ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	1614.scr
Full analysis:	https://app.any.run/tasks/ae3fd74d-119a-41fa-a810-392193049a94
Verdict:	Malicious activity
Analysis date:	September 04, 2022 at 06:56:43
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:	5991F6529039369B6676B8BD5AAAE84E
SHA1:	FA2BAA98688BDBF8641E443C90FCB244330DE041
SHA256:	8B75DC7056D22CF6B52D10867D70D86AB0A11CB953BC542D63C7F70558B93645
SSDEEP:	1536:xx9DjwWm3xtHvToPMgCD7+lbbbbbbbbbbbbbbbbbbbbbA6:x/YhtHboPMgOZ6

Software environment set and analysis options

Launch configuration

Task duration:	60 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)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
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

No malicious indicators.

SUSPICIOUS

Checks supported languages
1614.scr.exe (PID: 3104)

Reads the computer name
1614.scr.exe (PID: 3104)

Reads Environment values
1614.scr.exe (PID: 3104)

Executes application which crashes
1614.scr.exe (PID: 3104)

INFO

Dropped object may contain Bitcoin addresses
1614.scr.exe (PID: 3104)

Checks supported languages
ntvdm.exe (PID: 3608)

Static information

TRiD

.exe | Generic CIL Executable (.NET, Mono, etc.) (81)
.dll | Win32 Dynamic Link Library (generic) (7.2)
.exe | Win32 Executable (generic) (4.9)
.exe | Win16/32 Executable Delphi generic (2.2)
.exe | Generic Win/DOS Executable (2.2)

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	2022-Aug-18 05:36:53
FileDescription:	
FileVersion:	0.0.0.0

InternalName:	I3cJCRAAolumEcy.exe
LegalCopyright:	
OriginalFilename:	I3cJCRAAolumEcy.exe
ProductVersion:	0.0.0.0
Assembly Version:	0.0.0.0

DOS Header

e_magic:	MZ
e_cblp:	144
e_cp:	3
e_crlc:	0
e_cparhdr:	4
e_minalloc:	0
e_maxalloc:	65535
e_ss:	0
e_sp:	184
e_csum:	0
e_ip:	0
e_cs:	0
e_ovno:	0
e_oemid:	0
e_oeminfo:	0
e_lfanew:	128

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
NumberofSections:	4
TimeDateStamp:	2022-Aug-18 05:36:53
PointerToSymbolTable:	0
NumberOfSymbols:	0
SizeOfOptionalHeader:	224
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	8192	58852	58880	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	5.97592
.sdata	73728	488	512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	6.61888
.rsrc	81920	69052	69120	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	3.70892
.reloc	155648	12	512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.0815394

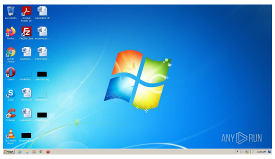
Resources

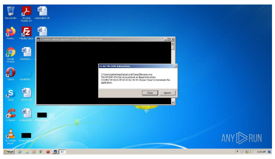
Title	Entropy	Size	Codepage	Language	Type
1	3.2495	612	UNKNOWN	UNKNOWN	RT_VERSION
2	3.63819	67624	UNKNOWN	UNKNOWN	RT_ICON
32512	2.16096	20	UNKNOWN	UNKNOWN	RT_GROUP_ICON
1 (#2)	5.00112	490	UNKNOWN	UNKNOWN	RT_MANIFEST

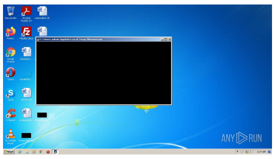
Imports

mscoree.dll

Video and screenshots



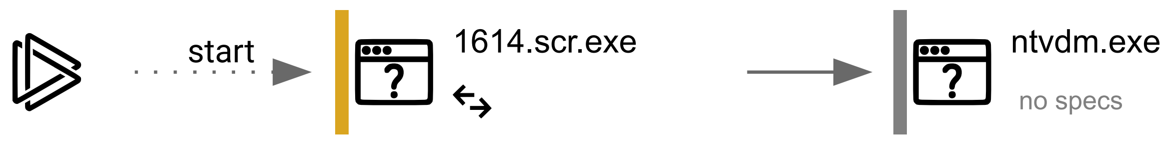




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
35	2	0	1

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
3104	"C:\Users\admin\AppData\Local\Temp\1614.scr.exe"	C:\Users\admin\AppData\Local\Temp\1614.scr.exe	⇆	Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:		**Exit code:**	0
Version:	0.0.0.0		

3608	"C:\Windows\system32\ntvdm.exe" -i1	C:\Windows\system32\ntvdm.exe	—	1614.scr.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	NTVDM.EXE
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

Registry activity

Total events	Read events	Write events	Delete events
1 159	1 139	20	0

Modification events

(PID) Process:	Operation:	Value:	Key:	Name:
(3104) 1614.scr.exe	write	0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	EnableFileTracing
(3104) 1614.scr.exe	write	0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	EnableConsoleTracing
(3104) 1614.scr.exe	write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	FileTracingMask
(3104) 1614.scr.exe	write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	ConsoleTracingMask
(3104) 1614.scr.exe	write	1048576	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	MaxFileSize
(3104) 1614.scr.exe	write	%windir%\tracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASAPI32	FileDirectory
(3104) 1614.scr.exe	write	0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	EnableFileTracing
(3104) 1614.scr.exe	write	0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	EnableConsoleTracing
(3104) 1614.scr.exe	write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	FileTracingMask
(3104) 1614.scr.exe	write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	ConsoleTracingMask
(3104) 1614.scr.exe	write	1048576	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	MaxFileSize
(3104) 1614.scr.exe	write	%windir%\tracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1614_RASMANCS	FileDirectory
(3104) 1614.scr.exe	write	1	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	ProxyBypass
(3104) 1614.scr.exe	write	1	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	IntranetName
(3104) 1614.scr.exe	write	1	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet
(3104) 1614.scr.exe			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
0	0	3	0

Dropped files

PID	Process	Filename	Type
3104	1614.scr.exe	C:\Users\admin\AppData\Local\Temp\filename.exe **MD5:** 67DB76AC5A9E737A57E0CC2AD789A37D **SHA256:** 76DDBC03E913198505745BB7734B5EF8EAC2890AAFE04BB24E27C11754D0CACE	html
3608	ntvdm.exe	C:\Users\admin\AppData\Local\Temp\scs6F57.tmp **MD5:** 8CF6DDB5AA59B49F34B967CD46F013B6 **SHA256:** EE06792197C3E025B84860A72460EAF628C66637685F8C52C5A08A9CC35D376C	text
3608	ntvdm.exe	C:\Users\admin\AppData\Local\Temp\scs6F58.tmp **MD5:** 4C361DEA398F7AEEF49953BDC0AB4A9B **SHA256:** 06D61C23E6CA59B9DDAD1796ECCC42C032CD8F6F424AF6CFEE5D085D36FF7DFD	text

Network activity

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

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3104	1614.scr.exe	GET	200	87.236.16.3:80	http://csomundibash.ru/files/filename.exe	RU	html	36.1 Kb	suspicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3104	1614.scr.exe	87.236.16.3:80	csomundibash.ru	Beget Ltd	RU	malicious

DNS requests

Domain	IP	Reputation
csomundibash.ru	87.236.16.3	suspicious

Threats

PID	Process	Class	Message
3104	1614.scr.exe	Potential Corporate Privacy Violation	AV POLICY HTTP request for .exe file with no User-Agent

Debug output strings

No debug info

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN