







General Info

File name:	VXUHEUR-Trojan.Script.Generic-5aac437dfc39d5.exe
Full analysis:	https://app.any.run/tasks/b66eb95f-ef83-45b0-83a1-190d79365d06
Verdict:	Malicious activity
Threats:	njRAT
	<div>njRAT is a remote access trojan. It is one of the most widely accessible RATs on the market that features an abundance of educational information. Interested attackers can even find tutorials on YouTube. This allows it to become one of the most popular RATs in the world.</div>
Analysis date:	August 22, 2022 at 12:36:29
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan rat njrat bladabindi
Indicators:	   
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
MD5:	169C8CD03048A2413456D1DEA82605E3
SHA1:	EAF3890A7062EEB47E97A7FA0E00FB5E3B74A2E6
SHA256:	5AAAC437DFC39D5A190EFCF166404E7C1AB9FD7EFF1EF50223528CC28779A796
SSDEEP:	12288:VYV6MorX7qzuC3QH09FQVHPF51jgc1Gd6hVXjnh7:KBXu9HGaVHHVzh7

Software environment set and analysis options

Launch configuration

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

Software preset

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

Hotfixes

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

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

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

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	KB4532945
	KB4536952
	KB4567409
	KB958488
	KB976902
	KB982018
	LocalPack AU Package
	LocalPack CA Package
	LocalPack GB Package
	LocalPack US Package
	LocalPack ZA Package
	Package 21 for KB2984976
	Package 38 for KB2984976
	Package 45 for KB2984976
	Package 59 for KB2984976
	Package 7 for KB2984976
	Package 76 for KB2984976
	PlatformUpdate Win7 SRV08R2 Package TopLevel
	ProfessionalEdition
	RDP BlueIP Package TopLevel
	RDP WinIP Package TopLevel
	RollupFix
	UltimateEdition
	WUClient SelfUpdate ActiveX
	WUClient SelfUpdate Aux TopLevel
	WUClient SelfUpdate Core TopLevel
	WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
<p>Drops executable file immediately after starts</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p>	<p>Checks supported languages</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p> <p>RegAsm.exe (PID: 3548)</p>	<p>Reads the computer name</p> <p>netsh.exe (PID: 1808)</p>
<p>Writes to a start menu file</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p>	<p>Reads mouse settings</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p>	<p>Checks supported languages</p> <p>netsh.exe (PID: 1808)</p>
<p>NJ RAT was detected</p> <p>RegAsm.exe (PID: 3548)</p>	<p>Reads the computer name</p> <p>RegAsm.exe (PID: 3548)</p>	
<p>Connects to CnC server</p> <p>RegAsm.exe (PID: 3548)</p>	<p>Drops a file with a compile date too recent</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p>	
	<p>Executable content was dropped or overwritten</p> <p>VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe (PID: 3136)</p>	
	<p>Reads Environment values</p> <p>RegAsm.exe (PID: 3548)</p> <p>netsh.exe (PID: 1808)</p>	

Static information

TRiD	EXIF
<p>.exe UPX compressed Win32 Executable (39.3)</p> <p>.exe Win32 EXE Yoda's Crypter (38.6)</p> <p>.dll Win32 Dynamic Link Library (generic) (9.5)</p> <p>.exe Win32 Executable (generic) (6.5)</p>	<p>EXE</p> <p>CharacterSet: Unicode</p> <p>LanguageCode: English (British)</p> <p>FileSubtype: 0</p>

.exe Generic Win/DOS Executable (2.9)		ObjectType:	Executable application
		FileOS:	Win32
		FileFlags:	(none)
		FileFlagsMask:	0x0000
		ProductVersionNumber:	0.0.0.0
		FileVersionNumber:	0.0.0.0
		Subsystem:	Windows GUI
		SubsystemVersion:	5.1
		ImageVersion:	0
		OSVersion:	5.1
		EntryPoint:	0xf7860
		UninitializedDataSize:	659456
		InitializedDataSize:	139264
		CodeSize:	352256
		LinkerVersion:	12
		PEType:	PE32
		TimeStamp:	2019:05:05 21:56:52+02:00
		MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	05-May-2019 19:56:52
Detected languages:	English - United Kingdom

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:	0x00000110

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	05-May-2019 19:56:52
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_LARGE_ADDRESS_AWARE

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
UPX0	0x00001000	0x000A1000	0x00000000	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
UPX1	0x000A2000	0x00056000	0x00055C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.93498
.rsrc	0x000F8000	0x00022000	0x00021400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.83694

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.40026	1007	Latin 1 / Western European	English - United Kingdom	RT_MANIFEST
2	2.05883	296	Latin 1 / Western European	English - United Kingdom	RT_ICON
3	2.25499	296	Latin 1 / Western European	English - United Kingdom	RT_ICON
4	7.63417	3829	Latin 1 / Western European	English - United Kingdom	RT_ICON
7	3.34702	1428	Latin 1 / Western European	English - United Kingdom	RT_STRING
8	3.2817	1674	Latin 1 / Western European	English - United Kingdom	RT_STRING
9	3.28849	1168	Latin 1 / Western European	English - United Kingdom	RT_STRING

10	3.28373	1532	Latin 1 / Western European	English - United Kingdom	RT_STRING
11	3.26322	1628	Latin 1 / Western European	English - United Kingdom	RT_STRING
12	3.25812	1126	Latin 1 / Western European	English - United Kingdom	RT_STRING
99	1.6789	20	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
162	2.02322	20	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
164	1.84274	20	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
166	2.68292	80	Latin 1 / Western European	English - United Kingdom	RT_MENU
169	2.02322	20	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
313	3.08572	344	Latin 1 / Western European	English - United Kingdom	RT_STRING
ACPPAGER	7.97555	7144	Latin 1 / Western European	UNKNOWN	RT_STRING
LPKSETUP1	7.97658	7144	Latin 1 / Western European	UNKNOWN	RT_STRING
SCRIPT	7.99841	104022	Latin 1 / Western European	UNKNOWN	RT_RCDATA

Imports

ADVAPI32.dll
COMCTL32.dll
COMDLG32.dll
GDI32.dll
IPHLPAPI.DLL
KERNEL32.DLL
MPR.dll
OLEAUT32.dll
PSAPI.DLL
SHELL32.dll
USER32.dll
USERENV.dll
UxTheme.dll
VERSION.dll
WININET.dll
WINMM.dll
WSOCK32.dll
ole32.dll

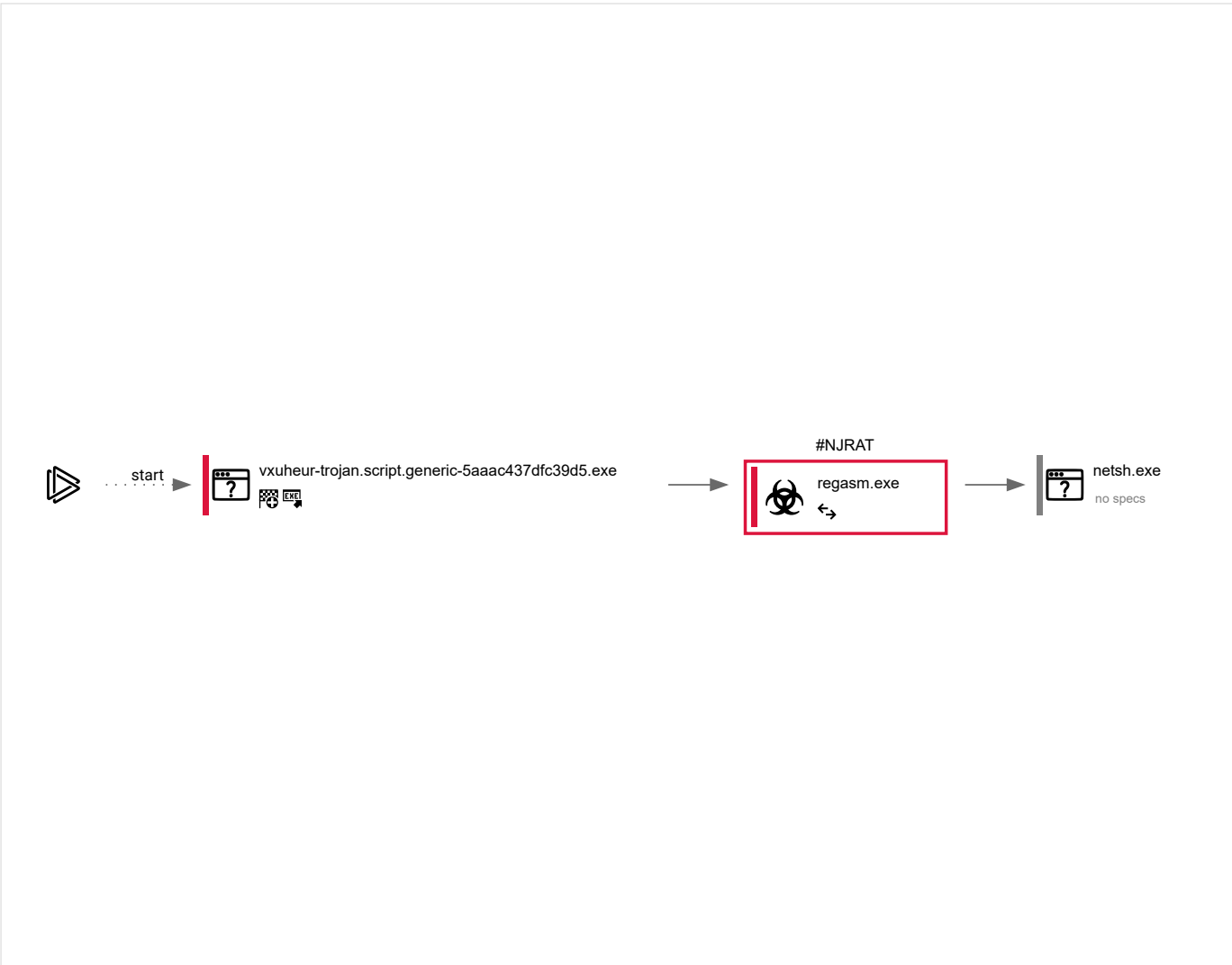
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
37	3	2	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
3136	"C:\Users\admin\AppData\Local\Temp\VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe"	C:\Users\admin\AppData\Local\Temp\VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe		Explorer.EXE
Information				
User: admin		Integrity Level: MEDIUM		
Exit code: 0				

3548

"C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

↔ 🔒

VXUHEUR-Trojan.Script.Generic-5aac437dfc39d5.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Microsoft .NET Assembly Registration Utility

Version:

2.0.50727.5483 (Win7SP1GDR.050727-5400)

1808

netsh firewall add allowedprogram
"C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
" "RegAsm.exe" ENABLE

C:\Windows\system32\netsh.exe

—

RegAsm.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Network Command Shell

Exit code:

1

Version:

6.1.7600.16385 (win7_rtm.090713-1255)

Registry activity

Total events	Read events	Write events	Delete events
981	913	68	0

Modification events

(PID) Process:	(3548) RegAsm.exe	Key:	HKEY_CURRENT_USER
Operation:	write	Name:	di
Value:	!		

(PID) Process:	(3548) RegAsm.exe	Key:	HKEY_CURRENT_USER\Environment
Operation:	write	Name:	SEE_MASK_NOZONECHECKS
Value:	1		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	LanguageList
Value:	en-US		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\dhcpcqec.dll,-100
Value:	DHCP Quarantine Enforcement Client		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\dhcpcqec.dll,-101
Value:	Provides DHCP based enforcement for NAP		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\dhcpcqec.dll,-103
Value:	1.0		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\dhcpcqec.dll,-102
Value:	Microsoft Corporation		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\napipsec.dll,-1
Value:	IPsec Relying Party		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\napipsec.dll,-2
Value:	Provides IPsec based enforcement for Network Access Protection		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\napipsec.dll,-4
Value:	1.0		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\napipsec.dll,-3
Value:	Microsoft Corporation		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\tsgqec.dll,-100
Value:	RD Gateway Quarantine Enforcement Client		

(PID) Process:	(1808) netsh.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	@%SystemRoot%\system32\tsgqec.dll,-101
Value:	Provides RD Gateway enforcement for NAP		

(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\tsgqec.dll,-102
Value: 1.0	
(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\tsgqec.dll,-103
Value: Microsoft Corporation	
(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\leapqec.dll,-100
Value: EAP Quarantine Enforcement Client	
(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\leapqec.dll,-101
Value: Provides Network Access Protection enforcement for EAP authenticated network connections, such as those used with 802.1X and VPN technologies.	
(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\leapqec.dll,-102
Value: 1.0	
(PID) Process: (1808) netsh.exe	Key: HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write	Name: @%SystemRoot%\system32\leapqec.dll,-103
Value: Microsoft Corporation	
(PID) Process: (3548) RegAsm.exe	Key: HKEY_CURRENT_USER\Software\bc7eb91c2fa2d14d3f8c9669e0422bdd
Operation: write	Name: [kl]
Value:	

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	0	2	0

Dropped files

PID	Process	Filename	Type
3136	VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\tscon.url	text
		MD5: 60D6C541B8B53D58A6E9F5D739094562 SHA256: BF3CAB13F071269D41B472707B5352E20F867C4566D3CDAFE4B856D2F20B7873	
3136	VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe	C:\Users\admin\AppData\Roaming\IntelCpHeciSvc\data.exe	executable
		MD5: F9C6BEACB1563BF328A1D24749407597 SHA256: 568E34F7DDCE5C649AF063C7718D14B8C85A67C3BB695D2213CD323595FCC89B	
3136	VXUHEUR-Trojan.Script.Generic-5aaac437dfc39d5.exe	C:\Users\admin\AppData\Roaming\IntelCpHeciSvc\tscon.vbs	text
		MD5: FB68AECB60BDBD2AE3DF003A351F2A2C SHA256: D19496CA159C9A0EB900A7FD632D1AF33FB5F81B8FAF80739675A0DBEAC237EF	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	29	3	32

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3548	RegAsm.exe	192.169.69.25:5553	redlocal.duckdns.org	Wowrack.com	US	malicious
—	—	192.169.69.25:5553	redlocal.duckdns.org	Wowrack.com	US	malicious

DNS requests

Domain	IP	Reputation
redlocal.duckdns.org	192.169.69.25	malicious

[illegible]

No debug info

