ID: 635097
Sample Name: recibo.exe
Cookbook: default.jbs
Time: 13:15:13
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

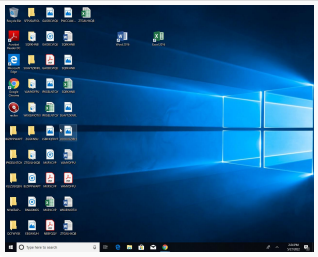
Windows Analysis Report

recibo.exe

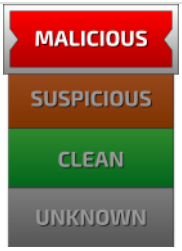
Overview

General Information

Sample Name:	recibo.exe
Analysis ID:	635097
MD5:	4680729edca682..
SHA1:	debf5126050330..
SHA256:	e18032a74c8138..
Tags:	exe
Infos:	



Detection



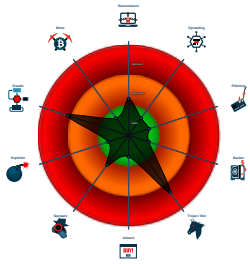
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- recibo.exe (PID: 3224 cmdline: "C:\Users\user\Desktop\recibo.exe" MD5: 4680729EDCA682D1B6DE8CF875BBFDF5)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1EX-TfU9P_N_SsQAtVtT8-t2zzMXng6WS"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.761876778.0000000002A50000.00000040.00001000.00020000.00000000.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

Data Obfuscation

Yara detected GuLoader

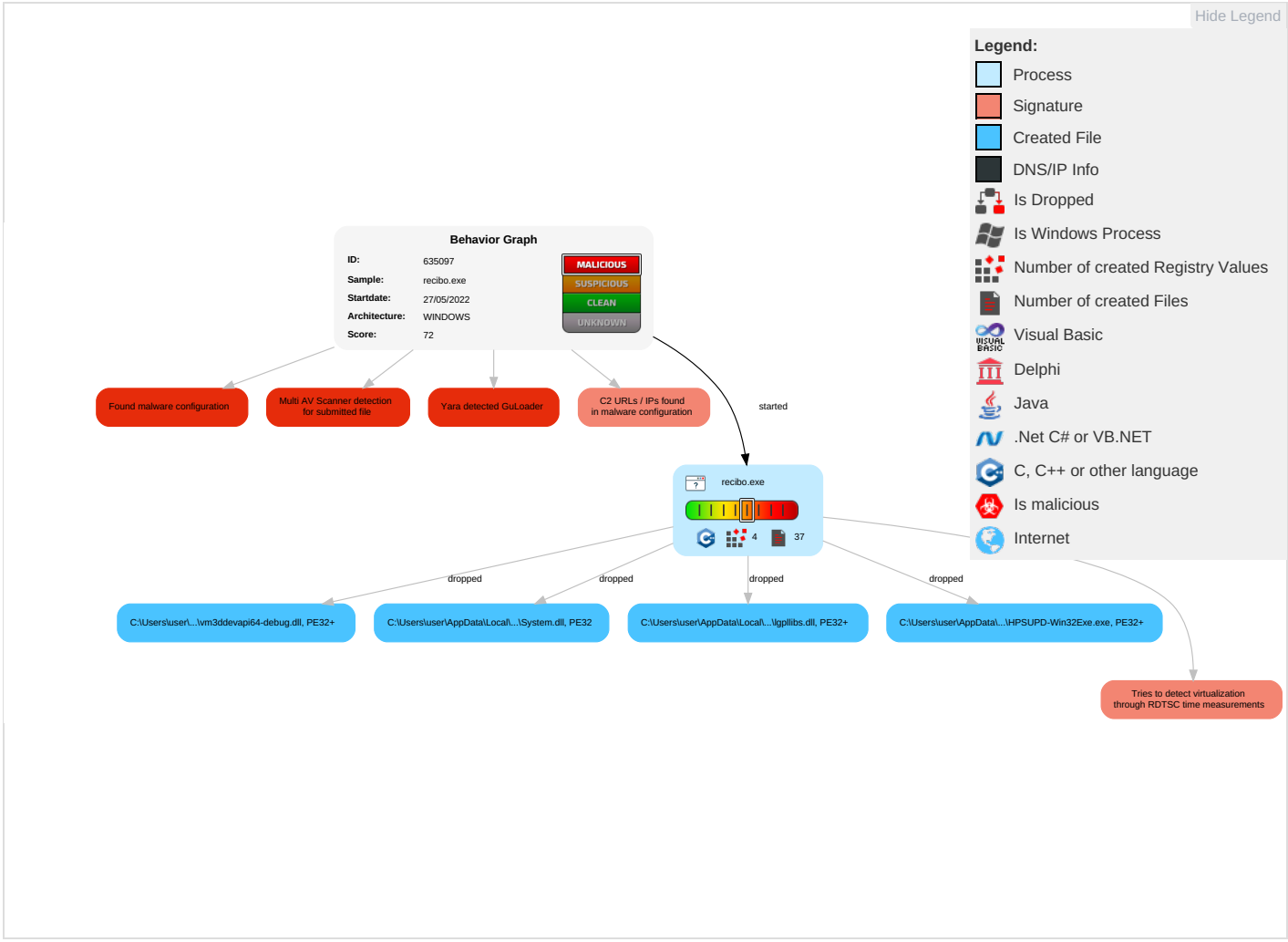
Malware Analysis System Evasion

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	1 Windows Service	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Windows Service	1 Obfuscated Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Timestomp	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

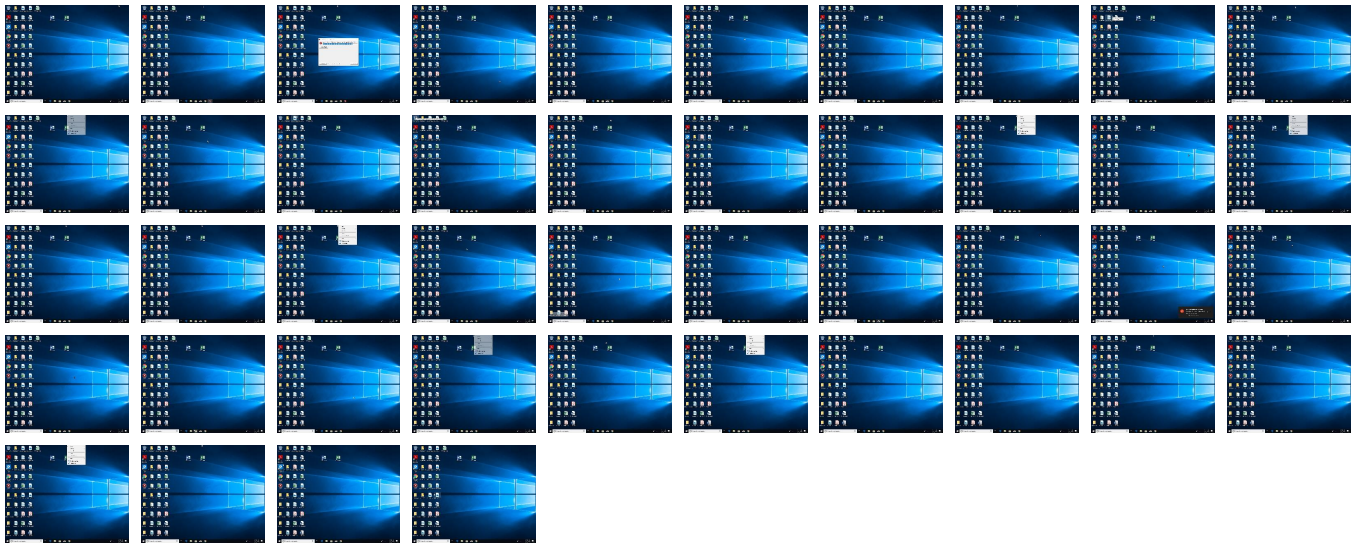
Behavior Graph



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
recibo.exe	55%	Virustotal		Browse
recibo.exe	26%	Metadefender		Browse
recibo.exe	50%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://mozilla.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sil.org/iso639-3/	iso_639-3.xml.0.dr	false		high
http://www.vmware.com/0/	recibo.exe, 00000000.00000002.761476867.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3ddevapi64-debug.dll.0.dr	false		high
http://www.vmware.com/0	recibo.exe, 00000000.00000002.761476867.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3ddevapi64-debug.dll.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	recibo.exe	false		high
http://www.symauth.com/cps0(	recibo.exe, 00000000.00000002.761476867.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3ddevapi64-debug.dll.0.dr	false		high
http://www.symauth.com/rpa00	recibo.exe, 00000000.00000002.761476867.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3ddevapi64-debug.dll.0.dr	false		high
http://https://mozilla.org0	lgpllibs.dll.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635097
Start date and time: 27/05/202213:15:13	2022-05-27 13:15:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	recibo.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.1% • Quality standard deviation: 21.6%
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, wuapihost.exe
- 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, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, time.windows.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

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\Adventure_19.bmp

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	10521
Entropy (8bit):	7.888779038440803
Encrypted:	false
SSDEEP:	192:oXRZxdt62XpqRigPYtY0CfKTQlh5NKW6F5oJxfskCjGmXa6Pbpwr4WmKM:KRfdt62X+XoElh/KW6ifskEGealpwr4n
MD5:	8D61CCB44C962D7831FB6703B4AF623D
SHA1:	2BFDC667151057B3A42CDD22F9EB0E5AB0B0EF3C
SHA-256:	1EFFB5A4A46B05C024518546D4C8BBB45AD3496590E3E86AF533CF31C61512F4
SHA-512:	FE0C304F73713552ACA3A28D9CCD6BD2C53A45F72052892CC8F94D835A213F2F3C4D8D1656BD8160AE874A63FACC6B79BA763D4A724281E5F0DEDAC87F8637 E
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*......Q...........Q..........aQ..........a.......C..C...n.n..".......... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?.....(..9...k....X.....&.2.Z.......k~I.....e...J...}..<..M..8.........."..../...O.u...........5.h...71]ZZ......v..Yc...<.i'..m2_..>..#...K...,.qq.^<2\|D.V...j..ae.0Mu.^K..#k..3<."F V$HV.)..vmG..H........z.\..#......3_..Wo.g.>.o..........|...V.}.Ho.]...q#..W667Z`..)..l._E'.....+\.w..K....O.o..5......4O..~.

C:\Users\user\AppData\Local\Temp\FLADBARMEDES.tub

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	data
Category:	dropped
Size (bytes):	95635
Entropy (8bit):	6.715584422233703
Encrypted:	false
SSDEEP:	768:9hlBFBNMGjjT0QwOqKvIRnCkPFG4ouc83ArsfQFaFL03ZLoeZ4YgXplXpyfHqvds:91XNMjjEqnIfsVFIhBQlYG22vAlGI
MD5:	0DBDB94BF9F058978C90852607F98DBD
SHA1:	DCA1907D14891499D855DEB23BF461799C7ED0C4
SHA-256:	11D6302EBD701AD527EC6358E33FC578AE0D88AC9A43AC03F4AD5276B186538E
SHA-512:	0D6C48216172958EFE0E305B81D8B0B5C3606F001969E80220D4EBCF818013416992BC8D0638F4B0F6E337040CCABD607731F1912BA9DCFAA2E69C824CFC287
Malicious:	false
Reputation:	low
Preview:	.i.....f....q._f....5j..k..<.f...........).Tsc......................................{Z&n..f.v........!`..}............................f...Of.....f.......f.v..([...lllllllllllllllllllllllllllllllllll.........f.. ..c..3B..!..!,O....n...f...f.e..0...@..g.......).D.>))...........f.....w?..PPPPPPPPPPPPP PPPPPPPPPPPP......t.........0...e..f.e../..~6...T7.z.......................................f.....f.i.f.t.f......-.j1.33333333333333 3333333333333333333333333333f..f.....f.q..f.......w.....f....5.G.[[...f.g.f.q.f.........$.pS.OOOOOOOOOOO OOOOOOOOOOOOOOOOOOOOOf...........f.q. .*..,..

C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	58368
Entropy (8bit):	5.856484138583398
Encrypted:	false
SSDEEP:	768:t2y20tpnvfSd9bbM9tmRtTkwv9QMdVk1QKVnjphRJy26xG0XFC19Io:J20t1SdN0kvZ9pdW1QKVjzy26opD
MD5:	D600D4F40A2BE641991044EE0814BFA4
SHA1:	3BDEF3488C28D43D285C47F46B82B980A8F41CD8
SHA-256:	B0D12A7AADF51B02D52E9E88295E6E6606F68C1508C8D9323B6549AA20EC82AA
SHA-512:	27B125260AA56FCAD4153A3259ECFB898681C9B096A4A37EB32AC3B722599EA4BFB5BF00F0247136F11F73F280B85844B37F6236331A0EF3B90ED2EC70CEDA5 5
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...Kc.....".....0..... .....@..... ....`...@.....@..... ..... .....8..... ..H.....text..... ..... ..`.rsrc.....@.. @.....H.....W..4.....N.((.....tS...}....*F.{....o....s....*F.{....o....s....*.0.....{....o....s.....&....*.....J.{....o.....s. ...*..((...*~.()....tV...}.....s....}....*2.{....o....*2.{....o....*F.{....o....s....*2.{....o....*2.{....o....*F.{....o....,..*.*2.{....o....*2.{....o....*2.{....o....*2.{....o....*2.{....o....*:.s....%.}y...*..(....*:. ().....}....*..(*....,...}....+.r...ps+...z.....s4...}....*.0.....

C:\Users\user\AppData\Local\Temp\Rekorddage.Res7

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	37188
Entropy (8bit):	3.999253187571331
Encrypted:	false
SSDEEP:	768:cqLtUhAIasZdPK3ukVO7103q1LjVG0I6Z93rWa1FLXSBhuj3KmuzoAgZ:coUvbkVORtVjVG0I6rbWa1FzSBh0Go9Z
MD5:	6001AAC06A6EB2B760F3DC4BE1B2D3F8
SHA1:	A88A72756DB347DE9507495A9F6D5E521EB5FB42
SHA-256:	0E1AB3CD23AE04019CAEBE185924D859E7017E933F824B1CBEB50FAD08B0CC76
SHA-512:	B400F2609A8E67BD53062E73FE8A0BD3960CD62A0D388F228C1DE4A01627C4A07F42961161CC2195DEA6961BBC43FF25E6E0E67963A55FEA31B42050F3C6842
Malicious:	false
Reputation:	low
Preview:	65FF458D7673B103962E00EB3124B20464827DB078E548E8A294899303A2D4B26244CDE2525A3176A4E8EBA229CBF8215F529302F79215A66E248561 9280B9F07D0F5D7F34853DD732803E9230FA52E1368AFF3ADB4D69A11E23189F458C5DB8C643DA0D9C2FBB18945457C8F6C9CE23E60636F70ED55FAA 0F0C6C12C79B7EC3AAEA70A1DA1D0A6F4F5FE558AB0E2C6E1C29796F8931D2F8D428465CA7B637D8F02AE89A7AC93A554AB4667C122E746A0090527C 71C6DE714F7C92C3B3C6C3970A6DF5E1810DD362093C012F8F022960DE89C2174441BB0FCDF3214938109206CFA36DEF03346BD5D65E022846E74B01 DC01A4AFA966C7D6FE4E9EAA973F402B465DE3D3D7D5424D98589A10A91BEDF63045FF792C2DF90C9B9AFEC37C0771B9771106EF952D5D913FD36B65 38078F86A1E71008D07CDA61CB102D1679ED96F46C7C5F5C7AEC4E409B023EAC095B78197F5C16F47795D7253A585A700005C1FBF8C869BD318613FB 508D946B75C70E99290F433B81CDFD660CEB126BC9EECFF96DE3B07B3E652ABD795716A914383F7009FF2440C2E1640CB16C11292430FF09E9077E6F CD41DA51CCF89AC2E3C46AD8DB2EF7B13C1DFD1115D44D55B201C10395327AF3A23C988789BFB543EB8635EF4F041E3EA55BE51BDFD81F99B56BF001 0BDF14B112E35982A7579BE396E235B34EFA0C08

C:\Users\user\AppData\Local\Temp\emoji-body-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	193
Entropy (8bit):	6.41289035005742
Encrypted:	false
SSDEEP:	6:6v/lhPys693pMeNKrccoz4OtOOFImbTM0t7zlyH//jp:6v/7adpfNWcVkqfTMyUf1
MD5:	F492568998D5783731D50D7CA73AC7A3
SHA1:	E87B96367BDB02176067336A1CCE3B32EBDCB3B2
SHA-256:	7A08D7B1CC724A453A0C3EB2F36369D7FD6AC6BD965CE0B4D075D570ED369A9B
SHA-512:	2C6C726426EA6DD4C7CCC141152E24DD46BDB11D3DB45ED7BA6EAC06DE922F69E5172D5431D63B9ACF96E54B89857317CA0F87880F7B03C43AF9F7416EE95 73
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d....xIDAT8.....0.E..#d.{Gp.k.q.WP....,m..$.BH....s...A<...9..L..Fp.E..7.....`.....6.n....]b.5...P.....r.W..#....U_....p.P.>.&.1.....IEND.B`.

C:\Users\user\AppData\Local\Temp\iso_639-3.xml

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1063988
Entropy (8bit):	4.881622518734141
Encrypted:	false
SSDEEP:	6144:z6ZdTZZl/WX4fVLcf9MvAadpxr5+ZiVHPZ6TZXjcePr:z6nTZZl/WX4fVLcqvV5+ZiX6TZXJ
MD5:	DCAD3B0F729144CE9EE9A6006D9C3E74
SHA1:	3EEF5F61BEF834B7089A87423D128990A1065E81
SHA-256:	D8AB9C2641481645A8ACF875FFA3E3CB271D2CD946691DD8E0BD48513FFF1370
SHA-512:	BB0ED1F9FBB122728776731B04C54C8FBA57BF2987D04DAD1167FC879FC8A2483093E1A8304A021D6238B408FED826E902386D7DB52B7988CE9DCC89ACB646 1
Malicious:	false
Reputation:	low

Preview:	<?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 languages in the ISO 639-3..standard, and is used to provide translations via gettext....Copyright . 2005 Alastair McKinstry <mckinstry@computer.org>..Copyright . 2008,2012,2013 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 FITNESS FOR A PARTICULAR PURPOSE. See the GNU.. Lesser General Public License for more details..... You should have received a co

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

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37816
Entropy (8bit):	6.374742588554942
Encrypted:	false
SSDEEP:	384:VbijnYW+DZZMwrusWsWQfRl30fP5/A5KFUkYvntA/QcP+ACxw/3MvDG/GhUVgt:dijnQDnzruRNQfv0fP5/oABCDGehHt
MD5:	9B623087B905D8FE157BDB7EC85009A8
SHA1:	4B6DD4C0292558513A840B40A991533735D55E02
SHA-256:	7FA4C9EA4BE0088D6D311BD93FA65BAF8828DA32A2FD4BF8CE0EADE552D46246
SHA-512:	8C06714F93EB05FAD19F1A96C0DB8FF030B1CD3C03D6B17C231CDE5BCE8DD8358014D87A74306C3BABEF7C573D4AF5AE80904AFBB0329D2D83FE3758EF02019
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...>..b......" .....F...*.....P.....`A.....@g.....n..x.....t.....Te.....`.....o..X.....text...FE.....F..... ..`.rdata..p...`.....J..... @..@.data...@.....d.....@....pdata.....f.....@..@.00cfg.....l.....@..@.rsrc.....n.....@..@.reloc.....r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\microphone-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1401
Entropy (8bit):	5.11645334711433
Encrypted:	false
SSDEEP:	24:t4CjIza3LWdwpQiL6Rch3jV81hF3Q59UPFkyKbRAecFhBrN3AGMH:1cL8w6iJjV8jF3894kNtAecFZTMH
MD5:	BAE5EB7B918D568E955B8885EEB5DB5A
SHA1:	FC4421C6A019D0147A13B08CBB2F0720F49E17C3
SHA-256:	273F11F9F8BD84F2A32E0CC857E21050A9A9C7713F33D9A220991DC232C470BA
SHA-512:	8A6AE1E26C9451A241655242D16368D87E23036D03D61FF75F5669D5E2930446D6003D5191622F576060E529EE21DD6E28D3408D28719A4D53BD291E673037B0
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <g fill="#2e3436">. <path d="m 213.531,228.469 -1.061,1.061 14,14 1.062,-1.062 z" transform="translate(-212 -228)"/>. <path d="m 220,228 c -1.662,0 -3,1.338 -3,3 v 1.64453 l 5.2832,5.2832 C 222.72383,237.4058 223,236.73965 223,236 v -5 c 0,-1.662 -1.338,-3 -3,-3 z m -6,6 v 2.00977 c 0,2.96574 2.16538,5.4238 5,5.90039 V 244 h 2 v -2.08984 c 0.64598,-0.10861 1.24984,-0.33194 1.80859,-0.62891 l -1.11132,-1.11133 C 221.17391,240.38 220.60353,240.5 220,240.5 c -2.50669,0 -4.5,-1.99014 -4.5,-4.49023 V 234 Z m 10.5,0 v 2.00977 c 0,1.15729 -0.44099,2.19439 -1.14844,2.98632 l 1.05274,1.05274 C 225.38802,238.9836 226,237.57264 226,236.00977 V 234 Z m -7.5,1.47266 V 236 c 0,1.662 1.338,3 3,3 0.16422,0 0.3216,-0.02370.47852,-0.0488 z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-se

C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll

Process:	C:\Users\user\Desktop\recibo.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false

Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 3%, 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\printer-symbolic.svg	
Process:	C:\Users\user\Desktop\recibo.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	213
Entropy (8bit):	4.950492507724413
Encrypted:	false
SSDEEP:	6:tI9mc4slzcpG+xW6UmUuksJtjdU0t/ZME:t4Cp9xW6zUmjW0tOE
MD5:	A4ACDD85E11EA101F3BB4B5BEC3382F0
SHA1:	2DC81694D5D3C403BF696B1796385D2F64C40D77
SHA-256:	AD87999B06B9C8035CCAC8EF29D54C9E00055EE9E2DBDD9B7BA24CCF56C471E6
SHA-512:	6C7C1E913CBF7CD6B91721BD60705B3A87C398B5D69D1FA03D67EDF7C69E23AB410938EC5E0770584E5B6E218443E53A702BD389C2253F05C2D4F48B944D481E
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z"/><path d="M4 9v5h8V9z"/></g></svg>

C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	
Process:	C:\Users\user\Desktop\recibo.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	288328
Entropy (8bit):	6.5244639850667605
Encrypted:	false
SSDEEP:	6144:TWMbKY5G780mQB8fkrOX9rn8ndvcA5abagLgandSUbJ:aMbKY5AlvfkSX9rSdkfbanUbJ
MD5:	9ECB2FA510DCDF4BFB06DC80A83294BD
SHA1:	65E0CEC428D010B94D81BA784EA709EBA598A1CD
SHA-256:	865868E3BE461332134EFBBA9F1D8AAA5E29A0C8AD3F5A2AC47311F47D4CFD62
SHA-512:	6F70D42EE2A6CA1F2D85A84947B74EAD03FA4CD00AE5D897FC80832111D88B0D9EEFE81B5FFBC229AE9E1D97467713AF0D385C8C2E96D67B5E9008033C02CE28
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....[.....s.....s.....s.....M.....z.....z.....G.....Rich.....PE..d.....`.....".....j.....N.....`A.....p.....x!.....Hb.....8.....8.....4...@.....text.....`..`.rdata.....@..@.data...0#.....@....pdata..x!.....".....@..@.didat..`....@.....@....gehcont$....P.....@..@_RDATA.....`.....@..@.rsrc.....p.....@..@.reloc.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.397735144960236
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:	recibo.exe
File size:	606778
MD5:	4680729edca682d1b6de8cf875bbfdf5
SHA1:	debf5126050330ecbfc29582d979101cd557dd42

SHA256:	e18032a74c8138c907ab2b6937ce66a4483a85e89b05a25153499efee4e85898
SHA512:	d1eaca1d1513ea5732f05dff1ad527aa48fbdab35386f73bb08a1e5d85569dd80a84217d78ca55a68688deb82a556f5338f45bccbfa16007014d6df2674624d9
SSDEEP:	12288:5bspFskmgHwg9jXbgO1xzSs9IKTQWfsmuYUD:5bsLskmZc0k9IKTQWkmuZD
TLSH:	4FD4F154BAC8ECABD01691785476AF656AD3EE1218358903173E3E2FF772193343B81E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	38e6d3b1b3a2cc71

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007EFE60AA23BAh

Instruction
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 00007EFE60AA238Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6b000	0x27620	.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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x35000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6b000	0x27620	0x27800	False	0.363744808149	data	4.74589509923	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6b2f8	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x7bb20	0x94a8	data	English	United States
RT_ICON	0x84fc8	0x5488	data	English	United States
RT_ICON	0x8a450	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 6356992, next used block 0	English	United States
RT_ICON	0x8e678	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x90c20	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x91cc8	0x100	data	English	United States
RT_DIALOG	0x91dc8	0x11c	data	English	United States
RT_DIALOG	0x91ee8	0xc4	data	English	United States
RT_DIALOG	0x91fb0	0x60	data	English	United States
RT_GROUP_ICON	0x92010	0x5a	data	English	United States
RT_VERSION	0x92070	0x270	data	English	United States
RT_MANIFEST	0x922e0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Insweepi

Description	Data
FileVersion	27.29.17
CompanyName	CHRYSALIDAH
LegalTrademarks	Vrdi24
Comments	reconnoiterlbni
ProductName	petiolispill
FileDescription	Pratalkoholis
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: recibo.exe PID: 3224, Parent PID: 2436

General

Target ID:	0
Start time:	13:16:17
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\recibo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\recibo.exe"
Imagebase:	0x400000
File size:	606778 bytes
MD5 hash:	4680729EDCA682D1B6DE8CF875BBFDF5
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: 00000000.00000002.761876778.0000000002A50000.00000040.00001000.00020000.00000000.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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nst55CD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nso5699.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso5699.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsz57C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsz57C4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FLADBARMEDES.tub	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Adventure_19.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Rekorddage.Res7	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\emoji-body-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\iso_639-3.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\microphone-disabled-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\printer-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsx6031.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsx6032.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsx6033.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsx6034.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsx6035.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nst55CD.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nso5699.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nso5699.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\FLADBARMEDES.tub	0	26185	0f 69 fd fd fd fd 66 0f fd fd 0f 71 fd 5f 66 0f fd fd fd 35 6a fd 0a 6b 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 fd fd 3c 0b 66 0f fd fd fd fd fd fd fd fd fd 29 0d 54 73 63 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 7b 5a 26 6e fd fd 66 0f 76 fd fd fd fd fd fd fd fd 21 60 fd fd 7d 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 66 fd fd fd 4f 66 0f fd fd fd fd 66 0f fd fd fd fd fd fd 66 0f 76 fd fd 28 5b fd fd 01 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c fd fd db fd fd fd	ifq_f5jk<f)Tsc{Z&nfv!`}fOfffv([llllllllllllllllllllllllllllllll	success or wait	4	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Adventure_19.bmp	0	10521	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\Rekorddage.Res7	0	28313	36 35 46 46 34 35 38 44 37 36 37 33 42 31 30 33 39 36 32 45 30 30 45 42 33 31 32 34 42 32 30 34 36 34 38 32 37 44 42 30 37 38 45 35 34 38 45 38 41 32 39 34 38 39 39 33 30 33 41 32 44 34 42 32 36 32 34 34 43 44 45 32 35 32 35 41 33 31 37 36 41 34 45 38 45 42 41 32 32 39 43 42 46 38 32 31 35 46 35 32 39 33 30 32 46 37 39 32 31 35 41 36 36 45 32 34 38 35 36 31 39 32 38 30 42 39 46 30 37 44 30 46 35 44 37 46 33 34 38 35 33 44 44 37 33 32 38 30 33 45 39 32 33 30 46 41 35 32 45 31 33 36 38 41 46 46 33 41 44 42 34 44 36 39 41 31 31 45 32 33 31 38 39 46 34 35 38 43 35 44 42 38 43 36 34 33 44 41 30 44 39 43 32 46 42 42 31 38 39 34 35 34 35 37 43 38 46 36 43 39 43 45 32 33 45 36 30 36 33 36 46 37 30 45 44 35 35 46 41 41 30 46 30 43 36 43 31 32 43 37 39 42 37 45 43	65FF458D7673B103962E00EB3124B20464827DB078E548E8A294899303A2D4B26244CDE2525A3176A4E8EBA229CBF8215F529302F79215A66E2485619280B9F07D0F5D7F34853DD732803E9230FA52E1368AFF3ADB4D69A11E23189F458C5DB8C643DA0D9C2FBB18945457C8F6C9CE23E60636F70ED55FAA0F0C6C12C79B7EC	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\HPSUPD-Win32Exe.exe	0	32768	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 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 50 45 00 00 64 fd 02 00 4b 63 0c 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 30 00 00 fd 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdKc"0 @ `@@	success or wait	3	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\emoji-body-symbolic.symbolic.png	0	193	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 78 49 44 41 54 38 fd 51 fd 09 fd 30 10 45 fd fd 23 64 0e 7b 47 70 1c 6b 17 71 07 57 50 fd 10 fd 10 2c 6d fd fd 24 10 42 48 fd fd fd fd 73 7d fd fd 41 3c 1d fd fd 39 fd 17 4c 0d fd 46 70 01 45 fd fd 37 fd fd 02 05 fd fd 60 fd 15 fd 0e fd fd 36 07 6e fd fd 13 fd 5d 62 fd 35 01 fd 02 50 fd fd 11 fd 14 72 fd 57 fd fd 23 fd 5b fd fd 55 5f 04 fd fd fd 70 1e 50 fd 3e fd 26 fd 31 fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dxIDAT8 0E#d{GpkqW P,m$BHsA<9LFpE7`6n]b 5PrW#U_pP>&1IENDB`	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\iso_639-3.xml	0	32768	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 6c 61 6e 67 75 61 67 65 73 20 69 6e 20 74 68 65 20 49 53 4f 20 36 33 39 2d 33 0d 0a 73 74 61 6e 64 61 72	<?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 languages in the ISO 639-3standar	success or wait	34	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lgpllibs.dll	0	32551	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 00 00 00 00 78 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 24 00 00 50 45 00 00 64 fd 07 00 3e 0e 2e 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 00 00 46 00 00 00 2a 00 00 00 00 00 00 50 13 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 00 00 00 04 00 00 1f fd 00 00 02 00 60 41 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEd>.b" F*P`A	success or wait	2	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\microphone-disabled-symbolic.svg	0	1401	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 32 31 33 2e 35 33 31 2c 32 32 38 2e 34 36 39 20 2d 31 2e 30 36 31 2c 31 2e 30 36 31 20 31 34 2c 31 34 20 31 2e 30 36 32 2c 2d 31 2e 30 36 32 20 7a 22 20 74 72 61 6e 73 66 6f 72 6d 3d 22 74 72 61 6e 73 6c 61 74 65 28 2d 32 31 32 20 2d 32 32 38 29 22 2f 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 32 32 30 2c 32 32 38 20 63 20 2d 31 2e 36 36 32 2c 30 20 2d 33 2c 31 2e 33 33 38 20 2d 33 2c 33 20 76 20 31 2e 36 34 34 35 33 20 6c	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"> <g fill="#2e3436"> <path d="m 213.531,228.469 -1.061,1.061 14,14 1.062,-1.062 z" transform="translate(-212 -228)"/> <path d="m 220,228 c -1.662,0 -3,1.338 -3,3 v 1.64453 l	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\printer-symbolic.svg	0	213	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 32 20 34 63 2d 2e 35 20 30 2d 31 20 2e 35 2d 31 20 31 76 34 63 30 20 2e 35 2e 35 20 31 20 31 68 31 56 38 68 31 30 76 32 68 31 63 2e 35 20 30 20 31 2d 2e 35 20 31 2d 31 56 35 63 30 2d 2e 35 2d 2e 35 2d 31 2d 31 2d 31 7a 6d 32 2d 33 76 32 68 38 56 31 7a 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 34 20 39 76 35 68 38 56 39 7a 22 2f 3e 3c 2f 67 3e 3c 2f 73 76 67 3e	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z"/><path d="M4 9v5h8V9z"/></g></svg>	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-debug.dll	0	27894	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 30 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 5b fd fd fd 1f 2a 1f 2a 1f 2a 0b fd fd fd 14 2a 0b fd fd fd 1a 2a 0b fd fd fd fd 2a 1f 2a 1e 2a 73 fd fd fd 15 2a 73 fd fd fd 11 2a 73 fd fd fd 02 2a 7b fd fd 1e 2a 4d fd fd fd 1c 2a fd fd fd fd 1e 2a 7a fd fd fd 1e 2a 7a fd fd fd 10 2a 1f 6a fd 2a fd fd fd fd 0f fd	MZ@0!L!This program cannot be run in DOS mode.$[sssMzz	success or wait	11	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\recibo.exe	unknown	512	success or wait	400	4060CA	ReadFile
C:\Users\user\Desktop\recibo.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\recibo.exe	unknown	4	success or wait	43	4060CA	ReadFile
C:\Users\user\Desktop\recibo.exe	unknown	4	success or wait	28	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Rekorddage.Res7	unknown	2	success or wait	1023	40275E	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\centrumpartiers	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\centrumpartiers\sindstilstand	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SENGEKANTERNE	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SENGEKANTERNE\stubben	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\dado	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\metaled	success or wait	1	406407	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\metaled\Filformatets	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\centrumpartiers\sindstilstand	Tiebold	binary	FF 91 0B 25	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SENGEKANTERNE\stubben	Roundabout87	unicode	Layia242	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\dado	Foresprgselens98	dword	1	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\metaled\Filformatets	Expand String Value	expand unicode	%WINDIR%\Stepsons66.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly