ID: 562499
Sample Name: 9TpV4rfMmJ
Cookbook: default.jbs
Time: 22:58:03
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

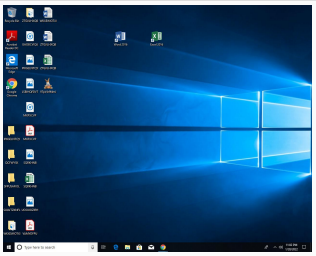
Windows Analysis Report

9TpV4rfMmJ

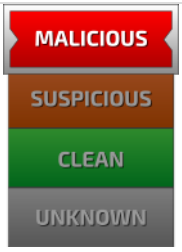
Overview

General Information

Sample Name:	9TpV4rfMmJ (renamed file extension from none to exe)
Analysis ID:	562499
MD5:	38034f18af511c3..
SHA1:	797252e9139d3d.
SHA256:	7babdd2c7d3752..
Tags:	32 exe trojan
Infos:	



Detection



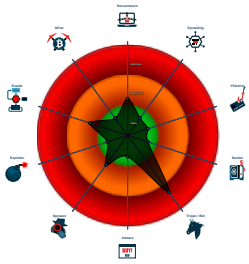
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to read the PE…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- 9TpV4rfMmJ.exe (PID: 4500 cmdline: "C:\Users\user\Desktop\9TpV4rfMmJ.exe" MD5: 38034F18AF511C3B04B25170735E8B8E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://www.konutmarket.com/2022file_iz"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1182087160.00000000027F0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

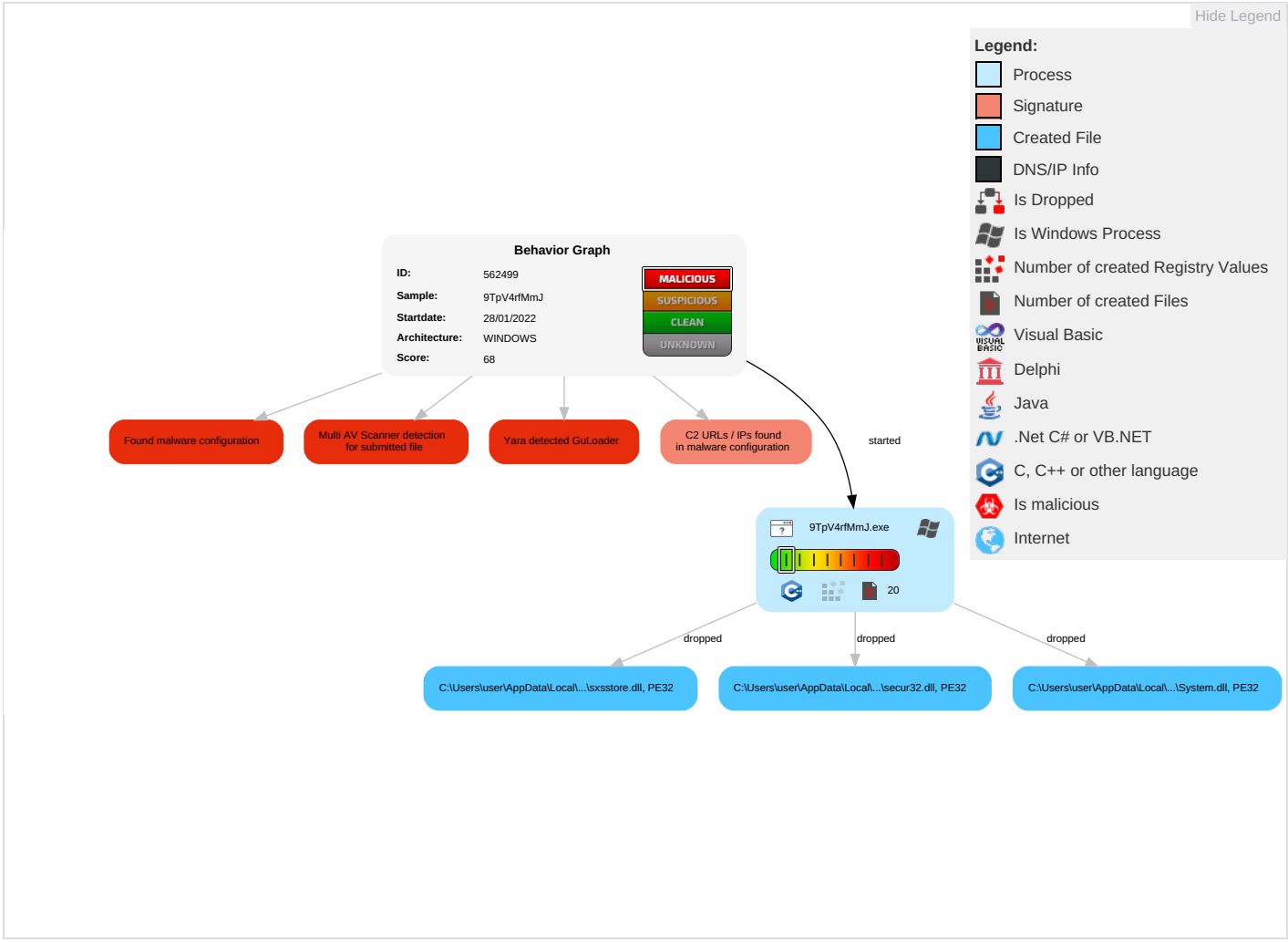
Data Obfuscation

Yara detected GuLoader

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 Timestomp	LSASS Memory	2 File and Directory Discovery	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)	1 Obfuscated Files or Information	Security Account Manager	3 System Information 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

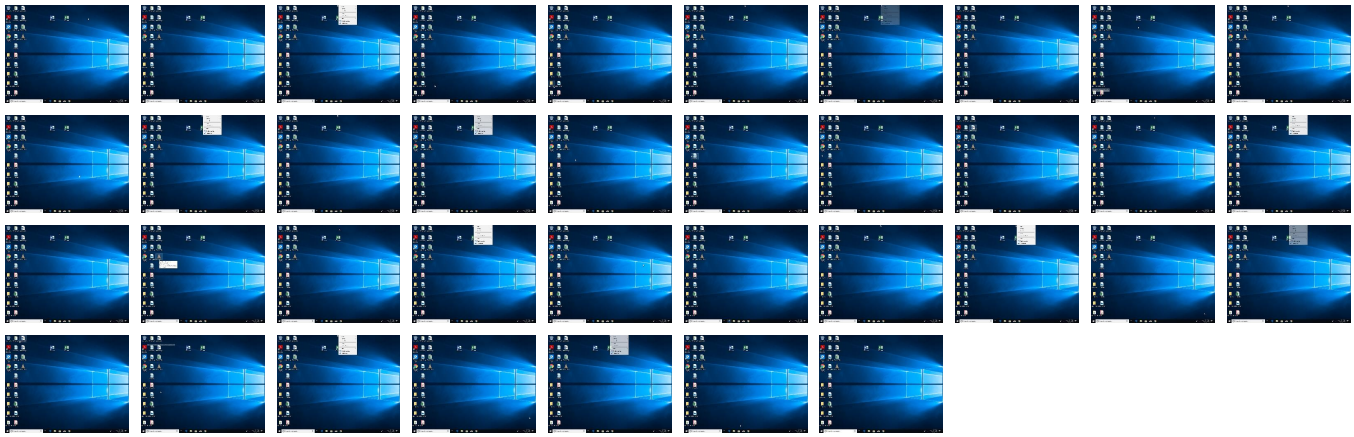
Behavior Graph



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
9TpV4rfMmJ.exe	25%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsd3616.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsd3616.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.konutmarket.com/2022file_iz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.konutmarket.com/2022file_iz	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	9TpV4rfMmJ.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562499
Start date:	28.01.2022
Start time:	22:58:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9TpV4rfMmJ (renamed file extension from none 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:	17
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:	mal68.troj.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 26.5%) • Quality average: 88.3% • Quality standard deviation: 21%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 204.79.197.222
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fp.msedge.net, a-0019.a-msedge.net, store-images.s-microsoft.com, a-0019.standard.a-msedge.net, ctldl.windowsupdate.com, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- VT rate limit hit for: 9TpV4rfMmJ.exe

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\nsd3616.tmp\System.dll

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.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: 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..... ....

C:\Users\user\AppData\Local\Temp\racehorse.dat

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	data
Category:	dropped
Size (bytes):	63168
Entropy (8bit):	6.498454279155086
Encrypted:	false
SSDEEP:	1536:TsB1Fc6jtZl4FMiQMaFIdINIK6SaUf6ROv:TsB1Fc6+uiXaFoINJ8mv
MD5:	D65C77AD010482FBF9F7983146D0A6B5
SHA1:	8400E92DA91E588A3CF2C9C419CB4BAB2CA60B7C
SHA-256:	F4BAA8F8FC7D5DF13DC487345B430C8733C59C0D37DD5E5462FBBD33945E724D
SHA-512:	55849D60E498EB6F39D7B629F9426B4DF7EB25A882B07C5A7E9FD288B1E7E245FB5A8839E434238EF026DFCD11C378AD8C91C12FC0659A66A5D4C2B1DFE169 E
Malicious:	false
Reputation:	low
Preview:	9....._8.f9..?.u...f9.....u...9.....u...9.9.....9.....;.xf9.....e.p.....r9.8....@l9.9....x<.8.8.. 3L9...W.....Z9.9.1.9...4..{<)9.f9....f9...9.u..9.Wf9.9...9.8..K...Yx=).y.0....T.\...N ...Q'.G..S..0\.....v..R#.B.`..=.f....c.....73t.C-.{!u0.....;...P.....poa.9...:..q.....^.>..7.....A.....^..2;.L....%....r(....G.M...2.(&.....$.n.W;..3...8n..w ..F..B}...[GEl3..7.(tv....d[K.....[W.....Z.i.....B..... .....\.2M.....5.....[K.....4..... .....[M.s8..mC....km.&.....

C:\Users\user\AppData\Local\Temp\secur32.dll

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	5.575148216618883
Encrypted:	false
SSDEEP:	384:A9zuL7jiVVvNORNHzTdXaP4osxlUoLYuC/NWiOCW:A8zc2RJdqP4oLoQ/8
MD5:	E1FA0E4751888A35553A93778A348A24
SHA1:	98667AE0AB2D955E69C365D62F2DD1A8C839E14E
SHA-256:	A074AA8C960FF9F9F609604DB0B6FEFDD454CEB746DE6749753A551FE7B99B51
SHA-512:	E93E62CC3FFBC2621FD87BD6DAEDF3699799217B49A006D4A891CDBFE4DD89B33DA258C6A4D8CC28FF615CC0F033D83BF761502169D05A6FC9CBC5FF5FC2/ BF1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...p...p...p...y.7.d...d...s...p...K...d...v...d...q...d...v...d.[.q...d...q...Ri chp.....PE..L.....!.....<..... .....P.....Q.....@E.....P3.....`.....X...`...T.....`.....1..... .....text...~;.....<..... ..`.data...8....P.....@.....@....idata..D....`.....D.....@..@.didat..0....p.....N.....@....rsrc.....P.....@..@.reloc.. X.....V.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sxsstore.dll

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	6.138116359523764
Encrypted:	false
SSDEEP:	384:4j1Pm6AenqNEb9jGvRtb30lEVybDPukC+Rfb6ql4PrxWpmWZr:xlMsP4l2ybJawRr
MD5:	3F305E85F2751C4AA1A4EFDF3240EDA6
SHA1:	FBD849B83E98E5D0F2A2B2F8E3649ADA7078B2E9
SHA-256:	95444BF7752F9092FE00CA6F96FD170820026ED990B1EA59CE34524978B4EB12

SHA-512:	3BC1B150ACC164818C169448E7BCD8BEC7780278E60581E3A21722BE947BDF6016D7A99FB1F06E59057F71A3C965CD882CA974EAF288172D5285B1CEA93769C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.I...'..'..'.....'...$...'...#...'...&.B.'...&...'...''...'..'..'.....'.....'...%.. .'.Rich..'.....PE..L.....{.....!....B.....pH.....`.....P....@A.....PQ.....(q.....T.....h..... ....p..$.....text....A.....B..... ..`.data.....`.....F.....@....idata.....p.....H.....@..@.rsrc.....R.....@..@.reloc.....V..... .@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.481059066220283
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:	9TpV4rfMmJ.exe
File size:	166200
MD5:	38034f18af511c3b04b25170735e8b8e
SHA1:	797252e9139d3d46825440335437ad9d538f6b5b
SHA256:	7babdd2c7d3752b7b48729110f0ab94de7cf74c478b7e1ea7a71a468748e70c0
SHA512:	da2ce49e148bc8877d391316d785a067083ebdf0884b9389f2e3db6b71f6e3269fed55d39a1a4557db1e628316abf50e520594d8b5a416c7535003f963d7038c
SSDEEP:	3072:cbG7N2kDTHUpou0lvStHlquLNLbzKhBvOQsn7DdTAk5RmIdaDm2ghplP:cbE/HUMFSeK+hYQsn7CXIoDyhpl
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:	e4fa3cf8888c88ce

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:	E=SANITISED@FILKOPIERINGS.Ans, CN=Knallerter4, OU=misarranged, O=Nonsecretory, L=Tllede6, S=melange, C=WS
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	• 1/28/2022 6:43:20 AM 1/28/2023 6:43:20 AM
Subject Chain	• E=SANITISED@FILKOPIERINGS.Ans, CN=Knallerter4, OU=misarranged, O=Nonsecretory, L=Tllede6, S=melange, C=WS
Version:	3
Thumbprint MD5:	C6282834878BB7165E5E606019677AD2
Thumbprint SHA-1:	8BB39E8EE588FA14DEED258E56A6E9A51D4F2730
Thumbprint SHA-256:	B7F1E132885ECBE632DEEACE43B09D8AAF984C146DB830BD5ACA8C82BCBE7D89
Serial:	00

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
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FA958BF187Ah
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 00007FA958BF184Ah
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

Instruction
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	0x4c000	0xd5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x274d0	0x1468	.data
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	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xd5c8	0xd600	False	0.704731308411	data	6.81165454669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c3b8	0x669e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x52a58	0x25a9	data	English	United States
RT_ICON	0x55008	0x10a9	data	English	United States
RT_ICON	0x560b8	0xea9	data	English	United States
RT_ICON	0x56f68	0x8a9	data	English	United States
RT_ICON	0x57818	0x669	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 251721983, next used block 4294967295	English	United States
RT_ICON	0x57e88	0x569	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x583f8	0x469	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x58868	0x2e9	data	English	United States
RT_ICON	0x58b58	0x129	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x58c88	0x100	data	English	United States
RT_DIALOG	0x58d88	0x11c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x58ea8	0xc4	data	English	United States
RT_DIALOG	0x58f70	0x60	data	English	United States
RT_GROUP_ICON	0x58fd0	0x92	data	English	United States
RT_VERSION	0x59068	0x220	data	English	United States
RT_MANIFEST	0x59288	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	Alidas
FileVersion	1.2.1
CompanyName	Alida
LegalTrademarks	Alida
Comments	Alida
ProductName	Alida
FileDescription	Alida
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: 9TpV4rfMmJ.exe PID: 4500, Parent PID: 6028

General

Target ID:	0
Start time:	22:58:56
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9TpV4rfMmJ.exe"
Imagebase:	0x400000
File size:	166200 bytes
MD5 hash:	38034F18AF511C3B04B25170735E8B8E
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: 00000000.00000002.1182087160.00000000027F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

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\nsh3327.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\racehorse.dat	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\secur32.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\sxsstore.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\nsd3616.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\nsd3616.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\nsd3616.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\nsd3616.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh3327.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsd3616.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\racehorse.dat	0	22198	39 fd fd fd fd 00 00 00 5f 38 fd 66 39 fd fd 3f fd 75 1b fd fd 66 39 fd fd 7f 03 00 75 10 fd fd 39 fd fd 7f 04 00 75 06 fd fd 39 fd 39 fd fd fd 00 03 00 00 fd fd 39 fd fd fd 12 02 00 00 fd 3b 13 78 66 39 fd fd 41 fd fd 65 fd 70 fd fd fd 41 fd fd 1d fd 72 39 fd 38 c1 fd fd 11 40 6c 39 fd 39 fd fd fd fd 78 3c fd 38 fd 38 c1 f6 20 33 4c 39 fd fd fd 57 fd fd 12 02 00 00 fd fd fd fd 5a 39 fd 39 fd 31 fd 39 fd fd 41 34 07 fd 7b 3c 29 39 fd 66 39 fd fd fd 04 66 39 fd fd fd 39 fd 75 fd fd 39 fd 57 66 39 fd 39 fd fd fd 39 fd 38 fd fd 4b fd fd fd 59 78 3d 29 fd 79 fd 30 fd fd 9e 01 54 fd 5c fd 88 05 4e fd fd 7f 51 27 fd 47 0b fd 53 03 fd 30 5c fd fd fd fd fd fd fd 76 0e fd 52 23 fd 42 0d 60 fd fd 3d fd 66 fd 1e 1d fd 63 fd fd 0a	9_8f9? uf9u9u999;xf9epr98@l99 x<88 3L9WZ99194{<)9f9f99u9 Wf9998 KYx=)y0T\NQ'GS0\vR#B `=fc	success or wait	3	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\secur32.dll	0	23040	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 34 fd fd fd 70 fd fd fd 70 fd fd fd 70 fd fd fd 79 fd 37 fd 64 fd fd fd 64 fd fd fd 73 fd fd fd 70 fd fd fd 4b fd fd fd 64 fd fd fd 76 fd fd fd 64 fd fd fd 71 fd fd fd 64 fd fd fd 76 fd fd fd 64 fd 5b fd 71 fd fd fd 64 fd fd fd 71 fd fd fd 52 69 63 68 70 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 14 00 3c 00	MZ@!L!This program cannot be run in DOS mode.$4pppy7ddspKdvd qdvd[qdqRichpPEL!<	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0	23040	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 4f fd 49 fd 0b fd 27 fd 0b fd 27 fd 0b fd 27 fd 02 fd fd fd 0f fd 27 fd 1f fd 24 fd 0a fd 27 fd 1f fd 23 fd 06 fd 27 fd 0b fd 26 fd 42 fd 27 fd 1f fd 26 fd 00 fd 27 fd 1f fd 22 fd 09 fd 27 fd 1f fd 27 fd 0a fd 27 fd 1f fd 2e fd 05 fd 27 fd 1f fd 13 0a fd 27 fd 1f fd 25 fd 0a fd 27 fd 52 69 63 68 0b fd 27 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$OI""$'#'&B'& """."%'Rich'PEL	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsd3616.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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9TpV4rfMmJ.exe	unknown	512	success or wait	181	4060CA	ReadFile
C:\Users\user\Desktop\9TpV4rfMmJ.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\9TpV4rfMmJ.exe	unknown	4	success or wait	10	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\racehorse.dat	unknown	63168	success or wait	1	6FC52C59	ReadFile

Disassembly

⊘ **No disassembly**