ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573
Full analysis:	https://app.any.run/tasks/d61fbea3-64f8-4c2f-a4e9-fe5c802d5609
Verdict:	Malicious activity
Threats:	Formbook
	FormBook is a data stealer that is being distributed as a MaaS. FormBook differs from a lot of competing malware by its extreme ease of use that allows even the unexperienced threat actors to use FormBook virus.
Analysis date:	August 22, 2022 at 10:04:01
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	formbook trojan stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	58A421EB4E04A1A6EE39B159CF63E79D
SHA1:	BA1B78C40A15EFF9EE9B6E82B80F8790C6B1B27B
SHA256:	A9DC9C199D302562CDF1B34D62CAE27450135CB98A86CAB4E1EE0590072B8C2C
SSDEEP:	12288:fc+2ltCNEdmSene/lUrMP6PSzQbT7grJFcuHdl51T9u6mr:fMjdteed7qUflFcu9lyr

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	off
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402
- KB2676562
- KB2685811

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)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
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)

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

Changes the autorun value in the registry
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Drops executable file immediately after starts
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Changes settings of System certificates
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

FORMBOOK detected by memory dumps
chkdsk.exe (PID: 3220)

Connects to CnC server
Explorer.EXE (PID: 636)

FORMBOOK was detected
Explorer.EXE (PID: 636)

SUSPICIOUS

Checks supported languages
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Reads the computer name
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Reads Environment values
chkdsk.exe (PID: 3220)

Loads DLL from Mozilla Firefox
chkdsk.exe (PID: 3220)

Executable content was dropped or overwritten
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Drops a file with a compile date too recent
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Adds / modifies Windows certificates
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

INFO

Reads settings of System Certificates
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Checks supported languages
iexpress.exe (PID: 1668)
chkdsk.exe (PID: 3220)
Firefox.exe (PID: 2388)

Checks Windows Trust Settings
SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe (PID: 2968)

Manual execution by user
chkdsk.exe (PID: 3220)

Reads the computer name
chkdsk.exe (PID: 3220)
iexpress.exe (PID: 1668)
Firefox.exe (PID: 2388)

Static information

TRiD

.exe | Win32 Executable Borland Delphi 7 (68.8)

EXIF

EXE

.exe | Win32 Executable Borland Delphi 6 (27.2)
.exe | Win32 Executable Delphi generic (1.4)
.scr | Windows screen saver (1.3)
.exe | Win32 Executable (generic) (0.4)

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	1992:06:20 00:22:17+02:00
PEType:	PE32
LinkerVersion:	2.25
CodeSize:	381440
InitializedDataSize:	304128
UninitializedDataSize:	0
EntryPoint:	0x5e100
OSVersion:	4
ImageVersion:	0
SubsystemVersion:	4
Subsystem:	Windows GUI
FileVersionNumber:	0.0.0.0
ProductVersionNumber:	0.0.0.0
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Win32
ObjectFileType:	Unknown
FileSubtype:	0
LanguageCode:	English (British)
CharacterSet:	Unicode
Comments:	Tec leader
FileDescription:	Tec leader
LegalCopyright:	Copyright ©2013 All Rights Reserved.
CompanyName:	
HomePage:	
Author:	WlxLife

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	19-Jun-1992 22:22:17
Detected languages:	English - United Kingdom
	English - United States
Comments:	Tec leader
FileDescription:	Tec leader
LegalCopyright:	Copyright ©2013 All Rights Reserved.
CompanyName:	
HomePage:	
Author:	WlxLife

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	0x0005D13C	0x0005D200	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.55532
DATA	0x0005F000	0x00001354	0x00001400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.30445
BSS	0x00061000	0x00000DB9	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x00062000	0x00002264	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.88849

.tls	0x00065000	0x00000010	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00066000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.20692
.reloc	0x00067000	0x00006938	0x00006A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.66488
.rsrc	0x0006E000	0x00040000	0x00040000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	7.22263

Resources

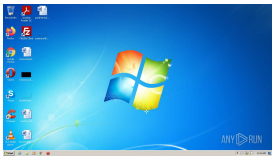
Title	Entropy	Size	Codepage	Language	Type
1	3.24482	544	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.91604	308	UNKNOWN	UNKNOWN	RT_CURSOR
51	2.9114	1024	UNKNOWN	UNKNOWN	RT_ICON
53	5.06437	4096	UNKNOWN	UNKNOWN	RT_ICON
55	4.66504	2048	UNKNOWN	UNKNOWN	RT_ICON
57	4.53279	17408	UNKNOWN	UNKNOWN	RT_ICON
59	4.5687	4608	UNKNOWN	UNKNOWN	RT_ICON
61	4.08707	1536	UNKNOWN	UNKNOWN	RT_ICON
4081	3.31892	636	UNKNOWN	UNKNOWN	RT_STRING
4082	3.24878	504	UNKNOWN	UNKNOWN	RT_STRING
4083	3.16232	284	UNKNOWN	UNKNOWN	RT_STRING
4084	3.22813	768	UNKNOWN	UNKNOWN	RT_STRING
4085	2.99542	192	UNKNOWN	UNKNOWN	RT_STRING
4086	3.12805	252	UNKNOWN	UNKNOWN	RT_STRING
4087	3.25129	584	UNKNOWN	UNKNOWN	RT_STRING
4088	3.20722	1016	UNKNOWN	UNKNOWN	RT_STRING
4089	3.18654	864	UNKNOWN	UNKNOWN	RT_STRING
4090	3.23478	996	UNKNOWN	UNKNOWN	RT_STRING
4091	3.23259	564	UNKNOWN	UNKNOWN	RT_STRING
4092	3.00616	236	UNKNOWN	UNKNOWN	RT_STRING
4093	3.22288	436	UNKNOWN	UNKNOWN	RT_STRING
4094	3.19757	996	UNKNOWN	UNKNOWN	RT_STRING
4095	3.26686	856	UNKNOWN	UNKNOWN	RT_STRING
4096	3.18591	692	UNKNOWN	UNKNOWN	RT_STRING
32761	1.83876	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32762	1.91924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32763	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32764	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32765	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32766	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32767	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
BBABORT	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBALL	3.16995	484	UNKNOWN	UNKNOWN	RT_BITMAP
BBCANCEL	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBCLOSE	3.68492	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBHELP	2.88085	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBIGNORE	3.29718	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBNO	3.58804	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBOK	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP

BBRETRY	3.53344	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBYES	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP
PREVIEWGLYPH	2.85172	232	UNKNOWN	English - United States	RT_BITMAP
DLGTEMPLATE	2.5627	82	UNKNOWN	UNKNOWN	RT_DIALOG
ASS	7.40249	209583	UNKNOWN	English - United States	RT_RCDATA
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
PACKAGEINFO	5.26778	896	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.58795	90	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

advapi32.dll
comctl32.dll
gdi32.dll
kernel32.dll
ole32.dll
oleaut32.dll
user32.dll
version.dll

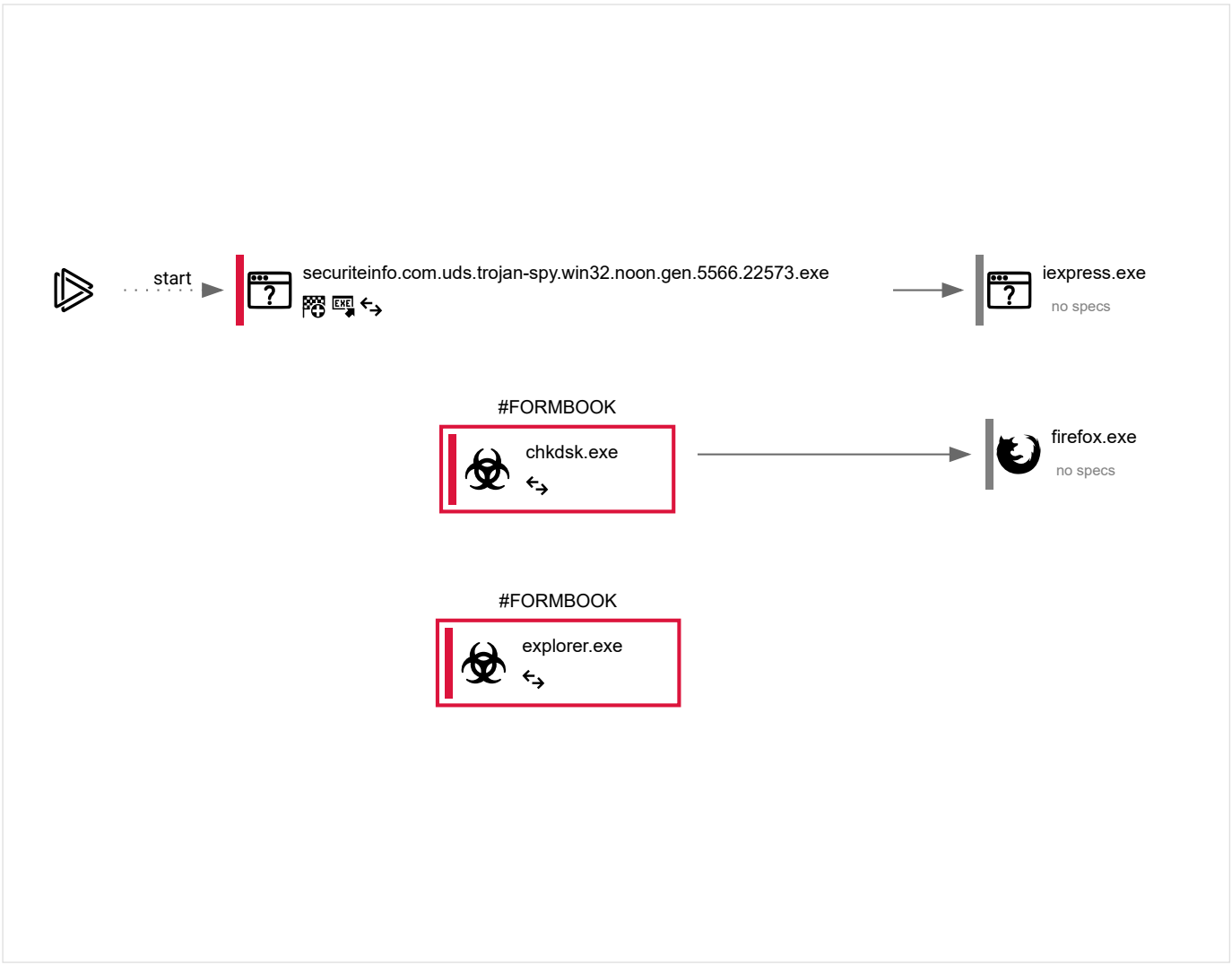
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
39	5	3	0

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
2968	"C:\Users\admin\AppData\Local\Temp\SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe"	C:\Users\admin\AppData\Local\Temp\SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe		Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:	Tec leader	**Exit code:**	0

1668	"C:\Windows\System32\iexpress.exe"	C:\Windows\System32\iexpress.exe	—	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Wizard
Exit code:	0	**Version:**	11.00.9600.16428 (winblue_gdr.131013-1700)

3220	"C:\Windows\System32\chkdsk.exe"	C:\Windows\System32\chkdsk.exe		Explorer.EXE

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Check Disk Utility
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

636	C:\Windows\Explorer.EXE	C:\Windows\Explorer.EXE		—

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Explorer
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

2388	"C:\Program Files\Mozilla Firefox\Firefox.exe"	C:\Program Files\Mozilla Firefox\Firefox.exe	—	chkdsk.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	MEDIUM	**Description:**	Firefox
Exit code:	0	**Version:**	83.0

Registry activity

Total events	Read events	Write events	Delete events
5 654	5 584	67	3

Modification events

(PID) Process: (636) Explorer.EXE
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0
Operation: write
Name: CheckSetting
Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000F51F4123F4CE8748A0D775775B8EDD5A000000000200000000001066000000010000200000000168BD4A8A58D67F376D2CE537B7FD014C6F588CE5D1F933E7C2DB27C4462C8C9000000000E8000000002000020000000002DD869AE0B31871F1DA9A13F59FFC5CB977E6B9CAF5BDEE99DF1E1344D48354B3000000053352FE2D5739B71B4B789617EF3A2F5DCC7F561E17D1C4375D2A57F3F6FE7B944EC98219DE6E6C71F06B5121C19A29C400000004EC6F7EB971BC1ADE3C1358AB571312D9B882F5D876EC19DA9F64C2EC8C76DCD185498E30D796F6385D2635E53FFABE6BC117E632481824874E4275D45742221

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write
Name: ProxyEnable
Value: 0

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 460000003B0100000900000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000100000002000000C0A80164000

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write
Name: CachePrefix
Value:

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write
Name: CachePrefix
Value: Cookie:

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write
Name: CachePrefix
Value: Visited:

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: ProxyBypass
Value: 1

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.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: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: DCF08A79E0B5D801

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.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: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.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: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.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: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: DCF08A79E0B5D801

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.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: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: write **Name:** Blob

Value: 040000000100000010000000E4A68AC854AC5242460AFD72481B2A44530000000100000040000000303E301F06096086480186FD6C0201301230100 60A2B0601040182373C0101030200C0301B060567810C01033012301006 0A2B0601040182373C0101030200C00F000000010000002000000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000001000000007DC30BC974695560A2F0090A6545556C14000000010000001400000004E2254201895E6E36EE60FFAFAB912ED06178F396200000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B060105050703020608 2B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820838E30820276A00302010202100033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530130603550400A130C44696769436572742496E633119301706035504 0B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D313330383031313230303030305A170D333830313131353132303030305A3061310B30090603550406130255533115301306035504 0A130C44696769436572742496E633119301706035504 0B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732308201223 00D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B13383298502030100 01A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F97050704741115 7194EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: delete key **Name:** (default)

Value:

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: write **Name:** Blob

Value: 5C000000010000000400000000800005300000001000000400000003 03E301F06096086480186FD6C0201301230100 60A2B0601040182373C0101030200C0301B060567810C01033012301006 0A2B0601040182373C0101030200C00F000000010000002000000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000001000000007DC30BC974695560A2F0090A6545556C14000000010000001400000004E2254201895E6E36EE60FFAFAB912ED06178F396200000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B060105050703020608 2B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820838E30820276A00302010202100033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530130603550400A130C44696769436572742496E633119301706035504 0B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D313330383031313230303030305A3061310B30090603550406130255533115301306035504 0A130C44696769436572742496E633119301706035504 0B13107777772E6469676963657274 2E636F6D3

120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B
26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0C
B948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3
496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F6731
4143D4676C387148921344DAF0F450CA649A1BABB9CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551
D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB0
5F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5
D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F970507047411157194EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F3
1445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB335
37E532B6

(PID) Process: (2968) SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** Bfpwlhgak
Value: C:\Users\Public\Libraries\kaghlwpfB.url

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003C0100000900000000000000000000000000000000000004000000000000000C0E333BBEAB1D30100000000000000000000000000010000000200000C0A864AF0000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3220) chkdsk.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: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: DCF08A79E0B5D801

(PID) Process: (3220) chkdsk.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: (3220) chkdsk.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: (3220) chkdsk.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: (3220) chkdsk.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 0E22198CE0B5D801

(PID) Process: (3220) chkdsk.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:	(3220) chkdsk.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:	(3220) chkdsk.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	0E22198CE0B5D801		
(PID) Process:	(3220) chkdsk.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	delete value	**Name:**	WpadDetectedUrl
Value:			

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	4	3	2

Dropped files

PID	Process	Filename	Type
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\9N0YM79B.txt **MD5:** 34B01D29F52C9B146EDA9F9DDFF210F4 **SHA256:** E060FEE734E8EC49F0F306066D906886A3D60AED2346A2C45DA4FD90B4F423C1	text
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 7B8D64344FC2A4BA66B679790001CDE3 **SHA256:** 6D1554277525411224185 9F74176F572B9D2967B456A234B01E5C1A733DBF466	binary
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 75E9E37B2AA8E2EF5E013EE4E603FCA5 **SHA256:** B59FAB5E6A633CF4F33474B96DC0398900DCF1C57E33AE6F858DCA2BC9C39169	der
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** 5D8114C0D7441F143C5BDEA775C5F660 **SHA256:** A91CFF0189272BCB8B350B256C4CA7AFF7295AEE7B0CFB84D465BA419091BD50	binary
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** 667B37D7F8D0A53855894A2706347B76 **SHA256:** C4C1D5EB3CA6EABDC53925E4C5B33EB6157D5855510117A85D00C8BA1B3C7D77	binary
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** 5279CC47C895B4647090B81DF1F7D18C **SHA256:** 18ACCA8C29A35998EDD804D521D3C38DEA839F17A4C8DCFCE9B0B6BDC4F9483A	der
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\Public\Libraries\kaghlwpfB.url **MD5:** E452D8D8C3F294C33E7723F925F87F50 **SHA256:** CC0A9280AE49DFAFCA5D91FA273FDBDC917CA22242320D633BB92A43A03373BC	text
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\YYOHVRPI.txt **MD5:** 9BF8EBB7D35FCB8915DBC8B667693856 **SHA256:** 9E73A80182DB9C70ECE9CDAC0E1AE198ADAA306ECCAC5902FA33B764B016B6D2	text
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	C:\Users\Public\Libraries\Bfpwlhgak.exe **MD5:** 58A421EB4E04A1A6EE39B159CF63E79D **SHA256:** A9DC9C199D302562CDF1B34D62CAE27450135CB98A86CAB4E1EE0590072B8C2C	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
30	32	16	61

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2968	SecuriteInfo.com.UDS.Trojan-	GET	200	8.253.204.249:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a2f0da7bc9e00d08	US	compressed	4.70 Kb	whitelisted

	Spy.Win32.Noon.gen.5566.22573.exe								
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	US	der	1.47 Kb	whitelisted
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc%3D	US	der	471 b	whitelisted
636	Explorer.EXE	GET	200	216.40.34.41:80	http://www.webuildamerica.org/uh89/?mnBXn=GDZyk+/0rQFRyZJT8mFE8WdhUpu6+cY9V8ZPDMouqVYkLOOBw/lfg1oCQg5XDFdLs/vlUybuSTpVR4TNDo+GY0n8Q4mlvMAPnK/BY9s=&2d=2d6HZl8xuhT8rJ4	CA	html	5.84 Kb	malicious
3220	chkdsk.exe	GET	404	45.33.6.223:80	http://www.sqlite.org/2014/sqlite-dll-win32-x86-3080500.zip	US	–	–	whitelisted
636	Explorer.EXE	POST	503	162.215.226.7:80	http://www.madhavroopa.com/uh89/	US	html	190 b	malicious
636	Explorer.EXE	POST	503	162.215.226.7:80	http://www.madhavroopa.com/uh89/	US	html	190 b	malicious
636	Explorer.EXE	GET	200	162.215.226.7:80	http://www.madhavroopa.com/uh89/?mnBXn=eu577vZLAHTTqfp8x6aCxG2K0HxJoPwaiVa8tHkzCEEFQmvHg+s28+dCGT9ravB3FNgVzpYLAtaC+xtudYfSeqAl1J3xv7X4DxxWvc4=&2d=2d6HZl8xuhT8rJ4	US	html	378 b	malicious
636	Explorer.EXE	POST	502	185.151.30.159:80	http://www.wplogsnag.com/uh89/	GB	html	107 b	malicious
636	Explorer.EXE	POST	502	185.151.30.159:80	http://www.wplogsnag.com/uh89/	GB	html	107 b	malicious
636	Explorer.EXE	POST	403	199.15.163.138:80	http://www.organikaserver.com/uh89/	US	html	146 b	malicious
636	Explorer.EXE	GET	404	185.151.30.159:80	http://www.wplogsnag.com/uh89/?mnBXn=bGZHcbKqjx03qByRqa+Xeqd5TzoTQqjmM0oKDHpM//43AspXjcYtcHiil8ISpLgsXVYJvY8UKT7+lf5F1tl1C5QdsIR/OYw2RfMfP8=&2d=2d6HZl8xuhT8rJ4	GB	html	196 b	malicious
636	Explorer.EXE	POST	403	199.15.163.138:80	http://www.organikaserver.com/uh89/	US	html	146 b	malicious
636	Explorer.EXE	GET	–	199.15.163.138:80	http://www.organikaserver.com/uh89/?mnBXn=RMgfVe8lo07VSjysjilu7KOgzDPqPF9yO+fFR+CTNcYe/7rgMSjWj+myYPdWTJxUawdajoxio/FmKVWfoYU78mlufVpLbsiHiB+MwVg=&2d=2d6HZl8xuhT8rJ4	US	–	–	malicious
636	Explorer.EXE	POST	200	199.59.243.220:80	http://www.ennedy.online/uh89/	US	html	1.31 Kb	malicious
636	Explorer.EXE	POST	200	199.59.243.220:80	http://www.ennedy.online/uh89/	US	html	4.61 Kb	malicious
636	Explorer.EXE	GET	200	199.59.243.220:80	http://www.ennedy.online/uh89/?mnBXn=VG3wVN1kiO5xVGJFtD7IFpqcVMm2GzrDRu7tV1W/8pOEpKriwkMV8L1Cg1/UaFcviDSeRToh1yQy0s3ab3ESSId+rF3ZfAN4TEdtqAc=&2d=2d6HZl8xuhT8rJ4	US	html	1.33 Kb	malicious
636	Explorer.EXE	POST	302	185.83.214.222:80	http://www.kurapharm.com/uh89/	PT	–	–	malicious
636	Explorer.EXE	POST	302	185.83.214.222:80	http://www.kurapharm.com/uh89/	PT	–	–	malicious
636	Explorer.EXE	GET	302	185.83.214.222:80	http://www.kurapharm.com/uh89/?mnBXn=tRaOZTjCNp8H+eV9juu7rw5j23zPI5f1+UpXIZ0fm8XLoTfvdWcaB6AfAj8sb5HMNG/8g6j1PwTUBiYip3MLuXdM3x5Kwc1ILGMdLpc=&2d=2d6HZl8xuhT8rJ4	PT	–	–	malicious
636	Explorer.EXE	POST	–	103.221.221.20:80	http://www.tuixachchangbom.com/uh89/	VN	–	–	malicious
636	Explorer.EXE	POST	–	103.221.221.20:80	http://www.tuixachchangbom.com/uh89/	VN	–	–	malicious
636	Explorer.EXE	GET	301	103.221.221.20:80	http://www.tuixachchangbom.com/uh89/?mnBXn=lB8nGdXHL324i0PTFL7+a/dkLueqE/oqtODfwq8Su3OPCAdjDq/0NVrhm1lvP4/3wQcXu9oTPAWSpT4WJpu8gN3kAZzVor2dKTN+lSQ=&2d=2d6HZl8xuhT8rJ4	VN	–	–	malicious
636	Explorer.EXE	POST	200	45.33.30.197:80	http://www.magadirect.co.uk/uh89/	US	html	6.74 Kb	malicious
636	Explorer.EXE	GET	404	45.33.30.197:80	http://www.magadirect.co.uk/uh89/?mnBXn=lpByS040JnK4lrlaifLZse5d6ollb/e3u/OTRvmlt21Tl8MPMkpuqNS7AduDhewzjm16x95vld+a07lRo78nzGvN3wFZHqK1x3B8toA=&2d=2d6HZl8xuhT8rJ4	US	html	175 b	malicious
636	Explorer.EXE	POST	–	161.132.46.23:80	http://www.asistenciadepersonal.com/uh89/	PE	–	–	malicious
636	Explorer.EXE	POST	200	45.33.30.197:80	http://www.magadirect.co.uk/uh89/	US	html	6.74 Kb	malicious
636	Explorer.EXE	POST	–	161.132.46.23:80	http://www.asistenciadepersonal.com/uh89/	PE	–	–	malicious
636	Explorer.EXE	POST	200	199.59.243.220:80	http://www.lacasax.site/uh89/	US	html	1.31 Kb	malicious
636	Explorer.EXE	GET	–	161.132.46.23:80	http://www.asistenciadepersonal.com/uh89/?mnBXn=eRBuRpPY+DTcUvw8I20b4DD0VTwejF18pY3Eyw/kJktRmDA1zk5tt2W8JavNFwIg/tvLPlWGZvXT7PbubXUAC+SupYvo/sskCfqZCKA=&2d=2d6HZl8xuhT8rJ4	PE	–	–	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2968	SecuriteInfo.com.UDS.Trojan-	8.253.204.249:80	ctldl.windowsupdate.com	Global Crossing	US	suspicious

	Spy.Win32.Noon.gen.5566.22573.exe					
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	13.107.42.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3220	chkdsk.exe	45.33.6.223:80	www.sqlite.org	Linode, LLC	US	suspicious
2968	SecuriteInfo.com.UDS.Trojan-Spy.Win32.Noon.gen.5566.22573.exe	13.107.42.12:443	nr3baq.dm.files.1drv.com	Microsoft Corporation	US	suspicious
636	Explorer.EXE	216.40.34.41:80	www.webuildamerica.org	Tucows.com Co.	CA	malicious
636	Explorer.EXE	162.215.226.7:80	www.madhavroopa.com	Unified Layer	US	malicious
636	Explorer.EXE	185.151.30.159:80	www.wplogsnag.com	Node4 Limited	GB	malicious
—	—	185.151.30.159:80	www.wplogsnag.com	Node4 Limited	GB	malicious
636	Explorer.EXE	199.59.243.220:80	www.ennedy.online	—	US	malicious
636	Explorer.EXE	185.83.214.222:80	www.kurapharm.com	—	PT	malicious
636	Explorer.EXE	199.15.163.138:80	www.organikaserver.com	—	US	malicious
636	Explorer.EXE	103.221.221.20:80	www.tuixachchangbom.com	The Corporation for Financing & Promoting Technology	VN	malicious
636	Explorer.EXE	161.132.46.23:80	www.asistenciadepersonal.com	Red Cientifica Peruana	PE	malicious
636	Explorer.EXE	45.33.30.197:80	www.magadirect.co.uk	Linode, LLC	US	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.42.13	shared
ctldl.windowsupdate.com	8.253.204.249 67.27.235.254 67.26.75.254 8.253.204.120 8.241.123.126	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
nr3baq.dm.files.1drv.com	13.107.42.12	unknown
www.webuildamerica.org	216.40.34.41	malicious
www.sqlite.org	45.33.6.223	whitelisted
www.madhavroopa.com	162.215.226.7	malicious
www.wplogsnag.com	185.151.30.159	malicious
www.organikaserver.com	199.15.163.138	malicious
www.ennedy.online	199.59.243.220	malicious
www.kurapharm.com	185.83.214.222	malicious
www.tuixachchangbom.com	103.221.221.20	malicious
www.magadirect.co.uk	45.33.30.197 173.255.194.134 72.14.185.43 45.33.18.44 45.33.23.183 45.33.20.235 198.58.118.167 96.126.123.244 45.79.19.196 45.56.79.23 45.33.2.79 72.14.178.174	malicious
www.asistenciadepersonal.com	161.132.46.23	malicious
www.lacasax.site	199.59.243.220	malicious

Threats

PID	Process	Class	Message
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)

636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
636	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body

Debug output strings

No debug info