ID: 544258
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.28165.16859
Cookbook: default.jbs
Time: 00:20:14
Date: 23/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.W32.AIDetect.malware2.28165.16859 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: 1112 Parent PID: 4260 14
General 14
File Activities 14
Analysis Process: cmd.exe PID: 5040 Parent PID: 1112 14
General 14
File Activities 15
Analysis Process: rundll32.exe PID: 1752 Parent PID: 5040 15
General 15
Analysis Process: WerFault.exe PID: 6184 Parent PID: 1752 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

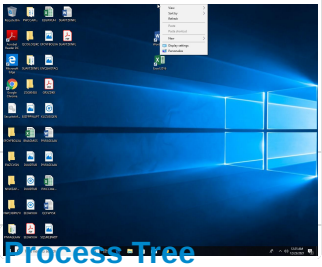
Windows Analysis Report SecuriteInfo.com.W32.AIDete…

Overview

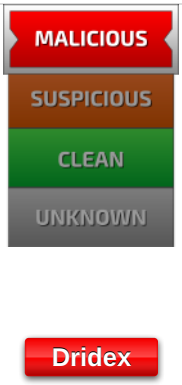
General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.28165.16859 (renamed file extension from 16859 to dll)
Analysis ID:	544258
MD5:	9d86b7a93411bd..
SHA1:	199faa9305b8a1f..
SHA256:	03d956e36d9625..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

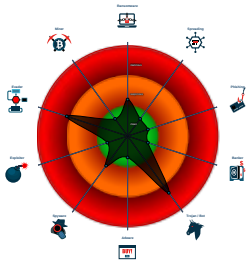


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- 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: 1112 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.28165.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5040 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.28165.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1752 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.28165.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6184 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1752 -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
00000003.00000000.259712771.000000006E861000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.261876126.000000006E861000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.296373547.000000006E861000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.778004464.000000006E861000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.6e860000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e860000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e860000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e860000.5.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:

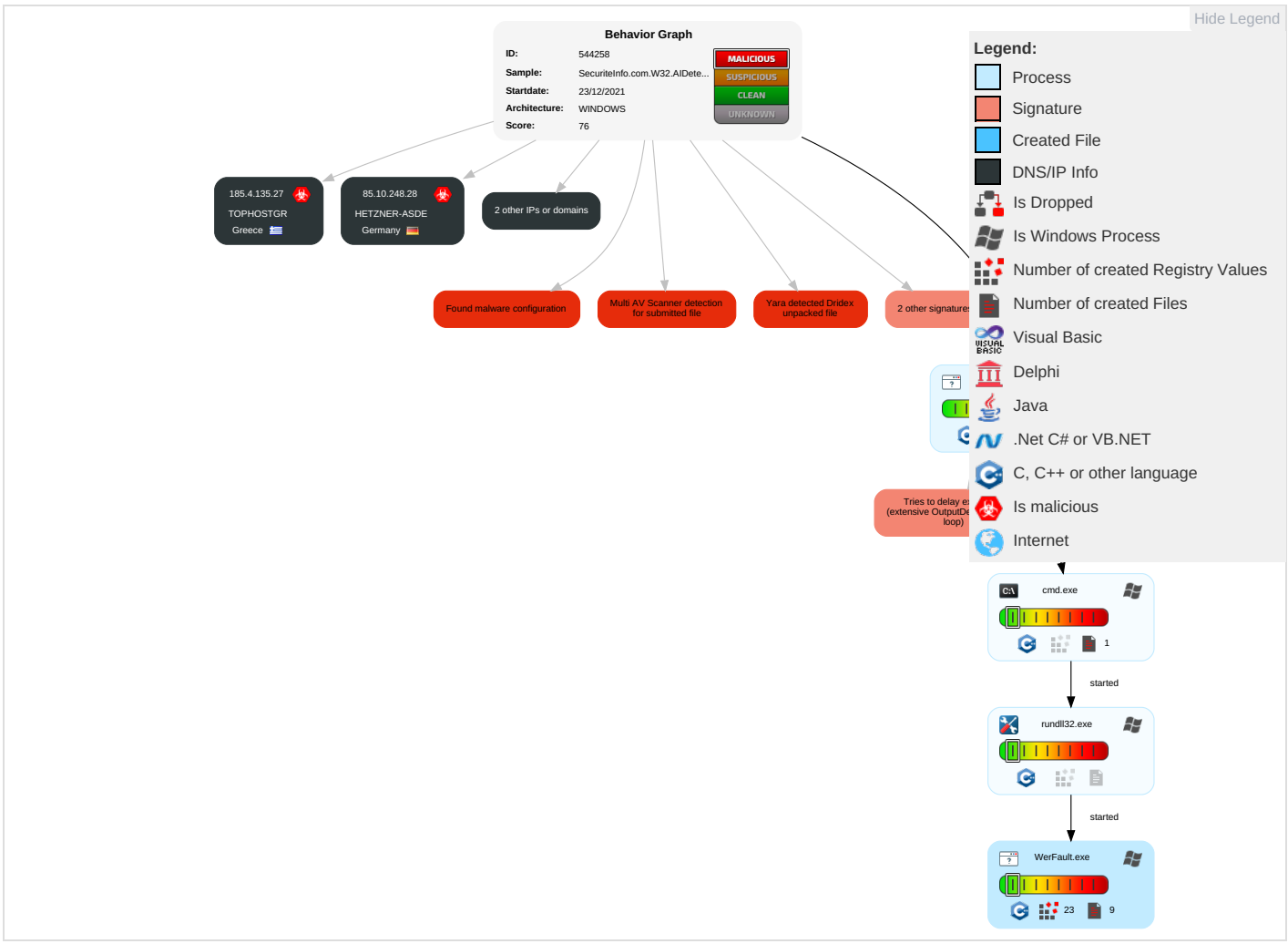
Malware Analysis System Evasion:

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 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	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 Devi 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

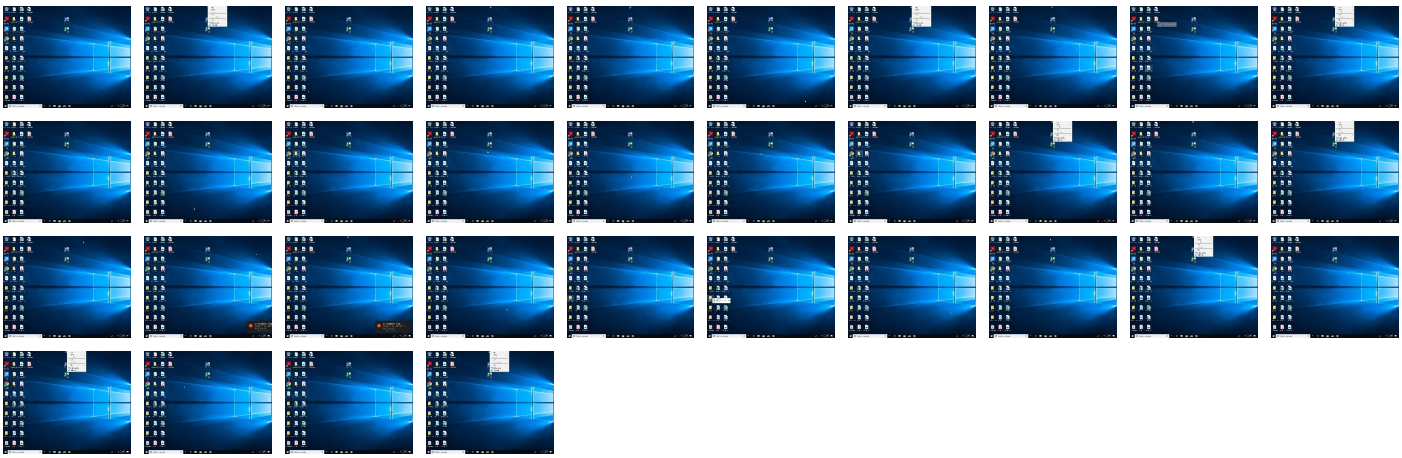
Behavior Graph



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.malware2.28165.dll	19%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.28165.dll	23%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.6e860000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.6e860000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.1080000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.3290000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6e860000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.3290000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.3290000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.6e860000.2.unpack	100%	Avira	HEUR/AGEN.1144420		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:	544258
Start date:	23.12.2021
Start time:	00:20:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.28165.16859 (renamed file extension from 16859 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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@6/6@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 98.6%) • Quality average: 79.8% • Quality standard deviation: 24.3%
HCA Information:	Failed

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

Simulations

Behavior and APIs

Time	Type	Description
00:21:33	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_cb141ddbd73935fa41bc7de65f3b5892ae8957_82810a17_19102adb\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):	0.9221392096330553
Encrypted:	false
SSDEEP:	192:jYi20oXPJ/HBUZMX4jed+fP/u7sBS274ItWc:siwXPJ/BUZMX4jeKP/u7sBX4ItWc
MD5:	22C62B74B234869135A4E9A714C759E7
SHA1:	B2BFE27101F367EA0F32D7D8130EB94404D2FDA5
SHA-256:	73870BAA34D39FDE9A317CF4F0BBF94291F9EE91FCC6E68A5EADB345E761C412
SHA-512:	71135017C1BFEA9DDD16BEF7B69DAC337B3E8FE5AE953C65E8D478E041568ACFEB9BF76B724663FF80112DC357E778857A11E10D5F104F4591DE529C5C1A08EC
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_cb141ddbd73935fa41bc7de65f3b5892ae8957_82810a17_19102adb\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.=.1.3.2.8.4.7.2.1.2.8.2.9.1.6.9.7.4.6.....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.=.1.3.2.8.4.7.2.1.2.8.8.8.2.3.1.9.7.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.7.5.3.d.a.2.-.e.1.5.f.-.4.1.3.5.-.b.5.e.6.-.f.6.5.b.7.3.a.6.8.0.f.6.....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.=.d.9.a.4.9.2.1.e.-.2.f.7.c.-.4.0.6.a.-.8.a.7.2.-.3.3.c.b.2.b.2.4.7.2.7.a.....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.=.0.0.0.0.0.6.d.8.-.0.0.0.1.-.0.0.1.7.-.d.c.f.1.-.d.5.0.d.d.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\WER169.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 08:21:24 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44176
Entropy (8bit):	2.186798806470374
Encrypted:	false
SSDEEP:	192:hoSl0XFtsbozvO5SkbmQDqi842IKCn7lEng:6tsum5LbpSkKCnxE
MD5:	CECE8F159FABEAE2D23EBEEB97377593
SHA1:	E615AE72674D9109EF641FF438A11B8748B53023
SHA-256:	DBC9352921AAC3757540AC520E5EA80DA264BAE3C87CC12592DB52289522F56B
SHA-512:	FBE3A7422A500A0642F381E8EAC29D2D154BDA9FA210E90B7C4907F50F1F2A7C9AC48467D2A772078350B0E7A59876DF7007A4C7DB3F820A1C2AF27FA76DAF5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....1.a.....-.....T.....8.....T.....@...P.....U.....B..... .....GenuineIntelW.....T.....{1.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\WER7E3.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):	3.690573663154269
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi0v67zH6Yih6FgmfT/WS4CprJ89b8csffUm:RrlsNiM6P6Y06FgmfT/WSm8vfZ
MD5:	C7EC3F984AD1C0CFE1533950A4E301CC
SHA1:	7105D01259A549F30F912ACE0668B8E6B2D9B0D9
SHA-256:	76988F5DA21FD3B0FE61643C3CF226756E553326EBC6850A04265CD2C732F347
SHA-512:	79ED62637549BDEFA17D7386C114577F6D25D2A557F8D15B22C1D288067AD39CD5A9B8D35BE457287897379A164CE26B4160B312725E9E2D30CDE826D3904D5
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.>.1.7.5.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBCC.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):	4.489200641127041
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9syWSC8Ba8fm8M4JCdsDIhFU8+q8/Q2Bu4SrSEd:uITfArTSNlJlN8VdDWEd
MD5:	3DD484F1C22DE35EF496E0D108A2144B
SHA1:	A4B75D58E1C7AB93E0BC23D596566BEFDD3705C1
SHA-256:	F2071FB8027F8AAB76A231E60A7E7CD1535975AFF6E19F1FE9ECDCA02930B56A
SHA-512:	34A2535839C897BFE5FE086D00BAB22326877C306620E26AFB8FC2FEEEB7C45A00E98A765A51381F7565EAC3488262274459EEF62D39A83C1B5BC846AF771437
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBCC.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):	4.279967674722502
Encrypted:	false
SSDEEP:	12288:J6qDtK4adayZdIep01Tt8KEPZTaNRu6H58oZkTDeJjd5kLd8Xe:EutK4adayZdIepMt+az
MD5:	1BBE68F4295DC4AD19C0BB363451D431
SHA1:	5F2D7EB58C594163EB7D901DCF9668C3BCA551F3
SHA-256:	0D231027E39BED35782A9A246624B0FCDBBF785447B76ED668048A6890C8CD52
SHA-512:	648F88E3A167434A410E9D93B3405A833CD24359DBF14D0CB053F6108B16247F3C62F14103A86668C9F8B6CC8CDDC185FD02F147058401D92FF28042BEF68944
Malicious:	false
Reputation:	low
Preview:	regfW...W...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.rmtmn]..... .....).L..... .....

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):	4.1178310120760155
Encrypted:	false
SSDEEP:	384:IYIgJ53ETxxk2Ru3cvYBno9SaP5SpafYtx+ygkhBzpfjLjQOA6XadM9xfc:IfgX3uxkSu36YBYSaPspafYtlygcfj3z
MD5:	26311DD3580FAA8C84B9DEC9826A55E3
SHA1:	9449469942F4AA525FD37CD4C3740E79E7DDFD18
SHA-256:	0041A6249B9EC43981E4E6C7314FB5FC7F45E451B2553CC4F1D5424D3C111F06
SHA-512:	2C3EBFD2CA53CDAF2A69EE80C8CBDADC5C663452501550D0D9EC9718DC6FD1E03DD74269D71B28AE24F0394EC61C917A65CAA433784A9E21DDEB677DF863CCB
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.rmtmn]..... .....).LHvLE.^.....V.....RD.zE....G.^R.....0.....hbin.....p.\.,.....nk,..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....8~..... .....Z.....Root.....lf.....Root....nk ....*.....DeviceCensus..... .....vk.....WritePermissions

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.2202707172455005
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.malware2.28165.dll
File size:	565248
MD5:	9d86b7a93411bd7cc5c68b4f49709c27
SHA1:	199faa9305b8a1f6645c07098990ac62da6a7d4d
SHA256:	03d956e36d96255794c7999c52cbc3ea5fc6ec52193a0a3db40e7fb1414b6219

General

SHA512:	35b7a39d10f5d570355065737264eeb469833d6a6526cc77da0d88144aea28381d81ec13e3afe5cdedfb0dcf1464847ee886c3bcefcf687c93cf5b7cc4b4c3e9
SSDEEP:	12288:znYoMi8KFy86zc86boq67oy6zq86xoG6V2C6FoE69oI6Vo8mHo06zo8knoz5fU56:zil0+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	0.380964006696	data	4.37724235459	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x7916e	0x7a000	False	0.28338322874	data	7.33164589989	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x696e	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	0x1baf	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: 1112 Parent PID: 4260

General

Start time:	00:21:15
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.malware2.28165.dll"
Imagebase:	0x1210000
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: 00000001.00000002.778004464.000000006E861000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5040 Parent PID: 1112

General

Start time:	00:21:15
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.malware2.28165.dll",#1
Imagebase:	0x870000
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: 1752 Parent PID: 5040

General

Start time:	00:21:15
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.malware2.28165.dll",#1
Imagebase:	0x320000
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: 00000003.00000000.259712771.000000006E861000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.261876126.000000006E861000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.296373547.000000006E861000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6184 Parent PID: 1752

General

Start time:	00:21:20
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1752 -s 684
Imagebase:	0x160000
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