ID: 544197
Sample Name:
SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll
Cookbook: default.jbs
Time: 20:36:43
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

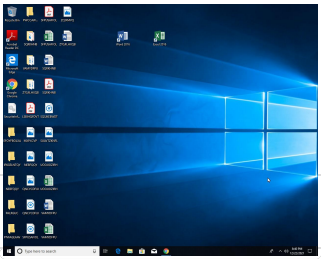
Windows Analysis Report SecuriteInfo.com.BehavesLik…

Overview

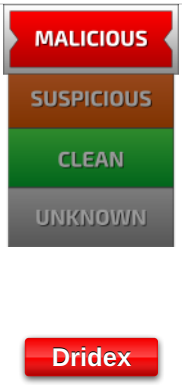
General Information

Sample Name:	SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll
Analysis ID:	544197
MD5:	5c9f3e803604beb.
SHA1:	3e775ec10dce6c…
SHA256:	a7efe0ee7f8d77a..
Tags:	dll Dridex
Infos:	

Most interesting Screenshot:



Detection

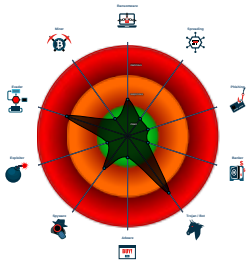


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Call by …
- Tries to delay execution (extensive O…
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Found a high number of Window / Us…
- AV process strings found (often use…
- Sample file is different than original …
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5212 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6932 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 484 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6720 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 484 -s 684 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "144.91.122.102:443",
    "85.10.248.28:593",
    "185.4.135.27:5228",
    "80.211.3.13:8116"
  ],
  "RC4 keys": [
    "3IC8sFlUX9XZuoBQY9u5LhcZnHsV7E5r",
    "hnk63OiMfIbUqQnY7gkPwplwC0Ue5ZkZBYMCTYTjntqX7zsy9OvtNUlthJZXRtFF6P52Zbz6R5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.668687209.000000006E701000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.1058145995.000000006E701000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.666259789.000000006E701000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.700452681.000000006E701000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.rundll32.exe.6e700000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6e700000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6e700000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.6e700000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

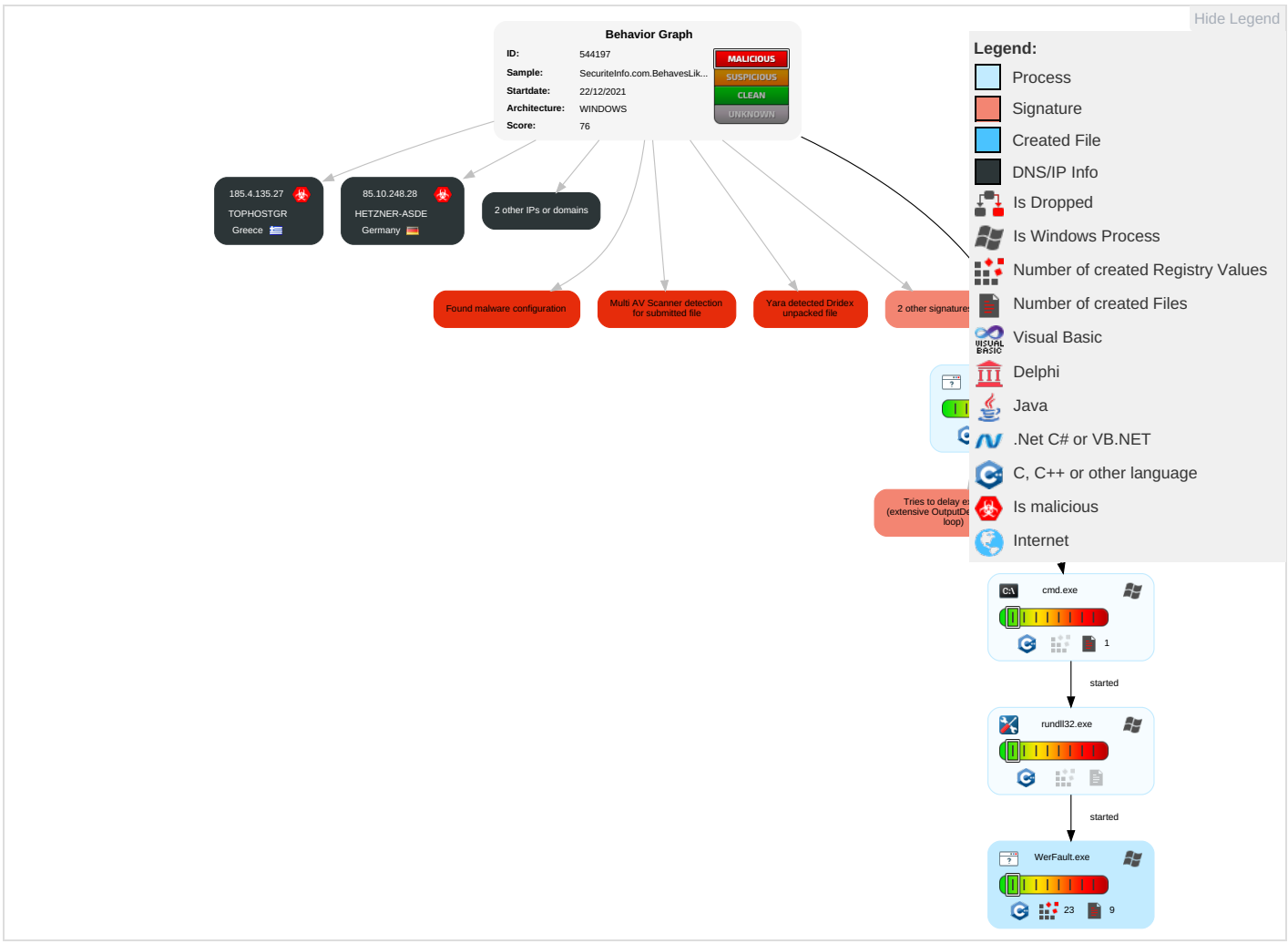
Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll	18%	Virustotal		Browse
SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll	26%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.rundll32.exe.ba0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6e700000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.2.rundll32.exe.6e700000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.a40000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6e700000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.6e700000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.2.rundll32.exe.ba0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.ba0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.n4pkg6fy8o.gaDVarFileInfo$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.4.135.27	unknown	Greece		199246	TOPHOSTGR	true
85.10.248.28	unknown	Germany		24940	HETZNER-ASDE	true
80.211.3.13	unknown	Italy		31034	ARUBA-ASNIT	true
144.91.122.102	unknown	Germany		51167	CONTABODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	544197
Start date:	22.12.2021
Start time:	20:36:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@6/6@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.8% (good quality ratio 51.4%) • Quality average: 78.8% • Quality standard deviation: 27.7%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_ec956fef9dabf4719f57ed463929b5a2167ca669_82810a17_1b64c96e\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9235792918556596
Encrypted:	false
SSDEEP:	192:Hgyix0oX7/HBUZMX4jed+R/u7sCS274ltWc:Di/X7/BUZMX4jes/u7sCX4ltWc
MD5:	FC092A755927F7FB196190805F465715
SHA1:	2AC3F6E6673E7670FCE801ED0820EE32D3120276
SHA-256:	1A40899BE4A975B17148FF0B9CE22C8C13389663499173A7AD7A9CAC46EF243C
SHA-512:	0966E17E17AB0D8C33538032570006B7B00880F61AF3E54BB7DBE89A8576C0B6EED289D9A616F7DE76C9C1B6F07A66C52A89B2CDA8DF71E2305F00D9BFE4720F
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_ec956fef9dabf4719f57ed463929b5a2167ca669_82810a17_1b64c96e\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.4.6.7.5.4.6.3.8.8.2.7.7.2.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.4.6.7.5.4.7.0.0.3.9.0.0.0.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.1.e.4.8.b.7.a.-.3.d.4.3.-.4.3.d.2.-.8.6.4.3.-.0.6.9.9.1.b.7.5.e.b.0.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.2.6.9.a.a.a.9.-.c.d.9.a.-.4.2.6.1.-.b.8.8.8.-.1.4.9.8.4.c.4.6.e.6.e.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.e.4.-.0.0.0.1.-.0.0.1.b.-.e.0.0.2.-.6.d.6.0.6.b.f.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB57.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Dec 22 19:37:45 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40152
Entropy (8bit):	2.2005856897512164
Encrypted:	false
SSDEEP:	192:ynjI9OK6eQO5Skb/bX9HUTOfFNNPJEXVtTBj9/pyRn:kTc5Lb/bjoX1j9/wR
MD5:	DE794CB3009E8F88013CA58667F948F7
SHA1:	865AE5B19BB10D2EE7CDEFD828817ED2EA76951F
SHA-256:	259DEC3D8B355579D5CF80AE49C6DD3659CDA7EC4040AE1E097112D5FFEEF982
SHA-512:	8C182828BD7B788164EA31F0924EC36FB83F963F0293BFAD18B7F07272C1F32AFC399ABDD637BB621121F4B7CFD34CEE9DE38532B49E264229FAA1BA552979C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....~.a.....d.....l.....*.....T.....8.....T.....@.....l.....X.....U.....B.....GenuineIntelW.....T.....~.a.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB356.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8336
Entropy (8bit):	3.6975014167210993
Encrypted:	false
SSDEEP:	192:RrI7r3GLNidB6/96Y986vgmfTTS6+prI89b+UsfSqm:RrlsNib6V6Ym6vgmfTTSz+Hfm
MD5:	F3C6E33D3022626D3C393EC9A2317434
SHA1:	4A9115CA377BB8A9ED6B1E5DA79C2CBD891340F4
SHA-256:	93D78D1669E1FB29AE2876AED3A484615EF1F9D0D3443F149E372964B922D2A6
SHA-512:	7B0A7C6838D483D62B7ADCF7826BB6F8638E3C7AF93F3CF6C8597FF85492B38ECF24AC9AD8ECBFC20C69BB014BA4BC18F9312733EF4B5ECFFE6A33B4A98C2B0
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5B9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4710
Entropy (8bit):	4.498226756879163
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9zLWSC8B38fm8M4JCdswOhFz+q8/9UBgiT4SrSVd:uITfr06SNaJ3aiTDWVd
MD5:	BBA4EA3158A563DE73FBE4511BAC4894
SHA1:	5E62581B07F03D9FE618AC54C4975C13FF9F2AA8
SHA-256:	4C34C446850D96801BE53C1E6AC8B274B3CDFBF80EF4A8A254DB0835512616D7
SHA-512:	20AD63F49D5E574A3BA4070DC58448DF6BBF2EF4D06A5C9207B00EBFB48ED3081BA91967CFDEBFD708A2705A3EE1F149FD74C6C3431953F089E73706B274DB34
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5B9.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1309248" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.23993506854759
Encrypted:	false
SSDEEP:	12288:teR8rJvlXp1Z77yBoa9mBdVSed4+hcq0Wu5SJKcGnLa+OcKM:oR8rJvlXp117yB6ke
MD5:	5FCCAA1F580580ADFBA6D01B21B7760A
SHA1:	F41F9AEE67E8C84AB55DC92F23CD540559C1FF98
SHA-256:	9372D3323C0368D1EFF1CE7DEA255304D280BC31A2B6262670F84505079BEFD5
SHA-512:	9454EF57659476E65F95F73C863813221EE10473AB7631DA1FD038F2DC32F11A58AC479AED13ED9CFB865661318BACF48E3B4B070B3A35644BF4297ED50AA641
Malicious:	false
Reputation:	low
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.Z.ck..... .....n.>..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.4054285395115174
Encrypted:	false
SSDEEP:	384:9Toli5K51Pv4EgnVVeeDze+1NKZtj2T8Gpw81533SY1:BgKdg/eeDzewNYtjTGpw8LSY
MD5:	2D4DC3EEC62F40AD1FD716F5AB51E0FB
SHA1:	11B406A201ADFC26F59007A628BCD3C573FD2CA9
SHA-256:	7F8B4D9FC5F08107BB29EC36163C697A57713D1592BD83ACEDA0E28488FE3AFF
SHA-512:	9E4C3BC14D015FB92A09277058140A7D5D86A8FE49E4239099482869B7159181580690BDF0737F60119E54C6A22DD5A0F65F11D07F576D679266B3192021249B
Malicious:	false
Reputation:	low
Preview:	regfG...G...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.Z.ck..... .....n.>HvLE.N.....G.....:.r..... ..hbin.....p.\..,.....nk,....ck..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....ck..... ....Z.....Root.....lf.....Root....nk ....ck..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.322542196260445
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll
File size:	544768
MD5:	5c9f3e803604beb0fd134699e214db4c
SHA1:	3e775ec10dce6ce1bfc8c7aa299eef7e762c5fcc
SHA256:	a7efe0ee7f8d77a65b1fff3ba0cee76acb43223365dc348fa43ceecf93bcf7f0

General

SHA512:	b9a1d3d646c998e8406698c3e4a25827de905f65cdd940cfaa396aa9d16ef9773fc0f6af29b68b697d7eee54004fdac431a09706877bd97f0a5c409d735f2a13
SSDEEP:	6144:54+RYf/Mv1UvT4vjYf/Glpov3KvfMvLo+jwHk3UryzU3+R7ff4evm35IQku4+pMe:54t2UAogoOwhx7nA4+pMpg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...<...<...<..k....<...=.S.<.=.....<.....<.....<.t.?...<.t.=.4.<.L.9...<.t...0.<..k....<..0..x.<.....<..1....<..k....<

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10004db0
Entrypoint Section:	.rdata
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61C2E245 [Wed Dec 22 08:31:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e980d287af7ef0ccd616c6efb9daaae8

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x6e65	0x7000	False	0.391671316964	data	4.47997370834	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x7424e	0x75000	False	0.316222622863	data	7.44066022726	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7d000	0x6190	0x5000	False	0.24609375	data	5.03782298504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x9e6	0x1000	False	0.09033203125	data	0.789164600932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x85000	0x1138	0x2000	False	0.2421875	data	4.12390144992	IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5212 Parent PID: 5316

General

Start time:	20:37:37
Start date:	22/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll"
Imagebase:	0x1e0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.1058145995.000000006E701000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6932 Parent PID: 5212

General

Start time:	20:37:37
Start date:	22/12/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 484 Parent PID: 6932

General

Start time:	20:37:38
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1
Imagebase:	0xc10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.668687209.000000006E701000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.666259789.000000006E701000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.700452681.000000006E701000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6720 Parent PID: 484

General

Start time:	20:37:41
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 484 -s 684
Imagebase:	0xb60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis