ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	adfind.exe
Full analysis:	https://app.any.run/tasks/fdefd315-167b-46e4-a5b5-75389fdcfd33
Verdict:	Malicious activity
Analysis date:	August 23, 2022 at 23:58:58
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
MD5:	FF3DAD91B266FEE1EA107A2C9964349A
SHA1:	4ACC9DDF7F23109216CA22801AC75C8FABB97019
SHA256:	79908F93DBE8E1006706D35FB44C64B278A9BD13993BC29F69ED9807F992EB6A
SSDEEP:	24576:2pT5rTZghUjrTtffaEfl8cJEOHRic5+B0hKDRiMm:2pTRZ+gxfiEGkc5+OhORiMm

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:	on	Route via Tor:	off	Autoconfirmation of UAC:	on
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)
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)

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

No malicious indicators.

SUSPICIOUS

Checks supported languages
adfind.exe (PID: 3432)
notepad++.exe (PID: 2772)

Reads the computer name
notepad++.exe (PID: 2772)

Reads Microsoft Outlook installation path
iexplore.exe (PID: 2188)

INFO

Checks supported languages
iexplore.exe (PID: 2168)
iexplore.exe (PID: 2188)

Changes internet zones settings
iexplore.exe (PID: 2168)

Reads settings of System Certificates
iexplore.exe (PID: 2168)

Checks Windows Trust Settings
iexplore.exe (PID: 2168)

Application launched itself
iexplore.exe (PID: 2168)

Reads the computer name
iexplore.exe (PID: 2168)
iexplore.exe (PID: 2188)

Reads internet explorer settings
iexplore.exe (PID: 2188)

Manual execution by user
notepad++.exe (PID: 2772)

Static information

TRiD

.exe | Win32 Executable Delphi generic (33.4)
.scr | Windows screen saver (30.8)
.dll | Win32 Dynamic Link Library (generic) (15.5)
.exe | Win32 Executable (generic) (10.6)

.exe | Generic Win/DOS Executable (4.7)

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_CUI
Compilation Date:	2012-Nov-01 01:50:38
Detected languages:	English - United States
CompanyName:	http://www.joeware.net
FileDescription:	
FileVersion:	1.47.0.2742
InternalName:	adfind
LegalCopyright:	Copyright 2001-2012 joeware.net
LegalTrademarks:	
OriginalFilename:	
ProductName:	AdFind
ProductVersion:	1.0.0.0
Comments:	
SpecialBuild:	
PrivateBuild:	

DOS Header

e_magic:	MZ
e_cblp:	80
e_cp:	2
e_crlc:	0
e_cparhdr:	4
e_minalloc:	15
e_maxalloc:	65535
e_ss:	0
e_sp:	184
e_csum:	0
e_ip:	0
e_cs:	0
e_ovno:	26
e_oemid:	0
e_oeminfo:	0
e_lfanew:	512

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
NumberofSections:	8
TimeDateStamp:	2012-Nov-01 01:50:38
PointerToSymbolTable:	0
NumberOfSymbols:	0
SizeOfOptionalHeader:	224
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_DEBUG_STRIPPED IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	4096	839680	836608	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.44912
.data	843776	421888	379392	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.0393
.tls	1265664	4096	512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	1269760	4096	512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.210826
.idata	1273856	8192	4608	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.91447
.edata	1282048	4096	512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	1.2539
.rsrc	1286144	45056	43520	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.0427
.reloc	1331200	61440	58880	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.5143

Resources

Title	Entropy	Size	Codepage	Language	Type
1	4.86203	4264	UNKNOWN	English - United States	RT_ICON
4090	2.22484	104	UNKNOWN	UNKNOWN	RT_STRING
4091	3.01073	228	UNKNOWN	UNKNOWN	RT_STRING
4092	2.80014	188	UNKNOWN	UNKNOWN	RT_STRING
4093	3.2622	812	UNKNOWN	UNKNOWN	RT_STRING
4094	3.22533	1032	UNKNOWN	UNKNOWN	RT_STRING
4095	3.24232	824	UNKNOWN	UNKNOWN	RT_STRING
4096	3.24612	880	UNKNOWN	UNKNOWN	RT_STRING

CHARTABLE	3.5072	33512	UNKNOWN	English - United States	RT_RCDATA
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	1.86096	20	UNKNOWN	English - United States	RT_GROUP_ICON
1 (#2)	3.33343	836	UNKNOWN	English - United States	RT_VERSION

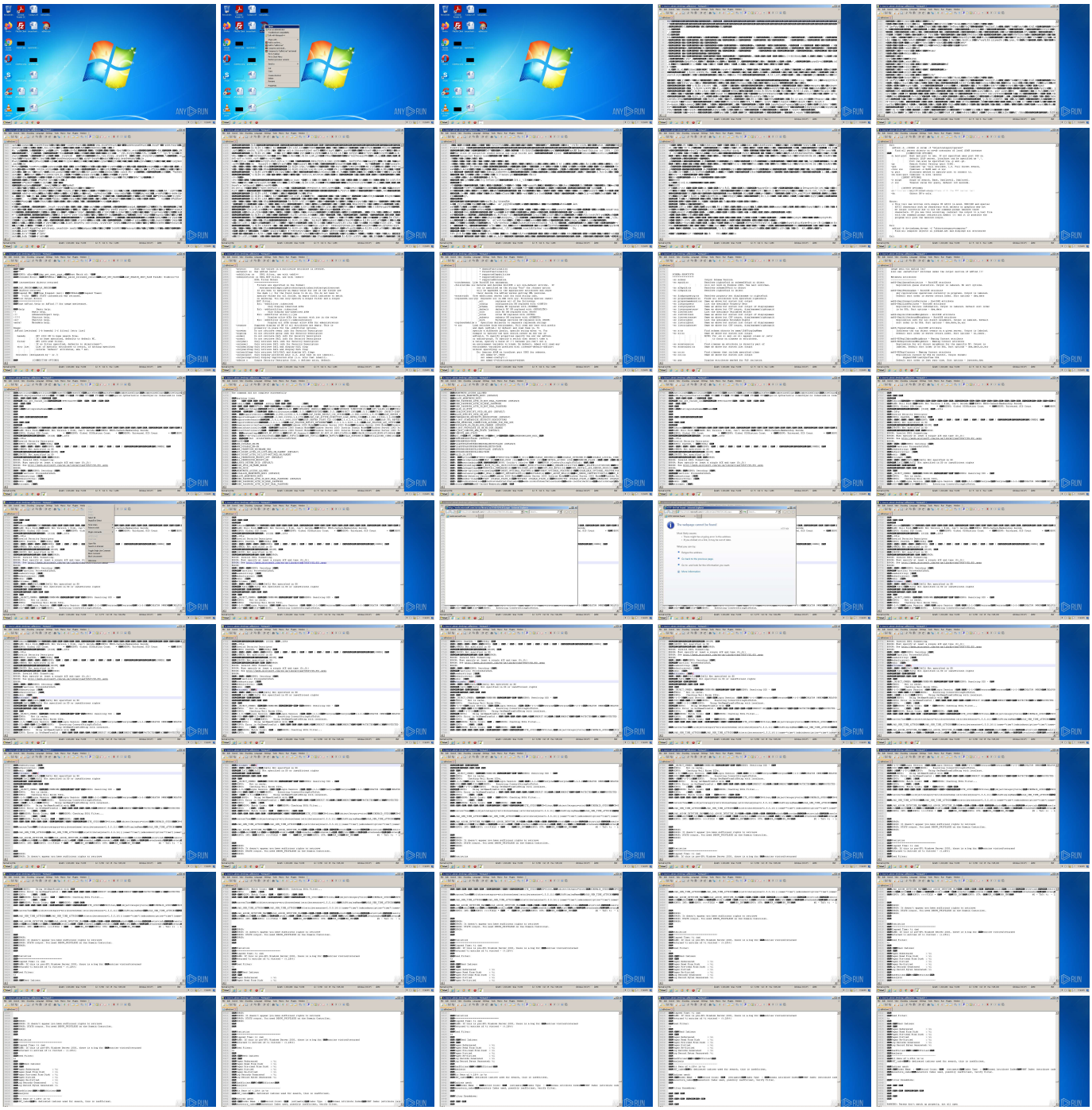
Imports

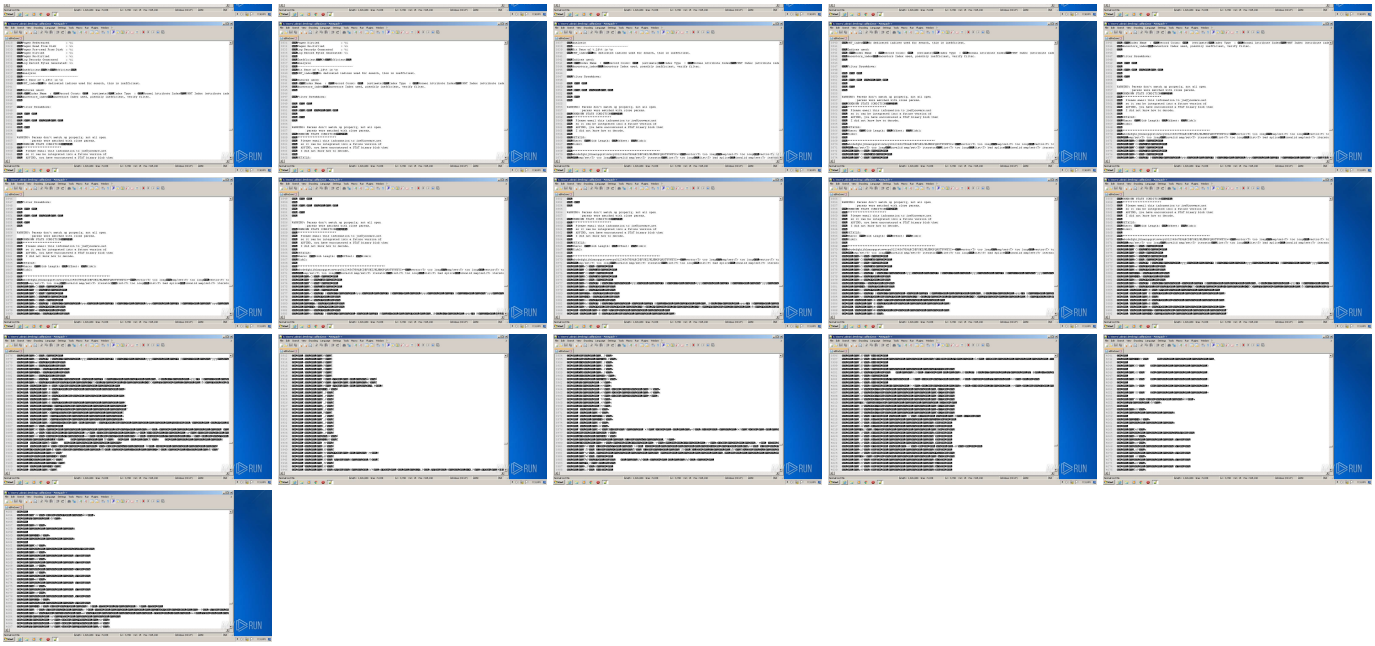
ADVAPI32.DLL
CRYPT32.DLL
KERNEL32.DLL
OLE32.DLL
OLEAUT32.DLL
USER32.DLL
WLDAP32.DLL
WSOCK32.DLL

Exports

Title	Ordinal	Address
__GetExceptDLLinfo	1	4773
___CPPdebugHook	2	843932

Video and screenshots

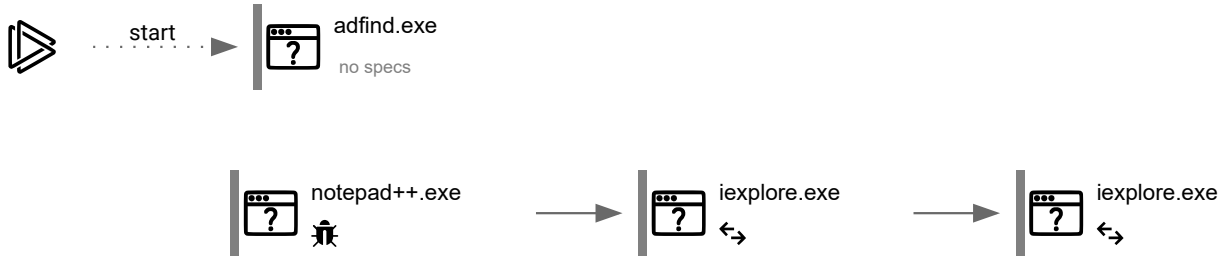




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
40	4	0	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
3432	"C:\Users\admin\Desktop\adfind.exe"	C:\Users\admin\Desktop\adfind.exe	–	Explorer.EXE

Information

User:	admin	Company:	http://www.joeware.net
Integrity Level:	MEDIUM	Exit code:	1
Version:	1.47.0.2742		

2772 "C:\Program Files\Notepad++\notepad++.exe" "C:\Users\admin\Desktop\adfind.exe" C:\Program Files\Notepad++\notepad++.exe Explorer.EXE

Information

User: admin Company: Don HO don.h@free.fr
Integrity Level: MEDIUM Description: Notepad++ : a free (GNU) source code editor
Version: 7.91

2168 "C:\Program Files\Internet Explorer\iexplore.exe" http://msdn.microsoft.com/en-us/library/aa379567(VS.85).aspx C:\Program Files\Internet Explorer\iexplore.exe notepad++.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: MEDIUM Description: Internet Explorer
Version: 11.00.9600.16428 (winblue_gdr.131013-1700)

2188 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2168 CREDAT:267521 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe iexplore.exe

Information

User: admin Company: Microsoft Corporation
Integrity Level: LOW Description: Internet Explorer
Version: 11.00.9600.16428 (winblue_gdr.131013-1700)

Registry activity

Total events	Read events	Write events	Delete events
8 110	7 982	127	1

Modification events

(PID) Process: (2772) notepad++.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPDaysSinceLastAutoMigration
Value: 1

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPLastLaunchLowDateTime
Value:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPLastLaunchHighDateTime
Value: 30979870

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation: write **Name:** NextCheckForUpdateLowDateTime
Value:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation: write **Name:** NextCheckForUpdateHighDateTime
Value: 30979870

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B010000090000000000000000000000000000000400000000000000C0E333BBEAB1D3010000000000000000000000000000000001000000020000000C0A801640000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\Active
Operation: write **Name:** {9EB67AEF-2311-11ED-8C90-12A9866C77DE}
Value: 0

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: C23B37611EB7D801

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C0000000000000001000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF20000000200000004003000078020000

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** Active
Value: 0

(PID) Process: (2188) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2188) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2188) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\LowCache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Type
Value: 10

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Count
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120 01E000B001F03

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Type
Value: 3

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count

Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120001E000B001F03

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Type
Value: 3

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120001E000B001F03

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Type
Value: 3

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 25

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120001E000B001F03

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 25

(PID) Process: (2168) iexplore.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: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 244D69611EB7D801

(PID) Process: (2168) iexplore.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: (2168) iexplore.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: (2168) iexplore.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: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 244D69611EB7D801

(PID) Process: (2168) iexplore.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: (2168) iexplore.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: (2168) iexplore.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: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{00021493-0000-0000-C000-000000000046}\Enum

Operation: write **Name:** Implementing

Value: 1C00000001000000E607080002001700120012001E000F001C0101000000644EA2EF78B0D01189E400C04FC9E26E

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{00021494-0000-0000-C000-000000000046}\Enum

Operation: write **Name:** Implementing

Value: 1C00000001000000E607080002001700120012001E000F009C0300000000

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\EUPP Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy\DSP

Operation: write **Name:** BackupDefaultSearchScope

Value: 00000000A60700005391AB6BCAF6B6036162ED727DB6B0DC060CE520A456BE98FBD292C8F64A3001FB1EBC0BD2ED66664D9D3BEEA83AAF425F5EF123190079B456F6A3BB17804540C19D744EB411F1CC1B51D3AC4BBF2BC378F1E5BEDFE6CCA4E062196B47DB106765AD310D81826A6E1D1E88B56CF8B2417F650B55762A7E0BC2B76988B57A80A7CAED7EEEC7600EB232A4F4CD8206517A935AA196FCEA0A3C7496E9F9887F619EDDFFE922B7CBBCEAD9824E4ECA09747CF7705D04644869A0F29D9BBBFD09C1B74882E93BFEE3CCD9D45A3C8B848221177F347D98EDF629DE2246E2B4F4C3862E62315CB0C10C9580DEFCA86C8E46F93D76B80C5405C5A44F4BEA778B6602C66A5BD5ABF9C639B3805C27541C2B71168B52AB966F79F4E26DB94E98B03F604E14C48F0072A6A7A002DFCF87FC37929C08A1693722E0D60DD5204D57D7BD2E2C3B78B76023D7F8612A418F4824819D5B847FAAE45DA8CAEB63BAC09773C55E56A38E78E79C94CDF3DD62809A03DCB3612A9C2AA6C52EB5ABFDE49275E83592DC3DA47D7A95F17A5D8E32CD7FDBCCE6C34E986279F4B5983D6FAFDCD957790D995FBFDF04B745DF874DA45FEF868559830B867C637E4AB485FA6689DA68AFA0BE12CEC7BBBAC72F87DBD7C1E1E53ECD8838B4A2568BB6DCBA6FF0A355D64E1E27A664517E14527C5BA5E9AD6BE73B84D893A24E57E1EC32AD3AEA236D462337E618FBA630C83247FB10780C88EAB731813E8F3A62B410887B5337641ECA955FFD44F320136350146F0F0FD93D25F7A575E43CC08D98BE300930890F4C6BFE0841037239013485A3AD688C1D70D9CD42B1E0FF8AB12F149B7E0917EF1EBBDCA2F9F2DA5AF83694C7BE890F2341DCDC3B4D5039A2F645CB4CAB0DC19D6E60B011FDF3C080059B80F294101F74A67045C1320F74235F228235B4A34A44483B14B7479A07822B6873B64A0C440B92ECD13664E5D1D5B7DAFA5887E7D2DDCAA33264E882B8CB42133374C25401C21D99990CE79104742E9DE7873D168CA3C3C039DCC7F015A58030182015AA93D2295B10C6C3E70EB8A8EE7963ADC743E06E479E710E29264AD5312E8A3B6314B5CF1BC7A5E2FCFA8D326F641FFABBC1CD8DF6B2A39B6F7D352D567E352AFFE766F67DAF9C5EE2C9DBDABFB9EE058998453D1434D6754931EE952F3E92E9DEF96FABA44ADC153423AE95D8B1BFF49103B1860B280B929056411585BA8457913A929F9F896173F6E076F59AC1557B3A1781C59EEB9651C672D069FB0AFFEDBAD0F4FD755174F9189D678201438E7372A36DFC4678084EF5167493D7B7C5100599DAB47BB2DE7443CBE130BA4338094187EE5B01906FD0C129662E7E73C8E06979FD64DA1A7505D0CBCC9FB3A0FB5B17279B83900C60F74414CED9DB2AAF7D882A00ADC7C53FCA7FA9BC6FA00D6F8BE7F87C15F4E4B5E2ACF321360F7DA2070BE90A2FC3C1B2E4FC0148413B4DE3B778D0F0AF6C3BD6B3D570A8E34F3DF49E3CE52E8ADB86897353471EB30D7D3601870521F3C1FF608990DFD782AE00AA6209901A5E731E5398C1482066F66EDC87B861E77F9D190684D1BA24B2CCC7CD730DB3784B78D81E71461117FA2513376BE1E08AF4922B95C302608112B4AA82F1D65960F1EF91D91F1212DA0FADF4BDCBD0413AF3F7DCF168312CB64491A097FC88859FEF0D8C94C219A2A045AAC170C9E1668E1AFEB9CD92BDDA0AE74B4FB4B464BE81E7C6D4627B0BC7943C03E88B83C786180B70A34861CD3AEB9A1EEC023A4062C9786837FC68205530956F3E071B2E2CF864ABCC72F59636FDFF093724AC16D4CA42FBC8FBAA775834EE83BD82AF570898C64D49A86D572604B53C70672B7773FFE5EFFB216279D31CE8E74F1761DA9002D21A2CF4EBB771915B497469D7B75F53015A4705AE31CBFC23BFA38A4FEC70B2268036098E648AEC9367DB43D0A7183836EE5D8AAF99A4DE3F8E1EF19B06CB5564CD155876172A48FCF22B4F36D3E028242DF28C85E4CF8EDC18D27A647A4AE42A8B308AC255EDAC35401D5729E4F84A6B6E1148512FC3749B5E88F3C9E6FD731AB108B7943F32E6E0EBEA5DC9A1A561AB9703A231644B521AF7DC6AEC6C1006D24827C00BB451429C3CB42A36640DC0835ECAA546D92465FA5069C3EB3B42A5F3CC9A3F4705209B08A3F32390C2D98D95131E69B149EAC1DB53FF7CE8F93F041E77075D6850C52FC6EAFC01F704B6BD80060D6190C650EA5DE9F186018DBCB7F115446C8DF6DC6075A890068BA094C6E4321CD6048DB18B2035715A580567600E768AF4D8F2EFBBB4FF80266CBFC8E9611AFFB02D35EC90C4D2F4A70B0EA93D131C32076816343E253C6009BA00EDEA97E3E05B2C258D53EAEAB4073CC736ADA17C054A5D0CA57E671E485295DE9F15262C35101FE14D3D302836A4095D6F1259271772D7A165AA19D8A81F1D650609AE2626D32700DFA53702E53694348EDDD99739F2F5157544DD712BED72DD2950CF55846F654108F09FF4BD89FBB4AC65C366F8F3D920B47E529EA5ECB46F1F492906503AF75E11E8080C0822605E9017B50C2611A2CA398617961DA2038CFC355CA7D1AAFE2F8083121F2398E1E74B9450EAFF4770C6F55ECE1FD9F67F92A59B07983A919A4425705EE35E03A0F0AF3A35DDD4896282A76E166483D9486462BECC70E340EC9777538AE8E370BC968CDD02324B969A6023DC8E2C5CDE7E2D45A44AD80900126D431C371AB2E154C9C16D59222B193758E12FD8B57DB241010000000E000000385835324E41646D516B41253364020000000000000

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\User Preferences

Operation: write **Name:** 88D7D0879DAB32E14DE5B3A805A34F98AFF34F5977

Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB010000002EE5C68BCE5CD846A6FEA2CAF34BE0620000000002000000000010660000000100002000000008D4C5554445239 38BA4F86F9191FB43AE8C53BCD00E5DEA81E7A493668CEE4CA000000000E80000000020000020000000016EF49EACDDF0161A3F1B93600F9CEE2BFD750AAD64727C07DE812B896F37C6150000000DFFF9194CD999C420419EA9A2D836BCDCCEC2C34CF2136553C0CF6085A84E138F5F88B3EFBC43588D5E9925A5C757CFCF70F2DBBA7260225AE075AAEE63792DB559371F256EC672A47BF975C9AD4E58E40000000A59BADFF2942AE56015CEFB49500184DA64FE1146D8F40592A1A9B97C8857A74EAB95C044A6495109972B4FA6F2C5043D227616A2D5EFF938AB9E6F1A8894044

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\EUPP Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy\DSP

Operation: write **Name:** ChangeNotice

Value: 0

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\User Preferences

Operation: write **Name:** 2D53CFFC5C1A3DD2E97B7979AC2A92BD59BC839E81

Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB010000002EE5C68BCE5CD846A6FEA2CAF34BE0620000000002000000000010660000000100002000000090091E331D849D1B440281D0558BF998FE12BD634AE838D82736FED041D153A4000000000E80000000020000020000000DBA96C342ECD7BC8B6D1131204091DB064D23E5CFA7B98322B406902F71BCB2310000000016F6A5842C2ECEA1005EB2233C749EF340000000F530CEE7E65A6AC585FFB74E35CF0863BF2EEC9E5BE9815B89163C30F4986A3858226C82AAEC915BBB09FDBE57DCA6344EA3E78DC08CE47AD39A9763636E0EF7

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Count

Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Time

Value: E607080002001700120012001E001100D102

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Blocked

Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Count

Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Time

Value: E607080002001700120012001E001100D102

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Blocked

Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore

Operation: write **Name:** Count
Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120001E001100D102

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E607080002001700120001E001100D102

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 26

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage
Operation: write **Name:** DecayDateQueue
Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB010000002EE5C68BCE5CD846A6FEA2CAF34BE062000000000200000000001066000000010000200000000C3534EE42778E47777E3BAEBC4A4D59552744869E77A568FE17866130515E334000000000E8000000002000020000000097AFB65E172898C550612A171C3A0F5BAFD33CC0A812551DB726D3FCCDB16AD720000000D0A2C358F51C2747BABF70C66DE7D2A65D408F4920DDC78DA69232635CDAB8AD4000000008F51E6ABA2A279BDD548C6D8CC6D3231AC398CDA9EC86E02F12BE9757030F62D6829C32D46DAC1944BE61AD1B841DB002320546B602F1AD70F0A697B308A075

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage
Operation: write **Name:** LastProcessed
Value: D01546D526B7D801

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation: write **Name:** NextCheckForUpdateHighDateTime
Value: 30979920

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\DomainSuggestion
Operation: write **Name:** NextUpdateDate
Value: 367441276

(PID) Process: (2168) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NextNTPConfigUpdateDate
Value: 367441445

Files activity

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

Dropped files

PID	Process	Filename	Type
2168	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{9EB67AF2-2311-11ED-8C90-12A9866C77DE}.dat **MD5:** 36FFD9C9A09665BC9EE0924D3DBEBFAF **SHA256:** 7BBA8EFADD1957C492805C2050F7415D4EE7B0B85D5321407873F8AB062B1127	binary
2168	iexplore.exe	C:\Users\admin\AppData\Local\Temp\~DF877959FDE6700C3D.TMP **MD5:** 277B006795F4C69437130A469E53C745 **SHA256:** 4EAB3CCA77217848F481E0885ED45B33D60F8264B506D4E89EBEF72E4EFEB7CD	gmc

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
7	17	13	9

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2188	iexplore.exe	GET	404	13.107.213.44:80	http://msdn.microsoft.com/en-us/library/aa379567(VS.85).aspx	US	xml	341 b	whitelisted
2168	iexplore.exe	GET	404	8.248.141.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/stati	US		341 b	

					c/trustedr/en/disallowedcertstl.cab?34d7f80edf0b880e		xml		whitelisted
2168	iexplore.exe	GET	404	8.248.141.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?02cbe5b945eb06d9	US	xml	341 b	whitelisted
2168	iexplore.exe	GET	404	8.241.78.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8ea091aab4154a9b	US	xml	341 b	whitelisted
2168	iexplore.exe	GET	404	8.241.78.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f470e3946b7d7b86	US	xml	341 b	whitelisted
384	svchost.exe	GET	404	8.241.78.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?764ebe3052156e9e	US	xml	341 b	whitelisted
2168	iexplore.exe	GET	404	8.241.78.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d85e4e17f8dc0a91	US	xml	341 b	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2168	iexplore.exe	204.79.197.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2168	iexplore.exe	8.248.141.254:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	suspicious
2188	iexplore.exe	13.107.213.44:80	msdn.microsoft.com	Microsoft Corporation	US	suspicious
2168	iexplore.exe	152.199.19.161:443	iecvlist.microsoft.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2168	iexplore.exe	8.241.78.126:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	suspicious
2168	iexplore.exe	96.16.143.41:443	go.microsoft.com	Akamai International B.V.	US	malicious
384	svchost.exe	8.241.78.126:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	suspicious

DNS requests

Domain	IP	Reputation
msdn.microsoft.com	13.107.246.44 13.107.213.44	whitelisted
api.bing.com	13.107.5.80	whitelisted
www.bing.com	204.79.197.200 13.107.21.200	whitelisted
ctldl.windowsupdate.com	8.248.141.254 8.248.135.254 8.238.28.254 8.241.80.126 67.27.235.254 8.241.78.126 67.27.235.126 8.253.95.249	whitelisted
iecvlist.microsoft.com	152.199.19.161	whitelisted
r20swj13mr.microsoft.com	152.199.19.161	whitelisted
ieonline.microsoft.com	204.79.197.200	whitelisted
go.microsoft.com	96.16.143.41	whitelisted

Threats

Found threats are available for the paid subscriptions

Debug output strings

Process	Message
notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\SciLexer.dll
notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
notepad++.exe	ED255D9151912E40DF048A56288E969A8D0DAFA3
notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\updater\gup.exe
notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
notepad++.exe	ED255D9151912E40DF048A56288E969A8D0DAFA3

notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\plugins\Config\nppPluginList.dll
notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
notepad++.exe	ED255D9151912E40DF048A56288E969A8D0DAFA3
notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\updater\gup.exe
notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
notepad++.exe	ED255D9151912E40DF048A56288E969A8D0DAFA3