ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	Popis nove narudzbe u prilogu.exe
Full analysis:	https://app.any.run/tasks/d4694d3a-130d-4943-9bf3-4c7ef368fe72
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 11:50:58
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:	DFEA6E8EEE2E4AE2E3DF115696904386
SHA1:	D5283886F1E16191EEF12A1FD450B940AE4587D8
SHA256:	9AD8CC5C8B88690A6A57096C475F5463A52C357F3C7FE3F8B41F3FA7830DE7B8
SSDEEP:	12288:JJv4Exdl+xPS9zFdqQxN42zvM/bgiXqYaSBW4:J54wUJSl3r42TAbgq44

Software environment set and analysis options

Launch configuration

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

Software preset

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

Hotfixes

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

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2685939
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)	KB2690533
Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972

Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461
Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178

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

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

Behavior activities

MALICIOUS

Changes settings of System certificates
Popis nove narudzbe u prilogu.exe (PID: 3208)

Drops executable file immediately after starts
Popis nove narudzbe u prilogu.exe (PID: 3208)

Changes the autorun value in the registry
Popis nove narudzbe u prilogu.exe (PID: 3208)

FORMBOOK detected by memory dumps
cmd.exe (PID: 3668)

FORMBOOK was detected
Explorer.EXE (PID: 1068)

Connects to CnC server
Explorer.EXE (PID: 1068)

SUSPICIOUS

Reads the computer name
Popis nove narudzbe u prilogu.exe (PID: 3208)
cmd.exe (PID: 3668)
cmd.exe (PID: 2064)

Checks supported languages
Popis nove narudzbe u prilogu.exe (PID: 3208)
cmd.exe (PID: 3668)
cmd.exe (PID: 2064)

Drops a file with a compile date too recent
Popis nove narudzbe u prilogu.exe (PID: 3208)

Adds / modifies Windows certificates
Popis nove narudzbe u prilogu.exe (PID: 3208)

Reads Environment values
cmd.exe (PID: 3668)

Application launched itself
cmd.exe (PID: 3668)

Executable content was dropped or overwritten
Popis nove narudzbe u prilogu.exe (PID: 3208)

INFO

Checks Windows Trust Settings
Popis nove narudzbe u prilogu.exe (PID: 3208)

Reads settings of System Certificates
Popis nove narudzbe u prilogu.exe (PID: 3208)

Checks supported languages
cmd.exe (PID: 3320)

Manual execution by user
cmd.exe (PID: 3668)

Static information

TRiD

.exe | Win32 Executable Borland Delphi 7 (68.8)

EXIF

EXE

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

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	1992:06:20 00:22:17+02:00
PEType:	PE32
LinkerVersion:	2.25
CodeSize:	331264
InitializedDataSize:	348160
UninitializedDataSize:	0
EntryPoint:	0x51be4
OSVersion:	4
ImageVersion:	0
SubsystemVersion:	4
Subsystem:	Windows GUI
FileVersionNumber:	9.9.0.3
ProductVersionNumber:	9.9.0.3
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Win32
ObjectFileType:	Unknown
FileSubtype:	0
LanguageCode:	English (British)
CharacterSet:	Unicode
FileVersion:	9,9,0,3
Comments:	OilCo Bangladesh
FileDescription:	OilCo Bangladesh
LegalCopyright:	Copyright ©2013 OilCo Bangladesh All Rights Reserved.
CompanyName:	OilCo Bangladesh
HomePage:	www.OilCo Bangladesh.org
Author:	BOilCo Bangladeshe

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:	9,9,0,3
Comments:	OilCo Bangladesh
FileDescription:	OilCo Bangladesh
LegalCopyright:	Copyright ©2013 OilCo Bangladesh All Rights Reserved.
CompanyName:	OilCo Bangladesh
HomePage:	www.OilCo Bangladesh.org
Author:	BOilCo Bangladeshe

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	0x00050C50	0x00050E00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.51529
DATA	0x00052000	0x000011A4	0x00001200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.17925

BSS	0x00054000	0x00000D2D	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x00055000	0x00001FE6	0x00002000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.90955
.tls	0x00057000	0x00000010	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00058000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.200582
.reloc	0x00059000	0x00005BF0	0x00005C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.67993
.rsrc	0x0005F000	0x0004C000	0x0004C000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.73096

Resources

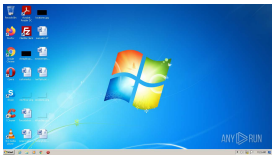
Title	Entropy	Size	Codepage	Language	Type
1	3.363	752	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.91604	308	UNKNOWN	UNKNOWN	RT_CURSOR
58	5.75354	9728	UNKNOWN	UNKNOWN	RT_ICON
59	5.2896	4608	UNKNOWN	UNKNOWN	RT_ICON
60	5.8952	2560	UNKNOWN	UNKNOWN	RT_ICON
61	4.54327	1536	UNKNOWN	UNKNOWN	RT_ICON
4081	3.20539	304	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	3.16178	248	UNKNOWN	UNKNOWN	RT_STRING
4086	3.14262	248	UNKNOWN	UNKNOWN	RT_STRING
4087	3.24593	540	UNKNOWN	UNKNOWN	RT_STRING
4088	3.2261	1024	UNKNOWN	UNKNOWN	RT_STRING
4089	3.16052	876	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
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
BBONNO	6.05111	218824	UNKNOWN	English - United States	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
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
PACKAGEINFO	5.32183	660	UNKNOWN	UNKNOWN	RT_RCDATA
TFORM2	5.3627	542	UNKNOWN	UNKNOWN	RT_RCDATA
ZOTRO	7.37704	51917	UNKNOWN	English - United States	RT_RCDATA
MAINICON	2.41812	62	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

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

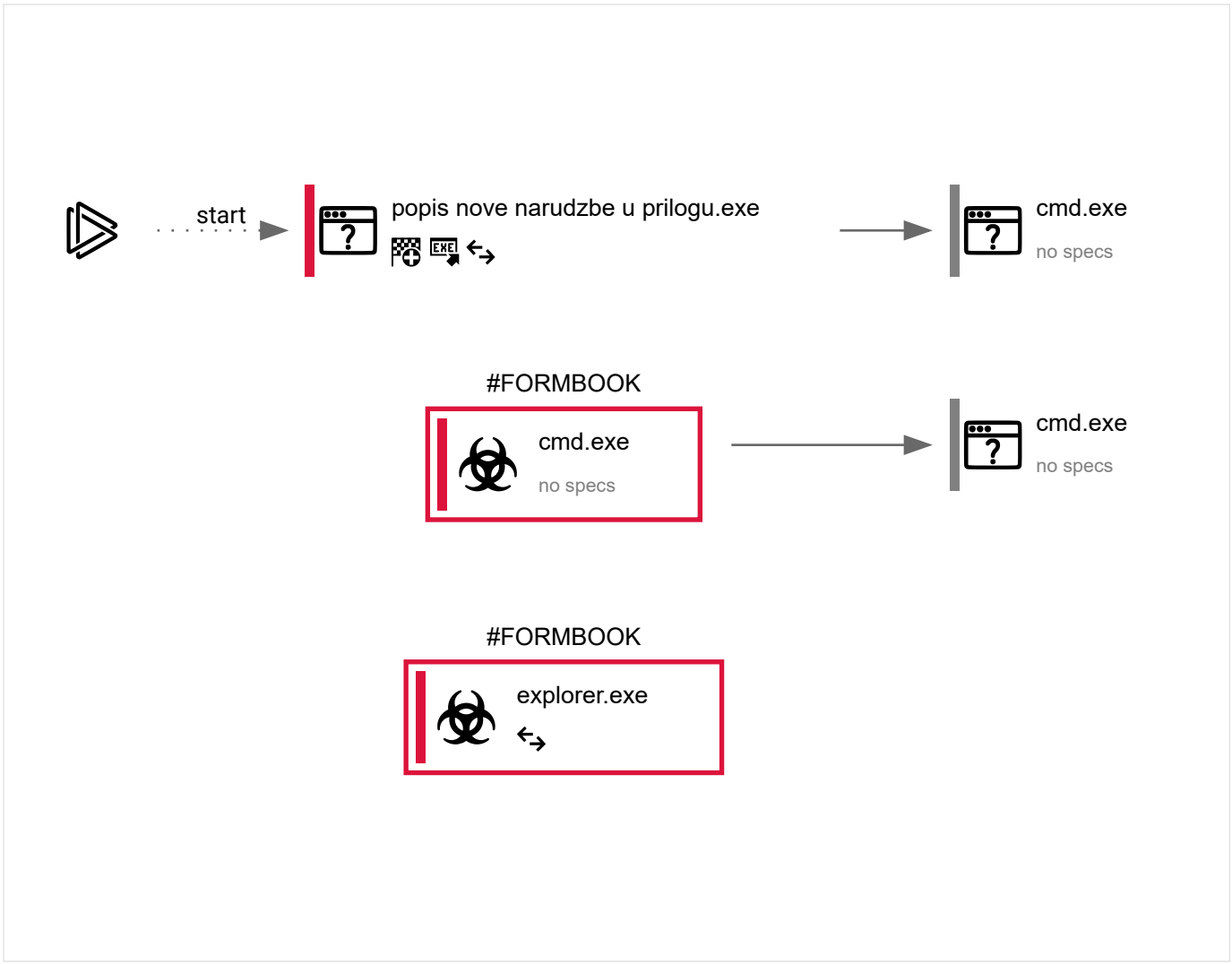
Video and screenshots



Processes

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

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
3208	"C:\Users\admin\AppData\Local\Temp\Popis nove narudzbe u prilogu.exe"	C:\Users\admin\AppData\Local\Temp\Popis nove narudzbe u prilogu.exe		Explorer.EXE

Information

User:	admin	**Company:**	OilCo Bangladesh
Integrity Level:	MEDIUM	**Description:**	OilCo Bangladesh
Exit code:	0	**Version:**	9,9,0,3

2064	"C:\Windows\System32\cmd.exe"	C:\Windows\System32\cmd.exe	—	Popis nove narudzbe u prilogu.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3668	"C:\Windows\System32\cmd.exe"	C:\Windows\System32\cmd.exe		Explorer.EXE

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)		

3320	/c del "C:\Windows\System32\cmd.exe"	C:\Windows\System32\cmd.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1068	C:\Windows\Explorer.EXE	C:\Windows\Explorer.EXE		SearchProtocolHost.exe

Information

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

Registry activity

Total events	Read events	Write events	Delete events
4 766	4 724	40	2

Modification events

(PID) Process: (1068) Explorer.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0

Operation: write **Name:** CheckSetting

Value: 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000DE56BD4EADDCEE4783BB227D6A41EE1100000000002000000000010660000000010000200000000B01123CC0ECCF333B2732BC8
391B61086ADEB00D0B66E88EFECA9A7B9A857C81000000000E8000000002000020000000C19E80B383A450362D53F512F3C089B4EDCF3673B20722BFD77C40DC5F6EA4F730000000D872F
A7C5A73FC15447EB615F27DC19F9D26FF88798DB9D8E02E304236CB1CFFD57CC2CDE6A2C937DD2D0E8989DEBE3140000000FBF7D985D7CC37A3BAFF984FD2A4BA2A91FD75BAAE9064E
AB159A6A9E914F383F2C101F06E7DF052499223BF3A29D34BBBBBBA5984E55CE5F202303E9330527E

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value: 460000003B0100000900000000000000000000000000000000004000000000000000C0E333BBEAB1D301000000000000000000000000000100000002000000C0A80164000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content

Operation: write **Name:** CachePrefix

Value:

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies

Operation: write **Name:** CachePrefix

Value: Cookie:

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

Operation: write **Name:** CachePrefix

Value: Visited:

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (3208) Popis nove narudzbe u prilogu.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: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}

Operation: write **Name:** WpadDecisionTime

Value: 09AEB66CEFB5D801

(PID) Process: (3208) Popis nove narudzbe u prilogu.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: (3208) Popis nove narudzbe u prilogu.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: (3208) Popis nove narudzbe u prilogu.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: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff

Operation: write **Name:** WpadDecisionTime

Value: 09AEB66CEFB5D801

(PID) Process: (3208) Popis nove narudzbe u prilogu.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: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: write **Name:** Blob

Value: 0400000001000000010000000E4A68AC854AC5242460AFD72481B2A44530000000100000040000000303E301F06096086480186FD6C0201301230100 60A2B0601040182373C0101030200C0301B060567810C01033012301 0060A2B0601040182373C0101030200C00F0000000100000020000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030 0000001000000140000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D0000000100000010000000 7DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201 895E6E36EE60FFAFAB912ED06178F396200000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B0000000100000030000000440069 0067006900430065007200740020004700 6C006F006200610060C00200052006F006F00740020004700320000001900000001000000100000001 4C3BD3549EE225AECE13734AD8CA0B809000 0000100000034000000303206082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820 38E30820276A003020102021003 3AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530 13060355040A130C44696769436 5727420496E6331193017060355040B13107777772E6469676963657274 2E636F6D3120301E0603550403131744696769436572742046 5CF62616C20526F6F74204732301E170D313330383 0313132303030305A170D333830313135313230303030305A3061310B3009060355040613025553311530 13060355040A130C44696769436572742046 5CF62616C20526F6F74204732301E170D313330383 0313132303030305A170D333830313135313230303030305A3061310B3009060355040613025553311530 13060355040A130C44696769436572742046 E6331193017060355040B13107777772E6469676963657274 2E636F6D3120301E0603550403131744696769436572742046 C6F62616C20526F6F74204732308201223 00D06092A864886F70D01010105000382010F003082010A028 2010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C3 0DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD 8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD8 3E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B13383298502030100 01A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101F F040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3 CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC 9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F97050704741115 7194EC08FAE06C49513172F1B259F75F2B18E99A16F13B1 4171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE 3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

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

Value:

(PID) Process: (3208) Popis nove narudzbe u prilogu.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: write **Name:** Blob

Value: 5C0000000100000004000000008000053000000010000004000000303E301F06096086480186FD6C0201301230100 60A2B0601040182373C0101030200C0301B060567810C01033012301 0060A2B0601040182373C0101030200C00F0000000100000020000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C 24F9BFD666761B268073FE06D1CC8D4F82A41D0000000100000010000000 7DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E6E36EE60FFAFAB912ED06 178F396200000001000000200000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B0000000100000030000000440069006700690043006500720074002 200047006C006F00620061006C00200052006F006F00740020004700320000001900000001000000100000001 4C3BD3549EE225AECE13734AD8CA0B809000000001000000340000000303206082B0601050507030206082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820 38E30820276A00302010202100033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530 13060355040A130C44696769436572742046 5CF62616C20526F6F74204732301E170D313330383 0313135313230303030305A3061310B3009060355040613025553311530 13060355040A130C44696769436572742046 E6331193017060355040B13107777772E6469676963657274 2E636F6D3

120301E06035504031317446967694365727420476C6F62616C20526F6F7420473230820122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B133832985020301000 1A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B0500038201010060672894 6F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A32133981674284 23F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F97050704741115719 4EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process:	(3208) Popis nove narudzbe u prilogu.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation:	write	**Name:**	Vhzrcqhor
Value:	C:\Users\Public\Libraries\rohqcrzhV.url		

Files activity

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

Dropped files

PID	Process	Filename	Type
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** 5279CC47C895B4647090B81DF1F7D18C **SHA256:** 18ACCA8C29A35998EDD804D521D3C38DEA839F17A4C8DCFCE9B0B6BDC4F9483A	der
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** 676CEBD1A69A38C1377712A516C2E9ED **SHA256:** D5FC59DC55E513CF064F0CC2E23DD698AC5FFDE7E25BDE1A69258C7C951AF17F	binary
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** 4E08B40FAED5F0F0DF3A1B90FF786C4A **SHA256:** B923D18960DF5A5B73F7581F629591C8FD8FA64F47E12BBD1649C46D76811047	binary
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\4NCL4OVK.txt **MD5:** F1E09F5E1D5ED6F3F0494104F038A0ED **SHA256:** FB05731287027CDFEA2250473E1D41E572A1DD86FC56D190D9389803AE1BFC39	text
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** CA9F0242A185C2D5977B3CE64E1AC42A **SHA256:** 42EE46B80862F2006B147CCB3B17598054A489BB7E38454864C3FF40CB8B4402	binary
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\7OOOL5A7.txt **MD5:** A51A6288C3E09F42BBF629D398805569 **SHA256:** ECBA9E8FF3BE6EC58A8595D6CA41B8F970AF81AC846D06AA1113A85FEBF16FB4	text
3208	Popis nove narudzbe u prilogu.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 75E9E37B2AA8E2EF5E013EE4E603FCA5 **SHA256:** B59FAB5E6A633CF4F33474B96DC0398900DCF1C57E33AE6F858DCA2BC9C39169	der
3208	Popis nove narudzbe u prilogu.exe	C:\Users\Public\Libraries\rohqcrzhV.url **MD5:** FE3A117B89BF8C72C533A675F30FC875 **SHA256:** 29843EF926837A0B5981EFE90EB3EF149FC72377B7D4D9C42326F74E94B8B531	text
3208	Popis nove narudzbe u prilogu.exe	C:\Users\Public\Libraries\Vhzrcqhor.exe **MD5:** DFEA6E8EEE2E4AE2E3DF115696904386 **SHA256:** 9AD8CC5C8B88690A6A57096C475F5463A52C357F3C7FE3F8B41F3FA7830DE7B8	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
12	14	20	37

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3208	Popis nove narudzbe u prilogu.exe	GET	200	93.184.221.240:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4e4be8160861ce9b	US	compressed	4.70 Kb	whitelisted
3208	Popis nove narudzbe u prilogu.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
1068	Explorer.EXE	GET	302	34.205.242.146:80	http://www.mobilpartes.com/euv4/?uZ-D=J+MdeyNdjn26ziw9P3aP5ZUaGN75Cuu5s8ynnkBdXOwSLgaZzPNbxEu9QMf7LqltvexU1w==&9rudG=Fbj8X	US	–	–	malicious

3208	Popis nove narudzbe u prilogu.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc%3D	US	der	471 b	whitelisted
1068	Explorer.EXE	GET	503	104.16.12.194:80	http://www.tracynicolalamond.com/euv4/?uZ-D=1/mAPClvbBMCaHRQk5XpdK/41pRPdnCbNDKAlFOMWz06cn5XEx2xpg5nQyU2+UpFlYB2nA==&9rudG=Fbj8X	US	html	7.27 Kb	malicious
1068	Explorer.EXE	GET	404	31.187.72.243:80	http://www.bubu3cin.com/euv4/?uZ-D=VDDx94hjPaHzS1noFdhTsMJmJeW9wjNyCbyht0TUh81VB08yJkrdA+zF4GwFa6eGwJDqcw==&9rudG=Fbj8X	US	html	278 b	malicious
1068	Explorer.EXE	GET	–	23.227.38.74:80	http://www.boardsandbeamsdecor.com/euv4/?uZ-D=vko974XMt3yvWkptLkv3OkMzdfNnydxLjvbV1wqhg7e5xVU6+MUUbQU32ueBjFdLznzfKg==&9rudG=Fbj8X	CA	–	–	malicious
1068	Explorer.EXE	GET	403	34.102.136.180:80	http://www.encludemedia.com/euv4/?uZ-D=ebwJIxyL1q3jbCcyx34seqN8tPJ/tVGRUDi6jelVHXViP+fZszJ7j4ILRNVsCWSaNmroVg==&9rudG=Fbj8X	US	html	291 b	whitelisted
1068	Explorer.EXE	GET	403	34.102.136.180:80	http://www.oprimanumerodos.com/euv4/?uZ-D=4aEdqqr3EIF8cU83J/2KBs8ILMMDPfCfJE6P4J3SSySvUmTClzbIDMamePohhsdSUi1J9g==&9rudG=Fbj8X	US	html	291 b	whitelisted
1068	Explorer.EXE	GET	404	162.0.232.169:80	http://www.game2plays.com/euv4/?uZ-D=cl3g5knLVtCaOLcY+3za8klzbxDoXV64MSSU+WvpicB73Hm45y9QKhak0/0SkuH6Eg9f0w==&9rudG=Fbj8X	CA	html	1.21 Kb	malicious
1068	Explorer.EXE	GET	–	160.153.136.3:80	http://www.shristiprintingplaces.com/euv4/?uZ-D=q4xZ/6OMD0aijkRnul0Gkk2qmIDvEbdT0YysQv4z12Cx0yCN0pZGJkp9l0e/qzeF36BkxA==&9rudG=Fbj8X	US	–	–	malicious
1068	Explorer.EXE	GET	403	23.227.38.74:80	http://www.rematedeldia.com/euv4/?uZ-D=E+AdldMuIq72wuB5GTeilCEOXtaM5yG6oWNBj19kfBe4Loakg6E6XBt7UPPx61bF/5skdA==&9rudG=Fbj8X	CA	html	5.03 Kb	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3208	Popis nove narudzbe u prilogu.exe	13.107.42.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
3208	Popis nove narudzbe u prilogu.exe	93.184.221.240:80	ctldl.windowsupdate.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3208	Popis nove narudzbe u prilogu.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
1068	Explorer.EXE	34.205.242.146:80	www.mobilpartes.com	Amazon.com, Inc.	US	malicious
3208	Popis nove narudzbe u prilogu.exe	13.107.43.12:443	2q4faa.ph.files.1drv.com	Microsoft Corporation	US	unknown
1068	Explorer.EXE	104.16.12.194:80	www.tracynicolalamond.com	Cloudflare Inc	US	shared
–	–	23.227.38.74:80	www.boardsandbeamsdecor.com	Shopify, Inc.	CA	malicious
1068	Explorer.EXE	31.187.72.243:80	www.bubu3cin.com	–	US	malicious
1068	Explorer.EXE	23.227.38.74:80	www.boardsandbeamsdecor.com	Shopify, Inc.	CA	malicious
1068	Explorer.EXE	34.102.136.180:80	www.encludemedia.com	–	US	whitelisted
–	–	162.0.232.169:80	www.game2plays.com	AirComPlus Inc.	CA	malicious
1068	Explorer.EXE	160.153.136.3:80	www.shristiprintingplaces.com	GoDaddy.com, LLC	US	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.42.13	shared
ctldl.windowsupdate.com	93.184.221.240	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
2q4faa.ph.files.1drv.com	13.107.43.12	unknown
www.crux-at.com	–	unknown
www.mobilpartes.com	34.205.242.146 54.161.222.85	malicious
www.tracynicolalamond.com	104.16.12.194 104.16.16.194 104.16.14.194 104.16.13.194 104.16.15.194	malicious
www.alert78.info	–	malicious
www.bubu3cin.com	31.187.72.243	malicious

www.boardsandbeamsdecor.com	23.227.38.74	malicious
www.encludemedia.com	34.102.136.180	whitelisted
www.oprimanumerodos.com	34.102.136.180	whitelisted
www.game2plays.com	162.0.232.169	malicious
www.rematedeldia.com	23.227.38.74	malicious
www.shristiprintingplaces.com	160.153.136.3	malicious
www.laidbackfurniture.store	—	malicious
www.berylgrote.top	—	malicious
www.lankasirinspa.com	—	malicious

Threats

PID	Process	Class	Message
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	Generic Protocol Command Decode	SURICATA HTTP Unexpected Request body
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)

1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
1068	Explorer.EXE	A Network Trojan was detected	ET TROJAN FormBook CnC Checkin (GET)
–	–	Potentially Bad Traffic	ET DNS Query to a *.top domain - Likely Hostile

Debug output strings

No debug info