ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	f6ea9784e18eb238af282efa0c776cb5.exe
Full analysis:	https://app.any.run/tasks/eed2fea2-4dfa-4c2a-b4b5-e23bbd936818
Verdict:	Malicious activity
Analysis date:	September 02, 2022 at 22:56:06
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan ransomware stop
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	F6EA9784E18EB238AF282EFA0C776CB5
SHA1:	75F6A473A56CBF118A976044D4181109875E7F07
SHA256:	8718C3FB8AF937BC27504FF5EB70C3C0C73B6B5212B7EBDBC6FDED506595E912
SSDEEP:	24576:hbW1P08mihAVWnKhH6BP0muJwrm1WIu4hG:hGhAVgKhH6Iwq1WihG

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	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 the autorun value in the registry
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)

Loads the Task Scheduler COM API
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

Drops executable file immediately after starts
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)

Changes settings of System certificates
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

STOP was detected
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

SUSPICIOUS

Checks supported languages
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3936)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 352)

Reads the computer name
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

Application launched itself
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3936)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 352)

Executable content was dropped or overwritten
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)

Uses ICACLS.EXE to modify access control list
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)

Drops a file with a compile date too recent
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3072)

Adds / modifies Windows certificates
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

INFO

Checks supported languages
icacls.exe (PID: 2824)

Reads the computer name
icacls.exe (PID: 2824)

Reads settings of System Certificates
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

Checks Windows Trust Settings
f6ea9784e18eb238af282efa0c776cb5.exe (PID: 3400)

Static information

TRiD

.exe	|	Win32 Executable MS Visual C++ (generic) (35.8)

.exe	|	Win64 Executable (generic) (31.7)
.scr	|	Windows screen saver (15)
.dll	|	Win32 Dynamic Link Library (generic) (7.5)
.exe	|	Win32 Executable (generic) (5.1)

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	2022-Jan-24 12:03:34
Detected languages:	Korean - Korea
Debug artifacts:	C:\zizibize\piyutepazas\roxawep.pdb

DOS Header

e_magic:	MZ
e_cblp:	144
e_cp:	3
e_crlc:	0
e_cparhdr:	4
e_minalloc:	0
e_maxalloc:	65535
e_ss:	0
e_sp:	184
e_csum:	0
e_ip:	0
e_cs:	0
e_ovno:	0
e_oemid:	0
e_oeminfo:	0
e_lfanew:	224

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
NumberofSections:	3
TimeDateStamp:	2022-Jan-24 12:03:34
PointerToSymbolTable:	0
NumberOfSymbols:	0
SizeOfOptionalHeader:	224
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	4096	180184	180224	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.08742
.data	184320	4798280	601088	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.99215
.rsrc	4984832	19296	19456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.9601

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.68558	1736	UNKNOWN	Korean - Korea	RT_ICON
2	5.94835	1384	UNKNOWN	Korean - Korea	RT_ICON
3	5.66235	4264	UNKNOWN	Korean - Korea	RT_ICON
4	5.76251	2440	UNKNOWN	Korean - Korea	RT_ICON
5	6.2359	1128	UNKNOWN	Korean - Korea	RT_ICON
6	4.09164	304	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.5416	304	UNKNOWN	UNKNOWN	RT_CURSOR
8	2.50404	240	UNKNOWN	UNKNOWN	RT_CURSOR
9	1.59806	4264	UNKNOWN	UNKNOWN	RT_CURSOR
26	3.01622	330	UNKNOWN	Korean - Korea	RT_STRING
27	3.13643	476	UNKNOWN	Korean - Korea	RT_STRING
28	1.854	68	UNKNOWN	Korean - Korea	RT_STRING
129	2.72482	76	UNKNOWN	Korean - Korea	RT_GROUP_ICON
191	3.04819	88	UNKNOWN	Korean - Korea	RT_ACCELERATOR
429	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
432	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
437	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
442	1.84644	10	UNKNOWN	Korean - Korea	UNKNOWN
446	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT

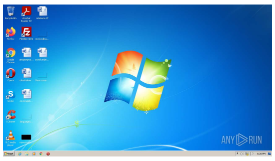
453	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
456	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
457	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
460	3.14856	320	UNKNOWN	UNKNOWN	RT_VERSION
591	3.12537	104	UNKNOWN	Korean - Korea	RT_ACCELERATOR
2371	1.98048	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
2374	2.55787	48	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
453 (#2)	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN

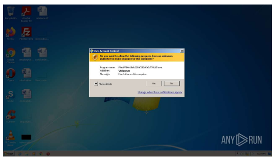
Imports

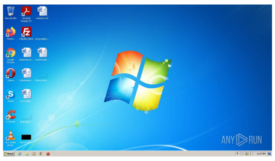
KERNEL32.dll

USER32.dll

Video and screenshots



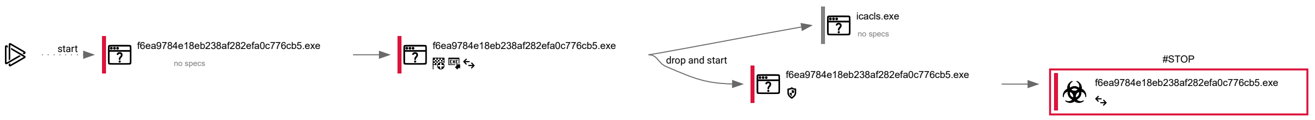




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
43	5	4	0

Behavior graph


start
f6ea9784e18eb238af282efa0c776cb5.exe
no specs
f6ea9784e18eb238af282efa0c776cb5.exe
drop and start
icacls.exe
no specs
f6ea9784e18eb238af282efa0c776cb5.exe
#STOP
f6ea9784e18eb238af282efa0c776cb5.exe

Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
3936	"C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe"	C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe	—	Explorer.EXE

Information

User: admin **Integrity Level:** MEDIUM

Exit code: 0

3072	"C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe"	C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe	⇆	f6ea9784e18eb238af282efa0c776cb5.exe

Information

User: admin Integrity Level: MEDIUM

Exit code: 0

2824	icacls "C:\Users\admin\AppData\Local\9d55a140-8dad-425b-878c-06c733a55f68" /deny *S-1-1-0:(OI)(CI)(DE,DC)	C:\Windows\system32\icacls.exe	—	f6ea9784e18eb238af282efa0c776cb5.exe

Information

User: admin Company: Microsoft Corporation

Integrity Level: MEDIUM Exit code: 0

Version: 6.1.7600.16385 (win7_rtm.090713-1255)

352	"C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe" --Admin IsNotAutoStart IsNotTask	C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe		f6ea9784e18eb238af282efa0c776cb5.exe

Information

User: admin Integrity Level: HIGH

Exit code: 0

3400	"C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe" --Admin IsNotAutoStart IsNotTask	C:\Users\admin\AppData\Local\Temp\f6ea9784e18eb238af282efa0c776cb5.exe	⇆	f6ea9784e18eb238af282efa0c776cb5.exe

Information

User: admin Integrity Level: HIGH

Registry activity

Total events	Read events	Write events	Delete events
5 635	5 547	87	1

Modification events

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value: 460000003B010000090000000000000000000000000000000400000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A80164000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content

Operation: write **Name:** CachePrefix

Value:

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies

Operation: write **Name:** CachePrefix

Value: Cookie:

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

Operation: write **Name:** CachePrefix

Value: Visited:

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.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: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 4618A71AF1BED801

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.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: (3072) f6ea9784e18eb238af282efa0c776cb5.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: (3072) f6ea9784e18eb238af282efa0c776cb5.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: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 4618A71AF1BED801

(PID) Process: (3072) f6ea9784e18eb238af282efa0c776cb5.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: (3072) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Operation: write **Name:** SysHelper

Value: "C:\Users\admin\AppData\Local\9d55a140-8dad-425b-878c-06c733a55f68\f6ea9784e18eb238af282efa0c776cb5.exe" --AutoStart

---

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value:
```
460000003C010000090000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000010000000200000 0C0A864B6000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
```

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content

Operation: write **Name:** CachePrefix

Value:

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies

Operation: write **Name:** CachePrefix

Value: Cookie:

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

Operation: write **Name:** CachePrefix

Value: Visited:

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap c776cb5.exe

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.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: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 4618A71AF1BED801

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.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: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDetectedUrl

Value:

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.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: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 2D080F42F1BED801

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.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: (3400) f6ea9784e18eb238af282efa0c776cb5.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: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 2D080F42F1BED801

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: delete value **Name:** WpadDetectedUrl

Value:

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E

Operation: write **Name:** Blob

Value:

```
0400000001000000100000001BFE69D191B71933A372A80FE155E5B5090000000100000054000000305206082B0601050507030206082B0601050507030306 0A2B0601040182370A0304060
82B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B060105050703080F0000000100000030000000066B764A96581128168CF208E374DDA
479D54E311F32457F4AEE0DBD2A6C8D171D531289E1CD22BFDBBD4CFD979625483030000000100000014000000 2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0B000000100000010
0000005300650063007400690067006F0000001D0000000100000010000000885010358D29A38F059B028559C95F90140000000100000014000000 5379BF5AAA2B4ACF5480E1D89BC09DF2
B20366CB62000000010000002000000 0E793C9B02FD8AA13E21C31228ACCB08119643B749C898964B1746D46C3D4CBD2190000000100000010000000EA6089055218053DD01E37E1D806E
EDF5300000001000000430000003041302 2060C2B06010401B2310102010501301230100 60A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C01
01030200C0200000000 1000000E2050000308205DE308203C6A003020102021001FD6D30FCA3CA51A81BBC640E35032D300D06092A864886F70D01010C0500308188310B30090603550406
13025553311330110603550408130A4E6577204A657273657931143012060355040 7130B4A65727365792043697479311E301C060355040A1315546865205553455254525553 54204E657477
6F726B312E302C0603550403132555534552547275737420525341204365727469666963 6174696F6E20417574686F72697479301E170D3130303230313030303030305A170D333830313138
3233353935395A308188310B300906035504061302555331133011060355040 8130A4E6577204A6572736579311430120603550407130B4A65727365792043697479311E301C060355040A1
3155468652055534552545255535420 4E6574776F726B312E302C0603550403132555534552547275737420525341204365727469666963 6174696F6E20417574686F7269747930820222300
D06092A864886F70D01010105000382020F003082020A0282020100 80126517360EC3DB08B3D0AC570D76EDCD27D34CAD508361E2AA204D092D6409DCCE899FCC3DA9ECF6CFC1DCF1D3
B1D67B3728112B47DA39C6BC3A19B45FA6BD7D9DA36342B676F2A93B2B91F8E26FD0EC162090093EE2E874C918B491D46264DB7FA306F188186A90223CBCFE13F087147BF6E41F8ED4E4
51C61167460851CB8614543FBC33FE7E6C9CFF169D18BD518E35A6A766C87267DB2166B1D49B7803C0503AE8CCF0DCBC9E4CFEAF0596351F575AB7FFCEF93DB72CB6F654DDC8E7123A4
DAE4C8AB75C9AB4B7203DCA7F2234AE7E3B68660144E7014E46539B3360F794BE5337907343F332C353EFDBAAFE744E69C76B8C6093DEC4C70CDFE132AECC933B517895678BEE3D56FE0
CD0690F1B0FF325266B336DF76E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490BDFD8808A0993628EB566CF2588CD84B8
B13FA4390FD9029EEB124C957CF36B05A95E1683CCB867E2E8139DCC5B82D34CB3ED5BFFDEE573AC233B2D00BF3555740949D849581A7F9236E651920EF3267D1C4D17BCC9EC4326D0B
F415F40A94444F499E757879E501F5754A83EFD74632FB1506509E658422E431A4CB4F0254759FA041E93D426464A5081B2DEBE78B7FC6715E1C957841E0F63D6E962BAD65F552EEA5CC6
2808042539B80E2BA9F24C971C073F0D52F5EDEF2F820F0203010001A3423040301D0603551D0E041604145379BF5AAA2B4ACF5480E1D89BC09DF2B20366CB300E0603551D0F0101FF040
403020106300F0603551D130101FF040530030101FF300D06092A864886F70D01010C050003820201005CD47C0DCFF7017D4199650C73C5529FCBF8CF99067F1BDA43159F9E0255579614F
1523C27879428ED1F3A0137A276FC5350C0849BC66B4EBA8C214FA28E556291F36915D8BC88E3C4AA0BFDEFA8E94B552A06206D55782919EE5F305C4B241155FF249A6E5E2A2BEE0B4D9
F7FF70138941495430709FB60A9EE1CAB128CA09A5EA7986A596D8B3F08FBC8D145AF18156490120F73282EC5E2244EFC58ECF0F445FE22B3EB2F8ED2D9456105C1976FA876728F8B8C36
AFBF0D05CE718DE6A66F1F6CA67162C5D8D083720CF16711890C9C134C7234DFBCD571DFAA71DDE1B96C8C3C125D65DABD5712B6436BFFE5DE4D661151CF99AEEC17B6E871918CDE49
FEDD3571A21527941CCF61E326BB6FA36725215DE6DD1D0B2E681B3B82AFEC836785D4985174B1B9998089FF7F78195C794A602E9240AE4C372A2CC9C762C80E5DF7365BCAE0252501B4
DD1A079C77003FD0DCD5EC3DD4FABB3FCC85D66F7FA92DDFB902F7F5979AB535DAC367B0874AA9289E238EFF5C276BE1B04FF307EE002ED45987CB524195EAF447D7EE6441557C8D590
295DD629DC2B9EE5A287484A59BB790C70C07DFF589367432D628C1B0B00BE09C4CC31CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7BB57088AE3E19CF4028D8FCC890
BB5D9922F552E658C51F883143EE881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD
```

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E

Operation: write **Name:** Blob

Value:

```
5C000000010000000400000000100000530000000100000043000000030413022060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C01033
0123010060A2B0601040182373C0101030200C019000000010000001000000EA6089055218053DD01E37E1D806EEDF620000000100000020000000E793C9B02FD8AA13E21C31228ACCB08
119643B749C898964B1746D46C3D4CBD214000000010000001400000005379BF5AAA2B4ACF5480E1D89BC09DF2B20366CB1D000000010000001000000885010358D29A38F059B028559C9
5F900B000000010000000100000005300650063007400690067006F000000030000000100000014000000002B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0F000000010000003000000066
B764A96581128168CF208E374DDA479D54E311F32457F4AEE0DBD2A6C8D171D531289E1CD22BFDBBD4CFD979625483090000000100000054000000305206082B0601050507030206082B0
6010505070303060A2B0601040182370A030406082B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B06010505070308040000000100000
0100000001BFE69D191B71933A372A80FE155E5B5200000000001000000E2050000308205DE308203C6A003020102021001FD6D30FCA3CA51A81BBC640E35032D300D06092A864886F70D01
010C0500308188310B3009060355040613025553311330110603550408130A4E6577204A65727365793114301206035504071308B4A65727365792043697479311E301C060355040A1315546
8652055534552545255535420E6574776F726B312E302C060355040313255553455254727573742052534120436572746966696361746696F6E20417574686F72697479301E170D313030323
0313030303030305A170D3338303131383233353935395A308188310B3009060355040613025553311330110603550408130A4E6577204A6572736579311430120603550407130B4A657273
65792043697479311E301C060355040A131554686520555345525452555354204E6574776F726B312E302C060355040313255553455254727573742052534120436572746966696361746696F
6E20417574686F7269747930820222300D06092A864886F70D01010105000382020F003082020A0282020100801265173 60EC3DB08B3D0AC570D76EDCD27D34CAD508361E2AA204D092D6
409DCCE899FCC3DA9ECF6CFC1DCF1D3B1D67B3728112B47DA39C6BC3A19B45FA6BD7D9DA36342B676F2A93B2B91F8E26FD0EC162090093EE2E874C918B491D46264DB7FA306F188186A
90223CBCFE13F087147BF6E41F8ED4E451C61167460851CB8614543FBC33FE7E6C9CFF169D18BD518E35A6A766C87267DB2166B1D49B7803C0503AE8CCF0DCBC9E4CFEAF0596351F575A
B7FFCEF93DB72CB6F654DDC8E7123A4DAE4C8AB75C9AB4B7203DCA7F2234AE7E3B68660144E7014E46539B3360F794BE5337907343F332C353EFDBAAFE744E69C76B8C6093DEC4C70CD
FE132AECC933B517895678BEE3D56FE0CD0690F1B0FF325266B336DF76E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490B
DFD8808A0993628EB566CF2588CD84B8B13FA4390FD9029EEB124C957CF36B05A95E1683CCB867E2E8139DCC5B82D34CB3ED5BFFDEE573AC233B2D00BF3555740949D849581A7F9236E6
51920EF3267D1C4D17BCC9EC4326D0BF415F40A94444F499E757879E501F5754A83EFD74632FB1506509E658422E431A4CB4F0254759FA041E93D426464A5081B2DEBE78B7FC6715E1C95
7841E0F63D6E962BAD65F552EEA5CC62808042539B80E2BA9F24C971C073F0D52F5EDEF2F820F0203010001A3423040301D0603551D0E041604145379BF5AAA2B4ACF5480E1D89BC09DF2
B20366CB300E0603551D0F0101FF040403020106300F0603551D130101FF040530030101FF300D06092A864886F70D01010C050003820201005CD47C0DCFF7017D4199650C73C5529FCBF8
CF99067F1BDA43159F9E0255579614F1523C27879428ED1F3A0137A276FC5350C0849BC66B4EBA8C214FA28E556291F36915D8BC88E3C4AA0BFDEFA8E94B552A06206D55782919EE5F305
C4B241155FF249A6E5E2A2BEE0B4D9F7FF70138941495430709FB60A9EE1CAB128CA09A5EA7986A596D8B3F08FBC8D145AF18156490120F73282EC5E2244EFC58ECF0F445FE22B3EB2F8E
D2D9456105C1976FA876728F8B8C36AFBF0D05CE718DE6A66F1F6CA67162C5D8D083720CF16711890C9C134C7234DFBCD571DFAA71DDE1B96C8C3C125D65DABD5712B6436BFFE5DE4D6
61151CF99AEEC17B6E871918CDE49FEDD3571A21527941CCF61E326BB6FA36725215DE6DD1D0B2E681B3B82AFEC836785D4985174B1B9998089FF7F78195C794A602E9240AE4C372A2CC
9C762C80E5DF7365BCAE0252501B4DD1A079C77003FD0DCD5EC3DD4FABB3FCC85D66F7FA92DDFB902F7F5979AB535DAC367B0874AA9289E238EFF5C276BE1B04FF307EE002ED45987CB
524195EAF447D7EE6441557C8D590295DD629DC2B9EE5A287484A59BB790C70C07DFF589367432D628C1B0B00BE09C4CC31CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8
F7BB57088AE3E19CF4028D8FCC890BB5D9922F552E658C51F883143EE881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD
```

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764D8E349
Operation: write
Name: Blob
Value:

```
0400000001000000100000000497904B0EB8719AC47B0BC11519B74D009000000010000005400000003052060 82B0601050507030206082B0601050507030306 0A2B0601040182370A0304060
82B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B060105050703080F0000000100000014000000 3E8E6487F8FD27D322A269A71EDAAC
5D5781128603000000010000001400000 0D1EB23A46D17D68FD92564C2F1F1601764D8E3491D000000010000001000000 02E0D6875874A44C820912E85E964CFDB1400000001000000 1400
0000A0110A233E96F107ECE2AF29EF82A57FD030A4B40B000000010000001C0000005300650063007400690067006F0020002800410041004100290000006200000001000000 20000000D7A
7A0FB5D7E2731D771E9484EBCDEF71D5F0C3E0A2948782BC83EE0EA699EF41900000000100000010000000 2AA1C05E2AE606F198C2C5E937C97AA2530000000100000043000000030413022
060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C02000000001000000360400003
08204323082031AA003020102020101300D06092A864886F70D0101050500307B310B3009060355040613024742311B301906035504080C1247726561746572204D616E636865737465723 1
10300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F204341204C696D69746564312130 1F06035504030C184141412043657274696669636174652053657 27
669636573301E170D3034303130313030303030305A170D3238313233313233353935395A307B310B3009060355040613024742311B301906035504080C1247726561746572204D616E6368
65737465723110300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F204341204C696D69746564312130 1F06035504030C1841414120436572746966696 3617
46520536572766963657330820122300D06092A864886F70D01010105000382010F003082010A0282010100BE409DF46EE1EA76871C4D45448EBE46C883069DC12AFE181F8EE402FAF3AB5
D508A16310B9A06D0C57022CD492D5463CCB66E68460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360E2DA8955F32258F3DEDCCFEF8386A28C944F9F68F29890468427C776
BFE3CC352C8B5E07646582C048B0A891F9619F762050A891C766B5EB78620356F08A1A13EA31A31EA099FD38F6F62732586F07F56BB8FB142BAFB7AACCD6635F738CDA0599A838A8CB17
783651ACE99EF4783A8DCF0FD942E2980CAB2F9F0E01DEEF9F9949F12DDFAC744D1B98B547C5E529D1F99018C7629CBE83C7267B3E8A25C7C0DD9DE6356810209D8FD8DED2C3849C0D5
EE82FC90203010001A381C03081BD301D0603551D0E04160414A0110A233E96F107ECE2AF29EF82A57FD030A4B4300E0603551D0F0101FF040403020106300F0603551D130101FF0405300
30101FF307B0603551D1F047430723038A036A0348632687474703A2F2F63726C2E636F6D6F646F63612E636F6D2F41414143657274696669636174655365727669636573 2E63726C3036A0
34A0328630687474703A2F2F63726C2E636F6D6F646F2E6E65742F414141436572746966696361746553657276696365732E63726C300D06092A864886F70D010105050003820101000856F
C02F09BE8FFA4FAD67BC64480CE4FC4C5F60058CCA6B6BC1449680476E8E6EE5DEC020F60D68D50184F264E01E3E6B0A5EEBFBC745441BFFDFC12B8C74F5AF48960057F60B7054AF3F6F
1C2BFC4B97486B62D7D6BCCD2F346DD2FC6E06AC3C334032C7D96DD5AC20EA70A99C1058BAB0C2FF35C3ACF6C37550987DE53406C58EFFCB6AB656E04F61BDC3CE05A15C69ED9F1594
8302165036CECE92173EC9B03A1E037ADA015188FFABA02CEA72CA910132CD4E50826AB229760F8905E74D4A29A53BDF2A968E0A26EC2D76CB1A30F9EBFEB68E756F2AEF2E32B383A09
81B56B85D7BE2DED3F1AB7B263E2F5622C82D46A004150F139839F95E93696986E
```

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764D8E349
Operation: write
Name: Blob
Value:

```
5C000000010000000400000000080000530000000100000043000000030413022060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C01033
0123010060A2B0601040182373C0101030200C01900000001000000100000002AA1C05E2AE606F198C2C5E937C97AA262000000010000002000000 0D7A7A0FB5D7E2731D771E9484EBCDE
F71D5F0C3E0A2948782BC83EE0EA699EF40B000000010000001C0000005300650063007400690067006F00200028004100410041002900000014000000010000001400000 0A0110A233E96F
107ECE2AF29EF82A57FD030A4B41D000000010000001000000 02E0D6875874A44C820912E85E964CFDB0300000001000000140000000D1EB23A46D17D68FD92564C2F1F1601764D8E3490F
0000000100000014000000 3E8E6487F8FD27D322A269A71EDAAC5D5781128609000000010000005400000030520608 2B0601050507030206082B0601050507030306 0A2B0601040182370A0
30406082B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B0601050507030804000000010000001000000 0497904B0EB8719AC47B0BC11
519B74D02000000010000003604000030820432308203 1AA003020102020101300D06092A864886F70D0101050500307B310B3009060355040613024742311B301906035504080C1247726
561746572204D616E636865737465723110300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F204341204C696D69746564312130 1F06035504030C18414141
20436572746966696361746520536572766963657330 1E170D3034303130313030303030305A170D3238313233313233353935395A307B310B3009060355040613024742311B301906035504
080C1247726561746572204D616E636865737465723110300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F204341204C696D69746564312130 1F060355040
30C18414141204365727469666963617465205365727669636573308201223000D06092A864886F70D01010105000382010F003082010A0282010100BE409DF46EE1EA76871C4D45448EBE46
C883069DC12AFE181F8EE402FAF3AB5D508A16310B9A06D0C57022CD492D5463CCB66E68460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360E2DA8955F32258F3DEDCCFEF8
386A28C944F9F68F29890468427C776BFE3CC352C8B5E07646582C048B0A891F9619F762050A891C766B5EB78620356F08A1A13EA31A31EA099FD38F6F62732586F07F56BB8FB142BAFB7
AACCD6635F738CDA0599A838A8CB17783651ACE99EF4783A8DCF0FD942E2980CAB2F9F0E01DEEF9F9949F12DDFAC744D1B98B547C5E529D1F99018C7629CBE83C7267B3E8A25C7C0DD9
DE6356810209D8FD8DED2C3849C0D5EE82FC90203010001A381C03081BD301D0603551D0E04160414A0110A233E96F107ECE2AF29EF82A57FD030A4B4300E0603551D0F0101FF04040302
0106300F0603551D130101FF040530030101FF307B0603551D1F047430723038A036A0348632687474703A2F2F63726C2E636F6D6F646F63612E636F6D2F414141436572746966696361746
553657276696365732E63726C3036A034A0328630687474703A2F2F63726C2E636F6D6F646F2E6E65742F414141436572746966696361746553657276696365732E63726C300D06092A8648
86F70D010105050003820101000856FC02F09BE8FFA4FAD67BC64480CE4FC4C5F60058CCA6B6BC1449680476E8E6EE5DEC020F60D68D50184F264E01E3E6B0A5EEBFBC745441BFFDFC12B
8C74F5AF48960057F60B7054AF3F6F1C2BFC4B97486B62D7D6BCCD2F346DD2FC6E06AC3C334032C7D96DD5AC20EA70A99C1058BAB0C2FF35C3ACF6C37550987DE53406C58EFFCB6AB6
56E04F61BDC3CE05A15C69ED9F15948302165036CECE92173EC9B03A1E037ADA015188FFABA02CEA72CA910132CD4E50826AB229760F8905E74D4A29A53BDF2A968E0A26EC2D76CB1A3
0F9EBFEB68E756F2AEF2E32B383A0981B56B85D7BE2DED3F1AB7B263E2F5622C82D46A004150F139839F95E93696986E
```

(PID) Process: (3400) f6ea9784e18eb238af282efa0c776cb5.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
Operation: write
Name: SysHelper
Value: 1

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	7	1	2

Dropped files

PID	Process	Filename	Type
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\SystemID\PersonalID.txt **MD5:** D621B7D1BDB5EAADA8AB3CC131CF8556 **SHA256:** AE393288708E5C402EE185DB3F3F3C9DDC6972CE0A7869639318976D921CA59B	text
3400	f6ea9784e18eb238af282efa0c	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB60	

	776cb5.exe	6228BC7A711E **MD5:** 6009A9199090F5EED5D8923CC3F777CF **SHA256:** 22A0F04B1A4DAA1FA6C30671BC876BB6490D7FCC5851B678C658042288F1D4B4	der
3072	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\Local\9d55a140-8dad-425b-878c-06c733a55f68\f6ea9784e18eb238af282efa0c776cb5.exe **MD5:** F6EA9784E18EB238AF282EFA0C776CB5 **SHA256:** 8718C3FB8AF937BC27504FF5EB70C3C0C73B6B5212B7EBDBC6FDED506595E912	executable
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PO2HN1X2\geo[1].json **MD5:** 8CC7BF1598635F18F2A22D76946C6B0F **SHA256:** C4D8435BEF59A5F7BBBFA883D18D7321F4200082AB3DEC67D2DB573BBDA06760	binary
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PO2HN1X2\get[1].htm **MD5:** 9569BDFE76709E090BF27D4DBA1A9F34 **SHA256:** 838AC74C0D0CEE7D5D914CEEE5687E9F183CFF69CA6752BD04A564E2856C9B8E	binary
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D **MD5:** F66CFA3E4D193C7D5B6D056D450F369C **SHA256:** 1957319C6951681BF7D76F79B4D0A41FBEB52CE2AF8C744E561DF68CFEBEDF55	binary
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\Local\bowsakkdestx.txt **MD5:** 9569BDFE76709E090BF27D4DBA1A9F34 **SHA256:** 838AC74C0D0CEE7D5D914CEEE5687E9F183CFF69CA6752BD04A564E2856C9B8E	binary
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** 5D6424D12CDDBB3BF102E101BD7259E5 **SHA256:** BB54F6F83BA3F899C332A1F203AD077C76CE713267F6302B0F54CE441EF88EE5	binary
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D **MD5:** A3646CE73502038670446CAE2659BBF4 **SHA256:** 4D0CF5D46B36D24BB1EA6F80F4AE0A7EA120886B7BA8E658E3945483E7F0595F	der
3400	f6ea9784e18eb238af282efa0c776cb5.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E **MD5:** 760107B361F81CAD9577FCB116DF34C2 **SHA256:** AB5AF49009CD4BB7A4C8A9FE89801567FF9DB7E2573935DCD2A10BA9050F66B6	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	8	9	16

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	200	8.241.90.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1ae242dd8cfcd23b	US	compressed	4.70 Kb	whitelisted
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	200	172.64.155.188:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D	US	der	1.42 Kb	whitelisted
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	200	172.64.155.188:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D	US	der	2.18 Kb	whitelisted
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	200	1.248.122.240:80	http://acacaca.org/test1/get.php?pid=B42FB304EAA23143BBE40F16A07AA93E&first=true	KR	binary	560 b	malicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	404	1.248.122.240:80	http://acacaca.org/files/1/build3.exe	KR	html	216 b	malicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	GET	—	211.40.39.251:80	http://rgyui.top/dl/build2.exe	KR	—	—	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3072	f6ea9784e18eb238af282efa0c776cb5.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	8.241.90.254:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	unknown
3400	f6ea9784e18eb238af282efa0c776cb5.exe	211.40.39.251:80	rgyui.top	LG DACOM Corporation	KR	malicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	172.64.155.188:80	ocsp.comodoca.com	—	US	suspicious
3400	f6ea9784e18eb238af282efa0c776cb5.exe	1.248.122.240:80	rgyui.top	SK Broadband Co Ltd	KR	malicious

DNS requests

Domain	IP	Reputation
api.2ip.ua	162.0.217.254	shared
dns.msftncsi.com	131.107.255.255	shared
ctldl.windowsupdate.com	8.241.90.254 8.248.137.254 8.248.135.254 8.248.131.254 8.253.204.121	whitelisted
ocsp.comodoca.com	172.64.155.188 104.18.32.68	whitelisted
ocsp.usertrust.com	172.64.155.188 104.18.32.68	whitelisted
rgyui.top	211.40.39.251 196.200.111.5 211.119.84.112 189.239.25.141 210.92.250.133 190.166.142.116 187.190.48.135 189.143.170.233 91.139.196.113 1.248.122.240	malicious
acacaca.org	1.248.122.240 189.153.246.166 211.40.39.251 175.119.10.231 211.171.233.129 95.107.163.44 109.102.255.230 84.224.193.200 195.158.3.162 203.91.116.53	malicious

Threats

PID	Process	Class	Message
—	—	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
—	—	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
3400	f6ea9784e18eb238af282efa0c776cb5.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)
—	—	Potentially Bad Traffic	ET DNS Query to a *.top domain - Likely Hostile
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Win32/Filecoder.STOP Variant Request for Public Key
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET CURRENT_EVENTS SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Win32/Vodkagats Loader Requesting Payload
3400	f6ea9784e18eb238af282efa0c776cb5.exe	Potentially Bad Traffic	ET INFO HTTP Request to a *.top domain
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request
3400	f6ea9784e18eb238af282efa0c776cb5.exe	A Network Trojan was detected	ET TROJAN Win32/Vodkagats Loader Requesting Payload

Debug output strings

No debug info

Interactive malware hunting service ANY.RUN