ID: 544197
Sample Name:
SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.21492
Cookbook: default.jbs
Time: 20:27:16
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

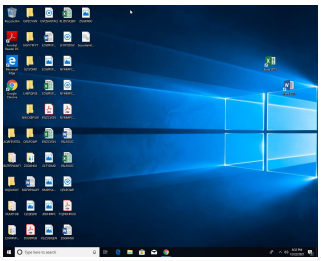
Windows Analysis Report SecuriteInfo.com.BehavesLik…

Overview

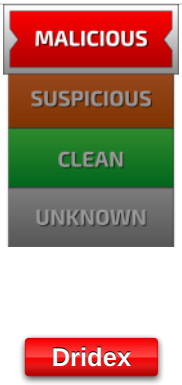
General Information

Sample Name:	SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.21492 (renamed file extension from 21492 to dll)
Analysis ID:	544197
MD5:	5c9f3e803604beb.
SHA1:	3e775ec10dce6c…
SHA256:	a7efe0ee7f8d77a..
Tags:	dll Dridex
Infos:	

Most interesting Screenshot:



Detection

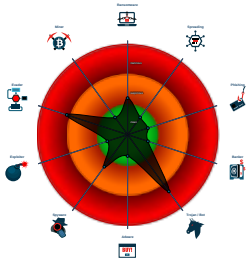


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Checks if the current process is bein…
- Internet Provider seen in connection

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7152 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 3456 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6228 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 3100 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6228 -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
00000002.00000000.252876779.000000006EE71000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.771472500.000000006EE71000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.250806872.000000006EE71000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.268170869.000000006EE71000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.6ee70000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6ee70000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.6ee70000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6ee70000.2.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:

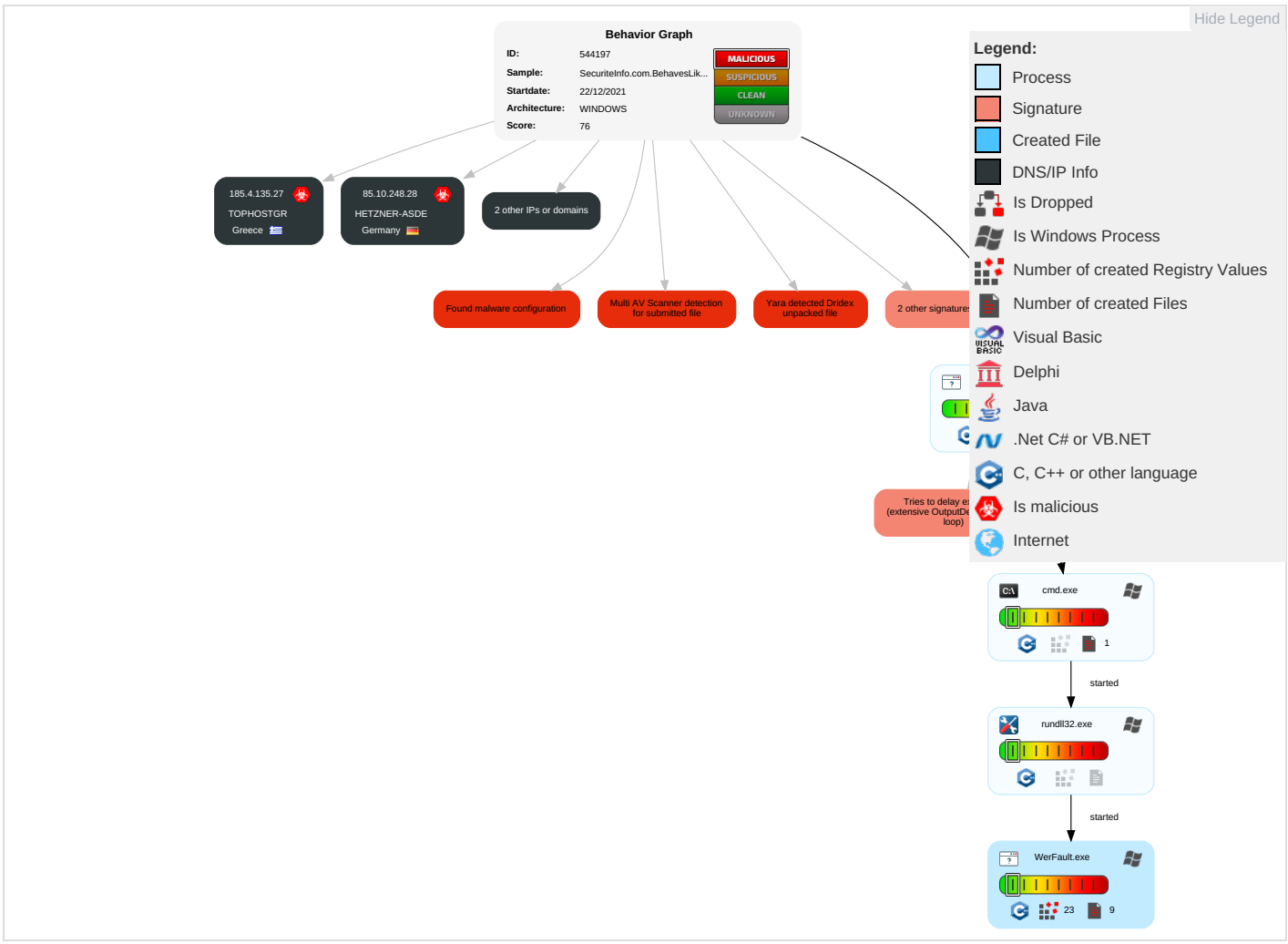
Malware Analysis System Evasion:

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	Query Registry 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	Security Software Discovery 3 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	Virtualization/Sandbox Evasion 1 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	Process 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	Application Window 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	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

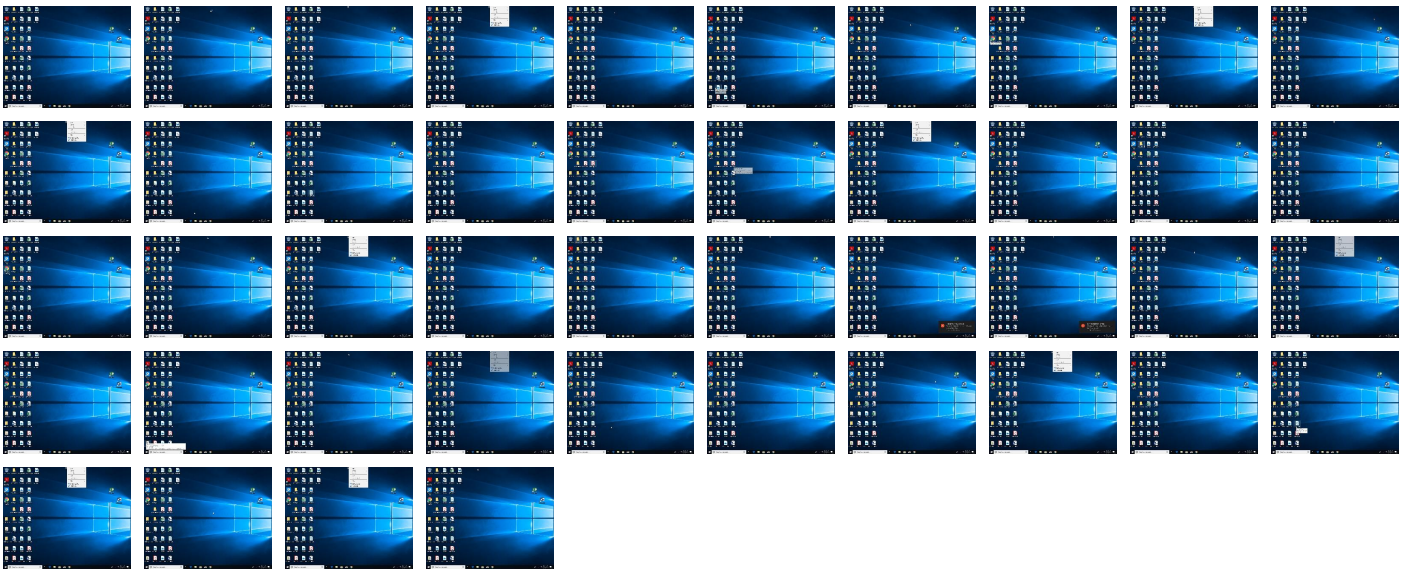
Behavior Graph



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
0.2.loaddll32.exe.6ee70000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.2ec0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.2ec0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.6ee70000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6ee70000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6ee70000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.2.rundll32.exe.2ec0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.980000.0.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:	20:27:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.BehavesLike.Win32.Drixed.hc.23689.21492 (renamed file extension from 21492 to 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
Number of analysed new started processes analysed:	34
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: 100% (good quality ratio 96.8%) • Quality average: 79% • Quality standard deviation: 26.3%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:28:24	API Interceptor	1x Sleep call for process: WerFault.exe modified

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_0c27d8ad\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):	0.9236353516877425
Encrypted:	false
SSDEEP:	192:86iN0oXU/HBUZMX4jed+t/u7sjS274ItWc:1iDXU/BUZMX4jeI/u7sjX4ItWc
MD5:	109A46E84FEB9C6D1F0BFA9157438420
SHA1:	147C9C69E3DD822BEBF204C2CBCA9859DBAFE39F
SHA-256:	626AA47CD69250748CEA8F30CB4459F4205A173C592709B377DED25128702E6D
SHA-512:	4EC23A498AFB690DBAE725EF48E317B61C0035C7D1A4B53C1E2D44B359D27172741E555AEBD2FE805631A5274B1C46B0F31743D524F6DF0BE056B240ED07261
Malicious:	false
Reputation:	low
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.=.1.3.2.8.4.7.0.7.3.0.0.9.6.3.1.0.5.0.....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.=.1.3.2.8.4.7.0.7.3.0.3.5.7.2.4.7.3.3.....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.=.f.0.3.0.b.c.8.4.-.0.8.f.b.-.4.2.7.d.-.9.1.5.2.-.a.3.3.c.4.6.0.d.5.e.1.1.....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.=.0.0.3.c.5.b.7.e.-.9.4.8.1.-.4.b.c.9.-.a.0.1.a.-.8.f.8.8.d.3.4.d.3.f.1.e.....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.=.0.0.0.0.1.8.5.4.-.0.0.0.1.-.0.0.1.6.-.1.d.e.0.-.d.d.8.0.b.5.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\WERC93C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 04:28:21 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45564
Entropy (8bit):	2.1179504783018945
Encrypted:	false
SSDEEP:	192:6JT6UQmL54bwSiCO5SkbP1ZFwvkzq6UllRPcxQCUyn:5OeUd5LbtZFwvcdPPcxSS
MD5:	E4951D32EF752C757D0ED3E56DF0DE15
SHA1:	0E6DB2B40525BAF3713E290EFDDDDC7B5F015AAC
SHA-256:	F7EA9B79AA968A2275BE4F76D5CA580FF8FED0CC671B154FAE2BAF0750F69001
SHA-512:	FFD6FBB1AF90BB86AAA231906C29D9E0050512379BFCD477599333B567CAA818641580CBF7DB61694AC08ED64D59A6C9E463F081DB326482F8EFED8635002E9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....-.....T.....8.....T.....@.....U.....B..... .....GenuineIntelW.....T.....T.....a.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .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\WERCD93.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):	8330
Entropy (8bit):	3.695246004560108
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiT267Og/K6Y/o6RgmfTTSrCprA89bPPsfpFm:RrlsNii6g6YA6RgmfTTS+P0fi
MD5:	74502353301A2DF396EB51802A752D82
SHA1:	10B277D1E671E0F449C18E9A524E164729817F9A
SHA-256:	53EF482395C2B0C5E09B48FE257FB277C8C8AF83D74F3F76E332A6F1712D1302
SHA-512:	18E0AB1907DDD6F39058AB9D09AFE84B5DD2183BC346AEC9D58CCB2E9FB2B1DE5502F6BE1E3DE3F9CDB34D7ADDE784B9DAB24E10F442B29923F60A95CC0A36EB
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.>.6.2.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10E.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):	4.4977367246200854
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9XAb6WSC8Bk8fm8M4JCdswOhFvE4+q8/9UBq04SrSud:uITfAnPSNbJDN40DWud
MD5:	9E5FBD2CE5C45DEDB467EE35C1ACF45C
SHA1:	C1E5B6BF43265CD06424BB3D1A3A29453E548A84
SHA-256:	A555260B2895CA65016B5562ED04B243A9BD49355ADF2620D0BA64575110E00E
SHA-512:	5C6A01C85690C4D3CB9C174DF6C221F5010075C455D8292C3D7E2A4920E59E332602BE521824D7A5E2C55F318390510E06A8833DBC368D32F3F40B93488B9FDE
Malicious:	false
Reputation:	low
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="1309779" />.. <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

C:\Windows\appcompat\Programs\Amcache.hve	
Size (bytes):	1572864
Entropy (8bit):	4.270910747322225
Encrypted:	false
SSDEEP:	12288:zuJso3pPpLf11P3BEqBb/k3LuRr3wbF6WMxHRFr6zaVzWuG4YTDaiZMN:SJso3pPpLf11P3BLs0XN
MD5:	7A268EF630547AA1B159C7CC0B6EB71E
SHA1:	0E2842F1264B311A978B8A236774CABA66FAA1E2
SHA-256:	23887AC36D140AACB7D6B8751B18D02AEA8B51DEBCD13EE03577F5B550EBDFA7
SHA-512:	56177DA760A42687AAA9BD558E2CF0808F8E0AA90B7EF5278A3FB506A340BE9DF6F988C9989B93BEDBB548C9A5EC94BC96804A32935B4BA24B349BE20D0AAAFB
Malicious:	false
Reputation:	low
Preview:	regfS...S...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.rmtmrm.x..... .....).%..... .....

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):	24576
Entropy (8bit):	2.947882843975742
Encrypted:	false
SSDEEP:	384:a085qXLnxOf2oAPmxwpxuN5cAR1KmN5cAR13:VKogf2oLxwpYN5RR1JN5RR1
MD5:	A4C208D26EDAEC04D51D22CAB938E1E9
SHA1:	33259A7C6D995D83F7100CFDB126ECF9104CB91D
SHA-256:	6B11D99BD102138A6BCEA4003310FD8F088868147BE1EBECF3DF396974990C41
SHA-512:	AD76F8044538C2A0ADB0BC928CA98040CBD2287267A13B51DF337FEEF442718E41A4E90F3D7BC2AF758EA51FC6493CA3E669BA00D9704BA8C6992C25BC12DF6
Malicious:	false
Reputation:	low
Preview:	regfR...R...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.rmtmrm.x..... .....).%HvLE.>.....R.....L0...8W.....v.....hbin.....p.\..,.....nk,.=.....@..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .=..... .....P..... .....Z.....Root.....lf.....Root....nk .=.....}..... .....*.....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
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: 7152 Parent PID: 5936

General

Start time:	20:28:14
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:	0x10000
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: 00000000.00000002.771472500.000000006EE71000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3456 Parent PID: 7152

General

Start time:	20:28:15
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:	0x150000
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: 6228 Parent PID: 3456

General

Start time:	20:28:15
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:	0x9d0000
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: 00000002.00000000.252876779.000000006EE71000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.250806872.000000006EE71000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.268170869.000000006EE71000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 3100 Parent PID: 6228

General

Start time:	20:28:19
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6228 -s 684
Imagebase:	0x9c0000
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