

General Info

35caf9822bd606a8c3f8cd650d2a8e24.exe File name:

Full analysis: https://app.any.run/tasks/f85030e4-ee25-460a-897e-30175158561c

Verdict: Malicious activity Analysis date: August 18, 2022 at 18:27:54

Windows 7 Professional Service Pack 1 (build: 7601, 32 bit) OS:

Indicators: MIME: application/x-dosexed

PE32 executable (GUI) Intel 80386, for MS Windows File info: 35CAF9822BD606A8C3F8CD650D2A8E24 MD5: SHA1: D33F4D2A3BCB4DFD8EB3142354AEA0937662B779

1D428C9072467D19BF60AAE861E9B64885616537970ACB7F78FEE71D20242526 SHA256: SSDEEP:

Software environment set and analysis options

Launch configuration

Task duration: 120 seconds Heavy Evasion option: off Network geolocation: off

MITM proxy: Public submission Additional time used: none off Privacy:

Fakenet option: Route via Tor: off Autoconfirmation of UAC: off

Network:

Hotfixes Software preset

Internet Explorer 11.0.9600.19596 KB4534251 Client LanguagePack Package

Adobe Acrobat Reader DC (20.013.20064) Client Refresh LanguagePack Package Adobe Flash Player 32 ActiveX (32.0.0.453) CodecPack Basic Package

Adobe Flash Player 32 NPAPI (32.0.0.453) Foundation Package

Adobe Flash Player 32 PPAPI (32.0.0.453) IE Hyphenation Parent Package English Adobe Refresh Manager (1.8.0) IE Spelling Parent Package English

IE Troubleshooters Package CCleaner (5.74) FileZilla Client 3.51.0 (3.51.0) InternetExplorer Optional Package

Google Chrome (86.0.4240.198) InternetExplorer Package TopLevel Google Update Helper (1.3.36.31) KB2479943

Java 8 Update 271 (8.0.2710.9) KB2491683 Java Auto Updater (2.8.271.9) KB2506212 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) KB2533552

Microsoft Office Access MUI (German) 2010 (14.0.4763.1000) KB2533623 Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000) KB2534111

Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000) KB2545698 Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000) KB2547666

Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000) KB2552343

Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000) KB2564958

Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013) KB2574819 Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000) KB2579686

Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000) KB2585542 Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000) KB2604115

Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000) KB2620704 Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000) KB2621440 Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000) KB2631813

Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000) KB2639308 Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000) KB2640148 Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000) KB2653956

Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000) KB2654428 Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013) KB2656356 Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000) KB2660075

Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000) KB2667402 Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000) KB2676562 Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000) 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

KB2560656

2,	10:09 PM 1d428c9072467d19bf60aae861e9b6488561653797	0acb7f78fee
	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

2,	10:09 PM	1d428c9072467d19bf60aae861e9b6488	5616537970acb7f78f
		Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
		Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
		Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
		Proof (Russian) 2010 (14.0.4763.1000) Proof (Spanish) 2010 (14.0.6029.1000)	KB3004375
		Proof (Spanish) 2010 (14.0.6029.1000) Proof (Turkish) 2010 (14.0.4763.1013)	KB3006121 KB3006137
		Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3000137
		Proofing (English) 2010 (14.0.6029.1000)	KB3010760
		Proofing (French) 2010 (14.0.4763.1000)	KB3013531
		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
		Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
		Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
		Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
		Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
		Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
		Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
		Publisher MUI (Korean) 2010 (14.0.4763.1000) Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046017 KB3046269
		Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3046269 KB3054476
		Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
		Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
		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
		SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
		SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
		Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
		Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
		Shared MUI (German) 2010 (14.0.4763.1000) Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3092601 KB3093513
		Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3093313
		Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
		Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
		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
		Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
		Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
		Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
		Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
		Word MUI (Spanish) 2010 (14.0.4763.1000) Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3133977 KB3137061
		X MUI (French) 2010 (14.0.4763.1010)	KB3137001
		X MUI (German) 2010 (14.0.4763.1000)	KB3138612
		X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
		X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
		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
		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 OGA (2 14 33) KR4474419 Skype version 8.29 (8.29) KR4490628 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

Behavior activities

MALICIOUS

Changes the autorun value in the registry 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Changes settings of System certificates 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Drops executable file immediately after starts 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

SUSPICIOUS

Checks supported languages

35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444) 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 3284)

Reads the computer name

35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Application launched itself

35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 3284)

Executable content was dropped or overwritten 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Drops a file with a compile date too recent 35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Adds / modifies Windows certificates

35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

INFO

WUClient SelfUpdate Core TopLevel WinMan WinIP Package TopLevel

Checks Windows Trust Settings

Reads settings of System Certificates

35caf9822bd606a8c3f8cd650d2a8e24.exe (PID: 2444)

Reads the computer name

icacls.exe (PID: 3180)

Checks supported languages

icacls.exe (PID: 3180)

Static information

TRID EXIF

| Win32 Dynamic Link Library (generic) (43.5) | Win32 Executable (generic) (29.8)

| Generic Win/DOS Executable (13.2) .exe | DOS Executable Generic (13.2)

FXF

FileSubtype: 0

ObjectFileType: Executable application FileOS: Windows NT 32-bit FileFlags: (none) FileFlagsMask: 0x003f 64.0.0.0 ProductVersionNumber:

7.0.0.0

Subsystem: SubsystemVersion: 5 ImageVersion: OSVersion: 5 EntryPoint: 0x92c0 UninitializedDataSize: 0 InitializedDataSize: 42673664 CodeSize: 151040 LinkerVersion: 9

TimeStamp: 2022:02:19 05:48:52+01:00 MachineType: Intel 386 or later, and compatibles

PF32

Summary

Architecture: IMAGE_FILE_MACHINE_I386 Subsystem: IMAGE_SUBSYSTEM_WINDOWS_GUI

Compilation Date: 19-Feb-2022 04:48:52 Detected languages: Korean - Korea

Debug artifacts: C:\figipe42_heganuvuvutas v.pdb

DOS Header

MZ Magic number: Bytes on last page of file: 0x0090 Pages in file: 0x0003 0x0000 Relocations: Size of header: 0x0004 Min extra paragraphs: 0x0000 0xFFFF Max extra paragraphs: Initial SS value: 0x0000 Initial SP value: 0x00B8 Checksum: 0x0000 Initial IP value: 0x0000 Initial CS value: 0x0000 Overlay number: 0x0000 OEM identifier: 0x0000 OEM information: 0x0000 0x000000D8 Address of NE header:

PE Headers

PEType:

Signature: PΕ

Machine: IMAGE_FILE_MACHINE_I386

Number of sections:

19-Feb-2022 04:48:52 Time date stamp: Pointer to Symbol Table: 0x00000000 Number of symbols: 0 Size of Optional Header: 0x00E0

Characteristics: IMAGE_FILE_32BIT_MACHINE

> IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x00024CD8	0x00024E00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.04315
.data	0x00026000	0x0288F700	0x00092800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.99208
.rsrc	0x028B6000	0x0000F2F8	0x0000F400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.17952

Resources

Title	Entropy	Size	Codepage	Language	Туре
1	5.16369	1736	UNKNOWN	Korean - Korea	RT_ICON
2	5.45057	1384	UNKNOWN	Korean - Korea	RT_ICON
3	5.5073	4264	UNKNOWN	Korean - Korea	RT_ICON
4	5.61873	2440	UNKNOWN	Korean - Korea	RT_ICON
5	6.05036	1128	UNKNOWN	Korean - Korea	RT_ICON
6	6.38996	9640	UNKNOWN	Korean - Korea	RT_ICON
7	6.8227	4264	UNKNOWN	Korean - Korea	RT_ICON
8	4.27221	3752	UNKNOWN	Korean - Korea	RT_ICON
9	4.9364	2216	UNKNOWN	Korean - Korea	RT_ICON
10	5.1558	1736	UNKNOWN	Korean - Korea	RT_ICON
11	4.88179	1384	UNKNOWN	Korean - Korea	RT_ICON
12	3.05799	9640	UNKNOWN	Korean - Korea	RT_ICON
13	3.38362	4264	UNKNOWN	Korean - Korea	RT_ICON
14	3.32183	2440	UNKNOWN	Korean - Korea	RT_ICON

15	3.36124	1128	UNKNOWN	Korean - Korea	RT_ICON
16	4.09164	304	UNKNOWN	Korean - Korea	RT_CURSOR
17	2.5416	304	UNKNOWN	Korean - Korea	RT_CURSOR
18	2.50404	240	UNKNOWN	Korean - Korea	RT_CURSOR
19	1.59806	4264	UNKNOWN	Korean - Korea	RT_CURSOR
20	2.97359	2216	UNKNOWN	Korean - Korea	RT_CURSOR
26	3.0109	334	UNKNOWN	Korean - Korea	RT_STRING
27	3.13751	460	UNKNOWN	Korean - Korea	RT_STRING
28	1.854	68	UNKNOWN	Korean - Korea	RT_STRING
125	2.38706	34	UNKNOWN	Korean - Korea	RT_GROUP_ICON
128	2.91481	118	UNKNOWN	Korean - Korea	RT_GROUP_ICON
129	2.72482	76	UNKNOWN	Korean - Korea	RT_GROUP_ICON
191	3.09656	96	UNKNOWN	Korean - Korea	RT_ACCELERATOR
460	3.14902	316	UNKNOWN	Korean - Korea	RT_VERSION
591	3.12537	104	UNKNOWN	Korean - Korea	RT_ACCELERATOR
2371	1.98048	20	UNKNOWN	Korean - Korea	RT_GROUP_CURSOR
2374	2.55787	48	UNKNOWN	Korean - Korea	RT_GROUP_CURSOR
2375	1.9815	20	UNKNOWN	Korean - Korea	RT_GROUP_CURSOR

Imports

ADVAPI32.dll	
KERNEL32.dll	
USER32.dll	

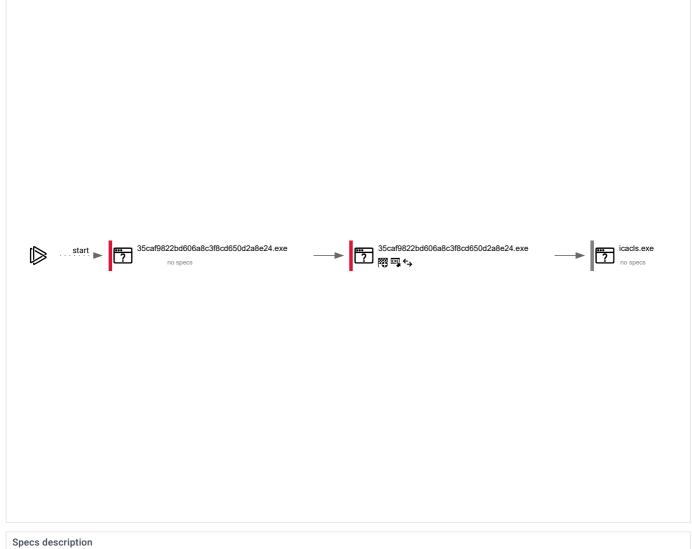
Video and screenshots

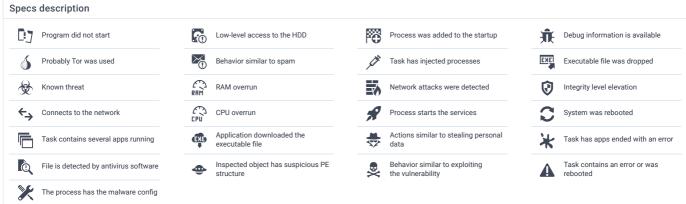


Processes

Total processes Monitored processes Malicious processes Suspicious processes 39 3 2 0

Behavior graph





Process information

PID	CMD	Path	Indicators	Parent process
3284	650d2a8e24.exe"	C:\Users\admin\AppData\Local\Temp\35caf9822bd606a8c3f8cd650d2a8e24.exe	-	Explorer.EXE
Informa	ition			
User: Exit c				

Registry activity

Total events Write events Read events Delete events

5 3 7 7 5 2 9 0 83 4

Modification events

(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation:	write	Name:	ProxyEnable
Value: 0			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER\\ Software\\ \ Microsoft\\ \ Windows\\ \ Current\\ \ Version\\ \ Internet\ Settings\\ \ Connections$
Operation:	write	Name:	SavedLegacySettings
0000000		0000000	00000400000000000000C0E333BBEAB1D3010000000000000000000000000000000000
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Current\\Version\\Internet\ Settings\\5.0\\Cache\\Content$
Operation:	write	Name:	CachePrefix
Value:			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet\ Settings\\5.0\\Cache\\Cookies$
Operation:	write	Name:	CachePrefix
Value: Cookie:			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet\ Settings\\5.0\\Cache\\History$
Operation:	write	Name:	CachePrefix
Value: Visited:			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER \setminus Software \setminus Microsoft \setminus Windows \setminus Current Version \setminus Internet\ Settings \setminus Zone Map$
Operation:	write	Name:	ProxyBypass
Value: 1			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER \setminus Software \setminus Microsoft \setminus Windows \setminus Current Version \setminus Internet\ Settings \setminus Zone Map$
Operation:	write	Name:	IntranetName
Value: 1			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER \setminus Software \setminus Microsoft \setminus Windows \setminus Current Version \setminus Internet\ Settings \setminus Zone Map$
Operation:	write	Name:	UNCAsIntranet
Value: 1			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$HKEY_CURRENT_USER \setminus Software \setminus Microsoft \setminus Windows \setminus Current Version \setminus Internet\ Settings \setminus Zone Map$
Operation:	write	Name:	AutoDetect
Value: 0			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$\label{lem:likely_current} HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet\ Settings\\Wpad\\\{FCC67766-6201-4AD1-A6B8-2F4553C93D47\}$
Operation:	write	Name:	WpadDecisionReason
Value: 1			
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	$\label{lem:hkey_current} \begin{tabular}{l} HKEY_CURRENT_USER\software\Microsoft\Windows\Current\Version\Internet\ Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47} \end{tabular}$
Operation:	write	Name:	WpadDecisionTime
Value: 30DBF1	3102B3D801		
(PID) Process:	(2444) 35caf9822bd606a8c3f8cd65 0d2a8e24.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}

1d428c9072467d19bf60aae861e9b64885616537970acb7f78fee71d20242526 | ANY.RUN - Free Malware Sandbox Online Name: WpadDecision Operation write Value: 0 (PID) Process: (2444) 35caf9822bd606a8c3f8cd65 Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-4D1 2F4553C93D47 WpadNetworkName Operation Name Value: Network 3 (2444) 35caf9822bd606a8c3f8cd65 Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff (PID) Process: 0d2a8e24.exe Operation WpadDecisionReason Name Value: (2444) 35caf9822bd606a8c3f8cd65 Key: (PID) Process: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff 0d2a8e24.exe Operation: write Name: WpadDecisionTime Value: 30DBF13102B3D801 Key: (PID) Process: (2444) 35caf9822bd606a8c3f8cd65 HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff Operation Value: 0 (2444) 35caf9822bd606a8c3f8cd65 HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E (PID) Process: Key: 0d2a8e24.exe Operation Name: LanguageList Value: en-US (2444) 35caf9822bd606a8c3f8cd65 Key: (PID) Process:

0d2a8e24.exe AB9AD8E Operation

040000000100000010000001BFE69D191B71933A372A80FE155E5B509000000010000054000000305206082B0601050507030206082B06010505070303060A2B0601040182370A030406082B0601050507030406082B0601050507030606082B0601050507030706082B0601050507030106082B060105050703080F000000010000003000000066B764A96581128168CF208E3740DA 479D54E311F32457F4AEE0DBD2A6C8D171D531289E1CD22BFDBBD4CFD979625483030000001000000140000002BF1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0B000000100000010 0000005300650063007400690067006F000001D0000010000010000010000085010358D29A38F059R028559C95F9014000000110000014000005379RF5AAA2RF4ACF5480F1D89RC09DF2 $\frac{13025553311330110603550408130A4E65777204A65727365793114301206035504071308A65727365792043697479311E301C060355040A131554686520555345525452555354204E65747756792043697479311E301C060355040A1313534686520555345525452555354204E65747756792043697479301E170D3130303230313030303030305170D333830313138323353935395A308188310B3009060355040613025553311330110603550408130A4E6577204A6572736579211430120603550407130B4A65727365792043697479311E301C060355040A1$ 403020106300F003351D13011FF0403500301011F14300050092A864886F70D10110C05000332020110050C47C0DDCFF7017D419950C73C5529FCBF8CF99067F1BDA43159F9E0255579614F
1523027879428ED1F3A0137A276FC5350C0849B0668B4BBA8C214FA28E55629FF369150B8088E3C4AA0BFDEFA8E94B55E2A919EE5F305C48E2195FE249A6E5E2A28EE0B4D9
F7FF70138941495430709FB60A9EE1CAB128CA09A5EA7986A596D8B3F08FBC8D145AF18156490120F73282EC5E2244EFC58ECF0F445FE22B3EB2F8ED2D9456105C1976FA876728F8B8C36
AFBF0D035C718DE6A666F1F6CA67162C5D8D083720CF16711890C9C134C72340FBCD571DFAA71DDE1B96C8C3C125D65DABD57122B6436BFFE5DE4D661151CF99AEEC17B6E871918CDE49
FEDD3571A21527941CCF61E326B86FA36725215DE6DD1D0B2E681B3B82AFEC836785D4985174B1B9998089FF7F8195C794A602E9240AE4C372A2CCC9C762C80E5DF7365BCAE0252501B4
DD1A079C77003FD0D0CD5EC3DD4FABB3FCC85D66F7FA92DDFB902F7F5979AB535DAC367B0874AA9289E238EFF5C276BE1B04FF307EE002ED45987C8524195EAF4447D7EE6441557C8D5590
295D0629DC289EE5A28748AA59B8790C70C07DFF589367432D628C1B0B00BE09C4CC31CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7B857088AE3E19CF4028D8FCC890

(2444) 35caf9822bd606a8c3f8cd65 Key: $HKEY_LOCAL_MACHINE \\ SOFTWARE \\ Microsoft \\ System Certificates \\ AuthRoot \\ Certificates \\ 2B8F1B57330DBBA2D07A6C51F70EE90DD \\ Machine \\ Machin$ 0d2a8e24.exe AB9AD8E

delete key (default) Operation Name:

BB5D9922F552E658C51F883143EE881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD

Value:

(2444) 35caf9822bd606a8c3f8cd65 Key: (PID) Process:

0d2a8e24.exe

 $HKEY_LOCAL_MACHINE \\ SOFTWARE \\ Microsoft \\ System Certificates \\ AuthRoot \\ Certificates \\ 2B8F1B57330DBBA2D07A6C51F70EE90DD$ AB9AD8F

Name: Operation

Bloh

 $500000001100000014000000011000009000000110000005400000030520608280601050507030206082806010505070303060A\\ 2806010505070303060A\\ 280601040182370A03040608280601050507030406082806$ 5354204E6574776F726B312E302C06035504031325555345525472757374205253412043657274696696174696F6E20417574686F7269747930820222300D06092A864886F70DD101010105 000382020F003082020A028202010080126517360EC3DB08B3D0AC570D76EDCD27D34CAD508361E2AA204D092D6409DCCE899FCC3DA9ECF6CFC1DCF1D3B1D67B3728112B47DA39C6BC 3A19B45FA6BD7D9DA36342B676F2A93B2B91F8E26FD0EC162090093EE2E874C918B491D46264DB7FA306F188186A90223CBCFE13F087147BF6E41F8ED4E451C61167460851CB8614543FB C33FE7E6C9CFF169D18BD518E35A6A766C87267DB2166B1D49B7803C0503AE8CCF0DCBC9E4CFEAF0596351F575AB7FFCEF93DB72CB6F654DDC8E7123A4DAE4C8AB75C9AB4B7203DCA7 F2234AE7E3B68660144E7014E46539B3360F794BE5337907343F332C353EFDBAAFE744E69C76B8C6093DEC4C70CDFE132AECC933B517895678BEE3D56FE0CD0690F1B0FF325266B336DF76E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490BDFD8808A0993628EB566CF2588CD84B8B13FA4390FD9029EEB124C957 CF36B05A95E1683CCB867E2E8139DCC5B82D34CB3ED5BFFDEE573AC233B2D00BF3555740949D849581A7F9236E651920EF3267D1C4D17BCC9EC4326D0BF415F40A94444F499E757879E5 E881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD

(2444) 35caf9822bd606a8c3f8cd65 **Key**: 0d2a8e24.exe $HKEY_LOCAL_MACHINE \\ SOFTWARE \\ Microsoft \\ System Certificates \\ AuthRoot \\ Certificates \\ D1EB23A46D17D68FD92564C2F1F1601764D8E349$ (PID) Process:

Name: Operation

 $7A0F85D722731D771E9484EBCDEF71D5F0C3E0A2948782E083EE0EA699EF419000000100000010000002A1C05E2AE606F198C2C5E93F097AA2530000000100000030413022\\060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0200000000100000364400003\\08204323082031AA003020102020101300D06092A864886F70D0101050500307B310B3009060355040613024742311B301906035504080C1247726561746572204D616E6368657374657231$ 46520536572766963657330820122300D06092A864886F70D01010105000382010F003082010A0282010100BE4090F46EF1EA76871C4D45448EBE46C883069DC12AFF181F8EE402FAF3AB5 D508A1631089A06D0C57022CD492D5463CCB66E68460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360EZDA8955F32258F3DEDCCFEF8386A28C944F9F6BF29890468427C776 BFE3CC352C8B5E07646582C048B0A891F9619F762050A891C766B5EB78620355608A1A13EA31AA099FD38F6F62732586F07F56BB8FB142BAFB7AACCD6635F738CDA0599A838A8CE77678386A28C7467B38CA0599EA784502035608A1A13EA31AA31EA099FD38F6F62732586F07F56BB8FB142BAFB7AACCD6635F738CDA0599A838A8CE7767838A3C02008180310098D58D50203849C0D5 EE82F90203010001A381C030381B0301D06035551D0E0116041A40110A233296F1079CE2AF29EF82A57FD030A4M8300E0603551D0F101F10F040403020106309F0603551D1011FF400503551D0F0116047430723398A036A0348632687474703A2F2F63726C2E636F6D6F646F63612E636F6D2F414141436572746966696361746553657276696365732E63726C3036A0 34A0328630687474703A2F2F63726C2E65742F414141436572746966696361746553657276696365732E63726C20300000092A864886F70D010105050003820101000856F C02F09BB8FFA4FA0F8C64480CE4FC4CSF60058CCA6BB6614496804768EB6EE5DEC09F06B05184F264E0F18256B0A5EBFBC745441BFFDFC12B8C74F55AF48960057F60B7054A7850CE488960057F608B051847664480CE4F4C4CSF60058CCA6BB6614496804768EB6EE5DEC09F06B0518AF264E0F18256B0A5EBFBE7C5444B8FDFDC712B8C74F55AF48960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE488960057F60B7054A7850CE48897486B62D7D6BCCD2F346DD2FC6E06AC3C334032C7D96DD5AC20EA70A99C1058BAB0C2FF35C3ACF6C37550987DE53406C58EFFCB6AB656E04F61BDC3CE05A15C69ED9F1594 8302165036CECE92173EC9B03A1E037AA0A01518BFFABA02CEA7CA9910139039795E93696986E 46520536572766963657330820122300D06092A864886F70D01010105000382010F003082010A0282010100BF409DF46FF1FA76871C4D45448FBF46C883069DC12AFF181F8FF402FAF3AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402FAF5AB5402F81B56B85D7BE2DED3F1AB7B263E2F5622C82D46A004150F139839F95E93696986E

(2444) 35caf9822bd606a8c3f8cd65 **Key:** 0d2a8e24.exe (PID) Process:

 $HKEY_LOCAL_MACHINE \\ SOFTWARE \\ Microsoft \\ System Certificates \\ AuthRoot \\ Certificates \\ D1EB23A46D17D68FD92564C2F1F1601764D8E349$

(default

Operation Value

(PID) Process: (2444) 35caf9822bd606a8c3f8cd65 Key:

Name: Blob Operation:

 $0130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C0301B060355040613024742311B301906035504080C1247726561746572204D616E636865737465723110300E06035504070C0753616C\\66667264311A3018060355040A0C11436F6D6F646F204341204C696D697465643121301F06035504030C18414141204365727469666963617465205365727669636573301E170D303430313$ 0313030303030305A170D3238313233313233353935395A307B310B3009060355040613024742311B301906035504080C1247726561746572204D616E6368857374657223110300E06035504
070C0753616C66667264311A3018060355040A0C11436F6D6F646F204341204C696D697465643121301F06035504030C1841414120436572746996696361746520536572766963657330820
122300D06092A864886F70D0110105000382010F0003082010A0282010100BE409DF46EE1EA76871C4D45448EBE46C883069DC12AFE181F8EE402FAF3AB5D508A16310B9A06D0C57022CD
492D5463CCB66E684460B53EACB4C24C0BC724EEAF115AEF4549A120AC37AB23360E2DA8955F32258F3DEDCCFEF8386A286944F9F68F29890468427C776BFE3CC352C8B5E07646582C048 49219403CL6666106401053CL6661264CUB0724EEAF113AE743493120AC37AB23360E2DA693753220875DEDCFFF63360A2C944F9F60F299406427C7769F53CS32C665E07440582CU466
B0A89176619F762050A891C766B5EB78620356F08A1A13EA31A31EA099FD38F6F62732586F07F56B8FB142BAFB7AACCD6635F738CDA05999A838A8CB17783651ACE99EF4783A8DCF0FD9
42E2980CAB2F9F0E01DEEF9F9949F12DDFAC744D1B98B547C5E529D1F99018C762926E83C7267B3E8A25C7C0DD9DE6356810209D8FD8DED2C3849C0D5EE82FC90203010001A381C03081
BD301D0603551D0E04160414A0110A233E96F107ECE2AF29EF82A57FD030A4B4300E0603551D0F0101FF040403020106300F0603551D130101FF040530030101FF307B0603551D1F047430 F5622C82D46A004150F139839F95E93696986E

(PID) Process: (2444) 35caf9822bd606a8c3f8cd65 Key:

0d2a8e24.exe

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

 $"C:\lbers\admin\AppData\Local\6040702c-cb75-42cb-9fc7-2f9d9eb9bd55\35caf9822bd606a8c3f8cd650d2a8e24.exe" -- AutoStart --$

Files activity

Executable files Suspicious files Text files Unknown types

1 0 3

Dropped files

PID	Process	Filename	Туре
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$localLowMicrosoftCryptnetUrlCacheContentB2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB60\\ 6228BC7A711E$	der
		MD5: AF87F050F5460889E174155A00AAE96E SHA256: A6875F0E4B237FEFCF65BDDE221052C7D14F87E9ACCFA0A06288E485	4B9077A6
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$C: \label{localLowMicrosoftCryptnetUrlCache} Content \S 7C8EDB 95DF 3F 0AD 4EE 2DC2B8 CFD 4157$	compressed
		MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701C	B927E36EA
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$C: \label{localLowMicrosoft} C: \label{localLocalLowMicrosoft} C: \label{localLocalLowMicrosoft} C: localLocalLocalLocalLocalLocalLocalLocal$	binary
		MD5: ABEB550DD95838A250F789A520972FE1 SHA256: 99DA2D987375A4EC94F5AC41CE19108A4240322EB8BC986D1930D6F2	22652C06E
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$C: \label{localLowMicrosoftCryptnetUrlCache} C: \label{localLocalLowMicrosoftCryptnetUrlCache} C: localLocalLocalLocalLocalLocalLocalLocal$	binary
		MD5: 2570BC388653944A64E63FF40DD108A3 SHA256: CBB5D2A60738B20D1E37E74BB7774515BB38DB1F3FD32A89AD1F4836	6DA5C15FB
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$ C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB6 06228BC7A711E $	binary
		MD5: E2210575F7AA10384E3C428F9A0B2792 SHA256: A33708B412F225B0A737B9A949C832F8B22342CB4BBFB97C84F14E1E	BE1AD8D4A
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$\label{thm:cond} C:\label{thm:cond} C:thm:$	binary
		MD5: 3A496034DF19E5F8C8D559FCAC638D93 SHA256: 76B7352380EA95F9A502D92AB83D747399DC581AC965B906201BCBD	708C93408
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$\label{thm:content} C:\label{thm:content} $	der
		MD5: FFA2C78A5E2A664F24CD259527B3D6CA SHA256: 331171ECE4D5B26022678BB0736FAB61A2B194C82CB4296865658636	A46A5EC7
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$C:\label{localLowMicrosoft} CryptnetUrlCache\\ Content\\ 07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB78182E9902850D$	der
		MD5: 3D4C1DE1F149182348CBDC85F4801C13 SHA256: 094E9CB02BEBB5D8A5BFBE0E83D3C0064D0F0E3A3F4ECCE0215FDCB	DA9FAB938
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	$C:\label{localLowMicrosoft} C:\label{localLowMicrosoft} C:\label{localLocalLowMicrosoft} C:\label{localLocalLocalLowMicrosoft} C:localLocalLocalLocalLocalLocalLocalLocal$	binary

		MD5: 3E3FD99C572AEB0B4A9B098862597B21	SHA256: 6CD89BFDEC87667C0AE8389747021B3DBF4545CD301E0F044835862345	53FA7CB	
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	C:\Users\admin\AppData\Local\6040702c-cb75-42cb-9fc7-2	7-2f9d9eb9bd55\35caf9822bd606a8c3f8cd650d2a8e24.exe execut		
		MD5: 35CAF9822BD606A8C3F8CD650D2A8E24	SHA256: 1D428C9072467D19BF60AAE861E9B64885616537970ACB7F78FEE71D202425		

Network activity

HTTP(S) requests DNS requests TCP/UDP connections Threats 4 5 6 3

HTTP requests

Process	Method	HTTP Code	IP	URL	CN	Туре	Size	Reputation
35caf9822bd606a 8c3f8cd650d2a8e 24.exe	GET	200	67.27.159.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static /trustedr/en/disallowedcertstl.cab?4a4852172227125e	US	compressed	4.70 Kb	whitelisted
35caf9822bd606a 8c3f8cd650d2a8e 24.exe	GET	200	172.64.155.188:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCG gUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs 4q8p74KIf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D	US	der	1.42 Kb	whitelisted
35caf9822bd606a 8c3f8cd650d2a8e 24.exe	GET	200	172.64.155.188:80	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl	US	der	978 b	whitelisted
35caf9822bd606a 8c3f8cd650d2a8e 24.exe	GET	200	172.64.155.188:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGg UABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorS s9Ug0HYm8Cd8rlDZssCEH1bUSa0droR23QWC7xTDac%3D	US	der	2.18 Kb	whitelisted
	35caf9822bd606a 8c3f8cdd50d2a8e 24.exe 35caf9822bd606a 8c3f8cd650d2a8e 24.exe 35caf9822bd606a 8c3f8cd650d2a8e 24.exe 35caf9822bd606a 8c3f8cd650d2a8e	35caf9822bd606a GET 8c3f8cd650d2a8e 24.exe Sc3f8cd650d2a8e GET 35caf9822bd606a GET 8c3f8cd650d2a8e GET 8c3f8cd650d2a8e GET 8c3f8cd650d2a8e GET 8c3f8cd650d2a8e GET 8c3f8cd650d2a8e	35caf9822bd606a GET 200 8c3f8cd650d2a8e 24.exe 200 35caf9822bd606a GET 200 35caf9822bd606a GET 200 35caf9822bd606a GET 200 8c3f8cd650d2a8e 24.exe 200 35caf9822bd606a GET 200 8c3f8cd650d2a8e 24.exe 200	35caf9822bd606a GET 200 67.27.159.254:80 8c3f8cd650d2a8e 24.exe 200 172.64.155.188:80	35caf9822bd606a	35caf9822bd606a	35caf9822bd606a GET 200 67.27.159.254:80 http://ctldl.windowsupdate.com/msdownload/update/v3/static US compressed /trustedr/en/disallowedcertstl.cab?4a4852172227125e	35caf9822bd606a GET 200 67.27.159.254:80 http://ctldl.windowsupdate.com/msdownload/update/v3/static US compressed 4.70 Kb 8c3f8cd650d2a8e 24.exe 200 172.64.155.188:80 http://csp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCG US der 1.42 Kb 24.exe 200 172.64.155.188:80 http://csp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCG US der 2.4 exe 4q8p74Kif9AwpLQCEDlyRDr5irdR19NsEN0xNZU%3D 4er 978 b 8c3f8cd650d2a8e 24.exe 25caf9822bd606a GET 200 172.64.155.188:80 http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl US der 978 b US 25caf9822bd606a GET 200 172.64.155.188:80 http://csp.usertrust.com/USERTrustRSACertificationAuthority.crl US der 2.18 Kb UABBTNMNJMNDQCqx8FcBWK16EHdimS6QQUU3m%2FWqqrS

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	172.64.155.188:80	ocsp.comodoca.com	-	US	suspicious
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	67.27.159.254:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	malicious
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	104.18.32.68:80	ocsp.comodoca.com	Cloudflare Inc	US	suspicious

DNS requests

Domain	IP	Reputation
api.2ip.ua	162.0.217.254	shared
ctldl.windowsupdate.com	67.27.159.254	whitelisted
	67.27.235.254	
	8.248.141.254	
	8.238.191.126	
	8.241.121.126	
ocsp.comodoca.com	172.64.155.188	whitelisted
	104.18.32.68	
ocsp.usertrust.com	104.18.32.68	whitelisted
	172.64.155.188	
crl.usertrust.com	172.64.155.188	whitelisted
	104.18.32.68	tonoted

Threats

PID	Process	Class	Message
_	-	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
2444	35caf9822bd606a8c3f8cd650d 2a8e24.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)

Debug output strings

10/15/22, 10:09 PM

