



# General Info

File name:	Nueva lista de pedidos.exe
Full analysis:	<a href="https://app.any.run/tasks/e7f16e11-f431-43a4-8f88-1c7a6e0684a9">https://app.any.run/tasks/e7f16e11-f431-43a4-8f88-1c7a6e0684a9</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 17, 2022 at 15:12:33
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:	67747EA5A5A7379F4F39A763150351B5
SHA1:	AF9A695620FA3FC09846B530EFFA1767B9E78AF1
SHA256:	5CAA7E1C0AE42CE33FFAFC7FD4CD355F4B0120A8FF19BEFA059A428AC4EE1B1D
SSDEEP:	24576:+Xgr/BEuCNYeA06CG7Dmo/KvouloQHO2XeLoPx1rGe:+XmsLMKf0LoJ

## 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> Nueva lista de pedidos.exe (PID: 3488)	<b>Checks supported languages</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Checks supported languages</b> cmd.exe (PID: 3100) msdt.exe (PID: 964) calc.exe (PID: 3880)
<b>Changes the autorun value in the registry</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Reads the computer name</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Reads settings of System Certificates</b> Nueva lista de pedidos.exe (PID: 3488)
<b>Drops executable file immediately after starts</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Executable content was dropped or overwritten</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Reads the computer name</b> msdt.exe (PID: 964) calc.exe (PID: 3880)
<b>FORMBOOK detected by memory dumps</b> msdt.exe (PID: 964)	<b>Drops a file with a compile date too recent</b> Nueva lista de pedidos.exe (PID: 3488)	<b>Manual execution by user</b> msdt.exe (PID: 964)
<b>Connects to CnC server</b> Explorer.EXE (PID: 588)	<b>Reads Environment values</b> msdt.exe (PID: 964)	<b>Checks Windows Trust Settings</b> Nueva lista de pedidos.exe (PID: 3488)
<b>FORMBOOK was detected</b> Explorer.EXE (PID: 588)	<b>Adds / modifies Windows certificates</b> Nueva lista de pedidos.exe (PID: 3488)	

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:0x86998

UninitializedDataSize:0

InitializedDataSize:402944

CodeSize:545792

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

Russian - Russia

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: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:9

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
.text	0x00001000	0x000849E0	0x00084A00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.56087
.itext	0x00086000	0x000009E0	0x00000A00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.2538
.data	0x00087000	0x00002380	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	3.80421
.bss	0x0008A000	0x00003878	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x0008E000	0x00002C42	0x00002E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.13963

.tls	0x00091000	0x00000040	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00092000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	0.205446
.reloc	0x00093000	0x00008E5C	0x00009000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.66931
.rsrc	0x0009C000	0x00054200	0x00054200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	6.73087

Resources

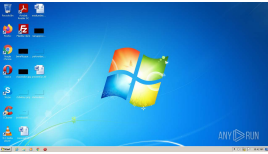
Title	Entropy	Size	Codepage	Language	Type
1	5.07235	399	UNKNOWN	Russian - Russia	RT_MANIFEST
2	2.80231	308	UNKNOWN	English - United States	RT_CURSOR
3	3.00046	308	UNKNOWN	English - United States	RT_CURSOR
4	2.56318	308	UNKNOWN	English - United States	RT_CURSOR
5	2.6949	308	UNKNOWN	English - United States	RT_CURSOR
6	2.62527	308	UNKNOWN	English - United States	RT_CURSOR
7	2.91604	308	UNKNOWN	English - United States	RT_CURSOR
50	2.93488	2048	UNKNOWN	UNKNOWN	RT_ICON
51	2.9114	1024	UNKNOWN	UNKNOWN	RT_ICON
52	2.0157	512	UNKNOWN	UNKNOWN	RT_ICON
53	5.06437	4096	UNKNOWN	UNKNOWN	RT_ICON
4081	3.25809	652	UNKNOWN	UNKNOWN	RT_STRING
4082	3.43376	1028	UNKNOWN	UNKNOWN	RT_STRING
4083	3.37918	664	UNKNOWN	UNKNOWN	RT_STRING
4084	3.51789	188	UNKNOWN	UNKNOWN	RT_STRING
4085	3.43398	272	UNKNOWN	UNKNOWN	RT_STRING
4086	3.39323	584	UNKNOWN	UNKNOWN	RT_STRING
4087	3.27996	1020	UNKNOWN	UNKNOWN	RT_STRING
4088	3.24508	944	UNKNOWN	UNKNOWN	RT_STRING
4089	3.34142	852	UNKNOWN	UNKNOWN	RT_STRING
4090	3.32267	968	UNKNOWN	UNKNOWN	RT_STRING
4091	3.25287	212	UNKNOWN	UNKNOWN	RT_STRING
4092	3.26919	164	UNKNOWN	UNKNOWN	RT_STRING
4093	3.35394	672	UNKNOWN	UNKNOWN	RT_STRING
4094	3.29437	1112	UNKNOWN	UNKNOWN	RT_STRING
4095	3.32482	908	UNKNOWN	UNKNOWN	RT_STRING
4096	3.2857	692	UNKNOWN	UNKNOWN	RT_STRING
32761	1.83876	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32762	1.91924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32763	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32764	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32765	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32766	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32767	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
LOGO	7.97536	44774	UNKNOWN	Russian - Russia	IMAGE
BBABORT	2.92079	464	UNKNOWN	English - United States	RT_BITMAP
BBALL	3.16995	484	UNKNOWN	English - United States	RT_BITMAP
BBCANCEL	2.92079	464	UNKNOWN	English - United States	RT_BITMAP
BBCLOSE	3.68492	464	UNKNOWN	English - United States	RT_BITMAP
BBHELP	2.88085	464	UNKNOWN	English - United States	RT_BITMAP
BBIGNORE	3.29718	464	UNKNOWN	English - United States	RT_BITMAP
BBNO	3.58804	464	UNKNOWN	English - United States	RT_BITMAP
BBOK	2.67459	464	UNKNOWN	English - United States	RT_BITMAP
BBOKK	5.66857	192616	UNKNOWN	English - United States	RT_BITMAP

BBRETRY	3.53344	464	UNKNOWN	English - United States	RT_BITMAP
BBYES	2.67459	464	UNKNOWN	English - United States	RT_BITMAP
PREVIEWGLYPH	2.85172	232	UNKNOWN	English - United States	RT_BITMAP
DLGTEMPLATE	2.5627	82	UNKNOWN	UNKNOWN	RT_DIALOG
TEXTFILEDLG	2.61605	82	UNKNOWN	UNKNOWN	RT_DIALOG
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
ENTRO	6.28317	40774	UNKNOWN	English - United States	RT_RCDATA
PACKAGEINFO	5.49993	1040	UNKNOWN	UNKNOWN	RT_RCDATA
TMXFRM	4.89108	34588	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.45107	62	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

URL
advapi32.dll
comctl32.dll
comdlg32.dll
gdi32.dll
kernel32.dll
msimg32.dll
ole32.dll
oleaut32.dll
user32.dll
version.dll

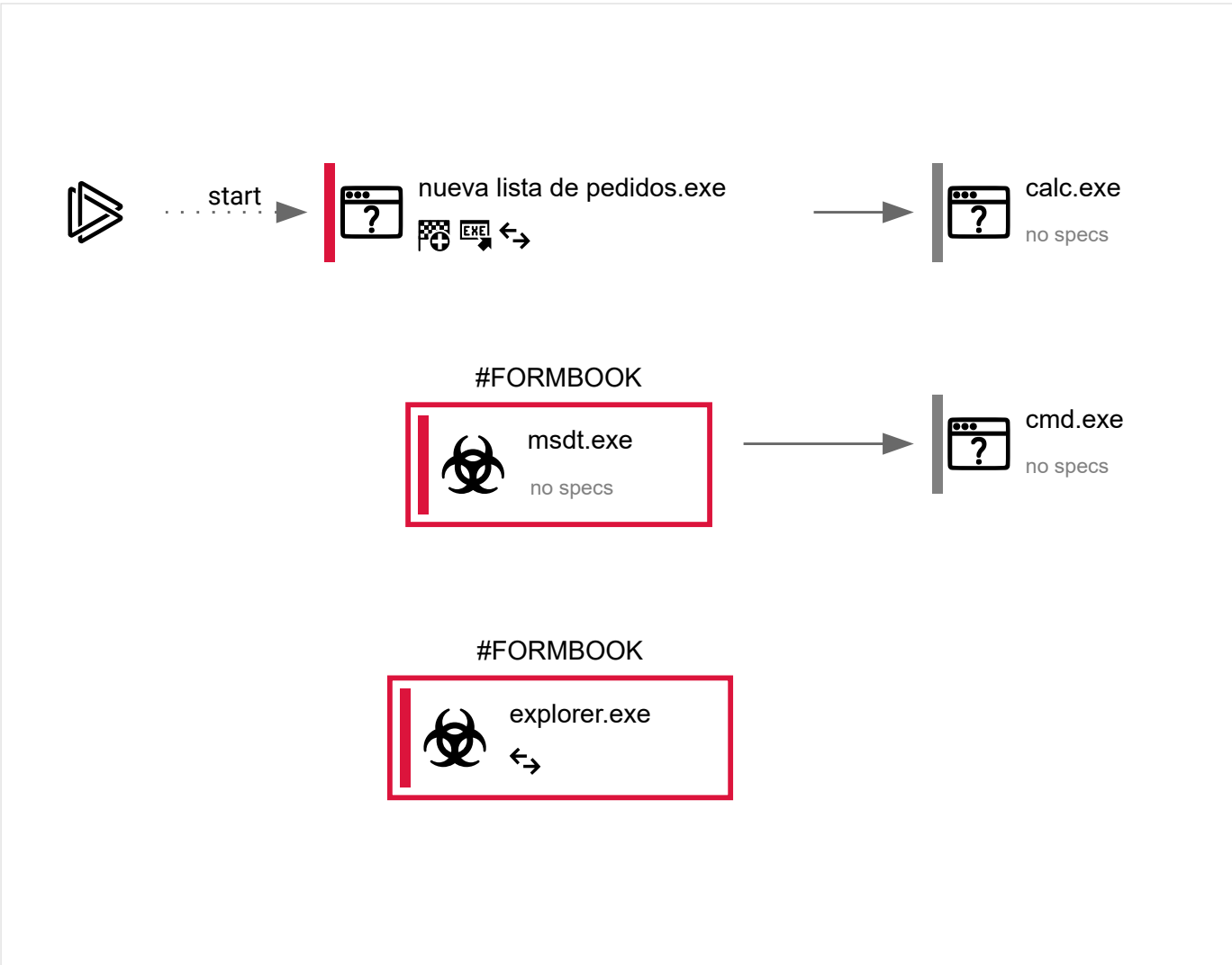
Video and screenshots



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
3488	"C:\Users\admin\AppData\Local\Temp\Nueva lista de pedidos.exe"	C:\Users\admin\AppData\Local\Temp\Nueva lista de pedidos.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	



3880	"C:\Windows\System32\calc.exe"	C:\Windows\System32\calc.exe	—	Nueva lista de pedidos.exe
<div>Information</div> <div> <div>User: admin</div> <div>Company: Microsoft Corporation</div> <div>Integrity Level: MEDIUM</div> <div>Description: Windows Calculator</div> <div>Exit code: 0</div> <div>Version: 6.1.7600.16385 (win7_rtm.090713-1255)</div> </div>				
964	"C:\Windows\System32\msdt.exe"	C:\Windows\System32\msdt.exe	✕ 	Explorer.EXE
<div>Information</div> <div> <div>User: admin</div> <div>Company: Microsoft Corporation</div> <div>Integrity Level: MEDIUM</div> <div>Description: Diagnostics Troubleshooting Wizard</div> <div>Version: 6.1.7600.16385 (win7_rtm.090713-1255)</div> </div>				
3100	/c del "C:\Windows\System32\calc.exe"	C:\Windows\System32\cmd.exe	—	msdt.exe
<div>Information</div> <div> <div>User: admin</div> <div>Company: Microsoft Corporation</div> <div>Integrity Level: MEDIUM</div> <div>Description: Windows Command Processor</div> <div>Exit code: 0</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>Company: Microsoft Corporation</div> <div>Integrity Level: MEDIUM</div> <div>Description: Windows Explorer</div> <div>Version: 6.1.7600.16385 (win7_rtm.090713-1255)</div> </div>				

## Registry activity

Total events	Read events	Write events	Delete events
4 650	4 608	40	2

## Modification events

[illegible]

Value: 1	
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Name: AutoDetect
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8} Name: WpadDecisionReason
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: AD70E8BF1DB2D801	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8} Name: WpadDecisionTime
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8} Name: WpadDecision
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: Network 4	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8} Name: WpadNetworkName
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff Name: WpadDecisionReason
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: AD70E8BF1DB2D801	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff Name: WpadDecisionTime
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff Name: WpadDecision
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: en-US	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E Name: LanguageList
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 040000000100000010000000E4A68AC854AC5242460AFD72481B2A44530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C03018060567810C010330123010060A2B0601040182373C0101030200C00F00000001000000200000004B4EB4B0742988828B5C003095A1084523FB951C0C88348B09C53E5BABA408A303000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000100000010000007DC30BC974695560A2F0090A6545556C140000001000000140000004E2254201895E636EE60FFAFAB912ED06178F39620000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F00740020004700320000001900000001000000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030106082B060105050703082000000001000000920300003082038E30820276A0030201020210033AF1E6A711A9A0BB2864811D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636FD3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636FD3120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95045949F3352D96E3496DD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAF83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA69A1BAB99CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101F04043020186301D0603551D0E04160414AE2254201895E636EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3C588B47FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF8FB0610C34A4AE204C84CDBF835E176D9DFA642BB408867F3674245ADA6C0D145935BDF249DD8B1FC9B30D472A30992FBB85CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F970507047411157194EC08FAE0649513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B948D90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 Name: Blob
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: delete key Value:	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 Name: (default)
(PID) Process: (3488) Nueva lista de pedidos.exe Operation: write Value: 5C00000001000000040000000080000530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C03018060567810C010330123010060A2B0601040182373C0101030200C00F00000001000000200000004B4EB4B0742988828B5C003095A1084523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D0000000100000010000007DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E636EE60FFAFAB912ED06178F39620000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F00740020004700320000001900000001000000014C3BD3549EE225AECE13734AD8CA0B809000000100000034000000303206082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030106082B060105050703082000000001000000920300003082038E30820276A0030201020210033AF1E6A711A9A0BB2864811D09FAE5300D06092A864886F70D01010B05003061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636FD3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D3133303830313132303030305A170D3338303131353132303030305A3061310B300906035504061302555331153013060355040A130C446967694365727420496E6331193017060355040B1310777772E64696769636572742E636FD3120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95045949F3352D96E3496DD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAF83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA69A1BAB99CC5B1338329850203010001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF04043020186301D0603551D0E04160414AE2254201895E636EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3C588B47FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF8FB0610C34A4AE204C84CDBF835E176D9DFA642BB408867F3674245ADA6C0D145935BDF249DD8B1FC9B30D472A30992FBB85CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F970507047411157194EC08FAE0649513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B948D90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 Name: Blob
(PID) Process: (3488) Nueva lista de pedidos.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Operation:	write	Name:	Dlptcbzec
Value:	C:\Users\Public\Libraries\cezbtcpID.url		

Files activity

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

Dropped files

PID	Process	Filename	Type
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: 76F5C1C5ADFB442525C357E62ECD38D3SHA256: 018E3CAB04E42FD316D03F09ADFA0A624E71B759BD49E45B830A6589BE3F7CD0	binary
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB24540769805E5BB30D193944DCESHA256: 6B88C6AC55BD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\UK1ZGE2L.txt MD5: 9A1E8515F4D305A676E9F82AC9868990SHA256: 0A2A2B7336959FE8AFC4A3459B0B2495CFC4DEF5FD45968948A4041DAF0B80AA	text
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 MD5: 8CA0C70984B6D8B63C33EA4C9CFEC180SHA256: 9A5DBC47F1AB18EDC792C7ED6591FD55D8946476E5D8F1302531EEAC8634B152	binary
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\388QE5U.txt MD5: DE12AEA84CCEBA9523CA493D1C232CCESHA256: 66A73D416D16DBFEE2829637F97F42897E21E67F92F561F0CF4720A9EF2D70DE	text
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 MD5: FBAF2BFE85FC0C711E66162D6ADE6EF7SHA256: 140133D75CF48B1D1B81DD5B3F679769574C055A901BA83E31C8A65D58A3FB41	binary
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 MD5: 8EB0E7608663B78E50C1B74920FA11F6SHA256: 36C2DF4B17E755CC280C420DA8BA10C80CA09BA166A10EA2C745B5F9E9DB702D	der
3488	Nueva lista de pedidos.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 MD5: 02D9399A19F596C69F0F3BC95A772F79SHA256: 0E6B8F6E66B26F2ADDFCC2672B93CE57AC94B6A7691F19FD0619C0316E7422FF	der
3488	Nueva lista de pedidos.exe	C:\Users\Public\Libraries\cezbtcpID.url MD5: DFCFA44850956BFF913DF51568055D34SHA256: 345A483A36323BFBC11A2203D75A20513DC339305D1B1AD6924F6D1E6DD8FAB3	text
3488	Nueva lista de pedidos.exe	C:\Users\Public\Libraries\Dlptcbzec.exe MD5: 67747EA5A5A7379F4F39A763150351B5SHA256: 5CAA7E1C0AE42CE33FFAFC7FD4CD355F4B0120A8FF19BEFA059A428AC4EE1B1D	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	19	19	50

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3488	Nueva lista de pedidos.exe	GET	200	8.248.117.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?09d7c56913ab4b76	US	compressed	4.70 Kb	whitelisted
3488	Nueva lista de pedidos.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
3488	Nueva lista de pedidos.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2F6%2BkrS7QYXjKCEAqvsXKY8RRQeo74ffHUxc%3D	US	der	471 b	whitelisted
588	Explorer.EXE	GET	302	18.141.90.247:80	http://www.ahmadfaizlajis.com/euv4/?uF00=XPxhJr4xG&6IJTLb=l4UI0FqBVilafngpdI4GuAr3NeMDDsn ekqdsrouJ39bXUnDbfwTz8sPjR75yC5zeWZQTdQ==	US	—	—	malicious
588	Explorer.EXE	GET	400	206.188.193.90:80	http://www.anniebapartments.com/euv4/?uF00=XPxhJr4xG&6IJTLb=2pA74KfkDPsfadUDkWFAi8e35ziQ8w4QNtzFGzi8j6WGLANLx+hvQWGemcXmbsFOJ0lyA==	US	html	163 b	malicious
588	Explorer.EXE	GET	403	34.98.99.30:80	http://www.leatherman-neal.com/euv4/?uF00=XPxhJr4xG&6IJTLb=9Q+CIVtbAjGRZfZbrbBII/BFZ6Klr/4O8KbjYeylwvpXlbaTbFkJUSgO5WB8A678XGQaPww==	US	html	291 b	malicious
588	Explorer.EXE	GET	403	23.227.38.74:80	http://www.rematedeldia.com/euv4/?6IJTLb=E+AdlFmMulq72wuB5GTeilCEOXtaM5yG6oWNBj19kfBe4Loakg6E6XBt7UPPx61bF/5skdA==&uF00=XPxhJr4xG	CA	html	5.03 Kb	malicious
588	Explorer.EXE	GET	200	23.202.231.167:80	http://www.68135.online/euv4/?	US	html	375 b	malicious

uF00=XPxhJr4xG&6lJTLb=xffN7lCDHf+T5gZeKgqTfB6Iny6s118zqQl2NmEA0aMsmEY6jCr7J51tD869jK+o7tzW6w==									
588	Explorer.EXE	GET	301	162.0.232.72:80	http://www.jasabacklinkweb20.com/euv4/?6lJTLb=ElavoBqKFBsYEkX0e+USRSu2MAjQbrjhdRyAoSVDVR15A7ZJTXSlbb00PvYzbnAKuccxg==&uF00=XPxhJr4xG	CA	html	707 b	malicious
588	Explorer.EXE	GET	—	154.90.64.134:80	http://www.t1uba.com/euv4/?uF00=XPxhJr4xG&6lJTLb=a7oTrd/rGYVlyNy8MvYHhwtmIDdFKKQLmughNAny6QeW5a2qGVG7jaOobFo5zSq8oghFw==	US	—	—	malicious
588	Explorer.EXE	GET	—	85.194.202.138:80	http://www.hagenbicycles.com/euv4/?6lJTLb=QC0bZYsS8NDggISjpHcBmlFp3ASQtsJ/UfgMvpEg2qX0NUAeKQpT8n+aAxPOH4W+1yZSug==&uF00=XPxhJr4xG	EE	—	—	malicious
588	Explorer.EXE	GET	200	23.202.231.167:80	http://www.byausorsm26-plala.xyz/euv4/?6lJTLb=VEsldkD67r2fupVtX6CMQ86VwrZvmVgbyRcO7EzUsMh0VnvOfws+h8cPYfNy/Va2yM7/Vw==&uF00=XPxhJr4xG	US	html	384 b	malicious
588	Explorer.EXE	GET	—	23.202.231.167:80	http://www.protection-onepa.com/euv4/?uF00=XPxhJr4xG&6lJTLb=m9J4puS0IHjKU+rfbs/scS90bVaUlcIF59SvndiUQtu7IPYzsPhsOHQbluwGVKspRtpz1w==	US	—	—	malicious
588	Explorer.EXE	GET	404	134.122.133.133:80	http://www.595531.com/euv4/?6lJTLb=+779LlhZs+2Gli78ny6OmU0z6AXaT2Z5wFD0mEWGDNIxmE5NGM++sSLOOusJ5sgxmTcL0g==&uF00=XPxhJr4xG	US	html	146 b	malicious
588	Explorer.EXE	GET	—	154.216.153.45:80	http://www.turkcuyuz.com/euv4/?6lJTLb=3OQtiNWZiQxLzrfwzfeMPGMDt0zVI+r60Wm2oPcgGvu85CsC9cbuxTypmEjol+pmL/w1NA==&uF00=XPxhJr4xG	US	—	—	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3488	Nueva lista de pedidos.exe	13.107.43.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
588	Explorer.EXE	206.188.193.90:80	www.annieapartments.com	Defense.Net, Inc	US	malicious
3488	Nueva lista de pedidos.exe	13.107.42.12:443	55yaza.ph.files.1drv.com	Microsoft Corporation	US	suspicious
588	Explorer.EXE	134.122.133.133:80	www.595531.com	—	US	malicious
3488	Nueva lista de pedidos.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
588	Explorer.EXE	18.141.90.247:80	www.ahmadfaizlajis.com	Massachusetts Institute of Technology	US	malicious
3488	Nueva lista de pedidos.exe	8.248.117.254:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	malicious
—	—	162.0.232.72:80	www.jasabacklinkweb20.com	AirComPlus Inc.	CA	malicious
588	Explorer.EXE	154.216.153.45:80	www.turkcuyuz.com	MULTACOM CORPORATION	US	malicious
588	Explorer.EXE	154.90.64.134:80	www.t1uba.com	MULTACOM CORPORATION	US	malicious
588	Explorer.EXE	23.202.231.167:80	www.68135.online	Akamai Technologies, Inc.	US	malicious
588	Explorer.EXE	34.98.99.30:80	www.leatherman-neal.com	—	US	whitelisted
588	Explorer.EXE	23.227.38.74:80	www.rematedeldia.com	Shopify, Inc.	CA	malicious
588	Explorer.EXE	85.194.202.138:80	www.hagenbicycles.com	Elkdata OU	EE	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.43.13	shared
ctldl.windowsupdate.com	8.248.117.254 8.253.95.121 8.253.95.249 67.27.158.126 8.241.11.126	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
55yaza.ph.files.1drv.com	13.107.42.12	unknown
www.ahmadfaizlajis.com	18.141.90.247 52.221.12.97 52.220.254.29	malicious
www.595531.com	134.122.133.133	malicious
www.annieapartments.com	206.188.193.90	malicious
www.jasabacklinkweb20.com	162.0.232.72	malicious
www.leatherman-neal.com	34.98.99.30	malicious

www.rematedeldia.com	23.227.38.74	malicious
www.turkcuyuz.com	154.216.153.45	malicious
www.68135.online	23.202.231.167 23.217.138.108	malicious
www.hagenbicycles.com	85.194.202.138	malicious
www.t1uba.com	154.90.64.134	malicious
www.byausorm26-plala.xyz	23.202.231.167 23.217.138.108	malicious
www.protection-onepa.com	23.202.231.167 23.217.138.108	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)
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)

		A Network Trojan was detected	
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	Potentially Bad Traffic	ET INFO Request to .XYZ Domain with Minimal Headers
588	Explorer.EXE	Potentially Bad Traffic	AV INFO HTTP Request to a *.xyz domain
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