ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9
Full analysis:	https://app.any.run/tasks/f8f2c37f-c661-4154-bba6-d707cdb01759
Verdict:	Malicious activity
Threats:	**Raccoon** Raccoon is an info stealer type malware available as a Malware as a Service. It can be obtained for a subscription and costs $200 per month. Raccoon malware has already infected over 100,000 devices and became one of the most mentioned viruses on the underground forums in 2019. **RedLine** RedLine Stealer is a malicious program that collects users' confidential data from browsers, systems, and installed software. It also infects operating systems with other malware.
Analysis date:	August 24, 2022 at 19:44:53
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	installer evasion trojan raccoon recordbreaker rat redline loader stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	1D1C4639EC7BD10BADD41968BC0FF797
SHA1:	AB1146F9AC9BBE1580BE4F16C1548A2600075BA9
SHA256:	BDBD5A0FB6A3AB99F0CFA3CEE7E3F7F8F7EC078EEB628AADFB8A32A5DF2BE3B9
SSDEEP:	49152:pAI+FNpJc7YrEa2u2h9swu+AU3Z9CcVL2wD+aRpXPaAt1DD4VR+Wg:pAI+/c8rHJ2jHxZYOTDrRxaAt1DEVwWg

Software environment set and analysis options

Launch configuration

Task duration:	60 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:**	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)

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

Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)	KB2667402
Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)	KB2676562
Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)	KB2685811
Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2685939
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)	KB2690533
Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292

Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972
Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461
Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071

Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3150220
KB3150513
KB3155178
KB3156016
KB3159398
KB3161102
KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

Drops executable file immediately after starts
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)
F0gel.exe (PID: 292)
real.exe (PID: 2484)

Application was dropped or rewritten from another process
kukurzka9000.exe (PID: 2364)
safert44.exe (PID: 2628)
me.exe (PID: 3240)
brokerius.exe (PID: 3060)
F0gel.exe (PID: 292)
namdoitntn.exe (PID: 2452)
jshainx.exe (PID: 2640)
real.exe (PID: 2484)
ordo_sec666.exe (PID: 2524)

RACCOON was detected
F0gel.exe (PID: 292)

Connects to CnC server
F0gel.exe (PID: 292)
namdoitntn.exe (PID: 2452)
safert44.exe (PID: 2628)
jshainx.exe (PID: 2640)

REDLINE was detected
safert44.exe (PID: 2628)

SUSPICIOUS

Checks supported languages
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)
F0gel.exe (PID: 292)
jshainx.exe (PID: 2640)
me.exe (PID: 3240)
kukurzka9000.exe (PID: 2364)
safert44.exe (PID: 2628)
real.exe (PID: 2484)
namdoitntn.exe (PID: 2452)
brokerius.exe (PID: 3060)
ordo_sec666.exe (PID: 2524)

Reads the computer name
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)
safert44.exe (PID: 2628)
real.exe (PID: 2484)
me.exe (PID: 3240)
jshainx.exe (PID: 2640)
namdoitntn.exe (PID: 2452)
brokerius.exe (PID: 3060)
F0gel.exe (PID: 292)

Creates files in the program directory
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)

INFO

Reads the computer name
iexplore.exe (PID: 2100)
iexplore.exe (PID: 2312)
iexplore.exe (PID: 2940)
iexplore.exe (PID: 2172)
iexplore.exe (PID: 2652)
iexplore.exe (PID: 3452)
iexplore.exe (PID: 2340)
iexplore.exe (PID: 1636)
iexplore.exe (PID: 3616)
iexplore.exe (PID: 1904)
iexplore.exe (PID: 3316)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 3612)
iexplore.exe (PID: 2708)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 488)

Checks supported languages
iexplore.exe (PID: 2652)
iexplore.exe (PID: 2100)
iexplore.exe (PID: 2312)
iexplore.exe (PID: 2172)
iexplore.exe (PID: 2940)
iexplore.exe (PID: 3452)
iexplore.exe (PID: 1636)

jshainx.exe (PID: 2640)
namdoitntn.exe (PID: 2452)

Steals credentials from Web Browsers
F0gel.exe (PID: 292)

Actions looks like stealing of personal data
F0gel.exe (PID: 292)

Stealing of credential data
real.exe (PID: 2484)
F0gel.exe (PID: 292)

Creates a directory in Program Files
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)

Creates a software uninstall entry
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)

Executable content was dropped or overwritten
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)
F0gel.exe (PID: 292)
real.exe (PID: 2484)

Drops a file with a compile date too recent
bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe (PID: 1584)
F0gel.exe (PID: 292)
real.exe (PID: 2484)

Reads Microsoft Outlook installation path
iexplore.exe (PID: 3616)
iexplore.exe (PID: 488)
iexplore.exe (PID: 2708)
iexplore.exe (PID: 3612)
iexplore.exe (PID: 1904)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 3316)

Checks for external IP
iexplore.exe (PID: 3616)
iexplore.exe (PID: 3316)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 488)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 3612)

Reads Environment values
F0gel.exe (PID: 292)
namdoitntn.exe (PID: 2452)
safert44.exe (PID: 2628)

Searches for installed software
F0gel.exe (PID: 292)

iexplore.exe (PID: 2340)
iexplore.exe (PID: 3616)
iexplore.exe (PID: 1904)
iexplore.exe (PID: 2708)
iexplore.exe (PID: 3316)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 3612)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 488)

Changes internet zones settings
iexplore.exe (PID: 2100)
iexplore.exe (PID: 2172)
iexplore.exe (PID: 3452)
iexplore.exe (PID: 2340)
iexplore.exe (PID: 2312)
iexplore.exe (PID: 2940)
iexplore.exe (PID: 1636)
iexplore.exe (PID: 2652)

Reads settings of System Certificates
real.exe (PID: 2484)
iexplore.exe (PID: 3616)
iexplore.exe (PID: 3316)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 2312)

Checks Windows Trust Settings
real.exe (PID: 2484)
iexplore.exe (PID: 3616)
iexplore.exe (PID: 3316)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 2312)

Application launched itself
iexplore.exe (PID: 2312)
iexplore.exe (PID: 2940)
iexplore.exe (PID: 2340)
iexplore.exe (PID: 2172)
iexplore.exe (PID: 3452)
iexplore.exe (PID: 2100)
iexplore.exe (PID: 2652)
iexplore.exe (PID: 1636)

Changes settings of System certificates
iexplore.exe (PID: 3616)

Dropped object may contain Bitcoin addresses
F0gel.exe (PID: 292)

Adds / modifies Windows certificates
iexplore.exe (PID: 3616)

Reads internet explorer settings
iexplore.exe (PID: 3616)
iexplore.exe (PID: 1080)
iexplore.exe (PID: 2044)
iexplore.exe (PID: 3316)

Static information

TRiD

.exe | InstallShield setup (49.2)
.exe | Win32 Executable Delphi generic (16.2)
.scr | Windows screen saver (14.9)
.dll | Win32 Dynamic Link Library (generic) (7.5)
.exe | Win32 Executable (generic) (5.1)

EXIF

EXE

LegalCopyright:	Company
FileVersion:	1.00
FileDescription:	NewProduct 1.00 Installation
CompanyName:	Company
Comments:	
CharacterSet:	Windows, Latin1
LanguageCode:	English (U.S.)
FileSubtype:	0
ObjectFileType:	Executable application
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	0.0.0.0
FileVersionNumber:	1.0.0.0
Subsystem:	Windows GUI

SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x25468
UninitializedDataSize:	0
InitializedDataSize:	31744
CodeSize:	148992
LinkerVersion:	2.25
PEType:	PE32
TimeStamp:	1992:06:20 00:22:17+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	19-Jun-1992 22:22:17
Detected languages:	English - United States
	Russian - Russia
Comments:	
CompanyName:	Company
FileDescription:	NewProduct 1.00 Installation
FileVersion:	1.00
LegalCopyright:	Company

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0050
Pages in file:	0x0002
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x000F
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x001A
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000100

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	8
Time date stamp:	19-Jun-1992 22:22:17
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_BYTES_REVERSED_HI
	IMAGE_FILE_BYTES_REVERSED_LO
	IMAGE_FILE_EXECUTABLE_IMAGE
	IMAGE_FILE_LINE_NUMS_STRIPPED
	IMAGE_FILE_LOCAL_SYMS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
CODE	0x00001000	0x000244CC	0x00024600	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.59443
DATA	0x00026000	0x00002894	0x00002A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	3.79376
BSS	0x00029000	0x000010F5	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x0002B000	0x00001798	0x00001800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.88555
.tls	0x0002D000	0x00000008	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x0002E000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.204488
.reloc	0x0002F000	0x00001884	0x00001A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.58665
.rsrc	0x00031000	0x00001CDC	0x00001E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	4.75165

Resources

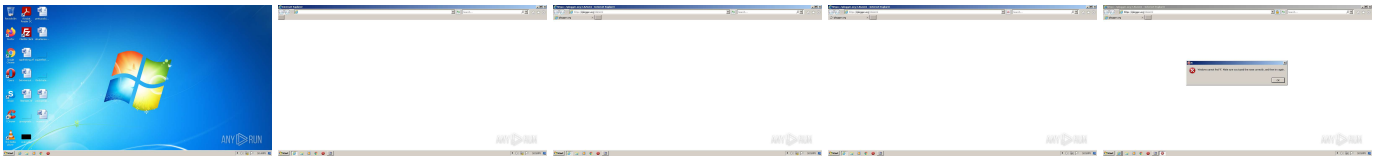
Title	Entropy	Size	Codepage	Language	Type
1	4.93923	886	UNKNOWN	Russian - Russia	RT_MANIFEST
50	3.25755	296	UNKNOWN	UNKNOWN	RT_ICON
51	4.01345	1384	UNKNOWN	UNKNOWN	RT_ICON
52	3.92897	744	UNKNOWN	UNKNOWN	RT_ICON
53	4.27475	2216	UNKNOWN	UNKNOWN	RT_ICON
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA

PACKAGEINFO	5.28362	272	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.57938	62	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

advapi32.dll
cabinet.dll
comctl32.dll
gdi32.dll
kernel32.dll
ole32.dll
oleaut32.dll
shell32.dll
user32.dll
winmm.dll

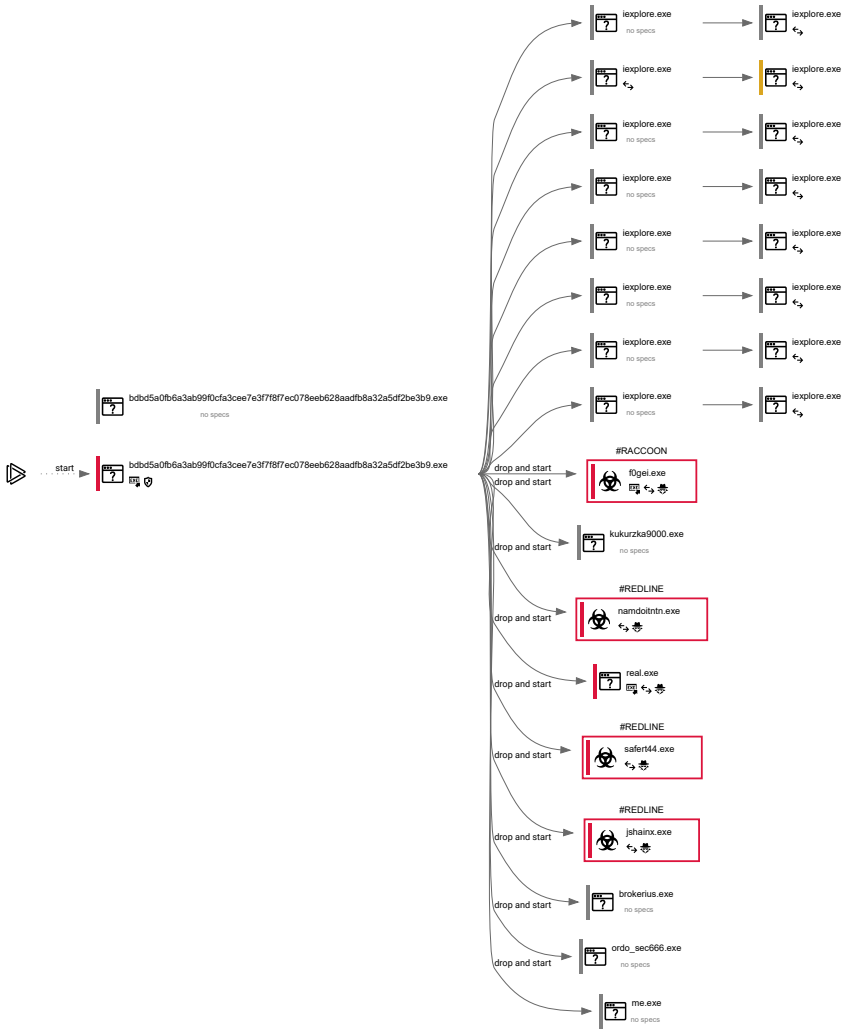
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
69	27	6	1

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
3248	"C:\Users\admin\AppData\Local\Temp\bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe"	C:\Users\admin\AppData\Local\Temp\bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	—	Explorer.EXE

Information

User:	admin	**Company:**	Company
Integrity Level:	MEDIUM	**Description:**	NewProduct 1.00 Installation
Exit code:	3221226540	**Version:**	1.00

1584	"C:\Users\admin\AppData\Local\Temp\bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe"	C:\Users\admin\AppData\Local\Temp\bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe		Explorer.EXE

Information

User:	admin	**Company:**	Company
Integrity Level:	HIGH	**Description:**	NewProduct 1.00 Installation
Exit code:	0	**Version:**	1.00

2100	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1ARmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

2312	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AAmX4	C:\Program Files\Internet Explorer\iexplore.exe		bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

2172	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AFmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

2652	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AGmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

2940	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AJmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

3452	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AKmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

2340	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AZmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

1636	"C:\Program Files\Internet Explorer\iexplore.exe" https://iplogger.org/1AVmX4	C:\Program Files\Internet Explorer\iexplore.exe	–	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

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

292	"C:\Program Files\Company\NewProduct\F0gel.exe"	C:\Program Files\Company\NewProduct\F0gel.exe		bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User:	admin	**Integrity Level:**	HIGH

2364 "C:\Program Files\Company\NewProduct\kukurzka9000.exe" C:\Program Files\Company\NewProduct\kukurzka9000.exe – bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH
Exit code: 2

2452 "C:\Program Files\Company\NewProduct\namdoitntn.exe" C:\Program Files\Company\NewProduct\namdoitntn.exe bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH
Description: Version: 0.0.0.0

2484 "C:\Program Files\Company\NewProduct\real.exe" C:\Program Files\Company\NewProduct\real.exe bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH

2628 "C:\Program Files\Company\NewProduct\safert44.exe" C:\Program Files\Company\NewProduct\safert44.exe bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH
Description: Version: 0.0.0.0

2640 "C:\Program Files\Company\NewProduct\jshainx.exe" C:\Program Files\Company\NewProduct\jshainx.exe bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH
Description: Version: 0.0.0.0

3060 "C:\Program Files\Company\NewProduct\brokerius.exe" C:\Program Files\Company\NewProduct\brokerius.exe – bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH

2524 "C:\Program Files\Company\NewProduct\ordo_sec666.exe" C:\Program Files\Company\NewProduct\ordo_sec666.exe – bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH

3240 "C:\Program Files\Company\NewProduct\me.exe" C:\Program Files\Company\NewProduct\me.exe – bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe

Information

User: admin Integrity Level: HIGH

3616 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2312 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe iexplore.exe

Information

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

1904 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2940 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe iexplore.exe

Information

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

2708 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2340 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe iexplore.exe

Information

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

3316 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2100 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe iexplore.exe

Information

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

2044 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2172 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe ↔ iexplore.exe

Information

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

3612 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3452 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe ↔ iexplore.exe

Information

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

1080 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2652 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe ↔ iexplore.exe

Information

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

488 "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1636 CREDAT:275457 /prefetch:2 C:\Program Files\Internet Explorer\iexplore.exe ↔ iexplore.exe

Information

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

Registry activity

Total events	Read events	Write events	Delete events
38 094	37 203	878	13

Modification events

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	DisplayName
Value:	NewProduct 1.00		

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	DisplayVersion
Value:	1.00		

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	VersionMajor
Value:	1		

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	VersionMinor
Value:	0		

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	Publisher
Value:	Company		

(PID) Process:	(1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation:	write	**Name:**	DisplayIcon
Value:	C:\Program Files\Company\NewProduct\Uninstall.exe		

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** UninstallString
Value: C:\Program Files\Company\NewProduct\Uninstall.exe

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** URLInfoAbout
Value: http://www.company.com/

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** HelpLink
Value: mailto:support@company.com

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** InstallLocation
Value: C:\Program Files\Company\NewProduct\

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** InstallSource
Value: C:\Users\admin\AppData\Local\Temp\

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** InstallDate
Value: 20220824

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** Language
Value: 1033

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** EstimatedSize
Value: 4879

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** NoModify
Value: 1

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NewProduct 1.00
Operation: write **Name:** NoRepair
Value: 1

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPDaysSinceLastAutoMigration
Value: 1

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPLastLaunchLowDateTime
Value:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation: write **Name:** NTPLastLaunchHighDateTime
Value: 30980035

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation: write **Name:** NextCheckForUpdateLowDateTime
Value:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation: write **Name:** NextCheckForUpdateHighDateTime
Value: 30980035

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1584) bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** GlobalAssocChangedCounter
Value: 101

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix

Value:

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

Operation: write **Name:** CompatibilityFlags
Value: 0

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003C01000009000000000000000000000000000000040000000000000000C0E333BBEAB1D30100000000000000000000000000000000010000000200000000C0A80164000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003E01000009000000000000000000000000000000040000000000000000C0E333BBEAB1D30100000000000000000000000000000000010000000200000000C0A80164000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003D01000009000000000000000000000000000000040000000000000000C0E333BBEAB1D30100000000000000000000000000000000010000000200000000C0A80164000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003F01000009000000000000000000000000000000040000000000000000C0E333BBEAB1D30100000000000000000000000000000000010000000200000000C0A80164000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3452) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: UNCAsIntranet
Value: 1

(PID) Process: (3452) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: AutoDetect
Value: 0

(PID) Process: (3452) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write
Name: SecuritySafe
Value: 1

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: ProxyBypass
Value: 1

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: IntranetName
Value: 1

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: UNCAsIntranet
Value: 1

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: AutoDetect
Value: 0

(PID) Process: (2172) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write
Name: ProxyEnable
Value: 0

(PID) Process: (2172) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 46000000410100000900000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A801640000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write
Name: ProxyEnable
Value: 0

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write
Name: SecuritySafe
Value: 1

(PID) Process: (2340) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 46000000400100000900000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A801640000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2100) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write
Name: ProxyEnable
Value: 0

(PID) Process: (2100) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 46000000420100000900000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A801640000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2940) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write
Name: ProxyEnable
Value: 0

(PID) Process: (2940) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 46000000430100000900000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A801640000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2940) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: ProxyBypass
Value: 1

(PID) Process: (2940) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: IntranetName
Value: 1

(PID) Process: (2940) iexplore.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 46000000440100000900000000000000000000000000000000000000400000000000000C0E333BBEAB1D30100000000000000000000000000100000002000000C0A80164000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
Operation: write **Name:** SecuritySafe
Value: 1

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 46000000450100000900000000000000000000000000000004000000000000000C0E333BBEAB1D301000000000000000000000000010000000200000000C0A80164000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {2321EB6B-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: E476D1E6C3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 983BD6E6C3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

Operation: write **Name:** Window_Placement

Value: 2C00000002000000030000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF2000000020000000400300007802000 0

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery

Operation: write **Name:** AdminActive

Value: 0

(PID) Process: (2484) real.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: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 5A27E2E6C3B7D801

(PID) Process: (2484) real.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: (2484) real.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: (2484) real.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: (2484) real.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 5A27E2E6C3B7D801

(PID) Process: (2484) real.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: (292) F0gel.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: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 5A27E2E6C3B7D801

(PID) Process: (292) F0gel.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: (292) F0gel.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: (292) F0gel.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: (292) F0gel.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 5A27E2E6C3B7D801

(PID) Process: (292) F0gel.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: (2312) 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: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Time
Value: E6070800030018000E000F0002006C03

(PID) Process: (2312) 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: (2312) 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: (2312) 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: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0002007C03

(PID) Process: (2312) 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: (2312) 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: (2312) 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: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0002008B03

(PID) Process: (2312) 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: (2312) 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: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0002008B03

(PID) Process: (2312) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {23329BE1-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {23434C57-23B7-11ED-B9F6-12A9866C77DE}

Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {231F8911-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 4600000046010000090000000000000000000000000000000000000004000000000000000C0E333BBEAB1D301000000000000000000000000000100000002000000C0A8646A00000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C0000000200000003000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3600000036000000560300008E020000

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {23291279-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {2339C2EF-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {23303987-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive
Operation: write **Name:** {2348110B-23B7-11ED-B9F6-12A9866C77DE}
Value: 0

(PID) Process: (2484) real.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C0000000200000003000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3600000036000000560300008E020000

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 5A27E2E6C3B7D801

(PID) Process: (2312) 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: (2312) 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: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 424784E7C3B7D801

(PID) Process: (2312) 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: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 424784E7C3B7D801

(PID) Process: (2312) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 1491EFE7C3B7D801

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 1491EFE7C3B7D801

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 6EF3F1E7C3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 6EF3F1E7C3B7D801

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 6EF3F1E7C3B7D801

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 6EF3F1E7C3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: C855F4E7C3B7D801

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch

Operation: write **Name:** UpgradeTime
Value: 7C1AF9E7C3B7D801

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: D67CFBE7C3B7D801

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: D67CFBE7C3B7D801

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 30DFFDE7C3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 30DFFDE7C3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 30DFFDE7C3B7D801

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch
Operation: write **Name:** UpgradeTime
Value: 30DFFDE7C3B7D801

(PID) Process: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0004008202

(PID) Process: (2100) 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: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0004008202

(PID) Process: (2100) 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: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0004008202

(PID) Process: (2100) 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: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0004008202

(PID) Process: (2100) 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: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000004701000009000000000000000000000000000000040000000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A8646A000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 424784E7C3B7D801

(PID) Process: (2100) 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: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 00F210E8C3B7D801

(PID) Process: (2100) 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: (2100) 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: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 00F210E8C3B7D801

(PID) Process: (2100) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

Operation: write **Name:** Window_Placement

Value: 2C0000000200000003000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF360000003600000056030000 8E020000

(PID) Process: (3616) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (3616) iexplore.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8

Operation: write **Name:** Blob

Value: 0400000001000000100000000CD2F9E0DA1773E9ED864DA5E370E74E0F00000001000000200000003F0411EDE9C4477057D57E57883B1F205B20CDC0F3263129B1EE0269A2678F63030000
00010000001400000CABD2A79A1076A31F21D253635CB039D4329A5E80900000000100000000C000000300A06082B060105050703011D00000001000000100000073B6876195F5D18E0485
10422AEF04E3140000000100000014000000079B459E67BB6E5E40173800888C81A58F6E99B6E0B000000010000001A00000049005300520047002000052006F006F007400200058003100000
0620000000100000020000000096BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6190000000100000010000002FE1F70BB05D7C92335BC5E05B984DA62000
0000010000006F0500003082056B30820353A003020102021100821 0CFB0D240E3594463E0BB63828B00300D06092A864886F70D01010B0500304F310B300906035504061302555331293 02
7060355040A1320496E7465726E6574205365637572697479205265736561726368204772 6F75703115301306035504031 30C4953524720526F6F74205831301E170D31353036303431 31303
433385A170D33353036303431313034333 85A304F310B3009060355040613025553312930270603550 40A1320496E7465726E65742053656375726974792052657365617263682047726F757
0311530130603550403130C4953524720526F6F7420583130820222300D06092A864886F70D01010105000382020F003082020A0282020100ADE82473F41437F39B9E2B57281C87BEDCB7D
F38908C6E3CE657A078F775C2A2FEF56A6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5DD79DFB3B8FF12F1219A4BC18A8671694A66666C8F7E3C70B
FAD292206F3E4C0E680AEE24B8FB7997E94039FD347977C99482353E838AE4F0A6F832ED149578C8074B6DA2FD0388D7B0370211B75F2303CFA8FAEDDDA63ABEB164FC28E114B7ECF0BE
8FFB5772EF4B27B4AE04C12250C708D0329A0E15324EC13D9EE19BF10B34A8C3F89A36151DEAC870794F46371EC2EE26F5B9881E1895C34796C76EF3B906279E6DBA49A2F26C5D010E10
EDED9108E16FBB7F7A8F7C7E50207988F360895E7E237960D36759EFB0E72B11D9BBC03F94905D881DD05B42AD641E9AC0176950A0FD8DFD5BD121F352F28176CD298C1A80964776E473
7BACEAC595E689D7F72D689C50641293E593EDD26F524C911A75AA34C401F46A199B5A73A516E863B9E7D72A712057859ED3E5178150B038F8DD02F05B23E7B4A1C4B730512FCC6EAE05
0137C439374B3CA74E78E1F0108D030D45B7136B407BAC130305C48B7823B98A67D608AA2A32982CCBABD83041BA2830341A1D605F11BC2B6F0A87C863B46A8482A88DC769A76BF1F6A
A53D198FEB38F364DEC82B0D0A28FFF7DBE21542D422D0275DE179FE18E77088AD4EE6D98B3AC6DD27516EFFBC64F533434F0203010001A3423040300E0603551D0F0101FF04040302010
6300F0603551D130101FF040530030101FF301D0603551D0E0416041479B459E67BB6E5E40173800888C81A58F6E99B6E300D06092A864886F70D01010B05000382020100551F58A9BCB2A
850D00CB1D81A6920272908AC61755C8A6EF882E5692FD5F6564BB9B8731059D321977EE74C71FBB2D260AD39A80BEA17215685F1500E59EBCEE059E9BAC915EF869D8F8480F6E4E9919
0DC179B621B45F06695D27C6FC2EA3BEF1FCFCBD6AE27F1A9B0C8AEFD7D7E9AFA2204EBFFD97FEA912B22B1170E8FF28A345B58D8FC01C954B9B826CC8A8833894C2D843C82DFEE9657
05BA2CBBF7C4B7C74E3B82BE31C822737392D1C280A43939103323824C3C9F86B255981DBE29868C229B9EE26B3B573A82704DDC09C789CB0A074D6CE85D8EC9EFCEABC7BBB52B4E45D
64AD026CCE572CA086AA595E315A1F7A4EDC92C5FA5FBFFAC28022EBED77BBBE3717B9016D3075E46537C3707428CD3C4969CD599B52AE0951A8048AE4C3907CECC47A452952BBAB8FB
ADD233537DE51D4D6DD5A1B1C7426FE64027355CA328B7078DE78D3390E7239FFB509C796C46D5B415B3966E7E9B0C963AB8522D3FD65BE1FB08C284FE24A8A389DAAC6AE1182AB1A84
3615BD31FDC3B8D76F22DE88D75DF17336C3D53FB7BCB415FFFDCA2D06138E196B8AC5D8B37D775D533C09911AE9D41C1727584BE0241425F67244894D19B27BE073FB9B84F817451E17
AB7ED9D23E2BEE0D52804133C31039EDD7A6C8FC60718C67FDE478E3F289E0406CFA5543477BDEC899BE91743DF5BDB5FFE8E1E57A2CD409D7E6222DADE1827

(PID) Process: (3616) iexplore.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8

Operation: write **Name:** Blob

Value: 5C000000010000000400000000100000190000000100000010000002FE1F70BB05D7C92335BC5E05B984DA6620000000100000020000000096BCEC06264976F37460779ACF28C5A7CFE8A3
C0AAE11A8FFCEE05C0BDDF08C60B000000010000001A00000049005300520047002000052006F006F0074002000580031000000140000000100000014000000079B459E67BB6E5E401738008
88C81A58F6E99B6E1D0000000100000010000000 73B6876195F5D18E048510422AEF04E30900000000100000000C000000300A06082B0601050507030103000000010000001400000CABD2A
79A1076A31F21D253635CB039D4329A5E80F0000000100000020000003F0411EDE9C4477057D57E57883B1F205B20CDC0F3263129B1EE0269A2678F63040000000100000010000000CD2
F9E0DA1773E9ED864DA5E370E74E200000000100000 06F0500003082056B30820353A003020102021100821 0CFB0D240E3594463E0BB63828B00300D06092A864886F70D01010B0500304F
310B3009060355040613025553312930270603550 40A1320496E7465726E6574205365637572697479205265736561726368204772 6F75703115301306035504031 30C4953524720526F6F74
205831301E170D3135303630343131303433385A170D33353036303431313034333 85A304F310B3009060355040613025553312930270603550 40A1320496E7465726E657420536563757269
74792052657365617263682047726F7570311530130603550403130C4953524720526F6F7420583130820222300D06092A864886F70D01010105000382020F003082020A0282020100ADE824
73F41437F39B9E2B57281C87BEDCB7DF38908C6E3CE657A078F775C2A2FEF56A6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5DD79DFB3B8FF12F121
9A4BC18A8671694A66666C8F7E3C70BFAD292206F3E4C0E680AEE24B8FB7997E94039FD347977C99482353E838AE4F0A6F832ED149578C8074B6DA2FD0388D7B0370211B75F2303CFA8FA
EDDDA63ABEB164FC28E114B7ECF0BE8FFB5772EF4B27B4AE04C12250C708D0329A0E15324EC13D9EE19BF10B34A8C3F89A36151DEAC870794F46371EC2EE26F5B9881E1895C34796C76E
F3B906279E6DBA49A2F26C5D010E10EDED9108E16FBB7F7A8F7C7E50207988F360895E7E237960D36759EFB0E72B11D9BBC03F94905D881DD05B42AD641E9AC0176950A0FD8DFD5BD121
F352F28176CD298C1A80964776E4737BACEAC595E689D7F72D689C50641293E593EDD26F524C911A75AA34C401F46A199B5A73A516E863B9E7D72A712057859ED3E5178150B038F8DD02
F05B23E7B4A1C4B730512FCC6EAE050137C439374B3CA74E78E1F0108D030D45B7136B407BAC130305C48B7823B98A67D608AA2A32982CCBABD83041BA2830341A1D605F11BC2B6F0A8
7C863B46A8482A88DC769A76BF1F6AA53D198FEB38F364DEC82B0D0A28FFF7DBE21542D422D0275DE179FE18E77088AD4EE6D98B3AC6DD27516EFFBC64F533434F0203010001A3423040
300E0603551D0F0101FF040403020106300F0603551D130101FF040530030101FF301D0603551D0E0416041479B459E67BB6E5E40173800888C81A58F6E99B6E300D06092A864886F70D010
10B05000382020100551F58A9BCB2A850D00CB1D81A6920272908AC61755C8A6EF882E5692FD5F6564BB9B8731059D321977EE74C71FBB2D260AD39A80BEA17215685F1500E59EBCEE05
9E9BAC915EF869D8F8480F6E4E99190DC179B621B45F06695D27C6FC2EA3BEF1FCFCBD6AE27F1A9B0C8AEFD7D7E9AFA2204EBFFD97FEA912B22B1170E8FF28A345B58D8FC01C954B9B82
6CC8A8833894C2D843C82DFEE965705BA2CBBF7C4B7C74E3B82BE31C822737392D1C280A43939103323824C3C9F86B255981DBE29868C229B9EE26B3B573A82704DDC09C789CB0A074D
6CE85D8EC9EFCEABC7BBB52B4E45D64AD026CCE572CA086AA595E315A1F7A4EDC92C5FA5FBFFAC28022EBED77BBBE3717B9016D3075E46537C3707428CD3C4969CD599B52AE0951A80
48AE4C3907CECC47A452952BBAB8FBADD233537DE51D4D6DD5A1B1C7426FE64027355CA328B7078DE78D3390E7239FFB509C796C46D5B415B3966E7E9B0C963AB8522D3FD65BE1FB08C
284FE24A8A389DAAC6AE1182AB1A843615BD31FDC3B8D76F22DE88D75DF17336C3D53FB7BCB415FFFDCA2D06138E196B8AC5D8B37D775D533C09911AE9D41C1727584BE0241425F6724
4894D19B27BE073FB9B84F817451E17AB7ED9D23E2BEE0D52804133C31039EDD7A6C8FC60718C67FDE478E3F289E0406CFA5543477BDEC899BE91743DF5BDB5FFE8E1E57A2CD409D7E62
22DADE1827

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

Operation: write **Name:** FullScreen

Value: no

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery

Operation: write **Name:** AdminActive

Value: 1

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery

Operation: write **Name:** AdminActive

Value: 0

(PID) Process: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Count
Value: 27

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0005005F00

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 27

(PID) Process: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count
Value: 27

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0005005F00

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 27

(PID) Process: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count
Value: 27

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0005005F00

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 27

(PID) Process: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 27

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0005005F00

(PID) Process: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 27

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (1904) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 4600000048010000090000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000010000000200000000C0A8646A00000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 00F210E8C3B7D801

(PID) Process: (2940) 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: (2940) 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: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 7E5151E8C3B7D801

(PID) Process: (2940) 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: (2940) 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: (2940) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 7E5151E8C3B7D801

(PID) Process: (2940) 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: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Count
Value: 28

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F000500DC00

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 28

(PID) Process: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count
Value: 28

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F000500DC00

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 28

(PID) Process: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count
Value: 28

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F000500DC00

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 28

(PID) Process: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 28

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F000500DC00

(PID) Process: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 28

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2708) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 46000000490100000900000000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000000100000002000000C0A8646A000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 7E5151E8C3B7D801

(PID) Process: (2340) 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: (2340) 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: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: F40162E8C3B7D801

(PID) Process: (2340) 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: (2340) 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: (2340) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: F40162E8C3B7D801

(PID) Process: (2340) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C0000000200000003000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF4C0000004C0000006C030000A4020000

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (3316) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: F40162E8C3B7D801

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 6CE9CAE8C3B7D801

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 6CE9CAE8C3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (2312) 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: 1C00000001000000E607080003001800 0E000F0006001100010000000644EA2EF78B0D01189E400C04FC9E26E

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Count
Value: 29

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006009D00

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 29

(PID) Process: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count
Value: 29

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006009D00

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 29

(PID) Process: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count

Value: 29

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006009D00

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 29

(PID) Process: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 29

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006009D00

(PID) Process: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 29

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3612) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000004A010000090000000000000000000000000000000400000000000000C0E333BBEAB1D3010000000000000000000000000000000001000000020000000C0A8646A0000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** FullScreen
Value: no

(PID) Process: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 6CE9CAE8C3B7D801

(PID) Process: (3452) 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: (3452) 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: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 6671F3E8C3B7D801

(PID) Process: (3452) 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: (3452) 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: (3452) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 6671F3E8C3B7D801

(PID) Process: (3452) 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: (2312) 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: 1C00000001000000E60708000300180000E000F000600DC0000000000

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C000000020000000300000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF62000000000000008203000058020000

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 6671F3E8C3B7D801

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 44AB0DE9C3B7D801

(PID) Process: (2100) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 44AB0DE9C3B7D801

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C000000020000000300000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF62000000000000008203000058020000

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Operation: write **Name:** Window_Placement
Value: 2C000000020000000300000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF62000000000000008203000058020000

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 1

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery
Operation: write **Name:** AdminActive
Value: 0

(PID) Process: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Count

Value: 30

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Time

Value: E60708000300180000E000F0006003402

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Blocked

Value: 30

(PID) Process: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Count

Value: 30

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Time

Value: E60708000300180000E000F0006003402

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

Operation: write **Name:** Blocked

Value: 30

(PID) Process: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore

Operation: write **Name:** Count

Value: 30

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore

Operation: write **Name:** Time

Value: E60708000300180000E000F0006003402

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore

Operation: write **Name:** Blocked

Value: 30

(PID) Process: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore

Operation: write **Name:** Count

Value: 30

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore

Operation: write **Name:** Time

Value: E60708000300180000E000F0006003402

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore

Operation: write **Name:** Blocked

Value: 30

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content

Operation: write **Name:** CachePrefix

Value:

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies

Operation: write **Name:** CachePrefix

Value: Cookie:

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Count
Value: 31

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006004302

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 31

(PID) Process: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count
Value: 31

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006004302

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 31

(PID) Process: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count
Value: 31

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E6070800030018000E000F0006004302

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 31

(PID) Process: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 31

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-

9C25C1C588A9}\iexplore

Operation: write **Name:** Time

Value: E6070800030018000E000F0006004302

(PID) Process: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore

Operation: write **Name:** Blocked

Value: 31

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (488) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value: 460000004C010000090000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000010000000200000C0A8646A0000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value: 460000004B010000090000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000010000000200000C0A8646A0000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content

Operation: write **Name:** CachePrefix

Value:

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies

Operation: write **Name:** CachePrefix

Value: Cookie:

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

Operation: write **Name:** CachePrefix

Value: Visited:

(PID) Process: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore

Operation: write **Name:** Count

Value: 32

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Time
Value: E60708000300180000E000F0006006302

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{28BCCB9A-E66B-463C-82A4-09F320DE94D7}\iexplore
Operation: write **Name:** Blocked
Value: 32

(PID) Process: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Count
Value: 32

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Time
Value: E60708000300180000E000F0006006302

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore
Operation: write **Name:** Blocked
Value: 32

(PID) Process: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Count
Value: 32

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Time
Value: E60708000300180000E000F0006006302

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{B4F3A835-0E21-4959-BA22-42B3008E02FF}\iexplore
Operation: write **Name:** Blocked
Value: 32

(PID) Process: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Count
Value: 32

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Time
Value: E60708000300180000E000F0006006302

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
Operation: write **Name:** Blocked
Value: 32

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (1080) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000004D0100000900000000000000000000000000000004000000000000000C0E333BBEAB1D301000000000000000000000000010000000200000000C0A8646A0000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 44AB0DE9C3B7D801

(PID) Process: (1636) 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: (1636) 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: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 989538E9C3B7D801

(PID) Process: (1636) 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: (1636) 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: (1636) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 989538E9C3B7D801

(PID) Process: (1636) 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: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 44AB0DE9C3B7D801

(PID) Process: (2172) 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: (2172) 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: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: F2F73AE9C3B7D801

(PID) Process: (2172) 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: (2172) 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: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: F2F73AE9C3B7D801

(PID) Process: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: F2F73AE9C3B7D801

(PID) Process: (2652) 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: (2652) 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: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 4C5A3DE9C3B7D801

(PID) Process: (2652) 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: (2652) 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: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 4C5A3DE9C3B7D801

(PID) Process: (2652) 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: (1080) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (2312) 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: 00000000A607000059EA0E7DB883443E9FF37D031B123245EC162088F64DA4328DA48DF638ACCBC5C171EC91808DA4A143F6E6788E87D872A56E17146BE6A22180FB05FFA9468E804BC2DBE5263C7B11C509CE016DEDEF0F925FFE5FEDB3747A76B4106409BE6EABBF7B806C73B0803093CE43280A3F9515A5890AB8E4D5669C746D4F25AB32C8E4C03DE36CF50853C40CE4F5EC249E03ABB98CFA3A2E6DDC8E42C7072046C4DEC227A9C099E5664F4FD7EAFCD82C2A88E84D0807775699B009A46271EB83928A40C25D8CC66CE9C50E8A820C222E034F74599D74A9AD7AACD5B2DEBABF82BE5D00F9FB3A2122B1C138614A82DC424946E831EB0C7ECE30D274C8DB6A757E67485BB7212E0391DD9793BCE4383D511C520C4092AD6B4DDC8A2262FA008AB8AC19417271264FB88F155BF2EF60EC5F9C7EDE6C321394FF9C5B1F52D9AA416CAF79EC0189E05FEDE6B171460BDC673FE9B769906A4D41BE91684A3A194ECA9B8E295CBD0A64853E020DE8A6D714762D23F77198DC8BE679DC1911FF5A1A7A476B1BAC4D95C21425030ED112F584A9686A4BE8AC279FBA0B9B03ADCB3C4B1BDE64E93087C839078F0806654B04AAF033DE5C37DDEBE4DC99EF55ACBE5F4842049BEA6666452427E033FB77A2A39B390A9F6759E0C841099FF86ACF9C63ADBBAF2E48B71FAA27CF15A3193A1474E6261ECDFFC0FE5EC5E451D7F13654E9ED062D3F9B05B0987C39567858547E16E5CC1588DA12194DDECD5AAA52E0008FF7DC9BEC0E1208B0B05A53D28A42F32853895CF06FAD36352846919255704 6F60CCF5E5743A7A9903057C8D0B4111F4C29E4F225A60012B6E1E87BB0AE50E8BEAEF0849E4A9D7FDAC57BBE943E5D7C215981A547FFB8407041F026229D1DAF87798E1FE385A8022CDCCC3D3D35A7C9461E22FA76FDB368032D4CF109736192F1A1FC8544EDFC8227412769EBA9FB4E5D60BCF5D2F0CCA70E064A9785A09D7B9D966F58E33BB9066CC6EEA5BD3AE642057C96F67BA171ED333BCA0AB718AF5C2925E853DFCA2E8099F648B0D5A8B3B3DD6E7EAA91DE0FB111C60404BD2D744836A12AF95753EA6E508BEF1A52A10A35877A0D9C34B046C248AFE393B847CAEA64AFCC646D7D9AE92F388E31540FCD78A2C3F3DF8447F6E77841E76CC9D1DCD253744FF33F06BC94D7A0AE7BFBD44DC8CDCA628BA1A4125041EC9B290EA4BEADA3E4464EEFF11F3EE97A3AF6664CD41CAA947B87AB34512C434CA2C7A8725A37F57598889B0933DA032386CDB7B171CAD7E4D1D2C2E49B4D1ED544DCB7D2A95BE714C34665C3280EC791F3170D4527D4F613FEB806B05E5B729C9D0A5C4A47381AFD3B916B09E3ECD3EE1D5A88215623A63E429397139D66DFEB5009B597460D2ED4D32ECF83B894C80D969D47A9888E86A53899953FDB6605F3CBFDE365658AC30838ABAF61022B472238D06C2384F438739AD42099D6A2834D23B106A7818679627A182D2C7B92EE9801A61604AE205B790EAF58250FE4FBA574443FDC6CF7F0C7A8DE67BD755D5FA385386558C1C48E910E755ED51ECA0C10DFEEAC6C0471C9E97B487F20D6FE3808E93F79C3D0F6730CD9785029E1CD569709A56E1D9E3CA2C20F8B9360E78B1A5472B071C29D5EA95A737F4F226FF0794F386FA6A8C70C1C37AF3FC5A7F74CA600A5C56FE13B91CF48BA727BC6E41A15E2F442722C50D8D727ACB333F3CE807AC0F52692DA04DF87C48804F474F93ECA6B42F9F3BCA58E73C64D86FF2BE83138890030FA7CDE477098E65ADAFD696A386F67954957828E901FC76C48AD87F77E4064D6C678CDB429F84E1D4D67315EFF97405095AAE66ECF8343E62DF9983EEEF10FB518BADAF15425FC076D768F66BFCA2BE5F5656954CEC9024AD0C95D1B26AF3EFB0F32490D909C52235A6CE29617EE78B88AE6D0242EBA7EC74F7CF3B6C77CF331CBE817B67C154D6C34E34F84A9457463755402E38FB7AB46CCAD9D427253027D6C43D616BAD9012A1BA13BA41418FD28D4F73BD291E53EC465F4EBD6C512B5851171CD44E955332E2FFE93CEF817ABC1C8E2A1A5D4BC09493CF1A56C62DCF7CFDC436DBFA84AF54490C5E3F8F5E1849871DB1C90F87B668E6F608F18E77F1418ECDC174E99325D035E0041BFAB3B4451F00983539E26AE2120C1F591F5F20451615031735B8F450FB99E032BBADB322E637919726423C9936D3713152D3A50535B9586B38D5B2147C1384B10C29E89F4EBB45961EBF3C4D2783B3EEA2DBD7A94F9F90118D1B5DAF096E65B6163876C68A9EB15F6D3F37FBA5F21E861974000D45D89AC67C696CAD65859C24A3D6A6F35BBDBDE8BBCD26319443B71340901E73BA6AF08D40BB6B8FD27405079F0B0A8D54224C59B46A83184450DC6842400DD00F47DB01B42C4ECF623BAE2871B8F5F965EE86344128FDA0C840DD220893CE58D66294C570A2553B56C83FB0F605D3C4430143B4BBE256B3C2044BF9ED61F96DF1EF8D9DE02B2AEC9221428AA5E54101BD64D6113EBDB04ED386E0674ADFDEA1E3B833C37CC14DBDC656D3D82B5132DF0718079E139BFE95FEEE44EBCACF79D70DD03263B072C208C55E75AF905B74B6A22B806C248FF96F960A421D4741D1A6424DD46C552FB91B71229C91AEEEA0131076102ACB846ED47B0016834A624FAAB2F89D4304F3A85A6BC7A9F09102EC7

E241AACB6B2A9D6E88FCA7BCD6E09112EC2071619A9CFE13A6731C3A360B9F8FB3F077655B3C15875766098A55C4021660160100000000E000000385835324E41646D516B4125336402000000000000

(PID) Process: (2044) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\User Preferences
Operation: write **Name:** 88D7D0879DAB32E14DE5B3A805A34F98AFF34F5977
Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000EF448E36AB176C48842DCC98025322870000000002000000000010660000000100002000000BCA15E5462BD1EEA5FC3691B43A0B9AB8702D74EB5223B61D7446B917A6FE720000000000E80000000020000200000007FEEBE4D62C46CD5C776BA6FC4E564ACDD7139B4A07EEF53F94AF8FACF3D3DCD500000000BCEB25908F03DC73F85C4AFB3B9A525DB9C9FA2F70AF2F2DD68F7314E13C0BF9CEB9FA8662AD6C02EB1BE33C4062769E0EEDF08FF99FB5C951A3A076E35152702DB211AD984DE692C594AAA392AE26840000000649C942111F3525748D682B8776ED24461C20FE8C3C0819749DEF69C43AC20193579204F4581A10EC2F9C4A143777B346B2F90AF077CDE7E87C2D1CD41FFF1C5

(PID) Process: (2312) 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: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\User Preferences
Operation: write **Name:** 2D53CFFC5C1A3DD2E97B7979AC2A92BD59BC839E81
Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000EF448E36AB176C48842DCC98025322870000000002000000000010660000000100002000000194E139E4DD23F13C036C07628013D7CE7C6DCAE16FD4CC2D0DCA7CBB2858C8B000000000E80000000020000200000046364DFB0F8872E352124C8722530C1D1934CE1E38D9040B41808079C5C378EC100000006D660463989FB6E36C9A502573544C61400000000DFCAD7FC8FBDA679D3209D3FBDEE24921C92DDBCB2DB041DDEA8372B962FFCCF8F9B0278AA2AE71904EEFAE2B54E06AC93DAC5B79BC5E83CAA866D47660C147

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 4C5A3DE9C3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: A4B218EAC3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: A4B218EAC3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: FE141BEAC3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: FE141BEAC3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: A4B218EAC3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 14EB51EAC3B7D801

(PID) Process: (2312) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 14EB51EAC3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 14EB51EAC3B7D801

(PID) Process: (2172) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 14EB51EAC3B7D801

(PID) Process: (2172) 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: (2312) iexplore.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 14EB51EAC3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime
Value: 76FC83EAC3B7D801

(PID) Process: (2652) iexplore.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 76FC83EAC3B7D801

Files activity

Executable files	Suspicious files	Text files	Unknown types
23	20	37	38

Dropped files

PID	Process	Filename	Type
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Users\admin\AppData\Local\Temp\$inst\temp_0.tmp	compressed
		MD5: 6755BB2E0A1EB238B1CDD7D3D9268718 **SHA256:** A36D46D4C9A0713CB2CCB313BD293E85041BEF5D994CA5C10AB450550787ACFE	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Users\admin\AppData\Local\Temp\$inst\2.tmp	compressed
		MD5: 8708699D2C73BED30A0A08D80F96D6D7 **SHA256:** A32E0A83001D2C5D41649063217923DAC167809CAB50EC5784078E41C9EC0F0F	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\real.exe	executable
		MD5: E0C8728412F5F7E97698C72DA925C5E6 **SHA256:** DAFCE710DB720216E5CCCE685848AAA84B27BBAF6DE356E73F09A125CFD0A618	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\kukurzka9000.exe	executable
		MD5: 3EC059BD19D6655BA83AE1E644B80510 **SHA256:** 7DC81DC72CB4F89AD022BB15419E1B6170CF77942B8EC29839924B7B4FE7896C	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\jshainx.exe	executable
		MD5: 2647A5BE31A41A39BF2497125018DBCE **SHA256:** 84C7458316ADF09943E459B4FB1AA79BD359EC1516E0AD947F44BDC6C0931665	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\namdoitntn.exe	executable
		MD5: BBD8EA73B7626E0CA5B91D355DF39B7F **SHA256:** 1AA3FDC24E789B01A39944B85C99E4AC08864D2EAE7530164CEA2821ACBF184E	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\safert44.exe	executable
		MD5: 414FFD7094C0F50662FFA508CA43B7D0 **SHA256:** D3FB9C24B34C113992C5C658F6A11F9620DA2E49D12D1ACABE871E1BEA7846EE	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\F0gel.exe	executable
		MD5: 501E0F6FA90340E3D7FF26F276CD582E **SHA256:** F07D918C6571F11ABF9AB7268AC6E2ECBCD931C3D9D878895C777D15052AAE2B	
2940	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{23291279-23B7-11ED-B9F6-12A9866C77DE}.dat	binary
		MD5: 3761A3CC2587DEF8BCF1F4D890EEA232 **SHA256:** B626FAB91325AB73D8D487139CA52610C12AB35F21FB8BC096C705B2FDD0ED16	
2100	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{23329BE1-23B7-11ED-B9F6-12A9866C77DE}.dat	binary
		MD5: 22D05F87E1C8358DA9F699F7D12F7ACA **SHA256:** CD86D117EFC319A2FB3C53EAB2946F5515D349353FD991CF7A88DD3593A029B3	
2340	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2339C2EF-23B7-11ED-B9F6-12A9866C77DE}.dat	binary
		MD5: E2FAA25D81EE27A47FEB398B60C0BFC5 **SHA256:** 672E0446E1381213DBBF7336ADFF9EFAA45E2F63B67C96ED6FBEB72EB338E9F5	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\brokerius.exe	executable
		MD5: F5D13E361F8B9ACA7103CB46B441034B **SHA256:** A5AD514ED54F1F8F0A8E054B0DC3A39D13D70E388711DDB9D44095A5A89317BF	
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	compressed
		MD5: F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\ordo_sec666.exe	executable
		MD5: 63FD052610279F9EB9F1FEE8E262F2A4 **SHA256:** 955C265A378008EFEE8F0D19C2880D1026F32F7CD6325E0AB1A24C833905BBBA	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\me.exe	executable
		MD5: 21C43007B3C14564CF459791F86DA430 **SHA256:** 62C0FA8AE93F0B4B6EC1CDCA23AC24AC55CED93CB11A06AC104CEC8AA44969AC	
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	binary
		MD5: 0A24ACF3EFC31F1AD297746E45A34DE7 **SHA256:** 530CF0713AF9053A963B255EC43A89BC378116492F8E8168F6A139F1315C9B11	
1584	bdbd5a0fb6a3ab99f0cfa3cee7e3f7f8f7ec078eeb628aadfb8a32a5df2be3b9.exe	C:\Program Files\Company\NewProduct\captain09876.exe	executable

		MD5: CE94CE7DE8279ECF9519B12F124543C3	**SHA256:** F88D6FC5FD36EF3A9C54CF7101728A39A2A2694A0A64F6AF1E1BEFACFBC03F20
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\vcruntime140.dll	executable
		MD5: 1B171F9A428C44ACF85F89989007C328	**SHA256:** 9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\nss3.dll	executable
		MD5: F67D08E8C02574CBC2F1122C53BFB976	**SHA256:** C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\msvcp140.dll	executable
		MD5: 1FB93933FD087215A3C7B0800E6BB703	**SHA256:** 2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
3616	iexplore.exe	C:\Users\admin\AppData\Local\Temp\Tar63CF.tmp	cat
		MD5: 5FE75D13824710AE2538A9E16592B701	**SHA256:** DD7F97F8D33665D2FF8338E3C01E9B2DD60EFAA2711A34CD385154CFF822585A
3616	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	compressed
		MD5: 6C6A24456559F305308CB1FB6C5486B3	**SHA256:** EFC3C579BD619CEAB040C4B8C1B821B2D82C64FDDD9E80A00EC0D7F6577ED973
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\vxoHFLC04910	sqlite
		MD5: CC104C4E4E904C3AD7AD5C45FBFA7087	**SHA256:** 321BE844CECC903EF1E7F875B729C96BB3ED0D4986314384CD5944A29A670C9B
3616	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	binary
		MD5: EA0AB466CCF92AC3787AF5E87A2A30BD	**SHA256:** ABE833ACB76365845D58A3AD9F3B03FE3CF16062CE00017A9147D0AAD4CD4FA6
3316	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\103621DE9CD5414CC2538780B4B75751	der
		MD5: EC8FF3B1DED0246437B1472C69DD1811	**SHA256:** E634C2D1ED20E0638C95597ADF4C9D392EBAB932D3353F18AF1E4421F4BB9CAB
2652	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2348110B-23B7-11ED-B9F6-12A9866C77DE}.dat	binary
		MD5: 754371C0476C4FBA8898A11792D81E8E	**SHA256:** 2A7F3BF9AC5BDAD9D1B819E0F16259A39DC6A1CC5C9F88EDD7BAEA9145E79458
3616	iexplore.exe	C:\Users\admin\AppData\Local\Temp\Cab63CE.tmp	compressed
		MD5: 6C6A24456559F305308CB1FB6C5486B3	**SHA256:** EFC3C579BD619CEAB040C4B8C1B821B2D82C64FDDD9E80A00EC0D7F6577ED973
1080	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1AGmX4[1].png	image
		MD5: EC6AAE2BB7D8781226EA61ADCA8F0586	**SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599
3316	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\RR2QQBZC.txt	text
		MD5: 67EB9E7CB5FB7D62883E3B22E900BDDF	**SHA256:** F92FC8B541110988E4B908116135D656E2128FABFE2EC36E46B5A35B5837B782
1080	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\Q4R36EI9.txt	text
		MD5: 11AABED090A56AD831934B8BCC6F932A	**SHA256:** F92E726A95BD69A5859B28E4521B216EA1F8D68AD679F6998446F26FE8B45EDC
3316	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1ARmX4[1].png	image
		MD5: EC6AAE2BB7D8781226EA61ADCA8F0586	**SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	der
		MD5: ACE5143083C383DA320215A327EACDBD	**SHA256:** 7DCAC877832F5C27E572A1EA609E351292558D58147DEA684BADC047835F2AEB
3316	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\ORVJ7NIF.txt	text
		MD5: 51DC8FE15DBDD51EC491AFC506D1ED6A	**SHA256:** FCF378F66292DD2307586271158220CF9E99F863624F75C4B84E169E7C114D4F
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\sqlite3.dll	executable
		MD5: DBF4F8DCEFB8056DC6BAE4B67FF810CE	**SHA256:** 47B643111719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\freebl3.dll	executable
		MD5: 15B61E4A910C172B25FB7D8CCB92F754	**SHA256:** B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
1080	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\HEADSOBM.txt	text
		MD5: 0E2DFBFFD267114DE49F727C31639385	**SHA256:** 4DF7764BDC6BC3220DB89333AE005EB7AE2D63C096E08C85D0FF8ACD1D82ACD2
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\softokn3.dll	executable
		MD5: 63A1FE06BE877497C4C2017CA0303537	**SHA256:** 44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	binary
		MD5: B3E7AB660D6CE6611E041E1EF3EFBED8	**SHA256:** D1D1D07D82F8CA13723330DF8CAF33661CF964B0C1B48B95CCB1419A1240BDB0
3316	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\103621DE9CD5414CC2538780B4B75751	binary
		MD5: 500FCA921B8FBBBA0161AD449AB27095	**SHA256:** 13E3430FB167A917DCAB8C95E9BD1C6D4A7693F577C7A8C6847B838606083FD5
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\mozglue.dll	executable
		MD5: F07D9977430E762B563EAADC2B94BBFA	**SHA256:** 4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\738FBC066DBD9E6001113366624890A3_53C5D34017BDB72400155AC2819BA60D	binary
		MD5: A7E468B4266B5E71C31880755BD01DE0	**SHA256:** 0EF59DD4BF1FFC7D038118697FB0390D9D15EDECD8251DA7AC75D21C53F44577
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\2T6a6zhbHysX	sqlite
		MD5: B8E63E7225C9F4E0A81371F29D6456D8	**SHA256:** 35A6919CE60EA8E0A44934F8B267BDE2C5A063C2E32F22D34724F168C43150C8
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\XpBb905TgJnK	sqlite
		MD5: D02907BE1C995E1E51571EEDB82FA281	**SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD
2044	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\A9CEY6UN.txt	text
		MD5: 5163D267F4FFF3ED9FC1DEB30DC3119D	**SHA256:** 4C9BDC729210C208531D0002CC2157E5CAD210DB9ABBEE1398C846C2196BDEAF
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F2	der

		61FA85A0B1771 **MD5:** 28CABE3C0EC8B3F9DFA405B181DFE63F **SHA256:** 546FFA789E6B9B8BE4037CCF0E71374022F91DC74BE81BEAA3023E40807BA63E	
3616	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1AAmX4[1].png **MD5:** EC6AAE2BB7D8781226EA61ADCA8F0586 **SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599	image
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF19E8851F02172643.TMP **MD5:** 5A3A779AD176F1EE047828A9B1A6D028 **SHA256:** 867130D8587DC60619EAF6727EE6E59C2342951AB4DEB2F6DD6B8CD3635D33AB	gmc
2044	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\RHJUQQOO.txt **MD5:** 88C0986B055ADD451642E574244E5E73 **SHA256:** DCF7E7DA3556CC2DB97D997CD98E0A047FC04A666CF2545BA5758CBFEAA51A22	text
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\738FBC066DBD9E6001113366624890A3_53C5D34017BDB72400155AC2819BA60D **MD5:** F0B80245BDD872E219C187F6FF1F9FEB **SHA256:** CD3394B0B30D1414253D42BB1ACC2033798F18916EE23EBB550B5DEF2165DC82	der
2484	real.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\XSFJ35IW.txt **MD5:** 39BD0E641E1F8C0F4198379D541D9731 **SHA256:** AB22BA9678B3B533E225CC1E7576D85A92DE0996F6D9A7C9D33A6B515D44CE02	text
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF28D4885916DC7263.TMP **MD5:** 387ACBDEEE45AE86801C471EF9C42CC6 **SHA256:** 291AB29CEAAB52BD76B00D5EE18D420B647DD6B53F6796F532E80C942B7D6F29	gmc
2044	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1AFmX4[1].png **MD5:** EC6AAE2BB7D8781226EA61ADCA8F0586 **SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599	image
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF1EA812D287A4E434.TMP **MD5:** D6A7000FEAA408EA6449B3ADE54D1FAE **SHA256:** FCB0A39E1F97D0B3A67B5B8B2E528AC86DC9045B1D0AA6508E526C325F9358A1	gmc
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\6B6v9TO63cgl **MD5:** 23D08A78BC908C0B29E9800D3D5614E7 **SHA256:** F6BD7DF5DFAE9FD88811A807DBA14085E00C1B5A6D7CC3D06CC68F6015363D59	sqlite
2484	real.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771 **MD5:** 819FC7DCC084ACC3A20A35662194819C **SHA256:** B39C9526D4128831D7239AF94F7D68CBFFBDD5567D0C41400D1873235D6F02D9	binary
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\852cY8Q42nqP **MD5:** 49E1E66E8EEFE2553D2ECEC4B7EF1D3E **SHA256:** A664C359ACE3BFC149323E5403BB7140A84519043BDBA59B064EBC1BDADD32D4	sqlite
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\jI6Ynn1xt2u3 **MD5:** D02907BE1C995E1E51571EEDB82FA281 **SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\Z4m89TCc3s40 **MD5:** E7CE898AADD69F4E4280010B7808116E **SHA256:** C9214BB54F10242AA254F0758372A440C8D8F49934021F8F08B6DF9FB377EB02	text
3616	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\TNF4I75D.txt **MD5:** 4C3E59C69BCDB87074F23D39848484C0 **SHA256:** 1418847DBFD9F7E4D13F74B51185025021502C45576384E28B1E032943ABF810	text
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\6B6v9TO63cgl-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF4842FA6823F60093.TMP **MD5:** 0BBB48DBC948490786F18FD1556617A3 **SHA256:** 84BFDA1B5340F1FB646DC0496D619E10B95FA8BDA682B0032BEF144004A19329	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF7AA58AC14DA48B69.TMP **MD5:** 60C6BD8989461E262D1807F3B8AF400A **SHA256:** 8DA97E724DE286760176231D9352DC86C2543EA3C859FDC0629555179F286B79	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFADEBDF819BBEEC5C.TMP **MD5:** DA7C618DBD4815D1A5F9028C2BC6DA63 **SHA256:** 03387B2779494DDF06CC4E7DB4E14A6A4B0AE36157F5C0CAB029E2E72E3B72FA	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFA6A5BF61EECEC903.TMP **MD5:** 9C06F1213E710EAE3C0E67D4813471CF **SHA256:** AAE68866C20AE2D59799CA0E04C5448CBE6BE09A18323375E574598AEF5968E6	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF3F0AA2BCAD1ADE4D.TMP **MD5:** 13B49AD5C83AFE04601FC1072853C3AA **SHA256:** 833EFCB939F67F3220E50908DE4E193B60164B77104751F1A8F4094809B15701	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF30045A206E58F1F5.TMP **MD5:** D247417DCA8214FBF0E481663BBECB91 **SHA256:** 042701D506ABEC14BB1C06C439B3D9AAD4515719C61839B471005474CDC90C9C	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF7B5B1F6950497BDF.TMP **MD5:** 009CD1B5009E44C4867642F7929DEAF3 **SHA256:** AE61D198B91F55781776B51E2266AB76F54F1D9A510D1B55AF261F1F7EDF1635	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF90A8320BB01E639E.TMP **MD5:** 9880FE9476E2D89D73497C6A97B27E4D **SHA256:** 94E6330A83B6907685E62DDE3A97CA2040BB67CC584DB5DE1627B29A38870AA6	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DF92C74C48EC0720D3.TMP **MD5:** AFE1A230EBB1B3648F455E6DDFA6E7AB **SHA256:** 772931F62AF79FD8AF732C65D2C1CFB997C11F23D2737D3C0905FB57FCEED1AD	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFAEE7D00393131FAE.TMP **MD5:** 36D8258745AAE819640E5FFC96EB222E **SHA256:** F8119E00C72197B23529F049AE2EC4ABD2FF372C2B5921C4AE38FEA99CDD0033	gmc
488	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\G000GUW2.txt **MD5:** 12CA30E04B6B73D4F6C6E6B7B364EF92 **SHA256:** 0C72C6B82750E187380A9B18AF20F001B2B7A0C3E5CDD028C85EB736335ED0A6	text
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFC403767E291C0FD5.TMP **MD5:** 1D606FCACFFD6E41D373901A584D2DC6 **SHA256:** 387057DB49B8452AE0CC5C482C231BD30DE8F5AAA6C90957D67BFCDBBB1DF401	gmc
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFDC928F1DD42F29A1.TMP	gmc

		MD5: 14F51A7BBB18A2DD7CD5DD8691AFAFB8 **SHA256:** 783F1286FEF8C32F41171A006CE1B7CB44694C4153E4EDE9B5B856ECB16DED3D	
488	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\VT5WAK7O.txt **MD5:** 9E8A138A4C737141AC9D97523C26B9D5 **SHA256:** B372EFD4A4F5A506B964300D545C4F8B4C3390B839F5E9592E26F0CC7659F5A8	text
488	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1AVmX4[1].png **MD5:** EC6AAE2BB7D8781226EA61ADCA8F0586 **SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599	image
2340	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2628	safert44.exe	C:\Users\admin\AppData\Local\Temp\~DFEB4D3ED8A0859392.TMP **MD5:** F6F001B3E8106586F045A7AD07DC3E6D **SHA256:** 2DFAF8112F2489E79DC965499F755B5CD0CCB4769F78D50CBBD0157B93ACA20C	gmc
2340	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63 **MD5:** 63E725FF462F4674431A26DC13037E9D **SHA256:** 6254050FE35765FA8AFD308223EC40465E2451F88951873E4DB0D8A75B306B74	binary
3612	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\927DQ9E5.txt **MD5:** 657BCAD7EE18A7A9AA973B88C04F9C6A **SHA256:** 8EECF83EA7CFD1360636A2302F9D978A501EF747A02A0B37BBAF759EDC6816DE	text
2340	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[5].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2100	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2100	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[3].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
3612	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\1AKmX4[1].png **MD5:** EC6AAE2BB7D8781226EA61ADCA8F0586 **SHA256:** B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599	image
2340	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63 **MD5:** BD9FE8448E8D580C299EE1DB2DA8D0F7 **SHA256:** FC0703829B2C3998FFADC685A439DF4709832B2617787572BB2FC28012CB35F3	der
2100	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[4].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2940	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
1636	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
3452	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2652	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2652	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2172	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[3].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
1636	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[6].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
3452	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[1].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
1636	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[1].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2940	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[1].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2484	real.exe	C:\ProgramData\635616655823194104455652921 **MD5:** — **SHA256:** —	—
2172	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62 **SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
292	F0gel.exe	C:\Users\admin\AppData\LocalLow\K0gL200l8g5q **MD5:** E5EB8572D4F3A59DB6C522CEEADD6D14 **SHA256:** BFCE4D443A6D1FD54F1986B844978D167D9A6B9CEAB0A4B8955676E741477476	image
2484	real.exe	C:\ProgramData\428993262242756330359001 15 **MD5:** 23D08A78BC908C0B29E9800D3D5614E7 **SHA256:** F6BD7DF5DFAE9FD88811A807DBA14085E00C1B5A6D7CC3D06CC68F6015363D59	sqlite
2484	real.exe	C:\ProgramData\softokn3.dll **MD5:** A2EE53DE9167BF0D6C019303B7CA84E5 **SHA256:** 43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083	executable
2484	real.exe	C:\ProgramData\vcruntime140.dll **MD5:** 7587BF9CB4147022CD5681B015183046 **SHA256:** C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D	executable

2484	real.exe	C:\ProgramData\mozglue.dll **MD5:** 8F73C08A9660691143661BF7332C3C27	**SHA256:** 3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD	executable
2484	real.exe	C:\ProgramData\91331742765925554154654500 **MD5:** CC104C4E4E904C3AD7AD5C45FBFA7087	**SHA256:** 321BE844CECC903EF1E7F875B729C96BB3ED0D4986314384CD5944A29A670C9B	sqlite
2484	real.exe	C:\ProgramData\428993262242756330359001l5-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
2484	real.exe	C:\ProgramData\635616655823191410445565292-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
2484	real.exe	C:\ProgramData\64868500522508080018641580 **MD5:** B98E46B09E0B97F0839DC7897AEA7F9A	**SHA256:** 45AF197F8FB09FC1BB9AFF9D76F1E8FF06B5906F6A9E8F4CF2213DE0A8B1213A	sqlite
2312	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\82CB34DD3343FE727DF8890D352E0D8F **MD5:** 087B0A72ED6A273964FFC321E9FA903A	**SHA256:** CB44118D4EB45960FDC9353DA02DED744653E6FA204BC73A782A0CE6B9D14532	binary
2484	real.exe	C:\ProgramData\26976570094230166932633325 **MD5:** D02907BE1C995E1E51571EEDB82FA281	**SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2312	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\82CB34DD3343FE727DF8890D352E0D8F **MD5:** 4C64E06D2B22838CC7D461E6FA5E44C3	**SHA256:** 4B1EEA2238D0EA7FB00F08CF793A38EB3EC27BD673BA684147ECB5A08E8E42DF	der
2484	real.exe	C:\ProgramData\36706815255304117567487677 **MD5:** 49E1E66E8EEFE2553D2ECEC4B7EF1D3E	**SHA256:** A664C359ACE3BFC149323E5403BB7140A84519043BDBA59B064EBC1BDADD32D4	sqlite
2640	jshainx.exe	C:\Users\admin\AppData\Local\Temp\~DFA5A684161B5122D3.TMP **MD5:** 4E4168394459152CB4C08DB102F8B984	**SHA256:** 1E8DE0B16B29379F19197C73070A4D64AED9B732740BB32E3E76B007D2B5E7D2	gmc
2484	real.exe	C:\ProgramData\56243872034996543786113134 **MD5:** B8E63E7225C9F4E0A81371F29D6456D8	**SHA256:** 35A6919CE60EA8E0A44934F8B267BDE2C5A063C2E32F22D34724F168C43150C8	sqlite
2484	real.exe	C:\ProgramData\01401360840793482795822205 **MD5:** D02907BE1C995E1E51571EEDB82FA281	**SHA256:** 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD	sqlite
2484	real.exe	C:\ProgramData\freebl3.dll **MD5:** EF2834AC4EE7D6724F255BEAF527E635	**SHA256:** A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA	executable
2484	real.exe	C:\ProgramData\nss3.dll **MD5:** BFAC4E3C5908856BA17D41EDCD455A51	**SHA256:** E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78	executable
2484	real.exe	C:\ProgramData\msvcp140.dll **MD5:** 109F0F02FD37C84BFC7508D4227D7ED5	**SHA256:** 334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4	executable
2312	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[2].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62	**SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image
2312	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\favicon[7].ico **MD5:** DA597791BE3B6E732F0BC8B20E38EE62	**SHA256:** 5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07	image

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
30	88	13	119

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
292	F0gel.exe	POST	200	45.95.11.158:80	http://45.95.11.158/	unknown	text	5.86 Kb	malicious
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll	unknown	executable	1.95 Mb	malicious
2484	real.exe	GET	200	178.79.242.0:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?cfa4f7c1fc62ba31	DE	compressed	4.70 Kb	whitelisted
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll	unknown	executable	438 Kb	malicious
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll	unknown	executable	612 Kb	malicious
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll	unknown	executable	78.2 Kb	malicious
3616	iexplore.exe	GET	200	178.79.242.0:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?61d9a381893bacd1	DE	compressed	60.3 Kb	whitelisted
3316	iexplore.exe	GET	200	96.16.145.230:80	http://x1.c.lencr.org/	US	der	717 b	whitelisted
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll	unknown	executable	248 Kb	malicious

292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll	unknown	executable	668 Kb	malicious
292	F0gel.exe	GET	200	45.95.11.158:80	http://45.95.11.158/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll	unknown	executable	1.05 Mb	malicious
2484	real.exe	GET	200	192.124.249.36:80	http://ocsp.godaddy.com//MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkF0Qh0pel3lfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D	US	der	1.66 Kb	whitelisted
292	F0gel.exe	POST	200	45.95.11.158:80	http://45.95.11.158/058ce41b4b2c98c84c41e769a6daaa51	unknown	text	8 b	malicious
3616	iexplore.exe	GET	200	178.79.242.0:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?9dcbba5193f362f1	DE	compressed	60.3 Kb	whitelisted
2484	real.exe	GET	200	192.124.249.36:80	http://ocsp.godaddy.com//MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQdI2%2BOBkuXH93foRUj4a7lAr4rGwQUOpqFBxBnKLbv9r0FQW4gwZTaD94CAQc%3D	US	der	1.69 Kb	whitelisted
292	F0gel.exe	POST	200	45.95.11.158:80	http://45.95.11.158/058ce41b4b2c98c84c41e769a6daaa51	unknown	text	8 b	malicious
2484	real.exe	GET	200	192.124.249.36:80	http://ocsp.godaddy.com//MEowSDBGMEQwQjAJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQMK9J47MNIMwojPX%2B2yz8LQsgM4CCQC2T6rhHiP0ng%3D%3D	US	der	1.74 Kb	whitelisted
292	F0gel.exe	POST	200	45.95.11.158:80	http://45.95.11.158/058ce41b4b2c98c84c41e769a6daaa51	unknown	text	8 b	malicious
2100	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQel%3D	US	der	1.47 Kb	shared
2484	real.exe	GET	200	77.91.103.222:80	http://77.91.103.222/1571	RU	text	193 b	malicious
2484	real.exe	GET	—	77.91.103.222:80	http://77.91.103.222/1441467285.zip	RU	—	—	malicious
2340	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQel%3D	US	der	1.47 Kb	shared
3452	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQel%3D	US	der	1.47 Kb	shared
2940	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQel%3D	US	der	1.47 Kb	shared
292	F0gel.exe	POST	200	45.95.11.158:80	http://45.95.11.158/058ce41b4b2c98c84c41e769a6daaa51	unknown	text	8 b	malicious
3452	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	shared
2484	real.exe	POST	—	77.91.103.222:80	http://77.91.103.222/	RU	—	—	malicious
—	—	GET	200	93.184.220.29:80	http://crl3.digicert.com/Omniroot2025.crl	US	der	7.78 Kb	shared
—	—	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	shared
—	—	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	shared

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
—	—	192.168.100.2:53	—	—	—	whitelisted
292	F0gel.exe	45.95.11.158:80	—	—	—	malicious
2484	real.exe	149.154.167.99:443	t.me	Telegram Messenger LLP	GB	malicious
2628	safert44.exe	176.113.115.146:9582	—	Dzinet Ltd.	RU	malicious
2452	namdoitntn.exe	103.89.90.61:34589	—	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	VN	malicious
2484	real.exe	178.79.242.0:80	ctldl.windowsupdate.com	Limelight Networks, Inc.	DE	malicious
3616	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
2640	jshainx.exe	195.54.170.157:16525	—	—	—	malicious
3616	iexplore.exe	178.79.242.0:80	ctldl.windowsupdate.com	Limelight Networks, Inc.	DE	malicious
3316	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
2484	real.exe	192.124.249.36:80	ocsp.godaddy.com	Sucuri	US	suspicious
1904	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
2708	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious

3616	iexplore.exe	96.16.145.230:80	x1.c.lencr.org	Akamai Technologies, Inc.	US	suspicious
3316	iexplore.exe	96.16.145.230:80	x1.c.lencr.org	Akamai Technologies, Inc.	US	suspicious
3612	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
488	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
2044	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
1080	iexplore.exe	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
2312	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2100	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
3452	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2940	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2340	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2312	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2484	real.exe	77.91.103.222:80	—	Foton Telecom CJSC	RU	malicious
2100	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2652	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
2340	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2940	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3452	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
1636	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
—	—	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2172	iexplore.exe	131.253.33.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
—	—	148.251.234.83:443	iplogger.org	Hetzner Online GmbH	DE	malicious
—	—	152.199.19.161:443	r20swj13mr.microsoft.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
—	—	13.107.22.200:443	www.bing.com	Microsoft Corporation	US	whitelisted

DNS requests

Domain	IP	Reputation
www.microsoft.com	—	whitelisted
iplogger.org	148.251.234.83	shared
t.me	149.154.167.99	whitelisted
ctldl.windowsupdate.com	178.79.242.0 178.79.242.128	whitelisted
ocsp.godaddy.com	192.124.249.36 192.124.249.41 192.124.249.23 192.124.249.24 192.124.249.22	whitelisted
x1.c.lencr.org	96.16.145.230	whitelisted
api.bing.com	13.107.5.80	whitelisted
www.bing.com	131.253.33.200 13.107.22.200	whitelisted
ocsp.digicert.com	93.184.220.29	shared
crl3.digicert.com	93.184.220.29	shared
r20swj13mr.microsoft.com	152.199.19.161	whitelisted
iecvlist.microsoft.com	152.199.19.161	whitelisted

Threats

PID	Process	Class	Message
–	–	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in DNS Lookup)
292	F0gel.exe	A Network Trojan was detected	ET TROJAN Win32/RecordBreaker CnC Checkin
292	F0gel.exe	A Network Trojan was detected	ET TROJAN Win32/Kryptik.HQAF Checkin
292	F0gel.exe	A Network Trojan was detected	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
292	F0gel.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
3616	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
3616	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
3316	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
292	F0gel.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host DLL Request
2044	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
2044	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
1080	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
292	F0gel.exe	Misc activity	ET INFO Possible Generic Stealer Sending System Information
3612	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
3612	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
488	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
488	iexplore.exe	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
2484	real.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host ZIP Request
292	F0gel.exe	Misc activity	ET INFO Possible Generic Stealer Sending a Screenshot
2484	real.exe	A Network Trojan was detected	ET TROJAN Arkei/Vidar/Mars Stealer Variant
–	–	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
–	–	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
–	–	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)
–	–	Potential Corporate Privacy Violation	ET POLICY IP Check Domain (iplogger .org in TLS SNI)

Debug output strings

No debug info