



General Info

File name:	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe
Full analysis:	https://app.any.run/tasks/c9dc3f98-f9f5-49f1-b7a6-30b4a2c826f1
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 18, 2022 at 12:09:50
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	installerformbooktrojanstealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	64B12EA2B1BFBF71CD0AB82DAE4A2A2B
SHA1:	3DD4C91BD3891A987BB14E553645BE0DCE769BE3
SHA256:	EE2CED66ADECCFE45722C49EFD8B99FD032D0426FF74CD10FC1E182521431404
SSDEEP:	12288:vGJufSEN4Nb+cuuUkyFnhPTWT50WZdavN2HuEGlemz5z:vGqN4Nb9SmL4Fvz

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)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	KB4532945
	KB4536952
	KB4567409
	KB958488
	KB976902
	KB982018
	LocalPack AU Package
	LocalPack CA Package
	LocalPack GB Package
	LocalPack US Package
	LocalPack ZA Package
	Package 21 for KB2984976
	Package 38 for KB2984976
	Package 45 for KB2984976
	Package 59 for KB2984976
	Package 7 for KB2984976
	Package 76 for KB2984976
	PlatformUpdate Win7 SRV08R2 Package TopLevel
	ProfessionalEdition
	RDP BlueIP Package TopLevel
	RDP WinIP Package TopLevel
	RollupFix
	UltimateEdition
	WUClient SelfUpdate ActiveX
	WUClient SelfUpdate Aux TopLevel
	WUClient SelfUpdate Core TopLevel
	WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Changes settings of System certificates 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)	Reads the computer name 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)	Reads the computer name calc.exe (PID: 3400) rundll32.exe (PID: 1808) Firefox.exe (PID: 2852)
FORMBOOK detected by memory dumps rundll32.exe (PID: 1808)	Checks supported languages 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)	Reads settings of System Certificates 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)
Connects to CnC server Explorer.EXE (PID: 1176)	Reads Environment values rundll32.exe (PID: 1808)	Checks supported languages calc.exe (PID: 3400) rundll32.exe (PID: 1808) Firefox.exe (PID: 2852)
FORMBOOK was detected Explorer.EXE (PID: 1176)	Adds / modifies Windows certificates 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)	Manual execution by user rundll32.exe (PID: 1808)
	Loads DLL from Mozilla Firefox rundll32.exe (PID: 1808)	Checks Windows Trust Settings 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe (PID: 1448)

Static information

TRiD

.exe		InstallShield setup (53.2)
.exe		Win32 Executable Delphi generic (17.5)
.scr		Windows screen saver (16.1)
.exe		Win32 Executable (generic) (5.5)
.exe		Win16/32 Executable Delphi generic (2.5)

EXIF

EXE	
Author:	BlueLife
HomePage:	www.scdum.org
CompanyName:	www.sc.org
LegalCopyright:	Copyright ©2013 www.sordum.org All Rights Reserved.

FileDescription:Microsoft Word CIX

Comments:Microsoft Word

FileVersion:1.2.0.0

CharacterSet:Unicode

LanguageCode:English (British)

FileSubtype:0

ObjectFileType:Unknown

FileOS:Win32

FileFlags:(none)

FileFlagsMask:0x003f

ProductVersionNumber:1.2.0.0

FileVersionNumber:1.2.0.0

Subsystem:Windows GUI

SubsystemVersion:4

ImageVersion:0

OSVersion:4

EntryPoint:0x5dfac

UninitializedDataSize:0

InitializedDataSize:332288

CodeSize:380928

LinkerVersion:2.25

PType: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 Kingdom

English - United States

FileVersion:1.2.0.0

Comments:Microsoft Word

FileDescription:Microsoft Word CIX

LegalCopyright:Copyright ©2013 www.sordum.org All Rights Reserved.

CompanyName:www.sc.org

HomePage:www.scdum.org

Author:BlueLife

DOS Header

Magic number:MZ

Bytes on last page of file:0x002E

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	0x0005CFF4	0x0005D000	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.5371
DATA	0x0005E000	0x000011FC	0x00001200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.18236
BSS	0x00060000	0x00000D29	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x00061000	0x00002306	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.9643
.tls	0x00064000	0x00000010	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0

.rdata	0x00065000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.20692
.reloc	0x00066000	0x000068BC	0x00006A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.67397
.src	0x0006D000	0x00046E30	0x00047000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.16003

Resources

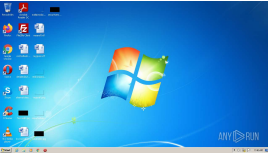
Title	Entropy	Size	Codepage	Language	Type
1	3.39217	692	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.91604	308	UNKNOWN	UNKNOWN	RT_CURSOR
65	2.23329	16936	UNKNOWN	UNKNOWN	RT_ICON
66	2.22424	14920	UNKNOWN	UNKNOWN	RT_ICON
71	3.09784	1720	UNKNOWN	UNKNOWN	RT_ICON
72	3.10512	1128	UNKNOWN	UNKNOWN	RT_ICON
4081	3.24693	1084	UNKNOWN	UNKNOWN	RT_STRING
4082	3.28456	460	UNKNOWN	UNKNOWN	RT_STRING
4083	3.25026	392	UNKNOWN	UNKNOWN	RT_STRING
4084	3.21127	432	UNKNOWN	UNKNOWN	RT_STRING
4085	3.24022	536	UNKNOWN	UNKNOWN	RT_STRING
4086	3.1103	236	UNKNOWN	UNKNOWN	RT_STRING
4087	3.243	628	UNKNOWN	UNKNOWN	RT_STRING
4088	3.20722	1016	UNKNOWN	UNKNOWN	RT_STRING
4089	3.16119	888	UNKNOWN	UNKNOWN	RT_STRING
4090	3.24134	1000	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
BBOKK	5.48978	187864	UNKNOWN	English - United States	RT_BITMAP
CL_MPBACK	3.02457	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPEJECT	2.84895	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPNEXT	2.84479	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPPAUSE	3.11386	232	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPPLAY	2.53843	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPPREV	2.69381	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPRECORD	3.00173	208	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPSTEP	2.82596	296	UNKNOWN	UNKNOWN	RT_BITMAP
CL_MPSTOP	2.71401	296	UNKNOWN	UNKNOWN	RT_BITMAP

DI_MPBACk	2.6952	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPEJECT	2.54697	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPNext	2.58769	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPPAUSE	2.65923	232	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPPLAY	2.28924	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPPREV	2.69381	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPRECORD	2.69136	208	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPSTEP	2.56887	296	UNKNOWN	UNKNOWN	RT_BITMAP
DI_MPSTOP	2.38849	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPBACk	2.68396	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPEJECT	2.47619	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPNext	2.49139	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPPAUSE	2.81646	232	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPPLAY	2.18621	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPPREV	2.35464	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPRECORD	2.50832	208	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPSTEP	2.47257	296	UNKNOWN	UNKNOWN	RT_BITMAP
EN_MPSTOP	2.2127	296	UNKNOWN	UNKNOWN	RT_BITMAP
ALOTRO	6.25231	40774	UNKNOWN	English - United States	RT_RCdATA
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCdATA
PACKAGEINFO	5.26161	728	UNKNOWN	UNKNOWN	RT_RCdATA
TFRMMAITRE	5.50769	1083	UNKNOWN	UNKNOWN	RT_RCdATA
MAINICON	2.83146	62	UNKNOWN	UNKNOWN	RT_Group_ICON

Imports

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

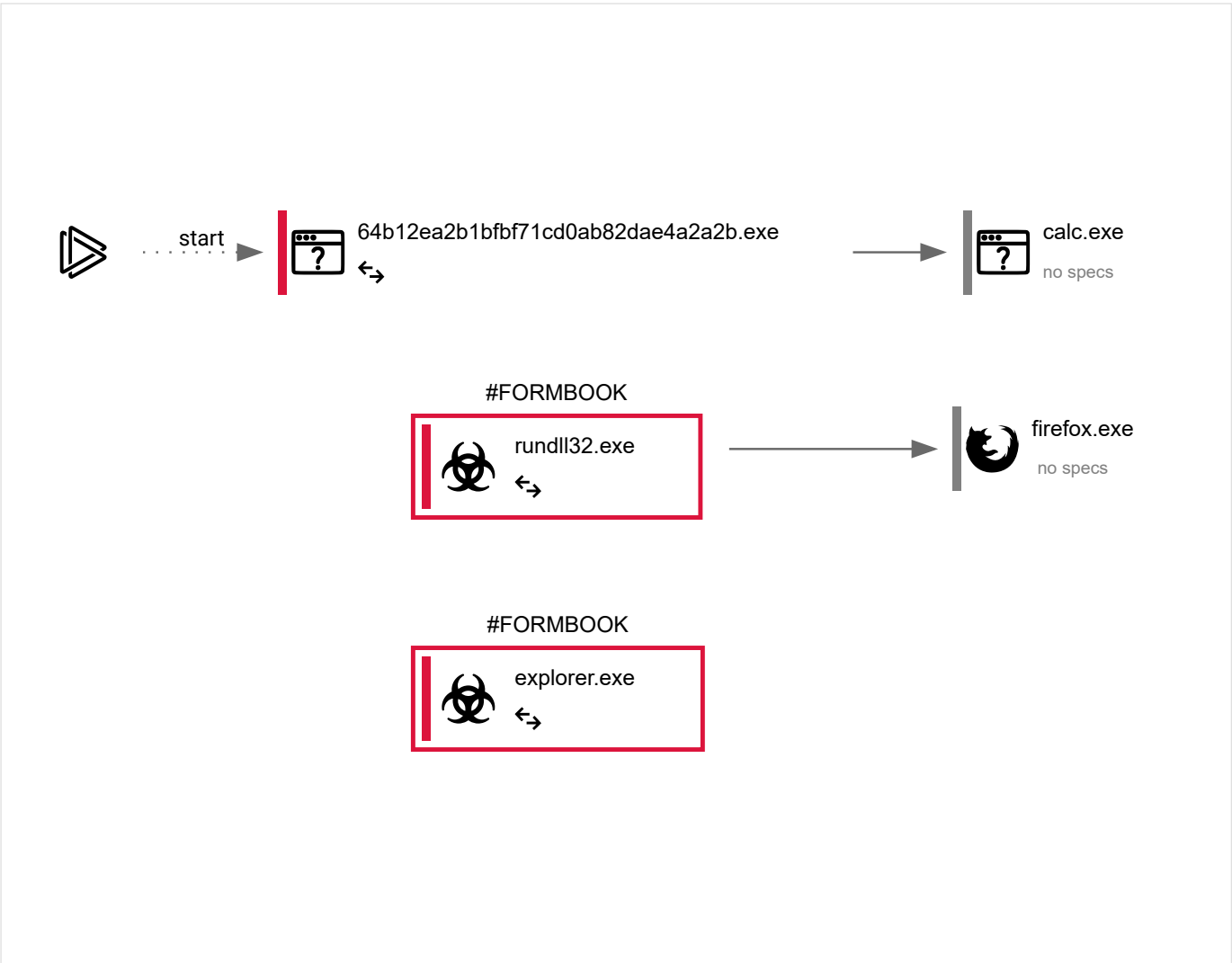
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
37	5	3	0

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
1448	"C:\Users\admin\AppData\Local\Temp\64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe"	C:\Users\admin\AppData\Local\Temp\64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe ↔		Explorer.EXE
Information				
User:	admin	Company:	www.sc.org	
Integrity Level:	MEDIUM	Description:	Microsoft Word CIX	
Exit code:	0	Version:	1.2.0.0	

3400

"C:\Windows\System32\calc.exe"

C:\Windows\System32\calc.exe

←

64b12ea2b1bfb71cd0ab82dae4a2a2b.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Windows Calculator

Exit code:

0


Version:

6.1.7600.16385 (win7_rtm.090713-1255)

1808

"C:\Windows\System32\rundll32.exe"

C:\Windows\System32\rundll32.exe

↔ 

Explorer.EXE

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Windows host process (Rundll32)


Version:

6.1.7600.16385 (win7_rtm.090713-1255)

1176

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)

2852

"C:\Program Files\Mozilla Firefox\Firefox.exe"

C:\Program Files\Mozilla Firefox\Firefox.exe

—

rundll32.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
5 473	5 404	66	3

Modification events

[illegible]

<div>Operation:write</div> <div>Value:1</div>	<div>Name:IntranetName</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:1</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap</div> <div>Name:UNCAsIntranet</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:0</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap</div> <div>Name:AutoDetect</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:1</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}</div> <div>Name:WpadDecisionReason</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:02B4E96DCDB2D801</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}</div> <div>Name:WpadDecisionTime</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:0</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}</div> <div>Name:WpadDecision</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:Network 4</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}</div> <div>Name:WpadNetworkName</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:1</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff</div> <div>Name:WpadDecisionReason</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:02B4E96DCDB2D801</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff</div> <div>Name:WpadDecisionTime</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:0</div>	<div>Key:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff</div> <div>Name:WpadDecision</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:en-US</div>	<div>Key:HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E</div> <div>Name:LanguageList</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:0400000001000000010000000E4A68AC854AC5242460AFD72481B2A4453000000010000004000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0F00000001000000200000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A303000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D00000001000000010000007DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E636EE60FFAFA8912ED06178F39620000000100000020000000CB3CCB876031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5A81CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AEC13734AD8CA0B8090000001000000340000000303206082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030106082B060105050703082000000010000000920300003082038E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9826890AD4A75FF46BA210A088DF51954C9FB88BDF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A988AD3AD499A48625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9BA4E992326BB5F357E85D1BCD8C1DA895049549F3352D96E3496DD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101F40403020186301D0603551D0E041604144E2254201895E636EE60FFAFA8912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B447FE9BEDB2B17DFB05F73772A3213398167428423F2456735CE88BFF8FB0610C34A4AE204C84C6DBF835E176D9DFA642BB874408867F3674245ADA6C0D145935BDF249DD861FC9B30D472A30992FB85CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F70507047411157194EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044FEA879532930EFE53462AC9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED0C3921BE5775F76EE3C8DC45D56BA2D966EB33537E532B6</div>	<div>Key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4</div> <div>Name:Blob</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:delete key</div> <div>Value:</div>	<div>Key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4</div> <div>Name:(default)</div>
<div>(PID) Process:(1448) 64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe</div> <div>Operation:write</div> <div>Value:05C00000001000000040000000080000530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C00F00000001000000200000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A303000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D00000001000000010000007DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E636EE60FFAFA8912ED06178F39620000000100000020000000CB3CCB876031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5A81CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000100000014C3BD3549EE225AEC13734AD8CA0B80900000001000000340000000303206082B0601050507030306082B0601050507030306082B0601050507030406082B060105050703082000000010000000920300003082038E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061</div>	

https://any.run/report/ee2ced66adeccfe45722c49efd8b99fd032d0426ff74cd10fc1e182521431404/c9dc3f98-f9f5-49f1-b7a6-30b4a2c826f1?_gl=... 11/15

(PID) Process: (1808) rundll32.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write	Name: WpadDecisionTime
Value: 3D90387FCDB2D801	
(PID) Process: (1808) rundll32.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
0	4	2	2

Dropped files

PID	Process	Filename	Type
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: 7FE74460AA8F651114972A90A238E06D SHA256: A236379906C8D4E38B2C1661AA457A0849FD016686CE7231F231A6830E5E283F	binary
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957B MD5: 503923D3E2FC05A33C4D86B060ACF3F1 SHA256: 0551D3781EA5E8111A7C1F15D5F169FEA2C772FE6070388D1C4955CF8874E8E9	der
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957 MD5: 72A005C1B95B102810A50821D23E6D3C SHA256: D21696B382F83639E7984261CEF7B5ECD1288977336CC8D50D0E1E494DB6DDB91	binary
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757 MD5: C104FFAC3C493E8FC459AC382DCB6359 SHA256: D447A21FDA22F6B8AC5B111B38288905505CDD6A23B940888DFCA2832D0FDA4	der
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\8K43S0SC.txt MD5: FFFAA679D519FBD219BE5033CFC5EB52 SHA256: 96C26661FD1027C27342A32FD931468F3685189901B4FAC06ED6FE8A05CCEAAC	text
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A275 MD5: 522D18BD04C02ECDD58B80FFC3FC13E4 SHA256: D802BCFD7CF64AAA41E17E5A3239B14F760D91493C774D755D25D59B91FD4A87	binary
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\PATCGJPR.txt MD5: 64DFAB958BE928D480CFE820BADFBE51 SHA256: 7BE7786C001D4CE28F67001A29E20C67AACC2361A9619399354AE652BB6EE0EA	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
23	25	13	61

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	GET	200	93.184.221.240:80	http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b3113470aed3406f	US	compressed	4.70 Kb	whitelisted
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.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
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	US	der	471 b	whitelisted
1176	Explorer.EXE	GET	404	2.57.90.16:80	http://www.gabrielasocialmedia.com/bgng/?Cd-de=CXaLeFo&x46HZlcx=SoxYW8ZfcNN1rN207X2Kss1PATPhnikH1T2RjM9kN3lqnLTUDfZsq4P1HFc8GAiAlIRIZ+i6HXVeOJ0btAsfvGHsrEHjdEXdn79Y4=	unknown	html	146 b	malicious
1176	Explorer.EXE	POST	—	72.52.228.217:80	http://www.somalixpogroup.com/bgng/	US	—	—	malicious
1808	rundll32.exe	GET	404	45.33.6.223:80	http://www.sqlite.org/2014/sqlite-dll-win32-x86-3080400.zip	US	—	—	whitelisted
1176	Explorer.EXE	POST	404	72.52.228.217:80	http://www.somalixpogroup.com/bgng/	US	compressed	1.92 Kb	malicious
1176	Explorer.EXE	GET	301	72.52.228.217:80	http://www.somalixpogroup.com/bgng/?	US	—	—	malicious

					x46HZlcx=RmZ/EwWF0tZ60lxkEMQDrejVaHliVfUeL/Iwl85CIJ1qA9vwcVcx9xG7gfzHu2s0gAJY1676H1D+H0gBeCWl7XaRfKnskG2lf2gz9zJY=&Cd-de=CXaLeFo				
1176	Explorer.EXE	POST	404	104.21.25.13:80	http://www.mtactr.online/bgnq/	US	html	245 b	malicious
1176	Explorer.EXE	POST	404	104.21.25.13:80	http://www.mtactr.online/bgnq/	US	html	245 b	malicious
1176	Explorer.EXE	GET	404	104.21.25.13:80	http://www.mtactr.online/bgnq/?Cd-de=CXaLeFo&x46HZlcx=xh8Ryn7M9EqWoOGDSBfaycMviP1H1hPcA+cSLasEjAzLEjLmo1ZlnY4wreDWi0tuuHcm/ETRHSLNePvEKfyMoC3oDbRpb0Ur74fLRpA=	US	html	315 b	malicious
1176	Explorer.EXE	POST	400	154.213.85.105:80	http://www.extraordinarysoap.com/bgnq/	US	text	13 b	malicious
1176	Explorer.EXE	GET	200	154.213.85.105:80	http://www.extraordinarysoap.com/bgnq/?x46HZlcx=KKauau51xmDh6RdjNNJpDGSN9+H0x+s3ibmqCCO5eTVJb6xfpmDRxcylz2dK24PZeDlssJyD6xsXeZoteBXSmD/IiWTBmKEmt3kkUMY=&Cd-de=CXaLeFo	US	binary	1 b	malicious
1176	Explorer.EXE	POST	400	154.213.85.105:80	http://www.extraordinarysoap.com/bgnq/	US	text	13 b	malicious
1176	Explorer.EXE	POST	—	138.201.141.77:80	http://www.aratta.org/bgnq/	DE	—	—	malicious
1176	Explorer.EXE	POST	—	138.201.141.77:80	http://www.aratta.org/bgnq/	DE	—	—	malicious
1176	Explorer.EXE	GET	—	138.201.141.77:80	http://www.aratta.org/bgnq/?Cd-de=CXaLeFo&x46HZlcx=PHa6/UzORPAL8TmNgYQDT6QTIt179VhO54ydZJXAHDRizq2tEgyuKwnbgUjAnlyja1Q1ZvKDzowZDDVxn4n+9bBrjEFtyMSqW3MAd7M=	DE	—	—	malicious
1176	Explorer.EXE	POST	404	38.63.19.20:80	http://www.adress-list.com/bgnq/	US	html	146 b	malicious
1176	Explorer.EXE	GET	404	38.63.19.20:80	http://www.adress-list.com/bgnq/?x46HZlcx=QTvEZOF0b6TE1H41dwcgVrCepF1w9WT0IUH4RwlyJK5dcFT3ag+PCr9PEoXj5zPzZJrTSwQuCNPcIlGe9kUsVKTT0/Zq56LxRBnKLd0=&Cd-de=CXaLeFo	US	html	146 b	malicious
1176	Explorer.EXE	POST	404	38.63.19.20:80	http://www.adress-list.com/bgnq/	US	html	146 b	malicious
1176	Explorer.EXE	GET	200	37.97.254.27:80	http://www.cavallotoys.com/bgnq/?Cd-de=CXaLeFo&x46HZlcx=Rah6Uc7Nh/4D6gtqvSFZY2CoE0DAXdD0l9T/nPzvSqpggGFwkW2igNjrnR51b26tqLm9LftSglq4WP2JYDT/fNLbjz4HcsgQXRVln/w=	NL	html	63.1 Kb	malicious
1176	Explorer.EXE	POST	—	37.97.254.27:80	http://www.cavallotoys.com/bgnq/	NL	—	—	malicious
1176	Explorer.EXE	POST	—	37.97.254.27:80	http://www.cavallotoys.com/bgnq/	NL	—	—	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	13.107.43.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	93.184.221.240:80	ctldl.windowsupdate.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
1448	64b12ea2b1bfbf71cd0ab82dae4a2a2b.exe	13.107.42.12:443	2yalgg.dm.files.1drv.com	Microsoft Corporation	US	suspicious
1176	Explorer.EXE	2.57.90.16:80	www.gabrielasocialmedia.com	—	—	malicious
1808	rundll32.exe	45.33.6.223:80	www.sqlite.org	Linode, LLC	US	suspicious
1176	Explorer.EXE	72.52.228.217:80	www.somaliexpogroup.com	Liquid Web, L.L.C	US	malicious
1176	Explorer.EXE	104.21.25.13:80	www.mtactr.online	Cloudflare Inc	US	malicious
1176	Explorer.EXE	154.213.85.105:80	www.extraordinarysoap.com	MULTACOM CORPORATION	US	malicious
1176	Explorer.EXE	138.201.141.77:80	www.aratta.org	Hetzner Online GmbH	DE	malicious
1176	Explorer.EXE	38.63.19.20:80	www.adress-list.com	Cogent Communications	US	malicious
1176	Explorer.EXE	37.97.254.27:80	www.cavallotoys.com	Transip B.V.	NL	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.43.13	shared
ctldl.windowsupdate.com	93.184.221.240	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
2yalgg.dm.files.1drv.com	13.107.42.12	unknown

www.gabrielasocialmedia.com	2.57.90.16	malicious
www.sqlite.org	45.33.6.223	whitelisted
www.somalixpogroup.com	72.52.228.217	malicious
www.mtactr.online	104.21.25.13 172.67.221.142	malicious
www.extraordinarysoap.com	154.213.85.105	malicious
www.aratta.org	138.201.141.77	malicious
www.adress-list.com	38.63.19.20	malicious
www.cavallotoys.com	37.97.254.27	malicious

Threats

PID	Process	Class	Message
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA STREAM CLOSEWAIT FIN out of window
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)

1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1176	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
—	—	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)

Debug output strings

No debug info



Interactive malware hunting service ANY.RUN
© 2017-2022 ANY.RUN LLC. ALL RIGHTS RESERVED