
**ID:** 544259
**Sample Name:** SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll
**Cookbook:** default.jbs
**Time:** 00:29:12
**Date:** 23/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Windows Analysis Report SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll 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: 6988 Parent PID: 2808 14
General 14
File Activities 14
Analysis Process: cmd.exe PID: 7064 Parent PID: 6988 14
General 14
File Activities 15
Analysis Process: rundll32.exe PID: 7096 Parent PID: 7064 15
General 15
Analysis Process: WerFault.exe PID: 6472 Parent PID: 7096 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

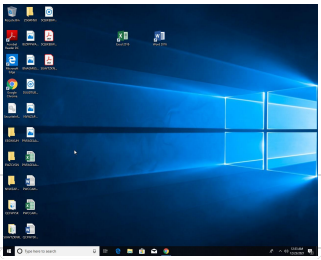
# Windows Analysis Report SecuriteInfo.com.ML.PE-A+Tr…

## Overview

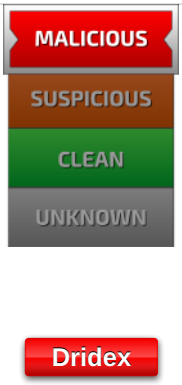
### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll |
| Analysis ID: | 544259 |
| MD5: | 5ca09f4e3e8adcf.. |
| SHA1: | 5c57296e6c7f361.. |
| SHA256: | b9dac63c888f98e.. |
| Tags: | dll |
| Infos: | |

Most interesting Screenshot:



### Detection

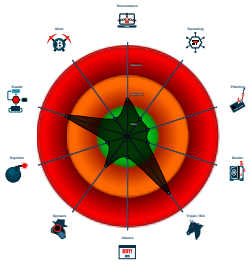



| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### 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: 6988 cmdline: loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7064 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7096 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6472 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7096 -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 |
|---|---|---|---|---|
| 00000002.00000002.684498846.000000006EBD1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000005.00000002.319816001.000000006EBD1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000005.00000000.289027157.000000006EBD1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000005.00000000.293983549.000000006EBD1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 5.2.rundll32.exe.6ebd0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 5.0.rundll32.exe.6ebd0000.5.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 5.0.rundll32.exe.6ebd0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 2.2.loaddll32.exe.6ebd0000.2.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:

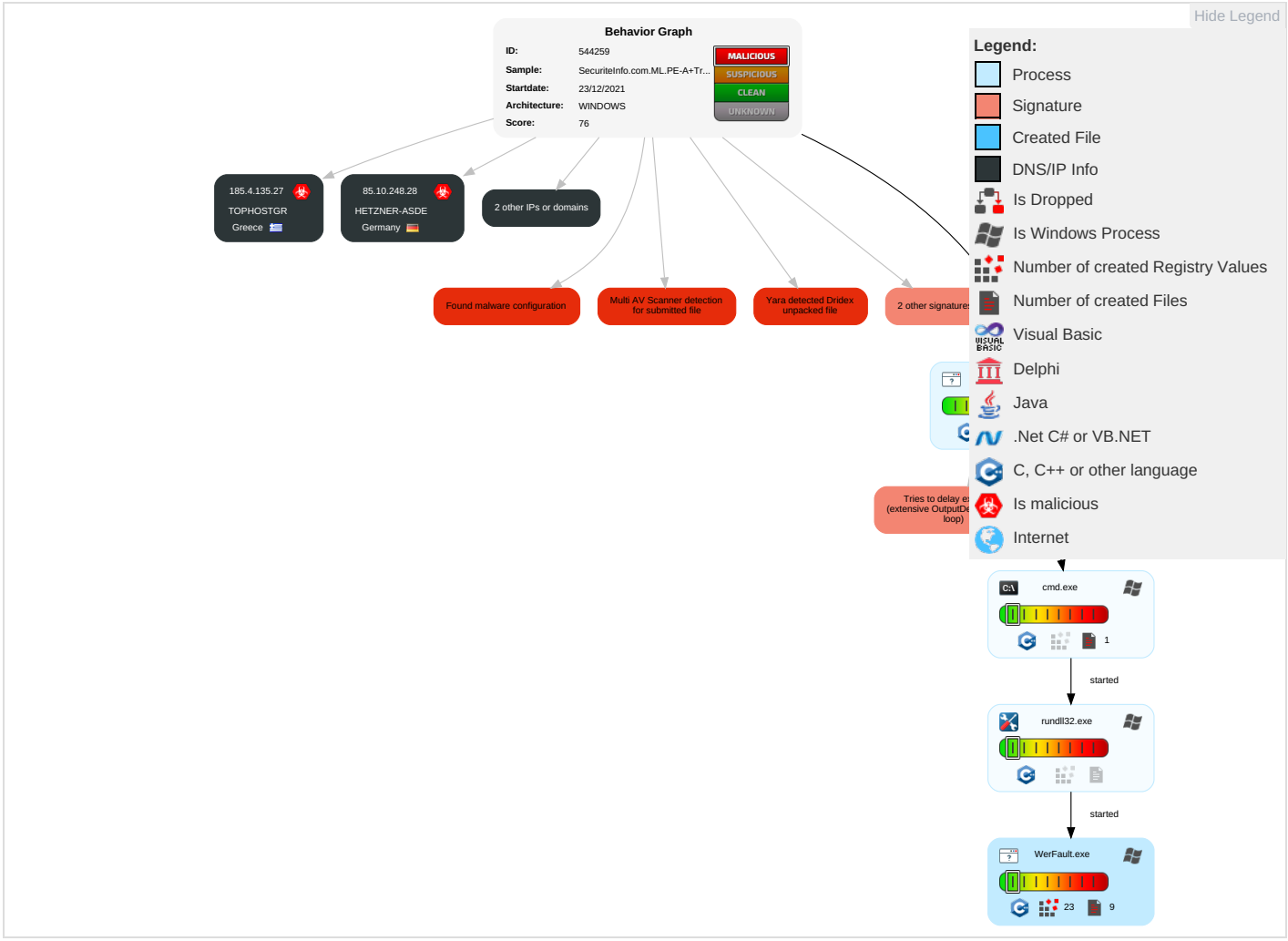
### Malware Analysis System Evasion:

**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 |

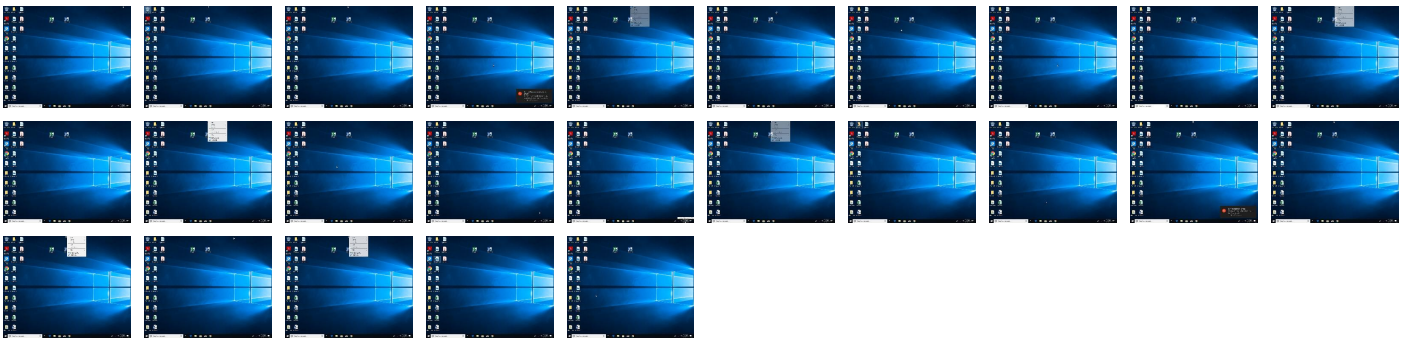
## Behavior Graph




## 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.ML.PE-A+Troj.Dridex-AJA.19171.dll | 21% | Virustotal | | Browse |
| SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll | 23% | ReversingLabs | Win32.Worm.Cridex | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 5.0.rundll32.exe.2dd0000.4.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 5.2.rundll32.exe.6ebd0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 5.0.rundll32.exe.6ebd0000.5.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 5.0.rundll32.exe.6ebd0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 2.2.loaddll32.exe.1e0000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 5.0.rundll32.exe.2dd0000.1.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 2.2.loaddll32.exe.6ebd0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 5.2.rundll32.exe.2dd0000.1.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: | 544259 |
| Start date: | 23.12.2021 |
| Start time: | 00:29:12 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 38s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.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: | 32 |
| 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: 54.5% (good quality ratio 52.3%)<br>• Quality average: 79.8%<br>• Quality standard deviation: 27.1% |
| 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_e288dc6ab8ca5a035f13ca982cf0804f04fb5_82810a17_1870e234\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): | 0.9235346194783932 |
| Encrypted: | false |
| SSDEEP: | 192:XB/iP0oXF/HBUZMX4jed++/u7suS274ltWc:x/ixXF/BUZMX4jeD/u7suX4ltWc |
| MD5: | 79B6682DFDC3181A6CACB79BD3FA4F0C |
| SHA1: | 4BF051547A2C3256AE29DE40EBF0EBCC9D98BF13 |
| SHA-256: | ACBBA9DEE061A9455FA170215AF272C66E560FB4B669506EDC97DB40FDDC6E61 |
| SHA-512: | 64406CA400A2CDEF0F8C4BC1AD19688E33E8423AA0D1F6B938E744B5945526C809CA94A141B0E952A567EBD823DFC710627EC74BD9598D805B0043C1239DDA5C |
| Malicious: | false |
| Reputation: | low |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_e288dc6ab8ca5a035f13ca982cf0804f04fb5_82810a17_1870e234\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.=.1.3.2.8.4.7.2.1.8.1.3.3.6.3.3.7.1.0.....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.=.1.3.2.8.4.7.2.1.8.1.7.5.1.9.5.9.6.1.....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.=.7.e.c.b.4.7.d.d.-.a.e.8.0.-.4.8.7.8.-.b.e.1.d.-.8.8.2.c.e.3.d.c.4.0.a.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.=.a.b.5.a.b.5.5.e.-.1.4.e.3.-.4.a.1.b.-.b.1.5.8.-.5.0.b.e.7.6.3.b.3.d.b.5.....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.b.b.8.-.0.0.0.1.-.0.0.1.c.-.b.b.e.2.-.2.b.4.a.d.7.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\WERCB8F.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Dec 23 08:30:14 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 45580 |
| Entropy (8bit): | 2.103974861176703 |
| Encrypted: | false |
| SSDEEP: | 192:ZtvaEcwN2uMO5Skbn8frsgr484B3EQp8c7WVIGxeM3hn:GLm5Lb84grYB3JZ7kIGxr |
| MD5: | 86337529B331211FA9589CDC55E5144F |
| SHA1: | 5F3ECD037714191ECCE4DF483AF8129DC6002F34 |
| SHA-256: | E2032069DF2BB60D00B0B84785CEC36B30A2904CA116F65E2D3281D8F7898A82 |
| SHA-512: | 95C9B5C443ACB86FD8B5AF9D9746CC698E8AE7F8954FD123CBF77D024F69CE14C5B37B82F5DA6196322F07C9EE380D105DEBA66E2259220977F8BFC9125933EA |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP..... .....3.a.....-.....T.....8.....T.....D.....U.....B..... .....GenuineIntelW.....T.....3.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\WERD2C4.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): | 8330 |
| Entropy (8bit): | 3.6974259901928446 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNiVD67zdG6Ymy6WgmfTSSICpra89buDsf+sam:RrlsNiR6E6Yz6WgmfTSSTuof+Q |
| MD5: | 06462DE20DE7AA72DC680695BBD2CB81 |
| SHA1: | DDB6AC6FE7454F56E090863434958FD3B472F6AE |
| SHA-256: | 79EE07AD40F8F1017B1DB5EF1803E828C25222ED277CC81C7DB8FF9D1BD5F0A2 |
| SHA-512: | D4E76D9907F4F7EE9AFDF04687421C9634E1098FEC634337896E6674CF6641F25146EB20AE76B3C4081D22606A43004F5584D13DD031CD7E3003BE424ACA6B61 |
| 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.>.7.0.9.6.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERD526.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4702 |
| Entropy (8bit): | 4.506337630379623 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs/JgtWI9mCfWSC8BQ8fm8M4JCdsQhF6+q8/BB34SrSchd:uITfhtCOSNnJNyDW4d |
| MD5: | E6F405FE59C3769DA137D1AE9E5B8C90 |
| SHA1: | 5721BF06A543A4E6DDFD8E6391F0E2A61E9F40F9 |
| SHA-256: | 1338F4FC815713CCC9B4ADC83B4AE1B5F7EBF933C4C3B3F7D89B42414394306D |
| SHA-512: | 8B89FD9A2AA7B429C5E99A0963E504218BD2A3FE5C00C47F001AE42B14D1CA769BCF65CCE95595D0A104C035212B9D67CC3D5731078F724B1FDA6A20006A404 |
| Malicious: | false |
| Reputation: | low |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERD526.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="1310020" />.. <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): | 4.276661789486948 |
| Encrypted: | false |
| SSDEEP: | 12288:N9Lv0GkJt5pTFelNQ17kWdr/ljglw5HRUJZgkIvdISrsB9fi3/rbut:7Lv0GkJt5pTFel2p |
| MD5: | E1326BC98DB9BF21A19CE753070DA36F |
| SHA1: | EB8D3DE9A89246CED6874620F816EC1CCA9A1898 |
| SHA-256: | 47F436C3254B23C411FF6EFC690869AE77ABBEBF57F01C049003BC0A72CB7930 |
| SHA-512: | 1BBFE06CB6FF4915F71F8E6C70887C55B23432BF4AE9EEDFC13696317C6D8C2D03A292CB5411D7327D21984AE599DD771A6F83139D7C04DE28EC842475F2B2E |
| 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...M..... .....5..... |

| C:\Windows\appcompat\Programs\Amcache.hve.LOG1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | MS Windows registry file, NT/2000 or above |
| Category: | dropped |
| Size (bytes): | 24576 |
| Entropy (8bit): | 4.0338934242540665 |
| Encrypted: | false |
| SSDEEP: | 384:+Yvn5Rftx1xPJ4XCsFcnE7kuPBqXhSeq5QMVyi6+/el4Lk4vZd1DoXznYXvwvt:7v5Rftx1RJ4XXFcE7DBqXoeq5QMVyi6N |
| MD5: | 8F51F8B9540D9B4AAF4A5F8E4C1E84CD |
| SHA1: | A12AF53A973FE073265446B2862EFC7424A44718 |
| SHA-256: | FDCA0807886A2D19584BDC4A08757E6278302F5A3BBB58CD81614B776DD477CA |
| SHA-512: | 3889E00E9334AED3D8E72D4B368A0881D463FE41C34231E7C9758234C543CB424AC0101763AB5A6100E414DA45F9B1221CF895EFDDFC263A9C09AE5635DD653 |
| 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...M..... .....3..HvLE.^.....Y.....Y.0.).:I8<LN.I.....0..... ..hbin.....p.\..,.....nk,...M.....(..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...M..... ..... .....Z.....Root.....lf.....Root....nk ...M.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.220307012367601 |
| 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.ML.PE-A+Troj.Dridex-AJA.19171.dll |
| File size: | 565248 |
| MD5: | 5ca09f4e3e8adcf9755415f40a43e89b |
| SHA1: | 5c57296e6c7f36156fe2062db0719b67383548d9 |
| SHA256: | b9dac63c888f98e13799568be23d934cc5e929b1e71282b3eb5c83d3cbf21e7a |

## General

| | |
|---|---|
| SHA512: | df66970e65d0362ed083ce105b38db040befd78a3cad6fd<br>350ee4fa123e0afc94897a113878bc94047a5b86697682c<br>4a14e0a8122c4ab55bc0aff422c851f130 |
| SSDEEP: | 12288:qnYoMi8KFy86zc86boq67oy6zq86xoG6V2C6Fo<br>E69oI6Vo8mHo06zo8knoz5fU56:qiI0+2OJljTR |
| File Content Preview: | MZ.....@.....!..L.!Th<br>is program cannot be run in DOS mode....$.....R...<...<br><...<..k....<...=.S.<.=.....<.....<.....<.t.?...<.t.=.4.<.L.9...<<br>.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 | 0x6eac | 0x7000 | False | 0.381382533482 | data | 4.37837175078 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x7916e | 0x7a000 | False | 0.283385229892 | data | 7.33168916922 | 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: 6988 Parent PID: 2808

#### General

| | |
|---|---|
| Start time: | 00:30:05 |
| Start date: | 23/12/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll" |
| Imagebase: | 0xd90000 |
| 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: 00000002.00000002.684498846.000000006EBD1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | moderate |

#### File Activities

Show Windows behavior

### Analysis Process: cmd.exe PID: 7064 Parent PID: 6988

#### General

| | |
|---|---|
| Start time: | 00:30:06 |
| 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.ML.PE-A+Troj.Dridex-AJA.19171.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: 7096 Parent PID: 7064

### General

| | |
|---|---|
| Start time: | 00:30:06 |
| Start date: | 23/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.ML.PE-A+Troj.Dridex-AJA.19171.dll",#1 |
| Imagebase: | 0x80000 |
| 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: 00000005.00000002.319816001.000000006EBD1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000005.00000000.289027157.000000006EBD1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000005.00000000.293983549.000000006EBD1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: WerFault.exe PID: 6472 Parent PID: 7096

### General

| | |
|---|---|
| Start time: | 00:30:11 |
| Start date: | 23/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 7096 -s 672 |
| Imagebase: | 0x920000 |
| 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