ID: 544194
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware1.11362.23809
Cookbook: default.jbs
Time: 20:24:44
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

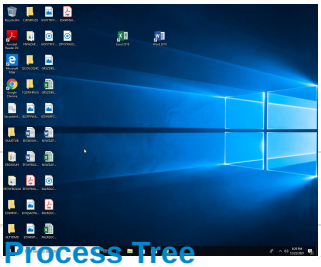
Windows Analysis Report SecuriteInfo.com.W32.AIDete…

Overview

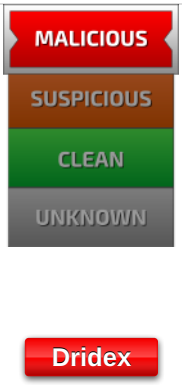
General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware1.11362.23809 (renamed file extension from 23809 to dll)
Analysis ID:	544194
MD5:	43d4b9318439f69.
SHA1:	06581c15c15cf83..
SHA256:	b06b7b05e576d1..
Tags:	dll Dridex
Infos:	

Most interesting Screenshot:



Detection

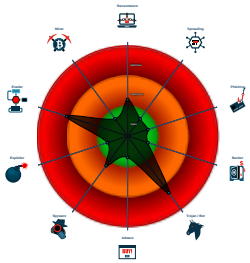


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 7096 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7160 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3092 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.11362.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6364 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3092 -s 672 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
00000004.00000000.302508511.000000006EB51000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.821591397.000000006EB51000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.326161614.000000006EB51000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.303906353.000000006EB51000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.6eb50000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6eb50000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.6eb50000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6eb50000.2.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:

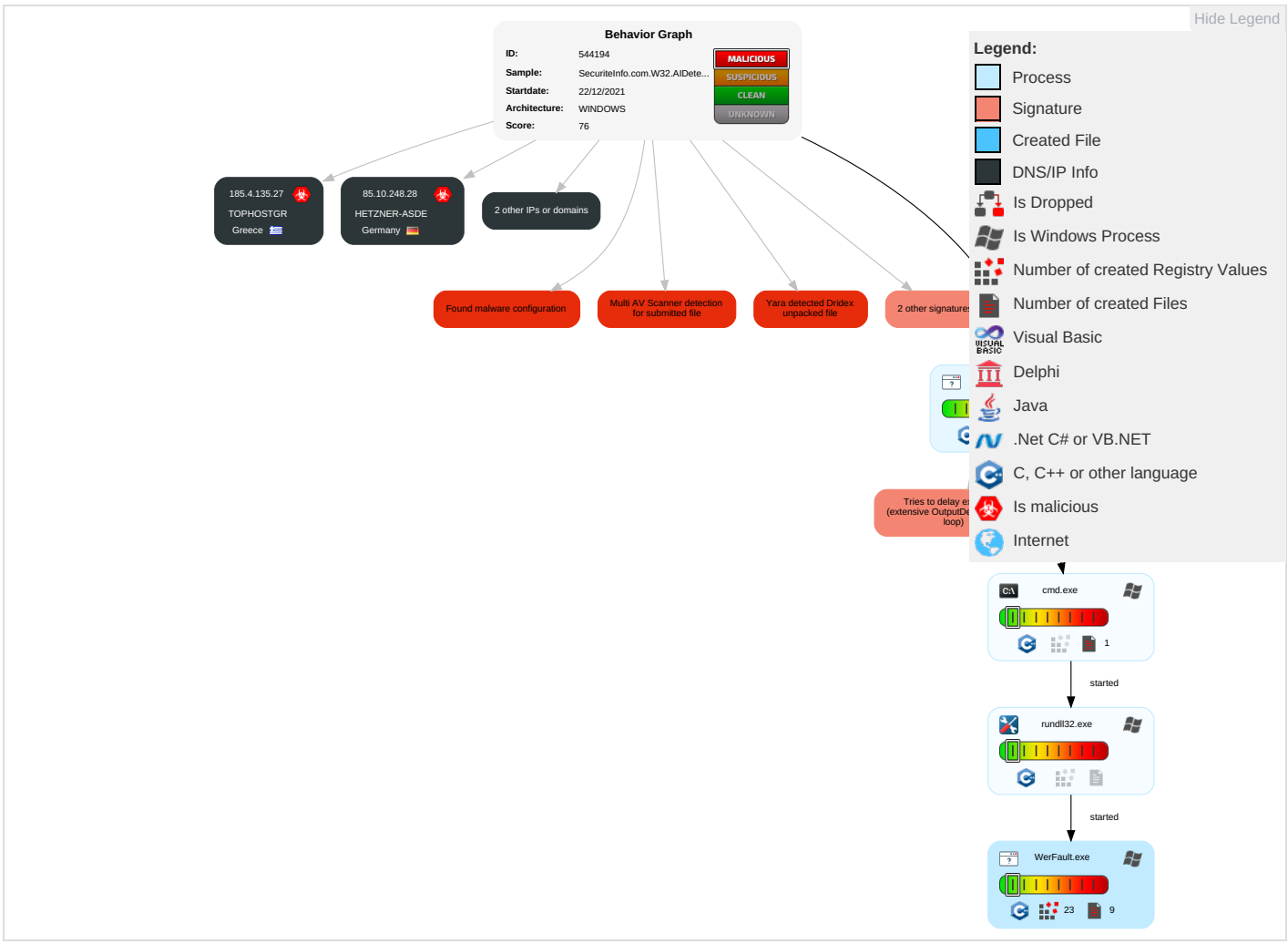
Malware Analysis System Evasion:

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

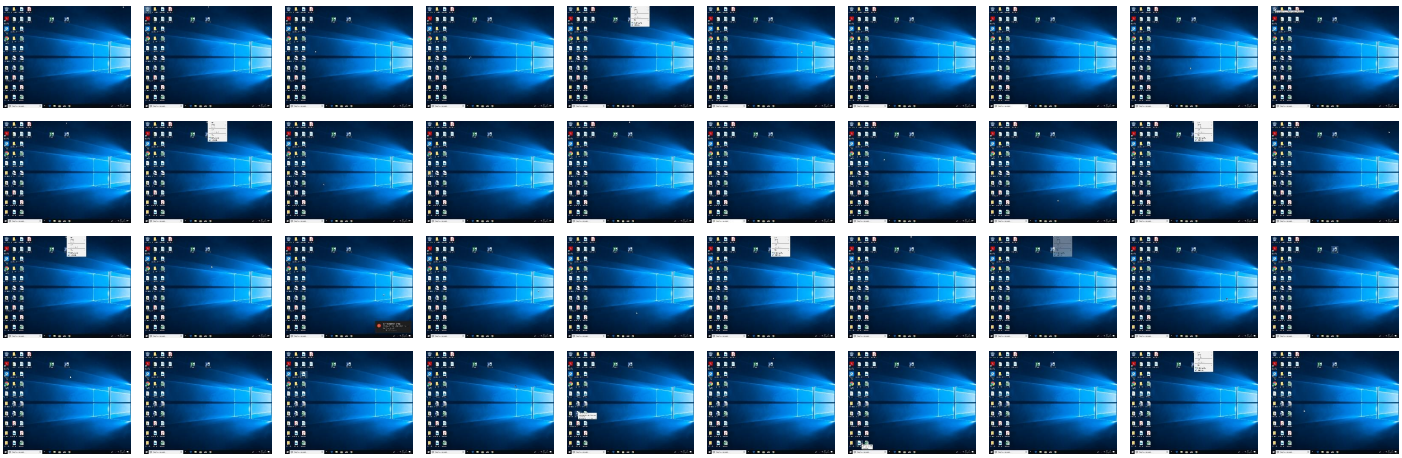
Behavior Graph



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.6eb50000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.2800000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.6eb50000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.6eb50000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.31e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.6eb50000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.31e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.31e0000.0.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:	20:24:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware1.11362.23809 (renamed file extension from 23809 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:	24
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: 52.3% (good quality ratio 50.7%) • Quality average: 79.5% • Quality standard deviation: 26.1%
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
20:25:56	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_f87e517ca7ba4e3ba229cb2ffa35583e25899a_82810a17_198b3aa3\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):	0.9219702689378206
Encrypted:	false
SSDEEP:	192:cuiz0oXCN/HBUZMX4jed+yL/u7sSS274ItWc:JitXCN/BUZMX4je3L/u7sSX4ItWc
MD5:	79CC54E8C141F5109F39A5F806AD2CEE
SHA1:	7845FDA8469C72F836649557F0F3A92455DE4236
SHA-256:	13C1D974F5EA0C00E96E1FBD52E5BC7A65776D8F0CFA0B5D14BC4848BB583022
SHA-512:	522D2795BDBE718752972297A7ADDD2BB4F31F3CF3E882BB4C79A100FC3E2125E6B9AE803AFFDF206A447E5F34DB1E74C2B3A28749C44F31F156BE951B4B7831
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f87e517ca7ba4e3ba229cb2ffa35583e25899a_82810a17_198b3aa3\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.=.1.3.2.8.4.7.0.7.1.5.0.7.5.0.7.4.0.5.....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.=.1.3.2.8.4.7.0.7.1.5.5.3.1.3.1.9.8.8.....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.=.a.2.c.d.b.4.9.7.-.9.8.f.2.-.4.c.f.d.-.9.7.f.d.-.f.0.a.d.c.e.a.3.2.a.0.e.....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.=.7.9.d.1.a.a.4.1.-.f.4.6.5.-.4.f.6.1.-.b.9.7.9.-.8.e.c.8.d.7.6.6.f.c.e.1.....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.c.1.4.-.0.0.0.1.-.0.0.1.c.-.f.5.1.7.-.5.8.2.7.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\WER2362.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 04:25:52 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	43000
Entropy (8bit):	2.2065773807704554
Encrypted:	false
SSDEEP:	192:xhBdSEcTQcJzZO5SkbmQcpxOlB/84P+ziet1gDI:x4JJY5LbpcpAlVUzieTgs
MD5:	85FB74CB0DB2B67D9BA3E9092034D4E9
SHA1:	7A9D86DE372B19FB2C89AE43D591BEA4B8074DF0
SHA-256:	559F0DFB85C8738298F6C4149ADDEB8F36F408564C06248EC38CEEBF297F537C
SHA-512:	68E63C068466EF527228F5DB0F9DF5099C07DF7B69207EFEC68FB67B7004E2A19FE8F9FC29B2E8EDD13A5D669AC89AB19C2BC577A268C82C4E8EDB16912B82 D
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....P..a.....-.....T.....8.....T.....0.....U.....B..... .....GenuineIntelW.....T.....I..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\WER2A0A.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):	3.6898439981167592
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi1e67OgksK6Yjx6SgmfT/CShCprY89bVOsf0pnm:RrlsNiM6A6Y16SgmfT/CScVNf9
MD5:	C6B41AF3498EF6E2E60EF50528E8154F
SHA1:	77F07D74EA2EF214CEB45DFD62AABA8AAFB00D23
SHA-256:	4E4E996FBD457F6077A79346F782B1CA500785D6C012E626F241C129F6BDF143
SHA-512:	D855A486DDC568D10689E92F0CC0773798E7D13307C4E62366B8EDE252761D07A995B17AF555B49F9841548D46F2E88E553D9C5B8A7F9EA2CC88D512FF810AE
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.>.3.0.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2C9B.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):	4.48880346018983
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWl9J/pWSC8Bw8fm8M4JCdsDChFV1y+q8/QQBY04SrSy6d:uITfliYSN3JlCEVr0DWy6d
MD5:	6BAC94B64344C795C1CD7AFDBABDDB2E
SHA1:	3A3D8B94C83ACE820EB1AFC75D0BE28F3FD9329A
SHA-256:	4F470C9CE0691D6F479DD3A6CF46C8FB1DEEC18D33609C85E254F6DDE49A8406
SHA-512:	152FB41F4BE4C0D13FE29BB01A9E90D8302C8EC399D273D1E18FF179A25808FB7A69F8DDE0A7CA3D89D62ED52420FC5F78C2FA46DC1F36222ABDAFDFABDFC 7E2
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2C9B.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="1309776" />.. <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):	4.27863854650369
Encrypted:	false
SSDEEP:	12288:U/fGlzNTU8JqhZ65qncwOzu5W4r1cpmaCeiZLmIQrp1H2G8RwdxsLT:gfGlzNTU8JqhZ6kn
MD5:	21D7305D19FE5B8CD51D2D0684510032
SHA1:	82253896E8F485117A50B9D05180A99382EE97FF
SHA-256:	E699C3B4FE6DC32FADBDB3483270E0511577D10A928735A1DBD6FD09029B99DD
SHA-512:	FDFE1AD1A59C5D9CD62C0C8E521B64CCB18F42B92218CD10BA9FE3542C18748CED5F692449EBAE7FC7EDFAF550D17706E7746A1584E9D3BA9A958CFB9DCA0C78
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.rmtm.,.)..... ....#h.t..... .....

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):	4.036168790025919
Encrypted:	false
SSDEEP:	384:1BAr5Rftx1wPJ4XjsFcnE7kPPBqXASeq5QMVyi6+/5l4Lk48Zd1DoXznqXvwvc:jAVRftx1GJ4XAFcE7oBqXTeq5QMVyi61
MD5:	443DE2D59B6BD26A036D75EBADD0082D
SHA1:	4D045F471E26251E784D2B42D3EA11D00C10CD45
SHA-256:	6AC20E3348C3DD0DCC0459290ADF55511CBBD7143A9A42045453386DF7027E3D
SHA-512:	F4F604B8C4475CAD3AB96577FA5FE8E25B830DE0FE72AE89DA85923EDCC365BD365E9CB1FE3FEFFB7581353F350800BDD596270D14ECA2D0FE8C753B93DD0CF
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.rmtm.,.)..... ....%h.tHvLE.^.....Y.....~..S8.[^@B$..`.2.....0..... ..hbin.....p.\..,.....nk,.H..)..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .H..)..... ....Z.....Root.....lf.....Root....nk .H..).....}..... .....*.....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

General

SHA256:	b06b7b05e576d19367c383aabd9c8fed8cd5e7955e2f149 3d326b9b5306c7439
SHA512:	1cd1903a05030e394056ec5c23f4d08d8959ef349ffeacc bc61feb620724e4555c7e5fae7b40bedcae308681af79b9 cb60f4b5d181d4e24d5ec2f547349cbe04
SSDEEP:	6144:+D+RYf/Mv1UvT4vjYf/Glpov3KvfMvLo+jwHk3Ury zU3+R7ff4evm35IQku4+pMl:+Dt2UAogoOwhx7nA4+p MAg
File Content Preview:	MZ.....@.....!..L.!Th is 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: 7096 Parent PID: 3100

General

Start time:	20:25:44
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:	0x270000
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: 00000001.00000002.821591397.000000006EB51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7160 Parent PID: 7096

General

Start time:	20:25:44

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: 3092 Parent PID: 7160

General

Start time:	20:25:45
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:	0x870000
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: 00000004.00000000.302508511.000000006EB51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.326161614.000000006EB51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.303906353.000000006EB51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6364 Parent PID: 3092

General

Start time:	20:25:48
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3092 -s 672
Imagebase:	0x13e0000
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