




General Info

File name: 1.bn
Full analysis: <https://app.any.run/tasks/73bc4068-11ee-4cae-a044-1fac7531caec>
Verdict: Malicious activity
Analysis date: August 22, 2022 at 18:52:58
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: trojan ransomware stop
Indicators: 
MIME: application/x-dosexec
File info: PE32 executable (GUI) Intel 80386, for MS Windows
MD5: B6C2D9032C0FB47F5D74220CD4616BBE
SHA1: 4383F04F1FF2353966053AA326930696206B777
SHA256: 98D0A83C9EABF2F3E31AF3E8934B9316E1D3FCB501FFC4B4E567A87F623A0896
SSDEEP: 24576:SxULYaRd5Ux7Ux7NBhqr1dPAkapBXjGP/Dqq:Sud5Ux7ar1xSptGpN

Software environment set and analysis options

Launch configuration

Task duration:	180 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	120 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

Internet Explorer 11.0.9600.19596 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)	KB3161102
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)	KB3161949
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)	KB3170735
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)	KB3172605
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)	KB3179573
Mozilla Firefox 83.0 (x86 en-US) (83.0)	KB3184143
Mozilla Maintenance Service (83.0.0.7621)	KB3185319
Notepad++ (32-bit x86) (7.9.1)	KB4019990
Opera 12.15 (12.15.1748)	KB4040980
QGA (2.14.33)	KB4474419
Skype version 8.29 (8.29)	KB4490628
VLC media player (3.0.11)	KB4524752
WinRAR 5.91 (32-bit) (5.91.0)	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	SUSPICIOUS	INFO
Changes settings of System certificates <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 1188)</div>	Reads the computer name <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 1188)</div> <div>1.bin.exe (PID: 3596)</div>	Checks supported languages <div>explorer.exe (PID: 3000)</div> <div>icacls.exe (PID: 3832)</div> <div>mmc.exe (PID: 3584)</div>
Changes the autorun value in the registry <div>1.bin.exe (PID: 1416)</div>	Checks supported languages <div>1.bin.exe (PID: 3324)</div> <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 3116)</div> <div>1.bin.exe (PID: 1292)</div> <div>1.bin.exe (PID: 3596)</div> <div>1.bin.exe (PID: 1188)</div>	Reads the computer name <div>explorer.exe (PID: 3000)</div> <div>icacls.exe (PID: 3832)</div> <div>mmc.exe (PID: 3584)</div>
Drops executable file immediately after starts <div>1.bin.exe (PID: 1416)</div>		Manual execution by user <div>explorer.exe (PID: 3000)</div> <div>mmc.exe (PID: 1968)</div> <div>mmc.exe (PID: 3584)</div>
STOP was detected <div>1.bin.exe (PID: 3596)</div>	Application launched itself <div>1.bin.exe (PID: 3324)</div> <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 3116)</div> <div>1.bin.exe (PID: 1292)</div>	Reads settings of System Certificates <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 3596)</div> <div>1.bin.exe (PID: 1188)</div>
Connects to CnC server <div>1.bin.exe (PID: 3596)</div>	Adds / modifies Windows certificates <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 1188)</div>	Checks Windows Trust Settings <div>1.bin.exe (PID: 1416)</div> <div>1.bin.exe (PID: 1188)</div> <div>1.bin.exe (PID: 3596)</div>
Renames files like Ransomware <div>1.bin.exe (PID: 3596)</div>	Executable content was dropped or overwritten <div>1.bin.exe (PID: 1416)</div>	
	Drops a file with a compile date too recent <div>1.bin.exe (PID: 1416)</div>	
	Executed via Task Scheduler <div>1.bin.exe (PID: 1292)</div>	

Static information

TRiD

.exe		Win32 Executable MS Visual C++ (generic) (52.5)
.scr		Windows screen saver (22)
.dll		Win32 Dynamic Link Library (generic) (11)
.exe		Win32 Executable (generic) (7.5)
.exe		Generic Win/DOS Executable (3.3)

EXIF

EXE	
FileSubtype:	0
ObjectFileType:	Executable application
FileOS:	Windows NT 32-bit
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	71.0.0.0
FileVersionNumber:	66.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	5
ImageVersion:	0
OSVersion:	5
EntryPoint:	0xa400
UninitializedDataSize:	0
InitializedDataSize:	4844544
CodeSize:	180736
LinkerVersion:	9
PEType:	PE32
TimeStamp:	2021:09:26 10:36:54+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	26-Sep-2021 08:36:54
Detected languages:	Korean - Korea
Debug artifacts:	C:\sumoce-sisapefun.pdb

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:	3
Time date stamp:	26-Sep-2021 08:36:54
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	0x0002C05C	0x0002C200	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.0792
.data	0x0002E000	0x00493708	0x00092C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.99178
.rsrc	0x004C2000	0x00004B60	0x00004C00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	4.95817

Resources

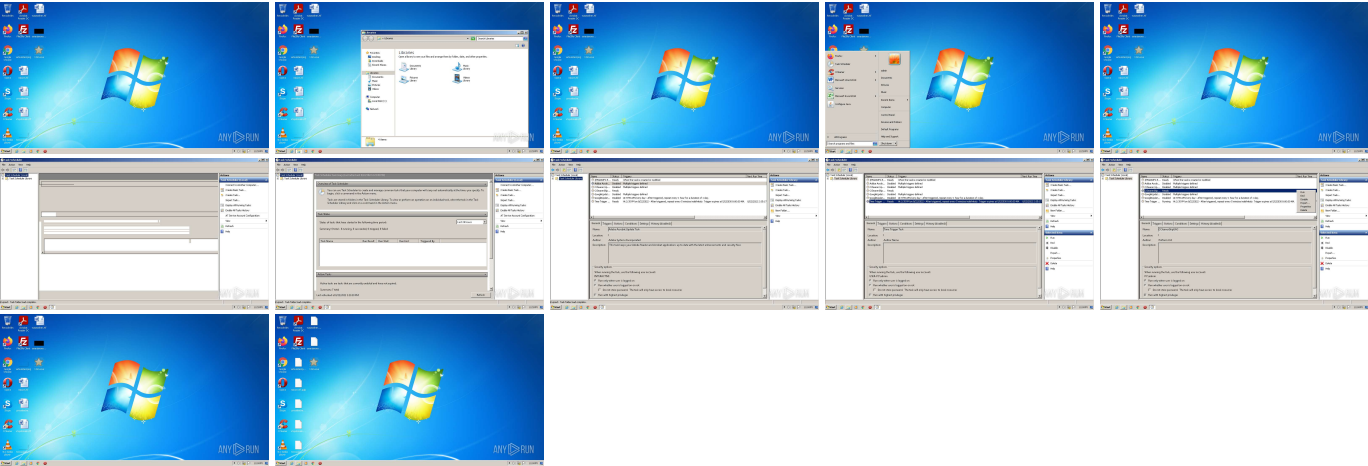
Title	Entropy	Size	Codepage	Language	Type
1	5.7051	1736	UNKNOWN	Korean - Korea	RT_ICON
2	5.97589	1384	UNKNOWN	Korean - Korea	RT_ICON
3	5.6609	4264	UNKNOWN	Korean - Korea	RT_ICON
4	5.79004	2440	UNKNOWN	Korean - Korea	RT_ICON
5	6.21854	1128	UNKNOWN	Korean - Korea	RT_ICON

6	4.09164	304	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.5416	304	UNKNOWN	UNKNOWN	RT_CURSOR
8	2.50404	240	UNKNOWN	UNKNOWN	RT_CURSOR
9	1.59806	4264	UNKNOWN	UNKNOWN	RT_CURSOR
26	3.01622	330	UNKNOWN	Korean - Korea	RT_STRING
27	3.13643	476	UNKNOWN	Korean - Korea	RT_STRING
28	1.854	68	UNKNOWN	Korean - Korea	RT_STRING
129	2.72482	76	UNKNOWN	Korean - Korea	RT_GROUP_ICON
191	3.04819	88	UNKNOWN	Korean - Korea	RT_ACCELERATOR
429	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
432	2.04644	10	UNKNOWN	Korean - Korea	UNKNOWN
437	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
442	1.84644	10	UNKNOWN	Korean - Korea	UNKNOWN
446	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
453	2.32193	10	UNKNOWN	Korean - Korea	UNKNOWN
456	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
457	1	2	UNKNOWN	UNKNOWN	AFX_DIALOG_LAYOUT
460	3.14856	320	UNKNOWN	UNKNOWN	RT_VERSION
591	3.12537	104	UNKNOWN	Korean - Korea	RT_ACCELERATOR
2371	1.98048	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
2374	2.55787	48	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR

Imports

KERNEL32.dll
USER32.dll

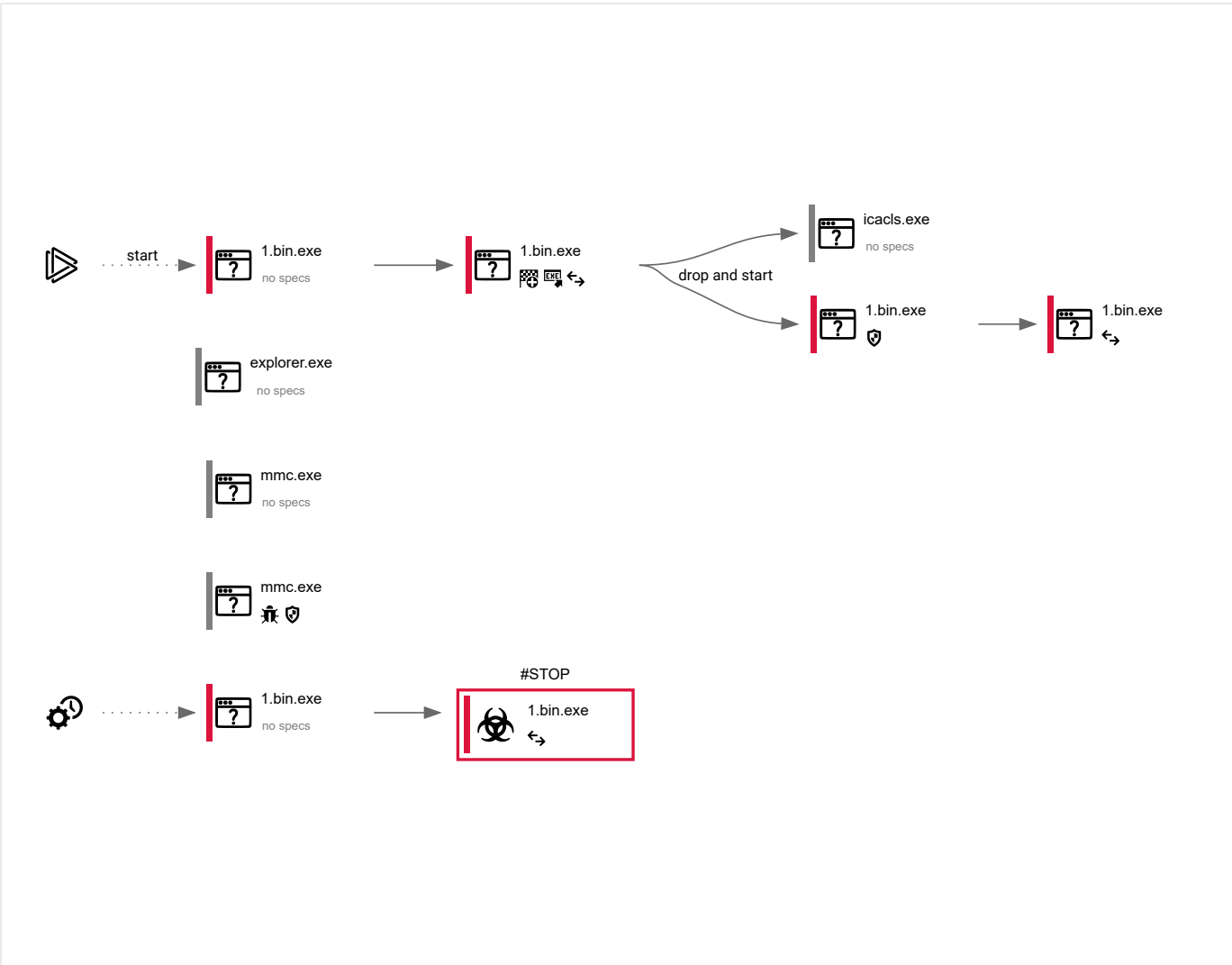
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
55	10	6	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
3324	"C:\Users\admin\Desktop\1.bin.exe"	C:\Users\admin\Desktop\1.bin.exe	—	Explorer.EXE
<div>Information</div> <div><div>User:adminIntegrity Level:MEDIUM</div><div>Exit code:0</div></div>				
1416	"C:\Users\admin\Desktop\1.bin.exe"	C:\Users\admin\Desktop\1.bin.exe		1.bin.exe

<div>Information</div> <div><div>User:adminIntegrity Level:MEDIUMExit code:0</div></div>					
3000	"C:\Windows\explorer.exe"	C:\Windows\explorer.exe	—	Explorer.EXE	
<div>Information</div> <div><div>User:adminCompany:Microsoft CorporationIntegrity Level:MEDIUMDescription:Windows ExplorerExit code:1Version:6.1.7600.16385 (win7_rtm.090713-1255)</div></div>					
3832	icaccls "C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a" /deny *S-1-1-0:(OI)(CI)(DE,DC)	C:\Windows\system32\icaccls.exe	—	1.bin.exe	
<div>Information</div> <div><div>User:adminCompany:Microsoft CorporationIntegrity Level:MEDIUMExit code:0Version:6.1.7600.16385 (win7_rtm.090713-1255)</div></div>					
3116	"C:\Users\admin\Desktop\1.bin.exe" --Admin IsNotAutoStart IsNotTask	C:\Users\admin\Desktop\1.bin.exe		1.bin.exe	
<div>Information</div> <div><div>User:adminIntegrity Level:HIGHExit code:0</div></div>					
1968	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\taskschd.msc" /s	C:\Windows\system32\mmc.exe	—	Explorer.EXE	
<div>Information</div> <div><div>User:adminCompany:Microsoft CorporationIntegrity Level:MEDIUMDescription:Microsoft Management ConsoleExit code:3221226540Version:6.1.7600.16385 (win7_rtm.090713-1255)</div></div>					
3584	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\taskschd.msc" /s	C:\Windows\system32\mmc.exe		Explorer.EXE	
<div>Information</div> <div><div>User:adminCompany:Microsoft CorporationIntegrity Level:HIGHExit code:0Version:6.1.7600.16385 (win7_rtm.090713-1255)</div></div>					
1188	"C:\Users\admin\Desktop\1.bin.exe" --Admin IsNotAutoStart IsNotTask	C:\Users\admin\Desktop\1.bin.exe		1.bin.exe	
<div>Information</div> <div><div>User:adminIntegrity Level:HIGH</div></div>					
1292	C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a\1.bin.exe --Task	C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a\1.bin.exe	—	taskeng.exe	
<div>Information</div> <div><div>User:adminIntegrity Level:MEDIUMExit code:0</div></div>					
3596	C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a\1.bin.exe --Task	C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a\1.bin.exe		1.bin.exe	
<div>Information</div> <div><div>User:adminIntegrity Level:MEDIUMExit code:0</div></div>					

Registry activity

Total events	Read events	Write events	Delete events
12 386	12 211	167	8

Modification events

(PID) Process:	(1416) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation:	write	Name:	ProxyEnable
Value:	0		

https://any.run/report/98d0a83c9eabf2f3e31af3e8934b9316e1d3fcb501ffc4b4e567a87f623a8096/73bc4068-11ee-4cae-a044-1fac7531caec?_gl... 9/21

EDF53000000010000004300000030413022060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C030100000002050000308205D5E308203C6A003020102021001FD6D30FCA3CA51A81BBC40E35032D300D06092A864886F7D0D1010C0500308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA465727365792043697479311E301C060355040A131554685205553455255345204E6574776F726B312E302C06035504031325555345525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D3338303131383233353935A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA465727365792043697479311E301C060355040A13155468520553455255345204E6574776F726B312E302C06035504031325555345525472757374205253412043657274696669636174696F6E20417574686F726974793082022230D06092A864886F7D0D1010500038202F00308202A028202010080126517360EC3DB08B3D0AC570D76EDC2D734CAD508361E2AA240D29D6409DCC8E99FCC3DA9EC6FC1DCF1D3B1D67B3728112B47DA39C6B3CA19845FA6BD7D9DA363428B67F629A382B91F8E26FD0EC16209003CE5E2874CA918B491D46264DB7FA306F188186A90223CBCE1F3087147BF6E41F8ED4E451C6176460851CB8614543BC33FE7E6C9FF169D18BD518E35A6A766C8726BD2166B1D94B7803C0583A8CCFC0DCBC9E4CFAE0596351F57A87FFCE93DB72CB6F654DDC8E71234ADAE4C8A875C9AB487203DCA7F223AAE7E3B866014AE701E46539B3360F794B8E5337907343F332C353EFDBAAEF744E69C76B8C6093DEAC70CDFE132AECC933B517895678BE3056FE0D169390F1B0FF32566B336DF6E47FA7343E57E0EA566B1297C3284635589C40DC19354301913ACD37D37A7EB5D3A6C355CDB41D712DAA9490BDFD880A0993628E5B66CF2588DC48B8B134F64390FD9029EBB124C957CF36B05A951683CCB867E2E8139DC358B2D3C3B93CDEB5FFDEE57AC2332800B0BF355740949D849581A7F9236E51920FEF3267D1C417BC9CE4326D0BF415F40A94444F499E757879E501F5754A836FD74632F1A5605096E58422E431AACB4AD0254759FA041E93042664A5081B2DEBE78B7FC615E1C957841E0F63D6E9628A065552EAE5CC628084253980E2BA9F24C971C073D0657FEDEF2F820F20310001A3420340301D0603551D0E041604145379BF5AAAB24ACF5480E1D89BC09DFB220366C3B00E603551D0F101FF0403020106300F0603551D103101FF040530030101FF300D06092A864886F7D0D1010C05003820201005CD47C0CDFC7F017D4199650C73C5529FCBF8CF990671BDA43159F9E0255579614F1523C27879428ED1F3A07137A276C3D080C49BC66B4EBA8291F36915D8BC88E3CA4A0BFDEFA8E948552A0620605578291EEC5F5048C4B241155FF249A6AE5E2ABEE0AD977FF70138941495430709F60A9EE1CAB128CA09A5EA7986A596D8B83F08FBC8D145AF1815649012D73282EC5E2244FC58ECF0F445FE22B3E2BF8ED2D9456105C1976FA876728F88BC36AFBFD05CE218DE6A66F1F6CA67162C5D8D083720CF1671890C9C134C7234DFBCD571DFAA71DDE1B96C8C3125D65DABD5712B6436BFFE5DEAD661151CF99AEEC1786E871918CDE49DD103571A21527941CCF61E326B86A636725215DE6DD1D0B2E6813B882AEFC836785D4985714B1B9998089FF7F78195C794A602E9240AEC372A2CC9262C80E5DF7365BCAE1552501B4D01A079C77003FDD0CD5EC3DDFA926667FA92DDF8902F7F5979A8539ADAC367B0874AA9289238FF5C276BE1B04FF3077EE002ED45987CB524195EAF4470E6441557C8050295D629DC2B9EEA5287484A59B790C70C07DFF589367432D628C1B0B00BE09CAC331CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7BB57088AE3E19CF4028D8FCC890295D629DC2B9EEA5287484A59B790C70C07DFF589367432D628C1B0B00BE09CAC331CD6FCE369B54746812FA282ABD3634470C48DFF2D33BAAD8F7BB57088AE3E19CF4028D8FCC890BB5D9922F552E658C51F883143EE881DD7C68E3C436A1DA718DE7D3D16F162F9CA90A8FD

(PID) Process:	(1416) 1.bin.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DDA B9AD8E
Operation:	delete key	Name:	(default)
Value:			
(PID) Process:	(1416) 1.bin.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\2B8F1B57330DBBA2D07A6C51F70EE90DDA B9AD8E
Operation:	write	Name:	Blob
Value:	5C00000001000000040000000100000090000000100000054000000305206082B0601050507030206082B06010505070303060A2B060104018237A0A30406082B0601050507030406082B0601050507030706082B0601050507030106082B060105050703080F000000010000003000000006B764A96581128168CF20B8374DA479D543E1F32457FA4EE0DBD2A6C8D171D531289E1CD22BFDBBD4CFD9796254830300000001000000140000002B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E0B0000000100000003000740069070060F0000001D0000000100000001000000088501358D29A3BF059B028559CF95F901400000001000000140000005379BF5AAA2B4ACF5480E1D89BC09DFB2B0366CB62000000010000002000000079939B02FD8AA13E21C31228ACB08119643B749C89864B1746D46C3D4CDB2190000000100000010000000EA6089055218053DD01E37E1D806EEDF53000000010000004300000304013022060C2B06010401B231010201050130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C03010000002050000308205D5E308203C6A003020102021001FD6D30FCA3CA51A81BBC640E35032D300D06092A864886F7D0D1010C0500308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A13155468652055345525452553452554204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A6572736579311430120603550407130BA4A65727365792043697479311E301C060355040A1315546865205534552545255534204E6574776F726B312E302C060355040313255534525472757374205253412043657274696669636174696F6E20417574686F72697479301E170D31303032303130303030305A170D333830303131383233353935395A308188310B3009060355040613025553311330110603550408130AAE6577204A657273657931143012		

<https://any.run/report/98d0a83c9eabf2f3e31af3e8934b9316e1d3fcb501ffc4b4e567a87f623a8096/73bc4068-11ee-4cae-a044-1fac7531caec?> g... 11/21

https://any.run/report/98d0a83c9eabf2f3e31af3e8934b9316e1d3fcb501ffc4b4e567a87f623a8096/73bc4068-11ee-4cae-a044-1fac7531caec?_... 13/21

Operation:	write	Name:	WpadDecisionReason
Value:	1		
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadDecisionTime
Value:	EE12AA762AB6D801		
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadDecision
Value:	0		
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadNetworkName
Value:	Network 3		
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	Name:	WpadDecisionTime
Value:	EE12AA762AB6D801		
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	delete value	Name:	WpadDetectedUrl
Value:			
(PID) Process:	(3596) 1.bin.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation:	write	Name:	LanguageList
Value:	en-US		
(PID) Process:	(3584) mmc.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Microsoft Management Console\Recent File List
Operation:	delete key	Name:	(default)
Value:			
(PID) Process:	(3584) mmc.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Microsoft Management Console\Recent File List
Operation:	write	Name:	File1
Value:	C:\Windows\system32\taskschd.msc		
(PID) Process:	(3584) mmc.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Microsoft Management Console\Recent File List
Operation:	write	Name:	File2
Value:	C:\Windows\system32\devmgmt.msc		
(PID) Process:	(3584) mmc.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Microsoft Management Console\Recent File List
Operation:	write	Name:	File3
Value:	C:\Windows\System32\services.msc		
(PID) Process:	(3584) mmc.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Microsoft Management Console\Recent File List
Operation:	write	Name:	File4
Value:	C:\Windows\system32\certmgr.msc		

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	48	77	11

Dropped files

PID	Process	Filename	Type
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 MD5: F7DCB24540769805E5BB30D193944DCE SHA256: 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB06228BC7A711E MD5: 8FDE325C0191758029AD06C16C6A173C SHA256: 15DA0C6D8DFD5D43C6834B944BEDE7920E440262612282F52B8F4BA878F43E24	der
1416	1.bin.exe	C:\Users\admin\AppData\Local\93f5b533-2857-4773-9483-54d3a623603a\1.bin.exe MD5: B6C2D9032C0FB47F5D74220CD4616BBE SHA256: 98D0A83C9EABF2F3E31AF3E8934B9316E1D3FCB501FFC4B4E567A87F623A8096	executable
3596	1.bin.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGX7LP\get[1].htm MD5: 7CE95DFF5FE26732B150EBC63EE79E21 SHA256: 325CBEA00CF9608E45C169109200341A2E12FBA8BC4AE8B6B2B170B07C31993F	binary
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D MD5: 3D4C1DE1F149182348CBDC85F4801C13 SHA256: 094E9CB02BEBB5D8A5BFBEOE83D3C0064D0F0EA3F4ECCE0215FDCBDA9FAB938	der
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D MD5: FF9F4B8F5480C240AC658D807D5DAE86 SHA256: 0051306F5A672355D56E860D8BF01BDAD3891162ABFFFC2457D0170C590A38B6	binary

3596	1.bin.exe	C:\Users\admin\AppData\Local\bowsakkestx.txt	binary
		MD5: 7CE95DFF5FE26732B150EBC63EE79E21	SHA256: 325CBEA00CF9608E45C169109200341A2E12FBA8BC4AE8B6B2B170B07C31993F
1188	1.bin.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\geo[1].json	binary
		MD5: AA09DD4B19ADB545B761FE02BCCA3BAC	SHA256: B42B22FD077DBB8146F597D5368A53B77EDBDFDC8DF8099C26395E18AD0F0BE
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E	binary
		MD5: A036BDBF79B78EEDB7EA0BF5B7B83B44	SHA256: A4DA6693BECC06DE1E5679DE7AB00CCA66C23B8C98F3B903B1994F88DC38653C
1416	1.bin.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\78RFYB7Z\geo[1].json	binary
		MD5: AA09DD4B19ADB545B761FE02BCCA3BAC	SHA256: B42B22FD077DBB8146F597D5368A53B77EDBDFDC8DF8099C26395E18AD0F0BE
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	binary
		MD5: 5AFFEB5027826727429414F827D7366	SHA256: 72BED33E988344815BA311EF9BD2DD728CA60BD7A0A106D1698F718AA364DC98
3596	1.bin.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B6QGXX7LP\geo[1].json	binary
		MD5: AA09DD4B19ADB545B761FE02BCCA3BAC	SHA256: B42B22FD077DBB8146F597D5368A53B77EDBDFDC8DF8099C26395E18AD0F0BE
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3538626A1FCCCA43C7E18F220BDD9B02	der
		MD5: 42439D7D234F28635712EE284AEC864C	SHA256: A6AF95E83C8EE1F135ACB0DD5FA9CDB240836DF89F0A51B510FB3A2672BE1D54
1416	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3538626A1FCCCA43C7E18F220BDD9B02	binary
		MD5: 33FCFA2A8EC69879C064A255A9DF7200	SHA256: 48309F3A7C6C55A1170AE745B146CD1F591A46765F0BF488B63E0F1B0E752639
3584	mmc.exe	C:\Users\admin\AppData\Roaming\Microsoft\MMC\taskschd	xml
		MD5: C1B8BDB46FA1AE18055D9E78A27C6F8	SHA256: 307F30E8C3AAA8F565C3A022309984BF56E66B430102FB52432B984CDC109517
3596	1.bin.exe	C:\Users\admin\oracle_jre_usage\90737d32e3abaa4.timestamp	binary
		MD5: 45D6750BB4FF6A24BDF6EDBED3278FCE	SHA256: CAC9AD592A17EF071E59D93F496CD92CCBFAD767DCDFBC6F8907A51EEB219570
3596	1.bin.exe	C:\Users\admin\AppData\Local\VirtualStore_readme.txt	text
		MD5: 5D4C6832C6E22BB93D08D5972206710A	SHA256: 1C1129990E813AEF83C66F4B34A1AB41C54566683CA7D05F78D1F44F048CAD31
3596	1.bin.exe	C:\Users\admin\Contacts\admin.contact.qqlo	xml
		MD5: 50AD46459FC2FF1C6C4F335DB875B1EE	SHA256: C819E6E433AF1A97E0DA76F4021F148E7ADCF5312141F9A2073B13F9D9DD3986
3596	1.bin.exe	C:\Users\admin_readme.txt	text
		MD5: 5D4C6832C6E22BB93D08D5972206710A	SHA256: 1C1129990E813AEF83C66F4B34A1AB41C54566683CA7D05F78D1F44F048CAD31
3596	1.bin.exe	C:\SystemID\PersonalID.txt	text
		MD5: 9AB2AE58D5B67D3D677EDF588C748E6A	SHA256: 38A7BE8D23B1BE751B49FA119956683E7F555ED8AEB4AF56AAC3F486E4EA4E0
3596	1.bin.exe	C:\Users\admin\oracle_jre_usage\90737d32e3abaa4.timestamp.qqlo	binary
		MD5: 45D6750BB4FF6A24BDF6EDBED3278FCE	SHA256: CAC9AD592A17EF071E59D93F496CD92CCBFAD767DCDFBC6F8907A51EEB219570
3596	1.bin.exe	C:\Users\admin\Contacts\admin.contact	xml
		MD5: 50AD46459FC2FF1C6C4F335DB875B1EE	SHA256: C819E6E433AF1A97E0DA76F4021F148E7ADCF5312141F9A2073B13F9D9DD3986
3596	1.bin.exe	C:\Users\admin\Desktop\artsunited.png	binary
		MD5: DEC245647E56158D74F98E4E5F2BD73D	SHA256: EC92F42C803DA18CF059008F1B1302FCCDF60D4946609128BD3A4F302F4A5241
3596	1.bin.exe	C:\Users\admin\Documents\abovereason.rtf	text
		MD5: 37F9B6C85248F0EB43DCF29738810716	SHA256: 4718C6793201FF5D2A5E36BE549D5E325956EA8D231D3FC01D1055F2565921AB
3596	1.bin.exe	C:\Users\admin\Desktop\yearsjersey.jpg.qqlo	image
		MD5: 22B4046689E668CC733DB2208D2FEBCEB	SHA256: 1BE6AFD3C17A54809ADD832909794012D26C355BD77F08C9BE04C530CDC33500
3596	1.bin.exe	C:\Users\admin\Desktop\presidentreport.rtf.qqlo	text
		MD5: F60FB56D3B98AE18CDB7AFDB101006C5	SHA256: 52CE01CE6DBE5EE3B9132F63A494CC97456B88FEFB0BC640249C26543A49F0C2
3596	1.bin.exe	C:\Users\admin\Desktop\stopdomain.rtf	text
		MD5: D3E20CB8779E9ED8DACBC9C8D0ACD6D9	SHA256: CC14CDCE38FA656813505703F7413AB739C16F03DCBE7FB6052794FACC775DF
3596	1.bin.exe	C:\Users\admin\Desktop\termssport.png.qqlo	binary
		MD5: 5162482992DAD896A4CDC634C7D0F65D	SHA256: 22823E1A0F23D501DCEE205430F4776A4534A4F5AA2F701F12FC8F124105714E
3596	1.bin.exe	C:\Users\admin\Documents\forumopen.rtf	text
		MD5: 1DA4964D9285F92348FEFA01AB62268D	SHA256: 69B1073764D95A97939491D36D94B67901BD9E51BA8E36A02BA2B7536EF559CB
3596	1.bin.exe	C:\Users\admin\Documents\positiveprior.rtf	text
		MD5: 873D722D67348FA111BCB46A4FB1FA28	SHA256: C3365DDDA7C185B8EDA8909E468A6A06000CFD0264C81FEFA79EEFA27208251
3596	1.bin.exe	C:\Users\admin\Desktop\wasmother.rtf	text
		MD5: 538A680209D13DBDEE1ED9F424CB2C91	SHA256: BA1EFF079D408014B32B031FB69252674F0849EB5C5E4F65721B43BEF517421F
3596	1.bin.exe	C:\Users\admin\Desktop\artsunited.png.qqlo	binary
		MD5: DEC245647E56158D74F98E4E5F2BD73D	SHA256: EC92F42C803DA18CF059008F1B1302FCCDF60D4946609128BD3A4F302F4A5241
3596	1.bin.exe	C:\Users\admin\Desktop\ystore.rtf.qqlo	text
		MD5: F18B3A8C840432E7210EA98AB771C436	SHA256: FA35E0762F61B5068496E3B6423B62BBBF22B1C4E2F97028FFC15C08E382DD8
3596	1.bin.exe	C:\Users\admin\Desktop\stopdomain.rtf.qqlo	text
		MD5: D3E20CB8779E9ED8DACBC9C8D0ACD6D9	SHA256: CC14CDCE38FA656813505703F7413AB739C16F03DCBE7FB6052794FACC775DF
3596	1.bin.exe	C:\Users\admin\Desktop\yearsjersey.jpg	

			MD5: 22B4046689E668CC733DB2208D2FEBCB	SHA256: 1BE6AFD3C17A54809ADD832909794012D26C355BD77F08C9BE04C530CDC33500	image
3596	1.bin.exe	C:\Users\admin\Documents\forumopen.rtf.qqlo	MD5: 1DA4964D9285F92348FEFA01AB62268D	SHA256: 69B1073764D95A97939491D36D94B67901BD9E51BA8E36A02BA2B7536EF559CB	text
3596	1.bin.exe	C:\Users\admin\Documents\abovereason.rtf.qqlo	MD5: 37F9B6C85248F0EB43DCF29738810716	SHA256: 4718C6793201FF5D2A5E36BE549D5E325956EA8D231D3FC01D1055F2565921AB	text
3596	1.bin.exe	C:\Users\admin\Desktop\presidentreport.rtf	MD5: F60FB56D3B98AE18CDB7AFDB101006C5	SHA256: 52CE01CE6DBE5EE3B9132F63A494CC97456B88FEFB0BC640249C26543A49F0C2	text
3596	1.bin.exe	C:\Users\admin\Desktop\instore.rtf	MD5: F18B3A8C840432E7210EA98AB771C436	SHA256: FA35E0762F61B5068496E3B6423B62BBBF22B1C4E2F97028FFC15C08E382DD8	text
3596	1.bin.exe	C:\Users\admin\Desktop\termssport.png	MD5: 5162482992DAD896A4CDC634C7D0F65D	SHA256: 22823E1A0F23D501DCEE205430F4776A4534A4F5AA2F701F12FC8F124105714E	binary
3596	1.bin.exe	C:\Users\admin\Documents\positiveprior.rtf.qqlo	MD5: 873D722D67348FA111BCB46A4FB1FA28	SHA256: C3365DDA7C185B8EDA8909E468A6A06000C7FD0264C81FEFA79EEFA27208251	text
3596	1.bin.exe	C:\Users\admin\Desktop\wasmother.rtf.qqlo	MD5: 538A680209D13DBDEE1ED9F4242BC91	SHA256: BA1EFF079D408014B32B031FB69252674F0849EB5C5E4F65721B43BEF517421F	text
3596	1.bin.exe	C:\Users\admin\Documents\willways.rtf	MD5: B682786BEFA0860121E484FDD6F1150D	SHA256: D9B365B7D4F5F4654DC315C0CBC55E4BA1015709572129D888D8B32658F0111	text
3596	1.bin.exe	C:\Users\admin\Downloads\actcareer.jpg	MD5: BB9A15571D6DA9CF4D90DF02B039A54D	SHA256: 4FA4725EC53CE60FEF4EB70A632772E00BB5D6503BA1DB9FE573319C84B3003A	image
3596	1.bin.exe	C:\Users\admin\Documents\presentedoptions.rtf	MD5: A77EC9509780C3276FD1111D6BB78E53	SHA256: 62634D830D9622EACAF7DE0EFC268BEF36E2510DCB720479B9C231B44742C127	text
3596	1.bin.exe	C:\Users\admin\Downloads\actcareer.jpg.qqlo	MD5: BB9A15571D6DA9CF4D90DF02B039A54D	SHA256: 4FA4725EC53CE60FEF4EB70A632772E00BB5D6503BA1DB9FE573319C84B3003A	image
3596	1.bin.exe	C:\Users\admin\Downloads\dogprofile.jpg	MD5: A2ECE34DE95382FACE612AFE4B7D5EF0	SHA256: CAAEBEE1BE59AFF93EE173141395A9117E46F410E015FBEE21909E019B50FAD0	image
3596	1.bin.exe	C:\Users\admin\Downloads\frenchbritish.png	MD5: FD59D55E8081040DB28D4E06C9C57F26	SHA256: 2C7BCFF6DCD6DE3AABAE27BA1CD23950DA28E90B02374196F9D5CDD79CD9C841	binary
3596	1.bin.exe	C:\Users\admin\Documents\willways.rtf.qqlo	MD5: B682786BEFA0860121E484FDD6F1150D	SHA256: D9B365B7D4F5F4654DC315C0CBC55E4BA1015709572129D888D8B32658F0111	text
3596	1.bin.exe	C:\Users\admin\Documents\presentedoptions.rtf.qqlo	MD5: A77EC9509780C3276FD1111D6BB78E53	SHA256: 62634D830D9622EACAF7DE0EFC268BEF36E2510DCB720479B9C231B44742C127	text
3596	1.bin.exe	C:\Users\admin\Downloads\frenchbritish.png.qqlo	MD5: FD59D55E8081040DB28D4E06C9C57F26	SHA256: 2C7BCFF6DCD6DE3AABAE27BA1CD23950DA28E90B02374196F9D5CDD79CD9C841	binary
3596	1.bin.exe	C:\Users\admin\Downloads\breakteam.jpg.qqlo	MD5: 34B7E79D688480D691DA0110B7A0D1A0	SHA256: FB6629F885E7BB0C686839153357206CC425049D5BE88B544E1A7168F2863C1D	image
3596	1.bin.exe	C:\Users\admin\Downloads\beforeusb.jpg.qqlo	MD5: 2050B366AD36A3F89B7AABE61AAB33EF	SHA256: 3F514DA790649ED129BD071B253D8F0B68E43C402687155674F25F0FF7EACF0A	image
3596	1.bin.exe	C:\Users\admin\Downloads\breakteam.jpg	MD5: 34B7E79D688480D691DA0110B7A0D1A0	SHA256: FB6629F885E7BB0C686839153357206CC425049D5BE88B544E1A7168F2863C1D	image
3596	1.bin.exe	C:\Users\admin\Downloads\beforeusb.jpg	MD5: 2050B366AD36A3F89B7AABE61AAB33EF	SHA256: 3F514DA790649ED129BD071B253D8F0B68E43C402687155674F25F0FF7EACF0A	image
3596	1.bin.exe	C:\Users\admin\Downloads\dogprofile.jpg.qqlo	MD5: A2ECE34DE95382FACE612AFE4B7D5EF0	SHA256: CAAEBEE1BE59AFF93EE173141395A9117E46F410E015FBEE21909E019B50FAD0	image
3596	1.bin.exe	C:\Users\admin\Downloads\maeconomy.jpg	MD5: 26D8416559DE256D2A4F7611689E88AB	SHA256: 597A69A2A98B2E899EA080DE5AF0D2FF5B099475B17A63CAEDD61020C35A1F56	image
3596	1.bin.exe	C:\Users\admin\Downloads\maeconomy.jpg.qqlo	MD5: 26D8416559DE256D2A4F7611689E88AB	SHA256: 597A69A2A98B2E899EA080DE5AF0D2FF5B099475B17A63CAEDD61020C35A1F56	image
3596	1.bin.exe	C:\Users\admin\Downloads\wallsecond.png	MD5: E9E9A44388DF15B212BEBACAC38DE0EBB	SHA256: 08928DD7A582972784ECC21339EEE8778F32656FEF97D301BB8587F4EC490557	binary
3596	1.bin.exe	C:\Users\admin\Downloads\wallsecond.png.qqlo	MD5: E9E9A44388DF15B212BEBACAC38DE0EBB	SHA256: 08928DD7A582972784ECC21339EEE8778F32656FEF97D301BB8587F4EC490557	binary
3596	1.bin.exe	C:\Users\admin\Pictures\angelesfixed.png	MD5: A7CABBC38DBD02453B3C0584E86FCF8D	SHA256: DA35D63941CAA35001129E306DED22261109A13C208B11C35576FCE75CEE1C51	binary
3596	1.bin.exe	C:\Users\admin\Pictures\angelesfixed.png.qqlo	MD5: A7CABBC38DBD02453B3C0584E86FCF8D	SHA256: DA35D63941CAA35001129E306DED22261109A13C208B11C35576FCE75CEE1C51	binary
3596	1.bin.exe	C:\Users\admin\Pictures\computeralbum.png			binary

		MD5: A56332ECDE6134BC5FB05BD6C0442E94	SHA256: 5AA46156EED6BC1F644735AA5E18603D3A9568FD649D17B2CA40B4DC5CA8A88B	
3596	1.bin.exe	C:\Users\admin\Pictures\usuallypublished.jpg.qqlo		image
		MD5: C1F57C9906586B366017D7E74222C472	SHA256: 6AB15252DDC8BCF2CE9A73448BDDBB8276217F4BFA568B7F7B3F24F1A35930D6	
3596	1.bin.exe	C:\Users\admin\Searches\Microsoft OneNote.searchconnector-ms.qqlo		xml
		MD5: 24B408AFC07B8517678A2C3A964CF785	SHA256: 3E311C0875A64D64F4C3AD4979169666FD4C74A14C6DEA746A60AA76B8F75DFC	
3596	1.bin.exe	C:\Users\admin\Pictures\computeralbum.png.qqlo		binary
		MD5: A56332ECDE6134BC5FB05BD6C0442E94	SHA256: 5AA46156EED6BC1F644735AA5E18603D3A9568FD649D17B2CA40B4DC5CA8A88B	
3596	1.bin.exe	C:\Users\admin\Pictures\smallshown.png		binary
		MD5: 2DDFDCD3E97E9999F305AC970E90C8A4	SHA256: 345242B48937CDF5909F0C985CA23C8E1BA1625DF75AC8DE520E8F6765966DA2	
3596	1.bin.exe	C:\Users\admin\Pictures\smallshown.png.qqlo		binary
		MD5: 2DDFDCD3E97E9999F305AC970E90C8A4	SHA256: 345242B48937CDF5909F0C985CA23C8E1BA1625DF75AC8DE520E8F6765966DA2	
3596	1.bin.exe	C:\Users\admin\Searches\Microsoft OneNote.searchconnector-ms		xml
		MD5: 24B408AFC07B8517678A2C3A964CF785	SHA256: 3E311C0875A64D64F4C3AD4979169666FD4C74A14C6DEA746A60AA76B8F75DFC	
3596	1.bin.exe	C:\Users\admin\Searches\Microsoft Outlook.searchconnector-ms		xml
		MD5: 30EB3FA6914C4562ED2FA280341DE14F	SHA256: 8289C3A1A32C0E666A069A4456AD0A92CFEF2817A854728726DB59D057E075EB	
3596	1.bin.exe	C:\Users\admin\Pictures\usuallypublished.jpg		image
		MD5: C1F57C9906586B366017D7E74222C472	SHA256: 6AB15252DDC8BCF2CE9A73448BDDBB8276217F4BFA568B7F7B3F24F1A35930D6	
3596	1.bin.exe	C:\Users\admin\Searches\Microsoft Outlook.searchconnector-ms.qqlo		xml
		MD5: 30EB3FA6914C4562ED2FA280341DE14F	SHA256: 8289C3A1A32C0E666A069A4456AD0A92CFEF2817A854728726DB59D057E075EB	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook Data File - NoMail.pst		binary
		MD5: 14D511C35282462D3C6C4757B56E492D	SHA256: 6B08A7F62EC54A232072EB4414815A5BB1B28A1148602FB1F7127E80567C5712	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook Data File - test.pst.qqlo		binary
		MD5: B7532F842D2BBCF2AF9A13821E8874DB	SHA256: BE2E12E6108BA3BAF835B7F1A39B8E484F6D89DEA92B3B1B8E2FF1240A0EA22D	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\honey@pot.com.pst		binary
		MD5: CCE4E299D4F0C9B5358CE844B9C59AEC	SHA256: 76172465691D9528E2C8EF7B2795C1AD57E8F33D4578515B535C9E8FA07C0E6	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\honey@pot.com.pst.qqlo		binary
		MD5: CCE4E299D4F0C9B5358CE844B9C59AEC	SHA256: 76172465691D9528E2C8EF7B2795C1AD57E8F33D4578515B535C9E8FA07C0E6	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook Data File - test.pst		binary
		MD5: B7532F842D2BBCF2AF9A13821E8874DB	SHA256: BE2E12E6108BA3BAF835B7F1A39B8E484F6D89DEA92B3B1B8E2FF1240A0EA22D	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook Data File - NoMail.pst.qqlo		binary
		MD5: 14D511C35282462D3C6C4757B56E492D	SHA256: 6B08A7F62EC54A232072EB4414815A5BB1B28A1148602FB1F7127E80567C5712	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\~\Outlook.pst.tmp		binary
		MD5: F88BCCF4ED95E12B51C31AD174C51194	SHA256: 060811D90074128A760DA561A65C4F6334D781AD980F8FD3BBE9509A5DF46143	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook.pst.qqlo		binary
		MD5: 338B3C67261C47490E84931E876B8263	SHA256: E453517E7A576D4891D9F598D8581602DC2BD96C69A7E5444ABF2AEFC33C40CF	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\Outlook.pst		binary
		MD5: 338B3C67261C47490E84931E876B8263	SHA256: E453517E7A576D4891D9F598D8581602DC2BD96C69A7E5444ABF2AEFC33C40CF	
3596	1.bin.exe	C:\Users\admin\Documents\Outlook Files\~\Outlook.pst.tmp.qqlo		binary
		MD5: F88BCCF4ED95E12B51C31AD174C51194	SHA256: 060811D90074128A760DA561A65C4F6334D781AD980F8FD3BBE9509A5DF46143	
3596	1.bin.exe	C:\Users\admin\Favorites\Links\Web Slice Gallery.url.qqlo		ini
		MD5: 4227951AD4068A0F6323EA1AD87AAA19	SHA256: 6AB09E83FD0F23A475E8D7DF7C11AF376AAFAA10C9FFDB93F14A104EA1E93119	
3596	1.bin.exe	C:\Users\admin\Favorites\Links\Suggested Sites.url		ini
		MD5: 08A175BC1C02D7672EFB7FDA30790F79	SHA256: 708EF109B27FC0E10F9C5CCEBC9CE86B2AEFAD4D36723EAC5B035B06F91A9196	
3596	1.bin.exe	C:\Users\admin\Favorites\Links for United States\GobiernoUSA.gov.url		ini
		MD5: 2B4D72CF5EF423BEF1106FD341DF1F64	SHA256: AED774BB82C99C8862BC8B88C9290BD071D7B987C57FF1D4E230F33B528CBA0C	
3596	1.bin.exe	C:\Users\admin\Favorites\Links\Suggested Sites.url.qqlo		ini
		MD5: 08A175BC1C02D7672EFB7FDA30790F79	SHA256: 708EF109B27FC0E10F9C5CCEBC9CE86B2AEFAD4D36723EAC5B035B06F91A9196	
3596	1.bin.exe	C:\Users\admin\Favorites\Links\Web Slice Gallery.url		ini
		MD5: 4227951AD4068A0F6323EA1AD87AAA19	SHA256: 6AB09E83FD0F23A475E8D7DF7C11AF376AAFAA10C9FFDB93F14A104EA1E93119	
3596	1.bin.exe	C:\Users\admin\Favorites\Links for United States\GobiernoUSA.gov.url.qqlo		ini
		MD5: 2B4D72CF5EF423BEF1106FD341DF1F64	SHA256: AED774BB82C99C8862BC8B88C9290BD071D7B987C57FF1D4E230F33B528CBA0C	
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\IE Add-on site.url		ini
		MD5: 723296EAB996C807C83760B18967B52E	SHA256: CAE90BB478BDF0775F7B656FBDCA6ADEA149017ACA40A15B3FFD6B5703AD904A	
3596	1.bin.exe	C:\Users\admin\Favorites\Links for United States\USA.gov.url.qqlo		ini
		MD5: 0F2CFCBC7E45BA4A2448A37B60AF2B7B	SHA256: 206F37DF130436FAF3C70C9D7ABFF0B299E9804B16E6C519973287E2F2064D6A	
3596	1.bin.exe	C:\Users\admin\Favorites\Links for United States\USA.gov.url		ini
		MD5: 0F2CFCBC7E45BA4A2448A37B60AF2B7B	SHA256: 206F37DF130436FAF3C70C9D7ABFF0B299E9804B16E6C519973287E2F2064D6A	

3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\IE Add-on site.url.qqlo	<div>ini</div>
		MD5: 723296EAB996C807C83760B18967B52E	SHA256: CAE90BB478BDF07757F7B656FBDCA6ADEA149017ACA40A15B3FFD6B5703AD904A
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft At Work.url	<div>ini</div>
		MD5: FEF7652B199B7B72DD9F130D5CAF991C	SHA256: D0AF4647A0F1918B60AA94BC40A7414A22F5C0FB38CD455ED8CC88ACA7833C65
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\IE site on Microsoft.com.url.qqlo	<div>ini</div>
		MD5: 026151BC1A00C2B65F1C68D91D480C4C	SHA256: E32BA52BAF6B111FE62749B76D9CCA2BC5CF01A1959E66A1F78BEB683038054B
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Autos.url	<div>ini</div>
		MD5: F176C5765EB304DE3D5D65B3AD97A9BA	SHA256: 2FAE73C75F654776A5810D511C073190DA8A04404208B6C1DE630FB45521347F
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft At Home.url.qqlo	<div>ini</div>
		MD5: 86A42493A17B6F04BC5E948EC55AD853	SHA256: 08F2280F5B2077A9E98894D67B5CD432BE69BB7E8BBB862D76B331E7BC415822
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft At Work.url.qqlo	<div>ini</div>
		MD5: FEF7652B199B7B72DD9F130D5CAF991C	SHA256: D0AF4647A0F1918B60AA94BC40A7414A22F5C0FB38CD455ED8CC88ACA7833C65
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft Store.url.qqlo	<div>ini</div>
		MD5: 2403566DBDA142918F0E8DFB6C03B084	SHA256: 0A875E05329621472CF2825D6B6802F9D48F9E968DF30E4CF743911CDCAC8CD1
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft Store.url	<div>ini</div>
		MD5: 2403566DBDA142918F0E8DFB6C03B084	SHA256: 0A875E05329621472CF2825D6B6802F9D48F9E968DF30E4CF743911CDCAC8CD1
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\IE site on Microsoft.com.url	<div>ini</div>
		MD5: 026151BC1A00C2B65F1C68D91D480C4C	SHA256: E32BA52BAF6B111FE62749B76D9CCA2BC5CF01A1959E66A1F78BEB683038054B
3596	1.bin.exe	C:\Users\admin\Favorites\Microsoft Websites\Microsoft At Home.url	<div>ini</div>
		MD5: 86A42493A17B6F04BC5E948EC55AD853	SHA256: 08F2280F5B2077A9E98894D67B5CD432BE69BB7E8BBB862D76B331E7BC415822
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Entertainment.url.qqlo	<div>ini</div>
		MD5: 7AC3F6BD8FED8D45DE245D96316DC914	SHA256: 74AA3F5B0B7583190A18A2E64E3C60BB1839E4864C38868C1C6FC600D8769FC1
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Entertainment.url	<div>ini</div>
		MD5: 7AC3F6BD8FED8D45DE245D96316DC914	SHA256: 74AA3F5B0B7583190A18A2E64E3C60BB1839E4864C38868C1C6FC600D8769FC1
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Autos.url.qqlo	<div>ini</div>
		MD5: F176C5765EB304DE3D5D65B3AD97A9BA	SHA256: 2FAE73C75F654776A5810D511C073190DA8A04404208B6C1DE630FB45521347F
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Money.url.qqlo	<div>ini</div>
		MD5: B0C0BB888DBD622A7E02440F71B6DF19	SHA256: 4BA7545D4ABB23EC448CFA0F649B60780A64E9A89244613D81F25A70841E6D63
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Sports.url.qqlo	<div>ini</div>
		MD5: 3DDC1C5FC6ED8485B055842736B3F121	SHA256: 4A02FAFDB148F5391241B1FE19E0774169EAAFAA0A88FC0238DC494F1F04D01
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Sports.url	<div>ini</div>
		MD5: 3DDC1C5FC6ED8485B055842736B3F121	SHA256: 4A02FAFDB148F5391241B1FE19E0774169EAAFAA0A88FC0238DC494F1F04D01
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN Money.url	<div>ini</div>
		MD5: B0C0BB888DBD622A7E02440F71B6DF19	SHA256: 4BA7545D4ABB23EC448CFA0F649B60780A64E9A89244613D81F25A70841E6D63
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN.url.qqlo	<div>ini</div>
		MD5: C4AFD800986224AB6598AC4F9564626E	SHA256: 080FE36208220E58DE6DC25816B94EA1936C5D3AE743D6DEFD590416C7F35727
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Get Windows Live.url	<div>ini</div>
		MD5: ED215F360878165812B09F0763EFA332	SHA256: F6A19B75E8831B92B02F3BE359B9C076ED1B8FDA6B55BE49A53405846C5A70D4
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Gallery.url.qqlo	<div>ini</div>
		MD5: EDD31710E1B8A69E6D97EB436E96CE9F	SHA256: C001DAFB30422D447D90C2EAD18004A2F0466FB06E44DF8F23433887966C63FB
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Mail.url	<div>ini</div>
		MD5: 9BE01B27E16CEE00535063DD8A4E956	SHA256: 1BBB6611D26E1CA552CE123E1E7817771A6CB04B3D9FC61E8C744BCA731BD716
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSN.url	<div>ini</div>
		MD5: C4AFD800986224AB6598AC4F9564626E	SHA256: 080FE36208220E58DE6DC25816B94EA1936C5D3AE743D6DEFD590416C7F35727
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Gallery.url	<div>ini</div>
		MD5: EDD31710E1B8A69E6D97EB436E96CE9F	SHA256: C001DAFB30422D447D90C2EAD18004A2F0466FB06E44DF8F23433887966C63FB
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Get Windows Live.url.qqlo	<div>ini</div>
		MD5: ED215F360878165812B09F0763EFA332	SHA256: F6A19B75E8831B92B02F3BE359B9C076ED1B8FDA6B55BE49A53405846C5A70D4
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Spaces.url	<div>ini</div>
		MD5: EF021B2A990F002C7563110CB5CF992D	SHA256: 7CCDA6B3063A0B7A7729E66B0027C8F9A160D0B27F2249CE8A2B74BA2850A66E
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Mail.url.qqlo	<div>ini</div>
		MD5: 9BE01B27E16CEE00535063DD8A4E956	SHA256: 1BBB6611D26E1CA552CE123E1E7817771A6CB04B3D9FC61E8C744BCA731BD716
3596	1.bin.exe	C:\Users\admin\Favorites\Windows Live\Windows Live Spaces.url.qqlo	<div>ini</div>
		MD5: EF021B2A990F002C7563110CB5CF992D	SHA256: 7CCDA6B3063A0B7A7729E66B0027C8F9A160D0B27F2249CE8A2B74BA2850A66E
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSNBC News.url.qqlo	<div>ini</div>
		MD5: 430FC8A5DDC68CB6426D8C972B6C72F9	SHA256: 5A63D86BA705843A1EFF79E08A5D65A5F7C6287E52F0C70AEE30169A23C66D10
3596	1.bin.exe	C:\Users\admin\Favorites\MSN Websites\MSNBC News.url	<div>ini</div>

				MD5: 430FC8A5DDC68CB426D8C972B6C72F9	SHA256: 5A6D386BA705843A1EFF79E08A5D65A5F7C6287E52F0C70AEE30169A2A3C66D10	
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\container.dat.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\EmieSiteList\container.dat.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\EmieUserList\container.dat.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Windows\AppCache\container.dat.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\General.one		MD5: 03A7F7DE830B40378FFD75FA8C89F11	SHA256: 5DD4FB6736580517A30D6442878A877CD41A3DB6D5B85DCA9A5A36A3377CFC0	binary
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\Unfiled Notes.one.qql		MD5: A5F1EF48AAAD4101DDAAF9F0D4DA4157	SHA256: DFFCE76CA6E7FA925808F172E2527FE44FCB38A350127BEDC45B987E2FFED27C	binary
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\Unfiled Notes.one		MD5: A5F1EF48AAAD4101DDAAF9F0D4DA4157	SHA256: DFFCE76CA6E7FA925808F172E2527FE44FCB38A350127BEDC45B987E2FFED27C	binary
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\Open Notebook.onetoc2		MD5: 1F86C2F87A62063DA7F94EC919FB7B3A	SHA256: 99C51F1D387266CDACE4595FAFF4A28501228B41EBD376CC934AE080EDE7AB2	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\F12\debugger\settings.json.qql		MD5: 63B674036C598B4ADB025AB4A400CF17	SHA256: 89399010D91343808B7F3FA29EFAE27DDA95F9738452AFF8BD778F2CFF23FDF	txt
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\General.one.qql		MD5: 03A7F7DE830B40378FFD75FA8C89F11	SHA256: 5DD4FB6736580517A30D6442878A877CD41A3DB6D5B85DCA9A5A36A3377CFC0	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\F12\debugger\settings.json		MD5: 63B674036C598B4ADB025AB4A400CF17	SHA256: 89399010D91343808B7F3FA29EFAE27DDA95F9738452AFF8BD778F2CFF23FDF	txt
3596	1.bin.exe	C:\Users\admin\Documents\OneNote Notebooks\Personal\Open Notebook.onetoc2.qql		MD5: 1F86C2F87A62063DA7F94EC919FB7B3A	SHA256: 99C51F1D387266CDACE4595FAFF4A28501228B41EBD376CC934AE080EDE7AB2	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\F12\header\MyCode.json.qql		MD5: ECAA88F7FA0BF610A5A26CF545DCD3AA	SHA256: F1945CD6C19E56B3C1C78943EF5EC18116907A4CA1EFC40A57D48AB1DB7ADFC5	text
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\Services\logo_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.en-US_100_gray.png.qql		MD5: 61173B8C9C7A4518CA2E2EB217094DBE	SHA256: 9F065479E3B52448647AE823FE6B7B04642E4F22243467BF0579B5C2341FB479	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Windows\AppCache\P5S0AQFP\container.dat.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\000003.log.qql		MD5: —	SHA256: —	—
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\Services\logo_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.en-US_100_gray.png		MD5: 61173B8C9C7A4518CA2E2EB217094DBE	SHA256: 9F065479E3B52448647AE823FE6B7B04642E4F22243467BF0579B5C2341FB479	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Sun\Java\Deployment\deployment.properties		MD5: 1A6C9FF08576BDA358A1A1CA928E523F	SHA256: 851CAC39AD7E8791AD3E96290FBE90475B18432469A0954CB4DB1103FB69C2D0	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\F12\perf\tools\memory\settings.json.qql		MD5: ECAA88F7FA0BF610A5A26CF545DCD3AA	SHA256: F1945CD6C19E56B3C1C78943EF5EC18116907A4CA1EFC40A57D48AB1DB7ADFC5	text
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\CYUQ4FPV\www.microsoft[1].xml		MD5: D2ACD534C9278E191CD9121A8C166C2C	SHA256: BB2B221210CBD9A9A811F33A354CA342FF48C4B91F5FABE1E8932F519A1B47E0	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Sun\Java\Deployment\deployment.properties.qql		MD5: 1A6C9FF08576BDA358A1A1CA928E523F	SHA256: 851CAC39AD7E8791AD3E96290FBE90475B18432469A0954CB4DB1103FB69C2D0	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\CYUQ4FPV\www.microsoft[1].xml.qql		MD5: D2ACD534C9278E191CD9121A8C166C2C	SHA256: BB2B221210CBD9A9A811F33A354CA342FF48C4B91F5FABE1E8932F519A1B47E0	binary
3596	1.bin.exe	C:\Users\admin\AppData\LocalLow\Microsoft\F12\perf\tools\visualprofiler\settings.json.qql		MD5: ECAA88F7FA0BF610A5A26CF545DCD3AA	SHA256: F1945CD6C19E56B3C1C78943EF5EC18116907A4CA1EFC40A57D48AB1DB7ADFC5	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
9	14	10	22

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1416	1.bin.exe	GET	200	172.64.155.188:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTNMNjMNDqCqx8FcBWK16EHdimS6QUU3m%2FWqorSs	US	der	2.18 Kb	whitelisted

9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D									
1416	1.bin.exe	GET	200	104.18.32.68:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRtU9uFggVGHhJwXZyWCNXmVR5ngQoBoBEKlz6W8Qfs4q8p74Klf9AwplQCEDlyRDr5lrdR19NsEN0xNZU%3D	US	der	1.42 Kb	whitelisted
1416	1.bin.exe	GET	200	67.27.233.254:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f6a8994a4074a634	US	compressed	4.70 Kb	whitelisted
1188	1.bin.exe	GET	—	211.171.233.129:80	http://acacaca.org/fhsgtsspen6/get.php?pid=4FADA754A641CFAD6036D5EAB829FF28&first=true	KR	—	—	malicious
1188	1.bin.exe	GET	—	110.14.121.125:80	http://rgyui.top/dl/build2.exe	KR	—	—	malicious
1188	1.bin.exe	GET	404	211.171.233.129:80	http://acacaca.org/files/1/build3.exe	KR	html	216 b	malicious
1416	1.bin.exe	GET	200	104.18.32.68:80	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl	US	der	978 b	whitelisted
1188	1.bin.exe	GET	—	211.171.233.129:80	http://acacaca.org/fhsgtsspen6/get.php?pid=4FADA754A641CFAD6036D5EAB829FF28&first=true	KR	—	—	malicious
3596	1.bin.exe	GET	200	211.171.233.129:80	http://acacaca.org/fhsgtsspen6/get.php?pid=4FADA754A641CFAD6036D5EAB829FF28	KR	binary	556 b	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1416	1.bin.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
1416	1.bin.exe	67.27.233.254:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	suspicious
1416	1.bin.exe	104.18.32.68:80	ocsp.comodoca.com	Cloudflare Inc	US	suspicious
1416	1.bin.exe	172.64.155.188:80	ocsp.comodoca.com	—	US	suspicious
1188	1.bin.exe	110.14.121.125:80	rgyui.top	SK Broadband Co Ltd	KR	malicious
3596	1.bin.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
1188	1.bin.exe	162.0.217.254:443	api.2ip.ua	AirComPlus Inc.	CA	suspicious
1188	1.bin.exe	211.171.233.129:80	acacaca.org	LG DACOM Corporation	KR	malicious
3596	1.bin.exe	211.171.233.129:80	acacaca.org	LG DACOM Corporation	KR	malicious

DNS requests

Domain	IP	Reputation
api.2ip.ua	162.0.217.254	shared
ctldl.windowsupdate.com	67.27.233.254 8.241.122.254 67.27.233.126 8.241.121.126 8.248.135.254	whitelisted
ocsp.comodoca.com	104.18.32.68 172.64.155.188	whitelisted
ocsp.usertrust.com	172.64.155.188 104.18.32.68	whitelisted
crl.usertrust.com	104.18.32.68 172.64.155.188	whitelisted
rgyui.top	110.14.121.125 37.34.248.24 58.235.189.192 185.95.186.58 31.166.139.4 176.44.116.130 93.152.141.65 222.236.49.123 109.98.58.98 190.195.107.105	malicious
acacaca.org	211.171.233.129 109.102.255.230 41.41.255.235 190.140.74.43 138.36.3.134 93.152.141.65 37.34.248.24 210.92.250.133 210.182.29.70 1.248.122.240	malicious

Threats

PID	Process	Class	Message
—	—	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip.ua)
—	—	A Network Trojan was detected	ET POLICY External IP Address Lookup DNS Query (2ip.ua)
1416	1.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api.2ip.ua in TLS SNI)
1188	1.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api.2ip.ua in TLS SNI)
—	—	Potentially Bad Traffic	ET DNS Query to a *.top domain - Likely Hostile
1188	1.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request
1188	1.bin.exe	A Network Trojan was detected	ET CURRENT_EVENTS SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Win32/Vodkagats Loader Requesting Payload
1188	1.bin.exe	Potentially Bad Traffic	ET INFO HTTP Request to a *.top domain
1188	1.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Win32/Filecoder.STOP Variant Request for Public Key
3596	1.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api.2ip.ua in TLS SNI)
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Win32/Vodkagats Loader Requesting Payload
3596	1.bin.exe	A Network Trojan was detected	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download
1188	1.bin.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
1188	1.bin.exe	Misc activity	ET INFO Possible EXE Download From Suspicious TLD
1188	1.bin.exe	A Network Trojan was detected	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download

Debug output strings

Process	Message
mmc.exe	Constructor: Microsoft.TaskScheduler.SnapIn.TaskSchedulerSnapIn
mmc.exe	OnInitialize: Microsoft.TaskScheduler.SnapIn.TaskSchedulerSnapIn
mmc.exe	AddIcons: Microsoft.TaskScheduler.SnapIn.TaskSchedulerSnapIn
mmc.exe	ProcessCommandLineArguments: Microsoft.TaskScheduler.SnapIn.TaskSchedulerSnapIn



Interactive malware hunting service ANY.RUN
© 2017-2022 ANY.RUN LLC. ALL RIGHTS RESERVED