ID: 510694
Sample Name: SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.20994
Cookbook: default.jbs
Time: 05:03:00
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

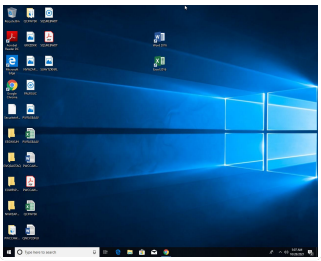
Windows Analysis Report SecuriteInfo.com.Drixed-FJX…

Overview

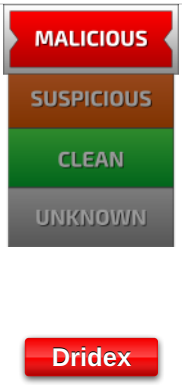
General Information

Sample Name:	SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.20994 (renamed file extension from 20994 to dll)
Analysis ID:	510694
MD5:	345eadc8b1f5d0b.
SHA1:	a0a170c3bf53be5.
SHA256:	31bcae869dbae8..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

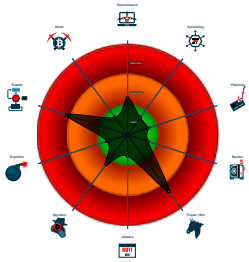


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Tries to delay execution (extensive O…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Uses 32bit PE files
- Found a high number of Window / Us…
- AV process strings found (often use…
- 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 (…
- Internet Provider seen in connection…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2152 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2104 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1820 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2184 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll,FFRgpmdlwwWde MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4888 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',CheckTrust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 480 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2068 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 480 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5644 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 480 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5836 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4608 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5756 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6040 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',DownloadFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5540 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 1692 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5012 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll',GetICifFileFromFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1340 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5012 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 2856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5012 -s 664 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
00000011.00000002.656454233.000000006E6A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000012.00000000.616956626.000000006E6A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000E.00000002.782709199.000000006E6A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000010.00000000.620998702.000000006E6A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000F.00000000.589866381.000000006E6A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.0.rundll32.exe.6e6a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
17.2.rundll32.exe.6e6a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
17.0.rundll32.exe.6e6a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
18.2.rundll32.exe.6e6a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
16.0.rundll32.exe.6e6a0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 10 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

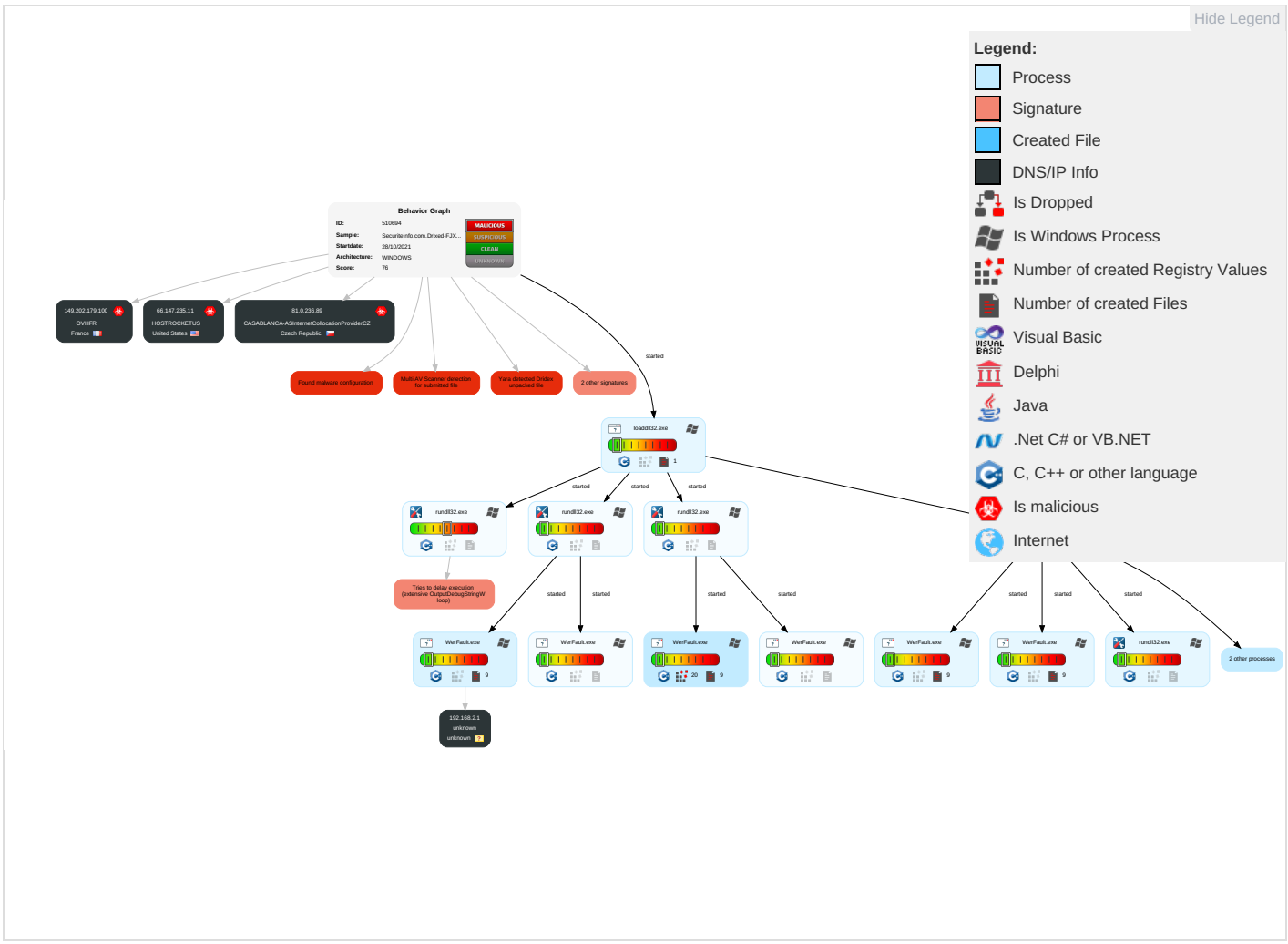
Malware Analysis System Evasion:

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	OS Credential Dumping	Security Software Discovery 2 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	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Process Discovery 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)	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 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 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	Rundll32 1	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	Software Packing 1	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

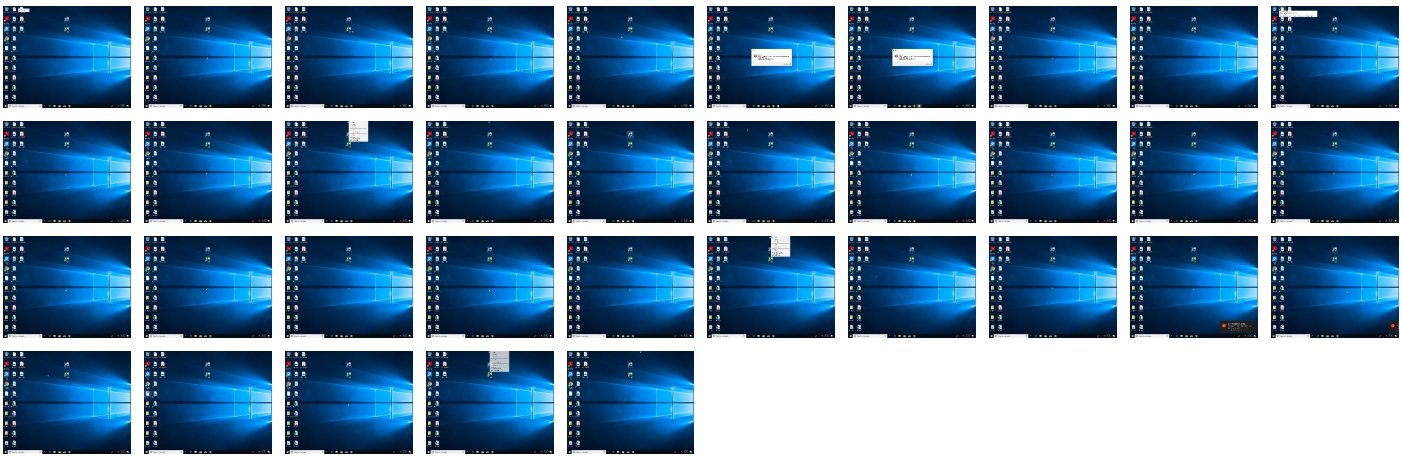
Behavior Graph



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.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
18.0.rundll32.exe.e14756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.rundll32.exe.e14756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.rundll32.exe.d00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
16.0.rundll32.exe.2ed0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
2.0.rundll32.exe.32c4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.32c4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
15.2.rundll32.exe.924756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
16.0.rundll32.exe.6e6a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
15.0.rundll32.exe.6e6a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
15.0.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.0.loaddll32.exe.aa0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.b74756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
18.0.rundll32.exe.6e6a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
15.0.rundll32.exe.7e0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.0.rundll32.exe.6d0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
16.0.rundll32.exe.4be4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.rundll32.exe.d00000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
2.0.rundll32.exe.2f70000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
2.0.rundll32.exe.2f70000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.1c0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.0.rundll32.exe.6e6a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
17.2.rundll32.exe.6d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
14.2.rundll32.exe.46f4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.2.rundll32.exe.4be4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.rundll32.exe.a74756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.rundll32.exe.2ed0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
15.0.rundll32.exe.924756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
18.2.rundll32.exe.e14756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.rundll32.exe.a40000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
18.2.rundll32.exe.d00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.0.loaddll32.exe.da4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.2.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
16.0.rundll32.exe.4be4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.rundll32.exe.6d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
16.0.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
15.0.rundll32.exe.7e0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.2.rundll32.exe.a74756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.2.rundll32.exe.7e0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.0.rundll32.exe.a74756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.6e6a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
16.2.rundll32.exe.2ed0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
15.0.rundll32.exe.924756.1.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:	05:03:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.20994 (renamed file extension from 20994 to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winDLL@33/18@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.7% (good quality ratio 52.7%) • Quality average: 76.4% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:05:18	API Interceptor	1x Sleep call for process: loaddll32.exe modified
05:06:54	API Interceptor	4x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.147.235.11	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-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-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-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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WGs54P9e8a	Get hash	malicious	Browse	• 216.120.241.108
	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
	Scan_0884218630071 Bank Swift.exe	Get hash	malicious	Browse	• 66.147.239.119
	BANK ACCOUNT DETAILS ATTACHED.pdf.exe	Get hash	malicious	Browse	• 66.147.239.119
OVHFR	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.179.100
	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	• 149.202.179.100
	ckrgvIQvmUux.dll	Get hash	malicious	Browse	• 149.202.179.100
	ckrgvIQvmUux.dll	Get hash	malicious	Browse	• 149.202.179.100
	Casting Invite.-859403670_20211027.xlsb	Get hash	malicious	Browse	• 149.202.179.100
	lyVSOhLA7o.dll	Get hash	malicious	Browse	• 51.210.102.137
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2d53275b1be4ca5e6593e323a54ecdeda8efe761_82810a17_08414ede\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):	0.9168707460564561
Encrypted:	false
SSDEEP:	192:jWHir0oXJHBUZMX4jed+W/u7sVS274ItWc:Si1X5BUZMX4je7/u7sVX4ItWc
MD5:	A6DA4BED5F8CE2330F7B159E656E0E7F
SHA1:	398876C9365ACC4B9C85337593C1F32F8AD7FFED
SHA-256:	5D219DB98224294451C144ECEE172E42D235C0F1AA3E441673648C8091ADE80C
SHA-512:	8C694A67121672D5E2C89A0A0EAAB8EC3C0FCF5A356401B09B3D884812A062EE9274B644AB3EC7EFBD20CE120C915187D3D10E7C3C2FD9F525AE736F15D4FE6
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2d53275b1be4ca5e6593e323a54ecdeda8efe761_82810a17_08414ede\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.=.1.3.2.7.9.8.9.6.4.0.0.8.8.6.9.3.8.4.....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.=.1.3.2.7.9.8.9.6.4.1.1.1.9.9.3.8.0.7.....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.=.8.5.d.6.a.e.4.a.-.3.b.d.5.-.4.0.1.5.-.9.6.5.8.-.6.d.8.3.4.b.2.0.3.f.4.2.....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.=.0.9.8.2.9.7.3.2.-.d.c.5.9.-.4.d.1.0.-.9.d.3.2.-.c.1.7.c.f.3.2.6.9.a.f.3.....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.=.0.0.0.0.0.1.e.0.-.0.0.0.1.-.0.0.1.7.-.3.4.8.9.-.9.1.1.1.f.4.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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_1254e5b4\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):	0.9167996513697367
Encrypted:	false
SSDEEP:	192:8JQ4Ki60oXNHBUZMX4jed+W/u7sAS274ItWc:NzisXdBUZMX4je7/u7sAX4ItWc
MD5:	986D6E8C397DA1BF6B12360C9C30BC6E
SHA1:	9E79BF5AEAD3F5DC92195FB87A3B9242A6302612
SHA-256:	6750A142CE274499987CEC5152D87C8F71AD368A993C33AC49E3FA4B00999C5A
SHA-512:	803B0FE4A6D99B9177EC13D57E59648C46E1C3B41E7AB12524B59DB73C0EE944BDFE1C5AA9FEAC4F3E33C818AB752F70391B4A1E93A9B97390E937EBCD15924A
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.=.1.3.2.7.9.8.9.6.4.0.5.2.6.9.0.4.3.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.9.8.9.6.4.1.5.6.1.2.7.8.0.4.....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.=.9.7.e.8.5.9.0.2.-.c.c.4.f.-.4.9.a.9.-.a.b.c.a.-.e.2.7.4.6.a.9.c.8.d.b.8.....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.=.6.9.1.d.5.2.6.e.-.8.b.0.7.-.4.f.b.7.-.a.b.a.7.-.f.c.6.7.3.4.0.a.d.3.0.f.....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.=.0.0.0.0.1.6.c.c.-.0.0.0.1.-.0.0.1.7.-.3.0.9.d.-.c.a.1.1.f.4.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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_056916a7\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):	0.9168964815492135
Encrypted:	false
SSDEEP:	192:TUlir0oXZHBUZMX4jed+W/u7sAS274ItWc:Ili1XJBUZMX4je7/u7sAX4ItWc
MD5:	474BB9CDDC0237DEC31BD8FB2803FC49
SHA1:	2C416606C4090AC0BFEFACE522C6A41DD8BE2017
SHA-256:	984F09474825582E0141A2A0ABD6D1F3BAB79D9DB8616861B0FD528563F0605A
SHA-512:	28BC5028DA321DF4F297AB70F63ACFC7BB84E99B384E35449BDF036E8ED15D529A42D126B96EB9C073B4136A6FFFBCA1C7A8A8FD9EDBEC2A6107EBD5CD7A528C
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.=.1.3.2.7.9.8.9.6.4.1.7.6.3.7.1.6.9.3.....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.=.1.3.2.7.9.8.9.6.4.2.8.5.4.3.3.5.3.9.....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.=.e.c.5.b.f.0.8.a.-.d.1.f.c.-.4.2.d.1.-.9.5.b.5.-.e.7.9.9.0.b.a.a.3.6.2.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.=.6.4.c.3.3.8.8.c.-.b.0.3.9.-.4.e.7.e.-.b.0.c.f.-.e.6.5.a.0.b.e.1.9.7.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.=.0.0.0.0.1.3.9.4.-.0.0.0.1.-.0.0.1.7.-.7.5.a.1.-.5.1.1.2.f.4.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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_15f10225\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):	0.9167882020509293
Encrypted:	false
SSDEEP:	192:XwwfqDi/0oXcHBUZMX4jed+W/u7sAS274ItWc:dEiBXkBUZMX4je7/u7sAX4ItWc
MD5:	890F72CB60412E41580851AD3ED63CCD
SHA1:	0C45ABFAC0526E1C50ED258DF4B9C7F9D1A50FF3
SHA-256:	F5E460CA09184DFE30831F094F2CB83D68F6FE4A38CE78C083EA6607910E8C53
SHA-512:	D5CC64A91B592386D2A744E45F459AC5DD7E034095AA9D35A394F83A91BDA98AC904FC0355D5F8303D83A2D3E0AF15CEFFC7F86B539B30EF515D20DA6CD7836
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_e9d070cbac24d3d3fafff9232a9e7f59cde72c2_82810a17_15f10225\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.=.1.3.2.7.9.8.9.6.4.0.8.3.8.5.2.3.1.0.....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.=.1.3.2.7.9.8.9.6.4.2.2.6.3.5.1.7.4.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.6.d.9.0.e.f.e.-.0.3.5.8.-.4.2.3.f.-.9.a.5.b.-.a.f.8.5.f.3.b.5.d.4.c.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.2.0.7.6.c.8.4.-.f.1.2.b.-.4.8.5.7.-.8.e.7.f.-.8.6.0.d.e.d.a.2.4.d.f.3.....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.=.0.0.0.0.1.7.9.8.-.0.0.0.1.-.0.0.1.7.-.e.c.2.e.-.0.c.1.2.f.4.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\WER199.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):	8332
Entropy (8bit):	3.6982304055967408
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7jr61F6Y2e6xgmfT5SGCprR/89bo0FsfZ+im:RrlsNi3r636YP6xgmfT5S/Ao0efMz
MD5:	75246DE0CBB10BBA12644D8FCF1259C6
SHA1:	24239B6301385750F71D495E1430419592F0222E
SHA-256:	888F9F2B510BD86627D151CD2EB767922C22CF59C173662D4AF9B6B70DE6B528
SHA-512:	5EB18078A420915FA422986010A7E8F2678D5CF7770B115D7382C1C093B5C44EB513F34AC8FE0319CBB5B12D6CE4C2BFAF2A0D0B57AFAC56BDCF6559AE16E3 3
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.>.5.0.1.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER544.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):	4.50237441374865
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9HHWSC8Bei8fm8M4JCdsmcF9h+q8/1DO4SrSWd:uITfho2SNk3J0GECDWWd
MD5:	84CE2FB6533DB345BE13DA78FA03CFF4
SHA1:	65211C1EDE51F3E6E1ABE5653A0B0744AF942F56
SHA-256:	2959C1CF07700549AFC2DEEF60F12196F998B76008F42E773697D6B3A019130D
SHA-512:	B16CAEBE9C85C6C139C4364A07E7B89AEB4A7F78787AA291B49A0D24B866E4761026C00DCC3F25CD4647C9BEC8B76509ACA6FD07BAA78899F8A7CF7790FF19 D9
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="1229597" />.. <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\WERA484.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 12:06:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45332
Entropy (8bit):	2.117774716570381
Encrypted:	false
SSDEEP:	192:EQCavQhueEG7ZM+STO5SkbPDJTEuPwuTWlDFpCcnf:/peEG6+SK5LbbJT9pWlnCcf
MD5:	9964AFF142D540AAD8A86FB513E85B10
SHA1:	D2798AECF25C0F2F693D59C78EF3F5466E8BC196
SHA-256:	764E5177568A5FED87245F8C7C6E79F37B84E6BEDDBAB6CAEAA250741E926ADE
SHA-512:	D99FA7BE57CB4FF414816E349E40FEFFA3993FB264FADD7DF40A399B871D2ED13073CD88280C4D880BDA8D33CEF4EC30848F7ABD116B1EB4AE78D67DA7CBE 38D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA484.tmp.dmp	
Preview:	MDMP..... .....V.za.....*-.....T.....8.....T.....0.....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\WERB5AB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 12:06:48 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45472
Entropy (8bit):	2.1072559411813168
Encrypted:	false
SSDEEP:	192:iQZbUvQhu7EL5pZzXO5SkbPL0HpLw2d+K4J5TkUUGKfQi62/NRTDnT:Rd87Ehz+5LbAJLwE+B+fPG2/vD
MD5:	1DE7E1D7A72C91C41B9C6C7CBAC73D20
SHA1:	E210EE3641A966FCA74852ADDE2EE166FFD10679
SHA-256:	3DCC9C67DFB1D09C0C6E4FF4E300AE2EE0300CB1E60BA4B591DDA2695C5F195A
SHA-512:	AF593F5B111AAC279231FDE29F908BE02A48A7F2F8840F90AD646B9C91E27919C68B0970506EFA65CADEB4474E900849E60DD1915FF4A0ADF19DC121D8D9D72
Malicious:	false
Preview:	MDMP..... .....X.za.....*-.....T.....8.....T.....0.....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\WERBADC.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8326
Entropy (8bit):	3.6965023492030364
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5l66v6Y2S6xgmfTDSGCprR+89bPssfRPlm:RrlsNiL6S6Yz6xgmfTDS/XP/fC
MD5:	ABEC197496892BF26395FA2DBB63D562
SHA1:	5ACDA78DEBAE03F9C0DFAED4C41FA9379558B6A4
SHA-256:	0E3CF49C64B61DB0B51CCA147705D5577C7D21BE7811B61BF7A9519EA3DE598E
SHA-512:	63D5FF15FF9AFF213DEB88A19923FA17C6893F4629D1F4DCBE21804E2DF1D50F75BAB99A7D53F8EE8DF91451FC3B1AD98E119A3F3AB29C2AAE17BA971722C03
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.>.4.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF32.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):	4.504054868311377
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9HHWSC8B4a8fm8M4JCdsmIFN+q8/1DO4SrSzd:uITfho2SN2vJ0wESDWzd
MD5:	E6A1B6AAF505DF2217F5F8F77D35CEBF
SHA1:	CC24A048D359F0D065884759703302E894BA88F9
SHA-256:	DF94D76B9E927036C41E05BE9F35B2D007C027BA2655033E8A515A2C11C25211
SHA-512:	9D5A2C8EB55C275F2BD50B2805D142FFCD9EEA62F455029620AD29C7B195968F0BB40C67FF8C466736F5DE0D164CA470B1F41A7BCC4A8C3A091739F9370611D
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="1229597" />.. <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\WERC1D0.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 12:06:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44256
Entropy (8bit):	2.158561115216556
Encrypted:	false
SSDEEP:	192:N2hXhvQhutE/GqmtO5SkbP3nMn34e7gn3o93HZegnHV:KBtEeI5LbPna4emY937
MD5:	431757921466C2E76AD42CB41F792151
SHA1:	B1C98FC8CAC1306B24F23EE77064D8CB4A70B7A0
SHA-256:	5A235521DC4F82D7221FD2777516DD25E29130CDC61A7326937B4DFF2C59A294
SHA-512:	3BBEF889F9F914BDBBAA85D3F4D6941DACAD117CDD2067729472D3D6BAA28F2F808098AEADC4D723F447C06FEA746DDFA8297E04B4FC695CA281533A246785A
Malicious:	false
Preview:	MDMP..... .....[.za.....*-.....T.....8.....T.....P.....0.....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\WERC4B0.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):	3.698574600711335
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiV26kSk/6Y2t6xgmfTOSGCprFQ89bopsfHYm:RrlsNiU6hk/6Ys6xgmfTOSBoCfd
MD5:	6A6EF04CC121CC43AC1B82CDD0DD2A8A
SHA1:	FB9021BE8455E47FD6FE4C5851EB52C79556E1BC
SHA-256:	DDD6F6F482B6A96D0FADA2E4FFD40548523FC3762E4C821EA2AF9EF6D7695EF9
SHA-512:	9713EE263415C7441DA44619A9AC57154B3864D8C290697E71D042464F87F245AA14876AA50A31D075306DD61C3752BFB071C1F14C2E62D8ECBB91D73435EA34
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.>.5.8.3.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC83B.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):	4.502680914484943
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9HHWSC8BKXK8fm8M4JCdsmpFF+q8/1Dg4SrSod:uITfho2SNIPJ0BEkDWod
MD5:	276C7379193CACB66CE31EC3CFE744EB
SHA1:	C0AF75A8A3E5C76B3462BEB232F52714EDA0C9B7
SHA-256:	3BDDD2CAF6310AB6EA7DA81D01468F6CB9E80475B1D7E875B447747489723901
SHA-512:	0FD26575CA351297EE82538085F5C63ED4C021F0E5645FD141C0C710DF0C60A33E089856CD97073DDCDC68B91F0ADC63DFDEAF8F0650BDDC679B33E11CAEACF
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="1229597" />.. <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\WERD1A0.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):	3.697547837339207
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1A0.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNi/66ex0bmXe6Y2996xgmfTtSGCprRD89bD4sfhfJhm:RrlsNiC6nH6Yu6xgmfTtS/UDrfpe
MD5:	C849DD61B025C83CA21AC3B89FDCC796
SHA1:	36338DBB58EDB666937DC327C373FE6422EB80A8
SHA-256:	5B236CAE14C478B608FA552439FC6A0B428BB1216978B846E0A45646D9A63517
SHA-512:	1C4DB439D36CAD27771493AB56B5B4FD03486CE0EFB6046CD60C82CE40AB845DC167A904C5F2ED87625AC1DD295DE0D743A4A0B9F72D03264811396639DA2C E
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.>.6.0.4.0.</./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD683.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):	4.505616126099928
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9HHWSC8BKI8fm8M4JCdsmYFs+q8/1Dw4SrSZd:uITfho2SNlIJ0lE0DWZd
MD5:	EA1BAE40796FE3F902D35562DC7096D8
SHA1:	CB3C4218DEC2E8977E158A9FF55A9FD80B759E85
SHA-256:	E48777A5A181B31692C647827C6ABAA664E25CC974D781B148C5F9A9186545D9
SHA-512:	EDB289ED6E7A786ED08D0072440BAD79F380CB8B8BF66BA55C598638A5F81C08C7B99ECD597E7AE662A5C8250784F7B90ABAEB0F0BA906E2A5E63076AB1FEC 4D
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="1229597" />.. <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\WERE5F2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 12:07:04 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39276
Entropy (8bit):	2.2452363191508313
Encrypted:	false
SSDEEP:	192:yVcBAvZDYJ2eZnNkwH1MO5SkbPxPhhN/vMa6s4TqCpybrPna:ASZNkmD5LbpPhhN/vMxrOCpyPa
MD5:	6356E291F00FDD4A65134D4717E19796
SHA1:	017FC64B6D14E3F84E17884A310844D9E4E78EEC
SHA-256:	AD912702D31F2586510E2B569FD2B77D17A3B3AEB2B9832DA4A47BF3C791F0A3
SHA-512:	130619CBDA5B3ECF079F58CCF9BB244C749684982499EABF4788336AC934448AF670AD5A5A47A9D237856EE4408C8C4BA86D5B89245EC35990588D9D5A3715C
Malicious:	false
Preview:	MDMP..... .....h.za.....d.....l.....*.....T.....8.....T.....|~.....U.....B.....GenuineIn telW.....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:\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):	4.281712359514596
Encrypted:	false
SSDEEP:	12288:ECaNncSoI08mN/d2n2azMkvkbTtnAl6Ey6cWfrT4+cymbzJawe:ZMncSoI08mN/d25nctj
MD5:	DD2F0F9AA989EEDF0A78397A3DB52094
SHA1:	D8954E896CE62DCE45AD694F4E256D1B35F47CD3
SHA-256:	E4B0A27BE2BA75F81CC8F699541AEFE080F97A7F34D407CC52C7C0EAEAC16A73
SHA-512:	1B36E203CB0C8C756724FAAA367E160350FB08504EBBC6E9D6DFCA2F52B7571DF1EAC3A747C94DF2C420164211715E594AAC81F0C089D5B87BD1873C9C1FD2 3

C:\Windows\appcompat\Programs\Amcache.hve	
Malicious:	false
Preview:	regfW...W...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..RB..... ....r.V..... .....

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):	4.1195720308053305
Encrypted:	false
SSDEEP:	384:xazrG53EJxxkwRu3evYBnX9SaPWSpafYtm+yg1hBzpfjljQOD6XadR9xfH:xaro3QxkMu3wYBtSaPlpafYtRygjfj2N
MD5:	753EBE8EAC65C84CAE8A55F8402BECB6
SHA1:	3F21B41D43045A800F173D873BB96AE6FCF69588
SHA-256:	6AF913BB20BDE9A24DD47A31BEB69DB0B245919852816C80744E1A89BB5AB677
SHA-512:	214B1C6D6C48F82389EDFBA5C632BD6C1C28CE02DEE1D9E5384FBC86B64AD5662ED5739706DE02FFE91DB05727EF27F71354FA127594AA951B070A696AB2828D
Malicious:	false
Preview:	regfV...V...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..RB..... ....t.V.HvLE.^.....V.....*.._...m...*.3j^.....0.....hbin.....p.\.,.....nk,..MUB..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..MUB..... .....8~..... .....Z.....Root.....lf.....Root....nk ..MUB..... ....*.....DeviceCensus.... .....vk.....WritePermissions

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% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll
File size:	1093632
MD5:	345eadc8b1f5d0b373b531902c06572e
SHA1:	a0a170c3bf53be55a625c7793bfe23edd4038f05
SHA256:	31bcae869dbae8bfd20fc177bf4158e75fc7fdf00c694ae13f23dff6229f8e8e
SHA512:	88573788ffb297007445449b45075e70e10f92a787954163ce74e4aa099d984530929f27f5c1c23e27e595e096831c10dcaf07ee39aaad6803f839047f8096c6
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

General

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: 2152 Parent PID: 6004

General

Start time:	05:03:57
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:	0xe50000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2104 Parent PID: 2152

General

Start time:	05:03:57
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:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 2184 Parent PID: 2152

General

Start time:	05:03:58
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:	0xe60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.372438457.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 1820 Parent PID: 2104

General

Start time:	05:03:58
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:	0xe60000
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: 00000003.00000002.787987512.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4888 Parent PID: 2152

General

Start time:	05:05:15
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:	0xe60000
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.00000002.782709199.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 480 Parent PID: 2152

General

Start time:	05:05:15
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:	0xe60000
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: 0000000F.00000000.589866381.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000F.00000002.629341225.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000F.00000000.614575496.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5836 Parent PID: 2152

General

Start time:	05:05:16
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:	0xe60000
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: 00000010.00000000.620998702.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000010.00000002.647541343.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000010.00000000.607704722.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6040 Parent PID: 2152

General

Start time:	05:05:16
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:	0xe60000
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: 00000011.00000002.656454233.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000011.00000000.613137054.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000011.00000000.624037137.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5012 Parent PID: 2152

General

Start time:	05:05:17
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',GetICffFileFromFile
Imagebase:	0xe60000
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: 00000012.00000000.616956626.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000012.00000000.626977254.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000012.00000002.662473761.000000006E6A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 2068 Parent PID: 480

General

Start time:	05:06:37
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 480 -s 664
Imagebase:	0xb80000
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: 4608 Parent PID: 5836

General

Start time:	05:06:40
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 664
Imagebase:	0xb80000
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: 5540 Parent PID: 6040

General

Start time:	05:06:46
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 664
Imagebase:	0xb80000
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: 5644 Parent PID: 480

General

Start time:	05:06:50
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 480 -s 664
Imagebase:	0xb80000
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: 5756 Parent PID: 5836

General

Start time:	05:06:53
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5836 -s 664
Imagebase:	0xb80000
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: 1692 Parent PID: 6040

General

Start time:	05:06:55
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 664
Imagebase:	0xb80000
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: 1340 Parent PID: 5012

General

Start time:	05:06:55
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5012 -s 664
Imagebase:	0xb80000
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: 2856 Parent PID: 5012

General

Start time:	05:06:56
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5012 -s 664
Imagebase:	0xb80000
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