General Info

File name:	85ffa97ed23bbf42794b9350981f6a00.exe
Full analysis:	https://app.any.run/tasks/98ddcebf-fe17-4fc8-99dd-901ad050586a
Verdict:	Malicious activity
Analysis date:	August 22, 2022 at 09:37:26
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	85FFA97ED23BBF42794B9350981F6A00
SHA1:	3E6E5DF482888B3BD414ADEB97071717B1DCDBF5
SHA256:	BC705785976B2CFF0ED09ECBE684A010FB6CC10EB2136E54544E261F6E0FE0F9
SSDEEP:	24576:XVrdC6YhFNHdSCIdIucDjLyItMVYYjEgtzWXR1:XwfHQCImuIjOItMVY+Egt

---

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)
Microsoft Office Groove MUI (Russian) 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
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)	KB3161102

Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	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
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Changes the autorun value in the registry
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Drops executable file immediately after starts
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

SUSPICIOUS

Checks supported languages
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3512)
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Reads the computer name
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Executable content was dropped or overwritten
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Drops a file with a compile date too recent
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Application launched itself
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3512)

Adds / modifies Windows certificates
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

INFO

Checks supported languages
icacls.exe (PID: 2584)

Reads settings of System Certificates
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Checks Windows Trust Settings
85ffa97ed23bbf42794b9350981f6a00.exe (PID: 3732)

Reads the computer name
icacls.exe (PID: 2584)

Static information

TRiD

.exe	|	Win32 Executable MS Visual C++ (generic) (52.5)
.scr	|	Windows screen saver (22)
.dll	|	Win32 Dynamic Link Library (generic) (11)
.exe	|	Win32 Executable (generic) (7.5)
.exe	|	Generic Win/DOS Executable (3.3)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2022:01:23 19:32:54+01:00
PEType:	PE32
LinkerVersion:	9
CodeSize:	180736
InitializedDataSize:	4887552
UninitializedDataSize:	0

EntryPoint:	0xa4c0
OSVersion:	5
ImageVersion:	0
SubsystemVersion:	5
Subsystem:	Windows GUI
FileVersionNumber:	66.0.0.0
ProductVersionNumber:	71.0.0.0
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Windows NT 32-bit
ObjectFileType:	Executable application
FileSubtype:	0

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	23-Jan-2022 18:32:54
Detected languages:	Korean - Korea
Debug artifacts:	C:\surop_getu\89\hulahuginubo.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:	0x000000D8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	23-Jan-2022 18:32:54
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	0x0002C1F8	0x0002C200	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.09306
.data	0x0002E000	0x004935C8	0x00092A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.99212
.rsrc	0x004C2000	0x0000F568	0x0000F600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.16453

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.16369	1736	UNKNOWN	Korean - Korea	RT_ICON
2	5.45057	1384	UNKNOWN	Korean - Korea	RT_ICON
3	5.5073	4264	UNKNOWN	Korean - Korea	RT_ICON
4	5.61873	2440	UNKNOWN	Korean - Korea	RT_ICON
5	6.05036	1128	UNKNOWN	Korean - Korea	RT_ICON
6	6.3843	9640	UNKNOWN	Korean - Korea	RT_ICON
7	6.81021	4264	UNKNOWN	Korean - Korea	RT_ICON
8	4.27221	3752	UNKNOWN	Korean - Korea	RT_ICON
9	4.9364	2216	UNKNOWN	Korean - Korea	RT_ICON
10	5.1558	1736	UNKNOWN	Korean - Korea	RT_ICON
11	4.88179	1384	UNKNOWN	Korean - Korea	RT_ICON
12	3.05799	9640	UNKNOWN	Korean - Korea	RT_ICON
13	3.38362	4264	UNKNOWN	Korean - Korea	RT_ICON
14	3.32183	2440	UNKNOWN	Korean - Korea	RT_ICON

15	3.36124	1128	UNKNOWN	Korean - Korea	RT_ICON
16	4.09164	304	UNKNOWN	UNKNOWN	RT_CURSOR
17	2.5416	304	UNKNOWN	UNKNOWN	RT_CURSOR
18	2.50404	240	UNKNOWN	UNKNOWN	RT_CURSOR
19	1.59806	4264	UNKNOWN	UNKNOWN	RT_CURSOR
20	2.97359	2216	UNKNOWN	UNKNOWN	RT_CURSOR
26	3.01622	330	UNKNOWN	Korean - Korea	RT_STRING
27	3.13552	472	UNKNOWN	Korean - Korea	RT_STRING
28	1.854	68	UNKNOWN	Korean - Korea	RT_STRING
125	2.38706	34	UNKNOWN	Korean - Korea	RT_GROUP_ICON
128	2.91481	118	UNKNOWN	Korean - Korea	RT_GROUP_ICON
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	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
456	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
457	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
460	3.15091	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
2375	1.9815	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR

Imports

KERNEL32.dll
USER32.dll

Video and screenshots
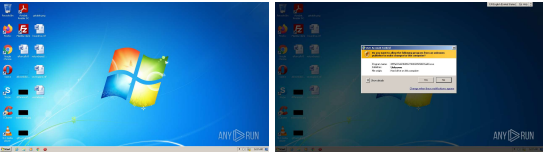
Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
42	3	2	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
3512	"C:\Users\admin\AppData\Local\Temp\85ffa97ed23bbf42794b93 50981f6a00.exe"	C:\Users\admin\AppData\Local\Temp\85ffa97ed23bbf42794b9 350981f6a00.exe	—	Explorer.EXE

Information			
User:	admin	Integrity Level:	MEDIUM
Exit code:	0		

| 3732 | "C:\Users\admin\AppData\Local\Temp\85ffa97ed23bbf42794b93 50981f6a00.exe" | C:\Users\admin\AppData\Local\Temp\85ffa97ed23bbf42794b9 350981f6a00.exe | | 85ffa97ed23bbf42794b9350981f6a00.exe |

Information			
User:	admin	Integrity Level:	MEDIUM

| 2584 | icacls "C:\Users\admin\AppData\Local\084224ab-a3aa-4574-8ed7-85b00ec513cd" /deny *S-1-1-0:(OI)(CI)(DE,DC) | C:\Windows\system32\icacls.exe | — | 85ffa97ed23bbf42794b9350981f6a00.exe |

Information			
User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Exit code:	0
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

Registry activity

Total events	Read events	Write events	Delete events
5 264	5 187	73	4

Modification events

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation:	write	Name:	ProxyEnable
Value:	0		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation:	write	Name:	SavedLegacySettings

Value: 460000003B010000090000000000000000000000000000000000004000000000000000C0E333BBEAB1D301000000000000000000000000010000000200000C0A8016400000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation:	write	Name:	CachePrefix
Value:			

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation:	write	Name:	CachePrefix
Value:	Cookie:		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation:	write	Name:	CachePrefix
Value:	Visited:		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.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:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation:	write	Name:	WpadDecisionTime
Value:	1A3106BFDCB5D801		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.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:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.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:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.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:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	1A3106BFDCB5D801		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.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:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	**Name:**	LanguageList
Value:	en-US		

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DD AB9AD8E
Operation:	write	**Name:**	Blob

Value: 040000000100000010000000100000001BFE69D191B71933A372A80FE155E5B509000000010000005400000305206082B0601050507030206082082B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B060105050703080F000000010000003000000066B764A96581128168CF208E374DDA 479D54E311F32457F4AEE0DBD2A6C8D171D531289E1CD22BFDBBD4CFD97962548303000000010000001400000002B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0B0000000100000010 00000530065006300300074006900640065007000610064080000010000000000000885010358D29A38F059B028559C95F9014000000010000001400000005379BF5AAA2B4ACF5480E1D89BC09DF2 B20366CB6200000001000000200000000E793C9B02FD8AA13E21C31228ACCB08119643B749C898964B1746D46C3D4CBD219000000010000001000000000EA6089055218053DD01E37E1D806E EDF53000000010000004300000030413022060C2B060104012310102010501301230100602B06010401823730101030200C0301B060567810C010330123010060602B06010401823730101030200C01 01030200C0200000000100000002050000308205D308203C6A003020102021001FD6D30FCA3CA51A81BBC640E35032D3002000006092A864886F70D01010105000308188310B30090603550406 130255533113301106035504081301A4E6577204A65727365793114301206035504071301B4A65727365792043697479931E301C060355040A131554686520550535545525425553542555353542042204E6574777476726B312E302C0603550403132555334552547275737420505253 41204365727246966696636174696F6E20417574686E7269747930820222300 D06092A864886F70D01010105000382020F00308202020A0282020100801265173360EC3DB08B3D0AC570D76EDCD27D34CAD508361E2AA204D092D6409DCCE899FCC3DA9ECF6CFC1DCF1D3 B1D67B3728112B47DA39C6BC3A19B45FA6BD7D9DA36342B676F2A93B2B91F8E26FD0EC162090093EE2E874C918B491D46264DB7FA306F188186A90223CBCFE13F087147BF6E41F8ED4E4 51C61167460851CB8614543FBC33FE7E6C9CFF169D18BD518E35A6A766C87267DB2166B1D49B7803C0503AE8CCF0DCBC9E4CFEAF0596351F575AB7FFCEF93DB72CB6F654DDC8E7123A4 DAE4C8AB75C9AB4B7203DCA7F2234AE7E3B68660144E7014E46539B3360F794BE5337907343F332C353EFDBAAFE744E69C76B8C6093DEC4C70CDFE132AECC933B517895678BEE3D56FE0 CD0690F1B0FF325266B336D76E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490BDFD8808A0993628EB566CF2588CD84B8 B13FA4390FD9029EEB124C957CF36B05A95E1683CCB867E2E8139DCC5B82D34CB3ED5BFFDEE573AC233B2D00BF3555740949D849581A7F9236E651920EF3267D1C4D17BCC9EC4326D0B F415F40A94444F499E757879E501F5754A83EFD74632FB1506509E658422E431A4CB4F0254759FA041E93D426464A5081B2DEBE78B7FC6715E1C957841E0F63D6E962BAD65F552EEA5CC6 2808042539B80E2BA9F24C971C073F0D52F5EDEF2F820F0203010001A3423040301D0603551D0E041604145379BF5AAA2B4ACF5480E1D89BC09DF2B20366CB300E0603551D0F0101FF040 403020106300F0603551D130101FF040530030101FF300D06092A864886F70D01010C050003820201005CD47C0DCFF7017D4199650C73C5529FCBF8CF99067F1BDA43159F9E0255579614F 1523C27879428ED1F3A0137A276FC5350C0849BC66B4EBA8C214FA28E556291F36915D8BC88E3C4AA0BFDEFA8E94B552A06206D55782919EE5F305C4B241155FF249A6E5E2A2BEE0B4D9 F7FF70138941495430709FB60A9EE1CAB128CA09A5EA7986A596D8B3F08FBC8D145AF18156490120F73282EC5E2244EFC58ECF0F445FE22B3EB2F8ED2D9456105C1976FA876728F8B8C36 AFBF0D05CE718DE6A66F1F6CA67162C5D8D083720CF16711890C9C134C7234DFBCD571DFAA71DDE1B96C8C3C125D65DABD5712B6436BFFE5DE4D661151CF99AEEC17B6E871918CDE49 FEDD3571A21527941CCF61E326BB6FA36725215DE6DD1D0B2E681B3B82AFEC836785D4985174B1B9998089FF7F78195C794A602E9240AE4C372A2CC9C762C80E5DF7365BCAE0252501B4 DD1A079C77003FD0DCD5EC3DD4FABB3FCC85D66F7FA92DDFB902F7F5979AB535DAC367B0874AA9289E238EFF5C276BE1B04FF307EE002ED45987CB524195EAF447D7EE6441557C8D590 295DD629DC2B9EE5A287484A59BB790C70C07DFF589367432D628C1B0B00BE09C4CC31CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7BB57088AE3E19CF4028D8FCC890 BB5D9922F552E658C51F883143EE881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DD AB9AD8E
Operation:	delete key	**Name:**	(default)
Value:			

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DD AB9AD8E
Operation:	write	**Name:**	Blob

Value: 5C0000000100000004000000010000009000000010000005400000305206082B0601050507030206082B0601050507030306082B0601040182370A030406082B0601050507030406082B06 01050507030606082B0601050507030706082B0601050507030106082B060105050703080F000000010000003000000066B764A96581128168CF208E374DDA479D54E311F32457F4AEE0DBD 2A6C8D171D531289E1CD22BFDBBD4CFD97962548303000000010000001400000002B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0B0000000100000010000000530065006300300074006900 67006F0000001D0000000100000014000000885010358D29A38F059B028559C95F9014000000010000001400000005379BF5AAA2B4ACF5480E1D89BC09DF2B20366CB6200000001000000200 0000000E793C9B02FD8AA13E21C31228ACCB08119643B749C898964B1746D46C3D4CBD219000000010000001000000000EA6089055218053DD01E37E1D806EEDF53000000010000004300000 030413022060C2B060104012310102010501301230100602B06010401823730101030200C0301B060567810C010330123010060602B06010401823730101030200C0201030200C0200000000100000 0E2050000308205D308203C6A003020102021001FD6D30FCA3CA51A81BBC640E35032D300E060092A864886F70D01010C0500308188310B30090603550406130255533113301106035504 08130A4E6577204A6572736579114301206035504071301B4A657273657920436974793114301207130255533113301106035504081301A4E6577204A657273657931143012060355040 1325553345525472573742025534120436572724796669636174696F6E204175747572696E6572796E0020436974793114301206035504071301B4A657273657920436974793119E301C06035504A131554686520550535545525425553542555 53542204E6574777476726B312E302C0603550403132555334552547275737420202534120436572724796669636174696F6E204175747577476F207472753009060355040681020100500382020F00308202020A0282020100801265173360EC3DB08B3D0AC570D76EDCD27D34CAD508361E2AA204D092D6409DCCE899FCC3DA9ECF6CFC1DCF1D3B1D67B3728112B47DA39C6BC 3A19B45FA6BD7D9DA36342B676F2A93B2B91F8E26FD0EC162090093EE2E874C918B491D46264DB7FA306F188186A90223CBCFE13F087147BF6E41F8ED4E451C61167460851CB8614543FB C33FE7E6C9CFF169D18BD518E35A6A766C87267DB2166B1D49B7803C0503AE8CCF0DCBC9E4CFEAF0596351F575AB7FFCEF93DB72CB6F654DDC8E7123A4DAE4C8AB75C9AB4B7203DCA7 F2234AE7E3B68660144E7014E46539B3360F794BE5337907343F332C353EFDBAAFE744E69C76B8C6093DEC4C70CDFE132AECC933B517895678BEE3D56FE0CD0690F1B0FF325266B336D7 6E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490BDFD8808A0993628EB566CF2588CD84B8B13FA4390FD9029EEB124C957 CF36B05A95E1683CCB867E2E8139DCC5B82D34CB3ED5BFFDEE573AC233B2D00BF3555740949D849581A7F9236E651920EF3267D1C4D17BCC9EC4326D0BF415F40A94444F499E757879E5 01F5754A83EFD74632FB1506509E658422E431A4CB4F0254759FA041E93D426464A5081B2DEBE78B7FC6715E1C957841E0F63D6E962BAD65F552EEA5CC62808042539B80E2BA9F24C971C 073F0D52F5EDEF2F820F0203010001A3423040301D0603551D0E041604145379BF5AAA2B4ACF5480E1D89BC09DF2B20366CB300E0603551D0F0101FF040403020106300F0603551D130101 FF040530030101FF300D06092A864886F70D01010C0500038202010D5CD47C0DCFF7017D4199650C73C5529FCBF8CF99067F1BDA43159F9E0255579614F1523C27879428ED1F3A0137A27 6FC5350C0849BC66B4EBA8C214FA28E556291F36915D8BC88E3C4AA0BFDEFA8E94B552A06206D55782919EE5F305C4B241155FF249A6E5E2A2BEE0B4D9F7FF70138941495430709FB60A9 EE1CAB128CA09A5EA7986A596D8B3F08FBC8D145AF18156490120F73282EC5E2244EFC58ECF0F445FE22B3EB2F8ED2D9456105C1976FA876728F8B8C36AFBF0D05CE718DE6A66F1F6CA6 7162C5D8D083720CF16711890C9C134C7234DFBCD571DFAA71DDE1B96C8C3C125D65DABD5712B6436BFFE5DE4D661151CF99AEEC17B6E871918CDE49FEDD3571A21527941CCF61E326B B6FA36725215DE6DD1D0B2E681B3B82AFEC836785D4985174B1B9998089FF7F78195C794A602E9240AE4C372A2CC9C762C80E5DF7365BCAE0252501B4DD1A079C77003FD0DCD5EC3DD4 FABB3FCC85D66F7FA92DDFB902F7F5979AB535DAC367B0874AA9289E238EFF5C276BE1B04FF307EE002ED45987CB524195EAF447D7EE6441557C8D590295DD629DC2B9EE5A287484A59B B790C70C07DFF589367432D628C1B0B00BE09C4CC31CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7BB57088AE3E19CF4028D8FCC890BB5D9922F552E658C51F883143E E881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764 D8E349
Operation:	write	**Name:**	Blob

Value: 040000000100000010000000100000000497904B0EB8719AC47B0BC11519B74D009000000010000005400000305206082B0601050507030206082082B0601050507030406082B0601040182370A030406 082B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B060105050703080F000000010000003E8E6487F8FD27D322A269A71EDAAC 5D578112860300000001000000140000000D1EB23A46D17D68FD92564C2F1F1601764D8E3491D00000001000000100000000E2DD6875874A44C820912E85E964CFDB14000000010000001400

0000A0110A233E96F107ECE2AF29EF82A57FD030A4B40B000000010000001C0000005300650063007400690067006F00020002800410041004100290000062000000100000020000000D7A
7A0FB5D7E2731D771E9484EBCDEF71D5F0C3E0A2948782BC83EE0EA699EF419000000100000010000002AA1C05E2AE606F198C2C5E937C97AA253000000010000004300000030413022
060C2B06010401B231010201050130123010060A2B06010401B82373C0101030200C0301B060567810C010330123010060A2B06010401B82373C0101030200C020000000001000000360400003
08204323082031AA00302010202010130D06092A864886F70D0101050500307B310B3009060355040613024742311B301906035504080C124772656174657722D04D616E6368D657374657231
10300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F4204341204C696D697465643121301F06035504030C1841414120436572746966696361746520536572
72696365573301E170D3034303130313030303030305A170D3238313233313233313233533935395A307B310B3009060355040613024742311B301906035504080C124772656174657722D04D616E6368
657374657231110300E06035504070C0753616C666F7264311A3018060355040A0C11436F6D6F646F4204341204C696D697465643121301F06035504030C1841414120436572746966696361746920
4652053656572726696365733307330820122300D06092A864886F70D01010105000382010F003082010A0282010100BE409DF46EE1EA76871C4D45448EBE46C883069DC12AFE181F8EE402FAF3AB5
D508A16310B9A06D0C57022CD492D5463CCB66E68460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360E2DA8955F32258F3DEDCCFEF8386A28C944F9F68F29890468427C776
BFE3CC352C8B5E07646582C048B0A891F9619F762050A891C766B5EB78620356F08A1A13EA31A31EA099FD38F6F62732586F07F56BB8FB142BAFB7AACCD6635F738CDA0599A838A8CB17
783651ACE99EF4783A8DCF0FD942E2980CAB2F9F0E01DEEF9F9949F12DDFAC744D1B98B547C5E529D1F99018C7629CBE83C7267B3E8A25C7C0DD9DE6356810209D8FD8DED2C3849C0D5
EE82FC90203010001A381C03081BD301D0603551D0E04160414A0110A233E96F107ECE2AF29EF82A57FD030A4B4300E0603551D0F0101FF040403020106300F0603551D130101FF0405300
30101FF307BD0603551D1F047430723038A036A03486326874747403A2F2F63726C2E636F6D6F646F63612E636F6D2F414141143657274696966696361746553657276696365732E63726C3036A0
34A0328630687474703A2F2F63726C2E636F6D6F646F63612E636F6D2F41414114365727469666696361746553657276696365732E63726C300D06092A864886F70D0101050500382010100856F
C02F09BE8FFA4FAD67BC64480CE4FC4C5F60058CCA6B6BC1449680476E8E6EE5DEC020F60D68D50184F264E01E3E6B0A5EEBFBC745441BFFDFC12B8C74F5AF48960057F60B7054AF3F6F
1C2BFC4B97486B62D7D6BCCD2F346DD2FC6E06AC3C334032C7D96DD5AC20EA70A99C1058BAB0C2FF35C3ACF6C37550987DE53406C58EFFCB6AB656E04F61BDC3CE05A15C69ED9F1594
8302165036CECE92173EC9B03A1E037ADA015188FFABA02CEA72CA910132CD4E50826AB229760F8905E74D4A29A53BDF2A968E0A26EC2D76CB1A30F9EBFEB68E756F2AEF2E32B383A09
81B56B85D7BE2DED3F1AB7B263E2F5622C82D46A004150F139839F95E93696986E

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764 D8E349
Operation:	delete key	Name:	(default)
Value:			

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\D1EB23A46D17D68FD92564C2F1F1601764 D8E349
Operation:	write	Name:	Blob

Value: 5C0000000100000004000000080000090000000010000005400000305206082B0601050507030206082B06010505070303060A2B0601040182370A030406082B0601050507030406082B06
01050507030606082B0601050507030706082B06010505070301060082B060105050703080F00000001000000140000003E8E6487F8FD27D322A269A71EDAAC5D5781128603000001000000
0140000000D1EB23A46D17D68FD92564C2F1F1601764D8E3491D00000001000000100000002E0D6875874A44C820912E85E964CFDB14000000010000001400000000A0110A233E96F107ECE2A
F29EF82A57FD030A4B40B000000010000001000000002AA1C05E2AE606F198C2C5E937C97AA25300000001000000430000030413022060C2B06010401B231010201051
0130123010060A2B06010401B82373C0101030200C0301B060567810C010330123010060A2B06010401B82373C0101030200C020000000001000003604000003082043082031020
20101300D06092A864886F70D0101050500307B310B3009060355040613024742311B301906035504080C124772656174657722D04D616E6368
657374657231110300E06035504070C0753616C
666F7264311A3018060355040A0C11436F6D6F646F4204341204C696D697465643121301F06035504030C184141412043657274696669636174652053657727696936573301E170D303430313
031303030303030305A170D3238313233313233335935395A307B310B3009060355040613024742311B301906035504080C124772656174657722D04D616E6368
122300D06092A864886F70D0101010500382010F003082010A0282010100BE409DF46EE1EA76871C4D45448EBE46C883069DC12AFE181F8EE402FAF3AB5D508A16310B9A06D0C57022CD
492D5463CCB66E68460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360E2DA8955F32258F3DEDCCFEF8386A28C944F9F68F29890468427C776BFE3CC352C8B5E07646582C048
B0A891F9619F762050A891C766B5EB78620356F08A1A13EA31A31EA099FD38F6F62732586F07F56BB8FB142BAFB7AACCD6635F738CDA0599A838A8CB17783651ACE99EF4783A8DCF0FD9
42E2980CAB2F9F0E01DEEF9F9949F12DDFAC744D1B98B547C5E529D1F99018C7629CBE83C7267B3E8A25C7C0DD9DE6356810209D8FD8DED2C3849C0D5EE82FC90203010001A381C03081
BD301D0603551D0E04160414A0110A233E96F107ECE2AF29EF82A57FD030A4B4300E0603551D0F0101FF040403020106300F0603551D130101FF040530030101FF307BD0603551D1F047430
723038A036A03486326874747403A2F2F63726C2E636F6D6F646F63612E636F6D2F41414114365727469666696361746553657276696365732E63726C3036A034A0328630687474703A2F2F637
26C2E636F6D6F646F63612E636F6D2F41414114365727469666696361746553657276696365732E63726C300D06092A864886F70D0101050500382010100856F C02F09BE8FFA4FAD67BC64480CE
4FC4C5F60058CCA6B6BC1449680476E8E6EE5DEC020F60D68D50184F264E01E3E6B0A5EEBFBC745441BFFDFC12B8C74F5AF48960057F60B7054AF3F6F1C2BFC4B97486B62D7D6BCCD2F3
46DD2FC6E06AC3C334032C7D96DD5AC20EA70A99C1058BAB0C2FF35C3ACF6C37550987DE53406C58EFFCB6AB656E04F61BDC3CE05A15C69ED9F15948302165036CECE92173EC9B03A1E
037ADA015188FFABA02CEA72CA910132CD4E50826AB229760F8905E74D4A29A53BDF2A968E0A26EC2D76CB1A30F9EBFEB68E756F2AEF2E32B383A0981B56B85D7BE2DED3F1AB7B263E2
F5622C82D46A004150F139839F95E93696986E

(PID) Process:	(3732) 85ffa97ed23bbf42794b93509 81f6a00.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation:	write	Name:	SysHelper
Value:	"C:\Users\admin\AppData\Local\084224ab-a3aa-4574-8ed7-85b00ec513cd\85ffa97ed23bbf42794b9350981f6a00.exe" --AutoStart		

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	5	0	2

Dropped files

PID	Process	Filename	Type
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB7818 21E9902850D **MD5:** 3D4C1DE1F149182348CBDC85F4801C13 **SHA256:** 094E9CB02BEBB5D8A5BFBE0E83D3C0064D0F0E3A3F4ECCE0215FDCBDA9FAB938	der
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\geo[1].json **MD5:** CD76F96502B3E0244432F94A4065BBCC **SHA256:** BD761088641FE48EDDF07F1946A69F9C599EF8864DE370497AEB74DFF4F31DDD	binary
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB6 06228BC7A711E **MD5:** 5352DDCF30966C9D336639E44529B456 **SHA256:** 4C03FE9BE0E1C1E65A2937EB0655997086536968BD0B849B31C077BEF4948C3E	binary
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** FB8B7CE32702F33B73187DB73F5D083D **SHA256:** BFBB5B5429798DD1410AFCA7DEF2DF4F9F11C83E2A4924B0349967F36814E089	binary
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\Local\084224ab-a3aa-4574-8ed7-85b00ec513cd\85ffa97ed23bbf42794b9350981f6a00.exe **MD5:** 85FFA97ED23BBF42794B9350981F6A00 **SHA256:** BC705785976B2CFF0ED09ECBE684A010FB6CC10EB2136E54544E261F6E0F0F9	executable
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB60 6228BC7A711E **MD5:** 8FDE325C0191758029AD06C16C6A173C **SHA256:** 15DA0C6D8DFD5D43C6834B944BEDE7920E440262612282F52B8F4BA878F43E24	der
3732	85ffa97ed23bbf42794b935098 1f6a00.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB78 1821E9902850D **MD5:** 8C52909441B6B5AB29073D66D32CF6B1 **SHA256:** 67A6CA65251CD787A891C2A34B5D59732924939BFD614AA135E93D7E8FC0471F	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
4	8	6	3

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3732	85ffa97ed23bbf42794b9350981f6a00.exe	GET	200	93.184.221.240:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?55a49bb65f17a958	US	compressed	4.70 Kb	whitelisted
3732	85ffa97ed23bbf42794b9350981f6a00.exe	GET	200	104.18.32.68:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rlDZssCEH1bUSa0droR23QWC7xTDac%3D	US	der	2.18 Kb	whitelisted
3732	85ffa97ed23bbf42794b9350981f6a00.exe	GET	200	104.18.32.68:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKlz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5lrdR19NsEN0xNZU%3D	US	der	1.42 Kb	whitelisted
1656	sipnotify.exe	HEAD	200	23.205.225.13:80	http://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2JgkA?v=132924875993280000	NL	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	51.124.78.146:443	–	Microsoft Corporation	GB	whitelisted
3732	85ffa97ed23bbf42794b9350981f6a00.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
3732	85ffa97ed23bbf42794b9350981f6a00.exe	104.18.32.68:80	ocsp.comodoca.com	Cloudflare Inc	US	suspicious
1656	sipnotify.exe	23.205.225.13:80	query.prod.cms.rt.microsoft.com	GTT Communications Inc.	NL	unknown
3732	85ffa97ed23bbf42794b9350981f6a00.exe	93.184.221.240:80	ctldl.windowsupdate.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
1352	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	Microsoft Corporation	GB	whitelisted

DNS requests

Domain	IP	Reputation
api.2ip.ua	162.0.217.254	shared
ctldl.windowsupdate.com	93.184.221.240	whitelisted
ocsp.comodoca.com	104.18.32.68 172.64.155.188	whitelisted
ocsp.usertrust.com	104.18.32.68 172.64.155.188	whitelisted
query.prod.cms.rt.microsoft.com	23.205.225.13	whitelisted
settings-win.data.microsoft.com	51.104.136.2	whitelisted

Threats

PID	Process	Class	Message
–	–	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
3732	85ffa97ed23bbf42794b9350981f6a00.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)

Debug output strings

No debug info