ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	NEW ORDER.exe
Full analysis:	https://app.any.run/tasks/3163e539-d8fd-4c95-b724-4ceecb27a848
Verdict:	Malicious activity
Analysis date:	August 17, 2022 at 18:21:05
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	stealer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	2CF2D228E85ED49B887A542BAD0CFF9C
SHA1:	902D3EDC69F56F2382FED65EF665058395B0E012
SHA256:	A3883A6C71F5C60204C4E62218DF3E7CDE638E8A06DC54AF5FBE73A7391BA78E
SSDEEP:	24576:h7eV6jTYDTlVsvdwcE4afbABK7STqIoQl0pgD0:8WTYDTlVsvdwcE4afKKGTq

Software environment set and analysis options

Launch configuration

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

Software preset

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

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

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)
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)

KB3161102
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

Drops executable file immediately after starts
NEW ORDER.exe (PID: 1040)
NEW ORDER.exe (PID: 3408)

Changes the autorun value in the registry
NEW ORDER.exe (PID: 3408)

Steals credentials from Web Browsers
AppLaunch.exe (PID: 3420)

Stealing of credential data
AppLaunch.exe (PID: 3420)

Actions looks like stealing of personal data
AppLaunch.exe (PID: 3420)

SUSPICIOUS

Reads the computer name
NEW ORDER.exe (PID: 1040)
NEW ORDER.exe (PID: 3408)
AppLaunch.exe (PID: 3420)

Checks supported languages
NEW ORDER.exe (PID: 1040)
NEW ORDER.exe (PID: 3408)
AppLaunch.exe (PID: 3420)

Drops a file with a compile date too recent
NEW ORDER.exe (PID: 1040)
NEW ORDER.exe (PID: 3408)

Executable content was dropped or overwritten
NEW ORDER.exe (PID: 1040)
NEW ORDER.exe (PID: 3408)

Application launched itself
NEW ORDER.exe (PID: 1040)

INFO

Reads the computer name
schtasks.exe (PID: 3336)

Checks supported languages
schtasks.exe (PID: 3336)

Reads settings of System Certificates
NEW ORDER.exe (PID: 3408)

Checks Windows Trust Settings
NEW ORDER.exe (PID: 3408)

Static information

TRiD

.exe	|	Generic CIL Executable (.NET, Mono, etc.) (63.1)
.exe	|	Win64 Executable (generic) (23.8)
.dll	|	Win32 Dynamic Link Library (generic) (5.6)
.exe	|	Win32 Executable (generic) (3.8)
.exe	|	Generic Win/DOS Executable (1.7)

EXIF

EXE

AssemblyVersion:	1.0.0.0
ProductVersion:	1.0.0.0
ProductName:	GamespyMasterServer
OriginalFileName:	WvRO.exe

LegalTrademarks:	
LegalCopyright:	Copyright © 2014 J. Weigelt
InternalName:	WvRO.exe
FileVersion:	1.0.0.0
FileDescription:	Gamespy Master Server Emulator
CompanyName:	janelo.net
Comments:	
CharacterSet:	Unicode
LanguageCode:	Neutral
FileSubtype:	0
ObjectFileType:	Executable application
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	1.0.0.0
FileVersionNumber:	1.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x125b6e
UninitializedDataSize:	0
InitializedDataSize:	174080
CodeSize:	1195008
LinkerVersion:	80
PEType:	PE32
TimeStamp:	2022:08:17 02:43:34+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	17-Aug-2022 00:43:34
Comments:	
CompanyName:	janelo.net
FileDescription:	Gamespy Master Server Emulator
FileVersion:	1.0.0.0
InternalName:	WvRO.exe
LegalCopyright:	Copyright © 2014 J. Weigelt
LegalTrademarks:	
OriginalFilename:	WvRO.exe
ProductName:	GamespyMasterServer
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-Aug-2022 00:43:34
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	0x00123B74	0x00123C00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	7.392

.rsrc	0x00126000	0x0002A488	0x0002A600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.50932
.reloc	0x00152000	0x0000000C	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	0.10191

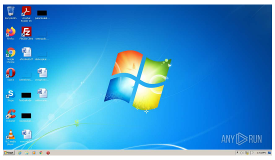
Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.00112	490	Latin 1 / Western European	UNKNOWN	RT_MANIFEST
2	3.58169	67624	Latin 1 / Western European	UNKNOWN	RT_ICON
3	4.19811	38056	Latin 1 / Western European	UNKNOWN	RT_ICON
4	4.14518	21640	Latin 1 / Western European	UNKNOWN	RT_ICON
5	3.91139	16936	Latin 1 / Western European	UNKNOWN	RT_ICON
6	4.47287	9640	Latin 1 / Western European	UNKNOWN	RT_ICON
7	4.47308	4264	Latin 1 / Western European	UNKNOWN	RT_ICON
8	5.03767	2440	Latin 1 / Western European	UNKNOWN	RT_ICON
9	5.16894	1128	Latin 1 / Western European	UNKNOWN	RT_ICON

Imports

mscoree.dll

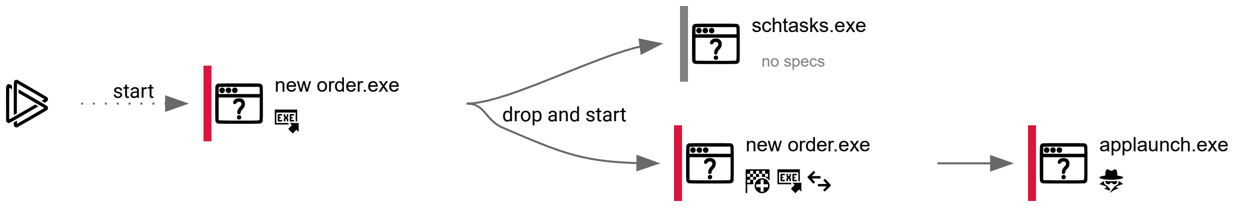
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	4	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
1040	"C:\Users\admin\AppData\Local\Temp\NEW ORDER.exe"	C:\Users\admin\AppData\Local\Temp\NEW ORDER.exe	EXE	Explorer.EXE

Information

User:	admin	**Company:**	janelo.net
Integrity Level:	MEDIUM	**Description:**	Gamespy Master Server Emulator
Exit code:	0	**Version:**	1.0.0.0

3336	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\XKHJsQnezkA" /XML "C:\Users\admin\AppData\Local\Temp\tmp8752.tmp"	C:\Windows\System32\schtasks.exe	—	NEW ORDER.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)

3408	"{path}"	C:\Users\admin\AppData\Local\Temp\NEW ORDER.exe	NEW ORDER.exe

Information

User:	admin	**Company:**	janelo.net
Integrity Level:	MEDIUM	**Description:**	Gamespy Master Server Emulator
Version:	1.0.0.0		

3420	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	NEW ORDER.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
5 138	5 093	45	0

Modification events

(PID) Process: (1040) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1040) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1040) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1040) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings
Operation: write **Name:** GetCONTACTSreg
Value: getcontact

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings
Operation: write **Name:** GetMessagesreg
Value: getmessges

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Operation: write **Name:** fireball
Value: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Templates\cusped.exe

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B0100000900000000000000000000000000000000000040000000000000C0E333BBEAB1D3010000000000000000000000000001000000002000000C0A8016400000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionReason
Value: 1

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 18B2362138B2D801

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecision
Value: 0

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadNetworkName
Value: Network 4

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionReason
Value: 1

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 18B2362138B2D801

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecision
Value: 0

(PID) Process: (3408) NEW ORDER.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	5	2	3

Dropped files

PID	Process	Filename	Type
1040	NEW ORDER.exe	C:\Users\admin\AppData\Roaming\XKHJsQnezkA.exe **MD5:** 2CF2D228E85ED49B887A542BAD0CFF9C **SHA256:** A3883A6C71F5C60204C4E62218DF3E7CDE638E8A06DC54AF5FBE73A7391BA78E	executable
3408	NEW ORDER.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Templates\cusped.exe **MD5:** 2CF2D228E85ED49B887A542BAD0CFF9C **SHA256:** A3883A6C71F5C60204C4E62218DF3E7CDE638E8A06DC54AF5FBE73A7391BA78E	executable
3420	AppLaunch.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt **MD5:** FE08634962BD497C4A6EF67894D2B155 **SHA256:** 40F55A452019EC22D35E17ACA5FCCF4253D8770AEF2F2D6FB0986DC44FF1C55C	text
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** 3B28AE504F010A80122BEA45F5D81704 **SHA256:** 0BE8B5E6285DAD11AF36F5A106C4D818A16149C20C5DEF82047A5135E9DB6E9C	binary

1040	NEW ORDER.exe	C:\Users\admin\AppData\Local\Temp\tmp8752.tmp **MD5:** A376541C92DFC1F1DFE021058F9ECFD0 **SHA256:** E613244EAE0F6C98BCA0472581167176AB8DA26B272960CCE4F20F1836E18FCF	xml
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D **MD5:** 8E415DF0B78E4802E7F48A5440EA8D55 **SHA256:** 2E19DADFD850949B62A507F36F99EF30A9DC7059B592DD0954E8476351766F44	der
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D **MD5:** A0ED6605B9A1104957B477857F09DA6C **SHA256:** DBB8F31CA4DEF03E93D84C35FD818518EE6655C6DDCDE57450A9D798145E60B4	binary
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771 **MD5:** 5E966C37783F31945029F5DF5B4B5F2B **SHA256:** 66B68681C65AB3658A7CB89E6F48BC77FDED05242B5715FFC3809F9E27178862	binary
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771 **MD5:** 76859172B2E1AB02A4D8651895FC2FD7 **SHA256:** 131FAD2D3E4A49BE632EED068298EF3076DFCF2823A8445A272D36CF73F564B0	der
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7EEA265692AC7955311B9E4CB27AFC35_3F411C6719032639C08C134E44D08A86 **MD5:** DC343D0028E7CC1005D3524E9D3D67AE **SHA256:** CA87C85C8AC994E56E0BDB7AB9B539574BA1CD87BA6001B5DBF82583978831D1	binary
3408	NEW ORDER.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7EEA265692AC7955311B9E4CB27AFC35_3F411C6719032639C08C134E44D08A86 **MD5:** F16D4BA9A2D7B5A21D4DCC475B7896AA **SHA256:** D8B90E0F67AF7BFEC828683D9D82FD8142E762AB5935317EEB1D6F97C3991873	der

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
4	3	3	3

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3408	NEW ORDER.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9552bd59e5b292f2	US	compressed	4.70 Kb	whitelisted
3408	NEW ORDER.exe	GET	200	192.124.249.24:80	http://ocsp.godaddy.com//MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkF0Qh0pel3lfHJ9GPAQU0sSw0pHUTBFxs2HLPaH%2B3ahq1OMCAxvnFQ%3D%3D	US	der	1.66 Kb	whitelisted
3408	NEW ORDER.exe	GET	200	192.124.249.24:80	http://ocsp.godaddy.com//MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQdI2%2BOBkuXH93foRUj4a7lAr4rGwQUOpqFBxBnKLbv9r0FQW4gwZTaD94CAQc%3D	US	der	1.69 Kb	whitelisted
3408	NEW ORDER.exe	GET	200	192.124.249.24:80	http://ocsp.godaddy.com//MEowSDBGMEQwQjAJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQMK9J47MNIMwojPX%2B2yz8LQsgM4CCQC%2F44%2BOnb8HBQ%3D%3D	US	der	1.74 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3408	NEW ORDER.exe	149.154.167.220:443	api.telegram.org	Telegram Messenger LLP	GB	malicious
3408	NEW ORDER.exe	209.197.3.8:80	ctldl.windowsupdate.com	Highwinds Network Group, Inc.	US	suspicious
3408	NEW ORDER.exe	192.124.249.24:80	ocsp.godaddy.com	Sucuri	US	suspicious

DNS requests

Domain	IP	Reputation
api.telegram.org	149.154.167.220	shared
ctldl.windowsupdate.com	209.197.3.8	whitelisted
ocsp.godaddy.com	192.124.249.24 192.124.249.36 192.124.249.41 192.124.249.22 192.124.249.23	whitelisted

Threats

PID	Process	Class	Message

—	—	Misc activity	ET INFO Telegram API Domain in DNS Lookup
3408	NEW ORDER.exe	Misc activity	ET INFO Observed Telegram API Domain (api .telegram .org in TLS SNI)
3408	NEW ORDER.exe	Misc activity	ET POLICY Telegram API Certificate Observed

Debug output strings

No debug info

ANY.RUN INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN