ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	SecuriteInfo.com.Variant.Zusy.436106.1689.2350
Full analysis:	https://app.any.run/tasks/280e4c7d-b3ea-4bb8-bdd9-172189c794eb
Verdict:	Malicious activity
Threats:	Remcos Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month.
Analysis date:	August 23, 2022 at 16:11:16
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	rat remcos trojan
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	6DF1FC198682F8D63F02E9D78C2A42AF
SHA1:	7EB382DECAB2DA5D0FB1A179B118C94415B95856
SHA256:	8044038EC5BAA7261F92D631C86EF26FAAA7F6F8090FDC984C32FDC0A0D44499
SSDEEP:	12288:k9GwutcDlvA4So4CK2xgIYc61RwnT7grJFcuHdl51T9u6mr:k8ztM64SQKigl01XlFcu9lyr

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	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)

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

Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)	KB2685813
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	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)
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 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)

KB3156016
KB3159398
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
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

REMCOS detected by memory dumps
cleanmgr.exe (PID: 2612)

Drops executable file immediately after starts
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Changes the autorun value in the registry
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

REMCOS was detected
cleanmgr.exe (PID: 2612)

Connects to CnC server
cleanmgr.exe (PID: 2612)

SUSPICIOUS

Checks supported languages
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Reads the computer name
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Drops a file with a compile date too recent
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Executable content was dropped or overwritten
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Adds / modifies Windows certificates
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Reads Environment values
cleanmgr.exe (PID: 2612)

INFO

Reads settings of System Certificates
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Reads the computer name
cleanmgr.exe (PID: 2612)

Checks supported languages
cleanmgr.exe (PID: 2612)

Checks Windows Trust Settings
SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe (PID: 2508)

Reads Microsoft Office registry keys
cleanmgr.exe (PID: 2612)

Static information

TRiD

.exe | Win32 Executable Borland Delphi 7 (68.8)
.exe | Win32 Executable Borland Delphi 6 (27.2)
.exe | Win32 Executable Delphi generic (1.4)
.scr | Windows screen saver (1.3)
.exe | Win32 Executable (generic) (0.4)

EXIF

EXE

Author:	WlxLife
HomePage:	
CompanyName:	
LegalCopyright:	Copyright ©2013 All Rights Reserved.
FileDescription:	Tec leader

Comments:	Tec leader
CharacterSet:	Unicode
LanguageCode:	English (British)
FileSubtype:	0
ObjectFileType:	Unknown
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	0.0.0.0
FileVersionNumber:	0.0.0.0
Subsystem:	Windows GUI
SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x6b75c
UninitializedDataSize:	0
InitializedDataSize:	299008
CodeSize:	436224
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
Comments:	Tec leader
FileDescription:	Tec leader
LegalCopyright:	Copyright ©2013 All Rights Reserved.
CompanyName:	
HomePage:	
Author:	WlxLife

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

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	8
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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
CODE	0x00001000	0x0006A7C8	0x0006A800	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.54296
DATA	0x0006C000	0x000015DC	0x00001600	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.17162
BSS	0x0006E000	0x00000DAD	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x0006F000	0x000023B6	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	5.04196
.tls	0x00072000	0x00000010	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00073000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.20692
.reloc	0x00074000	0x00007928	0x00007A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.68409
.rsrc	0x0007C000	0x0003DA00	0x0003DA00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	7.02734

Resources

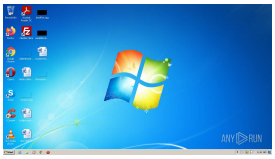
Title	Entropy	Size	Codepage	Language	Type
1	3.24482	544	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.91604	308	UNKNOWN	UNKNOWN	RT_CURSOR
67	2.18416	9640	UNKNOWN	UNKNOWN	RT_ICON
68	2.26867	6760	UNKNOWN	UNKNOWN	RT_ICON
72	2.98919	1128	UNKNOWN	UNKNOWN	RT_ICON
4079	3.13833	644	UNKNOWN	UNKNOWN	RT_STRING
4080	3.33429	788	UNKNOWN	UNKNOWN	RT_STRING
4081	3.22533	492	UNKNOWN	UNKNOWN	RT_STRING
4082	3.22332	316	UNKNOWN	UNKNOWN	RT_STRING
4083	3.24374	712	UNKNOWN	UNKNOWN	RT_STRING
4084	3.24999	424	UNKNOWN	UNKNOWN	RT_STRING
4085	3.10835	232	UNKNOWN	UNKNOWN	RT_STRING
4086	3.1381	312	UNKNOWN	UNKNOWN	RT_STRING
4087	3.2613	956	UNKNOWN	UNKNOWN	RT_STRING
4088	3.17999	932	UNKNOWN	UNKNOWN	RT_STRING
4089	3.214	932	UNKNOWN	UNKNOWN	RT_STRING
4090	3.24761	1000	UNKNOWN	UNKNOWN	RT_STRING
4091	2.94341	244	UNKNOWN	UNKNOWN	RT_STRING
4092	2.8794	196	UNKNOWN	UNKNOWN	RT_STRING
4093	3.24527	704	UNKNOWN	UNKNOWN	RT_STRING
4094	3.22956	1144	UNKNOWN	UNKNOWN	RT_STRING
4095	3.24474	940	UNKNOWN	UNKNOWN	RT_STRING
4096	3.18309	724	UNKNOWN	UNKNOWN	RT_STRING
32761	1.83876	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32762	1.91924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32763	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32764	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32765	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32766	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32767	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
BBABORT	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBALL	3.16995	484	UNKNOWN	UNKNOWN	RT_BITMAP
BBCANCEL	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBCLOSE	3.68492	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBHELP	2.88085	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBIGNORE	3.29718	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBNO	3.58804	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBOK	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBRETRY	3.53344	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBYES	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP
PREVIEWGLYPH	2.85172	232	UNKNOWN	English - United States	RT_BITMAP
DLGTEMPLATE	2.5627	82	UNKNOWN	UNKNOWN	RT_DIALOG

ASS	7.12828	209583	UNKNOWN	English - United States	RT_RCDATA
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
PACKAGEINFO	5.45926	916	UNKNOWN	UNKNOWN	RT_RCDATA
TFORMFILTER	5.49356	1663	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.73389	48	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

advapi32.dll
comctl32.dll
gdi32.dll
kernel32.dll
ole32.dll
oleaut32.dll
user32.dll
version.dll

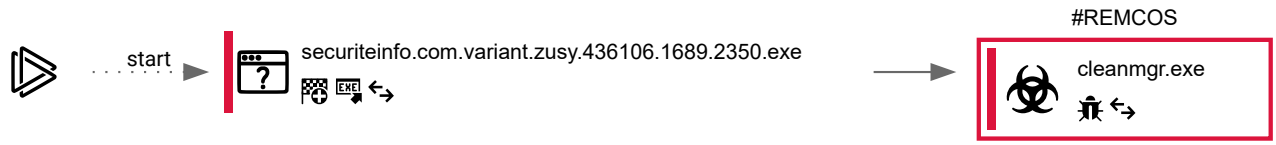
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
35	2	2	0

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
2508	"C:\Users\admin\AppData\Local\Temp\SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe"	C:\Users\admin\AppData\Local\Temp\SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe		Explorer.EXE

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:	Tec leader	**Exit code:**	0

2612	"C:\Windows\System32\cleanmgr.exe"	C:\Windows\System32\cleanmgr.exe		SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Disk Space Cleanup Manager for Windows

Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Registry activity

Total events	Read events	Write events	Delete events
5 322	5 225	95	2

Modification events

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B010000090000000000000000000000000000000000400000000000000C0E333BBEAB1D30100000000000000000000000001000000020000000C0A80164000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.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: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{362E934C-743B-4588-8259-D2482DB771A8}
Operation: write **Name:** WpadDecisionTime
Value: 006E87F0DCB6D801

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.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: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.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: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.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: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 006E87F0DCB6D801

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.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: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation: write **Name:** Blob
Value: 0400000001000000010000000E4A68AC854AC5242460AFD72481B2A44530000000100000040000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C010330123010060A2B0601040182373C0101030200C00F000000010000002000000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000001000000070DC30BC974695560A2F0090A6545556C14000000010000001400000004E2254201895E6E36EE60FFAFAB912ED06178F39620000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400200047006C006F00620061006C00200052006F006F007400200047003200000001900000001000000100000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B060105050703020608 2B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820 38E30820276A0030201020210033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530130603550 40A130C44696769436727420496E633119301706035040B13107777772E6469676936572742E636F6D3120301E060355040313174469676943657274204 76C6F62616C20526F6F74204732308122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0CB948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F67314143D4676C387148921344DAF0F450CA649A1BABB9CC5B13383298502030100 01A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF04040302018630 1D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB05F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F97050704741115719 4EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F31445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB33537E532B6

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation: delete key **Name:** (default)
Value:

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\DF3C24F9BFD666761B268073FE06D1CC8D4F82A4
Operation: write **Name:** Blob
Value: 5C0000000100000004000000008000053000000010000004000000303E301F06096086480186FD6C020130123010060A2B0601040182373C0101030200C0301B060567810C01033012301 0060A2B0601040182373C0101030200C00F000000010000002000000004B4EB4B074298B828B5C003095A10B4523FB951C0C88348B09C53E5BABA408A3030000000100000014000000DF3C 24F9BFD666761B268073FE06D1CC8D4F82A41D000000010000001000000070DC30BC974695560A2F0090A6545556C14000000010000001400000004E2254201895E6E36EE60FFAFAB912ED06 178F39620000000100000020000000CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F0B000000010000003000000044006900670069004300650072007400 200047006C006F00620061006C00200052006F006F007400200047003200000001900000001000000100000014C3BD3549EE225AECE13734AD8CA0B8090000000100000034000000303206082B060105050703020608 2B0601050507030306082B0601050507030406082B0601050507030106082B0601050507030820000000010000009203000030820 38E30820276A00302010202100033AF1E6A711A9A0BB2864B11D09FAE5300D06092A864886F70D01010B05003061310B3009060355040613025553311530130603550 40A130C44696769436727420496E633119301706035040B13107777772E6469676936572742E636F6D3120301E060355040313174469676943657274204 76C6F62616C20526F6F74204732308122300D06092A864886F70D01010105000382010F003082010A0282010100BB37CD34DC7B6BC9B 26890AD4A75FF46BA210A088DF51954C9FB88DBF3AEF23A89913C7AE6AB061A6BCFAC2DE85E092444BA629A7ED6A3A87EE054752005AC50B79C631A6C30DCDA1F19B1D71EDEFDD7E0C B948337AEEC1F434EDD7B2CD2BD2EA52FE4A9B8AD3AD499A4B625E99B6B00609260FF4F214918F76790AB61069C8FF2BAE9B4E992326BB5F357E85D1BCD8C1DAB95049549F3352D96E3 496DDD77E3FB494BB4AC5507A98F95B3B423BB4C6D45F0F6A9B29530B4FD4C558C274A57147C829DCD7392D3164A060C8C50D18F1E09BE17A1E621CAFD83E510BC83A50AC46728F6731 4143D4676C387148921344DAF0F450CA649A1BABB9CC5B13383298502030100 01A3423040300F0603551D130101FF040530030101FF300E0603551D0F0101FF04040302018630 1D0603551D0E041604144E2254201895E6E36EE60FFAFAB912ED06178F39300D06092A864886F70D01010B05000382010100606728946F0E4863EB31DDEA6718D5897D3CC58B4A7FE9BEDB2B17DFB0 5F73772A3213398167428423F2456735EC88BFF88FB0610C34A4AE204C84C6DBF835E176D9DFA642BBC74408867F3674245ADA6C0D145935BDF249DDB61FC9B30D472A3D992FBB5CBBB5 D420E1995F534615DB689BF0F330D53E31E28D849EE38ADADA963E3513A55FF0F97050704741115719 4EC08FAE06C49513172F1B259F75F2B18E99A16F13B14171FE882AC84F102055D7F3 1445E5E044F4EA879532930EFE5346FA2C9DFF8B22B94BD90945A4DEA4B89A58DD1B7D529F8E59438881A49E26D56FADDD0DC6377DED03921BE5775F76EE3C8DC45D565BA2D9666EB335 37E532B6

(PID) Process: (2508) SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** Hxmakapta
Value: C:\Users\Public\Libraries\atpakamxH.url

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @C:\Windows\System32\occache.dll,-1070
Value: Downloaded Program Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @C:\Windows\System32\occache.dll,-1071
Value: Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @C:\Windows\System32\occache.dll,-1072
Value: &View Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage
Operation: write **Name:** ProductFiles
Value:

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1002
Value: Previous Windows installation(s)

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1003
Value: Files from a previous Windows installation. Files and folders that may conflict with the installation of Windows have been moved to folders named Windows.old. You can access data from the previous Windows installations in this folder.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\System32\DATACLEN.DLL,-1010
Value: Setup Log Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\System32\DATACLEN.DLL,-1011
Value: Files created by Windows

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\werfault.exe,-100
Value: System error memory dump files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\werfault.exe,-101
Value: Remove system error memory dump files.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\werfault.exe,-102
Value: System error minidump files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\werfault.exe,-103
Value: Remove system error minidump files.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1000
Value: Temporary Windows installation files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1001
Value: Installation files used by Windows setup. These files are left over from the installation process and can be safely deleted.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1004
Value: Files discarded by Windows upgrade

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1005
Value: Files from a previous Windows installation. As a precaution, Windows upgrade keeps a copy of any files that were not moved to the new version of Windows and were not identified as Windows system files. If you are sure that no user's personal files are missing after the upgrade, you can delete these files.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-297
Value: Per user archived Windows Error Reporting Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-298
Value: Files used for error reporting and solution checking.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-295
Value: Per user queued Windows Error Reporting Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E

Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-296
Value: Files used for error reporting and solution checking.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-301
Value: System archived Windows Error Reporting Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-302
Value: Files used for error reporting and solution checking.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-299
Value: System queued Windows Error Reporting Files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%SystemRoot%\system32\wer.dll,-300
Value: Files used for error reporting and solution checking.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1006
Value: Windows upgrade log files

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16C\52C64B7E
Operation: write **Name:** @%systemroot%\system32\setupcln.dll,-1007
Value: Windows upgrade log files contain information that can help identify and troubleshoot problems that occur during Windows installation, upgrade, or servicing. Deleting these files can make it difficult to troubleshoot installation issues.

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CURRENT_USER\Software\Remcos-UJQ6LS
Operation: write **Name:** exepath
Value: FEAA

(PID) Process: (2612) cleanmgr.exe **Key:** HKEY_CURRENT_USER\Software\Remcos-UJQ6LS
Operation: write **Name:** licence
Value: 4CEB6F73CF458662CD173185D5B50440

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	8	3	2

Dropped files

PID	Process	Filename	Type
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** F7DCB24540769805E5BB30D193944DCE **SHA256:** 6B88C6AC55BBD6FEA0EBE5A760D1AD2CFCE251C59D0151A1400701CB927E36EA	compressed
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 83427DED120486A907899A8C6821DE63 **SHA256:** 9661397DB463E8956291E3DD7622008E5E97A97DD5F2E4B1A3EB22A1C3B9D165	der
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 **MD5:** A83DAF27149E13E6FFA806E06532CC8F **SHA256:** A21552016617AB35D43B3D90166A4E779112B280E9C4C1D8A7F030231F8ECF2D	binary
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\Public\Libraries\atpakamxH.url **MD5:** C5524FC3274DC7A6053D75C48E2BD9B1 **SHA256:** 439519C5E2887CB20F8D183CC6E8C5A16A940AFC522441A1D2C40502181B152A	text
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** D251952A353B0E8D243F4D284530B915 **SHA256:** BA8E4D80E9C9014790AFED82B2CAA752BA8621C5B91C4A99AB1A6833EFCF2F02	binary
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442 **MD5:** AE4A5D960EAAF76C153905A72624BEBE **SHA256:** F7C6A3FD1FFD6F476C992F1FFB88C21D097EF345A9F53754045FEE5E039C0196	der
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868 **MD5:** 13C0CEDD7E3D6B4F87021779C6168286 **SHA256:** 1B6C71175FC906584CD797E53CA0AF990BE005B96CB0D86DAA52027751A69068	binary
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\Public\Libraries\Hxmakapta.exe **MD5:** 6DF1FC198682F8D63F02E9D78C2A42AF **SHA256:** 8044038EC5BAA7261F92D631C86EF26FAAA7F6F8090FDC984C32FDC0A0D44499	executable
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\WAGTPIDO.txt **MD5:** 332515C364F29B496AF45B8676D7ABC9 **SHA256:** 63B0FAE357D16F55D6865E838F1FD85B852D87E37064E76CE71074A577D95728	text
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies\IKQ7VLEY.txt **MD5:** 12ABF7353F8728D4B1FAAA24CF6F84CF **SHA256:** 86952BA6833EA13E1031DDFFEA4482A9D2E3AB82489E3F68261817370600 98AD	text

2612	cleanmgr.exe	C:\Users\admin\AppData\Local\Temp\{3845C35A-DB12-4077-96B7-6EF24031DD74}	binary
		MD5: 44D91C4E24C9DD3DA39B35F98E032B60 **SHA256:** 070D8D6328DFBD852940162DB8802E3C41561A278173874B83EC1DB41F5855F5	
2612	cleanmgr.exe	C:\Users\admin\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	binary
		MD5: D471A0BB5F0B8A9AC834E0172491B7F9 **SHA256:** 418B6AE0A39787583DCD77DA0ED040F8C3DDA03410E71D04C235EE6E736F298F	
2612	cleanmgr.exe	C:\Users\admin\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	binary
		MD5: 44D91C4E24C9DD3DA39B35F98E032B60 **SHA256:** 070D8D6328DFBD852940162DB8802E3C41561A278173874B83EC1DB41F5855F5	
2612	cleanmgr.exe	C:\Users\admin\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{B80C13D1-937B-4090-9903-C828BD0463A6}.FSD	binary
		MD5: 59C2A15BB7F125FACCE3D1002002A05C **SHA256:** C7C0E8D6B1317811F64B4B595A529A871A4549FC9D06C8E7E70B2D8B0C970908	

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
3	53	6	22

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	GET	200	209.197.3.8:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ba66a84a9e4cebf6	US	compressed	4.70 Kb	whitelisted
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjlD1ie%2Bx%2BdSjo%3D	US	der	1.47 Kb	whitelisted
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc%3D	US	der	471 b	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	13.107.42.12:443	sub41a.db.files.1drv.com	Microsoft Corporation	US	suspicious
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	209.197.3.8:80	ctldl.windowsupdate.com	Highwinds Network Group, Inc.	US	suspicious
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
–	–	194.147.140.32:1970	godslovem.ddns.net	–	–	malicious
2612	cleanmgr.exe	194.147.140.32:1970	godslovem.ddns.net	–	–	malicious
2508	SecuriteInfo.com.Variant.Zusy.436106.1689.2350.exe	13.107.43.13:443	onedrive.live.com	Microsoft Corporation	US	malicious

DNS requests

Domain	IP	Reputation
onedrive.live.com	13.107.43.13	shared
ctldl.windowsupdate.com	209.197.3.8	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
sub41a.db.files.1drv.com	13.107.42.12	unknown
godslovem.ddns.net	194.147.140.32	malicious

Threats

PID	Process	Class	Message
–	–	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddns .net
2612	cleanmgr.exe	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 24
–	–	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.ddns .net

Debug output strings

Debug output strings

Process	Message
cleanmgr.exe	PID=2612 Failed to create. - CScavengeCleanup::Initialize(hr:0x800702e4)
cleanmgr.exe	DC:Process is not elevated.