ID: 544257
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.10228.10333
Cookbook: default.jbs
Time: 00:20:13
Date: 23/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.W32.AIDetect.malware2.10228.10333 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Dridex 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
E-Banking Fraud: 5
System Summary: 5
Malware Analysis System Evasion: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 13
Data Directories 13
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: loaddll32.exe PID: 5744 Parent PID: 6028 14
General 14
File Activities 14
Analysis Process: cmd.exe PID: 6164 Parent PID: 5744 14
General 14
File Activities 15
Analysis Process: rundll32.exe PID: 6244 Parent PID: 6164 15
General 15
Analysis Process: WerFault.exe PID: 6376 Parent PID: 6244 15
General 15

File Activities 15
File Created 15
File Deleted 15
File Written 16
Registry Activities 16
Key Created 16
Key Value Created 16
Disassembly 16
Code Analysis 16

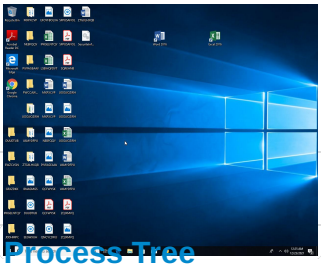
Windows Analysis Report SecuriteInfo.com.W32.AIDete…

Overview

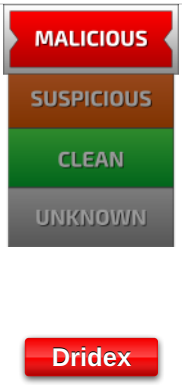
General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.10228.10333 (renamed file extension from 10333 to dll)
Analysis ID:	544257
MD5:	ce624816acb99a..
SHA1:	d971e7c7b27885..
SHA256:	af49104bb708fe0..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

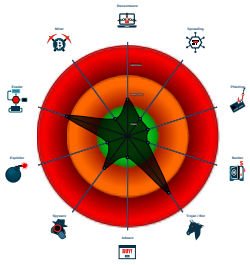


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5744 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6164 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6244 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6376 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6244 -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
00000003.00000000.354406335.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.394624997.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.874430193.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.352980099.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6f4b0000.5.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:

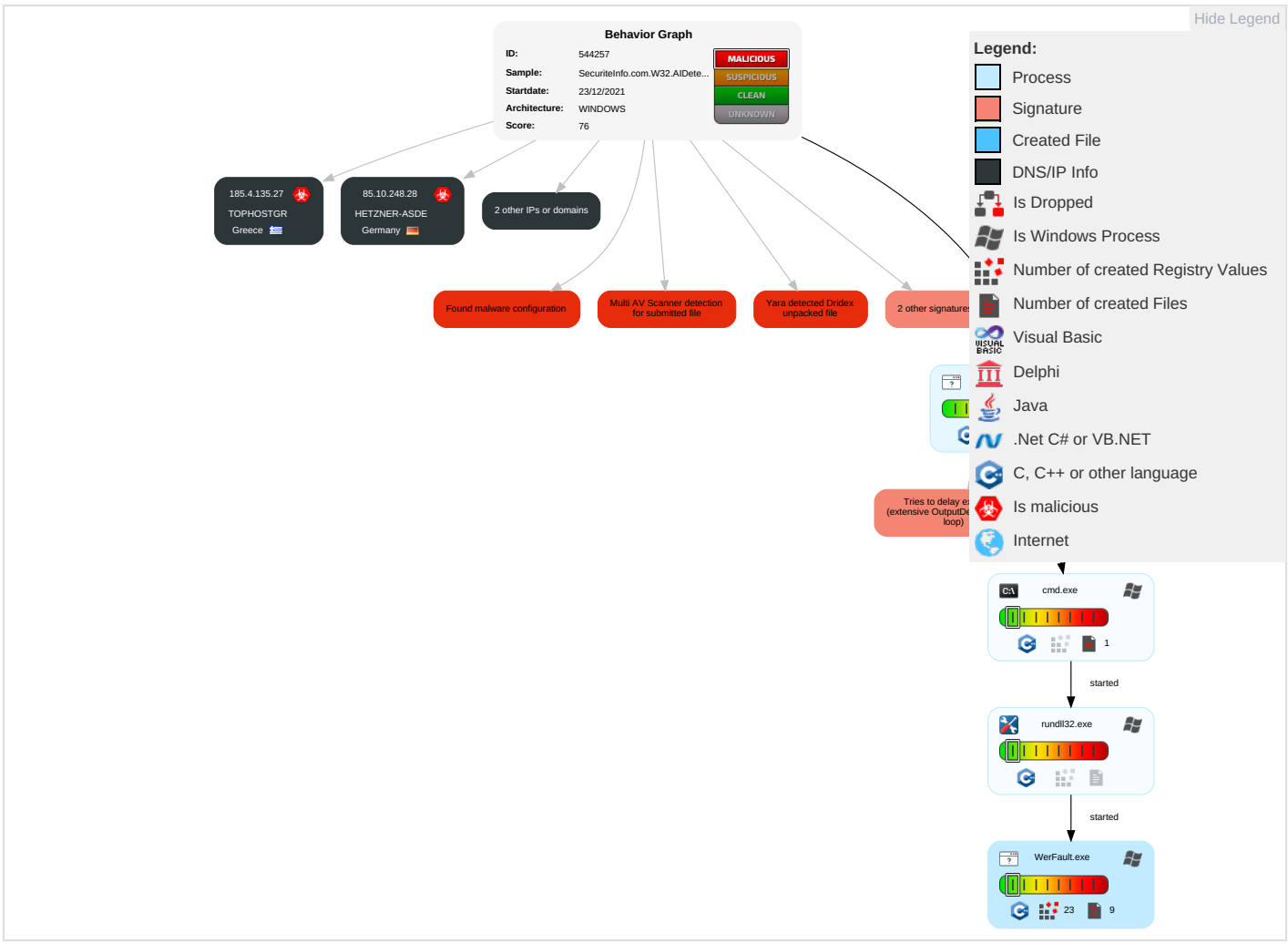
Malware Analysis System Evasion:

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	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

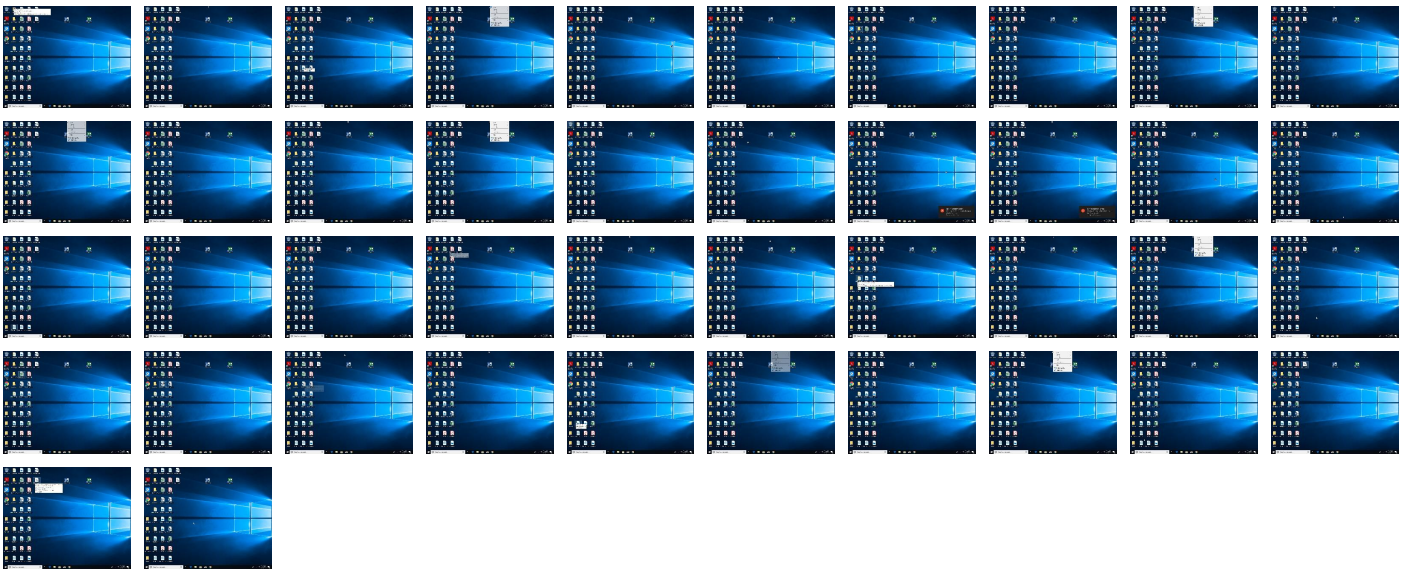
Behavior Graph



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.W32.AIDetect.malware2.10228.dll	22%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.10228.dll	23%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.de0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.6f4b0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.2fe0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.2fe0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.2fe0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.forex-broker.websiteDVarFileInfo$	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:	544257
Start date:	23.12.2021
Start time:	00:20:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.10228.10333 (renamed file extension from 10333 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:	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: 54.6% (good quality ratio 52.4%) • Quality average: 79.9% • Quality standard deviation: 27.1%
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
00:21:32	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_679a7d8d20d369749e733f7a1173ad271ef1b68_82810a17_194eccc1\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):	0.9218486148889585
Encrypted:	false
SSDEEP:	192:sjA2i40oXN4/HBUZMX4jed+uO/u7sBS274ltWc:mi+XN4/BUZMX4jeDO/u7sBX4ltWc
MD5:	FE1105B92DEC1508FCF74B76E5A11B5B
SHA1:	07F676965B966441880356072C53A652B30CDC14
SHA-256:	8C1DBF9DBBFE60E6836F2762FD0D784CD6BEDEFF3E2476374E070EDA010E007A
SHA-512:	F84A1EA44F3B274A4819E64E59AE830D0F8F557972F628778BE06C9FEE64C711A03C2FF9C9E27E0CEF635436E8EAC06CF11E3D6534CDF024B552A442CAC74CE7
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_679a7d8d20d369749e733f7a1173ad271ef1b68_82810a17_194eccc1\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.=.1.3.2.8.4.7.2.1.2.7.9.1.3.7.5.3.7.9.....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.=.1.3.2.8.4.7.2.1.2.9.1.2.7.8.1.7.9.9.....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.=.8.5.1.4.3.b.d.7.-.4.3.f.0.-.4.9.d.b.-.b.f.9.4.-.e.e.f.2.e.1.e.c.0.e.8.d.....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.=.6.e.f.2.5.7.7.a.-.1.2.b.c.-.4.6.d.7.-.b.c.a.5.-.a.2.7.c.9.5.6.3.d.8.9.3.....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.=.0.0.0.0.1.8.6.4.-.0.0.0.1.-.0.0.1.7.-.8.c.9.6.-.4.9.0.c.d.6.f.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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\WER2248.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 08:21:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44360
Entropy (8bit):	2.15607405144888
Encrypted:	false
SSDEEP:	192:VxCQbMeO06O5SkbmQROdbh5KY1qOn/vKCuKOn:hprF5LbpR6hJ1Dn/SCuT
MD5:	FD2E9994A8DE5AD87F3CB742FFD555F4
SHA1:	56E0691F7126F458D7ECCCE000BD6DBE157F5F7C
SHA-256:	0BB64E107650F8BA84BED9EE4B90AE841F1F7B2B15D0122D0BAD8072C31CA4E4
SHA-512:	FE9F72941FAA47F99C7F9E5A05DE437F4A9C4829B68B8C133FD8A39888F724C67696A89FBB5F3F8A981F0C12F1043F930AD5F7E3FAAABB1E0E4E547091764564
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....1.a.....-.....T.....8.....T.....@.....U.....B..... .....GenuineIntelW.....T.....d...y1.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\WER2D07.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):	3.6922389131568143
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipb67zPx6Y+i67gmfT/hSdCprB89bKhsfw+um:RrlsNi16h6YL67gmfT/hSrKafF
MD5:	AD1DA9DE49D4774BDCAFB6C2AF754C22
SHA1:	95DB8F2ED0CC911DE3325291637CEB215DE9EE94
SHA-256:	711A31E610D9927AB855EA3BF8F33578DDE035470B8432B1CC27E001F9E813CC
SHA-512:	03AE30935CAE3473E90B747F517A6E986C3BAD9C478A90CC769B2575D576038A7E0456E3C8BEB0451D21CA06E6F4F42FE5B99ABA464B2B4CCD5775F4355C355
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.>.6.2.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3219.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):	4.487830187276793
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9mwWSC8B+8fm8M4JCdsDnhFoz+q8/QzBtW4SrSid:uITfApJSN5Jl8VvWDWid
MD5:	6651AD79418DF85832BCAE552EB3AA63
SHA1:	F7367F55418EEEDABD65D34666C1032F075EE8E1
SHA-256:	4C002C406E936DF859BC9AD07399C6AFCA78B3ECEF3F6C812218FF177038ED1F
SHA-512:	D1EE152CCB5E787D3B825D2BCE2EB0CAF4317A20497A66F3A514258C8DA55E0485D07B61ACDE40E6688C2605D760058A874186A62277828CA940AAD5AE19F86
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3219.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="1310012" />.. <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):	4.220771934343298
Encrypted:	false
SSDEEP:	12288:wQXJ+Ay7GTa55TqWf82tqLE4iHQIty/e2GYKO4+h4auQWcsP3nAb/d:XXJ+Ay7GTafTqWRDM4FV
MD5:	693356C775F49212017B1CCC67621067
SHA1:	C8AE772007A2065F30B167C34BA97251DEEF9FC5
SHA-256:	3D71679432ABAC054DBE6EDA15017C68CC2CBD957A6CD24BAFFF5DB19C12F2F0
SHA-512:	ECE68D78573481B9B1EA66005662E6546311DB8F8E321626C8B9E6581523894FD6302463AFFAB7111686B5582FC6B1185D68F6E3CECD4213A425925FFDB8695D
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.d..... .....8p.S.....

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):	3.5241570923994403
Encrypted:	false
SSDEEP:	384:1h75onIrnc8TTVgGwK0X6mnQ7RdovOgls:fFEAc8XVgGb0XJnQ7YvP
MD5:	3AC54AE44B1357BFFD10DB28C3758835
SHA1:	A8D12B5F6E28A7CF8377DD5072D04294DE971621
SHA-256:	187EB7F751847BA62A07CED876AEAB65B0E01B72E2F3FE5F488E87F72D8E80BA
SHA-512:	9F26E65051FEE49D4858C46CC3390EE4E3C8BED23481EA89EAEA0DDEACF87190968EB1CC9695387F0CF7E921786A861F9D4FAD96395DCFFA35D835AAB9D401 41
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.d..... .....>p.SHvLE.N.....U.....T.S1%.%2.....`... ..hbin.....p.\..,.....nk,..d..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..d..... ....Z.....Root.....lf.....Root....nk ..d.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.219826049867601
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.malware2.10228.dll
File size:	565248
MD5:	ce624816acb99a24ed7adc77bb514136
SHA1:	d971e7c7b278859c3a28e3aa0e8c1e3c90e6f86e
SHA256:	af49104bb708fe05b3b491d74e8219a57c20a45a128b3b0 477d6b4035560a200

General

SHA512:	b3b0473cd860b7b3826ffa5ceb18c79ba4d1d618662c2671a6860ed8c979d3a4b4f0b904231b616e7e0c1cfbc555394805e1e78b0dbb61a1dd57ef8140d1b4d4
SSDEEP:	12288:rnYoMi8KFy86zc86boq67oy6zq86xoG6V2C6FoE69oI6Vo8mHo06zo8knoz5fU56:riI0+2OJljTR
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:	0x10004cd0
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:	0x61C34004 [Wed Dec 22 15:11:00 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:	6c630f89c340001062a2ada6a2273a4d

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x66be	0x7000	False	0.378208705357	data	4.35134797384	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x79ae0	0x7a000	False	0.283381227587	data	7.33165354236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x62ec	0x5000	False	0.247509765625	data	5.01040935971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x2f0	0x1000	False	0.09033203125	data	0.788492020975	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x1174	0x2000	False	0.242309570312	data	4.16996433109	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: 5744 Parent PID: 6028

General

Start time:	00:21:12
Start date:	23/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.dll"
Imagebase:	0xd00000
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: 00000001.00000002.874430193.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6164 Parent PID: 5744

General

Start time:	00:21:12
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.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: 6244 Parent PID: 6164

General

Start time:	00:21:13
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.10228.dll",#1
Imagebase:	0xa0000
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: 00000003.00000000.354406335.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.394624997.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.352980099.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6376 Parent PID: 6244

General

Start time:	00:21:16
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6244 -s 684
Imagebase:	0x150000
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