



## General Info

File name:	Se adjunta nueva lista de pedidos.exe
Full analysis:	<a href="https://app.any.run/tasks/071ea541-6670-47cc-b257-76aba37167ce">https://app.any.run/tasks/071ea541-6670-47cc-b257-76aba37167ce</a>
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 15:08:01
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:	A8E85A11F1F09B07AACB948E17BB377C
SHA1:	2234FA79B53172751A1E57BC0498AC322EF72409
SHA256:	9EF611ACF8B7D6DA11662D906AF98ED385D2B8CD6AE1FD3E1A9189098A11653B
SSDEEP:	12288:fc+2ItCNEdmSene/IUrMP6PSzQbT7grJFcuHdl51T9u6mr:fMjtteed7qUflFcu9lyr

### 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
<b>Changes settings of System certificates</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Reads the computer name</b> Se adjunta nueva lista de pedidos.exe (PID: 3428) cscript.exe (PID: 2384)	<b>Reads settings of System Certificates</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)
<b>Drops executable file immediately after starts</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Checks supported languages</b> Se adjunta nueva lista de pedidos.exe (PID: 3428) cscript.exe (PID: 2384)	<b>Checks Windows Trust Settings</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)
<b>Changes the autorun value in the registry</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Executable content was dropped or overwritten</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Checks supported languages</b> iexpress.exe (PID: 3992) cmd.exe (PID: 2052)
<b>FORMBOOK detected by memory dumps</b> cscript.exe (PID: 2384)	<b>Drops a file with a compile date too recent</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Reads the computer name</b> iexpress.exe (PID: 3992)
<b>FORMBOOK was detected</b> Explorer.EXE (PID: 588)	<b>Adds / modifies Windows certificates</b> Se adjunta nueva lista de pedidos.exe (PID: 3428)	<b>Manual execution by user</b> cscript.exe (PID: 2384)
<b>Connects to CnC server</b> Explorer.EXE (PID: 588)	<b>Reads Environment values</b> cscript.exe (PID: 2384)	

Static information

TRiD	EXIF
<div><div>.exe   Win32 Executable Borland Delphi 7 (68.8)</div><div>.exe   Win32 Executable Borland Delphi 6 (27.2)</div><div>.exe   Win32 Executable Delphi generic (1.4)</div><div>.scr   Windows screen saver (1.3)</div></div>	<div><div>EXE</div><div>Author:WixLife</div><div>HomePage:</div><div>CompanyName:</div></div>

.exe | Win32 Executable (generic) (0.4)

LegalCopyright:Copyright ©2013 All Rights Reserved.

FileDescription:Tec leader

Comments:Tec leader

CharacterSet:Unicode

LanguageCode:English (British)

FileSubtype:0

ObjectFileType:Unknown

FileOS:Win32

FileFlags:(none)

FileFlagsMask:0x003f

ProductVersionNumber:0.0.0.0

FileVersionNumber:0.0.0.0

Subsystem:Windows GUI

SubsystemVersion:4

ImageVersion:0

OSVersion:4

EntryPoint:0x5e100

UninitializedDataSize:0

InitializedDataSize:304128

CodeSize:381440

LinkerVersion:2.25

PEType:PE32

TimeStamp:1992:06:20 00:22:17+02:00

MachineType:Intel 386 or later, and compatibles

Summary

Architecture:IMAGE\_FILE\_MACHINE\_I386

Subsystem:IMAGE\_SUBSYSTEM\_WINDOWS\_GUI

Compilation Date:19-Jun-1992 22:22:17

Detected languages:English - United 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	7.01508
-------	------------	------------	------------	--	---------

Resources

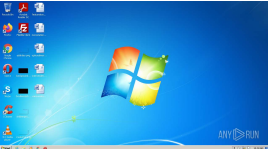
Title	Entropy	Size	Codepage	Language	Type
1	3.24482	544	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	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	7.1265	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

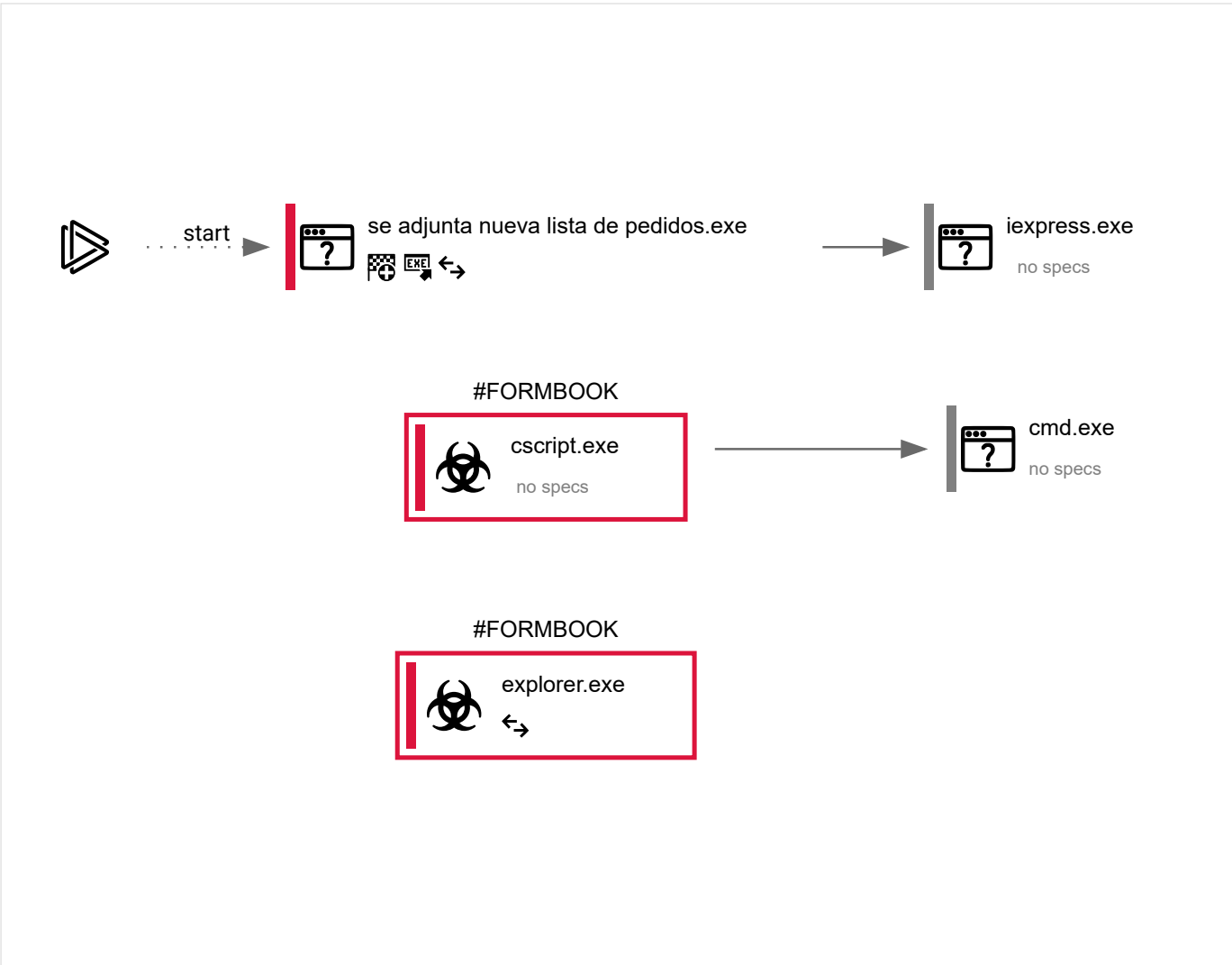
Video and screenshots



Processes

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

Behavior graph





Specs description

Program did not start	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
3428	"C:\Users\admin\AppData\Local\Temp\Se adjunta nueva lista de pedidos.exe"	C:\Users\admin\AppData\Local\Temp\Se adjunta nueva lista de pedidos.exe		Explorer.EXE
Information				
User:	admin	Integrity Level:	MEDIUM	
Description:	Tec leader	Exit code:	0	



3992	"C:\Windows\System32\iexpress.exe"	C:\Windows\System32\iexpress.exe	—	Se adjunta nueva lista de pedidos.exe
<div>Information</div> <div> <div>User: admin</div> <div>Integrity Level: MEDIUM</div> <div>Exit code: 0</div> </div> <div> <div>Company: Microsoft Corporation</div> <div>Description: Wizard</div> <div>Version: 11.00.9600.16428 (winblue_gdr.131013-1700)</div> </div>				
2384	"C:\Windows\System32\cscript.exe"	C:\Windows\System32\cscript.exe		Explorer.EXE
<div>Information</div> <div> <div>User: admin</div> <div>Integrity Level: MEDIUM</div> <div>Version: 5.8.7600.16385</div> </div> <div> <div>Company: Microsoft Corporation</div> <div>Description: Microsoft ® Console Based Script Host</div> </div>				
2052	/c del "C:\Windows\System32\iexpress.exe"	C:\Windows\System32\cmd.exe	—	cscript.exe
<div>Information</div> <div> <div>User: admin</div> <div>Integrity Level: MEDIUM</div> <div>Exit code: 0</div> </div> <div> <div>Company: Microsoft Corporation</div> <div>Description: Windows Command Processor</div> <div>Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)</div> </div>				
588	C:\Windows\Explorer.EXE	C:\Windows\Explorer.EXE		—
<div>Information</div> <div> <div>User: admin</div> <div>Integrity Level: MEDIUM</div> <div>Version: 6.1.7600.16385 (win7_rtm.090713-1255)</div> </div> <div> <div>Company: Microsoft Corporation</div> <div>Description: Windows Explorer</div> </div>				

## Registry activity

Total events	Read events	Write events	Delete events
4 853	4 808	42	3

## Modification events

[illegible]

Value: 1		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name: UNCA\$Intranet
Value: 1		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name: AutoDetect
Value: 0		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.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:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation:	write	Name: WpadDecisionTime
Value: 155A78F50AB6D801		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.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:	(3428) Se adjunta nueva lista de pedidos.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:	(3428) Se adjunta nueva lista de pedidos.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:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	Name: WpadDecisionTime
Value: 155A78F50AB6D801		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.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:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name: LanguageList
Value: en-US		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation:	write	Name: Blob
Value: 040000000100000010000000E4A68AC854AC5242460AFD72481B2A44530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C00F00000001000000200000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A303000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000000100000007D30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E6E36EE60FAFAB912ED06178F39620000000100000020000000C83CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B00000001000000300000004A006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AECE13734AD8CA0B809000000100000034000000303206082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030406082B0601050507030106082B0601050507030822000000010000009203000003082038E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777777E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B68C9B26890AD47A57F46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F91BD71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A48625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFA8912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7F9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BF88FB0610C34AA4E204C84C6DBF835E176D9DFA642B8C7440886F73674245ADA6C0D145935BDF249DD861FC9B30D472A30992FB5C8BB5D420E1995F534615DB689BF0F330D53E31E28D849E38ADADA963E3513A55FF0F70507047411157194EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E50644F4EA879532903E5F5346A2C9DF882B294BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D966EB83537E532B6		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation:	delete key	Name: (default)
Value:		
(PID) Process:	(3428) Se adjunta nueva lista de pedidos.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation:	write	Name: Blob
Value: 5C00000001000000040000000080000530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C00F00000001000000200000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000000100000007D30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E6E36EE60FAFAB912ED06178F39620000000100000020000000C83CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B00000001000000300000004A006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000003082038E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777777E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777777E64696769636572742E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B68C9B		

26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DD077E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BAB9CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BF88FB0610C34A4AE204C84C6DBF835E176D9DFA642B8C74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992F8B5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E313A55FF0F97050704711157194EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADD0D6C377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (3428) Se adjunta nueva lista de pedidos.exe

Operation: write

Value: C:\Users\Public\Libraries\gtqfpodtJ.url

Key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

Name: Jtdopfqtg

## Files activity

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

### Dropped files

PID	Process	Filename	Type
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957B A2B715AC5C442 MD5: 618D326741A269B5E63B7972691EE26B SHA256: 36F6CAF40239793D9A51F25563122F02638C934D01860FEFE9F2C846F79F6A5B	der
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957 BA2B715AC5C442 MD5: 1CCEDFA7890797FD330BD6FB262E0CB6 SHA256: E4E322D4438B6CC5F599EA7B6F4B4CCB64652C0251FBCEFC69B5D167357E1D45	binary
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\UK1ZGE2L.txt MD5: A80C1E7FC701E2920F1AD7D9F219EBEF SHA256: A428D390EAE0FD04E82F203F80B6A9F0E9D878CD5C8BE11066B3E9DCEEBA18AB	text
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757 D77746C10868 MD5: 75E9E37B2AA8E2EF5E013EE4E603FCA5 SHA256: B59FAB5E6A633CF4F33474B96DC0398900DCF1C57E33AE6F858DCA2BC9C39169	der
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: 9416B81500F70A3FF439F236B00AD5BC SHA256: 92DFB035A3882F99FD35C94010E489FCFFAB3DABF0F73686AD7F0EB97FC35104	binary
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\388QSE5U.txt MD5: BFB68458D322B16723965D4832006286 SHA256: F5D3D8E58B96CE53DAFD0205824702EC966D015D3193DBADEB2791D656CDA373	text
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\Public\Libraries\gtqfpodtJ.url MD5: 9FA2A352EE5A44E00189444325114B42 SHA256: ABBE3EBFD54D0BFCA51B1B60D92CD79BF8C0053002EA69F92CEDD562CE54FA94	text
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757 D77746C10868 MD5: A0CB8DBCD18BF0DFD39642FC82E4C253 SHA256: 3C89679D422236005FFD1F727CF97C91497304D1A6FF4FDDE896DF6495D76657	binary
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3428	Se adjunta nueva lista de pedidos.exe	C:\Users\Public\Libraries\Jtdopfqtg.exe MD5: A8E85A11F1F09B07AACB948E17BB377C SHA256: 9EF611ACF8B7D6DA11662D906AF98ED385D2B8CD6AE1FD3E1A9189098A11653B	executable

## Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
10	15	13	24

### HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3428	Se adjunta nueva lista de pedidos.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWmYs%2BghUNoZ70rUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	US	der	1.47 Kb	whitelisted
3428	Se adjunta nueva lista de pedidos.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWmYs%2BghUNoZ70rUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	US	der	471 b	whitelisted
3428	Se adjunta nueva lista de pedidos.exe	GET	200	95.140.236.0:80	http://ctdl.windowsupdate.com/msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?4a38564bafb39958	GB	compressed	4.70 Kb	whitelisted
3428	Se adjunta nueva	GET	200	95.140.236.0:80	http://ctdl.windowsupdate.com/msdownload/update/v3/static/	GB	compressed	4.70 Kb	whitelisted

lista de pedidos.exe				trusted/en/disallowedcertstl.cab?fde57fced51ba6c1						
588	Explorer.EXE	GET	403	34.102.136.180:80	http://www.encludemedia.com/euv4/?v6=ebwJlxyL1q3jbCcyx34seqN8tPJ/tVGRUDi6jelVHXViP+fZszJ7j4ILRNVsCWSaNmroVg==&1b=W6o0QBMX	US	html	291 b	whitelisted	
588	Explorer.EXE	GET	200	74.220.199.6:80	http://www.thecuratedpour.com/euv4/?v6=8RbMdnyCuUJJRr9u6KDY9v1Rs695dVPaPhiPgyB710djFZxzlUqZxtsp92wxZfxcZJeflw==&1b=W6o0QBMX	US	html	4.63 Kb	malicious	
588	Explorer.EXE	GET	403	23.251.40.122:80	http://www.handejqr.com/euv4/?v6=85mQjwU8sLES9A/6GuSrcIreOiba9zyWW+aCoFXLFB9hHue7fW4uQO76DIRSMxEsOXb26A==&1b=W6o0QBMX	US	html	159 b	malicious	
588	Explorer.EXE	GET	—	37.123.118.150:80	http://www.tajniezdrzi.quest/euv4/?v6=liNQ9bAmikKL/E2/7qVXrQLN2OwlNmSYNNmGNeNvyxaU1dh4bJGmupXs4qcmZGG+Un0Ahg==&1b=W6o0QBMX	GB	—	—	malicious	
588	Explorer.EXE	GET	302	103.224.182.210:80	http://www.drimev.com/euv4/?v6=v4MdxpN29Nw67PySAvRB7QyTm8baEOUbrF077IMSU50+VeA8qKBE8HdXoYIXJXSCOB56Jg==&1b=W6o0QBMX	AU	—	—	malicious	
588	Explorer.EXE	GET	301	103.120.80.144:80	http://www.77777.store/euv4/?v6=sV2k1WL9KF95twgHSRvAMNLFs+Ge3XGMDmPBhSsrGC2EmS3Swl6at5LXCDSNLVGrKkXAyg==&1b=W6o0QBMX	unknown	html	169 b	malicious	

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3428	Se adjunta nueva lista de pedidos.exe	13.107.43.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
3428	Se adjunta nueva lista de pedidos.exe	178.79.242.0:80	ctldl.windowsupdate.com	Limelight Networks, Inc.	DE	malicious
3428	Se adjunta nueva lista de pedidos.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3428	Se adjunta nueva lista de pedidos.exe	13.107.43.12:443	pppdxq.ph.files.1drv.com	Microsoft Corporation	US	unknown
3428	Se adjunta nueva lista de pedidos.exe	95.140.236.0:80	ctldl.windowsupdate.com	Limelight Networks, Inc.	GB	suspicious
588	Explorer.EXE	74.220.199.6:80	www.thecuratedpour.com	Unified Layer	US	malicious
588	Explorer.EXE	34.102.136.180:80	www.encludemedia.com	—	US	whitelisted
588	Explorer.EXE	23.251.40.122:80	www.handejqr.com	Shanghai Anchang Network Security Technology Co.,Ltd.	US	malicious
588	Explorer.EXE	103.120.80.144:80	www.77777.store	—	—	malicious
588	Explorer.EXE	37.123.118.150:80	www.tajniezdrzi.quest	UK-2 Limited	GB	malicious
588	Explorer.EXE	103.224.182.210:80	www.drimev.com	Trellian Pty. Limited	AU	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.43.13	shared
ctldl.windowsupdate.com	178.79.242.0 95.140.236.0	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
pppdxq.ph.files.1drv.com	13.107.43.12	unknown
www.encludemedia.com	34.102.136.180	whitelisted
www.thecuratedpour.com	74.220.199.6	malicious
www.handejqr.com	23.251.40.122	malicious
www.tajniezdrzi.quest	37.123.118.150	malicious
www.77777.store	103.120.80.144	malicious
www.gongwenbo.com	—	malicious
www.drimev.com	103.224.182.210	malicious

Threats

PID	Process	Class	Message
588	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body

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