ID: 544194
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware1.11362.dll
Cookbook: default.jbs
Time: 20:34:01
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

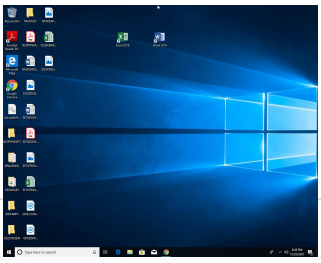
Windows Analysis Report SecuriteInfo.com.W32.AIDete…

Overview

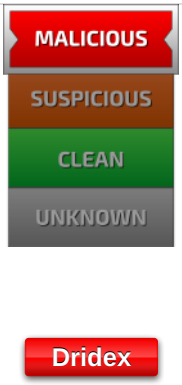
General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware1.11362.dll
Analysis ID:	544194
MD5:	43d4b9318439f69.
SHA1:	06581c15c15cf83..
SHA256:	b06b7b05e576d1..
Tags:	dll Dridex
Infos:	

Most interesting Screenshot:



Detection

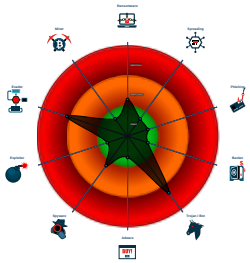


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6752 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 4756 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6324 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6712 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 696 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

Source	Rule	Description	Author	Strings
00000001.00000002.693021141.000000006ECF1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.334490741.000000006ECF1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.301040628.000000006ECF1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.303124420.000000006ECF1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.6ecf0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6ecf0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6ecf0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6ecf0000.2.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:

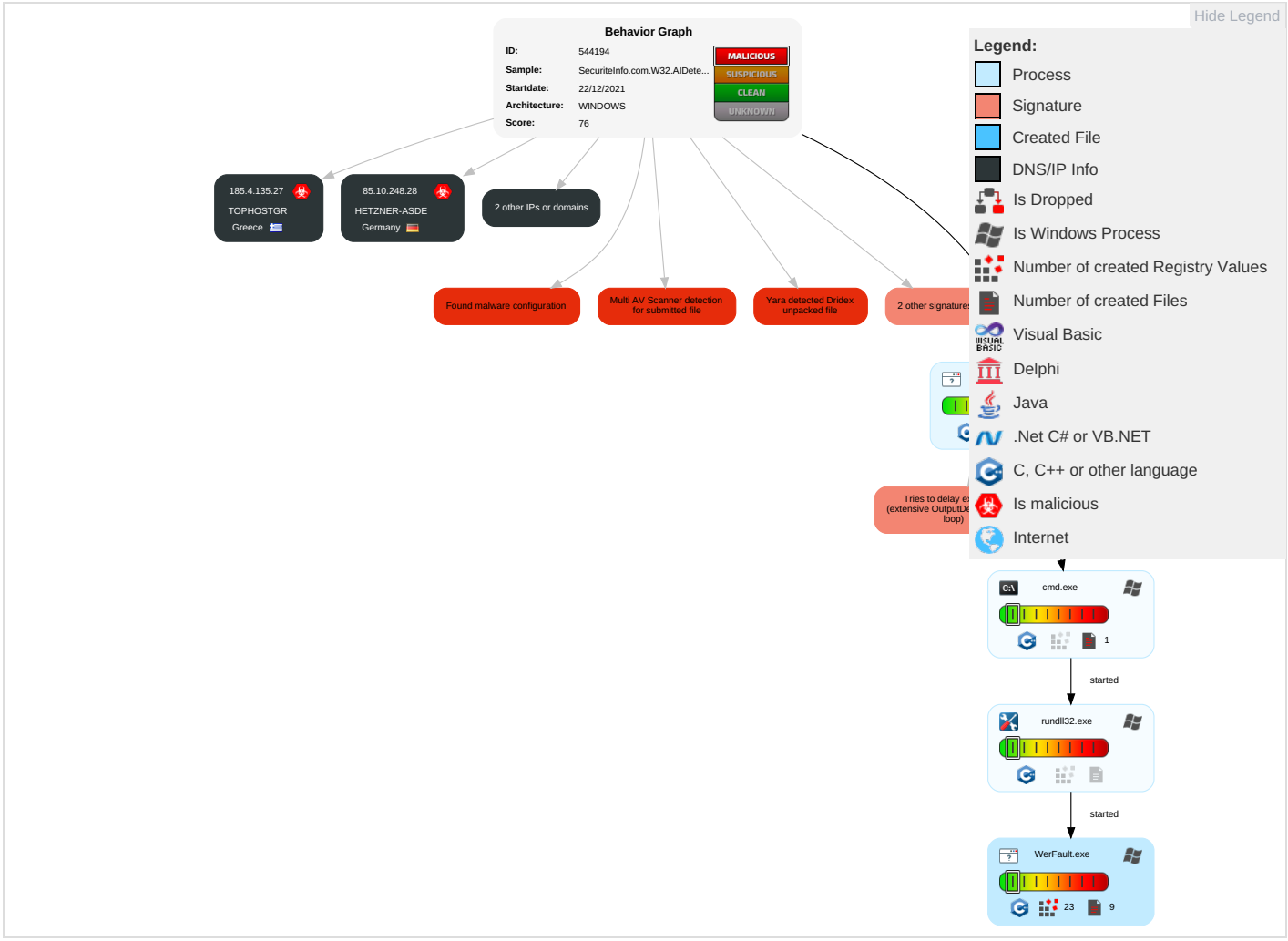
Malware Analysis System Evasion:

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	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 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	Data from Removable Media	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 Poi
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

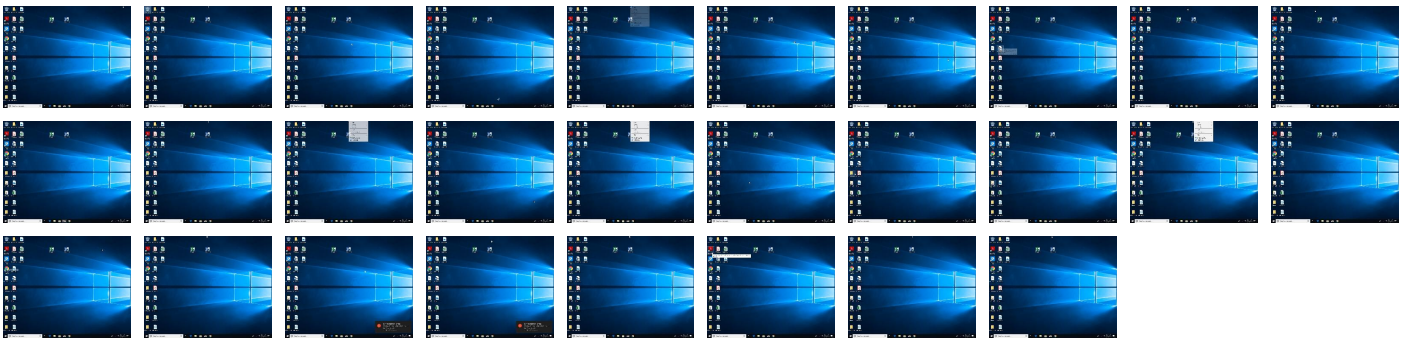
Behavior Graph



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.W32.AIDetect.malware1.11362.dll	24%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware1.11362.dll	26%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.6ecf0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.6ecf0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.6ecf0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.2.rundll32.exe.7d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.d90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6ecf0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.7d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.7d0000.0.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:	544194
Start date:	22.12.2021
Start time:	20:34:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware1.11362.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:	23
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: 78.6% • 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_f87e517ca7ba4e3ba229cb2ffa35583e25899a_82810a17_1ad75c0f\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):	0.9222363616068773
Encrypted:	false
SSDEEP:	192:4miE0oXSN/HBUZMX4jed+yL/u7sGS274ltWc:ViyXSN/BUZMX4je3L/u7sGX4ltWc
MD5:	CDBEF812024E2E1A36A4FE1846B67068
SHA1:	4665E12F1152E0C07821A73B2E9934274CB58624
SHA-256:	8C4EAC5F11909246248BCD4E4B6FC6B30B856A8A8C72D7445F5F34EB9E0A1BFA
SHA-512:	1A3D7F9ECAB3DE733B0DC929106FF20D226785AB28403BDA1DA4BCB23AF65187E0366C12E87BE865E8A63988E29782A3CB8B2432C9A57678E35162FD324E4B0
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.=.1.3.2.8.4.7.0.7.7.0.7.4.9.9.8.5.9.2.....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.=.1.3.2.8.4.7.0.7.7.1.2.0.4.6.7.3.3.7.....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.=.b.3.9.3.8.5.1.c.-.f.4.1.9.-.4.e.f.c.-.9.a.f.f.-.1.4.a.7.5.1.4.b.1.3.7.b.....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.=.5.0.2.e.e.e.3.7.-.e.9.b.4.-.4.2.6.8.-.b.0.9.6.-.f.3.b.a.b.8.8.d.4.0.c.0.....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.b.4.-.0.0.0.1.-.0.0.1.c.-.5.3.f.c.-.b.4.7.2.b.6.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\WER4413.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 04:35:08 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	43756
Entropy (8bit):	2.139472296500077
Encrypted:	false
SSDEEP:	192:JW+KDgVEc6yLjO5SkbmQwB/eKaGyPCAl5JA71mzccYB3AMI33Yq:hS5LbpwB/5aGyPCAzJs1mzccxYq
MD5:	726F7DFB2AE28150549639AC21BA4D43
SHA1:	607E2C2C07BDCF0974819C42937456F5097002BC
SHA-256:	1E3D0693B1E6AF37F2EEEE0C048673E18D3F45F30C7D56EB1632F47FFB0BACC6
SHA-512:	34CC19013C01779619EE975ED24949FAD970EBB6605716B4CF32E78FE64F07008DF7D9573EE32B776D97D86EEE4174B0C22583E9ED926EFBF3C16DF4F18827D
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....|..a.....-.....T.....8.....T.....$.....U.....B..... .....GenuineIntelW.....T.....u..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\WER4AEA.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):	8326
Entropy (8bit):	3.690869333314738
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqd067OgsG6YDo6EgmfT/CSsCprQ89ba5ysfH+m:RrlsNiqe6f6YM6EgmfT/CS5a5xfH
MD5:	2A3D2B8E09AC194B63597EE85C79E92E
SHA1:	EB1E1D40175BE420BD94D136BC7C71C0B79BB6F1
SHA-256:	47579AE72C9A54D68DEC1AAD71A8E9AACBFCA7DA1411EC9BB1FC014B782FD0B3
SHA-512:	F203B26566A7E752AE62A93722CE0A092FFE7B96929190020E994777F6E8289729BCD4664E0A50F5C5E9A39645CA5449CF4B6C0F7760E2E0E3A78B3AE14BCB98
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.>.6.3.2.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D6B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4698
Entropy (8bit):	4.4877009648952555
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9CcWSC8BJCs8fm8M4JCdsDChFeo+q8/QQBR24SrSWd:uITffNVSNnCRJlxoVJDWWd
MD5:	F8135692885414B84D256F717A796903
SHA1:	95F9A7AFBD5B1B7ADDD488656B6A0AFF3F0F33E7
SHA-256:	B6EBCF9CA1362EFA06D5FAC03FA9C05D99D53B057CEDCBF88725B75141687E7E
SHA-512:	AA781381BBBD4224F37EE4887E50F6826327AD4F8BEBCF5E004815BE115A7F884ED27C1A18EAAB696582E95B99C7A20068D8F3C0F1ED4EFD44B809A46CA3C6E
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="1309785" />.. <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):	4.276053824421805
Encrypted:	false
SSDEEP:	12288:BxqtC8mFD7M/S+UdeiL/NA9DDY1tm1juUKzDTkAOCNr36uc5hPkPkZ:vqtC8mFD7M/S+UkO
MD5:	5939F26615D7BB8628B14A9A7084D056
SHA1:	E3C638401E93AFF4E14191BCBD69A1FD9B0F625B
SHA-256:	94FA5148970DEFA008003BEE5925F7B4DD9916FDB2C6AB3712F7EDE7246408BD
SHA-512:	B20C466041932758986CA552FE1BAAE62CC223C545C882D9CCD91C75ED8281E0F85D0CCE2F3F0422474CD2AC50E4E75C3C95733029D967E1F4665B3011293BF
Malicious:	false
Reputation:	low
Preview:	regfZ...Z...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.rmtmJ.Ru..... ....V(..... .....

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):	4.032359811129686
Encrypted:	false
SSDEEP:	384:Bq5oQ5Rftx1vPJ4XMsFcnE7kgPBqX/Seq5QMVyi6+/Xl4Lk4uZd1DoXzn2Xvwvm:MomRftx1HJ4XJFcE7hBqXKeq5QMVyi6t
MD5:	8AD05CBB05EA2F708F36F397C03509F1
SHA1:	99319A049B54A63262E51B329E392C69DCC0388F
SHA-256:	A5938E9E435CD75D12A55DCDD66FFB6B1D020622762DCEDF0E95A56BEC957E3A
SHA-512:	CFC76D0840B0F66D95957FF1E99949E01D00DEB2EC2BFF967A76F479802030715DA8918355C7FA1823DCA3B18E3AC07D4D6B0A6FB22F7599CFDF0059E9BA5A0 4
Malicious:	false
Reputation:	low
Preview:	regfY...Y...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.rmtmJ.Ru..... ....V(HvLE.^.....Y.....i.r.}....!iM+.`.....0..... ..hbin.....p.\..,.....nk,...Tu..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...Tu..... ....Z.....Root.....lf.....Root....nk ...Tu.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.322437972026823
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.W32.AIDetect.malware1.11362.dll
File size:	544768
MD5:	43d4b9318439f6926dfbcf46a5291621
SHA1:	06581c15c15cf8345bef1cea5b32fbc7d7d71e03
SHA256:	b06b7b05e576d19367c383aabd9c8fed8cd5e7955e2f149 3d326b9b5306c7439
SHA512:	1cd1903a05030e394056ec5c23f4d08d8959ef349ffeacc bc61feb620724e4555c7e5fae7b40bedcae308681af79b9 cb60f4b5d181d4e24d5ec2f547349cbe04
SSDEEP:	6144:+D+RYf/Mv1UvT4vjYf/Glpov3KvfMvLo+jwHk3UryzU3+R7ff4evm35IQku4+pMl:+Dt2UAogoOwhx7nA4+pMAg
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	0x6b2e	0x7000	False	0.391496930804	data	4.47906652106	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x747db	0x75000	False	0.316222622863	data	7.44059897898	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	0x2f0	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: 6752 Parent PID: 4664

General

Start time:	20:35:00
Start date:	22/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll"
Imagebase:	0x2b0000
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: 00000001.00000002.693021141.000000006ECF1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4756 Parent PID: 6752

General

Start time:	20:35:00
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.W32.AIDetect.malware1.11362.dll",#1
Imagebase:	0xd80000
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: 6324 Parent PID: 4756

General

Start time:	20:35:01
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll",#1
Imagebase:	0x890000
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: 00000004.00000002.334490741.000000006ECF1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.301040628.000000006ECF1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.303124420.000000006ECF1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6712 Parent PID: 6324

General

Start time:	20:35:04
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 696
Imagebase:	0xe80000
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