ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	bookworm_kasp.exe
Full analysis:	https://app.any.run/tasks/e931b203-6e4f-4d97-b3e0-45da21dacfda
Verdict:	Malicious activity
Analysis date:	May 20, 2020 at 18:18:28
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, RAR self-extracting archive
MD5:	0D57D2BEF1296BE62A3E791BFAD33BCD
SHA1:	084ABCB69B8A1DB256B363746CE6EF6F7CD547D8
SHA256:	C9434A3B15609527D6A986D747AA13A90786D1E86FDDD864CBFBAF2F01BFE1FB
SSDEEP:	6144:DcWMJJhqryYP/daqQ1rysMltKkEn5+zP2/t24UYyeztON83bJd:DczJJhqrVPlerZMVk0+zP2V24Ugukbj

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)
- 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
- 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 (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)
QGA (2.10.63)
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)

Behavior activities

MALICIOUS

Loads dropped or rewritten executable
migwiz.exe (PID: 2376)
rundll32.exe (PID: 3324)
ushata.exe (PID: 4060)
ushata.exe (PID: 1520)

Application was dropped or rewritten from another process
ushata.exe (PID: 1520)
ushata.exe (PID: 4060)

Actions looks like stealing of personal data
bookworm_kasp.exe (PID: 1328)
dllhost.exe (PID: 2908)

Uses SVCHOST.EXE for hidden code execution
ushata.exe (PID: 1520)

SUSPICIOUS

Creates files in the Windows directory
DllHost.exe (PID: 1948)

Executable content was dropped or overwritten
DllHost.exe (PID: 1948)
migwiz.exe (PID: 2376)
bookworm_kasp.exe (PID: 1328)
ushata.exe (PID: 4060)

Creates files in the user directory
ushata.exe (PID: 4060)
svchost.exe (PID: 3036)

Executed via COM
DllHost.exe (PID: 1948)

Executed as Windows Service
ushata.exe (PID: 1520)

Creates or modifies windows services
migwiz.exe (PID: 2376)

Uses RUNDLL32.EXE to load library
ushata.exe (PID: 4060)

Removes files from Windows directory
DllHost.exe (PID: 1948)

Reads Internet Cache Settings
svchost.exe (PID: 3036)

INFO

No info indicators.

Static information

TRiD

.exe | Win32 Executable MS Visual C++ (generic) (42.2)
.exe | Win64 Executable (generic) (37.3)
.dll | Win32 Dynamic Link Library (generic) (8.8)
.exe | Win32 Executable (generic) (6)
.exe | Generic Win/DOS Executable (2.7)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2010:02:10 14:09:37+01:00
PEType:	PE32
LinkerVersion:	9
CodeSize:	67584
InitializedDataSize:	35840
UninitializedDataSize:	0
EntryPoint:	0xa785
OSVersion:	5
ImageVersion:	0
SubsystemVersion:	4
Subsystem:	Windows GUI

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	10-Feb-2010 13:09:37
Detected languages:	English - United States
	Process Default Language
Debug artifacts:	d:\Projects\WinRAR\SFX\build\sfxrar32\Release\sfxrar.pdb

DOS Header

PE Headers

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:	0x000000E8

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	10-Feb-2010 13:09:37
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_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x00010742	0x00010800	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.57241
.rdata	0x00012000	0x00001865	0x00001A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.32473
.data	0x00014000	0x0000BFF4	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	3.5458
.CRT	0x00020000	0x00000010	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	0.220914
.rsrc	0x00021000	0x00006D8C	0x00006E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.43887

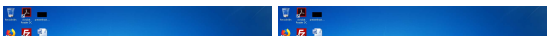
Resources

Title	Entropy	Size	Codepage	Language	Type
1	5.20816	1464	Latin 1 / Western European	English - United States	RT_MANIFEST
7	3.24143	556	Latin 1 / Western European	English - United States	RT_STRING
8	3.28574	946	Latin 1 / Western European	English - United States	RT_STRING
9	3.04375	530	Latin 1 / Western European	English - United States	RT_STRING
10	3.15563	638	Latin 1 / Western European	English - United States	RT_STRING
11	2.02306	76	Latin 1 / Western European	English - United States	RT_STRING
100	1.91924	20	Latin 1 / Western European	Process Default Language	RT_GROUP_ICON
101	4.19099	2998	Latin 1 / Western European	English - United States	RT_BITMAP
ASKNEXTVOL	3.42606	642	Latin 1 / Western European	English - United States	RT_DIALOG
GETPASSWORD1	3.33783	310	Latin 1 / Western European	English - United States	RT_DIALOG
LICENSEDLG	3.1404	232	Latin 1 / Western European	English - United States	RT_DIALOG
RENAMEDLG	3.08066	298	Latin 1 / Western European	English - United States	RT_DIALOG
REPLACEFILEDLG	3.27209	820	Latin 1 / Western European	English - United States	RT_DIALOG
STARTDLG	3.46021	542	Latin 1 / Western European	English - United States	RT_DIALOG

Imports

ADVAPI32.dll
COMCTL32.dll
COMDLG32.dll
GDI32.dll
KERNEL32.dll
OLEAUT32.dll
SHELL32.dll
USER32.dll
ole32.dll

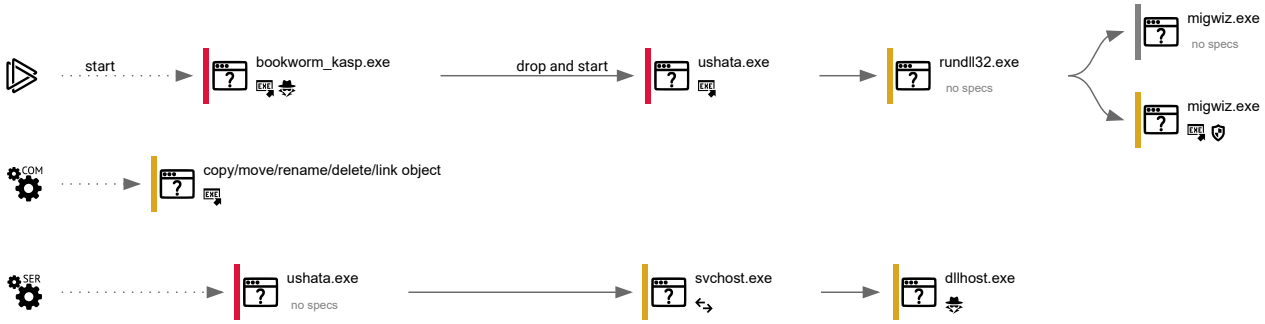
Video and screenshots




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
51	9	3	5

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
1328	"C:\Users\admin\AppData\Local\Temp\bookworm_kasp.exe"	C:\Users\admin\AppData\Local\Temp\bookworm_kasp.exe		explorer.exe
Information				
User: admin	Integrity Level: MEDIUM			
Exit code: 0				
4060	"C:\Users\admin\AppData\Local\Temp\RarSFX0\ushata.exe"	C:\Users\admin\AppData\Local\Temp\RarSFX0\ushata.exe		bookworm_kasp.exe

Information

User:	admin	**Company:**	Kaspersky Lab ZAO
Integrity Level:	MEDIUM	**Description:**	Kaspersky Anti-Virus
Exit code:	0	**Version:**	14.0.0.4651

3324 "C:\Users\admin\AppData\Local\Temp\bpu.dll",bpu C:\Windows\System32\rundll32.exe – ushata.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows host process (Rundll32)
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

1948 C:\Windows\system32\DllHost.exe /Processid:{3AD05575-8857-4850-9277-11B85BDB8E09} C:\Windows\system32\DllHost.exe svchost.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	COM Surrogate
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3096 "C:\Windows\system32\migwiz\migwiz.exe" "C:\Users\admin\AppData\Local\Temp\bpu.dll" C:\Windows\system32\migwiz\migwiz.exe – rundll32.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Easy Transfer Application
Exit code:	3221226540	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2376 "C:\Windows\system32\migwiz\migwiz.exe" "C:\Users\admin\AppData\Local\Temp\bpu.dll" C:\Windows\system32\migwiz\migwiz.exe rundll32.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Easy Transfer Application
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

1520 C:\Users\admin\AppData\Roaming\Surge\ushata.exe C:\Users\admin\AppData\Roaming\Surge\ushata.exe – services.exe

Information

User:	SYSTEM	**Company:**	Kaspersky Lab ZAO
Integrity Level:	SYSTEM	**Description:**	Kaspersky Anti-Virus
Exit code:	0	**Version:**	14.0.0.4651

3036 "C:\Users\admin\AppData\Roaming\Surge\" C:\Windows\System32\svchost.exe ushata.exe

Information

User:	SYSTEM	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Host Process for Windows Services
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

2908 C:\Windows\System32\dllhost.exe -user C:\Windows\System32\dllhost.exe svchost.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	COM Surrogate
Version:	6.1.7600.16385 (win7_rtm.090713-1255)		

Registry activity

Total events	Read events	Write events	Delete events
753	741	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types

8	6	1	0

Dropped files

PID	Process	Filename	Type
1520	ushata.exe	C: **MD5:** — **SHA256:** —	—
1948	DllHost.exe	C:\Windows\System32\migwiz\cryptbase.dll **MD5:** 3033A42281F75506014046DCDA16EDD6 **SHA256:** BDA084085D7B793859E843A9F94BCB8BEB163AFC4E5E89BD13AF5D5EAFEFE52A	executable
4060	ushata.exe	C:\Users\admin\AppData\Local\Temp\bpu.ini **MD5:** 76C78A0B62F6D7D148EDB0E70FFA9047 **SHA256:** 207FF8F8B6229C712000D90188254B405E116CB5AD970CB0F82FD93EF9DC5F77	binary
1328	bookworm_kasp.exe	C:\Users\admin\AppData\Local\Temp\RarSFX0\readme.txt **MD5:** 2E1D6CFF4B52694C0905113D999587F9 **SHA256:** 9420DEDECCB3F4BC47225A6D700D413CE4F72D8441F75E14D683578294C039F6	binary
4060	ushata.exe	C:\Users\admin\AppData\Local\Temp\bpu.dll **MD5:** 3033A42281F75506014046DCDA16EDD6 **SHA256:** BDA084085D7B793859E843A9F94BCB8BEB163AFC4E5E89BD13AF5D5EAFEFE52A	executable
4060	ushata.exe	C:\Users\admin\AppData\Roaming\Surge\ushata.dll **MD5:** 551AD5248ACA220EE2E9E87E4E4CCB66 **SHA256:** F79DE476C1560AE7A432C1FE26904A50B0DD4E776ED4C8410C78F48166413DB8	executable
3036	svchost.exe	C:\Users\admin\AppData\Roaming\Surge\E3410EE6 **MD5:** FFD3CBCBA93E59A808B5F3D5F56307A0 **SHA256:** 181EC6C72ACA6609F2212FF7EE47C42D5D387212623CCBCCE77CDFE63E1A47C7	text
2376	migwiz.exe	C:\Users\admin\AppData\Roaming\Surge\ushata.dll **MD5:** 551AD5248ACA220EE2E9E87E4E4CCB66 **SHA256:** F79DE476C1560AE7A432C1FE26904A50B0DD4E776ED4C8410C78F48166413DB8	executable
4060	ushata.exe	C:\Users\admin\AppData\Roaming\Surge\ushata.exe **MD5:** E26D04CECD6C7C71CFBB3F335875BC31 **SHA256:** 902D771612EDECC03757B289A6FE94CD18F2C88C0FC64F93F8AC449502E4EC52	executable
4060	ushata.exe	C:\Users\admin\AppData\Roaming\Surge\delete.txt **MD5:** 9EB1524D9B512F0C5E784A5716434424 **SHA256:** 8AE0A59ACBAF5FCE4749123A0C4C1F2CF53E4982A74588947C7EA12D878A395A	binary
2376	migwiz.exe	C:\Users\admin\AppData\Roaming\Surge\ushata **MD5:** F2F11E06867B49C26A34094311A12F29 **SHA256:** 7336147234C2767E912BBE76AA8ADD40D4E47E5A6407C9FFE4D7A9B3EEF03DDF	binary
4060	ushata.exe	C:\Users\admin\AppData\Roaming\Surge\sgkey.data **MD5:** 4C97E9CC1C54683410F6F129149F65F8 **SHA256:** D593977A5CCD1D866554D03D6103D9096AADFFBD07FBB323B5E7B6FAA244958D	binary
1328	bookworm_kasp.exe	C:\Users\admin\AppData\Local\Temp\RarSFX0\ushata.dll **MD5:** 551AD5248ACA220EE2E9E87E4E4CCB66 **SHA256:** F79DE476C1560AE7A432C1FE26904A50B0DD4E776ED4C8410C78F48166413DB8	executable
4060	ushata.exe	C:\Users\admin\AppData\Roaming\Surge\ushata **MD5:** F2F11E06867B49C26A34094311A12F29 **SHA256:** 7336147234C2767E912BBE76AA8ADD40D4E47E5A6407C9FFE4D7A9B3EEF03DDF	binary
2376	migwiz.exe	C:\Users\admin\AppData\Roaming\Surge\ushata.exe **MD5:** E26D04CECD6C7C71CFBB3F335875BC31 **SHA256:** 902D771612EDECC03757B289A6FE94CD18F2C88C0FC64F93F8AC449502E4EC52	executable
1328	bookworm_kasp.exe	C:\Users\admin\AppData\Local\Temp\RarSFX0\ushata.exe **MD5:** E26D04CECD6C7C71CFBB3F335875BC31 **SHA256:** 902D771612EDECC03757B289A6FE94CD18F2C88C0FC64F93F8AC449502E4EC52	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	0	3	0

HTTP requests

No HTTP requests

Connections

No data

DNS requests

Domain	IP	Reputation
news.nhknews.hk	—	unknown

Threats

No threats detected

Debug output strings

No debug info