







General Info

File name:	exe_from_html.exe_
Full analysis:	https://app.any.run/tasks/bd76a06b-1189-414e-ad50-5d140bd88bd7
Verdict:	Malicious activity
Analysis date:	September 23, 2020 at 04:57:07
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	trojan ramnit
Indicators:	   
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
MD5:	5B97603AF0FC8F1DD40FC69BD6CA89CF
SHA1:	18D63DBDE43A5BC700AE55B9A013C596021CCD13
SHA256:	33D3F697332B0FC4E09540CB9DC622AC0675FB8B2733554D4C0199307774AB52
SSDEEP:	3072:dR0zoTq0+R07lwnYZCWfhkDwyXZ7w0pLyE+BrRvPxFw:zkdNwBSCUycyXZ00pLj+BVHxFw

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:	on
Network:	on				

Software preset

Internet Explorer 11.0.9600.17843 KB3058515

Adobe Acrobat Reader DC MUI (15.023.20070)

Adobe Flash Player 26 ActiveX (26.0.0.131)

Adobe Flash Player 26 NPAPI (26.0.0.131)

Adobe Flash Player 26 PPAPI (26.0.0.131)

Adobe Refresh Manager (1.8.0)

CCleaner (5.35)

FileZilla Client 3.36.0 (3.36.0)

Google Chrome (75.0.3770.100)

Google Update Helper (1.3.34.7)

Java 8 Update 92 (8.0.920.14)

Java Auto Updater (2.8.92.14)

Microsoft .NET Framework 4.7.2 (4.7.03062)

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

KB2533623

KB2534111

KB2639308

KB2729094

KB2731771

KB2786081

KB2834140

KB2882822

KB2888049

KB2999226

KB4019990

KB976902

LocalPack AU Package

LocalPack CA Package

LocalPack GB Package

LocalPack US Package

LocalPack ZA Package

PlatformUpdate Win7 SRV08R2 Package TopLevel

ProfessionalEdition

UltimateEdition

Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)

Microsoft Office IME (Korean) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)

Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)

Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)

Microsoft Office O MUI (French) 2010 (14.0.4763.1000)

Microsoft Office O MUI (German) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)

Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)

Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)

Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)

Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)

Microsoft Office Professional 2010 (14.0.6029.1000)

Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)

Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)

Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)

Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)

Microsoft Office Proof (English) 2010 (14.0.6029.1000)

Microsoft Office Proof (French) 2010 (14.0.6029.1000)

Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)

Microsoft Office Proof (German) 2010 (14.0.4763.1000)

Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Single Image 2010 (14.0.6029.1000)
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)

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 68.0.1 (x86 en-US) (68.0.1)

Notepad++ (32-bit x86) (7.5.1)

Opera 12.15 (12.15.1748)

Skype version 8.29 (8.29)

Update for Microsoft .NET Framework 4.7.2 (KB4087364) (1)

VLC media player (2.2.6)

WinRAR 5.60 (32-bit) (5.60.0)

srvpost (2.12.72)

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Changes the login/logoff helper path in the registry iexplore.exe (PID: 1956)	Executable content was dropped or overwritten exe_from_html.exe_exe (PID: 928)	No info indicators.
RAMNIT was detected iexplore.exe (PID: 1956)	Starts Internet Explorer DesktopLayer.exe (PID: 3044)	
Connects to CnC server iexplore.exe (PID: 1956)	Starts itself from another location exe_from_html.exe_exe (PID: 928)	
	Creates files in the program directory iexplore.exe (PID: 1956)	

Static information

TRiD

.dll | Win32 Dynamic Link Library (generic) (34.2)

.exe | Win32 Executable (generic) (23.5)

.exe | Win16/32 Executable Delphi generic (10.8)

.exe | Clipper DOS Executable (10.5)

.exe | Generic Win/DOS Executable (10.4)

EXIF

EXE

MachineType: Intel 386 or later, and compatibles

TimeStamp: 2008:02:12 12:02:20+01:00

PEType: PE32

LinkerVersion: 7.4

CodeSize: 57344

InitializedDataSize: 4096

UninitializedDataSize: 122880

EntryPoint: 0x2c030

OSVersion: 10

ImageVersion: 8.1

SubsystemVersion: 4

Subsystem: Windows GUI

FileVersionNumber: 106.42.73.61

ProductVersionNumber: 106.42.73.61

FileFlagsMask: 0x003f

FileFlags: (none)

FileOS: Windows NT 32-bit

ObjectFileType: Executable application

FileSubtype: 0

LanguageCode: English (U.S.)

CharacterSet: Unicode

CompanyName: SOFTWIN S.R.L.

FileDescription: BitDefender Management Console

FileVersion: 106.42.73.61

InternalName: фжзрюкшэщ

LegalCopyright: 2528-6142

OriginalFileName: nedwp.exe

ProductName: люзанх

ProductVersion: 106.42.73.61

Summary

Architecture: IMAGE_FILE_MACHINE_I386

Subsystem: IMAGE_SUBSYSTEM_WINDOWS_GUI

Compilation Date: 12-Feb-2008 11:02:20

Detected languages: English - United States

	Russian - Russia
CompanyName:	SOFTWIN S.R.L.
FileDescription:	BitDefender Management Console
FileVersion:	106.42.73.61
InternalName:	фжэрюкшэщ
LegalCopyright:	2528-6142
OriginalFilename:	nedwp.exe
ProductName:	люзанх
ProductVersion:	106.42.73.61

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:	0x00000100

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	12-Feb-2008 11:02:20
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_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
UPX0	0x00001000	0x0001E000	0x00000000	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
UPX1	0x0001F000	0x0000E000	0x0000D200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.95361
.rsrc	0x0002D000	0x00015000	0x00015000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	6.919

Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.00532	360	UNKNOWN	Russian - Russia	RT_MANIFEST

Imports

KERNEL32.DLL
SHELL32.DLL
USER32.DLL

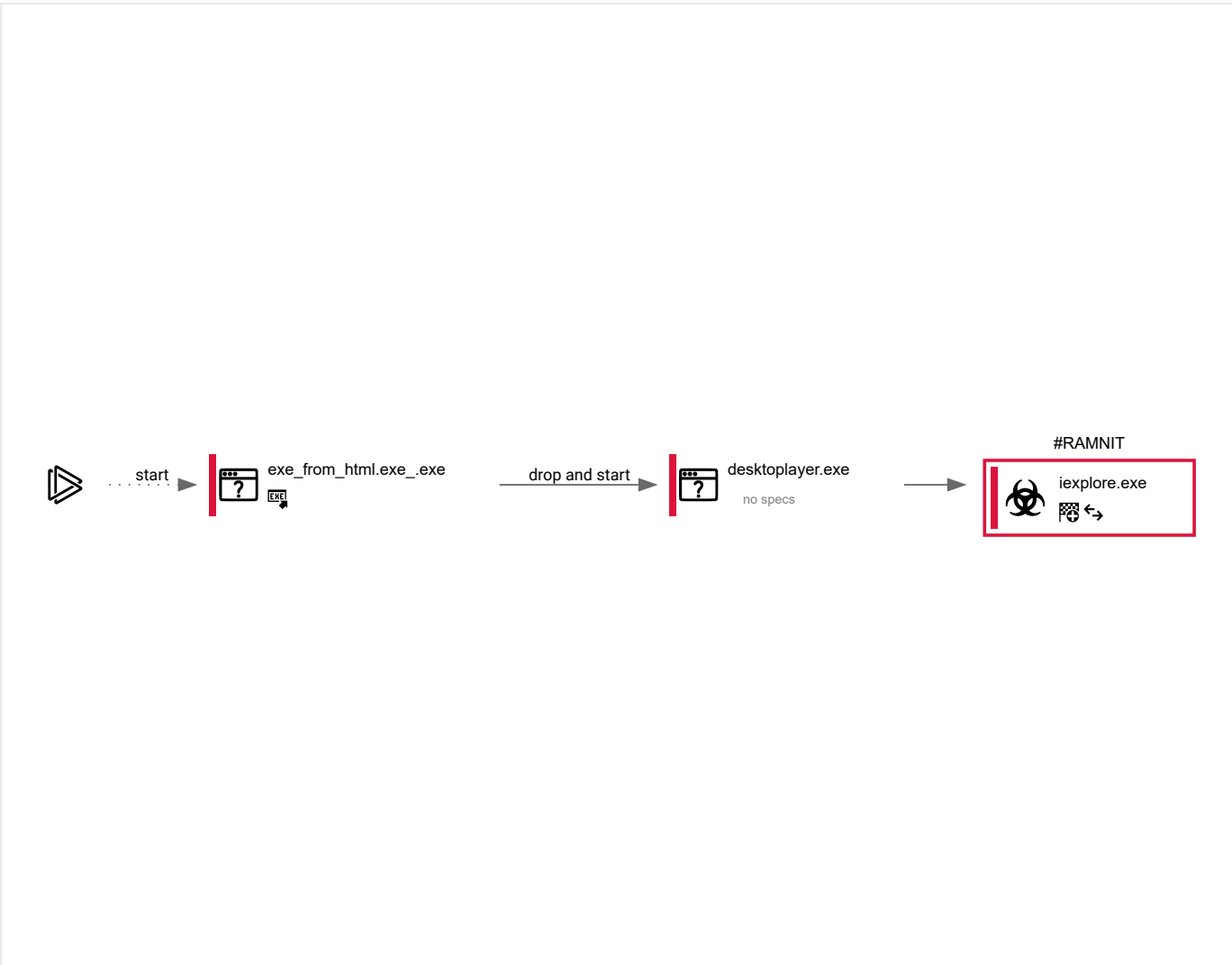
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
39	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
928	"C:\Users\admin\AppData\Local\Temp\exe_from_html.exe_exe" /SETUP	C:\Users\admin\AppData\Local\Temp\exe_from_html.exe_exe		explorer.exe
Information				
User:	admin	Company:	SOFTWIN S.R.L.	
Integrity Level:	MEDIUM	Description:	BitDefender Management Console	
Exit code:	0	Version:	106.42.73.61	

3044	C:\Users\admin\Microsoft\DesktopLayer.exe	C:\Users\admin\Microsoft\DesktopLayer.exe	—	exe_from_html.exe_exe
Information				
User:	admin	Company:	SOFTWIN S.R.L.	
Integrity Level:	MEDIUM	Description:	BitDefender Management Console	
Exit code:	0	Version:	106.42.73.61	

1956	"C:\Program Files\Internet Explorer\iexplore.exe"	C:\Program Files\Internet Explorer\iexplore.exe	↔ 🛡 🌐	DesktopLayer.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Internet Explorer	
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)			

Registry activity

Total events	Read events	Write events	Delete events
62	3	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	0	75	0

Dropped files

PID	Process	Filename	Type
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Berime.htm MD5: 505A0C91FC2503BF0E530AD542218C0F SHA256: 75970ED6DFC8F34CA2E027DC94093E2A5406DF087732C107EF3AEA8BED56B809	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Benioku.htm MD5: C933E05B7B280A1FD7A5FE586700D93F SHA256: B006625E7117465B242EA8CD26EE1C989D5A1BEA31DA36E9981459693ABBF5F5	html
928	exe_from_html.exe_exe	C:\Users\admin\Microsoft\DesktopLayer.exe MD5: 5B97603AF0FC8F1DD40FC69BD6CA89CF SHA256: 33D3F697332B0FC4E09540CB9DC622AC0675FB8B2733554D4C0199307774AB52	executable
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\IrakHau.htm MD5: 1CEFFD48BB9893D094D27C840A1C99CE SHA256: EF6444BCA2F9B5D0C122B512D7C231FCA2E0457E5E2CB2EB43C4220E7FE1918F	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Leame.htm MD5: 3671540C78B152B25B34F63E24893363 SHA256: 57C97916D9625AF1D05D1DF3AFCE87DCB9B23F4D06389FF334E6546D3310955F	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LeesMij.htm MD5: CD4A3F184635FF83B8D6BA6C2988860C SHA256: D2717F99F7F399ACDD3E3E00938D96F808953EFC7F039B331E0438DBC4FD9B33	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Llegiu-me.htm MD5: 2817810E82F9028354F570E84EF2B6C6 SHA256: C2F7E5731827629D491918900DF679D07FF43F6FE4780709F1AAD491AFE18CA6	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Liesmich.htm MD5: DC71F2B6E0D325BADA2FC9E7BC5CC530 SHA256: 426EE9B3CCA06A047FE4380FCA244C4E82457B0AD75F79A850880F31A0585178	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Leggimi.htm MD5: 37F12FF9D07E4B4CB9917B0C1874A2B5 SHA256: 30A5C05C2028E4AD9D0C945AB8F561DC07CB3BE790ADCB2684082786710B2190	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Lisezmoi.htm MD5: D671D94C9821CCBC8EFAB8F4F62BBACD SHA256: 006458935A3EA20BAF5AB458A86478D9A6EE320FB1EC9539CBAE19B3277D8CB7	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LeiaMe.htm MD5: E53828EDF5403EBAA0F5CDC471FF6251 SHA256: 126B1BC034FD6EB19B6F67C6A34CA3FF3C353EDDD3F01DBF9FE8AF73B536DC44	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LueMinut.htm MD5: 7D5890A89E2C3F987F0A0FD6502E02E3 SHA256: 7396F3A5D1B36B579DCB8DDC4F46238245B4CF333793619889E62D843C4EB2D8	html
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\CAT\license.html MD5: 0E160377FCE86BA819E1DAE6D26ADACA SHA256: 3335A9646041F5BBB8F723B88F9D924062A4F365A32D580D4DBD76D587248DA7	xml
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\CHT\license.html MD5: EA57A3B5850E521861E5E71FD675860B SHA256: 056D025232008262C71D79CDFE02C1AE4BA3AA0B076A5E3710FB4D06FEC11F16	xml

1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\CHS\license.html	xml
		MD5: 3CFDBD2589B37C66175CD7236CF1C3B2	SHA256: A237786D5BB0E89BE0E7BB0660D053DB1EE59E6CCA07C32772E661393E8EBD22
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\CZE\license.html	xml
		MD5: 21C8D9CAB349D05F36CFCFA04739B464	SHA256: EE5655333C7B2C867A4B49D3EB50805C165874D459556B6C231DABB7D2C96547
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\ENU\license.html	xml
		MD5: F52F0DCD10BA127443B40B4DB46DB8DF	SHA256: 49882B4BAE26D411B107340A9D76A1B742128BA209A9B183E22BAB3182C4D802
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\EUQ\license.html	xml
		MD5: 55C7442C7D3EA5EAD04CD3353732CC8B	SHA256: B38CCC6EEE716B35E8B56D7DB65888C64028C22757883B3052C12FA52B7FB97B
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\ DAN\license.html	xml
		MD5: AC08DE9FD1B4AE0577ADC79CEE210C47	SHA256: E33A875037597289703A4656C7160B3EA3B7FA7031A9B87439AFC9A9C4B6C3F2
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\FRA\license.html	xml
		MD5: 12A834D482A179657D5FF6C66FA08F78	SHA256: F65BFF0466C4D6534C5C3649DBD784EEFF75FF0B8E3E1DCE362AB476E3C3C6
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\DEU\license.html	xml
		MD5: 3D3692439AA5EEAEFC7812867CFE9066	SHA256: 10A6256A421CF5DFB47554A2E266656FB1F3B01C4A2FD6F60E0E0533CC30B3A4
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\ESP\license.html	xml
		MD5: 542421AC98EEBD1989D2B9E7B2F814DB	SHA256: 47A836C74151754E427B60FE512541591FD56384B5AE87F6437506491D068BDA
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\HRV\license.html	xml
		MD5: 6FBA91045B8C827F60DD58A6A985C6CF	SHA256: D69CB13184DC4CDC9272FADE8C350F490C269236CFA5827742FAD8E5805A7AE
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\ITA\license.html	xml
		MD5: 8C49A90FC702EB3DF5D7220C95F33D73	SHA256: B91C8AD5467BB2978A7A8D5FE078D0ABD789B214CDCA75DF1DE3FDA87BFA2150
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\HUN\license.html	xml
		MD5: 6B0B393FFE899900CF7A5AD7380645F	SHA256: DAF687AB24EC0E20E69B6B39B426CDAD42104808E61EFACFC9A7BAB884FA5AF1
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\JPN\license.html	xml
		MD5: 249BC7C8908C6016319E37BD5EA6D071	SHA256: A43895FB27C356604E258D3544B70E0155E84A3B046BD203536731E058B015FD
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\POL\license.html	xml
		MD5: 7FBE2F3009F516A8CF4DCFBEB8331A9C0	SHA256: EC33F5A196F369FCA33636EEC3F110E0256D55839A1C7220372026534E6EC154
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\KOR\license.html	xml
		MD5: CA5CE8AC9429C95717D4057A898AE565	SHA256: D14F8B37593AF20B5DBB0EA109F660173CF40918B9FDCDC5C1CECE118F1B5285
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\PTB\license.html	xml
		MD5: 314FB2E55E72A381BEBE9F9C40ED8EF2	SHA256: 1B6861374E5438F7D3E9235C97C012DE9333CD481CFB6872A0DBF9FFE4252262
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\NOR\license.html	xml
		MD5: 28352CF4E2ED4DB49DDBA16549111B3B	SHA256: C0098972FF7D1D5217D1B4098EBF08D840F120380F8FFB6F045BA0A206228D8
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\NLD\license.html	xml
		MD5: B0651C7346E73E63B3107F8AD13E11E5	SHA256: 7B49E16B58D593A5F16FB33DCEB2A8344449642BC0D7E22692EA30BC7FCC5C8D
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\RUM\license.html	xml
		MD5: B1908DFAC1F9B18AB8BA03CD5003D509	SHA256: 5167954FFA5B2266AE5C10C682734BC95F6ABDE86F5F27F4CF64C157FED70632
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\RUS\license.html	xml
		MD5: 836DF74772326BA8C7F989DCB53EB7BA	SHA256: C85969D8E3BBD862DA05D9B08755CC72709A1925A50AF2EC87B3E904A2A16F84
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\SLV\license.html	xml
		MD5: 35FC26047E90F570F888C911517A8EE9	SHA256: C256CDA38310E07C7827FFAA7F501FDCE6083E3D5C5C7CC251087C3AE628636B
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\TUR\license.html	xml
		MD5: 71BF2D9F325263DD42145CC799943010	SHA256: BEE776FF8A3CF67D5863538A2D1BA1EA08452C0ABCEBD93B13FD1A1072E3C23C
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\SKY\license.html	xml
		MD5: D524413B1AF64FE90A374330172D13BB	SHA256: 229432281E6CEA7632B73FA4271B29FC1E76AADF8452970D6C32ED0CC527EEFD
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\UKR\license.html	xml
		MD5: EF160B112A8F1F2665FB47E892B1F487	SHA256: BCE7A04C0DE08574261363B7ED40FD0F1E022B718243F5D2A25783C7B9056942
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	html
		MD5: 703D27ECEBB7C9C799746EE9F9431A78	SHA256: DF3E1DDDED6B83B44CB5D5AE8B5ABDE2814C373FBAB65C8C82C2B4DA04918D4
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\SVE\license.html	xml
		MD5: E0018D1774A60688D947F9D937854273	SHA256: 95C10295BF18A53360417A63BB8EB110DBE3E6A25627E55A6BDD5BBD1BC2299A
1956	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Reader\Legal\SUO\license.html	xml
		MD5: 71DE016CA198D95FD7D4E497BF3926A9	SHA256: F7FDCE1B444D8129E9AC20CB24287AB3470011F92D0BE7E31479548EDE74D6FF

Network activity

HTTP(S) requests

TCP/UDP connections

DNS requests

Threats

0

3

1

5

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1956	iexplore.exe	216.58.206.14:80	—	Google Inc.	US	<div>whitelisted</div>
1956	iexplore.exe	72.26.218.70:443	fget-career.com	Voxel Dot Net, Inc.	NL	<div>malicious</div>

DNS requests

Domain	IP	Reputation
fget-career.com	72.26.218.70	<div>malicious</div>

Threats

PID	Process	Class	Message
1956	iexplore.exe	<div>A Network Trojan was detected</div>	ET TROJAN Win32/Ramnit Checkin
1956	iexplore.exe	<div>A Network Trojan was detected</div>	MALWARE [PTsecurity] Win32/Ramnit Checkin
1956	iexplore.exe	<div>A Network Trojan was detected</div>	ET TROJAN Win32/Ramnit Checkin
1956	iexplore.exe	<div>A Network Trojan was detected</div>	MALWARE [PTsecurity] Win32/Ramnit Checkin

Debug output strings

No debug info