ANY ▷ RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe
Full analysis:	https://app.any.run/tasks/3fcae486-9cb6-4f8a-bd7a-a6fbebd9fd89
Verdict:	Malicious activity
Threats:	**njRAT**
	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.
Analysis date:	August 22, 2022 at 12:33:28
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
MD5:	15F364D2F942A4DDD1D9C3ECF7C26C32
SHA1:	F752C278FB4F2121F8CB4FFB910AD1E82656FCB4
SHA256:	F8C245665C74CC678F4A9182B3A593FF0DE9682FF0F96596EB59C158F2643373
SSDEEP:	24576:3AHnh+eWsN3skA4RV1Hom2KXMmHacA/aaxmJD1rSEn1+Ox7AH0dgN3dcyIz5j:qh+ZkIdoPK8YacAQJD1uEn7UHp3dcy0j

---

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	Hotfixes
Internet Explorer 11.0.9600.19596 KB4534251	Client LanguagePack Package
Adobe Acrobat Reader DC (20.013.20064)	Client Refresh LanguagePack Package
Adobe Flash Player 32 ActiveX (32.0.0.453)	CodecPack Basic Package
Adobe Flash Player 32 NPAPI (32.0.0.453)	Foundation Package
Adobe Flash Player 32 PPAPI (32.0.0.453)	IE Hyphenation Parent Package English
Adobe Refresh Manager (1.8.0)	IE Spelling Parent Package English
CCleaner (5.74)	IE Troubleshooters Package
FileZilla Client 3.51.0 (3.51.0)	InternetExplorer Optional Package
Google Chrome (86.0.4240.198)	InternetExplorer Package TopLevel
Google Update Helper (1.3.36.31)	KB2479943
Java 8 Update 271 (8.0.2710.9)	KB2491683
Java Auto Updater (2.8.271.9)	KB2506212
Microsoft .NET Framework 4.5.2 (4.5.51209)	KB2506928
Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)	KB2532531
Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)	KB2533552
Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)	KB2533623
Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)	KB2534111
Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)	KB2545698
Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)	KB2547666
Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2552343
Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)	KB2560656
Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)	KB2564958
Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)	KB2574819
Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB2579686
Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)	KB2585542
Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)	KB2604115
Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)	KB2620704
Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)	KB2621440
Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)	KB2631813
Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)	KB2639308
Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2640148
Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)	KB2653956
Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)	KB2654428
Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)	KB2656356
Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)	KB2660075
Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)	KB2667402
Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)	KB2676562
Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)	KB2685811

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2685939
Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)	KB2690533
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

Drops executable file immediately after starts
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
RegAsm.exe (PID: 3548)

Application was dropped or rewritten from another process
RegAsm.exe (PID: 3548)
RegAsm.exe (PID: 2344)
RegAsm.exe (PID: 3236)

Writes to a start menu file
RegAsm.exe (PID: 3548)

NJRAT was detected
RegAsm.exe (PID: 3548)

Connects to CnC server
RegAsm.exe (PID: 3548)

Changes the autorun value in the registry
RegAsm.exe (PID: 3548)

SUSPICIOUS

Reads mouse settings
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
aadcloudap.exe (PID: 3128)
aadcloudap.exe (PID: 1816)

Checks supported languages
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
RegAsm.exe (PID: 3548)
aadcloudap.exe (PID: 3128)
RegAsm.exe (PID: 2344)
RegAsm.exe (PID: 3236)
aadcloudap.exe (PID: 1816)

Reads the computer name
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
RegAsm.exe (PID: 3548)
aadcloudap.exe (PID: 3128)
RegAsm.exe (PID: 2344)
aadcloudap.exe (PID: 1816)
RegAsm.exe (PID: 3236)

Executable content was dropped or overwritten
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
RegAsm.exe (PID: 3548)

Drops a file with a compile date too recent
VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe (PID: 3280)
RegAsm.exe (PID: 3548)

Reads Environment values
RegAsm.exe (PID: 3548)

INFO

Checks supported languages
schtasks.exe (PID: 3368)
schtasks.exe (PID: 1204)
schtasks.exe (PID: 3068)

Reads the computer name
schtasks.exe (PID: 3368)
schtasks.exe (PID: 1204)
schtasks.exe (PID: 3068)

Executed via Task Scheduler
aadcloudap.exe (PID: 3128)
aadcloudap.exe (PID: 1816)

Static information

TRiD

.exe	|	Win64 Executable (generic) (64.6)
.dll	|	Win32 Dynamic Link Library (generic) (15.4)
.exe	|	Win32 Executable (generic) (10.5)
.exe	|	Generic Win/DOS Executable (4.6)
.exe	|	DOS Executable Generic (4.6)

EXIF

EXE

ProductVersion:	418.780.947.409
ProductName:	MdmDiagnosticsTool
LegalCopyright:	chglogon
FileVersion:	919.511.797.843
CompanyName:	mountvol
OriginalFileName:	slui.exe
FileDescription:	LicensingUI
CharacterSet:	Unicode
LanguageCode:	English (U.S.)
FileSubtype:	0
ObjectFileType:	Dynamic link library
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x0000
ProductVersionNumber:	1.0.0.0
FileVersionNumber:	1.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	5.1
ImageVersion:	0
OSVersion:	5.1
EntryPoint:	0x2800a
UninitializedDataSize:	0
InitializedDataSize:	865280
CodeSize:	581632
LinkerVersion:	12
PEType:	PE32
TimeStamp:	2019:02:10 00:43:14+01:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	09-Feb-2019 23:43:14
Detected languages:	English - United Kingdom
	English - United States
	Spanish - Spain (International sort)
FileDescription:	LicensingUI
OriginalFilename:	slui.exe
CompanyName:	mountvol
FileVersion:	919.511.797.843
LegalCopyright:	chglogon
ProductName:	MdmDiagnosticsTool
ProductVersion:	418.780.947.409

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

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	09-Feb-2019 23:43:14
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

OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000110

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x0008DFDD	0x0008E000	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.67525
.rdata	0x0008F000	0x0002FD8E	0x0002FE00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.76324
.data	0x000BF000	0x00008F74	0x00005200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	1.19638
.rsrc	0x000C8000	0x00097004	0x00097200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	7.3128
.reloc	0x00160000	0x00007134	0x00007200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.78396

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.40026	1007	Latin 1 / Western European	English - United Kingdom	RT_MANIFEST
2	4.61339	9640	Latin 1 / Western European	English - United Kingdom	RT_ICON
3	4.8187	4264	Latin 1 / Western European	English - United Kingdom	RT_ICON
4	5.14816	1128	Latin 1 / Western European	English - United Kingdom	RT_ICON
5	4.37591	16936	Latin 1 / Western European	English - United Kingdom	RT_ICON
6	3.97928	67624	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	2.86004	76	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
169	1.84274	20	Latin 1 / Western European	English - United Kingdom	RT_GROUP_ICON
313	3.08572	344	Latin 1 / Western European	English - United Kingdom	RT_STRING
ADVPACK3	3.99987	53258	Latin 1 / Western European	UNKNOWN	RT_MENU
NETCFGNOTIFYOBJECTHOST1	4.00005	53260	Latin 1 / Western European	UNKNOWN	RT_MENU
SDIAGNHOST2	3.99986	53260	Latin 1 / Western European	UNKNOWN	RT_MENU
SCRIPT	7.99945	346872	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
45	9	2	4

Behavior graph

#NJRAT

regasm.exe

vxuheur-trojan.script.generic-f8c245665c74cc6.exe

start

schtasks.exe
no specs

regasm.exe
no specs

aadcloudap.exe
no specs

schtasks.exe
no specs

regasm.exe
no specs

aadcloudap.exe
no specs

schtasks.exe
no specs
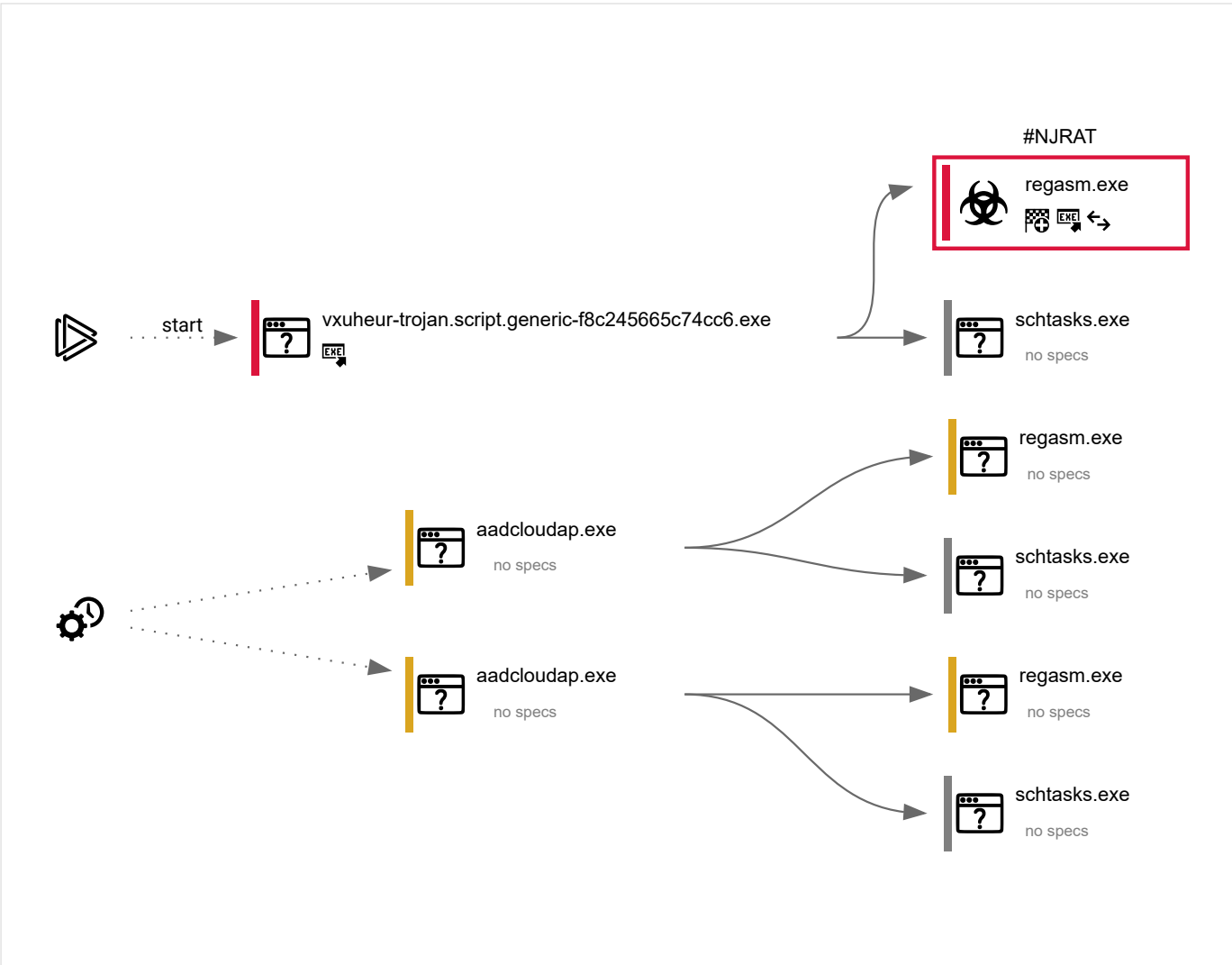
Specs description

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
3280	"C:\Users\admin\AppData\Local\Temp\VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe"	C:\Users\admin\AppData\Local\Temp\VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe		Explorer.EXE

Information			
User:	admin	Company:	mountvol
Integrity Level:	MEDIUM	Description:	LicensingUI
Exit code:	0	Version:	919.511.797.843

| 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-f8c245665c74cc6.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft .NET Assembly Registration Utility
Version:	2.0.50727.5483 (Win7SP1GDR.050727-5400)		

| 3368 | "C:\Windows\System32\schtasks.exe" /create /tn appidsvc /tr "C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe" /sc minute /mo 1 /F | C:\Windows\System32\schtasks.exe | — | VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

| 3128 | C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe | C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe | — | taskeng.exe |

Information

User:	admin	Company:	mountvol
Integrity Level:	MEDIUM	Description:	LicensingUI
Exit code:	0	Version:	919.511.797.843

| 2344 | "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe | — | aadcloudap.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft .NET Assembly Registration Utility
Exit code:	0	Version:	2.0.50727.5483 (Win7SP1GDR.050727-5400)

| 1204 | "C:\Windows\System32\schtasks.exe" /create /tn appidsvc /tr "C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe" /sc minute /mo 1 /F | C:\Windows\System32\schtasks.exe | — | aadcloudap.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

| 1816 | C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe | C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe | — | taskeng.exe |

Information

User:	admin	Company:	mountvol
Integrity Level:	MEDIUM	Description:	LicensingUI
Exit code:	0	Version:	919.511.797.843

| 3236 | "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" | C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe | — | aadcloudap.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft .NET Assembly Registration Utility
Exit code:	0	Version:	2.0.50727.5483 (Win7SP1GDR.050727-5400)

| 3068 | "C:\Windows\System32\schtasks.exe" /create /tn appidsvc /tr "C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe" /sc minute /mo 1 /F | C:\Windows\System32\schtasks.exe | — | aadcloudap.exe |

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Manages scheduled tasks
Exit code:	0	Version:	6.1.7600.16385 (win7_rtm.090713-1255)

Registry activity

Total events	Read events	Write events	Delete events
1 806	1 658	148	0

Modification events

(PID) Process:	(3280) VXUHEUR-	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

	Trojan.Script.Generic- f8c245665c74cc6.exe		
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(3280) VXUHEUR- Trojan.Script.Generic- f8c245665c74cc6.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(3280) VXUHEUR- Trojan.Script.Generic- f8c245665c74cc6.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(3280) VXUHEUR- Trojan.Script.Generic- f8c245665c74cc6.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(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:	(3548) RegAsm.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation:	write	Name:	Client.exe
Value:	"C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" ..		

(PID) Process:	(3548) RegAsm.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Operation:	write	Name:	Hidden
Value:	0		

(PID) Process:	(2344) RegAsm.exe	Key:	HKEY_CURRENT_USER
Operation:	write	Name:	di
Value:	!		

(PID) Process:	(3128) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(3128) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(3128) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(3128) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(PID) Process:	(3548) RegAsm.exe	Key:	HKEY_CURRENT_USER\Software\Client.exe
Operation:	write	Name:	[kl]
Value:			

(PID) Process:	(3236) RegAsm.exe	Key:	HKEY_CURRENT_USER
Operation:	write	Name:	di
Value:	!		

(PID) Process:	(1816) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(1816) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(1816) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(1816) aadcloudap.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect

Value: 0

Files activity

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

Dropped files

PID	Process	Filename	Type
3280	VXUHEUR-Trojan.Script.Generic-f8c245665c74cc6.exe	C:\Users\admin\AppData\Roaming\CloudExperienceHostBroker\aadcloudap.exe	executable
		MD5: E29FAC2917A186E2859580B8AC1ECFA5 SHA256: 154B5608498D6C7386151C98D2932B7F03DCDF18C7218106D5FCABAA3BD2E622	
3548	RegAsm.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Client.exe	executable
		MD5: 246BB0F8D68A463FD17C235DEB5491C0 SHA256: 32B60D7BBA22CC1682F4BA651D86C9FB357BDC82E9A284AB9668E5446BD24BB3	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	32	2	34

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	192.169.69.25:1041	smokin10.duckdns.org	Wowrack.com	US	malicious
3548	RegAsm.exe	192.169.69.25:1041	smokin10.duckdns.org	Wowrack.com	US	malicious

DNS requests

Domain	IP	Reputation
smokin10.duckdns.org	192.169.69.25	malicious

Threats

PID	Process	Class	Message
–	–	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)

3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
—	—	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)
3548	RegAsm.exe	A Network Trojan was detected	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)

Debug output strings

No debug info

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