






General Info

File name:	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23
Full analysis:	https://app.any.run/tasks/c2d6e541-ab06-45af-b588-cd889dcab32b
Verdict:	Malicious activity
Analysis date:	August 22, 2022 at 10:03:41
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojanstealer
Indicators:	  
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	24AD5D3DD00A5C74B2280AF26FF854D7
SHA1:	60081AE7B16738FA8315C650B240C82919044478
SHA256:	35E67BF049CB9C2D9C6AF0F2F29FFFE0279A0953732240B6CDC7C1B12121D23
SSDEEP:	6144:2e5lgH1bq3YhWeJB4Q0qXmRj/Ac08xtlxODiw/qyD2/k0sEuvXX8:756bqohWIB7XqYZ+xOV/q3PsA

Software environment set and analysis options

Launch configuration

Task duration:	180 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	120 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
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)

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Portuguese (Brazil)) 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

KB2685813

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)	KB31110329
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
Drops executable file immediately after starts 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Checks supported languages 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Reads settings of System Certificates 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)
Stealing of credential data 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Reads the computer name 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Checks Windows Trust Settings 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)
Loads dropped or rewritten executable 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Executable content was dropped or overwritten 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	
Steals credentials from Web Browsers 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Creates files in the program directory 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	
Actions looks like stealing of personal data 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	Drops a file with a compile date too recent 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	
	Reads Environment values 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	
	Reads CPU info 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	
	Searches for installed software 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe (PID: 2956)	

Static information

TRiD	EXIF
------	------

```

EXE
MachineType: Intel 386 or later, and compatibles
TimeStamp: 2021:09:25 04:58:17+02:00
PEType: PE32
LinkerVersion: 9
CodeSize: 151552
InitializedDataSize: 42228224
UninitializedDataSize: 0
EntryPoint: 0x9810
OSVersion: 5
ImageVersion: 0
SubsystemVersion: 5
Subsystem: Windows GUI
FileVersionNumber: 66.0.0.0
ProductVersionNumber: 71.0.0.0
FileFlagsMask: 0x003f
FileFlags: (none)
FileOS: Windows NT 32-bit
ObjectFileType: Executable application
FileSubType: 0

```

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	25-Sep-2021 02:58:17
Detected languages:	Korean - Korea
Debug artifacts:	C:\hihomu.pdb

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
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
Address of NE header:	0x000000E0

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	25-Sep-2021 02:58:17
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

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x00024EC2	0x00025000	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.03128
.data	0x00026000	0x02822960	0x00028E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.94673
.rsrc	0x02849000	0x0000F560	0x0000F600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.16744

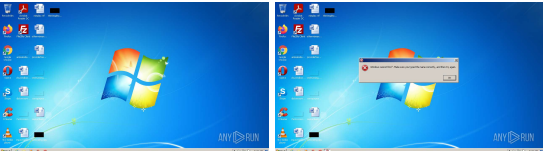
Title	Entropy	Size	Codepage	Language	Type
1	5.16369	1736	UNKNOWN	Korean - Korea	RT_ICON
2	5.45057	1384	UNKNOWN	Korean - Korea	RT_ICON
3	5.5073	4264	UNKNOWN	Korean - Korea	RT_ICON
4	5.61873	2440	UNKNOWN	Korean - Korea	RT_ICON
5	6.05036	1128	UNKNOWN	Korean - Korea	RT_ICON
6	6.39323	9640	UNKNOWN	Korean - Korea	RT_ICON
7	6.80952	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	UNKNOWN	RT_CURSOR
17	2.5416	304	UNKNOWN	UNKNOWN	RT_CURSOR
18	2.50404	240	UNKNOWN	UNKNOWN	RT_CURSOR
19	1.59806	4264	UNKNOWN	UNKNOWN	RT_CURSOR
20	2.97359	2216	UNKNOWN	UNKNOWN	RT_CURSOR
26	3.01209	326	UNKNOWN	Korean - Korea	RT_STRING
27	3.13604	468	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	3.04819	88	UNKNOWN	Korean - Korea	RT_ACCELERATOR
429	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
432	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
437	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
442	1.84644	10	UNKNOWN	Korean - Korea	UNKNOWN
446	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
453	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
456	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
457	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
460	3.15091	320	UNKNOWN	UNKNOWN	RT_VERSION
591	3.12537	104	UNKNOWN	Korean - Korea	RT_ACCELERATOR
2371	1.98048	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
2374	2.55787	48	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
2375	1.9815	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR

Imports

KERNEL32.dll
USER32.dll

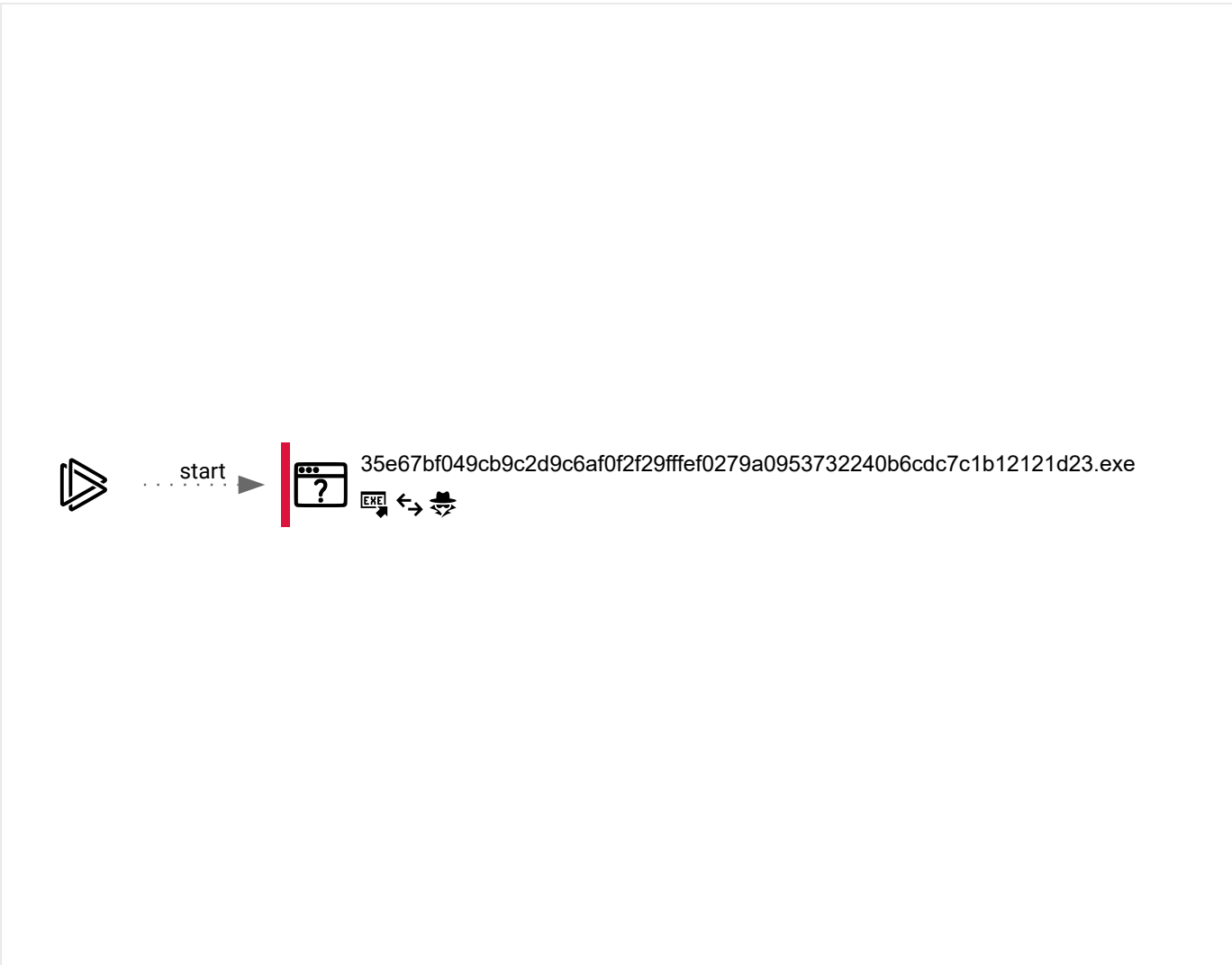
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
35	1	1	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
2956	"C:\Users\admin\AppData\Local\Temp\35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe"	C:\Users\admin\AppData\Local\Temp\35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe		Explorer.EXE
Information				
User: admin		Integrity Level: MEDIUM		

[illegible]

(PID) Process:	(2956) 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.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:	(2956) 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	Name:	WpadDecisionTime
Value:	2E0AB560E0B5D801		

(PID) Process:	(2956) 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.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:	(2956) 35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	LanguageList
Value:	en-US		

Files activity

Executable files	Suspicious files	Text files	Unknown types
6	7	1	11

Dropped files

PID	Process	Filename	Type
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\18516212075227702182026497	—
		MD5: — SHA256: —	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	compressed
		MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\738FBC066DBD9E6001113366624890A3_53C5D34017BDB72400155AC2819BA60D	binary
		MD5: 4FCA8FBB6087F4A7F66945E0DEF753E2 SHA256: 35B1EBA50F8F2566DD9F4E00E289C2D8FC14D6B14404D2697A864A36713D116A	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	binary
		MD5: 78E883927AF4B6F5261C8418C29144C1 SHA256: 4249DC568B2AE356142922EFC477BDDE3804BF03B4990FC388721CA9E9BEA857	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\5FE6SURX.txt	text
		MD5: 3109E7F3D9178566DD7F9B7ED54AF6D SHA256: BB5AA73646D5CC64FA396CAE7397A505B47C6A0151D98700EC27ECBDBE0F6C09	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\738FBC066DBD9E6001113366624890A3_53C5D34017BDB72400155AC2819BA60D	der
		MD5: 230A22F3E868854D8C57857589ED27AF SHA256: DB86B8EC6E27248941A7EB89FC47A54C7F73835CF71725B5E1C6268D4EFAD1B1	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	der
		MD5: BB70EB81C14C6CD23606070C5E2F379D SHA256: BD5A4F966FA88F129D9A7C763DF237290DD1364374EE290F5B8F445455D137D	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	binary
		MD5: 0467DA7CF13C224AE97E9D4CDA7F625A SHA256: 8E50AD2435A9AE9421FA73B8CCDF2140DD77BE6D42A708D8316148C280BCDFA6	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	der
		MD5: 523EF2600908BC92DD2FA45DE5EDF2C2 SHA256: 1EEC21FD9F5A998BCD48E28E84BF5705A36D7C38CF737A0E8E6A89C7D6C5B81A	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	binary
		MD5: 450D9244B0F05AC55CDF01E55586671C SHA256: C85353C830B66E0A906A9CDB065EFD5FAAD87D3C835F73E1498C6304701105AF	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\vcruntime140.dll	executable
		MD5: 7587BF9CB4147022CD5681B015183046 SHA256: C408B03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D	
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\softokn3.dll	executable

		MD5: A2EE53DE9167BF0D6C019303B7CA84E5	SHA256: 43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\nss3.dll	executable
		MD5: 8FAC4E3C5908856BA17D41EDCD455A51	SHA256: E2935B8528550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\msvcp140.dll	executable
		MD5: 109F0F02FD37C84BFC7508D4227D7ED5	SHA256: 334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\mozglue.dll	executable
		MD5: 87F3C08A9660691143661BF7332C3C27	SHA256: 3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\08234791970758875523759992	sqlite
		MD5: 49E1E668EEFE2553D2ECEC4B7EF1D3E	SHA256: A664C359ACE3BFC149323E5403BB7140A84519043BDBA59B064EBC1BDADD32D4
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\91386318515813846626676318	sqlite
		MD5: B8E63E7225C9F4E0A81371F29D6456D8	SHA256: 35A6919CE60EA8E0A44934F8B267BDE2C5A063C2E32F22D34724F168C43150C8
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\18516212075227702182026497-shm	binary
		MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\83761552727231201487947872	sqlite
		MD5: 23D08A78BC908C0B29E9800D3D5614E7	SHA256: F6BD7DF5DFAE9FD88811A807DBA14085E00C1B5A6D7CC3D06CC68F6015363D59
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\83761552727231201487947872-shm	binary
		MD5: B7C14EC6110FA820CA6B65F5AEC85911	SHA256: FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\freebl3.dll	executable
		MD5: EF2834AC4EE7D6724F255BEAF527E635	SHA256: A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\63776098862822941301055548	sqlite
		MD5: B98E46B09E0B97F0839DC7897AEA7F9A	SHA256: 45AF197F8FB09FC1BB9AFF9D76F1E8FF06B5906F6A9E8F4CF2213DE0A8B1213A
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\80249110013361325538847668	sqlite
		MD5: CC104C4E4E904C3AD7AD5C45FBFA7087	SHA256: 321BE844CECC903EF1E7F875B729C96BB3ED0D4986314384CD5944A29A670C9B
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	C:\ProgramData\00531639118937345186034160	sqlite
		MD5: D02907BE1C995E1E51571EEDB82FA281	SHA256: 2189977F6EA58BDAD5883720B099E12B869F223FB9B18AC40E7D37C5954A55DD

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
7	4	3	4

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	8.241.123.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?57de30f85aae83a6	US	compressed	4.70 Kb	whitelisted
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	192.124.249.22:80	http://ocsp.godaddy.com/MEqwQJBAMD4wPDAJBgUrDgMCGgUABBTklInKBazXkf0Qh0pel3IfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D	US	der	1.66 Kb	whitelisted
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	192.124.249.22:80	http://ocsp.godaddy.com/MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBBQdl2%2B0BKuXH93foRUj4a7Iar4rGwQUOpqFBxBnKLbv9r0FQW4gwZTaD94CAQc%3D	US	der	1.69 Kb	whitelisted
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	192.124.249.22:80	http://ocsp.godaddy.com/MEowSDBGMEqwQJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQMK9J47MNIMwojPX%2B2y8zLQsgM4CCQC2T6rhHiP0ng%3D%3D	US	der	1.74 Kb	whitelisted
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	95.217.245.31:80	http://95.217.245.31/977	DE	text	107 b	malicious
2956	35e67bf049cb9c2d9c6af0f2f29fffe0279a0953732240b6cdc7c1b12121d23.exe	GET	200	95.217.245.31:80	http://95.217.245.31/6406131259.zip	DE	compressed	3.47 Mb	malicious

9a0953732240b6cd c7c1b12121d23.exe							
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	POST	200	95.217.245.31:80	http://95.217.245.31/	DE	<div>text</div> 2 b <div>malicious</div>

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	149.154.167.99:443	t.me	Telegram Messenger LLP	GB	<div>malicious</div>
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	8.241.123.126:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	<div>unknown</div>
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	192.124.249.22:80	ocsp.godaddy.com	Sucuri	US	<div>suspicious</div>
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	95.217.245.31:80	—	Hetzner Online GmbH	DE	<div>malicious</div>

DNS requests

Domain	IP	Reputation
t.me	149.154.167.99	<div>whitelisted</div>
ctldl.windowsupdate.com	8.241.123.126 8.253.204.120 67.26.75.254 67.27.235.254 8.253.204.249	<div>whitelisted</div>
ocsp.godaddy.com	192.124.249.22 192.124.249.41 192.124.249.36 192.124.249.23 192.124.249.24	<div>whitelisted</div>

Threats

PID	Process	Class	Message
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	<div>Potentially Bad Traffic</div>	ET INFO Dotted Quad Host ZIP Request
2956	35e67bf049cb9c2d9c6af0f2f29ffef0279a0953732240b6cdc7c1b12121d23.exe	<div>A Network Trojan was detected</div>	ET TROJAN Arkei/Vidar/Mars Stealer Variant

Debug output strings

No debug info



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