JoeSandbox Cloud BASIC

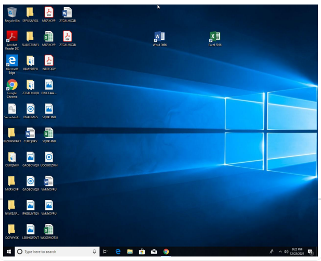
ID: 544184
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware1.23460.dll
Cookbook: default.jbs
Time: 20:18:38
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

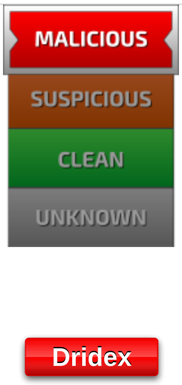
Windows Analysis Report SecuriteInfo.com.W32.AIDete…

Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware1.23460.dll
Analysis ID:	544184
MD5:	d633b0989e97dc..
SHA1:	6e5a7f0493fea40..
SHA256:	03ba158e40b1f9c.
Tags:	dll Dridex
Infos:	
Most interesting Screenshot:	

Detection

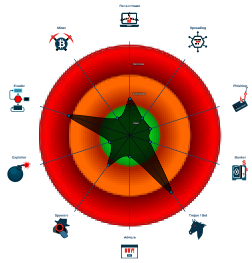


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6168 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1228 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4232 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4696 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4232 -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

Source	Rule	Description	Author	Strings
00000004.00000000.351015506.000000006F501000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.395029698.000000006F501000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.738911371.000000006F501000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.352673706.000000006F501000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.rundll32.exe.6f500000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6f500000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.6f500000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6f500000.5.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:

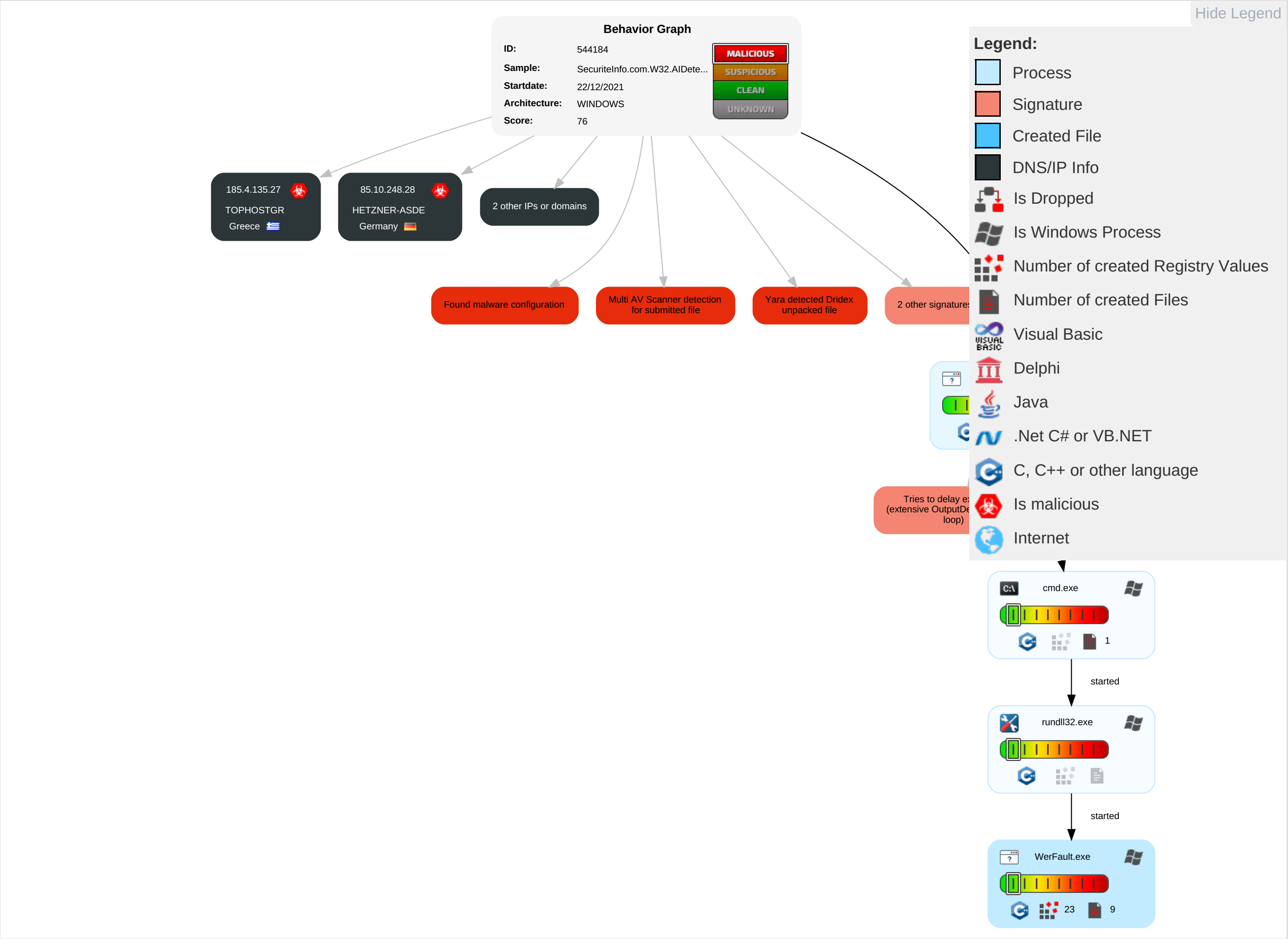
Malware Analysis System Evasion:

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	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
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	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	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 Communic
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-I 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 Static

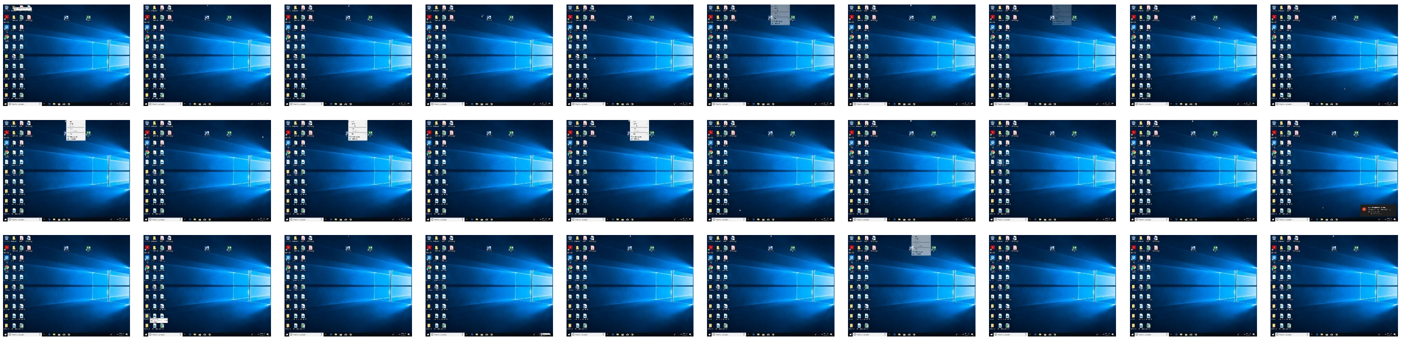
Behavior Graph

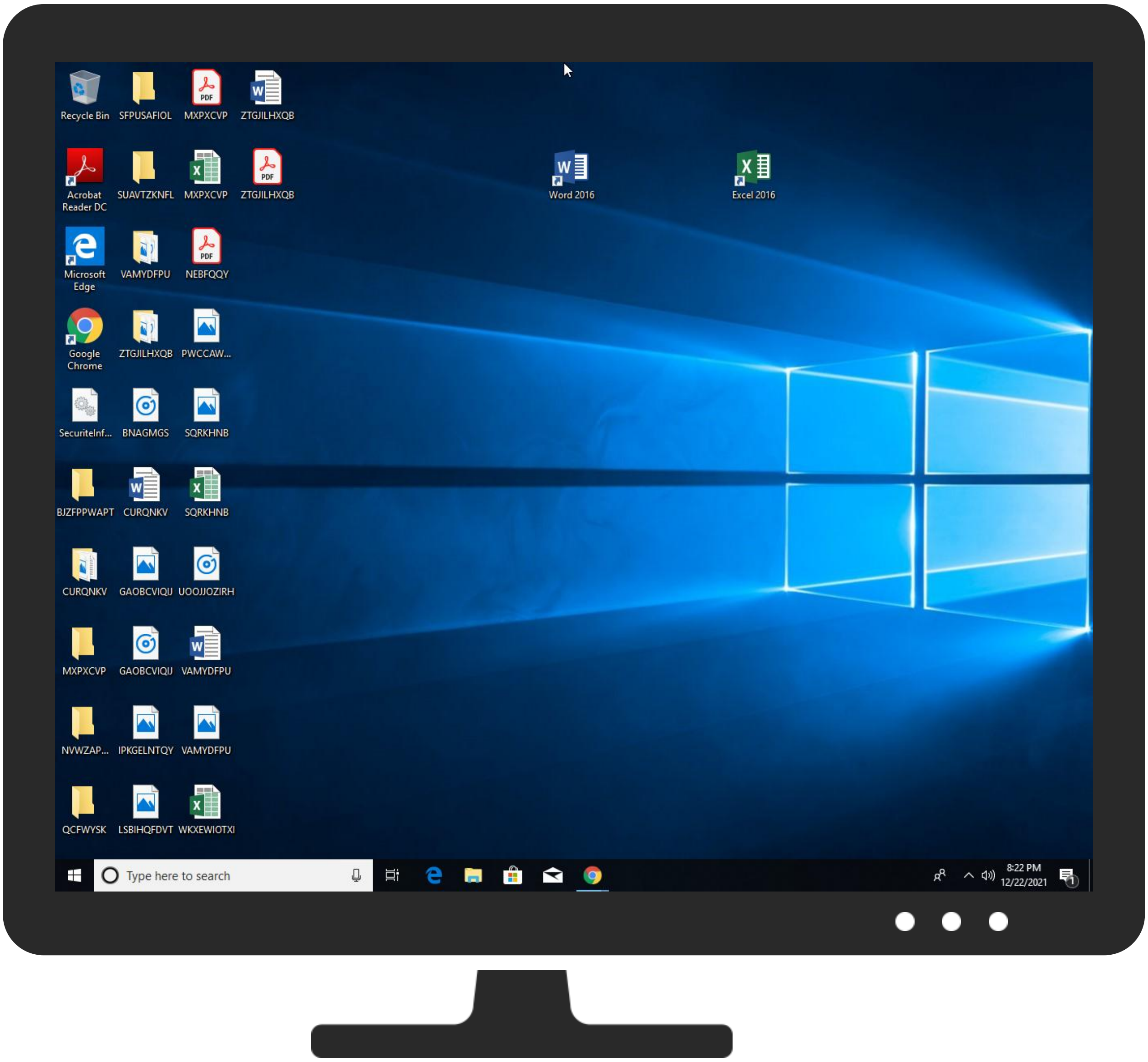


Screenshots

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.malware1.23460.dll	30%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.2a90000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.2a90000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6f500000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.2.rundll32.exe.6f500000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.1580000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.6f500000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.2a90000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.6f500000.5.unpack	100%	Avira	HEUR/AGEN.1144420		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:	544184
Start date:	22.12.2021
Start time:	20:18:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware1.23460.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:	25
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: 96.2% (good quality ratio 93.8%) • Quality average: 79.5% • Quality standard deviation: 25.7%
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_435bf9987f6a7ee95ec1aabecf98fbf5b0b7b2_82810a17_13c89011\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):	0.922046286040136
Encrypted:	false
SSDEEP:	192:kuif0oXD5/HBUZMX4jed+uf/u7sQS274ItWc:xihXD5/BUZMX4jeDf/u7sQX4ItWc
MD5:	528060B5278288935D8E6E6CF8D7AA55
SHA1:	FF1EF30180D490BB6A85C15D68F2B1119475EA94
SHA-256:	C4D626A7AF577A1F8EBCD56B59087B49387B53CBD5A04428F9B6D298F1CF35B4
SHA-512:	723AA4D573412B9810A4150B22E4776C1B986D57AC2671135709ED76EABFC1D94E8A1A1E2AA8BAC2FB31A0E6E53A8AEC1D188A1D562290ABC533D1B57076B0 A
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_435bf9987f6a7ee95ec1aabecf98fbf5b0b7b2_82810a17_13c89011\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.=.1.3.2.8.4.7.0.6.7.8.2.5.9.7.9.6.3.2.....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.=.1.3.2.8.4.7.0.6.7.9.5.9.1.0.3.3.3.8.....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.=.c.e.8.d.2.f.6.9.-.4.1.8.2.-.4.e.f.4.-.9.f.9.8.-.c.c.2.4.b.8.2.2.e.b.4.4.....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.=.b.c.1.f.7.1.5.7.-.7.5.1.3.-.4.3.4.d.-.b.2.2.3.-.0.8.1.c.8.5.0.e.7.7.7.3.....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.=.0.0.0.0.1.0.8.8.-.0.0.0.1.-.0.0.1.7.-.e.0.3.e.-.2.4.4.b.b.4.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.!.0.0.0.0.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\WER55D7.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 04:19:44 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45716
Entropy (8bit):	2.1093383506020773
Encrypted:	false
SSDEEP:	192:Jw7nbKPGzO5SkbmQvomqJuK1J2Ba/9dU9nEQ:mg5Lbpgmm19/9diL
MD5:	BDCA39B95DCCA06B3BC45BF211957E91
SHA1:	68BC6890AC691D3D2F409C14E2C4460A546FB14B
SHA-256:	0D370B79901BC4C5146EE15791B426EEA3E2F468C0E1EE5033410DB53F1B7794
SHA-512:	8A43057934049A0DF909028404F23115F4C255CF9D0280FF10537733B2E9183F62C0782EE207659E99F276D6C09DB28D17989C268A28B0CC3785FB0042509154
Malicious:	false
Reputation:	low
Preview:	MDMP....... ....a...-..........T.......8...........T..........@...T..U...........B...... ....GenuineIntelW...........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\WER5D4A.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):	3.693310442719386
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqf67Og9sTk6Y6z6AgmfT/mS/I4CprX89blssfbXm:RrlsNii6L6Y+6AgmfT/mS9l/fC
MD5:	0A7BC57EF58024A7A991B0B14B694B99
SHA1:	85AF48EF4DFA78D86ADAE9794F4BD40C44E48946
SHA-256:	156B0D27C80F18941CFCE06A2F78C31439DA7BC751E27979B14FF557020C94A1
SHA-512:	01265703B4D0FBF63C46786555DFAB0301789E18692CCEEFE0DE45C9DF453059125B4CCEAFC39820BB452C2347EFF85FCBB87264AF354CD6B2081EB92F65D4AD
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.>.4.2.3.2.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6097.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):	4.490534423613956
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9RtWSC8B+8fm8M4JCdsD6hF5+q8/QYB754SrSSd:uITfjqcSNRJlqVU5DWSd
MD5:	671F09B31CC9A830D437045318954C3A
SHA1:	268D9552435BD588930BAA6FE561B848A93039A7
SHA-256:	E1CCEF37FF3FFDA37AE3F4434CEEFC4A4B7DAC35C8243AF7A015A6FDECC65B2E
SHA-512:	3DB8207532713FB5BC8326BAA9024E6004F5564F2BC31B73AC5D1ED148267FA8BA9520E0FD791EEAD8A6BE89B240E389347598D44AE98315C397EBA4138034F3
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6097.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="1309770" />.. <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):	4.219198579898536
Encrypted:	false
SSDEEP:	12288:wnlDQ2UkoV/2qweb5Qnxbrmkk7I9ln/2VugiFlEkamEf2/6zfmBTS0:wlDQ2UkoV/nwebSaYlqu
MD5:	1FDF042991087FEB000304EDE09873FD
SHA1:	86F4A5960772839EB54FACAF2EB0AEE18D2E0C47
SHA-256:	F12745B570720D489952167E0305BE1D9285D956AC9B570F8BF294FA0ABB4EA9
SHA-512:	8E4AA41021B04E494C19EA13CC5D3DCBA5E89F0B104E16D0664DC99E2D6A77CD461D01E6E0B8EBA9A010BD8CB2B3F80A698F15840223D31DA90801744EBAB4 22
Malicious:	false
Reputation:	low
Preview:	regfV...V...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..1N.. ....5... ....

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):	3.5233007303433506
Encrypted:	false
SSDEEP:	384:RsA5NnIrnc8WTVgG1K0XQmnQIRNovOgl8:a2xAc80VgGU0X7nQIIvP
MD5:	D13F80EEE1683F406026292ED83DF361
SHA1:	809EFC26106DAF98C9B149AF9A1BB7EE8BA14BF3
SHA-256:	6C6F3169DB17CA0E2B55FFD7ABEBAB7EF1807181C916243FFD86AA9426E067B7
SHA-512:	9F35A8207DB3AD34A5ED40F7E6428859DEFB42C83A6824EB1381228C3DEC33502A091FE9E203D4562FFE7C07D967811DB4A814B2E995F421A69427FD9CABCDA 4
Malicious:	false
Reputation:	low
Preview:	regfU...U...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..1N.. ....5.HvLE.N......U............w..{..qx@?..Q`_.................`... ..hbin................p.\..,..........nk,.z3BN.................................. ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}......nk .z3BN........ ....Z.......................Root........lf......Root....nk .z3BN.....................}............. ....*...............DeviceCensus.......... ....vk..................WritePermissionsCheck.......p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.322432304733337
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.malware1.23460.dll
File size:	544768
MD5:	d633b0989e97dc05b09b6233fb53cf37
SHA1:	6e5a7f0493fea40bd213209ad06f4dd9069969ed

General

SHA256:	03ba158e40b1f9c80c0430cd9a06f00bcbddd3826a5965fccb4ac5b242b91a2c
SHA512:	28a594e2f150c7f9a970f068072fe92bcc4c08dc28893023675fec9ea60926c36c044f8200ff6b5759c6173a2ab3771fa18545c3fa8b9c5328ff54e615eb705c
SSDEEP:	6144:0k+RYf/Mv1UvT4vjYf/Glpov3KvfMvLo+jwHk3UryzU3+R7ff4evm35IQku4+pMs:0kt2UAogoOwhx7nA4+pMTg
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	0.391671316964	data	4.4813428029	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x7424e	0x75000	False	0.316216362847	data	7.44062865664	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: 6168 Parent PID: 5288

General

Start time:	20:19:35
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.malware1.23460.dll"
Imagebase:	0xad0000
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: 00000001.00000002.738911371.000000006F501000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 1228 Parent PID: 6168

General

Start time:	20:19:35

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.malware1.23460.dll",#1
Imagebase:	0x2a0000
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: 4232 Parent PID: 1228

General

Start time:	20:19:35
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.malware1.23460.dll",#1
Imagebase:	0x200000
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: 00000004.00000000.351015506.000000006F501000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.395029698.000000006F501000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.352673706.000000006F501000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4696 Parent PID: 4232

General

Start time:	20:19:39
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4232 -s 684
Imagebase:	0x3c0000
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

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal