



General Info

File name:	srlldcyj.exe
Full analysis:	https://app.any.run/tasks/3d3a7ba1-e2b9-4879-8559-170b9439f79e
Verdict:	Malicious activity
Analysis date:	April 06, 2020 at 12:54:58
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
MD5:	FE36FB1073E6F8FA14D7250501A29AAF
SHA1:	6C7E01278362797DABCF3E666B68227CB9AF10F
SHA256:	F34E5AF97CCB3574F7D5343246138DAF979BFD1F9C37590E9A41F6420ddb3BB6
SSDEEP:	3072:nr6W2wlcju6lIXINPQmTh907Y6IP/8qkrHKl:r6gl4u6lXnxh65QN

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)

Behavior activities

MALICIOUS

Writes to a start menu file
iexplore.exe (PID: 2252)

RAMNIT was detected
iexplore.exe (PID: 2252)

Connects to CnC server
iexplore.exe (PID: 2252)

Changes the login/logoff helper path in the registry
iexplore.exe (PID: 2252)

SUSPICIOUS

Starts Internet Explorer
srildcyj.exe.scr (PID: 3088)

Creates files in the program directory
iexplore.exe (PID: 2252)

INFO

Creates files in the user directory
iexplore.exe (PID: 2252)

Static information

TRiD

.scr | Windows screen saver (46.4)

.dll | Win32 Dynamic Link Library (generic) (23.3)

.exe | Win32 Executable (generic) (15.9)

.exe | Generic Win/DOS Executable (7.1)

.exe | DOS Executable Generic (7)

EXIF

EXE

MachineType: Intel 386 or later, and compatibles

TimeStamp: 2011:02:03 13:18:25+01:00

PEType: PE32

LinkerVersion: 8

CodeSize: 2048

InitializedDataSize: 104960

UninitializedDataSize: 0

EntryPoint: 0x1100

OSVersion: 4

ImageVersion: 0

SubsystemVersion: 4

Subsystem: Windows GUI

FileVersionNumber: 7.6.0.59

ProductVersionNumber: 7.6.0.59

FileFlagsMask: 0x0000

FileFlags: (none)

FileOS: Windows NT 32-bit

ObjectFileType: Dynamic link library

FileSubtype: 0

LanguageCode: Neutral

CharacterSet: Unicode

Comments:

CompanyName: Avira GmbH

FileDescription: AntiVir Command Line Scanner for Windows

FileVersion: 7.6.0.59

InternalName: AntiVir/Win32

LegalCopyright: Copyright © 2007 Avira GmbH. All rights reserved.

LegalTrademarks: AntiVir® is a registered trademark of Avira GmbH, Germany

OriginalFileName:

PrivateBuild:

ProductName:

ProductVersion: 7.6.0.59

SpecialBuild:

Summary

Architecture: IMAGE_FILE_MACHINE_I386

Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	03-Feb-2011 12:18:25
Detected languages:	English - United States
Comments:	
CompanyName:	Avira GmbH
FileDescription:	AntiVir Command Line Scanner for Windows
FileVersion:	7.6.0.59
InternalName:	AntiVir/Win32
LegalCopyright:	Copyright © 2007 Avira GmbH. All rights reserved.
LegalTrademarks:	AntiVir® is a registered trademark of Avira GmbH, Germany
OriginalFilename:	
PrivateBuild:	
ProductName:	
ProductVersion:	7.6.0.59
SpecialBuild:	

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:	0x000000D8

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	5
Time date stamp:	03-Feb-2011 12:18:25
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
.text	0x00001000	0x000006D6	0x00000800	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	5.62622
.rdata	0x00002000	0x00000798	0x00000800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.88282
.data	0x00003000	0x00015A38	0x00015C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	6.73095
.rsrc	0x00019000	0x00003400	0x00003400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	6.58803
.reloc	0x0001D000	0x0000D000	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	2.88659

Resources

Title	Entropy	Size	Codepage	Language	Type
1	3.42776	1020	UNKNOWN	English - United States	RT_VERSION
2	5.93872	3240	UNKNOWN	English - United States	RT_ICON
3	5.29481	872	UNKNOWN	English - United States	RT_ICON
MANIFEST	5.00532	360	UNKNOWN	English - United States	RT_MANIFEST

Imports

ADVAPI32.dll
GDI32.dll
KERNEL32.dll
USER32.dll
comdlg32.dll
ole32.dll

Video and screenshots

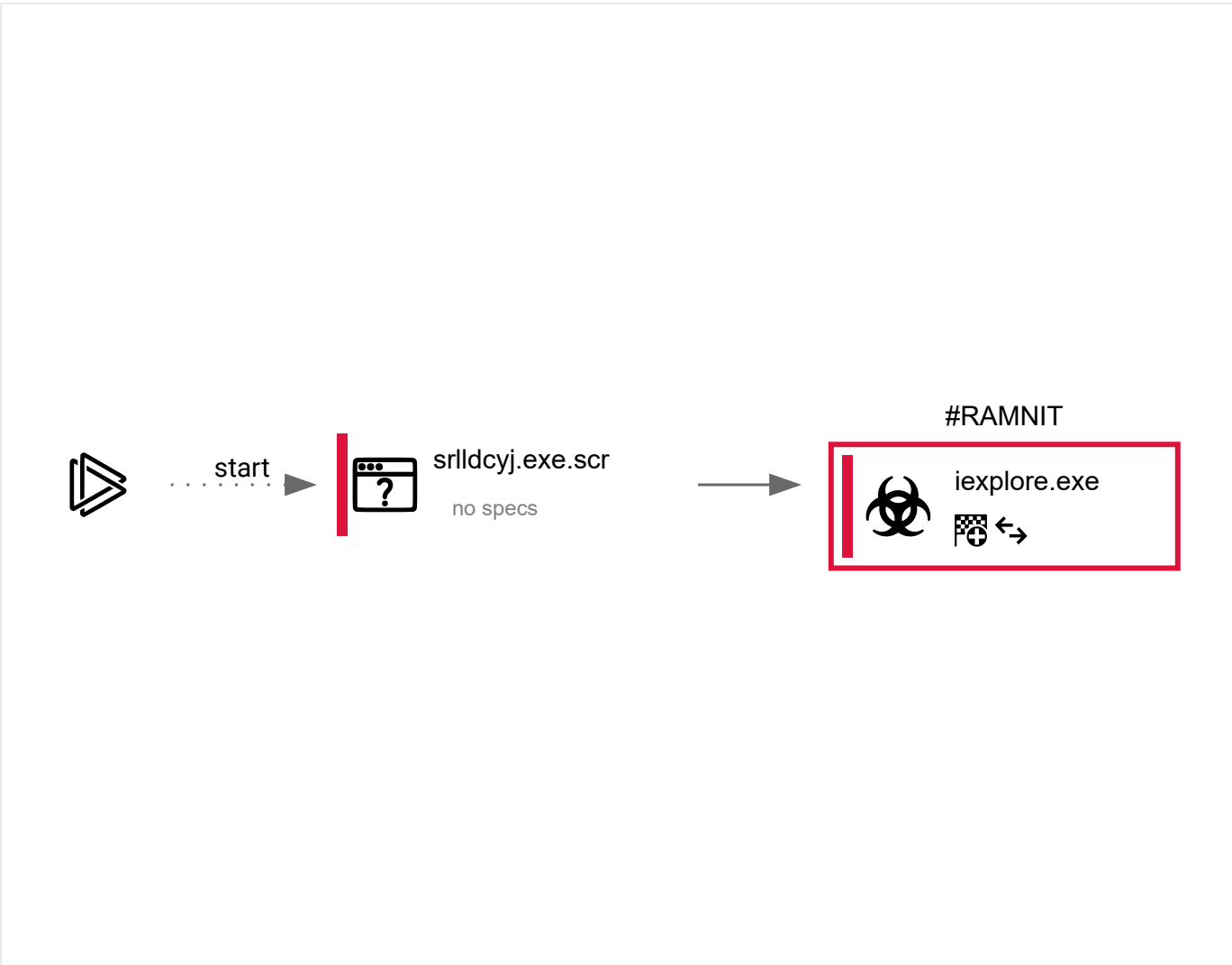




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
36	2	2	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															
3088	"C:\Users\admin\AppData\Local\Temp\srlldcyj.exe.scr" /S	C:\Users\admin\AppData\Local\Temp\srlldcyj.exe.scr	—	explorer.exe															
<div>Information</div> <table><tr><td>User:</td><td>admin</td><td>Company:</td><td colspan="2">Avira GmbH</td></tr><tr><td>Integrity Level:</td><td>MEDIUM</td><td>Description:</td><td colspan="2">AntiVir Command Line Scanner for Windows</td></tr><tr><td>Exit code:</td><td>0</td><td>Version:</td><td colspan="2">7.6.0.59</td></tr></table>					User:	admin	Company:	Avira GmbH		Integrity Level:	MEDIUM	Description:	AntiVir Command Line Scanner for Windows		Exit code:	0	Version:	7.6.0.59	
User:	admin	Company:	Avira GmbH																
Integrity Level:	MEDIUM	Description:	AntiVir Command Line Scanner for Windows																
Exit code:	0	Version:	7.6.0.59																

2252	"C:\Program Files\Internet Explorer\iexplore.exe"	C:\Program Files\Internet Explorer\iexplore.exe		srlldcyj.exe.scr
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	59	0

Modification events

(PID) Process:	(2252) iexplore.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Operation:	write	Name:	Userinit
Value:	C:\Windows\system32\userinit.exe,C:\Program Files\vkjsglxp\enbfqohg.exe		

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	0	22

Dropped files

PID	Process	Filename	Type
3088	srlldcyj.exe.scr	C:\Users\admin\AppData\Local\Temp\~TME037.tmp MD5: — SHA256: —	—
3088	srlldcyj.exe.scr	C:\Users\admin\AppData\Local\Temp\~TME057.tmp MD5: — SHA256: —	—
2252	iexplore.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\enbfqohg.exe MD5: — SHA256: —	—
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Leggimi.htm MD5: 1AA38D80A5AE3C44DD12A901859CE1E2 SHA256: 96C0DBD497364493DF1505752DE74035DFE9A35CEA303E2415E3C8FD83DAC6DE	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Berime.htm MD5: 434C1912B36D995CD0F47914A371A350 SHA256: 29BEDF4D5432634194B9760DEC0C305F0C30BD9EC5C767835149A3A264810F19	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LeiaMe.htm MD5: 1BAE50A84A0F2DFF5EDA04EE97D836FB SHA256: 483667290AF1113C7D86EE38230CFF6B1E06F24384EBA895F8BCA7B81933A143	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LeesMij.htm MD5: CD354D9940E53E6E8B5549D66E821EB4 SHA256: BEBC1CCD4A2C3999E80BA86285F70FBC015FFA903127804D5267CF63CFD814B	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Benioku.htm MD5: 5C0870892881CEFA70F2BFFAC962245A SHA256: 10E14CF2AC1E9708E57456A2A846C2DAA2334C1C7D042C2D21355CD7EA0C9D3E	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\IrakHau.htm MD5: 92523DDC2C89B3119D4E6612830ACACE SHA256: 0E0E248F6722257588370E0B912C61DA6744995546458CCC5CD3D9FA7DC3C986	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Leame.htm MD5: 0ECC849D2905AC8BEC76F6DAB88A77A1 SHA256: 53F6BE8BB207BA55FC0794457A01CFC45673C17DF436D31F0DBE23F1A428DBE3	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Liesmich.htm MD5: 27C78E559F91D00E5A5CB9677746E191 SHA256: 0C00FD502E80110FB2EB4B2B1DFDB093468F9BE0174BA11C81C7F17D86411C8B	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\LueMinut.htm MD5: E6B4397F5643A45B38E35C20CEFBDECB SHA256: F0F4C5311C8DD3AEDB83AD5FA32203B73233FCC245991168EF1F926C4F1917EE5	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Lisezmoi.htm MD5: C8E2889C230589D3BE97B7CC4C72226 SHA256: A22185F80A40512652051B3AC07701AD013438EFEE75D275C7D856DECBFE7B3	html
2252	iexplore.exe	C:\Users\admin\AppData\Local\VirtualStore\Program Files\Adobe\Acrobat Reader DC\Legiu-me.htm MD5: 60AC600D8A43B18F6B0F389A01988538 SHA256: C0886992833E336C1659C334A23C209DA93F478CB73EEA2957599900AB1E134B	html

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
------------------	---------------------	--------------	---------

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2252	iexplore.exe	172.217.23.174:80	google.com	Google Inc.	US	<div>whitelisted</div>
2252	iexplore.exe	3.229.157.246:443	promoliks.com	—	US	<div>malicious</div>

DNS requests

Domain	IP	Reputation
google.com	172.217.23.174	<div>whitelisted</div>
stromoliks.com	0.0.0.0	<div>malicious</div>
promoliks.com	3.229.157.246	<div>malicious</div>

Threats

PID	Process	Class	Message
2252	iexplore.exe	<div>A Network Trojan was detected</div>	ET TROJAN Win32/Ramnit Checkin
2252	iexplore.exe	<div>A Network Trojan was detected</div>	MALWARE [PTsecurity] Win32/Ramnit Checkin
2252	iexplore.exe	<div>A Network Trojan was detected</div>	ET TROJAN Win32/Ramnit Checkin
2252	iexplore.exe	<div>A Network Trojan was detected</div>	MALWARE [PTsecurity] Win32/Ramnit Checkin
2252	iexplore.exe	<div>A Network Trojan was detected</div>	MALWARE [PTsecurity] Banker Ramnit CnC Connection

Debug output strings

No debug info