



ID: 755926
Sample Name: D009780.exe
Cookbook: default.jbs
Time: 10:24:07
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report D009780.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 5
AV Detection 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
General Information 8
Warnings 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp\System.dll 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Anhydridizes.Imi121 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\Psammologist.Pan 10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\libxml2-2.0.typelib 10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\memstat.c 10
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\selection-end-symbolic.symbolic.png 11
Static File Info 11
General 11
File Icon 11
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 13
Data Directories 13
Sections 13
Resources 14
Imports 14
Possible Origin 15
Network Behavior 15
Statistics 15
System Behavior 15
Analysis Process: D009780.exePID: 3772, Parent PID: 3452 15
General 15
File Activities 15
File Created 15
File Deleted 18
File Written 18
File Read 20
Registry Activities 21
Key Created 21

Disassembly 21

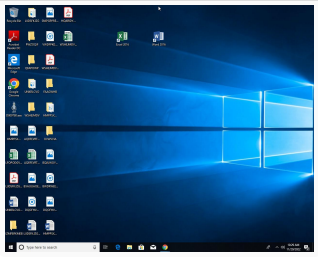
Windows Analysis Report

D009780.exe

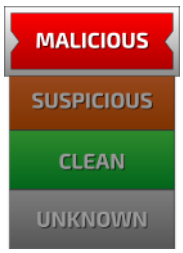
Overview

General Information

Sample Name:	D009780.exe
Analysis ID:	755926
MD5:	649e0964d04ac8..
SHA1:	5debabb563c0c4..
SHA256:	2b5120f2d732c6..
Tags:	exe
Infos:	



Detection

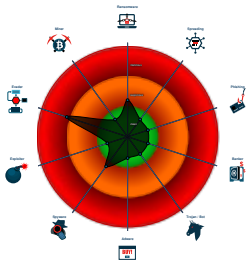


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 (…
- Detected potential crypto function
- Stores files to the Windows start me…
- Contains functionality to dynamicall…
- Abnormal high CPU Usage
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- D009780.exe (PID: 3772 cmdline: C:\Users\user\Desktop\D009780.exe MD5: 649E0964D04AC89667C1F59FE99C7799)
- **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

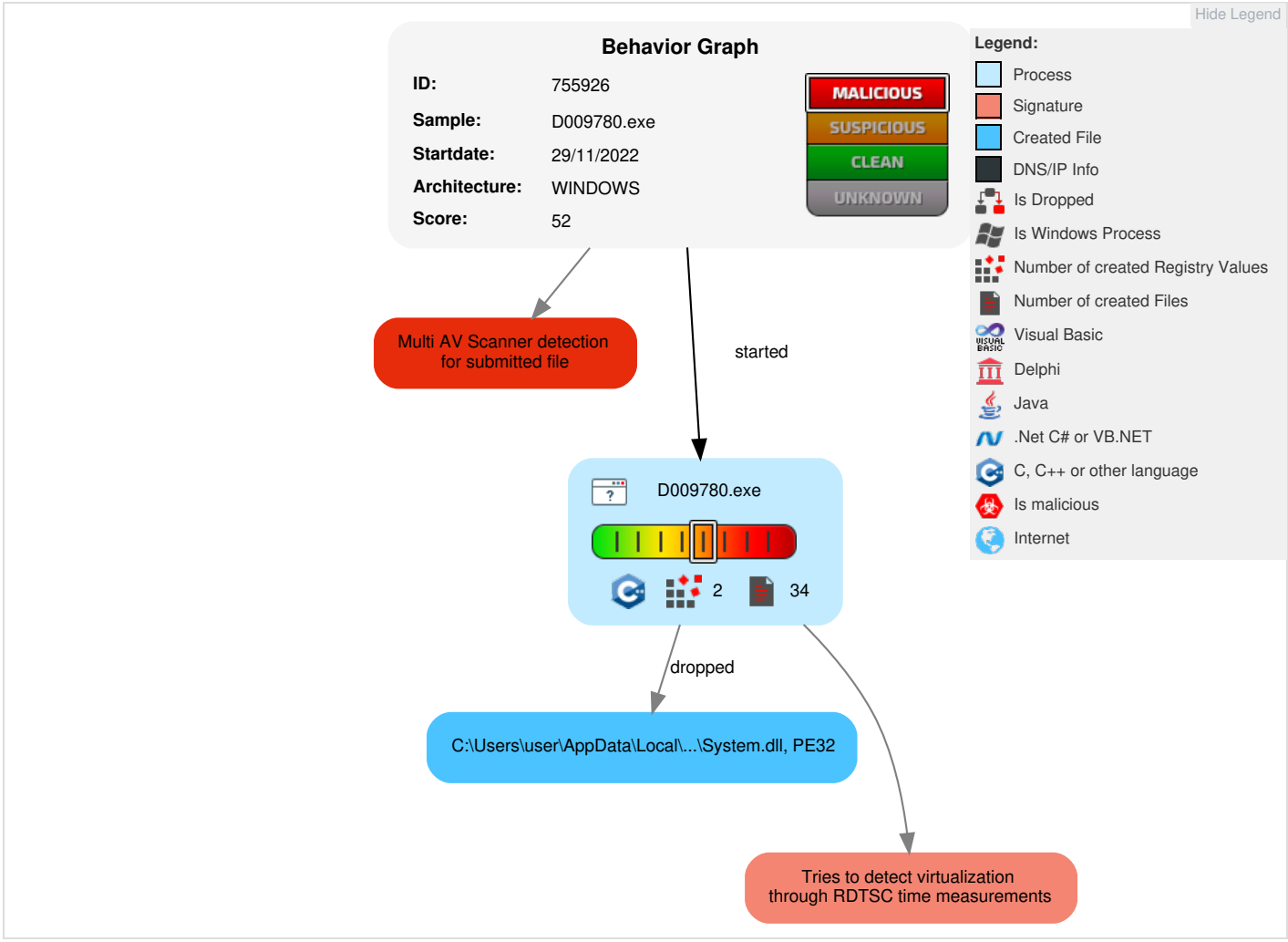


Tries to detect virtualization through RDTSC time measurements

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	1 Windows Service	1 Access Token Manipulation	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	1 Registry Run Keys / Startup Folder	1 Windows Service	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)	1 Registry Run Keys / Startup Folder	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

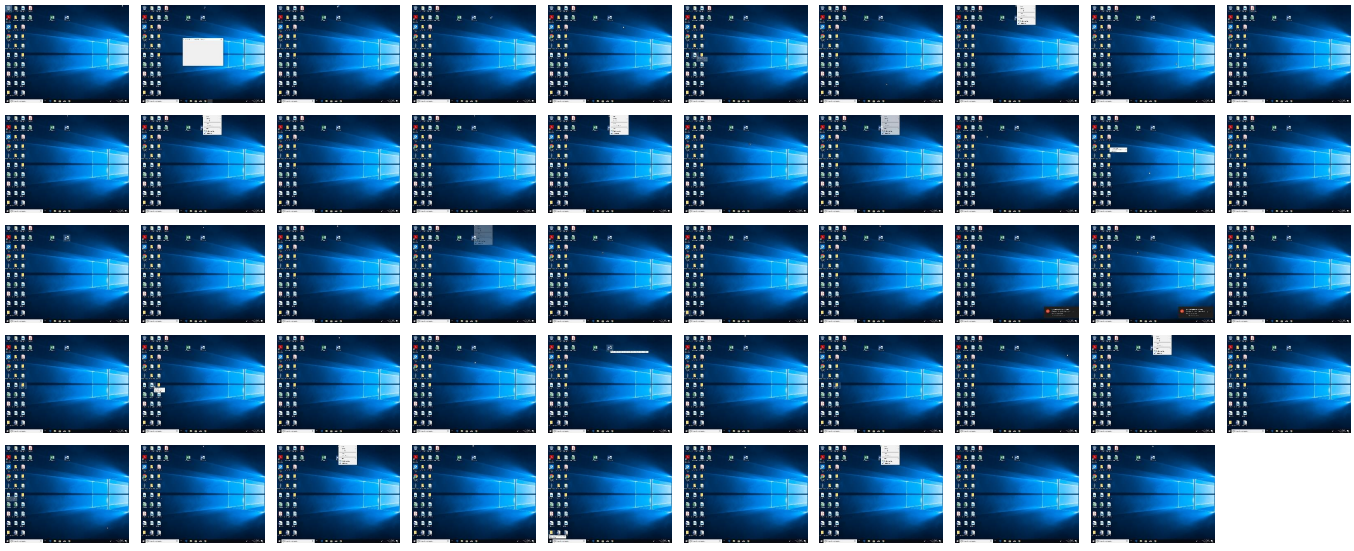
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
D009780.exe	22%	ReversingLabs	Win32.Trojan.Guloader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	D009780.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755926
Start date and time:	2022-11-29 10:24:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	D009780.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@1/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.6%) • Quality average: 87% • Quality standard deviation: 21.1%
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 IPs from analysis (whitelisted): 93.184.221.240
- Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: D009780.exe

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\Temp\nsn8FFA.tmp\System.dll

Process:	C:\Users\user\Desktop\D009780.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8QIl972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......1...u.u.u...s.u.a....r.!..q....t....t.Richu.........................PE..L.....uY.. ....!..... ....'.......0...............................`.......................................2.......0..P...........................P.........................................................0..X...........................text............ ........ .......... ..`.rdata..S....0.......$..............@..@.data...x....@.......(..............@....reloc..`....P.......*..............@..B.. ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Anhydridizes.lmi121

Process:	C:\Users\user\Desktop\D009780.exe
File Type:	data
Category:	dropped
Size (bytes):	166213

Entropy (8bit):	6.7188897468610635
Encrypted:	false
SSDEEP:	1536:yyKNH91XkciA5V8SsuXEkWtJbVKrUp+3Rdtt03z2pXy5gMRKhKcfhby09qVLDerk:8rXEA5V2mPa+XVHpXE3RKLwLcppDa
MD5:	8F8B455423728EC3F56CC534165292C8
SHA1:	B7BC0FBD5826D73287D66560C7D0DA6738B5AFD8
SHA-256:	38583A88A0AD9F6B776B25BEFF612F21A8AD8289F1FC5E75AD0D411BF5FED52F
SHA-512:	0906AFFD2078F6DB365EBFCB89EB052F9C343976B851ACCB9FA91299414F33632F8F52A59C9E1BAC49D83A34335302E747285DB5AA34C133FB51F444FA5BB52!
Malicious:	false
Reputation:	low
Preview:	::

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\Psammologist.Pan

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\D009780.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>41040</td></tr>
<tr><td>Entropy (8bit):</td><td>7.995359137976442</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:wNhagjlZc4ExPMbCVVsT62u53N+qUy22/aJKHBO2jj5dJQ:LeZcpeEVsTp03Nu2CJK5jj5dy</td></tr>
<tr><td>MD5:</td><td>14E3BC546122A6AABCBAA4FD77EB0DF9</td></tr>
<tr><td>SHA1:</td><td>6D6F937F85083A6B7D3CD784FD7FD2F9D602B8A0</td></tr>
<tr><td>SHA-256:</td><td>E3DBEFBAE9D754C328269CF29CDDC926ECE497029B763FCC322B431AE03D940D</td></tr>
<tr><td>SHA-512:</td><td>8BD0F74C31573CEF3B68B8CCD575822C22197D880CA331F884669316C17047DB3AE49BD79DCFC4EC21257399EA7E238226956BF681130D5263BC5BDFFB84D28</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>..@.....6..R...Ev.Rt.E...}WR.h.+..c.N...8.......7V.}!..I0#.....pS....i..=d........e..+h.M. .../;...(.|...S.I....#.2A|...W..E..........+.A.!o..n0O%...^.,......I.R..4..4d.Oj..f....>.4..#.qh.|.....J?.... ....&.5.....&..cz...N.BA......~..:~$....9...#..$w..o.h...G1....R.C:F...juFe..`_...J.7'..\.#.r.:vp............n...B.I..@L...V....4x..I.......z.....l7..y........T.}.r....c.._.....4H.....e...Q<..k...Sh....../. .O...... [.^.s...t........r..S........_.5.v..s.+n.t.g=/.}3...._:da@...r.Jd.............]W...k_..W.E...}.e....c....8y.>.L..3i..x.?...+.2..^.X...........f.{.~I.x.u..R..1.j^p..K(........&.Z.R2..D.n... .C|i.m..... d=..`....N..[...t......D.......{..2zk.."........S.A...s.5......*.x.a.XSL....1,Z.W.......(m...V.~.....Q..=......|"/..|@rp+.o..!..r!../..!6T....e.y.3.u.J...}.X$...\..fJ.K..K.[zZZ....0&.ZX.c4..;.v...._.;a ...:iI&G................u....{....d1....X......N..\!..M...|.../6.....v..!....Z...H.@..C...X/ ?...........o.........g:0b.....</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\libxml2-2.0.typelib

Process:	C:\Users\user\Desktop\D009780.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>..<div id="header"><h1>Server Error</h1></div>..<div id="content">.. <div class="co

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\memstat.c

Process:	C:\Users\user\Desktop\D009780.exe
File Type:	C source, ASCII text

Category:	dropped
Size (bytes):	13484
Entropy (8bit):	5.15716859322729
Encrypted:	false
SSDEEP:	192:B3tdgdRmAMgyWkSctse3XX6ZjuguOixHRYqx0NzZW+08e:B3tuPdjJ0TCzZWv
MD5:	BD46EB22C1A1B4EA40373E8F57BFF4E3
SHA1:	CC2943E660BBB1697B7561F2776A7BCE2F36718A
SHA-256:	8361836BCB172722E5F2EE90AF31834B9B08B828A90E80E0BB930C336001B4CE
SHA-512:	5994643BCDFDF59B7EBF8FE36BC30CF0A454966FA95741D80AC81E9C42126A66ACDD782F6D7852A35CAE171FCC0DE1218EC1CD951829F7EC1C72B35EE7487 74
Malicious:	false
Reputation:	low
Preview:	/*.** 2018-09-27.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** **********.**.** This file demonstrates an eponymous virtual table that returns information.** from sqlite3_status64() and sqlite3_db_status()..**.** Usage example :.**.** .load ./memstat.** .mode quote.** .header on.** SELECT * FROM memstat;.*/.#if !defined(SQLITE_CORE) || defined(SQLITE_ENABLE_M EMSTATVTAB).#if !defined(SQLITEINT_H).#include "sqlite3ext.h".#endif.SQLITE_EXTENSION_INIT1.#include <assert.h>.#include <string.h>..#ifndef SQLITE_OM IT_VIRTUALTABLE../* memstat_vtab is a subclass of sqlite3_vtab which will.** serve as the underlying representation of a memstat virtual table.*/.typedef struct memstat_vtab memsta

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\selection-end-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\D009780.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	138
Entropy (8bit):	5.559646592748364
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllO9p2hkq8PQ1/kbcw1w9lDk7kup:6v/lhPys8pQt8PQ2cw1llDXup
MD5:	9863709F8F136F0F38A5D9CF2740143A
SHA1:	0EC6AA74A3FED4719B1B8D2E8468239489D84427
SHA-256:	2C86B3EDF2A397608FE0C12A634F175DE1E3C4E5C4610B8457578B549069A7B0
SHA-512:	B1D8DC9CAFF35264E117201C0DB2112F4C07BAB9235188D32F90B9D00DC2E7AC27ECC1FC9753C5F50949C95D91EEA0C5F318D6D1C8D7587CA0A68AD2CC1C EB5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....sBIT....|.d....AIDAT8.c`.....X..X.....C...u..(&.%.. ..t.H6...$.....S.F.....a/..&I.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.727040003614326
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:	D009780.exe
File size:	296621
MD5:	649e0964d04ac89667c1f59fe99c7799
SHA1:	5debabb563c0c457670b925c4c8f4830484a0067
SHA256:	2b5120f2d732c6b78ddac5ac679cbbf279d96108d50cc02e569be1e07813b604
SHA512:	5fb49e4d8199e28f018f21d7d5eff3eafeade9c4f72c2bf5dabb6476c84a7945a5f67681de6df40a95a47412dc89586497bd4a7cb0ad2934d962db8b376d80ea
SSDEEP:	6144:nQ606xDpoDTOfHQerv77Um8RHZ9USC/U3zP9wnZwC2djTTv/o:FpoPOfQqvHUmIkS53zPunZwd7Ho
TLSH:	1854122063A0C433D6AA0A30DD1386F79FB59C69EE096F87D3507E9C7C72246D52E35A
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...6.uY.....f.....

File Icon



Icon Hash:	c60ccd1616164e46

Static PE Info

General

Entrypoint:	0x403373
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:	0x59759536 [Mon Jul 24 06:35:34 2017 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:	b34f154ec913d2d2c435cbd644e91687

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [00434EECh], eax
je 00007FC9C0A66683h
push ebx
call 00007FC9C0A69919h
cmp eax, ebx
je 00007FC9C0A66679h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FC9C0A69893h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FC9C0A6665Ch
push 0000000Ah

Instruction
call 00007FC9C0A698ECh
push 00000008h
call 00007FC9C0A698E5h
push 00000006h
mov dword ptr [00434EE4h], eax
call 00007FC9C0A698D9h
cmp eax, ebx
je 00007FC9C0A66681h
push 0000001Eh
call eax
test eax, eax
je 00007FC9C0A66679h
or byte ptr [00434EEFh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [00434FB8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0042B208h
call dword ptr [00408188h]
push 0040A2C8h

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	0x8608	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x76000	0x16898	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	0x65ef	0x6600	False	0.6750919117647058	data	6.514810500836391	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x149a	0x1600	False	0.43803267045454547	data	5.007075185851696	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2aff8	0x600	False	0.5162760416666666	data	4.036693470004838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x35000	0x41000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x76000	0x16898	0x16a00	False	0.7946089433701657	data	7.153289056271752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x76478	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x767e0	0x9d19	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x80500	0x4102	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x84608	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x86bb0	0x16e8	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x88298	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x89340	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x8a1e8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x8aa90	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x8b0f8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x8b660	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x8bac8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x8bdb0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x8bed8	0x144	data	English	United States
RT_DIALOG	0x8c020	0x13c	data	English	United States
RT_DIALOG	0x8c160	0x100	data	English	United States
RT_DIALOG	0x8c260	0x11c	data	English	United States
RT_DIALOG	0x8c380	0xc4	data	English	United States
RT_DIALOG	0x8c448	0x60	data	English	United States
RT_GROUP_ICON	0x8c4a8	0xae	data	English	United States
RT_MANIFEST	0x8c558	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage

Copyright Joe Security LLC 2022

DLL	Import
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

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: D009780.exe PID: **3772**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:24:59
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\D009780.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\D009780.exe
Imagebase:	0x400000
File size:	296621 bytes
MD5 hash:	649E0964D04AC89667C1F59FE99C7799
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	40583E	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nst86C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DE2	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	2	40583E	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	2	40583E	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	2	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\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	2	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Anhydridizes.Imi121	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40583E	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583E	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\libxml2-2.0.typelib	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\Psammologist.Pan	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\memstat.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\selection-end-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DE2	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	40583E	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	40583E	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	40583E	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	40583E	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	40583E	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsn8FFA.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	4057FE	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DA0	CreateFileW
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405DA0	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nst86C1.tmp	success or wait	1	403624	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsn8FFA.tmp	success or wait	1	4059BF	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Anhydridizes.Imi121	0	28404	3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a	:::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::::::::::::::::: :::::::::::::::	success or wait	7	405E40	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\libxml2-2.0.typelib	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 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 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	405E40	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\Psammologist.Pan	0	32768	0f fd 40 fd fd 0d fd fd 36 fd fd 52 fd fd 06 45 76 0a 52 74 fd 45 fd fd 1b 7d 57 52 07 68 fd 2b fd fd 63 fd 4e 06 fd fd 38 fd fd fd 8d fd fd fd 37 56 fd 7d 21 fd fd 49 30 23 fd 05 fd 1e fd 70 53 03 fd 07 fd 69 fd 01 3d 64 10 fd fd 04 d0 04 fd fd 65 fd fd 2b 68 fd 4d fd 20 fd fd fd 2f 3b 13 fd 13 28 fd 7c 03 02 fd 53 fd 49 07 fd fd fd 23 fd 32 41 7c fd fd fd 57 fd 0c 45 fd fd fd 03 fd 02 fd fd fd fd 2b fd 41 fd 21 6f fd 07 6e 30 4f 25 fd fd fd 5e 1b 2c fd 1d fd 00 fd fd 49 fd 52 fd fd 34 fd fd 34 64 fd 4f 6a fd 0a 66 fd 07 fd fd 3e fd 34 07 fd 23 fd 71 68 1b 7c fd fd 0f fd fd 4a 3f fd 17 fd 75 1f 14 fd fd 18 0d fd fd 26 fd 35 15 fd 0a 04 fd 26 fd 17 63 7a fd 0f fd 4e fd 42 41 fd 19 fd fd fd 3a 7e 0a fd 3a 7e 24 fd	@6REvRtE}WRh+cN87V}!I0#pSi=de+hM /;(|SI#2A|WE+A!on0O%^,IR44dOjf>4#qh|J?&5&czNBA~:~$	success or wait	2	405E40	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\memstat.c	0	13484	2f 2a 0a 2a 2a 20 32 30 31 38 2d 30 39 2d 32 37 0a 2a 2a 0a 2a 2a 20 54 68 65 20 61 75 74 68 6f 72 20 64 69 73 63 6c 61 69 6d 73 20 63 6f 70 79 72 69 67 68 74 20 74 6f 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65 2e 20 20 49 6e 20 70 6c 61 63 65 20 6f 66 0a 2a 2a 20 61 20 6c 65 67 61 6c 20 6e 6f 74 69 63 65 2c 20 68 65 72 65 20 69 73 20 61 20 62 6c 65 73 73 69 6e 67 3a 0a 2a 2a 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 64 6f 20 67 6f 6f 64 20 61 6e 64 20 6e 6f 74 20 65 76 69 6c 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 66 69 6e 64 20 66 6f 72 67 69 76 65 6e 65 73 73 20 66 6f 72 20 79 6f 75 72 73 65 6c 66 20 61 6e 64 20 66 6f 72 67 69 76 65 20 6f 74 68 65 72 73 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 73 68 61 72 65 20 66 72 65 65 6c	/*** 2018-09-27**** The author disclaims copyright to this source code. In place of** a legal notice, here is a blessing:**** May you do good and not evil.** May you find forgiveness for yourself and forgive others.** May you share freel	success or wait	1	405E40	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\selection-end-symbolic.symbolic.png	0	138	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 41 49 44 41 54 38 fd 63 60 18 fd fd fd fd fd fd fd 58 fd fd 58 fd 18 19 18 18 fd 43 fd 07 fd 75 fd 7f 28 26 fd 25 fd 0c 20 fd 10 74 03 48 36 04 fd 01 24 19 fd c0 fd fd 14 53 04 46 0d 18 0c 00 00 61 2f 18 00 26 49 fd fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dAIDAT8c`XXCu(&%tH6$SFa/&IIENDB`	success or wait	1	405E40	WriteFile
C:\Users\user\AppData\Local\Temp\nsn8FFA.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 fd 00 00 00 0e 1f fd 0e 00 fd 09 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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELuY!	success or wait	1	405E40	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D009780.exe	unknown	512	success or wait	256	405E11	ReadFile
C:\Users\user\Desktop\D009780.exe	unknown	4	success or wait	2	405E11	ReadFile
C:\Users\user\Desktop\D009780.exe	unknown	4	success or wait	17	405E11	ReadFile
C:\Users\user\Desktop\D009780.exe	unknown	4	success or wait	2894	405E11	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Staveren\Kolkhozy\Fatalists\Cassythaceae\Psammologist.Pan	unknown	2	success or wait	277	4026B6	ReadFile
C:\Users\user\Desktop\D009780.exe	unknown	4	success or wait	2	405E11	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Ydervgg\Superassume\dodecaheddra\Anhydridizes.Imi121	unknown	1052672	success or wait	1	1000295D	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fivefoldness	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fivefoldness\Endosseringerne	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fivefoldness\Endosseringerne\Fouragen	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Fruticeta	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Fruticeta\Lavandin	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Fruticeta\Lavandin\Kingliest	success or wait	1	40614C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Fruticeta\Lavandin\Kingliest\Ernringsenhed	success or wait	1	40614C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fivefoldness\Endosseringerne\Fouragen	Arigue	dword	0	success or wait	1	40246F	RegSetValueExW
HKEY_CURRENT_USER\Software\Fruticeta\Lavandin\Kingliest\Ernringsenhed	Legating	binary	FF 8A 3B 51	success or wait	1	40246F	RegSetValueExW

Disassembly

No disassembly

Copyright Joe Security LLC 2022