



General Info

File name:	MV NEW LONDON EAGLE.exe
Full analysis:	https://app.any.run/tasks/43a4700f-6770-4fde-a684-83eefed76e1a
Verdict:	Malicious activity
Threats:	Quasar RAT
Quasar is a very popular RAT in the world thanks to its code being available in open-source. This malware can be used to control the victim's computer remotely.	
Analysis date:	August 17, 2022 at 14:21:02
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	evasionstealerquasar
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	EBA4D2AE1E21DD2D6D8FFFE408D6ADB
SHA1:	EC8874543247658819EBD6DFBF8F14C2B4A4F0A3
SHA256:	D4480D07C420969D1A3FA0F5520BC27017FCA825B45ED625FE10A7F6F6852E84
SSDEEP:	12288:otBaV1ki3P+/ScJHm1cFtaikJnZ4IX+3JzT+juwYOqxJlZ:ot4Vui3VlqglXsJ3+ju

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
Stealing of credential data AppLaunch.exe (PID: 2596)	Reads the computer name AppLaunch.exe (PID: 2596) MV NEW LONDON EAGLE.exe (PID: 3712) MV NEW LONDON EAGLE.exe (PID: 3944)	Reads settings of System Certificates MV NEW LONDON EAGLE.exe (PID: 3712)
QUASAR detected by memory dumps MV NEW LONDON EAGLE.exe (PID: 3712)		
Steals credentials from Web Browsers AppLaunch.exe (PID: 2596)	Checks supported languages AppLaunch.exe (PID: 2596) MV NEW LONDON EAGLE.exe (PID: 3712) MV NEW LONDON EAGLE.exe (PID: 3944)	Checks Windows Trust Settings MV NEW LONDON EAGLE.exe (PID: 3712)
Actions looks like stealing of personal data AppLaunch.exe (PID: 2596)	Reads CPU info AppLaunch.exe (PID: 2596)	
	Application launched itself MV NEW LONDON EAGLE.exe (PID: 3944)	
	Reads Environment values AppLaunch.exe (PID: 2596)	
	Checks for external IP AppLaunch.exe (PID: 2596)	

Static information

TRiD

.exe		Generic CIL Executable (.NET, Mono, etc.) (72.2)
.scr		Windows screen saver (12.9)
.dll		Win32 Dynamic Link Library (generic) (6.4)

EXIF

EXE	
AssemblyVersion:	1.0.0.0
ProductVersion:	1.0.0.0

<div><div><div><div><div><div></div></div></div><div><div><div>.exe</div><div> </div><div>Win32 Executable (generic) (4.4)</div></div></div><div><div><div>.exe</div><div> </div><div>Generic Win/DOS Executable (1.9)</div></div></div></div></div></div>	<div><div><div><div><div><div></div></div></div><div><div><div>ProductName:</div><div>TextBasedGameDataTool</div></div></div><div><div><div>OriginalFileName:</div><div>ukgS.exe</div></div></div><div><div><div>LegalTrademarks:</div><div></div></div></div><div><div><div>LegalCopyright:</div><div>Copyright © 2019</div></div></div><div><div><div>InternalName:</div><div>ukgS.exe</div></div></div><div><div><div>FileVersion:</div><div>1.0.0.0</div></div></div><div><div><div>FileDescription:</div><div>TextBasedGameDataTool</div></div></div><div><div><div>CompanyName:</div><div></div></div></div><div><div><div>Comments:</div><div></div></div></div><div><div><div>CharacterSet:</div><div>Unicode</div></div></div><div><div><div>LanguageCode:</div><div>Neutral</div></div></div><div><div><div>FileSubtype:</div><div>0</div></div></div><div><div><div>ObjectFileType:</div><div>Executable application</div></div></div><div><div><div>FileOS:</div><div>Win32</div></div></div><div><div><div>FileFlags:</div><div>(none)</div></div></div><div><div><div>FileFlagsMask:</div><div>0x003f</div></div></div><div><div><div>ProductVersionNumber:</div><div>1.0.0.0</div></div></div><div><div><div>FileVersionNumber:</div><div>1.0.0.0</div></div></div><div><div><div>Subsystem:</div><div>Windows GUI</div></div></div><div><div><div>SubsystemVersion:</div><div>4</div></div></div><div><div><div>ImageVersion:</div><div>0</div></div></div><div><div><div>OSVersion:</div><div>4</div></div></div><div><div><div>EntryPoint:</div><div>0xaaeee6</div></div></div><div><div><div>UninitializedDataSize:</div><div>0</div></div></div><div><div><div>InitializedDataSize:</div><div>1536</div></div></div><div><div><div>CodeSize:</div><div>708608</div></div></div><div><div><div>LinkerVersion:</div><div>48</div></div></div><div><div><div>PEType:</div><div>PE32</div></div></div><div><div><div>TimeStamp:</div><div>2092:10:23 12:28:11+02:00</div></div></div><div><div><div>MachineType:</div><div>Intel 386 or later, and compatibles</div></div></div></div></div></div>
--	--

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	17-Sep-1956 03:59:55
Comments:	
CompanyName:	
FileDescription:	TextBasedGameDataTool
FileVersion:	1.0.0.0
InternalName:	ukgS.exe
LegalCopyright:	Copyright © 2019
LegalTrademarks:	
OriginalFilename:	ukgS.exe
ProductName:	TextBasedGameDataTool
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:	17-Sep-1956 03:59:55
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	0x000ACEEC	0x000AD000	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	7.36422
.src	0x000B0000	0x00000398	0x00000400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	2.90682
.reloc	0x000B2000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

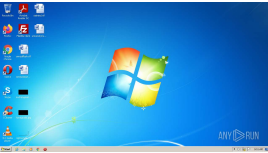
Resources

Title	Entropy	Size	Codepage	Language	Type
1	3.29054	828	UNKNOWN	UNKNOWN	RT_VERSION

Imports

mscoree.dll

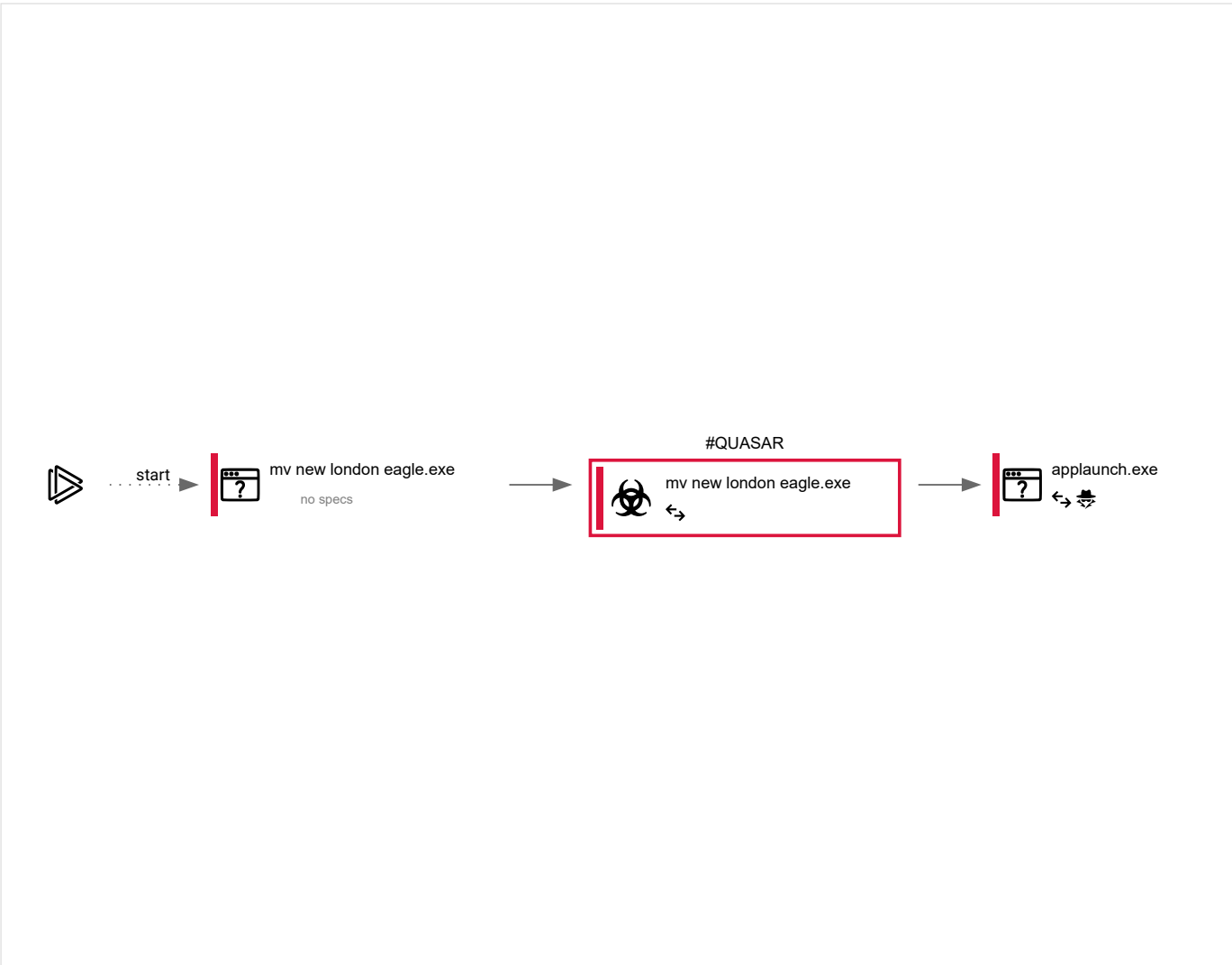
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
37	3	3	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
3944	"C:\Users\admin\AppData\Local\Temp\MV NEW LONDON EAGLE.exe"	C:\Users\admin\AppData\Local\Temp\MV NEW LONDON EAGLE.exe	—	Explorer.EXE
Information				
User:	admin	Integrity Level:	MEDIUM	
Description:	TextBasedGameDataTool	Exit code:	0	
Version:	1.0.0.0			

3712	"C:\Users\admin\AppData\Local\Temp\MV NEW LONDON EAGLE.exe"	C:\Users\admin\AppData\Local\Temp\MV NEW LONDON EAGLE.exe		MV NEW LONDON EAGLE.exe
Information				
User:	admin	Integrity Level:	MEDIUM	
Description:	TextBasedGameDataTool	Version:	1.0.0.0	

2596	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe		MV NEW LONDON EAGLE.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Microsoft .NET ClickOnce Launch Utility	
Exit code:	0	Version:	4.0.30319.34209 built by: FX452RTMGDR	

Registry activity

Total events	Read events	Write events	Delete events
5 224	5 178	46	0

Modification events

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	EnableConsoleTracing
Value:	0		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	ConsoleTracingMask
Value:			

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	MaxFileSize
Value:	1048576		

(PID) Process:	(2596) AppLaunch.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\AppLaunch_RASMANCS
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(3712) MV NEW LONDON EAGLE.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

[illegible]

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	5	1	3

Dropped files

PID	Process	Filename	Type
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE9EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771 MD5: 0D01807A78CCBA080E9CD364048E8781SHA256: 762687C426BD06C9618E894A90D84CEC3D8FA233591A96E4E1867EF248A75E38	binary
2596	AppLaunch.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt MD5: 1043169205608AAC3AA66EE8E58EE243SHA256: B87D113063C7179A2B96BFB58AED1847B60D6B3BB9AC162B1CFF148492DDBF62	text
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B6FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D MD5: 8E415DF0B78E4802E7F48A5440EA8D55SHA256: 2E19DADF850949B62A507F36F99EF30A9DC7059B592DD0954E8476351766F44	der
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7EEA265692AC7955311B9E4CB27AFC35_3F411C6719032639C08C134E44D08A86 MD5: 1965E9EAD5413A74CDEBD202CB89CEDDSHA256: CE04088C301B75864B9197CDE128E4B31DA6125C09830726BE857E8937B96C93	binary
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B6FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D MD5: A89298B1C775B09E8A938B05490B6E67SHA256: FBAEF9B084862B8514A967ADB4644BA4F0FEB743FE01A9B754E8285B05706789	binary
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE9EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771 MD5: 2F0EF87BF02AB98C1EB39D2E42F60F96SHA256: EB5CF0C83A5E7862304575F0DE94585159661E35C6639DA208EDE4F2DCE124D4	der
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7EEA265692AC7955311B9E4CB27AFC35_3F411C6719032639C08C134E44D08A86 MD5: 1B202AB1169C9DF6331D017BC57139F1SHA256: C8BE37E80C45B47ACB7E8A4D2AEC16EEBD937511939F66CED02D9DDA1DCF2372	der
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: 011D544B34AC6CBC37F92C8810AA32FA SHA256: 8D588411269F180C7897D8043BE2089CCFE0FE271142F211430249E083AFA7D1	binary
3712	MV NEW LONDON EAGLE.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB2450769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
5	4	4	4

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2596	AppLaunch.exe	GET	200	104.18.114.97:80	http://icanhazip.com/	US	text	14 b	shared
3712	MV NEW LONDON EAGLE.exe	GET	200	192.124.249.41:80	http://ocsp.godaddy.com//MEIwQDA%2BMDwwOjAJBgUrDgMCGGUABBTklnKBzXkF0Qh0pel3lfHJ9GPAQU0sSw0pHUTBFxs2HL9r0FQW4gwZTaD94CAQc%3D	US	der	1.69 Kb	whitelisted
3712	MV NEW LONDON EAGLE.exe	GET	200	192.124.249.41:80	http://ocsp.godaddy.com//MEQwQjBAMD4wPDAJBgUrDgMCGGUABBTklnKBzXkF0Qh0pel3lfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D	US	der	1.66 Kb	whitelisted
3712	MV NEW LONDON EAGLE.exe	GET	200	72.21.81.240:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9552bd59e5b292f2	US	compressed	4.70 Kb	whitelisted
3712	MV NEW LONDON EAGLE.exe	GET	200	192.124.249.41:80	http://ocsp.godaddy.com//MEowSDBGMEQwQjAJBgUrDgMCGGUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQMK9J47MNMwojPX%2B2y28LQsgM4CCQC%2F44%2B0nb8HBQ%3D%3D	US	der	1.74 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3712	MV NEW LONDON EAGLE.exe	192.124.249.41:80	ocsp.godaddy.com	Sucuri	US	suspicious
3712	MV NEW LONDON EAGLE.exe	72.21.81.240:80	ctldl.windowsupdate.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2596	AppLaunch.exe	104.18.114.97:80	icanhazip.com	Cloudflare Inc	US	malicious
3712	MV NEW LONDON EAGLE.exe	149.154.167.220:443	api.telegram.org	Telegram Messenger LLP	GB	malicious

DNS requests

--

Domain	IP	Reputation
icanhazip.com	104.18.114.97 104.18.115.97	shared
api.telegram.org	149.154.167.220	shared
ctldl.windowsupdate.com	72.21.81.240	whitelisted
ocsp.godaddy.com	192.124.249.41 192.124.249.22 192.124.249.23 192.124.249.36 192.124.249.24	whitelisted

Threats

PID	Process	Class	Message
2596	AppLaunch.exe	Attempted Information Leak	ET POLICY IP Check Domain (icanhazip. com in HTTP Host)
—	—	Misc activity	ET INFO Telegram API Domain in DNS Lookup
3712	MV NEW LONDON EAGLE.exe	Misc activity	ET INFO Observed Telegram API Domain (api .telegram .org in TLS SNI)
3712	MV NEW LONDON EAGLE.exe	Misc activity	ET POLICY Telegram API Certificate Observed

Debug output strings

No debug info



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