JoeSandbox Cloud BASIC

**ID:** 544184
**Sample Name:**
SecuriteInfo.com.W32.AIDetect.malware1.23460.908
**Cookbook:** default.jbs
**Time:** 20:09:32
**Date:** 22/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Windows Analysis Report SecuriteInfo.com.W32.AIDete…

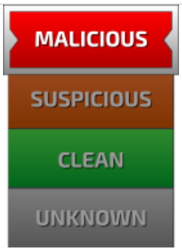
## Overview

### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.W32.AIDetect.malware1.23460.908 (renamed file extension from 908 to dll) |
| Analysis ID: | 544184 |
| MD5: | d633b0989e97dc.. |
| SHA1: | 6e5a7f0493fea40.. |
| SHA256: | 03ba158e40b1f9c. |
| Tags: | dll Dridex |
| Infos: | |

Most interesting Screenshot:

### Detection



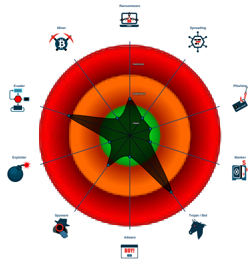
Dridex

| | |
|---|---|
| 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: 6196 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 3324 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2964 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.23460.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4764 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -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 |
|---|---|---|---|---|
| 00000000.00000002.819315155.000000006EC31000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000003.00000000.300409127.000000006EC31000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000003.00000002.329263853.000000006EC31000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000003.00000000.298329265.000000006EC31000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 3.0.rundll32.exe.6ec30000.5.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 3.2.rundll32.exe.6ec30000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 3.0.rundll32.exe.6ec30000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 0.2.loaddll32.exe.6ec30000.2.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:

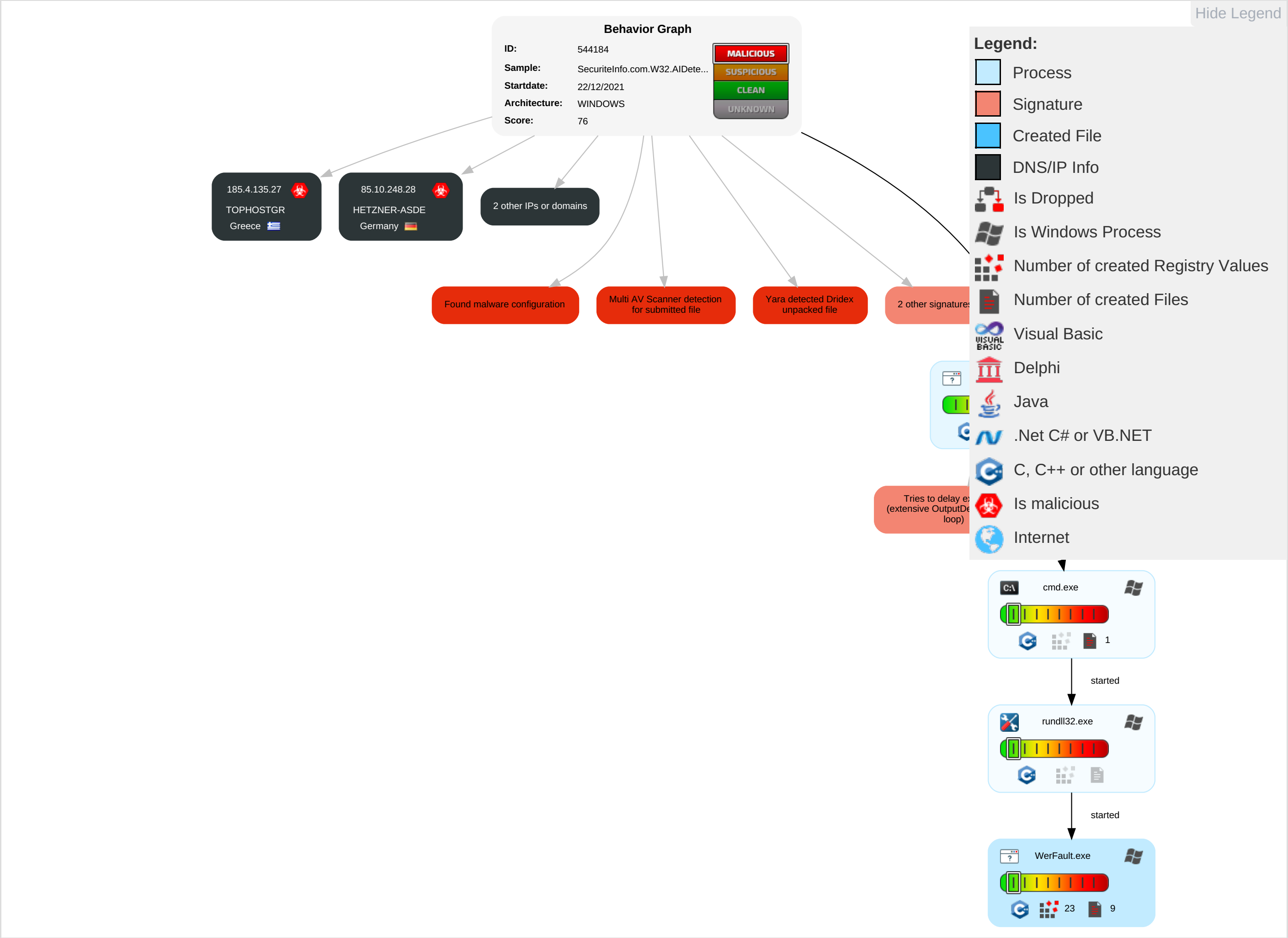
### Malware Analysis System Evasion:

**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



Behavior Graph

ID: 544184

Sample: SecuriteInfo.com.W32.AIDete...

Startdate: 22/12/2021

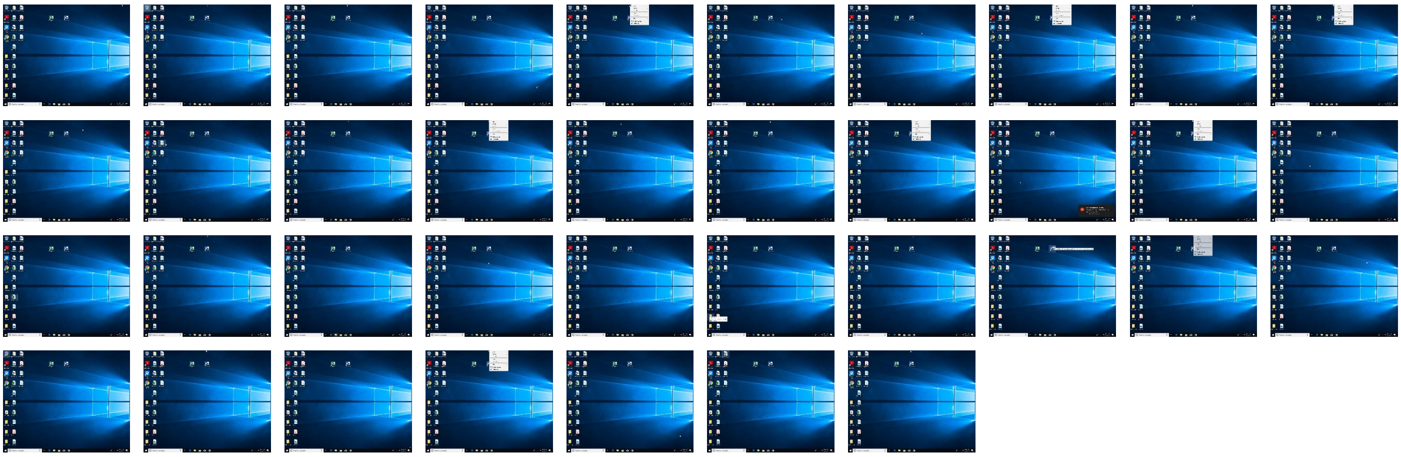
Architecture: WINDOWS

Score: 76

## 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 | 21% | Virustotal | | Browse |
| 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 |
|---|---|---|---|---|---|
| 3.0.rundll32.exe.230000.3.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 3.0.rundll32.exe.230000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 3.0.rundll32.exe.6ec30000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 0.2.loaddll32.exe.af0000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.2.loaddll32.exe.6ec30000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 3.2.rundll32.exe.6ec30000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 3.2.rundll32.exe.230000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 3.0.rundll32.exe.6ec30000.5.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: | 20:09:32 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 12s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.W32.AIDetect.malware1.23460.908 (renamed file extension from 908 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal76.troj.evad.winDLL@6/6@0/4 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 53.8% (good quality ratio 51.4%)<br>• Quality average: 78.7%<br>• Quality standard deviation: 27.6% |
| HCA Information: | Failed |

| | |
|---|---|
| Cookbook Comments: | - Adjust boot time<br>- Enable AMSI<br>- Override analysis time to 240s for rundll32 |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 20:10:42 | 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_435bf9987f6a7ee95ec1aabecf98fbf5b0b7b2_82810a17_131cfb8a\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): | 0.9219508196362544 |
| Encrypted: | false |
| SSDEEP: | 192:3EZiT0oXy5/HBUZMX4jed+yf/u7sYS274ItWc:GiNXy5/BUZMX4je3f/u7sYX4ItWc |
| MD5: | D9FB776CB5A4EF1F641889E6E9193B1B |
| SHA1: | C9C86D8EFB07E52133951F821B054C8C7BA3FA78 |
| SHA-256: | AD8A021C47C521CA5F0437F2197D7A0BF831319A24A380FD6A8DE275C6199D5D |
| SHA-512: | 5EC1929C8E8D86B888C60694C8AFE1070848DC2B7B0CDE0265A008059BB027954E5386BCB5C62C424E35C8D5BAB331AF4C202D2F041B3141028F142AF485C63 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.4.7.0.6.2.3.6.4.0.6.4.1.4.6.....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.=.1.3.2.8.4.7.0.6.2.4.0.7.9.7.0.2.0.6.....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.=.1.4.e.7.e.5.7.4.-.5.8.3.c.-.4.c.a.2.-.b.7.a.1.-.b.4.5.3.e.8.1.6.2.2.f.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.=.3.b.3.f.0.d.7.8.-.5.d.e.7.-.4.1.7.a.-.b.6.d.0.-.8.7.8.6.9.c.f.7.7.8.8.1.....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.=.0.0.0.0.0.0.b.9.4.-.0.0.0.1.-.0.0.1.c.-.0.4.8.4.-.4.0.0.6.b.3.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\WERE1C9.tmp.dmp** | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Dec 23 04:10:37 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 46356 |
| Entropy (8bit): | 2.0556218445180456 |
| Encrypted: | false |
| SSDEEP: | 192:WpMgAEEcxd3VvzLO5SkbmQsMO5efz9g3jF0F+MOl9NdniI:Q3Fe5LbpsMOWzS0FtOl9vi |
| MD5: | D33CA82EBE6E92E8C9EE3BF9999FE093 |
| SHA1: | F9B632E7D4E0AFCB543086B5F1858720220575CB |
| SHA-256: | 0AFA0AC6A780D0EDF0ECFD74C0468568FA4715940874F9D73AEABB5536D1005D |
| SHA-512: | BCF9D1FD6C48CA06FDF0F15EE4C044C3834AAF15999AD872AD8FC4E01E7F4CD43CB8E28BB99942D86AC664081A1D51F2479227A63BB08284786EF16799E557E 4 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP....... ..........a........................................-..........T.......8...........T..............L...........................................................................................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\WERE8FD.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): | 3.6885132910410148 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNicp67Og56YBDq6cgmfT/mSWCprk89bXEsf3Adm:RrlsNii676YBO6cgmfT/mSfX3f3 |
| MD5: | A19806F072B83C8F9677DE08F86CB46E |
| SHA1: | 2F9E8BF4485B23CA8F91777A8648D2091A12E1D9 |
| SHA-256: | 6A2050363CCD46EC2B084E078F8066624B4819D01F9888765C09AA4E6FD2E30A |
| SHA-512: | 3E8E90340C69DE87B750866483032133CCC6E11C16C5C957D190FB29B79E33985D8625BE22BC11741D97FDC2C689065A0AA2810AB97214CB530FBF46D859A0C |
| 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.>.2.9.6.4.<./.P.i.d.>....... |

| **C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBBD.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): | 4.490369220814527 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zsPJgtWI9XHWSC8B18fm8M4JCdsD6hF+NgW+q8/QYBH4SrSh6d:uITfxE2SNMJlTgWVeDWh6d |
| MD5: | BA36C1BA3C0332D7CE22587788D18B9A |
| SHA1: | 00E9266E46602FB7F9BDF52C9347468CFF0A7B91 |
| SHA-256: | 8CDF1624CA332715098C4F4ABFB257ECE778B94981822151202E1FCEAA8A17F7 |
| SHA-512: | 2BCD053D5F1E890851B3AFE45CBD860533B5183434AB274F64DAA4B5B9E28AD375B46BF3DBD511B86EE021B3CDED159AED9E11F03FCE30C7CA233F0910B4E 89 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">..  <tlm>..    <src>..      <desc>..        <mach>..          <os>..            <arg nm="vermaj" val="10" />..            <arg nm="vermin" val="0" />..            <arg nm="verbld" val="17134" />..            <arg nm="vercsdbld" val="1" />..            <arg nm="verqfe" val="1" />..            <arg nm="csdbld" val="1" />..            <arg nm="versp" val="0" />..            <arg nm="arch" val="9" />..            <arg nm="lcid" val="1033" />..            <arg nm="geoid" val="244" />..            <arg nm="sku" val="48" />..            <arg nm="domain" val="0" />..            <arg nm="prodsuite" val="256" />..            <arg nm="ntprodtype" val="1" />..            <arg nm="platid" val="2" />..            <arg nm="tmsi" val="1309761" />..            <arg nm="osinsty" val="1" />..            <arg nm="iever" val="11.1.17134.0-11.0.47" />..            <arg nm="portos" val="0" />..            <arg nm="ram" val="4096" />.. |

| **C:\Windows\appcompat\Programs\Amcache.hve** | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | MS Windows registry file, NT/2000 or above |
| Category: | dropped |

| C:\Windows\appcompat\Programs\Amcache.hve | |
|---|---|
| Size (bytes): | 1572864 |
| Entropy (8bit): | 4.276319444681263 |
| Encrypted: | false |
| SSDEEP: | 12288:n7n8Dpvri2L28pTOUEr71nmFnj40sd22Cq69fqiELV1XeaeTsllkqU:7n8Dpvri2L28pTbz |
| MD5: | 1FED069D51D64B2EF9E749426956732F |
| SHA1: | CDD1104BFD69A697852499ABBF5006E98AE7AB8F |
| SHA-256: | D6774A26604D1DAF5505219F21A1B9221CDBEBDB769C051A661F72308868A734 |
| SHA-512: | 508644E48D9D894E37E99146E9BE12B437AF5299EA0EFB10E9B7E6A31A8D278649B74D4871A2A1BDDAB08800869CA37EFF1C30BB32431D9AA05FFE514AA96873 |
| 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.*.................................................... ........................................................................................................................................................................................................................ ...............-n.U.......................................................................................................................................................................................................... ................................................................................................................................................................................ |

| 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): | 4.032823767487586 |
| Encrypted: | false |
| SSDEEP: | 384:FJYJ5Rftx1QPJ4XLsFcnE7kvPBqXASeq5QMVyi6+/Jl4Lk4UZd1DoXznZXvwv0:PYXRftx1mJ4XoFcE74BqXTeq5QMVyi6o |
| MD5: | C5C78BB71FE7AB8673AEE48EF6AA728D |
| SHA1: | A471D1595856DC590BE90997573CD33E1168A753 |
| SHA-256: | 9430DBD473E740ACCF71017BEB7808AF2F945697F3A1E48023BB16EA5465DBA3 |
| SHA-512: | 7C4266C37736119F4DD01677C8BF44DA0B49E75DCB112D0A4CEC7755F9C3DDD121DD10BCC3863B626AED725708F7AF3FF72B6FEF665FC3B74AAC70041124036 |
| 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.*.................................................... ........................................................................................................................................................................................................................ ...............+n.UHvLE.^......Y............b..\..N..\i.............0................... ..hbin................p.\..,..........nk,.9...........0.......................... ...........................&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}......nk .9........... .......................... .......Z.......................Root........lf......Root....nk .9........................}............. ...............*...............DeviceCensus..................... ..vk.................WritePermissionsCheck... |

## 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%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• 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 |
| 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: 6196 Parent PID: 2236

#### General

| | |
|---|---|
| Start time: | 20:10:29 |
| 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: | 0x12a0000 |
| 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: 00000000.00000002.819315155.000000006EC31000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | moderate |

#### File Activities

Show Windows behavior

### Analysis Process: cmd.exe PID: 3324 Parent PID: 6196

#### General

| | |
|---|---|
| Start time: | 20:10:30 |
| 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: | 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: 2964 Parent PID: 3324

### General

| | |
|---|---|
| Start time: | 20:10:30 |
| 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: | 0x250000 |
| 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: 00000003.00000000.300409127.000000006EC31000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.329263853.000000006EC31000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.298329265.000000006EC31000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: WerFault.exe PID: 4764 Parent PID: 2964

### General

| | |
|---|---|
| Start time: | 20:10:34 |
| Start date: | 22/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -s 672 |
| Imagebase: | 0x11b0000 |
| 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