC01C954B9B826CC8A8833894C2D843C82DFEE965705BA2
CBBF7C4B7C74E3B82BE31C822737392D1C280A43939103323824C3C9F86B255981DBE29868C229B9EE26B3B573A82704DDC09C789CB0A074D6CE85D8EC9EFCEABC7BBB52B4E45D64AD
026CCE572CA086AA595E315A1F7A4EDC92C5FA5FBFFAC28022EBED77BBBE3717B9016D3075E46537C3707428CD3C4969CD599B52AE0951A8048AE4C3907CECC47A452952BBAB8FBADD
233537DE51D4D6DD5A1B1C7426FE64027355CA328B7078DE78D3390E7239FFB509C796C46D5B415B3966E7E9B0C963AB8522D3FD65BE1FB08C284FE24A8A389DAAC6AE1182AB1A84361
5BD31FDC3B8D76F22DE88D75DF17336C3D53FB7BCB415FFFDCA2D06138E196B8AC5D8B37D775D533C09911AE9D41C1727584BE0241425F67244894D19B27BE073FB9B84F817451E17AB
7ED9D23E2BEE0D52804133C31039EDD7A6C8FC60718C67FDE478E3F289E0406CFA5543477BDEC899BE91743DF5BDB5FFE8E1E57A2CD409D7E6222DADE1827
```

Files activity

Executable files	Suspicious files	Text files	Unknown types
4	7	3	3

Dropped files

PID	Process	Filename	Type
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Temp\Cab1386.tmp **MD5:** 589C442FC7A0C70DCA927115A700D41E **SHA256:** 2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A	compressed
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\103621DE9CD5414CC2538780B4B75751 **MD5:** EC8FF3B1DED0246437B1472C69DD1811 **SHA256:** E634C2D1ED20E0638C95597ADF4C9D392EBAB932D3353F18AF1E4421F4BB9CAB	der
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** E35D2244E4CB63C8ACC78E3C44C63246 **SHA256:** 0E341AD50BC57C26BF9FE65C4969F4F08AA806B4A551B8027F1BC6B8E5FE9FE6	binary
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PO2HN1X2\Clipper[1].htm **MD5:** 9527755784F5014D2C94DCABDF6AE892 **SHA256:** 5B111EF9F2DBAF8E8870567DC8E2302EFE2B0FEB9D4BA62CE74C1039AB663523	html
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Temp\Tar1387.tmp **MD5:** 7EE994C83F2744D702CBA18693ED1758 **SHA256:** 5DB917AB6DC8A42A43617850DFBE2C7F26A7F810B229B349E9DD2A2D615671D2	cat
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Temp\302019708150	image

		MD5: D76D4FCE1FD859CB408F343CAD700821 **SHA256:** F9C840A8D81C37FE98CA855DE9C2455401D488B88FEF873EC5D905D59CC982CA	
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3240	a093c3a1e9dac0ed3259a5e7976897a1.exe	C:\Users\admin\AppData\Local\Temp\7ce0308eb7\wfyoot.exe **MD5:** A093C3A1E9DAC0ED3259A5E7976897A1 **SHA256:** CDDEBFB93CDDF19DC65C5B2E2BB93B15EC280795A22BED578FC46B83F242837D	executable
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 **MD5:** 46B86C7063352D904E49AE261B96C2FB **SHA256:** 723BE30BB2D721D19EFA3DB77E9E75A053074B31C91CA9F6BC75250F79A4F6C3	binary
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\103621DE9CD5414CC2538780B4B75751 **MD5:** D46E379EBED1521B8B51D19ADEEF5DF7 **SHA256:** 7F2B91309B31E1C314E1D6D6634DC22C03174469BAE2B050667AA164438A7E02	binary
3980	wfyoot.exe	C:\Users\admin\AppData\Roaming\9034267ed8b4ad\cred.dll **MD5:** A81511E199A9AA34DA15D12C2F294B2C **SHA256:** B9FA703B80C7D124148F64AE3474F1F2B01A42CD1ED6871BE2BB6C9D15ECF871	executable
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E00821B6FB36D72EF56707263DB1D9D3 **MD5:** 380EFD0BBA67F1ADA1166075E4405A5C **SHA256:** D13C2350FDBF9848973669D1A46C66845325627219A31021924620832A05BDD9	binary
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 **MD5:** 589C442FC7A0C70DCA927115A700D41E **SHA256:** 2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A	compressed
3980	wfyoot.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E00821B6FB36D72EF56707263DB1D9D3 **MD5:** CC3B3BEFE90AF9F599EB24B9F5CDAC0D **SHA256:** BF42A13BBF92995817F9C49BE8EDB73553D250112517673CC937EDEED8F195F9	der
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\cred[1].dll **MD5:** A81511E199A9AA34DA15D12C2F294B2C **SHA256:** B9FA703B80C7D124148F64AE3474F1F2B01A42CD1ED6871BE2BB6C9D15ECF871	executable
3980	wfyoot.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\Clipper[1].exe **MD5:** 4AD1041B33752303AC4F701F2DE81FB1 **SHA256:** 25C94F4B0DCF642C9D7195A598BAD6A87940FC6EF48423D7B5CBE3E5A8105623	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
12	8	4	8

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3980	wfyoot.exe	GET	200	88.221.25.162:80	http://r3.o.lencr.org/MFMwUTBPME0wSzAJBgUrDgMCGgUABBRI2smg%2ByvTLU%2Fw3mjS9We3NfmzxAQUFC6zF7dYVsuuUAlA5h%2BvnYsUwsYCEgT4o4x%2BULWxwiBn4qG5Z0hGXQ%3D%3D	unknown	der	503 b	shared
3712	rundll32.exe	POST	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php	PT	—	—	malicious
3980	wfyoot.exe	GET	200	104.73.131.204:80	http://x1.c.lencr.org/	NL	der	717 b	whitelisted
3980	wfyoot.exe	GET	301	5.23.51.236:80	http://dhjytjngtr.site/Clipper.exe	RU	html	169 b	suspicious
3980	wfyoot.exe	POST	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php?scr=1	PT	—	—	malicious
3980	wfyoot.exe	GET	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/Plugins/cred.dll	PT	executable	126 Kb	malicious
3980	wfyoot.exe	POST	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php	PT	text	68 b	malicious
3980	wfyoot.exe	POST	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php	PT	—	—	malicious
3980	wfyoot.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?f792aad79232c83b	US	compressed	60.2 Kb	whitelisted
3980	wfyoot.exe	POST	—	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php?scr=1	PT	—	—	malicious
3980	wfyoot.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b1f846155c21a6a8	US	compressed	4.70 Kb	whitelisted
3980	wfyoot.exe	POST	200	185.215.113.204:80	http://185.215.113.204/f84Nls2/index.php	PT	text	6 b	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3980	wfyoot.exe	5.23.51.236:443	dhjytjngtr.site	TIMEWEB GmbH	RU	malicious
3712	rundll32.exe	185.215.113.204:80	—	Ebonyhorizon Telecomunicacoes S.A.	PT	malicious
3980	wfyoot.exe	104.73.131.204:80	x1.c.lencr.org	Akamai International B.V.	NL	unknown
3980	wfyoot.exe	185.215.113.204:80	—	Ebonyhorizon Telecomunicacoes S.A.	PT	malicious

3980	wfyoot.exe	209.197.3.8:80	ctldl.windowsupdate.com	Highwinds Network Group, Inc.	US	suspicious
3980	wfyoot.exe	5.23.51.236:80	dhjytjngtr.site	TIMEWEB GmbH	RU	malicious
3980	wfyoot.exe	88.221.25.162:80	r3.o.lencr.org	Akamai International B.V.	—	whitelisted

DNS requests

Domain	IP	Reputation
dhjytjngtr.site	5.23.51.236	suspicious
ctldl.windowsupdate.com	209.197.3.8	whitelisted
x1.c.lencr.org	104.73.131.204	whitelisted
r3.o.lencr.org	88.221.25.162	shared

Threats

PID	Process	Class	Message
3980	wfyoot.exe	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 21
3980	wfyoot.exe	A Network Trojan was detected	ET TROJAN Amadey CnC Check-In
3980	wfyoot.exe	A Network Trojan was detected	AV TROJAN Agent.DHOA System Info Exfiltration
3980	wfyoot.exe	A Network Trojan was detected	ET CURRENT_EVENTS SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016
3980	wfyoot.exe	Potential Corporate Privacy Violation	AV POLICY HTTP request for .exe file with no User-Agent
3980	wfyoot.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
3980	wfyoot.exe	Potential Corporate Privacy Violation	AV POLICY HTTP request for .dll file with no User-Agent
3712	rundll32.exe	A Network Trojan was detected	AV TROJAN Trojan/Win32.Agent InfoStealer CnC Checkin

Debug output strings

No debug info

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN