
**ID:** 544174
**Sample Name:**
SecuriteInfo.com.W32.AIDetect.malware1.4295.dll
**Cookbook:** default.jbs
**Time:** 20:02:55
**Date:** 22/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

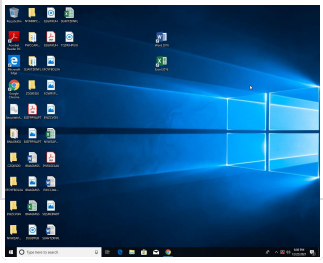
# Windows Analysis Report SecuriteInfo.com.W32.AIDete…

## Overview

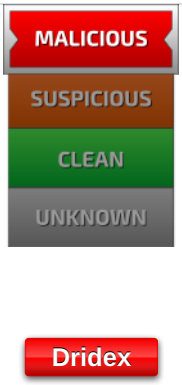
### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.W32.AIDetect.malware1.4295.dll |
| Analysis ID: | 544174 |
| MD5: | 57cc0ec93c5534… |
| SHA1: | bcf46bb64fc5a67.. |
| SHA256: | 60bd3eba4dac7d.. |
| Tags: | dll Dridex |
| Infos: | |

Most interesting Screenshot:



### Detection

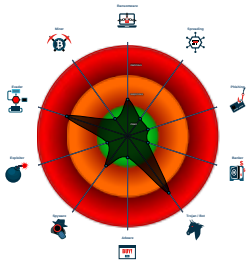



| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### 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: 6296 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.4295.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6328 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.4295.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6368 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.4295.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6564 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -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 |
|---|---|---|---|---|
| 00000002.00000000.263879217.000000006E831000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000000.00000002.654367413.000000006E831000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000002.00000002.303178231.000000006E831000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000002.00000000.261899992.000000006E831000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 2.0.rundll32.exe.6e830000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 0.2.loaddll32.exe.6e830000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 2.2.rundll32.exe.6e830000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 2.0.rundll32.exe.6e830000.5.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:

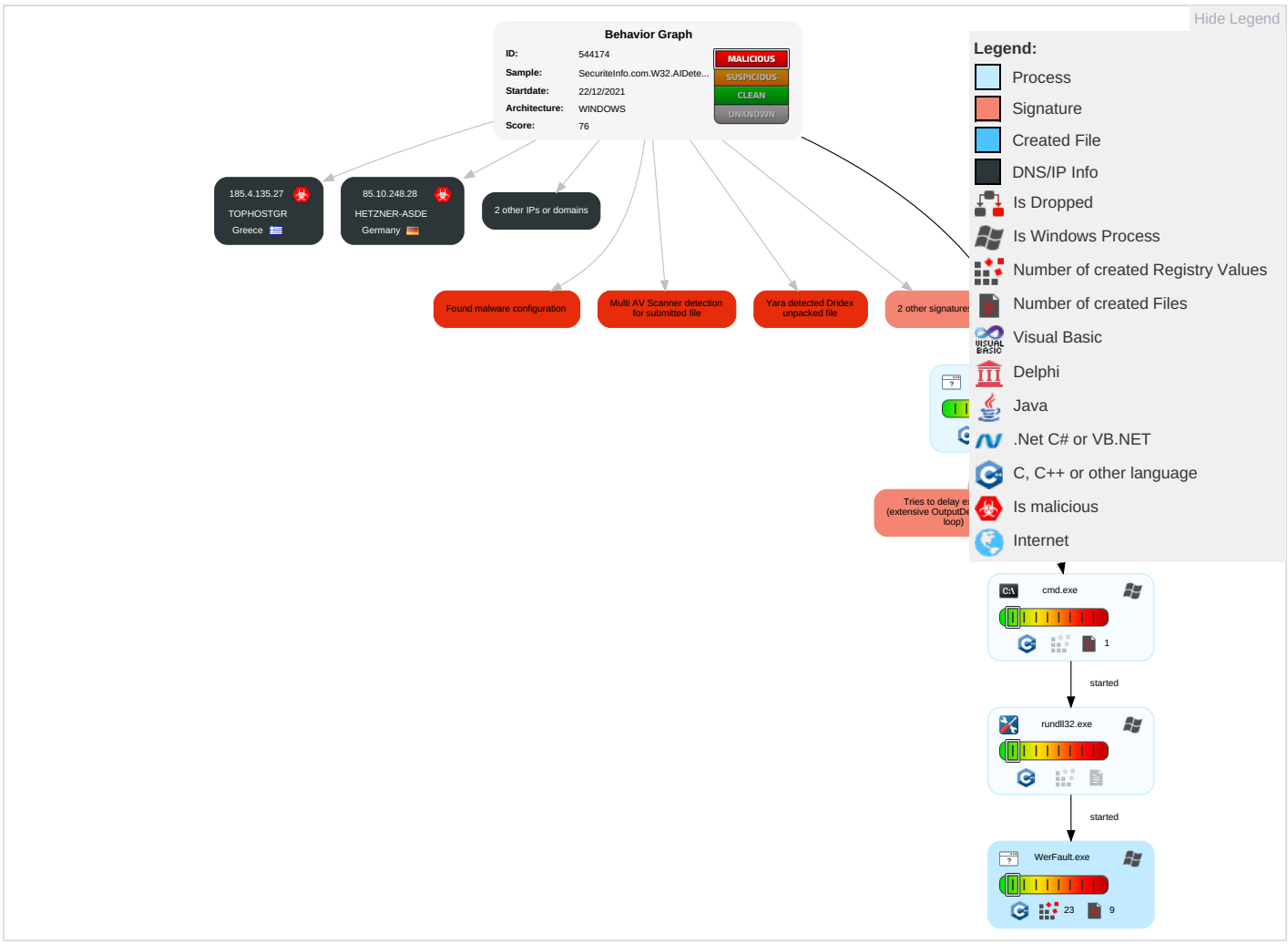
### Malware Analysis System Evasion:

**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 |

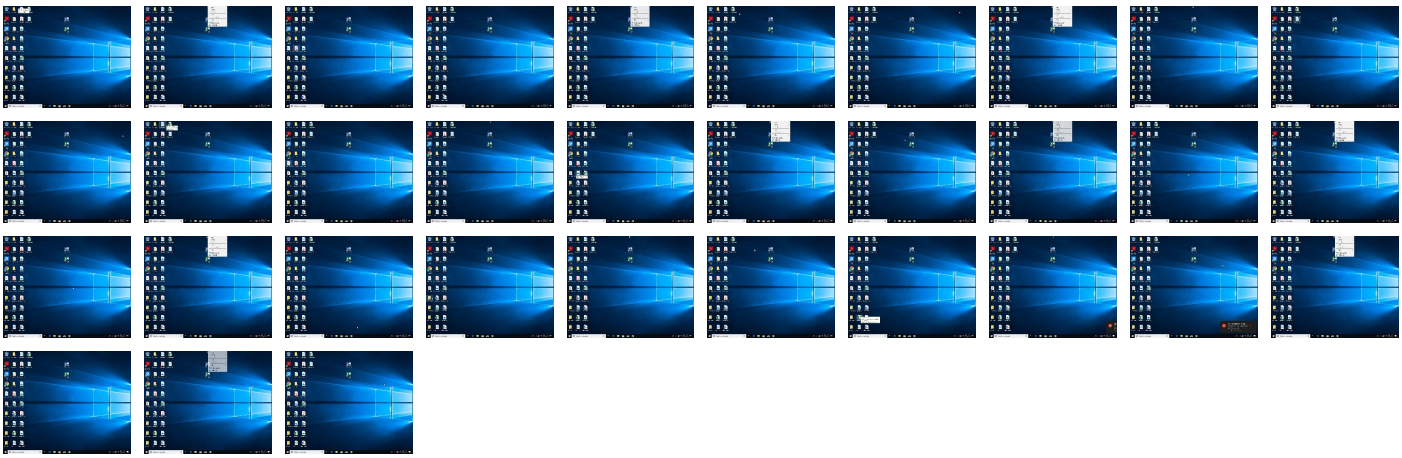
## Behavior Graph




## 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.malware1.4295.dll | 23% | Virustotal | | Browse |
| SecuriteInfo.com.W32.AIDetect.malware1.4295.dll | 26% | ReversingLabs | Win32.Worm.Cridex | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.loaddll32.exe.6e830000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 2.0.rundll32.exe.3220000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.0.rundll32.exe.3220000.3.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.2.rundll32.exe.6e830000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 2.2.rundll32.exe.3220000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.2.loaddll32.exe.f60000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.0.rundll32.exe.6e830000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 2.0.rundll32.exe.6e830000.5.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: | 544174 |
| Start date: | 22.12.2021 |
| Start time: | 20:02:55 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 24s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.W32.AIDetect.malware1.4295.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: | 29 |
| 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: 100% (good quality ratio 96.8%)<br>• Quality average: 78.9%<br>• Quality standard deviation: 26.2% |
| HCA Information: | Failed |

| | |
|---|---|
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Sleeps bigger than 120000ms are automatically reduced to 1000ms<br>• 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_acf0c1b1d931196b9999224049caaf48ed8bd9_82810a17_18eecba7\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): | 0.922125224955901 |
| Encrypted: | false |
| SSDEEP: | 192:xmMiC0oXuA/HBUZMX4jed+fm/u7sCS274ItWc:AMiEXuA/BUZMX4jeKm/u7sCX4ItWc |
| MD5: | 499007EBF56D77B0189DDA896BA1C4DE |
| SHA1: | 91D7878017B238972F91D5C792BB959FEC82DE4E |
| SHA-256: | EBD2A36EBCA81495AFA4DD1E7028AC93E78A009519858BDAF3073E0837EADC3C |
| SHA-512: | 2B7B64D821BE1A4653C867F05C390A9A8B897ABDD17A108FC8B1E8C8B53BC4DC328682F593F2C01DD0BF1D326098062F77BDA0EFD9E84A715AC7A37DD256B3D |
| Malicious: | false |
| Reputation: | low |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_acf0c1b1d931196b9999224049caaf48ed8bd9_82810a17_18eecba7\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.=.1.3.2.8.4.7.0.5.8.4.3.0.4.1.3.8.3.1.....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.=.1.3.2.8.4.7.0.5.8.5.4.6.9.7.5.8.4.4.....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.=.f.6.e.b.f.d.c.4.-.8.8.6.c.-.4.4.7.c.-.b.4.6.5.-.1.c.d.6.1.8.e.5.4.7.f.b.....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.=.0.4.8.d.9.9.2.a.-.d.b.3.0.-.4.8.9.c.-.b.1.b.c.-.9.f.3.1.5.b.a.f.7.7.9.c.....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.e.0.-.0.0.0.1.-.0.0.1.7.-.8.8.4.0.-.5.7.1.b.b.2.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\WER97B6.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Dec 23 04:04:04 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 45498 |
| Entropy (8bit): | 2.1178952305241547 |
| Encrypted: | false |
| SSDEEP: | 192:SDrw0XFeUH/qO5SkbP/drlei+HEEqxKxjyCrmYny:6eUf15Lb3drXYxjyvYy |
| MD5: | 797BC81A1158FB63989497B035879FC6 |
| SHA1: | 626D53CAE42D30730110E4E1CB86ED4127EA47CD |
| SHA-256: | 73104FFC864263D171093BC3EEF03AFFE06660EAAADF320F76C447916C9B3533 |
| SHA-512: | 874F47E20AE83DAF648AA7F5CC04DFFBC9E11CD746D99A08CB32D9DBE0CC9ACE8775473517C9EF300C36F3365ABE074EEACFCF244FE54F2F8612BFB2DF7C5AF8 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP..... .....4..a.....-.....T.....8.....T.....@...z.....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\WER9F87.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): | 8324 |
| Entropy (8bit): | 3.6916703589045934 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNiOp67OgmsTB6Y086KgmfT/ZSuCpro89bsWsfrEm:RrlsNiw6N6Y/6KgmfT/ZSjs1fN |
| MD5: | F5B52B104E61752E08FA79034F86427A |
| SHA1: | 0A8365C70C11F7117C1C5A159BE4E210067BD68E |
| SHA-256: | 45CC1E4E430B0564D53DB748A41848C884685CD94A4BD9F2B347DC3745A1190D |
| SHA-512: | FBD4FD83351BE5B43DA74F54CA5EB53AB13E79F6BC2EB6BDA30E3C726A7022CDACABC61964589FE1E7021C8A7FCEB5F2F0A634E603CC3E9656284178323F46C7 |
| 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.>.6.3.6.8.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERA219.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4696 |
| Entropy (8bit): | 4.487517127877766 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zsTJgtWI9m4WSC8BI8fm8M4JCdsDvhF3e+q8/QLBBc4SrSEd:uITftdxSN3Jl7eVsDWEd |
| MD5: | FF5A047CF993A42F5B5BABA30DE99647 |
| SHA1: | ED221F555C69E434400FCFC08768397CE74AE74C |
| SHA-256: | 60518FEBB19DBDACCB3E4D644C22BC1B737F2BDDEB9F459B6EBEC57C23B231DA |
| SHA-512: | F18D60FE1983B9C3F0C45C12089539753FD5D0A5B37667DA7A95D69851A8042728AD0B5587E77B9E48C1905CAB3DB1B11FE6FE50AB1369966FAA2285E852434B |
| Malicious: | false |
| Reputation: | low |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERA219.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="1309754" />.. <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): | 4.281346260961785 |
| Encrypted: | false |
| SSDEEP: | 12288:no7Mhuoq0S69Kuz5mQPg4hGZVkT4Tn6dwkmEOhdeYtsEhJXUJy:owhuoq0S69Kuz5kqBTh |
| MD5: | B759349E398B9119E7DA64ABBC34BE62 |
| SHA1: | BB1060988E3111E18F01292140BA7BDE6B4E2601 |
| SHA-256: | 75D1B4D1ACB47072856B6D166B08F678ADC1C5FFC9405014EADE4B76CB38FB97 |
| SHA-512: | A172121E871AD20B23A86B6ECB5E12A3640C2AC6B7D37ED85354357FE66A5C3651B2AF3BFA79E4BFEFA811F503985B63F0F9EF8480B1B6296F30AD7915F2CB6 |
| 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.rmtmj.-..... .....u)C..... ..... |

| 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): | 4.116206154896422 |
| Encrypted: | false |
| SSDEEP: | 384:kXFpse53Elxxk7Ru39vYBnt9SaPlSpafYt7+ygEhBzpfjrjQOe6Xadp9xfd:k1pl3LxkNu35YBPSaPIpafYtCyg8fjXW |
| MD5: | 8B67F4AE3DE37568249414D50233DAB8 |
| SHA1: | CEB8AE6992BD6AE8AC6A2DCA0F68FCDA77F9E726 |
| SHA-256: | 0A39149007089E4916B6426C2F3C22F2E304977B7F5CBA417F5625BAE1CCC274 |
| SHA-512: | 753183DE302ACB5E5A5853BE41FADFFB92343E091ACF30FDC479CE2E36887782CDF618CA12B4B3A7C2EF7FAF273A19E776791182F6ED91B2CD94C1F3A8ED8E04 |
| 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.rmtmj.-..... .....u)CHvLE.^.....V.....V.D`}x2..s.?.....0.....hbin.....p.\..,.....nk,..c/..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..c/..... .....8~..... .....Z.....Root.....lf.....Root....nk ..c/..... .....*.....DeviceCensus..... .....vk.....WritePermissions |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.322458028777742 |
| 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.malware1.4295.dll |
| File size: | 544768 |
| MD5: | 57cc0ec93c55348dd7b864e26ec96379 |
| SHA1: | bcf46bb64fc5a673e7889d9ba9baad26bfab0ff7 |

## General

| | |
|---|---|
| SHA256: | 60bd3eba4dac7d37cd07e375f4dbfe5e816b0ab599f28da31c5cf5b180b5849a |
| SHA512: | 562b44d23cbfa0ccec2bee34dfd5cdbad64f87adc8b152c2874d9a4f5b249ff7dfa437aa150fe33e919b3aa3871bf8b92dcbc8cc11b47aed69e791e1d4a9a784 |
| SSDEEP: | 6144:D7+RYf/Mv1UvT4vjYf/Glpov3KvfMvLo+jwHk3UryzU3+R7ff4evm35lQku4+pMQ:D7t2UAogoOwhx7nA4+pMXg |
| 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 | 0.391636439732 | data | 4.47964770197 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x7424e | 0x75000 | False | 0.316228882879 | data | 7.44062687646 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x7d000 | 0x66d8 | 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: 6296 Parent PID: 1988

#### General

| | |
|---|---|
| Start time: | 20:03:55 |
| 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.malware1.4295.dll" |
| Imagebase: | 0x8b0000 |
| 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: 00000000.00000002.654367413.000000006E831000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | moderate |

#### File Activities

Show Windows behavior

### Analysis Process: cmd.exe PID: 6328 Parent PID: 6296

#### General

| | |
|---|---|
| Start time: | 20:03:56 |

| | |
|---|---|
| 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.malware1.4295.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: 6368 Parent PID: 6328

### General

| | |
|---|---|
| Start time: | 20:03:56 |
| 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.malware1.4295.dll",#1 |
| Imagebase: | 0xb80000 |
| 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: 00000002.00000000.263879217.000000006E831000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.303178231.000000006E831000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.261899992.000000006E831000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: WerFault.exe PID: 6564 Parent PID: 6368

### General

| | |
|---|---|
| Start time: | 20:04:00 |
| Start date: | 22/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -s 684 |
| Imagebase: | 0xc30000 |
| 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