



ID: 559536
Sample Name: SdEkI4IDqd.exe
Cookbook: default.jbs
Time: 13:18:52
Date: 25/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SdEkI4IDqd.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: GuLoader 3
Yara Overview 3
Memory Dumps 3
Sigma Overview 3
Jbx Signature Overview 4
AV Detection 4
Networking 4
Data Obfuscation 4
Malware Analysis System Evasion 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
C:\Users\user\AppData\Local\Temp\OVERROMANTICIZED.dat 8
C:\Users\user\AppData\Local\Temp\gamer.txt 9
C:\Users\user\AppData\Local\Temp\nsv7EA4.tmp\System.dll 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 10
Rich Headers 11
Data Directories 11
Sections 12
Resources 12
Imports 12
Version Infos 13
Possible Origin 13
Network Behavior 13
Statistics 13
System Behavior 13
Analysis Process: SdEkI4IDqd.exePID: 5912, Parent PID: 5316 13
General 13
File Activities 14
File Created 14
File Deleted 15
File Written 15
File Read 16
Disassembly 16

Copyright Joe Security LLC 2022

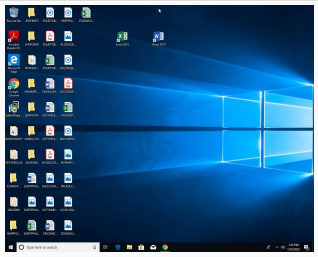
Windows Analysis Report

SdEkI4IDqd.exe

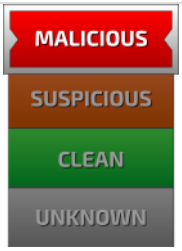
Overview

General Information

Sample Name:	SdEkI4IDqd.exe
Analysis ID:	559536
MD5:	003a7c37f9c06d…
SHA1:	a847ef8c72d267..
SHA256:	4f29b22b6b787b..
Tags:	exe signed
Infos:	



Detection



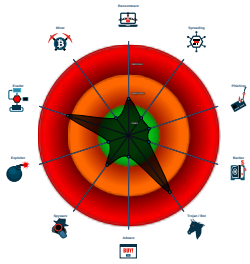
GuLoader

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
- Drops PE files
- Contains functionality to read the PE…
- 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**
- SdEkI4IDqd.exe (PID: 5912 cmdline: "C:\Users\user\Desktop\SdEkI4IDqd.exe" MD5: 003A7C37F9C06D75AAAA6F9B25DC3C41)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://dariamob.ro/wed/eee_XScUCMEVL47.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.823231609.0000000004300000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2022

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

Malware Analysis System Evasion

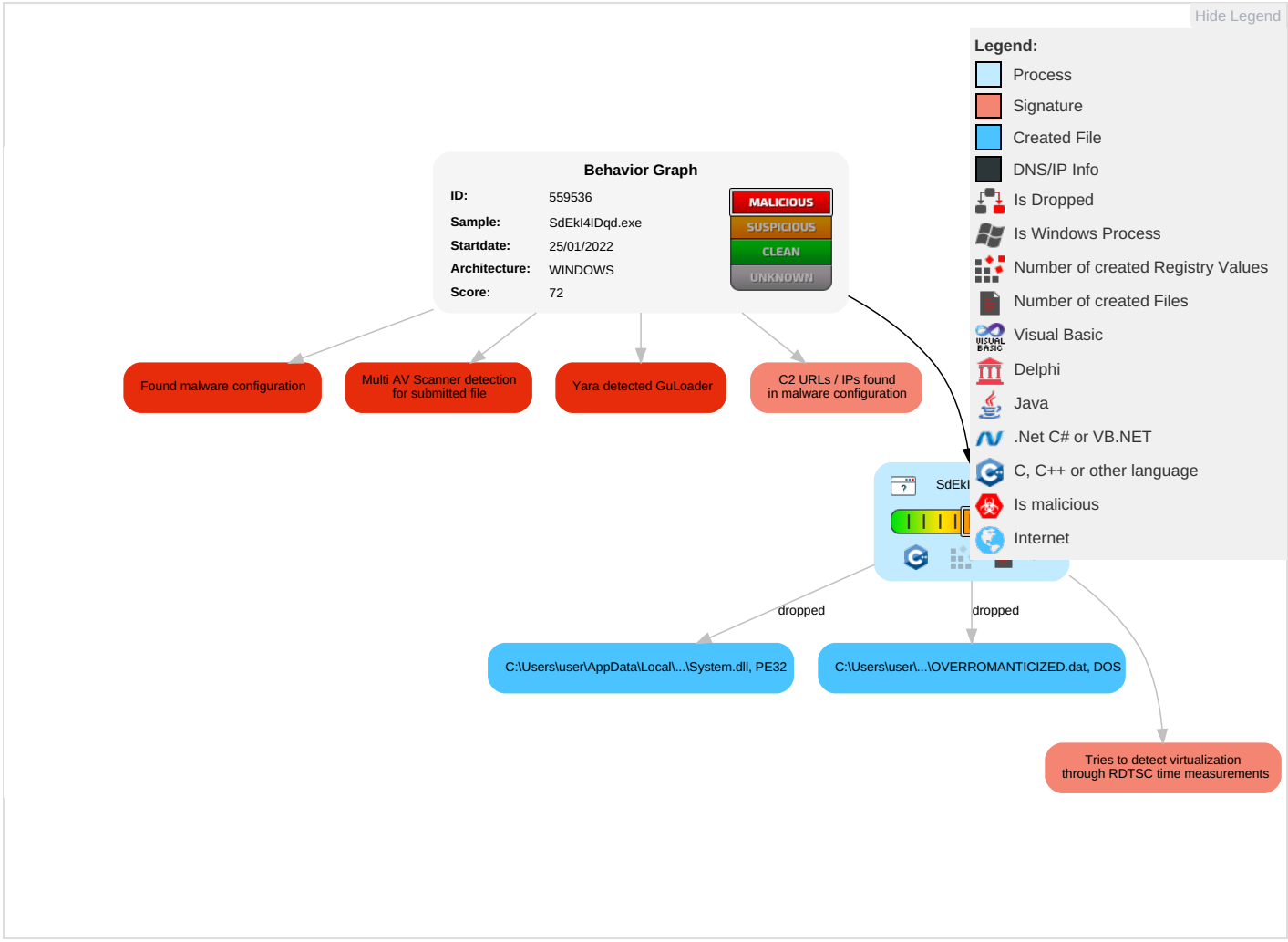


Tries to detect virtualization through RDTSC time measurements

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 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	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)	Obfuscated Files or Information	Security Account Manager	1 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

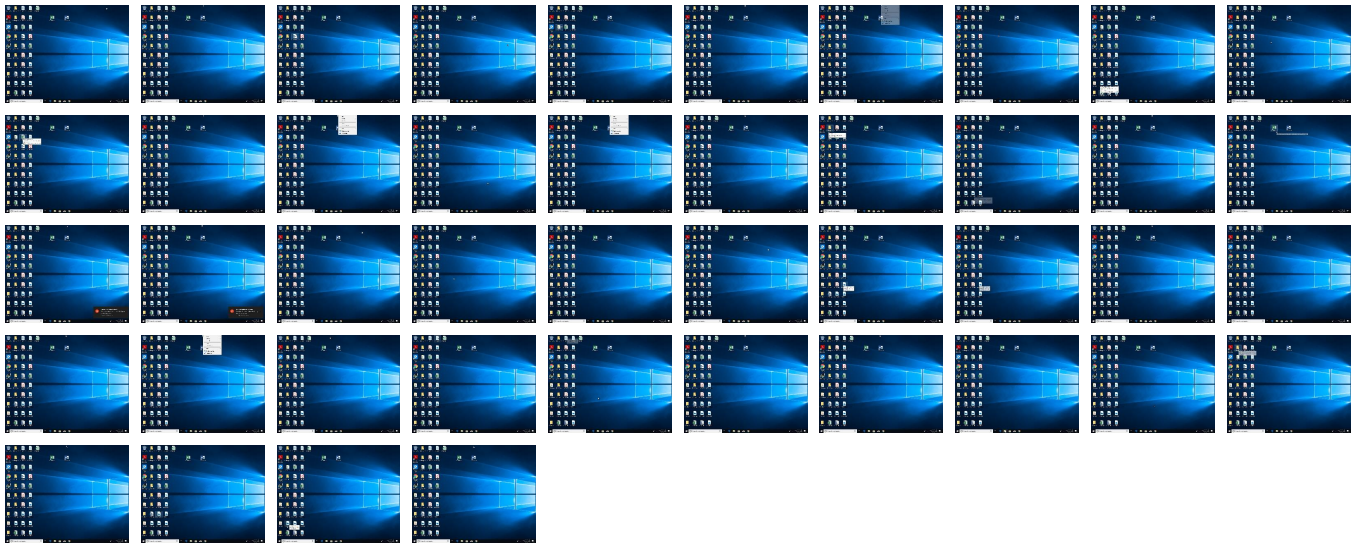
Behavior Graph



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
SdEkI4IDqd.exe	6%	Virustotal		Browse
SdEkI4IDqd.exe	12%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsv7EA4.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsv7EA4.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsv7EA4.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://dariamob.ro/wed/eee_XScUCMEVL47.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dariamob.ro/wed/eee_XScUCMEVL47.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SdEkI4IDqd.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	559536
Start date:	25.01.2022
Start time:	13:18:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SdEkI4IDqd.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:	20
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: 39.9% (good quality ratio 39.3%) • Quality average: 86.9% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2022

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\OVERROMANTICIZED.dat

Process:	C:\Users\user\Desktop\SdEkI4IDqd.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	36366
Entropy (8bit):	7.621225978231947
Encrypted:	false
SSDEEP:	768:RcwJQKlTyjsiu4sY3Hs4bvuSyEXCjYL7XoaFZLkcszAI:a+FlOoiuJYMS2SyEyULTZI
MD5:	448942A62FED29DEF36D74EECFE7D736
SHA1:	4312E7D4BE729BF6200A1F87C1C84391CF0706F3
SHA-256:	87ADB3A77D22DD8C88F4900513775B411512F1964EBAC4DD4354554B4C36A68E
SHA-512:	3DC538388099228A260F1F48F50F713C9A476EE1E23F70F50A6D1758456E6024CA34DC17291A47E65A7F347BAA287DE36EEAB5548768EB3FE94E10DE03E4FFEE
Malicious:	false

Reputation:	low
Preview:	.__.?.u.....u.....u.....O4|..J.YH.. elC..\<.....+..0.0R.....Z1..4..,.%....9.u.W.....%.}"M.jB .d..+.3...O..Tl.T....=\...,5..M...|...._.I.4.v..K....gl.rs....s...$...dD.P.~...#...N.0.+}D. ...n.....J..t5D.cU).m..<.$...X..]{.C....4K...;<..Z...u....H.^.#.a..B....p@.{d..v.z...-...mS.G.i...*...G.9."jM....g.....]C...w..C(.`...C.....Y..{.y.|...h..P..y..`.h.Y.....*.....p(...:$.,.%.,>....%.. ...Ca.YB.....,`..Y.Th>..Kc%.D....."|...%.1..W...("P.x..yz.%.i.....\0..e....E.%.i.C..`..K9.....L,,...,.%.t.%...=I..],...L`...`...*.5.%.MW..T.%.F....%..{..,...h"-'...X"-.q.u.X"-/.H.X"-..... ..:=kk.'qd.....n.....%.V...5g....$bs).....0..Q.."....1*..J...t=&...$.,..1.e.....U..m.....v...}...-.%yOH>.DiS.!5D..$.2.........x.h..."U.....(...*....GyuKZj....,.....$.............E....".Y...[.A....,.. 8.IM.Z.|...$.,....Q...?....&)...j.y~...-.%y..Y.D..7...5a.C..*...D6.("q.-.M.8...*',.c-...../...f:.;..[wt1z..=..%.......L...N-.K..M...ny.*.d."......5"H._...~8...

C:\Users\user\AppData\Local\Temp\gamer.txt

Process:	C:\Users\user\Desktop\SdEkI4IDqd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOk6soHG6Nun3UPBApXPE8eMag91APl7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A
SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5(
Malicious:	false
Reputation:	low
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1I3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8 otpHEpw0OGDSzOwMl9VCfHuXXhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGN0toQLHc2vjrb52VFWESFWMUHsKSZfQ4PbqkiII zeyLOvDdo44fuucajegzqku9brw7f8p9R2zFXqooBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdGfPhd7dzPgYFxqUkZaqo2ckBxUeh3QLr4p 1ievUUewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrvrU2YzKVhY5ajHSj55DsIeOSl066y24ayag5YtldIsnpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wIpTCqM6CfIHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaoIfCjrIqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBa58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJDr5HYJN0ESkrvn77s4vH90F55tPEmd6Z jNInCzW2BOZfhfO10qNfHa7ZhuyiWVIf05P6uzThDVcRpFtIjVTvGctBTjxS6LEiUlof2CsVigpyEGuXekSTdPsfIqGf5sMzKcxKlDJc6mtYp7gIqQODeycT

C:\Users\user\AppData\Local\Temp\nsv7EA4.tmp\System.dll

Process:	C:\Users\user\Desktop\SdEkI4IDqd.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):	7.540130212507592
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:	SdEkI4IDqd.exe

File size:	97752
MD5:	003a7c37f9c06d75aaaa6f9b25dc3c41
SHA1:	a847ef8c72d26731963b189caff925a8a757d563
SHA256:	4f29b22b6b787babc2f984172f8ae0e3999b7621aeb6775ce023f2ef5db0b2e7
SHA512:	4067ddae5bdf8f620d1cf1673536a8383664fd47a2b6bb0f7932eb005e43fdf0c5269d0f84a9aef6afd215bddbcc1536584216d07179a1bb66bb3f7645b0f1a2
SSDEEP:	1536:K/T2X/jN2vxZz0DTHUpouZZbnneGmqJdg9i6/g7ld317J1H8k29xE+19+coGd:KbG7N2kDTHUpouZZbnnnJdl11T4Pd
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:	b2a88c96b2ca6a72

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=Blosteret@HOVEDPUNKT.fl, CN=Tallowed4, OU=SEKSUALFORBRYDERES, O=Fiorin, L=Nonlyrically, S=CARPOPTOSIS, C=CN
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	• 1/25/2022 1:49:28 AM 1/25/2023 1:49:28 AM
Subject Chain	• E=Blosteret@HOVEDPUNKT.fl, CN=Tallowed4, OU=SEKSUALFORBRYDERES, O=Fiorin, L=Nonlyrically, S=CARPOPTOSIS, C=CN
Version:	3
Thumbprint MD5:	80D66677069923CF4D67981C0E1FBA70
Thumbprint SHA-1:	E8B77C74D42CA6EC42A14CF926CC0D402018DB27
Thumbprint SHA-256:	CF9CD9DC0548C1F076D43ECBF2CD2398423AE538B83271032EEBA04757E6E5E1
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

Instruction
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 00007F71B8C025BAh
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 00007F71B8C0258Ah
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	0x4c000	0xe28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x16968	0x1470	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Is in Section
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	0xe28	0x1000	False	0.378662109375	data	4.00654037497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c208	0x2e8	data	English	United States
RT_DIALOG	0x4c4f0	0x100	data	English	United States
RT_DIALOG	0x4c5f0	0x11c	data	English	United States
RT_DIALOG	0x4c710	0xc4	data	English	United States
RT_DIALOG	0x4c7d8	0x60	data	English	United States
RT_GROUP_ICON	0x4c838	0x14	data	English	United States
RT_VERSION	0x4c850	0x294	data	English	United States
RT_MANIFEST	0x4cae8	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

Copyright Joe Security LLC 2022

DLL	Import
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	Lesney Products
FileVersion	1.2.1
CompanyName	Lesney Products
LegalTrademarks	Lesney Products
Comments	Lesney Products
ProductName	Lesney Products
FileDescription	Lesney Products
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: SdEkI4IDqd.exe PID: 5912, Parent PID: 5316

General

Target ID:	1
Start time:	13:19:53
Start date:	25/01/2022
Path:	C:\Users\user\Desktop\SdEkI4IDqd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SdEkI4IDqd.exe"
Imagebase:	0x400000
File size:	97752 bytes
MD5 hash:	003A7C37F9C06D75AAAA6F9B25DC3C41
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: 00000001.00000002.823231609.0000000004300000.00000040.00000800.00020000.00000000.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\nsp7CAF.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\OVERROMANTICIZED.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\gamer.txt	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\nsv7EA4.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\nsv7EA4.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\nsv7EA4.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\nsv7EA4.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\nsp7CAF.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsv7EA4.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\OVERROMANTICIZED.dat	0	18031	fd 5f 5f fd 3f fd 75 0e fd 7f 03 00 75 08 fd 7f 04 00 75 02 fd c1 fd 00 03 00 00 fd fd fd 01 00 00 fd fd 4f 34 7c fd fd 4a fd 59 48 fd fd 20 65 6c 43 fd fd 5c 3c fd fd fd 15 fd 2b 41 fd 30 fd 30 52 fd fd fd 01 00 00 5a 31 fd fd 34 07 11 2c 06 25 fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd fd fd fd 06 25 11 7d 22 4d fd 6a 42 20 fd 64 fd fd 2b fd 33 fd 15 fd 4f 19 0f 54 6c fd 54 fd fd fd 13 3d 5c fd fd fd 2c 35 fd fd 4d fd 1c 7b 7c fd fd fd fd 5f 00 49 fd 34 0d 76 fd fd 4b fd 08 19 fd 67 49 fd 72 73 fd fd 7f fd 73 02 fd 01 24 fd 1c fd 64 44 fd 50 fd 7e fd 0e fd 23 fd fd 1e 4e fd 30 fd 2b 7d 44 fd 1a fd 0b 6e 08 fd fd fd fd fd 4a 15 fd 74 35 44 fd 63 55 29 fd 6d fd fd 3c fd 24 fd 02 fd 58 10 18 5d 7b fd 43 fd fd fd 04 34 4b fd fd fd 3b	__?uuuO4|JYH elC\ <+00RZ14,%9uW%}"MjB d+3OTlT=\,5M|_l4vKgIrss $dDP~#N0+}DnJt5DcU) m<$X]{C4K;	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gamer.txt	0	16555	45 4d 72 38 74 30 48 68 71 37 31 35 52 51 6a 70 56 38 6c 39 4c 6f 6f 55 64 57 4a 67 4d 74 4d 66 32 70 45 38 33 55 32 77 73 73 73 38 31 47 35 4b 4a 46 4c 65 49 58 4d 61 31 54 39 33 48 47 6a 4e 45 62 46 66 79 34 49 52 61 57 6a 63 74 45 48 31 49 33 68 57 47 37 34 77 73 4a 59 64 5a 58 4e 6d 4c 54 71 54 65 6e 76 67 65 63 38 71 70 75 39 38 5a 70 34 58 6c 72 72 41 68 62 75 56 65 50 42 67 35 6e 78 4d 65 6f 78 49 6f 6a 67 6c 4f 75 4a 41 76 41 5a 65 66 30 4e 61 6b 37 67 6d 30 69 78 38 78 53 45 37 30 51 65 46 4a 4d 46 6a 4a 76 45 41 57 52 46 46 46 74 5a 4f 59 6b 63 48 68 43 67 65 77 70 37 59 42 45 38 4f 65 6b 4f 73 4f 72 63 65 78 61 66 52 47 34 41 64 5a 61 57 42 7a 33 79 43 45 34 71 4d 50 30 4e 41 63 78 4a 34 44 48 65 43 64 7a 62 63 36 68 57 38 69 38 6f 74 70 48 45	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1I3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5nxMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8otpHE	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsv7EA4.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