ID: 755473
Sample Name: 6culQoI97a.exe
Cookbook: default.jbs
Time: 18:32:09
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 6culQoI97a.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
AV Detection 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 7
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 7
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\Microsoft\Windows\INetCache\Bracker\Feberkosten\Lavkonjunkturen.pro 8
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice\Grabbers145.Scu187 8
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\UrationeIt\call-missed-symbolic.svg 9
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll 9
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Rich Headers 11
Data Directories 11
Sections 12
Resources 12
Imports 12
Possible Origin 13
Network Behavior 13
Statistics 13
System Behavior 13
Analysis Process: 6culQoI97a.exePID: 5172, Parent PID: 3452 13
General 13
File Activities 14
File Created 14
File Deleted 16
File Written 16
File Read 17
Registry Activities 17
Key Created 17
Key Value Created 18
Disassembly 18

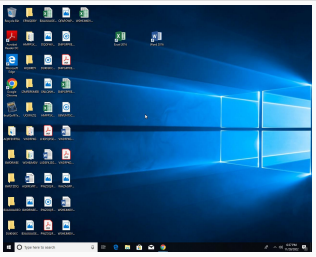
Windows Analysis Report

6culQoI97a.exe

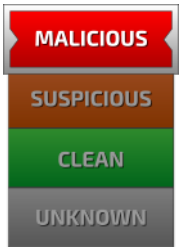
Overview

General Information

Sample Name:	6culQoI97a.exe
Analysis ID:	755473
MD5:	d9aa122b8c3944..
SHA1:	0175baf7a240c2..
SHA256:	317b5db72d7c43..
Tags:	exe
Infos:	



Detection

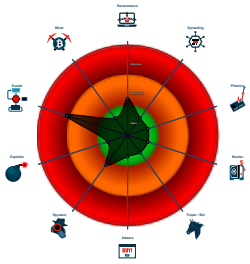


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Tries to detect virtualization through…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- 6culQoI97a.exe (PID: 5172 cmdline: C:\Users\user\Desktop\6culQoI97a.exe MD5: D9AA122B8C39444799E60EABBAB69502)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

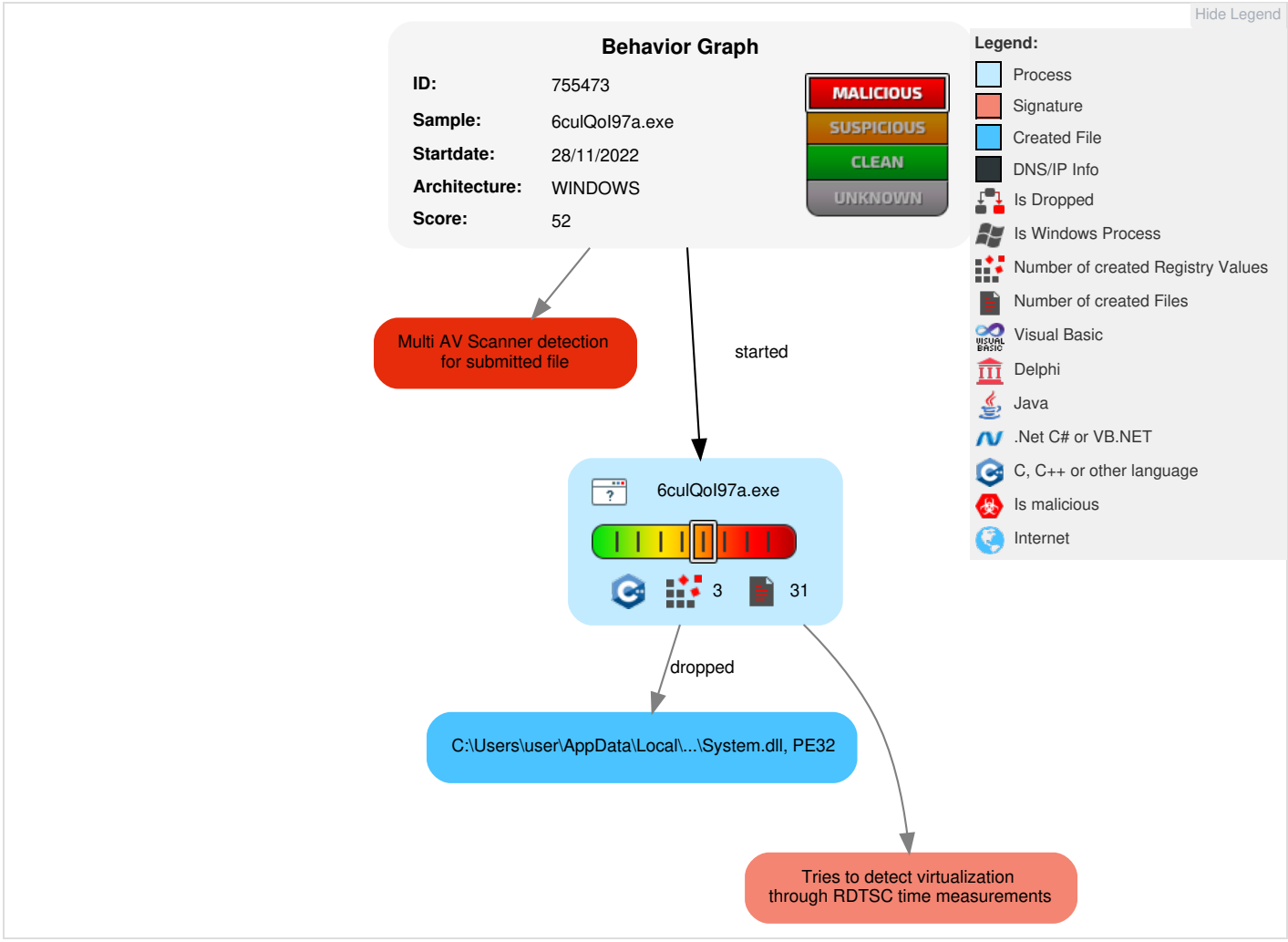
Malware Analysis System Evasion

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 1 Masquerading	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 Access Token Manipulation	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	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	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

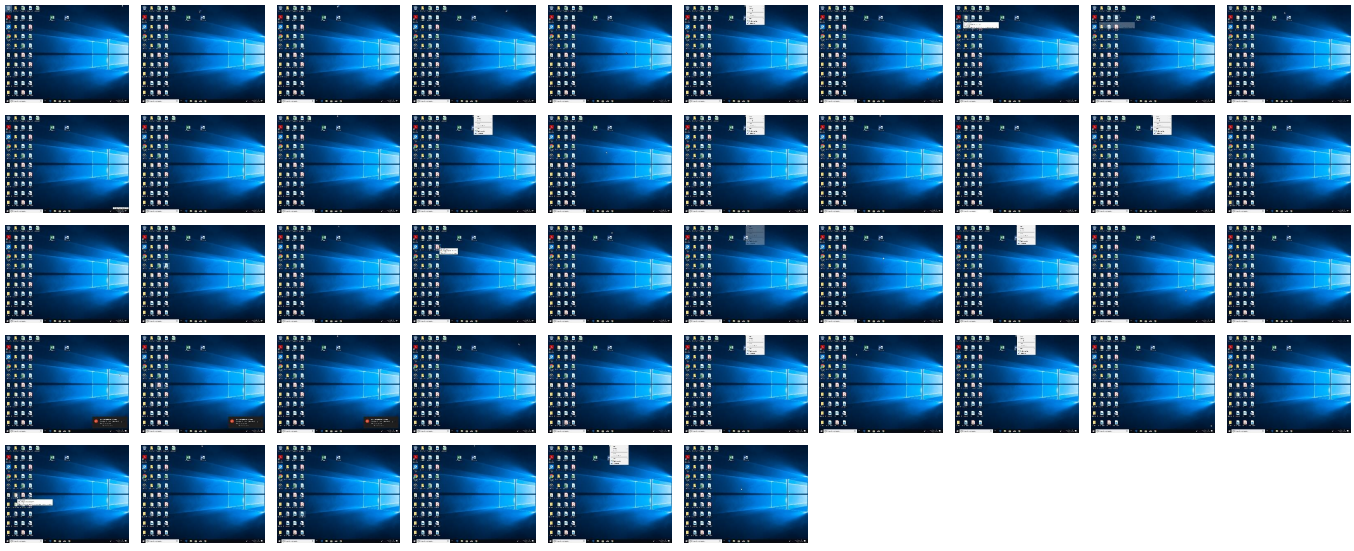
Behavior Graph



Screenshots

Thumbnails

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



Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
6culQol97a.exe	73%	ReversingLabs	Win32.Trojan.Worefflint	
6culQol97a.exe	58%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll	0%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.6culQol97a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.0.6culQol97a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

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_Error	6culQoI97a.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	6culQoI97a.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755473
Start date and time:	2022-11-28 18:32:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6culQoI97a.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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:	mal52.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.2% (good quality ratio 83.7%) • Quality average: 87.2% • Quality standard deviation: 22%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Copyright Joe Security LLC 2022

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\Microsoft\Windows\INetCache\Bracker\Feberkosten\Lavkonjunkturen.pro

Process:	C:\Users\user\Desktop\6culQoI97a.exe
File Type:	data
Category:	dropped
Size (bytes):	151484
Entropy (8bit):	6.722739524237379
Encrypted:	false
SSDEEP:	3072:i/XcPN2AMaEryngg6xwigaQTpHJVoBMQ/fV:ikUUhnfJrZzcMQ/fV
MD5:	7D35914613D5AE2EE21358270112B5F2
SHA1:	ED7CBBBBC35EBCA9F221B1E22927BF2845B54807
SHA-256:	DF9AA833D7E0B7455D5112DF644234B735D4F8C4E2A1527148E655DE16DA4BA3
SHA-512:	29F422C4B45EE72141D040EA7682A6D4C90858EA42F2FF461A6301B90195F5DF6F79B5F364B55D61A327EE1E5BAAE26F317E42B3965EDBD1ED42EF7F4FCB7793
Malicious:	false
Reputation:	low
Preview:	..zx'il...Y.....W.7...HF..$K..B.+.z.$i.z.M6.O..0wG;~Fm.....!gJn..M;&..-Lm.S<.....B..*Q.N.).C....x.h`.[o....*...IL@..^..e(...H....F<U...,.M8m>.I..F...o...W.....4....I<h..f....yK...a..n.. ...LM.*.U..S7]..b..V..;.W-..pL.k.....w...U...9F..;y.....H..jc.....u....\.V...%.O..r.a3=&.mE9.....G..c..Y.&.....|...*..X.~.`...=...e6..W.....w..7..B.U.".m....Q;T..D..A[...E.{...[..f.."... ..D#a.....sd...l,..t....)tU.[.u\.M...{3UP...~c_u.....dK..=.1.?..}8.TP.+P.z.H{.>'..2%a...}.f.e|3C.....R(...Q.`F~..N}Q]H.!.....+.....Y.G...d.\U."......Z...../c..%.t.....@8...D.1.S... .N.....q.....Kq.....f.....I.d)f.....f.e....f.b..i.LZ..... .....f!.....H...6qqqqqqqqqqqqqqqqqqqqqq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice\Grabbers145.Scu187

Process:	C:\Users\user\Desktop\6culQoI97a.exe
File Type:	ASCII text, with very long lines (42820), with no line terminators

Category:	dropped
Size (bytes):	42820
Entropy (8bit):	3.999720795205128
Encrypted:	false
SSDEEP:	768:Y8gLgZjz0mqZY9XVZ3z0Aqa2ogrBpnu2L9l6+EfD5u6lZ46hj0HJPn1W4:LgLgNuYBrA75olpu2Rl6+20v46QF17
MD5:	63EE366B70BC4507D462A94DD9C637BA
SHA1:	E0E3D34620C83C47F0590BD059AE2066D7F26FE7
SHA-256:	D032E1E9FA29373C0D811D0ED484D69F64DF02C0353DC2B7B4F2D08C44094F8A
SHA-512:	096C8D578842BE10D2B5D88DF5B130EE3D352190158CBF893DC2AC106D2DF6A91BFA17A92F5F48D3EC952A83DB785A05076AC340015832E5EF4D08D5E584EF 0
Malicious:	false
Reputation:	low
Preview:	FEE6A8669E78D118DC67A5CFBFFEC42B41EA106FBB6439C877770204CA485EF518706580B268717463D5CB797335A0A4350DCD796FC17224C6434BF0 95F7CA6B1DB91696C2ADB472E0F9E1E2D5D9262D956F3DB187372096F1F921757D6CF3BF2C192545E4EC2E0119B230B5AE2A35C6F37BA1074F96373F 828DDB9E588D13955D1AB94FE615E94016E252B8B38104F562E874B8886AF764B43D98BB66EA7A4F47209579E550F48880977DB1721FBE84477DACD8 8B7A9715F0DB819F886D56CCEFBB7CF44E40BEFCFF574D5E029E1762B75A84AEB88BC477AD0C2EEA118D4BEE4BCF2EB8DDD0207D78B0EC8551401E1F 79E9FB8B2FBE5C4F4026E771F2713CF19CDF0CB33B72276EC057B36A339D1B55FF594867C79F91E160A4306CB89DC803C9D2A891E3B0250832C9561D 97669476859BD0FA173F47CCE4052D59DB63C8DA7F75B11332DBC582649E24CAD546663CE0C14FBBE1C832071D322EA51419FF51CF67B56DC3A1EC75 B588F2C7B20CAE80771F166C55894E635141CFA69FAE881544C83F0F60B59833A61A433C6F47427621250CE45F35855E28554832210A2F46F0BBC264 0B9A2CD045EC3AEF8BDAD8D15D0B80E2F82BA296742D4481221961F2BB57D4461407EAB6FEB6DC9E558BE2DB318A22CDEB0E26889BCA6482843DEB5C 73A1C673197F30B4DA15D73000C3C08C5F8CDCD8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Urationelt\call-missed-symbolic.svg

Process:	C:\Users\user\Desktop\6culQoI97a.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1626
Entropy (8bit):	5.039495966615547
Encrypted:	false
SSDEEP:	24:t42w+Fdw6OyKbRAecFxVrGMalOY3bYnfS/YH6AAHD1gyKbRAecFxVrGMaFC:fONtAecFmMiScmNtAecFmMmC
MD5:	CCC1083D634E112EBE2FAD8D1809FEB7
SHA1:	AFBBB71D1B029B7FBE45E09C7217945A2668D262
SHA-256:	3D961823A04BAC2FF8748D7624AF7D06B10B3D2566AA93540ADB1FC46F6FA6CF
SHA-512:	3962F71527D2B662D5B9EACA2AF12AE414F01497871F3E818D86A9DF03DC9C08F1A9873265F70745857D65ADA87E623E523BEB80B51CCA99E820C459757B96D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16.006" height="16.013"><path d="M12.98 0a1 1 0 00-.11.01H8v.832A1 1 0 009 2.01h1.586L8 4.596 5.707 2.303a1 1 0 10-1.414 1.414l3 3a1 1 0 001.414 0L12 3.424V5.01a1 1 0 001.158 1H14V1.137a1 1 0 000-.275V.01h-.854A1 1 0 0012.98 0z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" color="#000" font-weight="400" font-family="sans-serif" overflow="visible" fill="#2e3436"/><path class="error" d="M14.242 15.725a.979.979 0 01-1.387 0l-1.04-1.04-1.041-1.04a.979.979 0 010-1.387l.493-.493a6.838 6.838 0 00-6.534 0l.493.493a.979.979 0 010 1.387l-1.04 1.04-1.04 1.04a.979.979 0 01-1.388 0l-1.

C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll

Process:	C:\Users\user\Desktop\6culQoI97a.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.854450882766351
Encrypted:	false
SSDEEP:	192:jPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4l:u7VpNo8gmOyRsVc4
MD5:	34442E1E0C2870341DF55E1B7B3CCCDC
SHA1:	99B2FA21AEAD4B6CCD8FF2F6D3D3453A51D9C70C
SHA-256:	269D232712C86983336BADB40B9E55E80052D8389ED095EBF9214964D43B6BB1
SHA-512:	4A8C57FB12997438B488B862F3FC9DC0F236E07BB47B2BCE6053DCB03AC7AD171842F02AC749F02DDA4719C681D186330524CD2953D33CB50854844E74B33D5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....`.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ....`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.777623756268328
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:	6culQoI97a.exe
File size:	334430
MD5:	d9aa122b8c39444799e60eabbab69502
SHA1:	0175baf7a240c2050571a6df273a892e8b192d81
SHA256:	317b5db72d7c43ab63caffa88412395a1b010d24f234eb1b7eeabc92105db143
SHA512:	4ba7e997ffad2ce396faa08d8be8cd6b7073e37828b347fad1ca3f1112d257ecd235c7df9d3d6c78e6b9f96ce878c5fbe2d2a70f7428648f1d2aa14aba7f5d38
SSDEEP:	6144:0x/MQs/IvHdjSzIH1qrb+WECj3wc0ibE0+lx:wxAIVu8VWb+WEY3LbEt6
TLSH:	7964F1253F64DC27C2A906708EF3D329D6F9D9406E634717BB8177ACBD31780B91A18A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.@.@...@...@../O...@...@..L@../O...@...c...@..+F...@..Rich.@.....PE..L.....`.....d....9.....%3.....@

File Icon

Icon Hash:	6070dee2bab2c43c

Static PE Info

General

Entrypoint:	0x403325
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x60FC909C [Sat Jul 24 22:13:48 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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h

Instruction
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A2F6Ch], eax
je 00007F11089BBEB3h
push ebx
call 00007F11089BF016h
cmp eax, ebx
je 00007F11089BBEA9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F11089BEF92h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F11089BBE8Dh
push 0000000Bh
call 00007F11089BEFEAh
push 00000009h
call 00007F11089BEFE3h
push 00000007h
mov dword ptr [007A2F64h], eax
call 00007F11089BEFD7h
cmp eax, ebx
je 00007F11089BBEB1h
push 0000001Eh
call eax
test eax, eax
je 00007F11089BBEA9h
or byte ptr [007A2F6Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [007A3038h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0079E528h
call dword ptr [0040816Ch]
push 0040A188h

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	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c7000	0x28868	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Is in Section
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	0x29c	.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	0x6230	0x6400	False	0.6699609375	data	6.441889952551939	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.4337890625	data	5.061067348371254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x399078	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a4000	0x23000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c7000	0x28868	0x28a00	False	0.5296875	data	5.194338163153121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x3c73b8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x3c7720	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x3d7f48	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x3e13f0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x3e6878	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x3eaaa0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x3ed048	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x3ee0f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x3eea78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x3eeee0	0x144	data	English	United States
RT_DIALOG	0x3ef028	0x13c	data	English	United States
RT_DIALOG	0x3ef168	0x100	data	English	United States
RT_DIALOG	0x3ef268	0x11c	data	English	United States
RT_DIALOG	0x3ef388	0xc4	data	English	United States
RT_DIALOG	0x3ef450	0x60	data	English	United States
RT_GROUP_ICON	0x3ef4b0	0x76	data	English	United States
RT_MANIFEST	0x3ef528	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

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: 6culQoI97a.exe PID: 5172, Parent PID: 3452

General

Target ID:	0
Start time:	18:33:04
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\6culQoI97a.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6culQoI97a.exe
Imagebase:	0x400000
File size:	334430 bytes

MD5 hash:	D9AA122B8C39444799E60EABBAB69502
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nskAD76.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
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	3	40574A	CreateDirectoryA
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	3	40574A	CreateDirectoryA
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	3	40574A	CreateDirectoryA
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	3	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nskAE13.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
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	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nskAE13.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	40570A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Lavkonjunkturen.pro	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\UrationeIt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\UrationeIt\call-missed-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice\Grabbers145.Scu187	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\nsrB0A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	9	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nskAD76.tmp	success or wait	1	40359C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nskAE13.tmp	success or wait	1	4058CB	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Lavkonjunkturen.pro	0	32768	fd fd 7a 78 27 69 6c 0f 0b fd 59 fd fd fd fd 14 fd 17 57 fd 37 fd fd fd 48 46 fd fd 24 4b fd d3 42 fd 2b 12 7a fd 24 69 fd 7a cf 4d 36 fd 4f fd 2e 30 77 47 3b 7e 46 6d fd fd fd 10 fd 21 67 4a 6e fd fd 4d 3b 26 1e fd 2d 4c 6d fd 53 3c fd 07 fd fd 15 fd 42 fd fd 2a 51 fd 4e fd 29 fd 43 03 fd 00 1f 78 fd 68 60 fd 5b 6f fd fd fd 0b 2a 13 fd fd 49 4c 40 fd fd 5e 18 fd 65 28 fd 1a fd 48 0e fd fd fd 46 3c 55 00 fd fd 2c fd 4d 38 6d 3e 1f 6c fd fd 46 fd fd fd 6f 1e 0e 7f 57 fd fd 18 fd fd fd 34 fd fd 02 fd 6c 3c 68 fd 08 66 fd f9 fd fd 79 4b fd 88 fd 61 2e fd 6e fd fd 0f fd fd 4c 4d fd 2a 01 55 04 fd 53 37 5d fd fd 62 fd 68 56 fd 1c 3b fd 57 2d 02 fd 70 4c fd 6b fd 2e 15 fd fd 0a fd fd 96 fd 77 fd fd 1b 55 fd fd 05 39 46	zx'ilYW7HF$KB+z$izM6O.0wG;~Fm!gJnM;&-LmS<B*QN)Cxh`[o*IL@^e(HF<U,M8m>lFoW4l<hfyKa.nLM*US7]bV;W-pLk.wU9F	success or wait	5	405D2E	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\UrationeIt\call-missed-symbolic.svg	0	1626	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 2e 30 30 36 22 20 68 65 69 67 68 74 3d 22 31 36 2e 30 31 33 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 32 2e 39 38 20 30 61 31 20 31 20 30 20 30 30 2d 2e 31 31 2e 30 31 48 38 76 2e 38 33 32 41 31 20 31 20 30 20 30 30 39 20 32 2e 30 31 68 31 2e 35 38 36 4c 38 20 34 2e 35 39 36 20 35 2e 37 30 37 20 32 2e 33 30 33 61 31 20 31 20 30 20 31 30 2d 31 2e 34 31 34 20 31 2e 34 31 34 6c 33 20 33 61 31 20 31 20 30 20 30 30 30 31 2e 34 31 34 20 30 4c 31 32 20 33 2e 34 32 34 56 35 2e 30 31 61 31 20 31 20 30 20 30 30 31 2e 31 35 38 20 31 48 31 34 56 31 2e 31 33 37 61 31 20 31 20 30 20 30 30 30 2d 2e 32 37 35 56 2e 30 31 68 2d 2e 38	<svg xmlns="http://www.w3.org/2000/svg" width="16.006" height="16.013"><path d="M12.98 0a1 1 0 00-.11.01H8v.832A1 1 0 009 2.01h1.586L8 4.5965.707 2.303a1 1 0 10-1.414 1.414l3 3a1 1 0 001.414 0L123.424V5.01a1 1 0 001.158 1H14V1.137a1 1 0 000-.275V.01h-.8	success or wait	1	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice\Grabbers145.Scu187	0	32768	46 45 45 36 41 38 36 36 39 45 37 38 44 31 31 38 44 43 36 37 41 35 43 46 42 46 46 45 43 34 32 42 34 31 45 41 31 30 36 46 42 42 36 34 33 39 43 38 37 37 37 37 30 32 30 34 43 41 34 38 35 45 46 35 31 38 37 30 36 35 38 30 42 32 36 38 37 31 37 34 36 33 44 35 43 42 37 39 37 33 33 35 41 30 41 34 33 35 30 44 43 44 37 39 36 46 43 31 37 32 32 34 43 36 34 33 34 42 46 30 39 35 46 37 43 41 36 42 31 44 42 39 31 36 39 36 43 32 41 44 42 34 37 32 45 30 46 39 45 31 45 32 44 35 44 39 32 36 32 44 39 35 36 46 33 44 42 31 38 37 33 37 32 30 39 36 46 31 46 39 32 31 37 35 37 44 36 43 46 33 42 46 32 43 31 39 32 35 34 35 45 34 45 43 32 45 30 31 31 39 42 32 33 30 42 35 41 45 32 41 33 35 43 36 46 33 37 42 41 31 30 37 34 46 39 36 33 37 33 46 38 32 38 44 44 42 39 45 35 38 38 44 31 33 39	FEE6A8669E78D118DC6 7A5CFBFFEC4 2B41EA106FBB6439C87 7770204CA48 5EF518706580B2687174 63D5CB7973 35A0A4350DCD796FC17 224C6434BF0 95F7CA6B1DB91696C2A DB472E0F9E1 E2D5D9262D956F3DB18 7372096F1F9 21757D6CF3BF2C19254 5E4EC2E0119 B230B5AE2A35C6F37B A1074F96373F 828DDB9E588D139	success or wait	2	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\nskAE13.tmp\System.dll	0	11776	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 69 72 2a fd 2d 13 44 fd 2d 13 44 fd 2d 13 44 fd fd 0f 4a fd 2a 13 44 fd 2d 13 45 fd 3e 13 44 fd fd 1c 19 fd 2a 13 44 fd 79 30 74 fd 29 13 44 fd 4e 31 6e fd 2c 13 44 fd fd 33 40 fd 2c 13 44 fd 52 69 63 68 2d 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 60 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$ir*-D-D-DJ*D-E >D*Dy0t)DN1n,D3@,DRi ch-DPEL`.! !)	success or wait	1	405D2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\6culQoI97a.exe	unknown	512	success or wait	397	405CFF	ReadFile
C:\Users\user\Desktop\6culQoI97a.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\Desktop\6culQoI97a.exe	unknown	4	success or wait	13	405CFF	ReadFile
C:\Users\user\Desktop\6culQoI97a.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Pollen47\Disvoice\Grabbers145.Scu187	unknown	1	success or wait	1023	405CFF	ReadFile
C:\Users\user\Desktop\6culQoI97a.exe	unknown	4	success or wait	2	405CFF	ReadFile
C:\Users\user\Desktop\6culQoI97a.exe	unknown	4	success or wait	8	405CFF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Bracker\Feberkosten\Lavkonjunkturen.pro	unknown	1048576	success or wait	1	73542AF9	ReadFile

Registry Activities

Key Created

Copyright Joe Security LLC 2022

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microoperations	success or wait	1	405FB7	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microoperations\benison	success or wait	1	405FB7	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Udsvedt	success or wait	1	405FB7	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Vaterliniers	success or wait	1	405FB7	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Vaterliniers\Svesken	success or wait	1	405FB7	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Vaterliniers\Svesken\unintersecting	success or wait	1	405FB7	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microoperations\benison	Tankegangs	binary	FF 81 16 03	success or wait	1	402507	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Udsvedt	Brandying	unicode	Forvandles	success or wait	1	402507	RegSetValueExA
HKEY_CURRENT_USER\Software\Vaterliniers\Svesken\unintersecting	Swallowpipe223	binary	FF 88 1C 8F	success or wait	1	402507	RegSetValueExA

Disassembly

No disassembly