ID: 625379
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.8516.26511
Cookbook: default.jbs
Time: 16:57:14
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

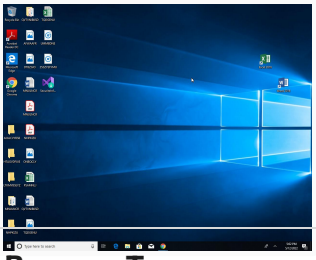
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.8516.26511

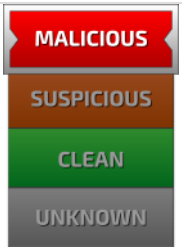
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.8516.26511 (renamed file extension from 26511 to exe)
Analysis ID:	625379
MD5:	90e91d605fb261..
SHA1:	1737b52ca84665..
SHA256:	4700f996868b46..
Tags:	exe
Infos:	



Detection



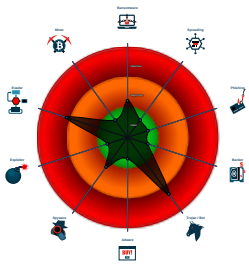
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetect.malware2.8516.exe (PID: 6984 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe" MD5: 90E91D605FB261FA827093074C0D7178)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1o9xcx-d3Bxjd3qTkG604DI9J3fWxwqqB"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.955923216.00000000028B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

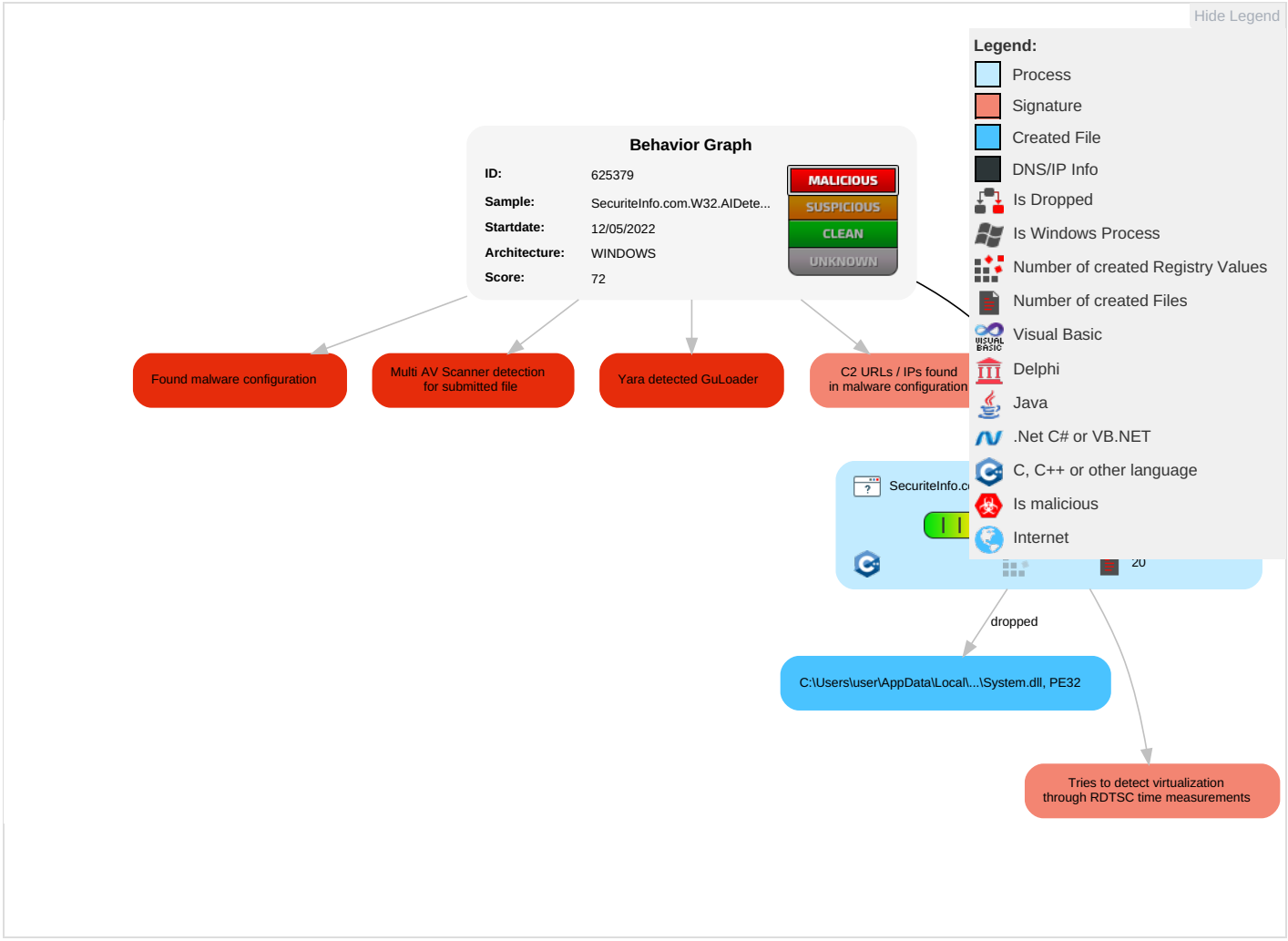
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

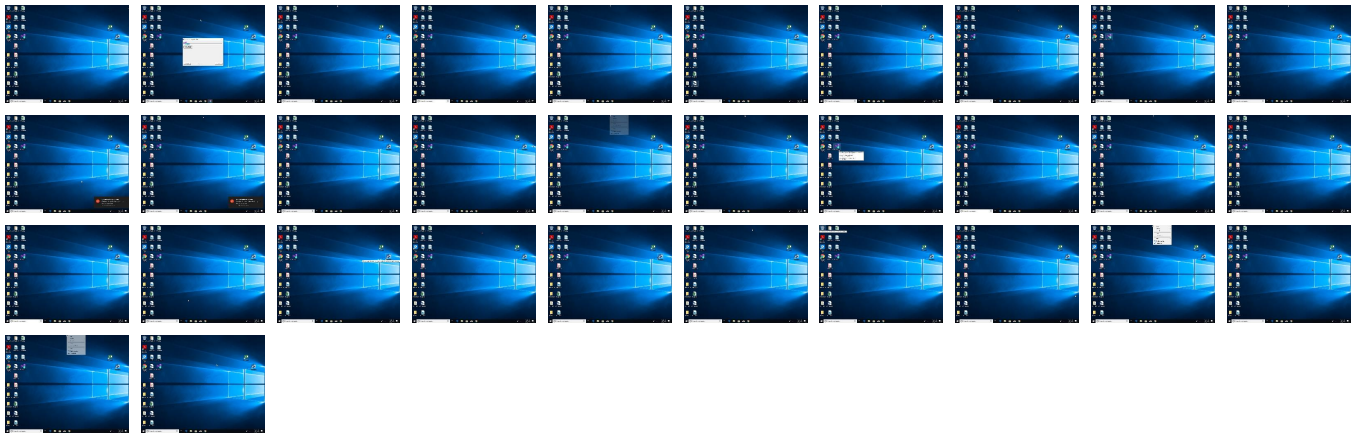
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	13%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	7%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625379
Start date and time: 12/05/202216:57:14	2022-05-12 16:57:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.8516.26511 (renamed file extension from 26511 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.2% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Aftapningers.unc

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe
File Type:	data
Category:	dropped
Size (bytes):	164654
Entropy (8bit):	7.328477148984372
Encrypted:	false
SSDEEP:	3072:0OjNBC83H7WOOnQkvcWeC4tQMrbfGPmSliWj1KYOcvH:0OjjCmH7bOnQkvczC4tjGOSlii1pOc/
MD5:	4F4AB714DFE3298940A65606E9D71F3D
SHA1:	ACAA9B62D1E2245695F551374C3B529AF49D378D
SHA-256:	B9E09B4CE4FD0A5A9AF776CD64CDAD0C1B06FDA01B479E93B9B202B9F2927F4B
SHA-512:	921B8C6651FABFA684E911A83439AC43D389F451B07430FF3F98CCD4E7616251C9835B1666039E506B7DABC0FE53EA388B7E0E42FE94D90E70690423838E987E
Malicious:	false
Reputation:	low
Preview:	4...5..`X..iSg.a$3;.....A.ZM...'.*uM...u.....=c}.+..3f...=a.ex&G.\}...K6..S....H.Dflv.~...5'a..+.3.',4..E..tk{#.]..-....#...}p. .k....[.&...H.GE.."....#Z..k$..`gG..@...&=sp...#./..C....R.-C.$.q...?.R.t.s.... B..1....7...Fm..q.#.|.i....WXV9.&.U].....w.`...nc.3.=r..[....x..EP.X.0_..J.(6....5h..|.>...$.NXZc..7.....d.,[..4.....{]...(....V-... .....Z...(et..t.!....r9+..3!.\}..q..e. .a~`T5.@..^TS..o.....HE....%....*ul=.si6.s.e.+...|C.a.k<v.'.<._@.O.....yZ...`...Q.. ...pd7....Pc...Fg...F<Z.....|.N.NW5..F.....Q!..%o.....I.T2.{.+T.'C..6.....u._nT.....:...*.>..h..VFM ...}...z"A.....".P..m.;V....._M..h)..yxjP.....sL(....x.x...2..|.....vu.c*[.....PHb....L...K.w2#[.oyu....jj....o...7.jU..G0U.,...W.1/Y.X...8\..aU6..k....|a2C)I..OYG.<.F.....<.+.B.M...W .I.6'..Q....JSU.&z...e...H./\....)...C.....-.....,>.Z.....m.....Z....._2.l..k.['.`..T....N..sb.!.v..Y.m.D..3..Q.<.E..6k0.r.wR..f..(gr>....s..FkAC.{,....TdK..u.q..D...llF....'....+..8..

C:\Users\user\AppData\Local\Temp\Extracontinental91.lnk

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide

Category:	dropped
Size (bytes):	876
Entropy (8bit):	2.9539437222480642
Encrypted:	false
SSDEEP:	12:8gl0URsXU1e/tz+7RafgKDNwpZlEg/rNJkKAh4t2Y+xIBjK:84+vaRMgKKXy45HAL7aB
MD5:	741C3F7F4826CD353D69ACC3942A9888
SHA1:	280625DAE84AE42F7B289E3D1C5656A6ED52C07B
SHA-256:	1366E655F303777243535B89C7D81C3812A78E8C792C1AE36DAEB46A1296E835
SHA-512:	3CD3833FA6F6C2C0F0968C769E547C053DEE9474DF79F2CDEFE2CA9498D09D04CBD9362BA08EE4EB213218FE347F9397B6EE6C1DD728ADA542E04772B9F8D EC
Malicious:	false
Reputation:	low
Preview:	L.....F.....3....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>..... .....a.l.f.o.n.s.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.. .....T.e.m.p.....l.2.....UNBLAZONED.exe..N.....U.N.B.L.A.Z.O.N.E.D...e.x.e.....\.U.N.B.L.A.Z.O.N.E.D...e.x.e.....(.... .....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.554007831073136
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.W32.AIDetect.malware2.8516.exe
File size:	253128
MD5:	90e91d605fb261fa827093074c0d7178
SHA1:	1737b52ca846659954692ac55235addf749e405b
SHA256:	4700f996868b461bae3a5b57efcd8719169d0c9acb400fa77d6a36787b37b0e1
SHA512:	e637de93126346d108bd7d7dbda163d2dd492be4645d6bd7e9f7d6af63de094d4839581009ea55b3387aaec8b74311d86f17332246d42e7418eba4b243a3d6cd
SSDEEP:	6144:qbE/HUKlmkDdr0OjjCmH7FOnQkvWqYlKPwjH25:qboFJHuc7FivWqNPwj25
TLSH:	C234D01E3661C0EAF88883751B3A9B0B2A9FBC07138219573771B7785B352D3D91E9D8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	8803969c49c2c3c0

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="gedske Bladring2 Germinates4 ", O=overcull, L=Sucy-en-Brie, S=ÃŽle-de-France, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/12/2022 2:38:46 AM 5/12/2023 2:38:46 AM
Subject Chain	• CN="gedske Bladring2 Germinates4 ", O=overcull, L=Sucy-en-Brie, S=ÃŽle-de-France, C=FR
Version:	3
Thumbprint MD5:	D0ACA7F1FD1382B9C35DFC16B627DDFD
Thumbprint SHA-1:	BDE2B99E0FDE745B68290E3A60150DFA90A8EE08
Thumbprint SHA-256:	EFD99FBE0F355D7F5157F6E6BC35D3ABB4549B7B947F6131A6F6EAFE73957876
Serial:	4F99C01EF8C999C6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx

Instruction
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F26DCAEE5AAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F26DCAEE57Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x68000	0x139f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3d650	0x678	.ndata
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x32000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x139f8	0x13a00	False	0.570984275478	data	6.55035103954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x68358	0x8592	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x708f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 1056964863	English	United States
RT_ICON	0x74b18	0x25a8	data	English	United States
RT_ICON	0x770c0	0x1a68	data	English	United States
RT_ICON	0x78b28	0x10a8	data	English	United States
RT_ICON	0x79bd0	0x988	data	English	United States
RT_ICON	0x7a558	0x6b8	data	English	United States
RT_ICON	0x7ac10	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x7b078	0x100	data	English	United States
RT_DIALOG	0x7b178	0x11c	data	English	United States
RT_DIALOG	0x7b298	0xc4	data	English	United States
RT_DIALOG	0x7b360	0x60	data	English	United States
RT_GROUP_ICON	0x7b3c0	0x76	data	English	United States
RT_VERSION	0x7b438	0x280	data	English	United States
RT_MANIFEST	0x7b6b8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Schenklensc
FileVersion	24.1.20
CompanyName	Lipoclasisbi233
LegalTrademarks	Theophilanthro36
Comments	Noteform
ProductName	Beignetdeje162
FileDescription	Guatemalan
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.8516.exe PID: 6984, Parent PID: 4368

General

Target ID:	0
Start time:	16:58:26
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe"
Imagebase:	0x400000
File size:	253128 bytes
MD5 hash:	90E91D605FB261FA827093074C0D7178
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.955923216.00000000028B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsdAC87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	9	406059	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Aftapningers.unc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	6	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsdAC87.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsiAD43.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\Aftapningers.unc	0	16379	34 fd fd fd 35 fd 16 60 58 01 fd 69 53 67 11 61 24 33 3b fd fd 19 1a 1d 14 41 fd 5a 4d 0b fd fd 27 fd 2a 75 4d fd 1d fd 75 2e fd 14 fd 2e fd 3d 63 7d fd 2b ae 09 33 66 7f fd fd 3d 61 fd 65 78 26 47 fd 5c 7d fd fd fd 4b 36 fd fd 53 fd 0e fd fd 48 fd 44 66 6c 76 fd 7e fd fd fd 35 27 61 fd fd 2b fd 33 fd 27 2c 34 fd fd 45 16 fd 74 6b 7b 23 fd 5d fd 07 2d fd fd fd 23 fd fd fd 7d 70 05 20 18 6b fd 05 15 fd 5b fd 26 fd fd 09 48 fd 47 45 fd fd 22 fd 67 fd fd 23 5a 1f a7 6b 24 fd 0e 60 67 47 fd fd 40 05 04 fd 26 3d 73 70 fd 0e fd 23 fd 05 2f fd fd 43 0f fd fd 0f 52 fd 2d 43 fd 24 0e 71 fd fd 03 3f 13 52 fd 74 0d 73 fd fd fd 12 20 42 fd fd 31 05 fd 08 fd 37 fd 7f fd 46 6d fd fd 71 23 fd 7c fd 69 fd fd fd fd 57 58 56 39 fd 26 fd	45`XiSga$3;AZM'*uMu..=c}+3f=aex&G\}K6SHDflv~5'a+3',4Etk{#]-#}pk[&HGE"#Zk$`gG@&=sp#/CR-C$q?RtsB17Fmq#|iWXV9&	success or wait	8	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	unknown	512	success or wait	233	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.8516.exe	unknown	4	success or wait	11	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Aftapningers.unc	unknown	1048576	success or wait	1	72EF2C59	ReadFile

Disassembly

No disassembly