
**ID:** 510694
**Sample Name:** SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll
**Cookbook:** default.jbs
**Time:** 05:14:26
**Date:** 28/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

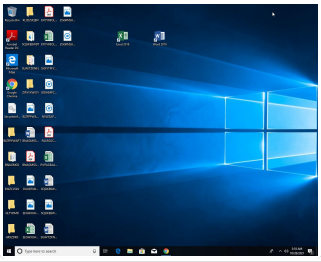
# Windows Analysis Report SecuriteInfo.com.Drixed-FJX…

## Overview

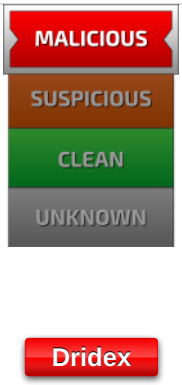
### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll |
| Analysis ID: | 510694 |
| MD5: | 345eadc8b1f5d0b. |
| SHA1: | a0a170c3bf53be5. |
| SHA256: | 31bcae869dbae8.. |
| Tags: | dll |
| Infos: | |

Most interesting Screenshot:



### Detection

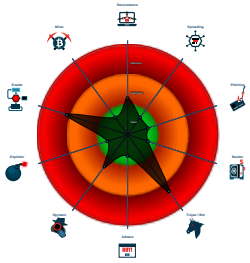



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Found detection on Joe Sandbox Clo…
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Tries to delay execution (extensive O…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- One or more processes crash
- Contains functionality to query locale…
- Uses code obfuscation techniques (…

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3104 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4784 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6408 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6416 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll,FFRgpmdlwwWde MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5884 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',CheckTrust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6256 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5532 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6256 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5060 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6256 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 3192 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4708 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3192 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 4800 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3192 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6488 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DownloadFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3340 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6488 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5356 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6488 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6552 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',GetICifFileFromFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6188 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6552 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 460 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6552 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

## Malware Configuration

### Threatname: Dridex

```
{
  "Version": 22201,
  "C2 list": [
    "149.202.179.100:443",
    "66.147.235.11:6891",
    "81.0.236.89:13786"
  ],
  "RC4 keys": [
    "9fRysqcdPgZffBlroqJaZHyCvLvD6BUV",
    "ranVAwtYINZG8jFJSjh5rR8jx3HIZIvSCern79nVFUhfeb2NvJlOKPsGO1osGE0VchV9bFDjym"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000E.00000000.666915392.000000006E9E1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000008.00000002.692811464.000000006E9E1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000009.00000000.630165009.000000006E9E1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000003.00000000.412312975.000000006E9E1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 00000000.00000000.686620423.000000006E9E1000.00000020.00020000.sdmp | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| Click to see the 11 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 10.0.rundll32.exe.6e9e0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 12.0.rundll32.exe.6e9e0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 14.0.rundll32.exe.6e9e0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 10.2.rundll32.exe.6e9e0000.2.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| 9.0.rundll32.exe.6e9e0000.5.unpack | JoeSecurity_Dridex_1 | Yara detected Dridex unpacked file | Joe Security | |
| Click to see the 11 entries | | | | |

# Sigma Overview

**No Sigma rule has matched**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

## Networking:

**C2 URLs / IPs found in malware configuration**

## E-Banking Fraud:

**Yara detected Dridex unpacked file**

## System Summary:

**Found detection on Joe Sandbox Cloud Basic with higher score**

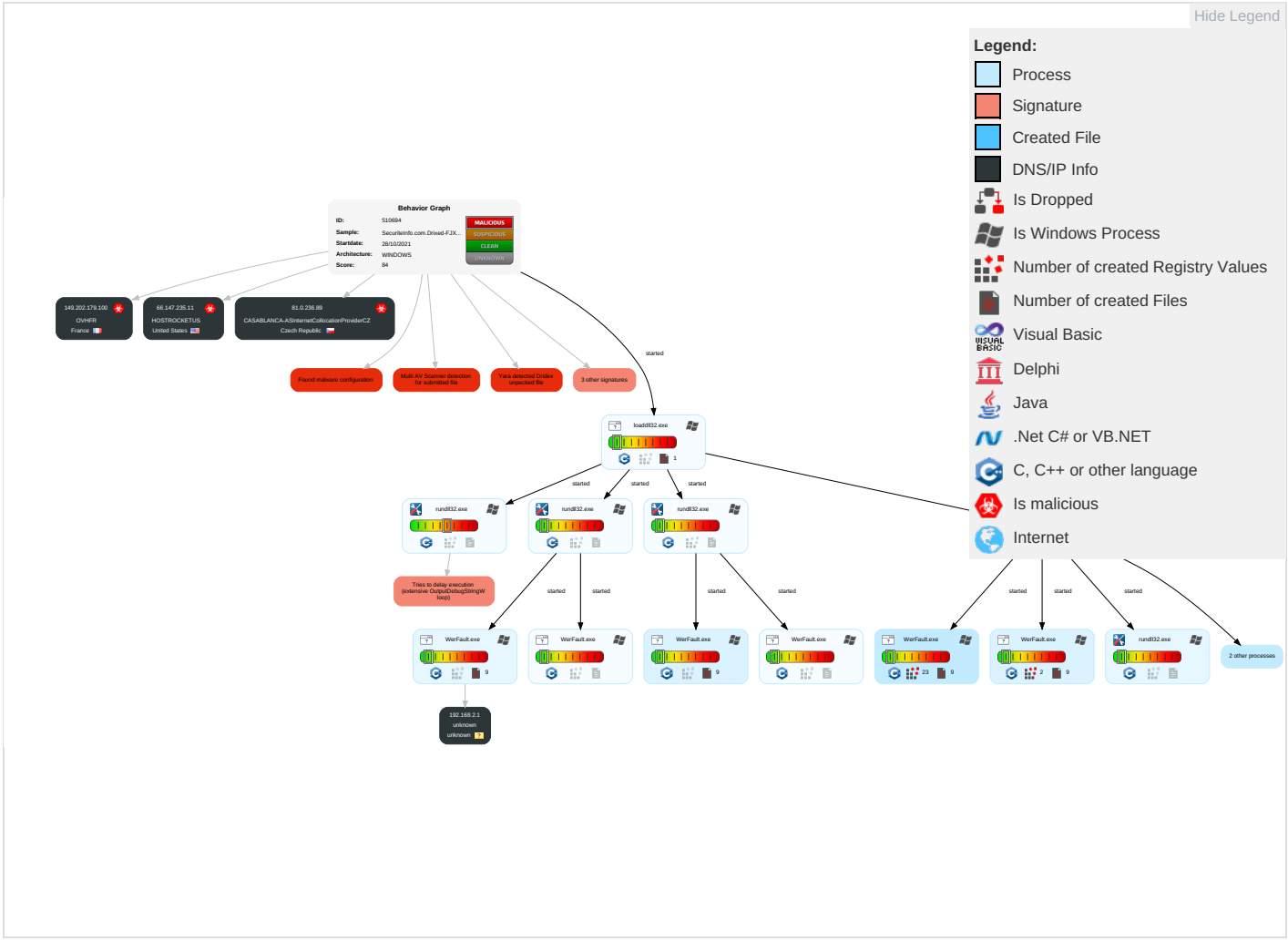
## Malware Analysis System Evasion:

**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 | Disable or Modify Tools 1 | Input Capture 1 | Security Software Discovery 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop or Insecure Network Communicati |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 1 | LSASS Memory | Process Discovery 1 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 t Redirect Pho Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 2 | Security Account Manager | Virtualization/Sandbox Evasion 1 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 t Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | Account Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Rundll32 1 | LSA Secrets | System Owner/User Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicati |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 1 | Cached Domain Credentials | Remote System 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 | System Information Discovery 1 3 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Point |

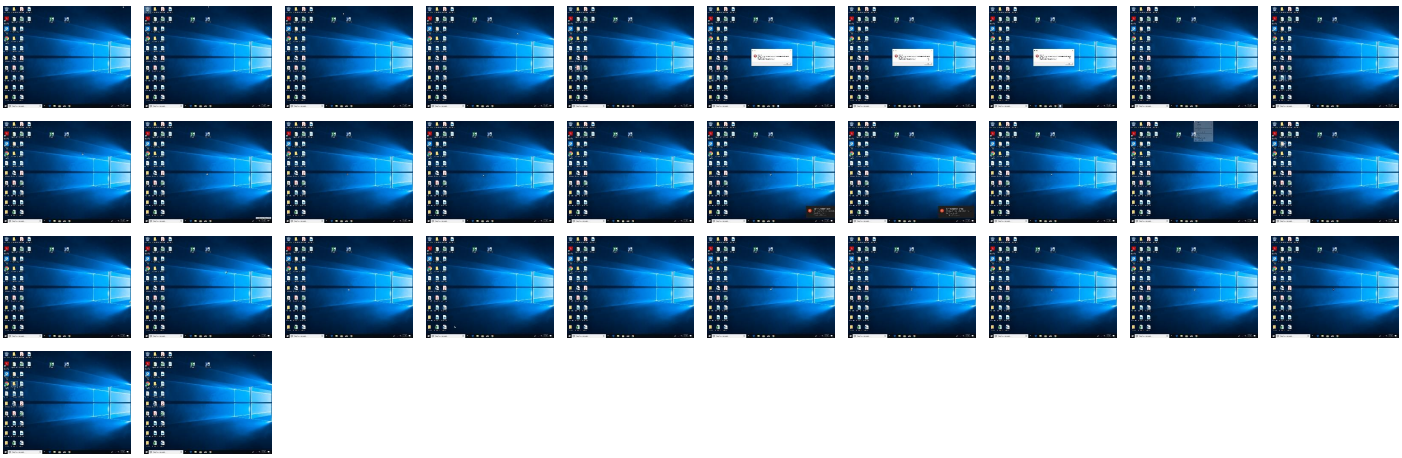
# Behavior Graph




## 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.Drixed-FJX345EADC8B1F5.514.dll | 22% | Virustotal | | Browse |
| SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | 27% | ReversingLabs | Win32.Trojan.Drixed | |
| SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 12.0.rundll32.exe.3220000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 14.0.rundll32.exe.3a0000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 9.2.rundll32.exe.3370000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 12.0.rundll32.exe.3220000.3.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 3.0.rundll32.exe.9c4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 12.0.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 9.0.rundll32.exe.3370000.3.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 8.2.rundll32.exe.6b0000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 9.0.rundll32.exe.6e9e0000.5.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 10.0.rundll32.exe.30d4756.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 12.2.rundll32.exe.4c64756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 9.0.rundll32.exe.4f34756.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 3.0.rundll32.exe.690000.3.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 3.0.rundll32.exe.690000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 14.0.rundll32.exe.3a0000.3.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 10.0.rundll32.exe.30d4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 10.0.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 4.2.rundll32.exe.920000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 14.0.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 12.2.rundll32.exe.3220000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 8.2.rundll32.exe.dd4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 3.0.rundll32.exe.9c4756.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 10.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 12.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 0.0.loaddll32.exe.2554756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 4.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 12.0.rundll32.exe.4c64756.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 10.2.rundll32.exe.30d4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 14.2.rundll32.exe.8e4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 14.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 14.0.rundll32.exe.8e4756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 3.0.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 10.2.rundll32.exe.b90000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 10.0.rundll32.exe.b90000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 4.2.rundll32.exe.b54756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 0.0.loaddll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 10.0.rundll32.exe.b90000.3.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 10.0.rundll32.exe.6e9e0000.5.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 8.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 14.2.rundll32.exe.3a0000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 9.0.rundll32.exe.4f34756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 9.2.rundll32.exe.4f34756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 9.0.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 14.0.rundll32.exe.6e9e0000.5.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 14.0.rundll32.exe.8e4756.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 9.0.rundll32.exe.3370000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 0.0.loaddll32.exe.3d0000.0.unpack | 100% | Avira | TR/ATRAPS.Gen2 | | Download File |
| 9.2.rundll32.exe.6e9e0000.2.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 12.0.rundll32.exe.6e9e0000.5.unpack | 100% | Avira | HEUR/AGEN.1144420 | | Download File |
| 12.0.rundll32.exe.4c64756.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |

### Domains

**No Antivirus matches**

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.vomfass.deDVarFileInfo$ | 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 |
|---|---|---|---|---|---|---|
| 66.147.235.11 | unknown | United States | | 23535 | HOSTROCKETUS | true |
| 149.202.179.100 | unknown | France | | 16276 | OVHFR | true |
| 81.0.236.89 | unknown | Czech Republic | | 15685 | CASABLANCA-ASInternetCollocationProviderCZ | true |

### Private

| IP |
|---|
| 192.168.2.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 510694 |
| Start date: | 28.10.2021 |
| Start time: | 05:14:26 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 0s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.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: | 30 |
| 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: | mal84.troj.evad.winDLL@33/17@0/4 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 99.5% (good quality ratio 91.8%)<br>• Quality average: 77%<br>• Quality standard deviation: 30.6% |
| HCA Information: | • Successful, ratio: 67%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| 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

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 66.147.235.11 | SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | Early_Access.-3878_20211027.xlsb | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | Casting Invite.-859403670_20211027.xlsb | Get hash | malicious | Browse | |
| 149.202.179.100 | SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | Early_Access.-3878_20211027.xlsb | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | Casting Invite.-859403670_20211027.xlsb | Get hash | malicious | Browse | |
| 81.0.236.89 | SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | |
| | Early_Access.-3878_20211027.xlsb | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | |
| | Casting Invite.-859403670_20211027.xlsb | Get hash | malicious | Browse | |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| HOSTROCKETUS | SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | • 66.147.235.11 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | Early_Access.-3878_20211027.xlsb | Get hash | malicious | Browse | • 66.147.235.11 |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | • 66.147.235.11 |
| | Casting Invite.-859403670_20211027.xlsb | Get hash | malicious | Browse | • 66.147.235.11 |
| | s1uOMLvpO4.exe | Get hash | malicious | Browse | • 216.120.23 6.127 |
| | WGs54P9e8a | Get hash | malicious | Browse | • 216.120.24 1.108 |
| | ba2Eq178BGXyW5T.exe | Get hash | malicious | Browse | • 216.120.237.68 |
| | 4TXvMuUjTxE2kqz.exe | Get hash | malicious | Browse | • 66.147.239.119 |
| | Requirements-oct_2020.exe | Get hash | malicious | Browse | • 66.147.239.119 |
| | JESEE FRIED FIRDAY.exe | Get hash | malicious | Browse | • 66.147.239.119 |
| OVHFR | SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | protocol-1096018033.xls | Get hash | malicious | Browse | • 192.99.46.215 |
| | protocol-1096018033.xls | Get hash | malicious | Browse | • 192.99.46.215 |
| | arm7 | Get hash | malicious | Browse | • 8.33.207.78 |
| | #U0191ACTU#U0156A_wfpqacDkwlb__Z2676679.vbs | Get hash | malicious | Browse | • 144.217.33.249 |
| | Byov62cXa1.exe | Get hash | malicious | Browse | • 94.23.24.82 |
| | Early_Access.-3878_20211027.xlsb | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | ckrgvIQvmUux.dll | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | Casting Invite.-859403670_20211027.xlsb | Get hash | malicious | Browse | • 149.202.17 9.100 |
| | lyVSOhLA7o.dll | Get hash | malicious | Browse | • 51.210.102.137 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2d53275b1be4ca5e6593e323a54ecdeda8efe761_82810a17_15a172f5\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): | 0.9140610265091967 |

**C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2d53275b1be4ca5e6593e323a54ecdeda8efe761_82810a17_15a172f5\Report.wer**

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 192:yyi80oX6HBUZMX4jed+z/u7sfS274ItWc:HiaXSBUZMX4je+/u7sfX4ItWc |
| MD5: | 578308542CFF74025D18BA29948DD74B |
| SHA1: | A84361FD63C6FD29AB2DAE72F7DBD20C8624DF14 |
| SHA-256: | D9D391B23E0675EB99EFFD0963522FC3704D1FC2DBAE1D74DD2F510AEFDB6637 |
| SHA-512: | AE57C7C80D5878FD0127BC47A35183E81DE26DE443132949EB0D68E945813D0130A4A0C72757270139DB582E75C4D64DC4D165C99C623160B23E964CD38574D |
| Malicious: | false |
| 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.=.1.3.2.7.9.8.9.7.0.7.4.4.5.5.9.0.2.4.....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.=.1.3.2.7.9.8.9.7.0.8.9.8.6.2.0.7.3.3.....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.=.6.f.3.4.f.0.0.0.-.9.2.b.1.-.4.c.7.7.-.b.4.f.a.-.9.a.a.3.e.8.c.a.2.0.a.3.....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.=.e.d.5.a.4.2.9.0.-.f.8.3.f.-.4.c.e.d.-.9.5.0.0.-.3.0.5.5.1.b.8.b.7.a.2.1.....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.=.0.0.0.0.1.8.7.0.-.0.0.0.1.-.0.0.1.c.-.5.e.e.f.-.5.5.9.d.f.5.c.b.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\ReportQueue\AppCrash_rundll32.exe_4eea1987c3498f452f209a432782d7d6bd992397_82810a17_1259968a\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): | 0.9164027719636145 |
| Encrypted: | false |
| SSDEEP: | 192:LSi40oX/HBUZMX4jed+z/u7sES274ItWc:2i+X/BUZMX4je+/u7sEX4ItWc |
| MD5: | 0CECBA5DE8275CBFC21886A6EA1712B2 |
| SHA1: | 3F021FD464047D4674988A545F270B7DF2EABA39 |
| SHA-256: | CED54CC38A6B5392AC7108A930B63CC0D077FD529AA284AD9BD95C520E0DB829 |
| SHA-512: | 17E0497AF58B70E5A8592116645A6484EF8BA8502D07FF5D9132652639BFA6A495B1D5E377B4A19F3358BE48EC381A851A160D0115448C474E55A78379B516EA |
| Malicious: | false |
| 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.=.1.3.2.7.9.8.9.7.0.8.6.5.7.3.9.5.6.2.....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.=.1.3.2.7.9.8.9.7.0.9.9.7.7.7.0.1.9.5.....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.d.a.2.3.4.7.a.-.f.d.d.5.-.4.a.4.a.-.b.d.3.c.-.6.6.c.9.e.e.4.8.c.b.d.7.....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.=.4.0.b.1.f.1.5.c.-.3.a.b.e.-.4.4.e.6.-.8.7.7.2.-.1.f.e.5.9.7.1.c.6.5.5.0.....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.c.7.8.-.0.0.0.1.-.0.0.1.c.-.c.6.f.b.-.8.4.9.d.f.5.c.b.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\ReportQueue\AppCrash_rundll32.exe_86cc7caaf91494aa6af1cec8da5ba37782e9_82810a17_1811a30d\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): | 0.9163549584990345 |
| Encrypted: | false |
| SSDEEP: | 192:o9liE0oXhHBUZMX4jed+z/u7sES274ItWc:giyXxBUZMX4je+/u7sEX4ItWc |
| MD5: | 92FF5D41081D17BEBC3CFD94F9416872 |
| SHA1: | 09CEF1AAB65B50DDD539F6D9C3E8EC28F1495458 |
| SHA-256: | 435D2B7674BB1372AB5FD3621728D4A8AA926F9C827B25B610BFFDAA6939D238 |
| SHA-512: | 21104F8F6C44379ED191542B389B7C061192AB299787B4D4A7DAE2AB54961D7C93B4060C00E7D1A092BE4D21A6A6981B3E3556BB9F4C74FE9CDA8340657FD6F |
| Malicious: | false |
| 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.=.1.3.2.7.9.8.9.7.0.8.8.8.3.7.7.1.0.8.....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.=.1.3.2.7.9.8.9.7.1.0.0.4.7.8.3.0.3.4.....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.=.8.e.f.c.6.c.9.d.-.a.0.0.1.-.4.3.c.6.-.a.7.6.c.-.c.4.0.2.f.0.6.3.f.e.8.2.....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.=.e.2.e.2.1.b.b.1.-.c.6.f.a.-.4.d.f.f.-.8.8.a.f.-.5.9.2.c.3.a.9.1.3.e.d.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.=.0.0.0.0.1.9.9.8.-.0.0.0.1.-.0.0.1.c.-.7.b.7.c.-.f.c.9.d.f.5.c.b.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\ReportQueue\AppCrash_rundll32.exe_e9d070cbac24d3d3fafff9232a9e7f59cde72c2_82810a17_0d31a2af\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): | 0.9168934363039568 |
| Encrypted: | false |
| SSDEEP: | 192:Z+MiW0oXwHBUZMX4jed+z/u7sES274ItWc:piQXYBUZMX4je+/u7sEX4ItWc |
| MD5: | C853E9F6E9151D536844FA09C6F06ED7 |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_e9d070cbac24d3d3fafff9232a9e7f59cde72c2_82810a17_0d31a2af\Report.wer | |
|---|---|
| SHA1: | B9FF0441C6BD6695BB35B9E0CE1E43DB314E0D62 |
| SHA-256: | 530E6EBC0BE0BD69F58C04D0705BAD872C0E6CB6935A20173A9AE5E33D6A2BAB |
| SHA-512: | 9BA4BD93BC5BCD2C8025DB375E8D82347119B04CE297BAB4B80C6BE1CBC13313D204ECE66092D51879F73788C8D294FEE55709EFA87643341040A45C0A66C4E5 |
| Malicious: | false |
| 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.=.1.3.2.7.9.8.9.7.0.8.7.1.8.5.3.1.3.0.....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.=.1.3.2.7.9.8.9.7.0.9.9.9.9.7.7.5.5.5.....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.=.5.5.2.2.e.3.f.3.-.9.4.0.2.-.4.5.5.0.-.b.6.5.a.-.f.9.1.7.f.8.5.6.3.6.b.c.....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.=.c.2.c.b.8.3.4.8.-.0.2.6.9.-.4.d.d.d.-.8.c.7.7.-.f.1.9.1.f.5.9.f.1.e.2.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.=.0.0.0.0.1.9.5.8.-.0.0.0.1.-.0.0.1.c.-.1.3.d.4.-.c.3.9.d.f.5.c.b.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\WER2988.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Oct 28 12:17:57 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 38304 |
| Entropy (8bit): | 2.33186675708019 |
| Encrypted: | false |
| SSDEEP: | 192:x/HDw8vZjmHq3xByO5SkbPd6iZ/jzWyDvJGSTakU+W/3:hhHN5LbH1jz9DvJlak8 |
| MD5: | 0C6446CD7314BCE39CAFF7E07F705974 |
| SHA1: | 42B562C283A3DCBCCDD51D4189E8E943E96E7BF1 |
| SHA-256: | 7651F87690CA9C55340A89C07D523A7C4D1BE8ECF29D59D79241DC6B98B3B3AF |
| SHA-512: | 4D258F905B263FDE57BC4E6E0465694DF91615C52E31B11D0F945BFC96561055CE54838A5DE61163964F988888AF4A6ECB084E38007B23FFFE66CA1B9AE994FE |
| Malicious: | false |
| Preview: | MDMP..... .....za.....d.....l.....*.....T.....8.....T.....z.....U.....B.....GenuineIntelW.....T.....p.....za.....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\WER3A52.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): | 8350 |
| Entropy (8bit): | 3.6970070970643776 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNiqe6F6YYrk6ppgmfTDSZXECprB89b248sfZ0Om:RrlsNib6F6YH6ppgmfTDS8xPfI |
| MD5: | 7B3D672F40F4C181D8E4B900C5FA5EB9 |
| SHA1: | 1947A8561DE745A0D9715971C39598E5D4A4331A |
| SHA-256: | DA9A98555A99704089482C6BE68BFBC9420103235E63802ADFC608F9CB21378C |
| SHA-512: | 7F6832C6028B00832E7D730D241CF4B548A8CFBFC884ED8B3FB8CAD6F4A22C5EE1E4991CEC1FE19462E7667965005892E47D901482864C47A1D1AE93C5AC566 |
| Malicious: | false |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.5.6.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F06.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): | 4.502235591625177 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs7+JgtWI9SkrWSC8B+8fm8M4JCdsmIFMq0k+q8/1DJ4SrSSd:uITf701FSNZJ01MEVDWSd |
| MD5: | BA65FDD0C2C517B931D1E47ECAFBFAE8 |
| SHA1: | 947CDC89286B8C5C86D3BD974E0E20CCDA818944 |
| SHA-256: | 7484C0BA66E226962F8F351B547980000396151BD5E0DA8AE4CF2E07690CE35D |
| SHA-512: | F247CDA921C4EF94D8321F3A1925044D0F7C6427E4D8D02585A951C22180A6B9B63085F6F6A555536B9896E3EEA4460FEBA16DA99F78712C2A26849AF4B57CB3 |
| Malicious: | false |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER3F06.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="1229608" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER5897.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Oct 28 12:18:11 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 45744 |
| Entropy (8bit): | 2.0758438400580133 |
| Encrypted: | false |
| SSDEEP: | 96:5h8QB88/qjKsApTqbVXG/oi75SkNnus95gEPWlAhgFedON5P1URlRgWlnWIXd8lY:cQN+zApqzO5SkbPdONB1UBpfHc4uh |
| MD5: | CA0A2D2967E6849F08BED8BC52938CEA |
| SHA1: | 83E08A274FCF2F940A966BF01DEE2B41A0824F20 |
| SHA-256: | 84FB5C381DD37BC2BBD6DC4031EBC7F10A8CAEF98A5027757BE85D14E167932E |
| SHA-512: | 5503A49CE3B65D0DE864693B1D7685C3974A0A284EE2A6C0EA267D887B420BDF4146E57CA7CF34A113B1BE88F4EF0F00D9B44344B965EA4EB3D0C55037D50B4F |
| Malicious: | false |
| Preview: | MDMP..... .....za.....*-.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....x.....za.....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\WER5AF8.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Oct 28 12:18:12 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 44984 |
| Entropy (8bit): | 2.132776344933645 |
| Encrypted: | false |
| SSDEEP: | 192:DQvtDzApZoy6O5SkbPJOJ804IMTKdV1hbC3Kg6H9ujtkMks:kVFyF5Lb6hTMTKph23P6H98j/ |
| MD5: | 284EF73EC946D91A1D66B5A66E7E2597 |
| SHA1: | 6DBBB2155A4E195D1CACEC127F951DF8653BF6E0 |
| SHA-256: | 37C437EB8E448CE989F938C604B50CA6BA1DB628D5F74135A9BF410A273AA82E |
| SHA-512: | EC4DA4BFB8A6E3ECA6155C047526992C822FA64DD876911664C19E970506963AF9F34B9670B42F0284D5019A14743002931CE7B21104676EB60AF4B0236AA0E0 |
| Malicious: | false |
| Preview: | MDMP..... .....za.....*-.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....X.....za.....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\WER6170.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Thu Oct 28 12:18:14 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 38504 |
| Entropy (8bit): | 2.2768482036605207 |
| Encrypted: | false |
| SSDEEP: | 192:t9k58vZjmHq3sB7SdO5SkbPd7lYqHiH+tmk0SnJA6lu8NQ8TZ7ugP:kOhHgb5LbF7IYqCNkHbA8NHug |
| MD5: | 42B6B2C1003C52A64C49BBC9899A0389 |
| SHA1: | 07EE4EEDC32042C1A2B65A213BFF0C775F87DBF4 |
| SHA-256: | 872CBDA9AA966397C8EF26A62E9FE50E90D7DBEAA3F2049F4C7783F857B45E48 |
| SHA-512: | 3CB1B057C553274CC0AFC243B080CB952898589B6839A6F776D8879C5E5E51051D8DED7A3262228100B574FFBFD2EBCCC5C4D4C4716C5F5A86F23CA522CC30 |
| Malicious: | false |
| Preview: | MDMP..... .....za.....d.....l.....*.....T.....8.....T.....P{.....U.....B.....GenuineIntelW.....T.....za.....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\WER6DB6.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DB6.tmp.WERInternalMetadata.xml | |
|---|---|
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8352 |
| Entropy (8bit): | 3.6962577194915953 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNiMh66X6YYrY6ppgmfTOSZXECprRH89b2wtsfo02m:RrlsNi666X6Y76ppgmfTOSrYpmfh |
| MD5: | 09585E8AC18CA1B0033EB262AE925DB4 |
| SHA1: | 0D9CAE7B9D173E5A43F988595B30E74C2F269522 |
| SHA-256: | 28A7B5BA3336E9D5132C0F7EF1244964706E503A20BD5D0A1C954542DE910360 |
| SHA-512: | 89344D2741159AD49F08A09DEB936B812E8CCC7CCEC6CFF410C673A5E63DCA995DBA5DDD9A76A0B1213A09D7B440025A1930F914559EEAB5C38671A8A46A834 |
| Malicious: | false |
| 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.>.3.1.9.2.</.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER7131.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): | 4.5046486653392535 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs7+JgtWI9SkrWSC8B98fm8M4JCdsmpFYv+q8/1DO4SrSVd:uITf701FSNMJ00vECDWVd |
| MD5: | DA7904AF1ABA14728E1D939F23AF1AF9 |
| SHA1: | 50CCE2696E5CA67733E022D9D55BEE72F474BD1C |
| SHA-256: | 1F13D44F837F94CE8B71AC1C059EC4EC944B5B6D64C7A8CCB60DA8F13E4559AF |
| SHA-512: | 00DB8286A3F47F2256FCB0996995998355E793149535D5B95048DC782330306813489F729AE11E34152C4C846D0D5C9CDFF6A671A0D6DBEE757E0E9308540C25 |
| Malicious: | false |
| 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="1229608" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER768F.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): | 8352 |
| Entropy (8bit): | 3.698285676014007 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNivQ6n6YYre6ppgmfTtSZXECprRt89b2Pksfz0fm:RrlsNio6n6YN6ppgmfTtSrK2XfX |
| MD5: | DC7F527257F91360B545730F06FAABCD |
| SHA1: | 70A3604AAC6ABF2C968C7D6579D303B4C7C92599 |
| SHA-256: | F396415ED5717A6005EC6853B6D48554EF93C3102BDBF76D3F1B71C21691A43F |
| SHA-512: | 7D672486651D6F1E91E34A2D43616DC5BDBD1BEDA7A40A739578F88CF3AF8E40B0D96D8CC178971F512A2E82A74A5540F64D74039A24F30F0FA8732FE5D3796( |
| Malicious: | false |
| 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.>.6.4.8.8.</.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D28.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): | 4.505966922915317 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs7+JgtWI9SkrWSC8B58fm8M4JCdsmYFus4+q8/1DSu4SrSy6d:uITf701FSNcJ0s4EWuDWy6d |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D28.tmp.xml | |
|---|---|
| MD5: | 907F392A9030B8289FE729AAE7A3CE6B |
| SHA1: | BB8D390E1D325114C2FEB4578A0615168FF90EAB |
| SHA-256: | A4D890A2AFC57D53CC57E8E0E89014B1FC8A37A3E3B1F4065BA92A05EC842205 |
| SHA-512: | 2F73B2B2A471EA7D9C0EDD3E6A26FC95E2335C6E17B97B7A558FBF9EF1125C7A4BDE72C35140D68B6D3A2F1B8AE27A4B82D40E52CC04E6C34FB3376A8179DE<br>12 |
| Malicious: | false |
| 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="1229608" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER7D94.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): | 8352 |
| Entropy (8bit): | 3.695325784298672 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNix06T76YYrz6ppgmfT5SZXECprz89b2U8sft0Cm:RrlsNiC6P6Yw6ppgmfT5SWNPfI |
| MD5: | 012C49EB65729BE5D6DABA5A8179BFDC |
| SHA1: | 371270CCC6F15E68668A31D1DB2A6A8F8414B8A5 |
| SHA-256: | 9888583FB03961D1B1306D844728D035899C7B0AEF6CE125E4CAD727E8EDD8C8 |
| SHA-512: | 341A5F5E7C5B6008C8C78F8B76161997BD6F09574693A1E45C29BFAB8804F19D868FCF92748796D583083148445393C315FCC9894DFB424815259FD78EDF2F14 |
| Malicious: | false |
| 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.>.6.5.5.2.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER81DB.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): | 4.502353144285801 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs7+JgtWI9SkrWSC8Bv8fm8M4JCdsmcFk+q8/1DZJ4SrSRd:uITf701FSNWJ05EPDWRd |
| MD5: | 43FEBBFD677E2C67D87CDD3A92A3E8FA |
| SHA1: | 42CC666DBF0EB7A36CD884D5999491D6C3C449D8 |
| SHA-256: | D00A459F2A8228DB9D57CA7EFEFBE9740224EA7A94D577176557BDEB6BE8417F |
| SHA-512: | 3488AB796C0C9EF6ACFEBFC1F63242499205063F358FA0E408B4BEB724199899FF8DE1FA0DCAC1424B52A51994061F886686F403E2AB8E23D7D36DE91290DD6( |
| Malicious: | false |
| 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="1229608" />.. <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:\Users\user\AppData\Local\Temp\WERDE3.tmp.WERDataCollectionStatus.txt | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF, CR line terminators |
| Category: | dropped |
| Size (bytes): | 4878 |
| Entropy (8bit): | 3.2564303290467054 |
| Encrypted: | false |
| SSDEEP: | 96:pwpwi+kXkkX4kj0uWn0Q50Qu0Qga0QXm0QIO0QjiFg+XQYszeuzSzbxGQI5UhmNc:pTlZZuqEGWoeyOkNKgtlJ |
| MD5: | 39F254F5A4E96785B1604BB50699C1F8 |
| SHA1: | D973C28A1868F1930451DCC95BC7469098BDAAD2 |
| SHA-256: | 8F10F8E17D8EB791E53D5812533CB1BFE6C359BF02320CF465A685ACCFE9F256 |
| SHA-512: | CEABA9EF8E7489025B76BC064752AAA5C26801F7CC29066F4067485746508B6DE935F443FC9A542124E8ACDA483E716670E989D087D53D620B6FC97988D97B41 |
| Malicious: | false |

| C:\Users\user\AppData\Local\Temp\WERDE3.tmp.WERDataCollectionStatus.txt | |
|---|---|
| Preview: | .....S.n.a.p.s.h.o.t. .s.t.a.t.i.s.t.i.c.s.:.....-. .S.i.g.n.a.t.u.r.e. . . . . .:. .P.S.S.D.....-. .F.l.a.g.s./.C.a.p.t.u.r.e.F.l.a.g.s. . . . . .:. .0.0.0.0.0.0.0.9./.d.0.0.0.3.9.f.f.....-. .A.u.x. .p.a.g.e.s. . . . . .:. .1. .e.n.t.r.i.e.s. .l.o.n.g.....-. .V.A. .s.p.a.c.e. .s.t.r.e.a.m. . . . . .:. .4.3.6.5.6. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .H.a.n.d.l.e. .t.r.a.c.e. .s.t.r.e.a.m. . . . . .:. .0. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .H.a.n.d.l.e. .s.t.r.e.a.m. . . . . .:. .1.0.9.7.2. .b.y.t.e.s. .i.n. .s.i.z.e.....-. .T.h.r.e.a.d.s. . . . . .:. .2. .t.h.r.e.a.d.s.....-. .T.h.r.e.a.d. .s.t.r.e.a.m. . . . . .:. .1.6.6.4. .b.y.t.e.s. .i.n. .s.i.z.e.....S.n.a.p.s.h.o.t. .p.e.r.f.o.r.m.a.n.c.e. .c.o.u.n.t.e.r.s.:.....-. .T.o.t.a.l.C.y.c. l.e.C.o.u.n.t. . . . . .:. .1.2.1.5.5.0.7.5.2. .c.y.c.l.e.s.....-. .V.a.C.l.o.n.e.C.y.c.l.e.C.o.u.n.t. . . . |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.160650328982938 |
| 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.Drixed-FJX345EADC8B1F5.514.dll |
| File size: | 1093632 |
| MD5: | 345eadc8b1f5d0b373b531902c06572e |
| SHA1: | a0a170c3bf53be55a625c7793bfe23edd4038f05 |
| SHA256: | 31bcae869dbae8bfd20fc177bf4158e75fc7fdf00c694ae13f23dff6229f8e8e |
| SHA512: | 88573788ffb297007445449b45075e70e10f92a787954163ce74e4aa099d984530929f27f5c1c23e27e595e096831d10dcaf07ee39aaad6803f839047f8096c6 |
| SSDEEP: | 24576:ojsXggYiykQsMy2GSuCAaimSQws2yyq+YoWEUK6ES0wOyeSGwswWquEQq2GiMciB:d |
| File Content Preview: | MZ.....@.....IZ..(4..(4..(4..z..&)4.....Z)4..Q...)4..u5..(4.....K(4..v6."(4.7....(4. ...,(4....i(4.....Z(4..(5.f)4.Rich.(4.....PE..L...&.ya.....!.... `...P.....K.....p..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x10004b90 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x10000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x61798526 [Wed Oct 27 16:58:14 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: | ae858e1bcf44b240b65263bbd6945db2 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x5dfe | 0x6000 | False | 0.384562174479 | data | 4.44056461685 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7000 | 0xf4032 | 0xf5000 | False | 0.135153260523 | data | 7.11996208116 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xfc000 | 0xbd1c | 0xb000 | False | 0.234153053977 | data | 5.69509557044 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x108000 | 0x3e8 | 0x1000 | False | 0.119873046875 | data | 1.03136554304 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x109000 | 0x2e14 | 0x3000 | False | 0.231608072917 | data | 5.67874721692 | IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Exports

### Version Infos

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: loaddll32.exe PID: 3104 Parent PID: 3120

### General

| | |
|---|---|
| Start time: | 05:15:24 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll' |
| Imagebase: | 0xe40000 |
| File size: | 893440 bytes |
| MD5 hash: | 72FCD8FB0ADC38ED9050569AD673650E |
| 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: 00000000.00000000.686620423.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | moderate |

**File Activities** Show Windows behavior

## Analysis Process: cmd.exe PID: 4784 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:15:24 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.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: 6416 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:15:24 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll,FFRgpmdlwwWde |
| Imagebase: | 0xfe0000 |
| 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: 00000003.00000000.412312975.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: rundll32.exe PID: 6408 Parent PID: 4784

### General

| | |
|---|---|
| Start time: | 05:15:24 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',#1 |
| Imagebase: | 0xfe0000 |
| 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: 00000004.00000002.692542013.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: rundll32.exe PID: 5884 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:16:19 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',CheckTrust |
| Imagebase: | 0xfe0000 |
| 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: 00000008.00000002.692811464.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: rundll32.exe PID: 6256 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:16:19 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllCanUnloadNow |
| Imagebase: | 0xfe0000 |
| 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: 00000009.00000000.630165009.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000009.00000000.610084790.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000009.00000002.659636393.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 3192 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:16:20 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllGetClassObject |
| Imagebase: | 0xfe0000 |
| 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: 0000000A.00000000.620992103.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.682477446.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000000.653774914.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6488 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:16:20 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DownloadFile |
| Imagebase: | 0xfe0000 |
| 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: 0000000C.00000000.642318739.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000002.687730478.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000000.653718345.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6552 Parent PID: 3104

### General

| | |
|---|---|
| Start time: | 05:16:20 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',GetICifFileFromFile |
| Imagebase: | 0xfe0000 |
| 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: 0000000E.00000000.666915392.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000E.00000000.654050879.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000E.00000002.683460659.000000006E9E1000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: WerFault.exe PID: 5532 Parent PID: 6256

### General

| | |
|---|---|
| Start time: | 05:17:50 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6256 -s 652 |
| Imagebase: | 0xdf0000 |
| 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

## Analysis Process: WerFault.exe PID: 4708 Parent PID: 3192

### General

| | |
|---|---|
| Start time: | 05:18:00 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 3192 -s 652 |
| Imagebase: | 0xdf0000 |
| 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 Modified**

## Analysis Process: WerFault.exe PID: 3340 Parent PID: 6488

### General

| | |
|---|---|
| Start time: | 05:18:01 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6488 -s 652 |
| Imagebase: | 0xdf0000 |
| 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 Modified**

## Analysis Process: WerFault.exe PID: 6188 Parent PID: 6552

### General

| | |
|---|---|
| Start time: | 05:18:06 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6552 -s 652 |
| Imagebase: | 0xdf0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Modified

## Analysis Process: WerFault.exe PID: 5060 Parent PID: 6256

### General

| | |
|---|---|
| Start time: | 05:18:07 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6256 -s 652 |
| Imagebase: | 0xdf0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: WerFault.exe PID: 4800 Parent PID: 3192

### General

| | |
|---|---|
| Start time: | 05:18:14 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 3192 -s 652 |
| Imagebase: | 0xdf0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: WerFault.exe PID: 5356 Parent PID: 6488

### General

| | |
|---|---|
| Start time: | 05:18:14 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6488 -s 652 |
| Imagebase: | 0xdf0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: WerFault.exe PID: 460 Parent PID: 6552

### General

| | |
|---|---|
| Start time: | 05:18:20 |
| Start date: | 28/10/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6552 -s 652 |
| Imagebase: | 0xdf0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis