ID: 624323
Sample Name:
PO#4200000866.exe
Cookbook: default.jbs
Time: 14:37:07
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

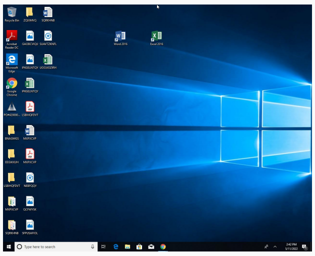
Windows Analysis Report

PO#4200000866.exe

Overview

General Information

Sample Name:	PO#4200000866.exe
Analysis ID:	624323
MD5:	5d0444b70ff5caa..
SHA1:	27309fdae9005f7.
SHA256:	fd620fd2a9d5ca1..
Tags:	exe guloader
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

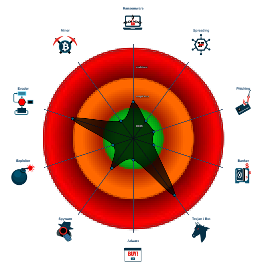
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64**
- PO#4200000866.exe (PID: 5108 cmdline: "C:\Users\user\Desktop\PO#4200000866.exe" MD5: 5D0444B70FF5CAA4EC3B2CA2E563E724)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://finseb.com/qwer/COrg_ZBOJvB194.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.777573204.0000000003AA0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

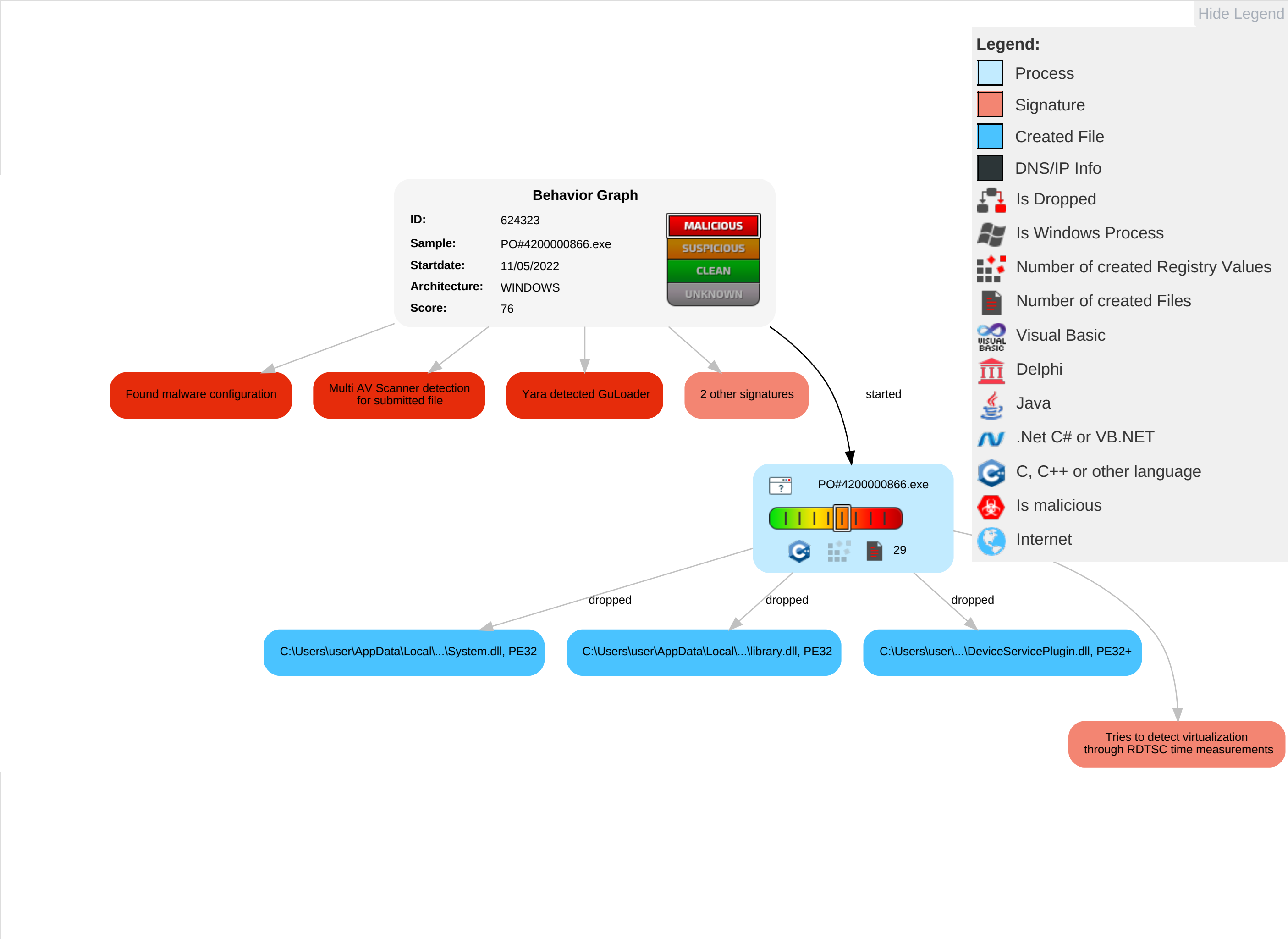
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	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

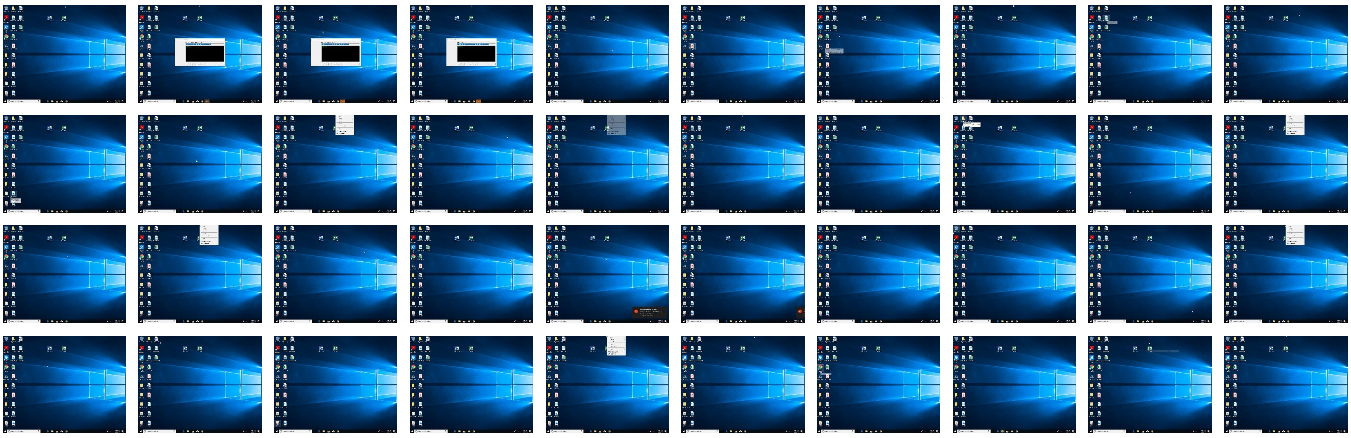
Behavior Graph



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
PO#4200000866.exe	10%	Virustotal		Browse
PO#4200000866.exe	5%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DeviceServicePlugin.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\DeviceServicePlugin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\library.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\library.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://finseb.com/qwer/COrg_ZBOJvB194.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://finseb.com/qwer/COrg_ZBOJvB194.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.asus.com/campaign/aura/global/download.php	PO#4200000866.exe, 00000000.00000002.777285149.0000000002773000.00000004.00000800.00020000.00000000.sdmp, DeviceServicePlugin.dll.0.dr	false		high
http://crl.certum.pl/ctsca2021.crl0o	PO#4200000866.exe	false		high
http://repository.certum.pl/ctnca.cer09	PO#4200000866.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	PO#4200000866.exe	false		high
http://crl.certum.pl/ctnca.crl0k	PO#4200000866.exe	false		high
http://subca.ocsp-certum.com05	PO#4200000866.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com02	PO#4200000866.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	PO#4200000866.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	PO#4200000866.exe	false		high
http://repository.certum.pl/ctnca2.cer09	PO#4200000866.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	PO#4200000866.exe	false		high
http://www.iso.org/iso/country_codes	PO#4200000866.exe, 00000000.00000002.777285149.0000000002773000.00000004.00000800.00020000.00000000.sdmp, iso_3166.xml.0.dr	false		high
http://www.certum.pl/CPS0	PO#4200000866.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624323
Start date and time: 11/05/202214:37:07	2022-05-11 14:37:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#4200000866.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:	22
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:	mal76.troj.evad.winEXE@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63% (good quality ratio 62%) • Quality average: 88.5% • Quality standard deviation: 21.8%
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 • Adjust boot time • Enable AMSI • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- 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\DeviceServicePlugin.dll

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	202472
Entropy (8bit):	6.000052926475626
Encrypted:	false
SSDEEP:	3072:GoFZlM8vbzCukOsa+tGuHBUXph7RZuUq+tZflXOdc+KTq6ZPGiHIxY4am/Vle2gL:GofuMbWukLdYuHBUX9Tcle2gyl
MD5:	78B266FFCEA0C7FFDF364EFB4D61F623
SHA1:	ADB3B29F96E70A60969F3CA4896372F303FAC264
SHA-256:	647BDB2E881AEDB7FB350FB20BE46555F4B8156EC2A7757DC2FA43EA92A2BBB9
SHA-512:	065F019A570ADED1E21BA9564CA51A1C974FD113663F9CF69AE4BE1472CFDD9649AFEDB65689FD20E6236EA5B58B0B7F3FE764C57540D5FE05E22EFD402697 F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........S..2.2.2.Js..2..Z.2..Z.2..Z.2..Z.2..Z.2.&[.2..[.2..Z.2..Z.2.2.k2..[.2..[.2.. [...2.2w..2..[.2.Rich.2.........PE..d....5.a.........\" ....@...........`.........................................0...X.......T.... ..p.......8............0..$... g..p.................. .h..(....g...............................................text.............................. ..`.rdata..:..........................@..@.data..............................@....pdata..8..........................@..@.rsrc...p.... ....@..@.reloc..$....0......................@..B... ....

C:\Users\user\AppData\Local\Temp\Galvanosurgery9.hom

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\PO#4200000866.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>25002</td></tr>
<tr><td>Entropy (8bit):</td><td>7.991900167248316</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:Ux8/kU33emF41RQTsWfIZVKJrS+oAZPN1ZE:jOmu4AquVkLZPN1ZE</td></tr>
<tr><td>MD5:</td><td>ADDF085CA091DB730D3B31F40AB8BE09</td></tr>
<tr><td>SHA1:</td><td>8DBF909A5622DA49EAD2DB877D4CF34C2AB4C708</td></tr>
<tr><td>SHA-256:</td><td>3AF396E6C7AA54E6D8AB991196B413EB84363DF7A75DF52474A7DB65CCDF7198</td></tr>
<tr><td>SHA-512:</td><td>BE490EBAA09F7E4781F96E162F0DED2E3ADFB682B8E08AC888D0DE78578878B077085A03E6CDBE87C15523AB245F92F272262BEB57304C5C728A657BC759017 4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>....l...+Zp"!.\.z.|.f|.o......".x=.&B@...O..U.ad.6....:P....]....E.n......<..e..=....#DCD...=K.h.`....|...:7..m..oy....8vU.....Q.R..}.1...E..J_....i.5p.4.2tYF.l<.A.lt7Z....>..^J...&.z.'.x.....F....h.. p....\0..y....v....G[."?..?UPv]..c...0........D.s......).3.....C...2...,,..-.9. y.......0;E.,..bTr4^...(........o.8.i.3...8m..=..A.y.t&s.H.1:..J.U..-.@.{..a.:..4..^;.+.P.....q...$@.^.[.......4...Mx... tH.................R..A.:..Go+[F......{......Ei..k.[....G...0.?4N...Kgg`.....G\..........^..+T......U...3.n.....Lz..vQ4......2{b.....Y.i..:.......F...f...!.n.8.|......V\6..df....\%%.....1..F.0t.d.L.+....E...5. ...^...qV...9h....X.#.=.[....:.'....qsQ..7......[.G..j...8nK.Ep?;W.....j(.Ln.xU."..M..O..SY.<.o@..S...."Y....`Zc..Yrd.....'.v..b,.......ka..w!T..Q.}p..P#*..z...4..Bgp..+`.*..3wW...d."......0 H....ra.u95.I..4`.....I..Lt!.B.>(.YkQ."$...p^.\H.'.......K9D.I.q..>n..._...........+%....<..3n$....H.d.}."....L).c..b...8.'I..(...T</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\KUNDSKABSRIGESTES.lna

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	data
Category:	dropped
Size (bytes):	87438
Entropy (8bit):	6.436902007549056
Encrypted:	false
SSDEEP:	1536:omUT7ai9UNcEshv2cA4CAD4bSv0tgxhnriGFyHuvYIpf:oZuiwcEQ2H49LhrZ7YI1
MD5:	7E187F93F378A4AE3BD099E5A17AE036
SHA1:	22B04988E767283FFB168FC95DC60446B79C1A31
SHA-256:	11F2F67A97D28648FB806E7049026DC1FF4E74DC51A158831CEF6FA7AA4DB1F4

SHA-512:	B63C1B128A2D1E14443E8F6349F809AFDF03C4004C2B07C394CA49A4496FBE32977C26FB65DA2B510A1F690056486A0111AE7C876F1480EE19F38954BA2B73D6
Malicious:	false
Reputation:	low
Preview:	..f.h....&..?A...%..V..4..JH..f...f......3.<j.wwwwwwwwwwwwwwwwwwwwwww wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwf.........f.......H(.)..f.s.....u..a....5-..f...f.`..0...6............................... ............D............W..~.........................f!....f.r.#.i.....5..errrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr,.....g.f.s.l.)"Z.>WWWWWWWWWWWWWWWWWWWWWWWWWWWWWW WWWWWWWWWWWWf....f.r.D........-.j..``f...f......g....h.f.d..7.U...4.f....c.....'...!\\........... b...2E.m...f!.....k.f.s.6......#.!Dr...............................f..f.a....e...f.c..5.8....................................

C:\Users\user\AppData\Local\Temp\ac-adapter-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	290
Entropy (8bit):	6.848704057450045
Encrypted:	false
SSDEEP:	6:6v/lhPys1ZJmBXeD3e6gv7ksqwDkgrb2DezQq+lp:6v/7VZJwUuLNLvH2Pr
MD5:	AFB944CEF06D0CE65E2CB6763EF2472D
SHA1:	1D340D8BD9B52EDC71C6F06D6F31A9C8F4E566BF
SHA-256:	CD6FB10C2F3455A8479455B59AB69C176322747AD857AC9C387A7B0C717A21BB
SHA-512:	7BA8C6D91A068EA257DF44D6571FA9230E3167D0B73DAAA296ED1B94BE9C94CEC9B7C49F21FEE95BB1C06A40C4F5085451426D3863DE381B5E5CE975EC62E 40
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR................a....sBIT....|.d.....IDAT8...1K.1....IAZ\.....A".....Q].<.]\:v.I.. .P.$..I..3>......o...M..a.Ejn..'.a......t..d.p.e.........r@..Z.&mR..Tc.K..i.j.G.....PW.t...].t.fq1.. ...U..G....."d.o.[.....{x..>..8...Xu.J.q.....'..uO.^@.....p.........IEND.B`.

C:\Users\user\AppData\Local\Temp\csv.c	
Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	28997
Entropy (8bit):	4.9868097347943605
Encrypted:	false
SSDEEP:	384:ieB8/8fGGqYRUIFFS/uNYd5elGVFg83Sg8hNRKlGnnJWXgg+0lk4m4V/:i/Ef5FLFkuNYd5elGVpqR5Rgb
MD5:	987A2F0FFB9995CA5AFF8D379FEC14EE
SHA1:	74DDC3FCD9358898C68D056BA727EEBE78644EFC
SHA-256:	53A1373C331314E3A17B83A89AAF81766C28E0C55B5A814F85FEC7C04EDDBC0E
SHA-512:	0B177AA7ABBF9E4345DC0ABD6B982C8971A01ECFB34568B15C9CEF222BC9521199F19F71682D37F61AF8E6608170A119DF68323DAEE7C127B01F3CB97708214
Malicious:	false
Reputation:	low
Preview:	/*.** 2016-05-28.**.** 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 contains the implementation of an SQLite virtual table for.** reading CSV files..**.** Usage:.**.** .load ./csv.** CREATE VIRTUAL TABLE temp.csv USING csv(filename=FILENAME);.** SELECT * FROM csv;.**.** The columns are named "c1", "c2", "c3", ... by default. Or the.** application can define its own CREATE TABLE statement using the.** schema= parameter, like this:.**.** CREATE VIRTUAL TABLE temp.csv2 USING csv(.** filename = "../ http.log",.** schema = "CREATE TABLE x(date,ipaddr,url,referrer,userAgent)".**);.**.** Instead of specifying a file, the text of the CSV can be loaded

C:\Users\user\AppData\Local\Temp\emoji-travel-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	245
Entropy (8bit):	6.799965885939206
Encrypted:	false
SSDEEP:	6:6v/lhPysTDJwk/rbsobd9vbRyWtQ2DF9+EGbgsup:6v/7z3n9DRyWtrukN
MD5:	C5152E9074692BE446A7234C15D8168D
SHA1:	E1550AEFED9917D3ADABCC113318D6FA35F74260
SHA-256:	65F9B122E0735B5E18188420AFE0E1D49B290636AC6FEB4006DBA1C616B7BD67
SHA-512:	33FA7E9F48E2B638A292E39489FE67CDE02099BA0B6EDB9B30B20E6C3C9814C2F940EFE896B49437272BD0563BE0AFC0C4EFC6C66C86120487A866BD306F050 E
Malicious:	false

Preview:	.PNG........IHDR................a....sBIT....|.d.....IDAT8......0.......AxQB.(.@7$...x.....p>{.$...I....=...8.>1....U...($.R.K9...c...)aT..a.,[......kl..u.=.%7|..96@..#.!..<dg.f..<...m4..#.. w0.f..K...v....../X.~U.%.....=..K.v'dl....IEND.B`.

C:\Users\user\AppData\Local\Temp\iso_3166.xml

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	41363
Entropy (8bit):	5.191528382819999
Encrypted:	false
SSDEEP:	384:pihUuz2NdAbqF370l+8tWZAmzBJ7vGF+04IUuJRq4e1Z5S:6Uuzl+v8tWZAuuI04Ab8nk
MD5:	38D25CBB82CF16B9D71DDDED2A7B1016
SHA1:	838A61D41ECD85FF6F45D305F71C0F92EBA7AD84
SHA-256:	53AB9D04A1DD23BE7336BB9DF3E1998A5938E2E5696D3BF4DCB367D20D506F0B
SHA-512:	823D753BA289DEC05C616675D380DBD06B6E77A35AE567902C0A451C766843EB11E7F2838A53F22F6871E2D93CB0ADA957FA0E3EF2CA3869E43BE21A507FF13 F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" ?>.... ....WARNING: THIS FILE IS DEPRECATED.....PLEASE USE THE JSON DATA INSTEAD.....Usually, this data can be f ound in /usr/share/iso-codes/json.....This file gives a list of all countries in the ISO 3166..standard, and is used to provide translations via gettext....Copyright (C) 2002, 2004, 2006 Alastair McKinstry <mckinstry@computer.org>..Copyright (C) 2004 Andreas Jochens <aj@andaco.de>..Copyright (C) 2004, 2007 Christian Perrier <bub ulle@debian.org>..Copyright (C) 2005, 2006, 2007 Tobias Quathamer <toddy@debian.org>.... This file is free software; you can redistribute it and/or.. modify it under the terms of the GNU Lesser General Public.. License as published by the Free Software Foundation; either.. version 2.1 of the License, or (at your option) any later version..... This file is distributed in the hope that it will be useful,.. but WITHOUT ANY WARRANTY; without even the implied warranty of.. MERCHANTABILITY or FITNE

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

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	528
Entropy (8bit):	2.454669672012672
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32Zp9XojoW2mnKt3MGHlXml/4XSkVlXllXl/l5:idq2Vg3F+X32RojB5nKKZ4i
MD5:	56D41F7E91B9DCD5E8AF747A13C6004B
SHA1:	C59F6AE0DE9D72F3046293E9CEE3A8E5077A3F58
SHA-256:	9B8494152724313033EE4A2C2112212816F9C11AB5DEF42D3325617ADFF6DE49
SHA-512:	CB28A005BFE866102538AF218606269018D7B433DA559E3496C21A63815D439A397A1B9281C4DDEB1D575BC0645D4C0F8D6156171611534F9CA8F6124CB21CA5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......)...m.o.m.o.m.o...i.l.o.2.e.l.o.Richm.o.........PE..L......:...................... ....@...rsrc...............................@..@...... ....

C:\Users\user\AppData\Local\Temp\network-cellular-signal-excellent-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	127
Entropy (8bit):	5.509837934582196
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllnxnF1wQLLts39BBPa9UspcuRjp:6v/lhPysZf19J69PaxcuRjp
MD5:	B16AB36FAD8BB36B66DCF80B4447AAC5
SHA1:	020FC710033BB672D59DD3D23DCA5BE9FAD21ED9
SHA-256:	F41B83B907535EE547881030EE0F138651E711BB5943D7DC9FDBDE4A1B200D33
SHA-512:	4B45C9A71F0437269881A84C3144AE39DFF741F84516F9FA32863E7AED4F668A766AC550E6C2F9E5EA4238181124E5CF7F3B30458C954599B08E8116AB15B7EB
Malicious:	false
Preview:	.PNG........IHDR................a....sBIT....|.d....6IDAT8.c`..0...?.~&J]@..,D.Aq2.]@./.u2.]@./..d..`..@1....."l..$....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll

Process:	C:\Users\user\Desktop\PO#4200000866.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:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.........PE..L.....Oa...........!....."...........*.......@..............................p............@..........................B.......@..P...........................`.......................................................@..X. ...........................text.... ......."................. ..`.rdata..c....@.......&.............@..@.data...x....P.......*.............@....reloc.......`.......,.............@..B.. ....

C:\Users\user\AppData\Local\Temp\user-trash-full-symbolic.symbolic.png

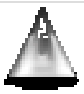
Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	357
Entropy (8bit):	7.118113286231142
Encrypted:	false
SSDEEP:	6:6v/lhPysrTeNeLussfmVacXJ0NzdkvArQFOs95hpKTFJrl0Cau3mOZK+pbp:6v/7LTwMufeacZ0Zd65yZn0C7ZKy
MD5:	CACAC26309C82D65E30BCC2CFCA0E51C
SHA1:	D18566ECAA9A916FCF0D3BF4D856D3DB8D673391
SHA-256:	4A4A91C24410D8CBB16314AAD56F2F751464CFBF88C3FCB27E92C1110AE34706
SHA-512:	33E88DC3E45EC413830582544EC31DFDEB270C685DDA51CD6D681B438F1208B6867976D9C382C39ED966ADE22ADC0B8962B6CF6B1C9D78081B26582BE3A53 A
Malicious:	false
Preview:	.PNG........IHDR................a....sBIT....|.d.....IDAT8....N.Q.E..T..*.@.........`AeBei....../.@~..l.. jhl,..*..(X..x..!..e...ww..<..%0..1...b....a..,...Z...q....V~.4..&p"..b.w*....gPuL..5......... ..|.oK..H)....g..~.........!.d.....}.b:.....h....gP...w.F...XRl...... ...j./...=.+ng....H.n.[D.........=.._u.5.<2.W...ty..;o[3..t.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.3914685624967245
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:	PO#4200000866.exe
File size:	379352
MD5:	5d0444b70ff5caa4ec3b2ca2e563e724
SHA1:	27309fdae9005f71dcde3501f023819ae6dba6cb
SHA256:	fd620fd2a9d5ca1dea1e11013eb4ec486f2f5cb340cd28bcbe39e78271fc5d26
SHA512:	436da2ee2bad47ef2027fb4a3dfda2e1070cb7c9a888bb594c4f25a15adb103f6c686e35b7d10bccad6f824a503fedebe6c6c5ba404ac8f50398837791d66e05
SSDEEP:	6144:ZYa6W/pzBlsLyHIlr3SkSHyO5AxPO5khaL6YSsA2gaRD:ZYwxY3pC3Qmeaqspt
TLSH:	2A84F141BBA8D4A7C5720B300CEA96A55ABDAD502996070B338077ED3FB37D19F1E319
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.....Oa.................h...*.....

File Icon



Icon Hash:	30b0e969e8dccc00

Static PE Info

General

Entrypoint:	0x403640
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:	0x614F9B1F [Sat Sep 25 21:56:47 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:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Cunzie3 Brevsamlerens9 ", O=hovedstningers, L="Chemnitz, Sachsen", S=Sachsen, C=DE
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/11/2022 8:49:05 AM 5/11/2023 8:49:05 AM
Subject Chain	• CN="Cunzie3 Brevsamlerens9 ", O=hovedstningers, L="Chemnitz, Sachsen", S=Sachsen, C=DE
Version:	3
Thumbprint MD5:	7EB0C866C3B021249A083B3B2649C8F2
Thumbprint SHA-1:	16CC515505D981DB017A84FD49AAD119D768FE27
Thumbprint SHA-256:	674CD0F94F9959B355B9421AE98E15ED7994315E7C5BE0D60BF14B056E24CF52
Serial:	947ABF3A4FA2102E

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
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

Instruction
test eax, eax
jne 00007F0A1CA0375Ah
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 00007F0A1CA0372Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], 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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d000	0x284c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5ab38	0x1ea0	.rsrc
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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x22000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4d000	0x284c0	0x28600	False	0.253543440402	data	3.51609274329	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4d358	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x5db80	0x94a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x67028	0x5488	data	English	United States
RT_ICON	0x6c4b0	0x4228	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x706d8	0x25a8	data	English	United States
RT_ICON	0x72c80	0x10a8	data	English	United States
RT_ICON	0x73d28	0x988	data	English	United States
RT_ICON	0x746b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x74b18	0x120	data	English	United States
RT_DIALOG	0x74c38	0xf8	data	English	United States
RT_DIALOG	0x74d30	0xa0	data	English	United States
RT_DIALOG	0x74dd0	0x60	data	English	United States
RT_GROUP_ICON	0x74e30	0x76	data	English	United States
RT_VERSION	0x74ea8	0x2d8	data	English	United States
RT_MANIFEST	0x75180	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, 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	Metaldyne Corporation
FileVersion	26.10.23
CompanyName	Peoples Energy Corp.
LegalTrademarks	Fifth Third Bancorp
Comments	Wm Wrigley Jr Company
ProductName	Home Depot Inc.
FileDescription	Micron Technology Inc.
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: PO#4200000866.exe PID: **5108**, Parent PID: **5604**

General

Target ID:	0
Start time:	14:38:43
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\PO#4200000866.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO#4200000866.exe"
Imagebase:	0x400000
File size:	379352 bytes
MD5 hash:	5D0444B70FF5CAA4EC3B2CA2E563E724
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.777573204.0000000003AA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshE67.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nshE68.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsn105D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsn105D.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	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	406184	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\KUNDSKABSRIGESTES.Ina	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\DeviceServicePlugin.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Galvanosurgery9.hom	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ac-adapter-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\csv.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\emoji-travel-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\iso_3166.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\library.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\network-cellular-signal-excellent-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\user-trash-full-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	726	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshE67.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsn105D.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsn105D.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile
unknown	37319	24480	75 6e 6b 6e 6f 77 6e	unknown	success or wait	16	406224	WriteFile
C:\Users\user\AppData\Local\Temp\KUNDSKABSRIGESTES.Ina	0	16384	fd fd 66 0f 68 fd fd d0 fd 26 15 fd 3f 41 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 25 11 fd 56 05 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 0f fd fd fd fd fd fd fd fd 34 fd fd 4a 48 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 0f fd fd fd fd fd fd 66 0f fd fd 66 0f fd fd fd fd fd 33 fd 3c 6a 1e 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 77 66 fd fd 00 fd fd fd fd fd fd 66 0f fd 1b fd fd fd	fh&?A%V4JHff3<jwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwff	success or wait	6	406224	WriteFile
C:\Users\user\AppData\Local\Temp\DeviceServicePlugin.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 53 fd fd 32 30 32 30 32 39 4a 73 fd fd 32 fd fd 5a 74 32 fd fd 5a 6b 32 fd fd 5a 78 32 fd fd 5a 72 32 fd 26 5b 72 32 fd 11 5b 73 32 fd fd 5a 72 32 fd fd 5a 65 32 30 32 fd 6b 32 fd 15 5b 7a 32 fd 15 5b 71 32 fd 15 5b 1f fd fd 32 30 32 77 fd fd 32 fd	MZ@!L!This program cannot be run in DOS mode.$S222Js2Z2Z2Z2Z2&[2[2Z2Z22k2[2[2[22w2	success or wait	13	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Galvanosurgery9.hom	0	16384	fd fd 0c fd 6c fd fd fd 2b 5a 70 22 21 fd 5c fd 7a fd 7c fd 66 7c 1b 6f fd fd fd 1e fd b1 22 fd 78 3d ee 26 42 40 fd fd fd 4f 15 0f 55 fd 61 64 fd 36 fd fd fd fd 3a 50 fd 69 2e fd 5d 19 ff fd fd 45 fd 6e 0d fd 04 fd fd fd 3c fd fd 65 fd fd 3d 1c fd 06 1a 23 44 43 44 fd fd fd 3d 4b fd 68 1b 60 04 fd 1b 3a 7c fd 06 fd 3a 37 fd fd 6d 0e fd 6f 79 17 fd fd fd 38 76 55 fd 42 fd 99 04 51 fd 52 fd fd 7d 03 31 fd 2e 14 45 fd fd 4a 5f 42 fd fd fd 69 9c 35 70 fd 34 2e 32 74 59 46 fd 6c 3c fd 41 fd 6c 74 37 5a fd 1c fd fd 3e fd 0f 5e 4a fd fd fd 26 fd 7a fd 27 fd 78 0e fd 17 fd fd 46 93 1e fd fd 68 0f fd 70 fd fd 0d fd 5c 30 fd 3d 79 15 fd fd fd 76 fd fd fd 07 47 5b fd 22 3f fd fd 3f 55 50 76 5d fd fd 63 fd fd fd 30 fd 02 fd 0e 02	l+Zp"!\z|f|o"x=&B@OUad6:P.]En<e=#DCD=Kh`|:7moy8vUQR}1.EJ_i5p4.2tYFl<Alt7Z>^J&z'xFhp\0yvG["??UPv]c0	success or wait	16	406224	WriteFile
C:\Users\user\AppData\Local\Temp\ac-adapter-symbolic.symbolic.png	0	290	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 fd 49 44 41 54 38 fd fd fd 31 4b 03 31 00 fd fd fd 49 41 5a 5c fd fd fd fd fd 41 27 27 42 fd fd fd fd 51 5d fd 3c 0e 5d 5c 3a 76 fd 49 fd fd 20 0f 50 1c 24 0e fd 49 fd fd 33 3e 08 17 bd fd fd fd 6f fd fd 18 4d fd 7f 61 fd 45 6a 6e 15 00 27 18 61 fd fd 1d fd fd fd 74 fd fd 64 1e 70 fd 65 fd fd fd 1d a0 20 7a fd 4f 72 40 fd fd 5a fd 26 6d 52 fd fd 54 63 fd 4b 0b 2e 69 fd 6a fd 47 1c fd 05 fd fd 50 57 fd 74 fd 12 17 5d fd 74 01 66 71 31 fd fd fd fd 18 55 fd 06 47 05 fd fd 16 10 22 64 17 6f fd 5b fd 16 fd fd 01 7b 78 fd 19 3e fd 0b 38 fd 13 fd 58 75 fd 4a fd 71 18 fd fd	PNGIHDRasBIT|dIDAT81K1IAZ\A"Q]<]\:vIP$I3>oMaEjn'atdper@Z&mRTcKijGPWt]tfq1UG"do[{x>8XuJq	success or wait	1	406224	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\csv.c</td><td>0</td><td>16384</td><td>2f 2a 0a 2a 2a 20 32 30 31 36 2d 30 35 2d 32 38 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</td><td>/*** 2016-05-28**** 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</td><td>success or wait</td><td>2</td><td>406224</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\emoji-travel-symbolic.symbolic.png</td><td>0</td><td>245</td><td>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 fd 49 44 41 54 38 fd fd fd fd 0d fd 30 10 04 fd fd 1b fd fd 41 78 51 42 fd 28 05 40 37 24 12 fd 07 78 fd 0c fd fd 03 70 3e 7b fd 24 fd fd fd 49 fd fd bb fd 3d fd fd fd 38 00 3e 31 fd fd 0b fd 55 06 72 02 28 24 fd 52 fd 4b 39 fd fd fd 63 02 fd fd 29 61 54 fd fd 61 fd 2c 5b fd 04 fd fd fd 17 6b 6c 5f f2 75 fd 3d 18 25 37 7c fd fd 39 36 40 09 fd 23 fd 21 fd 01 3c 64 67 fd 66 19 fd 3c 84 fd 1b 6d 34 11 07 23 fd fd 77 30 01 66 fd fd 4b fd fd 16 76 0f fd fd 1f 7f 13 2f 58 fd 7e 55 fd 25 fd fd fd fd 1c 3d fd 14 4b fd 76 27 64 6c 00 00 00 00 49 45 4e 44 fd 42 60 fd</td><td>PNGIHDRasBIT|dIDAT80AxQB(@7$xp>{$I=8>1U($RK9c)aTa,[klu=%7|96@#!<dgf<m4#w0fKv/X~U%=Kv'dlIENDB`</td><td>success or wait</td><td>1</td><td>406224</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iso_3166.xml	0	16384	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 3f 3e 0d 0a 0d 0a 3c 21 2d 2d 0d 0a 0d 0a 57 41 52 4e 49 4e 47 3a 20 54 48 49 53 20 46 49 4c 45 20 49 53 20 44 45 50 52 45 43 41 54 45 44 2e 0d 0a 0d 0a 50 4c 45 41 53 45 20 55 53 45 20 54 48 45 20 4a 53 4f 4e 20 44 41 54 41 20 49 4e 53 54 45 41 44 2e 0d 0a 0d 0a 55 73 75 61 6c 6c 79 2c 20 74 68 69 73 20 64 61 74 61 20 63 61 6e 20 62 65 20 66 6f 75 6e 64 20 69 6e 20 2f 75 73 72 2f 73 68 61 72 65 2f 69 73 6f 2d 63 6f 64 65 73 2f 6a 73 6f 6e 2e 0d 0a 0d 0a 54 68 69 73 20 66 69 6c 65 20 67 69 76 65 73 20 61 20 6c 69 73 74 20 6f 66 20 61 6c 6c 20 63 6f 75 6e 74 72 69 65 73 20 69 6e 20 74 68 65 20 49 53 4f 20 33 31 36 36 0d 0a 73 74 61 6e 64 61 72 64	<?xml version="1.0" encoding="UTF-8" ?> WARNING: THIS FILE IS DEPRECATED.PLEASE USE THE JSON DATA INSTEAD.Usually, this data can be found in /usr/share/iso-codes/json.This file gives a list of all countries in the ISO 3166standard	success or wait	3	406224	WriteFile
C:\Users\user\AppData\Local\Temp\library.dll	0	528	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 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 29 fd 01 fd 6d fd 6f fd 6d fd 6f fd 6d fd 6f fd fd fd 69 fd 6c fd 6f fd 32 fd 65 fd 6c fd 6f fd 52 69 63 68 6d fd 6f fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 0c fd fd 3a 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 00 40 00 10 00 00 00 10 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$)momomoilo2elo RichmoPEL:@	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\network-cellular-signal-excellent-symbolic.symbolic.png	0	127	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 36 49 44 41 54 38 fd 63 60 fd 10 30 fd fd fd 3f fd 7e 26 4a 5d 40 fd 01 2c 44 fd 41 71 32 fd 5d 40 13 2f fd 75 32 fd 5d 40 15 2f fd fd 64 fd fd 60 18 18 40 31 00 00 fd fd 04 22 6c fd fd 24 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d6IDAT8c`0?~&J]@, DAq2]@/u2]@/d`@1"l$IENDB`	success or wait	1	406224	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\user-trash-full-symbolic.symbolic.png</td><td>0</td><td>357</td><td>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 01 1c 49 44 41 54 38 fd fd fd fd 4e 02 51 10 45 fd 2e 54 10 1a 2a fd 40 fd fd fd fd 01 fd 18 fd 7f 60 41 65 42 65 69 fd 03 7f fd fd fd 2f fd 40 7e fd 0e 6c fd fd 20 6a 68 6c 2c fd 10 2a 09 fd 28 58 fd fd 78 fd 0d 21 fd fd 65 fd fd fd 77 77 fd fd 3c fd fd 25 30 00 fd 31 fd 1b fd 62 09 fd 12 fd 61 0a fd 2c 09 fd fd 5a 08 fd 78 71 1c 11 fd fd 56 7e 0a 34 2d fd 26 70 22 92 fd 62 06 77 2a fd 1c fd fd 67 50 75 4c e4 fd 35 fd fd 0a 05 fd fd 1d 01 19 e0 08 7c fd 6f 4b fd 01 48 29 fd fd fd fd 67 fd 01 7e fd 03 fd 0f fd 0a fd 09 fd 21 09 64 fd fd f8 fd 02 7d fd 62 3a 04 fd fd fd fd 68</td><td>PNGIHDRasBIT|dIDAT8NQE.T*@`AeBei/@~ljhl,*(Xx!eww<%01ba,ZqV~4&p"bw*gPuL5|oKH)g~!d}b:h</td><td>success or wait</td><td>1</td><td>406224</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO#4200000866.exe	unknown	512	success or wait	398	4061F5	ReadFile
C:\Users\user\Desktop\PO#4200000866.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nshE68.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nshE68.tmp	unknown	8802	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nshE68.tmp	unknown	4	success or wait	18	4061F5	ReadFile
C:\Users\user\Desktop\PO#4200000866.exe	unknown	16384	success or wait	10	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Galvanosurgery9.hom	unknown	2	success or wait	443	40275E	ReadFile

Disassembly

No disassembly