ID: 510686
Sample Name: SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.12131
Cookbook: default.jbs
Time: 04:49:29
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

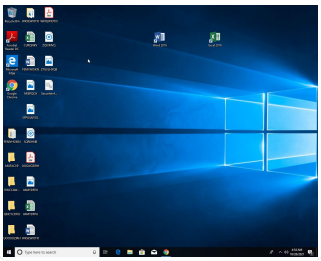
Windows Analysis Report SecuriteInfo.com.Drixed-FJX…

Overview

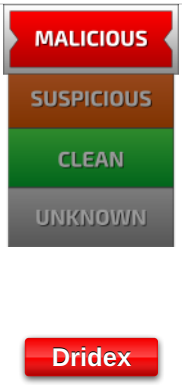
General Information

Sample Name:	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.12131 (renamed file extension from 12131 to dll)
Analysis ID:	510686
MD5:	e53a16bea7918b..
SHA1:	10d4d3d7fac35f6..
SHA256:	212cae7b05ecbc…
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

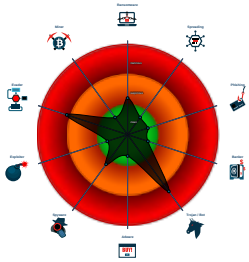


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6476 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6500 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6544 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6528 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll,FFRgpmdlwwWde MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7080 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',CheckTrust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7088 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5056 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7088 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5588 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7088 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7100 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1312 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5440 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7112 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',DownloadFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1768 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5452 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7124 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll',GetICifFileFromFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1536 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5016 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -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
0000000D.00000000.732486689.000000006F021000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000D.00000000.723436557.000000006F021000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000C.00000002.756877122.000000006F021000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000B.00000000.712349151.000000006F021000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000D.00000002.765113573.000000006F021000.00000020.00020000.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.6f020000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
13.0.rundll32.exe.6f020000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
11.0.rundll32.exe.6f020000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
10.2.rundll32.exe.6f020000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
10.0.rundll32.exe.6f020000.2.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

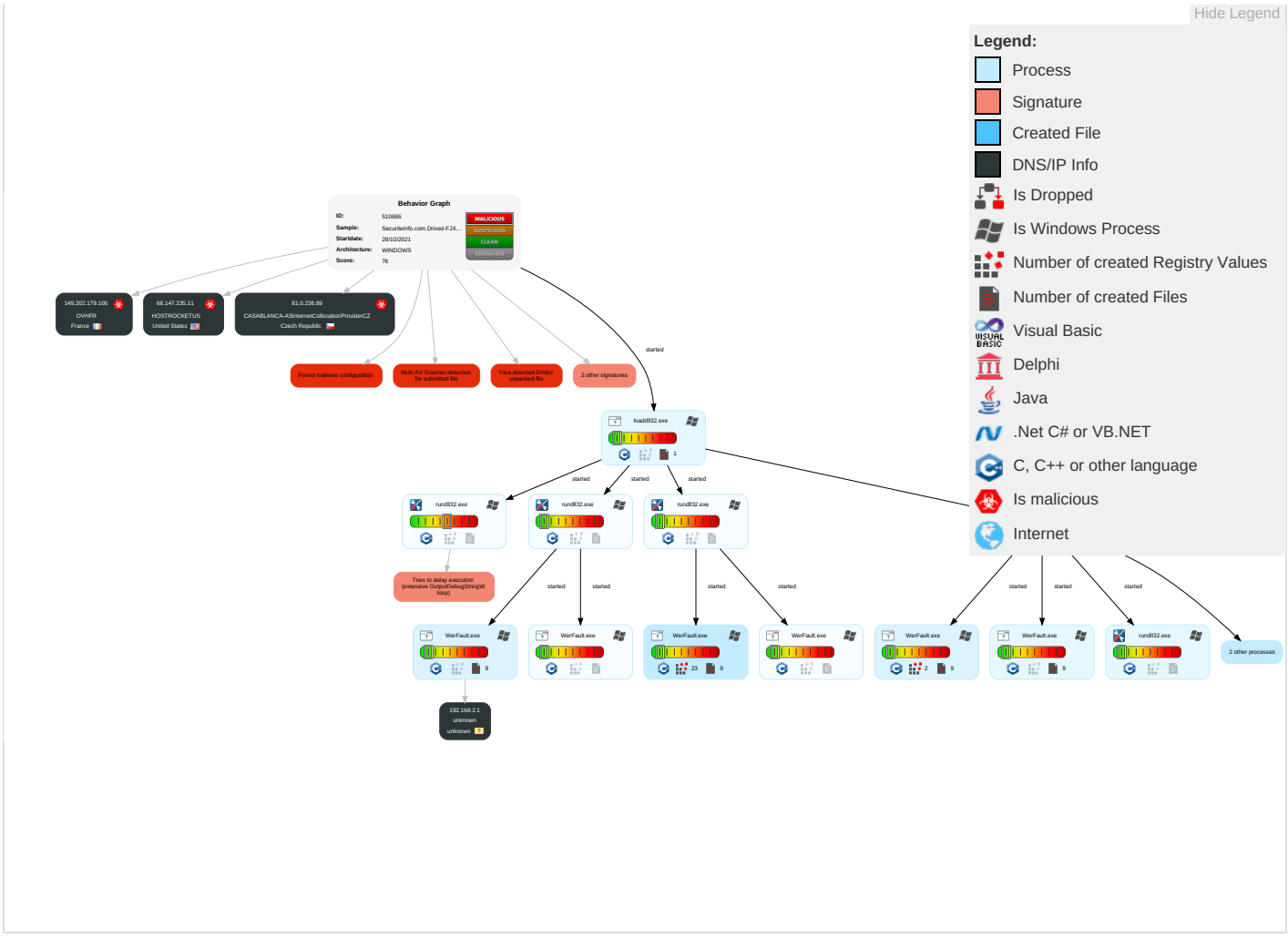
Malware Analysis System Evasion:

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	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1 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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

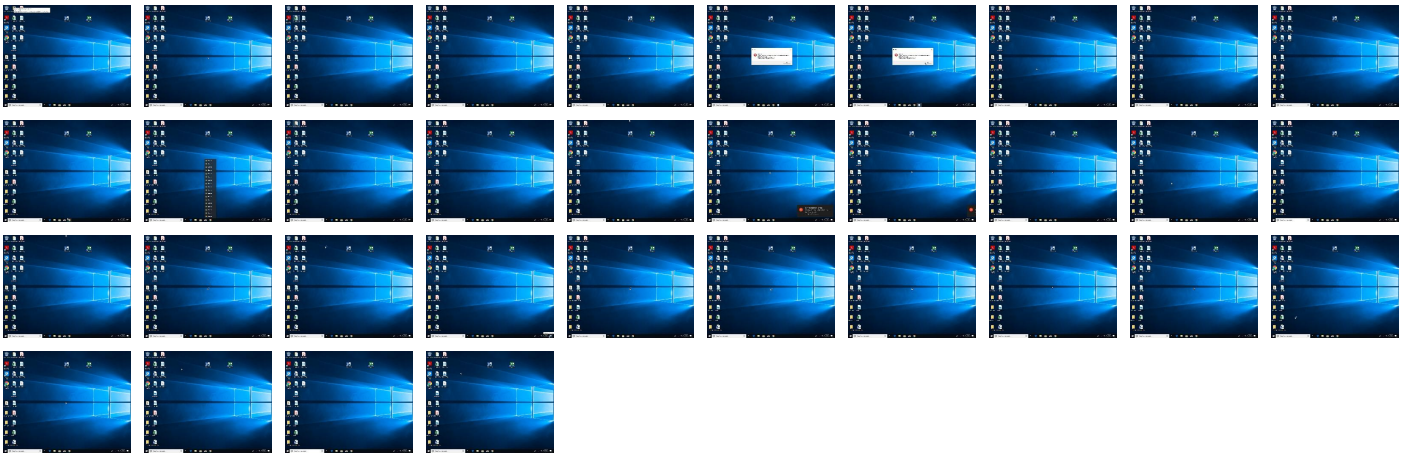
Behavior Graph



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-FJXE53A16BEA791.13728.dll	21%	Virustotal		Browse
SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	32%	ReversingLabs	Win32.Trojan.Drixed	
SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2ba4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.2bd0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
10.2.rundll32.exe.44c4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rundll32.exe.2bf4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.3fe4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rundll32.exe.2a00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.0.rundll32.exe.6f020000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.27b0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
10.0.rundll32.exe.6f020000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.2bd0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.0.rundll32.exe.2580000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.0.rundll32.exe.2dd4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.3fe4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.0.rundll32.exe.2580000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
11.2.rundll32.exe.2bf4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
11.0.rundll32.exe.2bf4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rundll32.exe.44c4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.rundll32.exe.4034756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.6f020000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
11.0.rundll32.exe.28e0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.0.loaddll32.exe.5b0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.2.rundll32.exe.2dd4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.rundll32.exe.6f020000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.0.loaddll32.exe.5b0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.4034756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.2dd4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.2580000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.0.loaddll32.exe.e04756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rundll32.exe.28e0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.0.loaddll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
11.0.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.2.rundll32.exe.2a00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.2.rundll32.exe.28e0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.2.rundll32.exe.4034756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rundll32.exe.44c4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.loaddll32.exe.e04756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.2580000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
10.0.rundll32.exe.2a00000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
9.2.rundll32.exe.2894756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.2bd0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.0.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
9.2.rundll32.exe.2790000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.2.rundll32.exe.2580000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
9.2.rundll32.exe.6f020000.2.unpack	100%	Avira	HEUR/AGEN.1144420		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:	510686
Start date:	28.10.2021
Start time:	04:49:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.12131 (renamed file extension from 12131 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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • 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: 57.2% (good quality ratio 52.1%) • Quality average: 77% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 67% • 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
04:51:44	API Interceptor	1x Sleep call for process: loaddll32.exe modified
04:53:32	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-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-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-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-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	• 216.120.236.127
	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
	XYmX3bLQJ9.xls	Get hash	malicious	Browse	• 66.147.238.141
	payment730.xls	Get hash	malicious	Browse	• 66.147.238.141
	Inf328.xls	Get hash	malicious	Browse	• 66.147.238.141
OVHFR	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll	Get hash	malicious	Browse	• 149.202.179.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1086855687.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1086855687.xls	Get hash	malicious	Browse	• 192.99.46.215
	New order payment.exe	Get hash	malicious	Browse	• 51.210.240.92
	v2c.exe	Get hash	malicious	Browse	• 5.39.3.130

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2b57d984458e21441755dcb7fd69ad7959479eb3_82810a17_06ac9ba8\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):	0.9174528397587974
Encrypted:	false
SSDEEP:	192:7Ri70oXmHBUZMX4jed+d/u7suS274ItWc:9ilXeBUZMX4jeo/u7suX4ItWc
MD5:	CF7CD7EB4BAA98CDB4DFA099BE62AF48
SHA1:	C1CBF75E010B107E05B919F52BA64B3989A0E3DF
SHA-256:	09C4023481DA95298694FEC463CF2FBDD12C106962E0A5D35DB3EEAE0D9ED4A4
SHA-512:	29381A14C5A6993E8737B6A2126F8E19584167068F167288BF636127C9F8696B8309FCC21E753D508D77118D354CB698ADB72C82766B6A14CFA1805035686277
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.=.1.3.2.7.9.8.9.5.6.0.1.4.1.6.1.1.5.7.....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.=.1.3.2.7.9.8.9.5.6.1.5.2.5.9.8.0.0.7.....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.=.b.f.a.6.4.0.3.2.-.6.f.b.b.-.4.f.8.8.-.a.0.6.c.-.d.5.1.c.6.6.8.f.9.7.d.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.=.8.b.4.a.f.5.0.3.-.1.f.0.7.-.4.8.2.1.-.a.9.1.0.-.7.b.d.3.f.f.4.0.6.9.3.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.c.8.-.0.0.0.1.-.0.0.1.7.-.9.8.a.2.-.6.f.2.d.f.2.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_5f8c232292098bd3183b3bd76fd57ba47bd4c4b_82810a17_056488dc\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):	0.9171776919766541

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_5f8c232292098bd3183b3bd76fd57ba47bd4c4b_82810a17_056488dc\Report.wer	
Encrypted:	false
SSDEEP:	192:82mit0oXmHBUZMX4jed+d/u7suS274ItWc:ZmijXeBUZMX4jeo/u7suX4ItWc
MD5:	A4E2D7D8C3B761D8F55E4B27013DB19A
SHA1:	77FFCF59E0C5CC3DB91F3BB603F9B79FD20E7776
SHA-256:	97D7E2678CD2EF7A49260D184CCCF3CA0A252D52FCCB9CD5BF8F47A86F8B9790
SHA-512:	34A5DA7B1D8B738F85123F613921A8703A4C336DA1056309B5D8A5B6E33EC6393D2511B6A767EBE92038B0B43C76C6DC6192116EEE5602CD61C8A51C451B894
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.=.1.3.2.7.9.8.9.5.5.9.4.6.4.9.1.1.6.9.....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.=.1.3.2.7.9.8.9.5.6.1.1.1.9.5.8.7.9.9.....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.=.9.8.4.b.3.a.7.9.-.3.f.5.b.-.4.9.8.4.-.8.7.c.7.-.a.4.d.a.7.0.8.f.4.c.d.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.8.6.e.5.7.3.-.9.e.a.8.-.4.5.1.4.-.a.5.e.3.-.3.c.5.2.b.4.b.a.d.a.6.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.b.c.-.0.0.0.1.-.0.0.1.7.-.4.b.f.0.-.4.2.2.d.f.2.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_af1de8448413c76b457f536b7859b51ff1ab58_82810a17_0644a712\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):	0.9169366768249558
Encrypted:	false
SSDEEP:	192:xnim0oXgHBUZMX4jed+d/u7suS274ItWcb:RiAXIBUZMX4jeo/u7suX4ItWcb
MD5:	52C5577C1D0F67DE06749DC5CD2579A7
SHA1:	562EFF5560B3EC885F54484399F2A966DC789E2B
SHA-256:	A90C59201AE0DDC5579D586AAB18CAAA937C7363D91A76DFE3BDC4459191925B
SHA-512:	26B79EAB74365840D9517F3872BBFCA2EB2828C6A95F3647B93BB1C751FBDB4BF25D0982ADD51D3E72048F8090A4D7B7D6A5DFFA01EBC5C5F3646C135FB17A A
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.=.1.3.2.7.9.8.9.5.6.1.0.4.2.3.9.5.0.4.....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.=.1.3.2.7.9.8.9.5.6.1.9.5.3.3.2.6.8.2.....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.=.b.f.b.7.3.a.b.b.-.f.c.d.1.-.4.c.7.4.-.8.c.1.a.-.4.5.7.9.4.e.a.9.f.7.d.f.....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.=.d.3.2.c.9.9.7.1.-.8.6.5.8.-.4.c.b.2.-.8.8.4.0.-.3.e.1.b.d.b.2.d.f.b.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.b.d.4.-.0.0.0.1.-.0.0.1.7.-.4.c.4.e.-.a.3.2.d.f.2.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_c316961cf9547f4477c913cd7ccdecd11bd19_82810a17_1384863c\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):	0.9170555310689312
Encrypted:	false
SSDEEP:	192:s8pib0oXSHBUZMX4jed+d/u7suS274ItWc:vpiFXqBUZMX4jeo/u7suX4ItWc
MD5:	136E2022FE3668BE06BF4D9CA54E8C40
SHA1:	A44E90D03671726C3176577FAC94942601DF12D6
SHA-256:	46FE6DB306F2A2E67744B49483DE10010A69AC166D4978F9A532702C0A745695
SHA-512:	D9D9B9F2E16058730E642E5A5AC34B748D201EEAD105B12C2C8C530CFC7382ACDEC43DCE2A16E21C1B31121C7A1C24FFB8070BD02ABE926A24053F1DB2D33 D8
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.=.1.3.2.7.9.8.9.5.5.9.2.4.2.5.3.0.1.2.....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.=.1.3.2.7.9.8.9.5.6.0.9.3.7.8.3.0.4.9.....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.=.9.5.3.5.a.e.7.b.-.3.4.9.e.-.4.1.2.b.-.b.3.7.2.-.4.c.e.6.6.b.3.7.1.f.f.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.=.d.4.e.f.2.6.2.b.-.d.f.a.9.-.4.7.2.4.-.9.f.e.e.-.7.d.8.5.0.5.c.5.b.d.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.b.b.0.-.0.0.0.1.-.0.0.1.7.-.8.a.1.7.-.1.5.2.d.f.2.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\WER3916.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 11:53:15 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45496
Entropy (8bit):	2.143027220745551
Encrypted:	false
SSDEEP:	192:+9TTNgJvRpO5Skb5a8/gS68oGwH1k7bEmMP5e2IjWIrNxQkn6d:Cyy5LbIvSBon8zMheXjWwL8
MD5:	BEC3FEE4BDB7C15EA5A63901CB714201

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3916.tmp.dmp	
SHA1:	5CD6654B5950A02ABA79D6A78466D748E3069593
SHA-256:	EB377D71C2B3470B08011992990098219B5FAE7077104F5819C3615B1FB7545D
SHA-512:	70EB91B800C7BA058536FF2CEEC2C041473A1A0222EEB6682373E67464AF18E5CA95A5D9550A4EF5F0E6CE8F804C9AF7B9D78676484B0D1822F0D87986CD315
Malicious:	false
Preview:	MDMP..... .....+.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\WER41C1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 11:53:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46344
Entropy (8bit):	2.0980430418663416
Encrypted:	false
SSDEEP:	192:xAwTNgwFnm2O5Skby+/QUjrxXkHjQm168lOs67uI+XnxH:BTS5LbydqXuX967uNB
MD5:	9166A0C57EA401C40279942ECBE4962B
SHA1:	79B6D015AF7E4022EC3E4DCD399794947461D3D2
SHA-256:	0556A7F7D118E536AE09FAB5E501FE92988ACD20B968CC0CDF9B597CBB337ACD
SHA-512:	68B1F9AC3A6D0E60EFF247C9637F7F3C3461589D01A852F7940F24FECD6DBF939AAC00C8C35E884BECBB5F6B11F4EA5332707E18E7957ED5B3BCA7AF0DF985B5
Malicious:	false
Preview:	MDMP..... .....0.za.....-.....T.....8.....T.....x.....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\WER524C.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):	8336
Entropy (8bit):	3.6976470102343444
Encrypted:	false
SSDEEP:	192:RrI7r3GLNia26RGfk/6Ypk6UGgmfT5SOCprM89b+gsfH7AKm:RrlsNij6Yk/6Y66UGgmfT5Sf+zfHY
MD5:	41685C54F4CDB54041A01238ED37A234
SHA1:	6D69DDB1AC93E29704C61D63334E15F800AFB298
SHA-256:	39EDE2DC7B4F2602C4063FA459B5A5C2E258892F527E5A6ED96BEFB25F756CF0
SHA-512:	9134F3D499E4ED24D565878B00C449346D7F364425E852EC120AB0B6B9308E72F73B1DC793CB52EBB2AD349AE8AE65FF8F5CE8904C060CC9681990CC2375793
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.>.7.0.8.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER575E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4700
Entropy (8bit):	4.504328157835534
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9SCrWSC8Bv8fm8M4JCdsPF2/H+q8/hNU4SrSWd:uITfwBCaSNaJmjDWWd
MD5:	ACB43C10C671E9BE172B578068D0E298
SHA1:	CCE46738C7513524BB0C746C0D5F12D4ACBD380C
SHA-256:	40F51E7D47C7C3B99C00453ED5CA3A3619E749BEB441299A505E7271469A22FF
SHA-512:	E2422ED8BD2B0D0E5B8266D586C46C87E51AA322D660C9F5D4D5F7AB59191F9E59167F73F86D6509CB35E1DE6EC3C6696F4AF3F2C3A2FEBED8868B241498C0B
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER575E.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="1229583" />.. <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\WER5B55.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):	8336
Entropy (8bit):	3.696536986814097
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiDR6HfXe6Ypl6UGgmfTYSOCpr289bFasf+Xm:RrlsNiV6m6Yb6UGgmfTYSZF5ff
MD5:	9E19BA093FECC4B050823625C7FAF9B8
SHA1:	07C2AE77903973666D4452B613416C7AF1B44907
SHA-256:	0E02ECD9D6168DAE822C1EB0C45D24B86974FFD5A721A17FC1BA9D86A9CDB3AD
SHA-512:	2D5DA57A9BA34EF5431E99F2D40BBE0ADCC67045AB5C130E22EC70B3EDCA0402DB0AA435C93B2A6BF019AAE30334D3333684C927323AF9472FECF3398EDDDB3
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.>.7.1.0.0.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C2E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 11:53:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	42904
Entropy (8bit):	2.2176430681154145
Encrypted:	false
SSDEEP:	192:EwJoTNgYoGjO5SkbG33eExZZUKZ036wX4wOeA2BKtsdYnu:ye55LbGOw036qCeA22u
MD5:	F1B70EC3886F544E53F61634D143AAF5
SHA1:	82B02996B6927E98B3B7FA4D8221B4A3B4281922
SHA-256:	197A27AEF881D9AA396CDD7CE67CF2393A83F93F719E52444A0E4B9996A14CD6
SHA-512:	2F940679FB60F1634DA72800B6AF1863C72D791C72F571BDF583D7FF378B499EC4B5AE67C4F28A2020083A4DB423D5E0B2FDAFA7BF4E9A39997E950D74603EE(
Malicious:	false
Preview:	MDMP..... .....5.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\WER61FD.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4700
Entropy (8bit):	4.50513207131416
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9SCrWSC8BL8fm8M4JCdsCF3+q8/hxJ4SrSzd:uITf9BCaSNSJS+DWzd
MD5:	62DB1090DC907F046049B3D174C72850
SHA1:	B86FA95A97F742D777422258AE0DC34EE709AA84
SHA-256:	0DAD5DE5E468354CF7FC4D1B56604E607AE3F22C969CEA8D91E6284A8DFA4AEB
SHA-512:	8601725E29A34E25CF9AADDA7E5392CF6098C0B90B783D1542A58A764E760C886F55038A90A02EA4A0ACC2DB1786DA515485485E8398D825A94514C202786ED4
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="1229584" />.. <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\WER716D.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):	8338
Entropy (8bit):	3.6979926180722007
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigj96j86Ypk6UGgmfT3SOCprJ89bTYsf1xm:RrlsNiK9646Y66UGgmfT3SgTLfa
MD5:	513A869F0DF8F62CD0DCAA506841CB38
SHA1:	79DB8DD1D5B2EC5A6626721F2524C0726234D07A
SHA-256:	FFE0C86992CB2BCCE3EBFADC66D0949BF3F3A970AA1EE96CAFBF13D467863FE0
SHA-512:	7E92BC808B44034F2AC3A1B67998AEA34B758AB2D07CBE00CCAF06142A6186DCCB7F46289A499ACCBDF904339F104F4254F08A0690BD59ABA95AE0088147724D
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.>.7.1.1.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7650.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4700
Entropy (8bit):	4.506054323545336
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9SCrWSC8BP8fm8M4JCds7F2J+q8/haD4SrSh6d:uITf9BCaSN+JqnDDWh6d
MD5:	FFF9E77B6F3D1786A8A9DA10BAD0AF11
SHA1:	34A1EDD1AE0072362AE28415F12A7337149C04CA
SHA-256:	216D954D69EB38411EA005440CEF5C372F556E6511CEB2652D32858D8FC7C8A9
SHA-512:	24843BC93AAFDB91149990A3295A46ED7FFA1165A9FD3A7A30D6B08F83D7ED16751227F92974BB4AFE1A0569D2BC464AEDDECECB285C92EC7B40FDDE2D06EA8F
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="1229584" />.. <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\WER7F66.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 11:53:33 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46780
Entropy (8bit):	2.080780581834969
Encrypted:	false
SSDEEP:	192:cm8v3TNgd6VO5SkbQTsY6/X35vbstTk7fysRvPZ9UuyjMUbXn:sh/45Lbest35vETk7fysRvh9UuyZ
MD5:	3252341FA4E6AAA340C86BE569B9B887
SHA1:	396413E0DF4DA5C36E2C8A2F27EB9B923BEBFD5D
SHA-256:	4235090E7060960CAEEDA542366BE61213CBEA65231CA0010CA88B3DA96091EB
SHA-512:	0DC5105CB2A5B95C823C647CF1ED4928D685CE823F7E45DA787B9CB5ED58E81291A6F538EED3421E517081218F46F42C6D36CEE2C1EB4DDD2B7BD7731AADD53
Malicious:	false
Preview:	MDMP..... .....=.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\WER9168.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):	8338
Entropy (8bit):	3.6972286046051592

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9168.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilB6q86YpH26UGgmfTDSOCprRV89b7Csfwpm:RrlsNiD6h6Y46UGgmfTDSHC7Bfj
MD5:	35FE3F27DCF32FE4EC829F835278479E
SHA1:	D89F2546047CDDC57935D5DD124C03DCA162FB7F
SHA-256:	D412817C9BB092531DD5F4FE42AAF432F9AC71F9CDB5FBEAF0F740B040404182
SHA-512:	78F1F02C2DCFF470D48C3B5A2BFB4E6511E6B5E497BCC666CB4B05319B507B7761E7F8DE89B62C8D914413F651445A807A2313AE64E0B4226BEE383619E476BA
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.>.7.1.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER97D2.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4700
Entropy (8bit):	4.504516774345163
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9SCrWSC8Bys8fm8M4JCdsbFx+q8/h94SrSld:uITf9BCaSN8RJdYDWld
MD5:	727815519B03DAD3AF59D1F6118DB2A9
SHA1:	602837B2F4405F5ADB8C4CC82533B4BF068EB29D
SHA-256:	FB3093C323633B6C1A0CE189BE47004145EFCF055F0CFC0F9F1E2F0E9832F311
SHA-512:	9546B2871F163E4A55F0D28C3345C134937916AB5763B308DABF8FD91B843815B22E09EADCDEA3665EA6B4BF4EDADA7BF729AEAF5EA5F8FFAE8D192FE19299 36
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="1229584" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.219812702838393
Encrypted:	false
SSDEEP:	12288:tmJcDpPaXSu5Pl5b9He4JpjoNPKHQh/GRH66BmjW0I2nej3Pq47Dw6:4JcDpPaXSu9l5bf+Ym/e
MD5:	B614A3B1ECD297D659BE03B0AB7C45B3
SHA1:	889FBB8C0D61ADE8295658FB48DF3E88513F028E
SHA-256:	A9F980CEF056EC64C47CF7B8CE374F1551D1BA94A263ED1F72B604B209CC83A4
SHA-512:	140296B1DE41CAEB366D0ECFAB17C43682411FB1ED7C37C4A514A6944330E4EF9115A81EAF1E1C3E88C635064BEFB785C8836B373CAB93E539BC056647574DA F
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.rmtmN..`..... ....-.=..... .....

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):	20480
Entropy (8bit):	3.527735715021905
Encrypted:	false
SSDEEP:	384:1/FEP54XnIrnc83XTVgGQXK0XBmnQmRNovOglb:NFEx43Ac83DVgGQa0X8nQmUvP
MD5:	298C01B000B90A25B63089430DFCCF86
SHA1:	AD0E9DD2A27ADCB4619FBED9AFA634A93FBFF4D6
SHA-256:	368BFE7355199AC75CC44744FF406D8DCD3B48BF8424E55B76B6DC4ABBC230D3
SHA-512:	263A9564D1B4E3003B090EC264A2E260B4DA58DF17190332CA2DD7CFFD476BD7DC204AB2BF7A4E946C352F3DC07CBD0A261FA7D122470CFA7394CEF3D5D7E E6

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Malicious:	false
Preview:	regfU...U...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.rmtmN..`..... ..... .....-.=HvLE.N.....U.....!.....6>G.YK.....`... ..hbin.....p.\..,.....nk,.M..`..... ..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .M..`..... ....Z.....Root.....lf.....Root....nk .M..`.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.159938943426644
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-FJXE53A16BEA791.13728.dll
File size:	1093632
MD5:	e53a16bea7918b1f7d4c0e659febc766
SHA1:	10d4d3d7fac35f6492cda2fb04aebf46903481f0
SHA256:	212cae7b05ecbc938b3a1fda4753d119f69360165955937b836fdbc7a6d514eb
SHA512:	014561ee3d96f09222cb1187c8b0a785e59e2d7dd1d3bec234088c2c382da693acc5cee4b21252462939574c1c666da8f09e45161b0856b0b413f7b687567eb5
SSDEEP:	24576:ljsXggYiykQsMy2GSuCAaimSQws2yyq+YoWEUK6ES0wOyeSGwswWquEQq2GiMciL:+
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	0.379720052083	data	4.39803113711	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0xf4032	0xf5000	False	0.135154257015	data	7.11996019927	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	0x2a38	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: 6476 Parent PID: 5820

General

Start time:	04:50:24
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-FJXE53A16BEA791.13728.dll'
Imagebase:	0xa10000
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: 00000000.00000000.523799622.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6500 Parent PID: 6476

General

Start time:	04:50:25
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-FJXE53A16BEA791.13728.dll',#1
Imagebase:	0x2a0000
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: 6528 Parent PID: 6476

General

Start time:	04:50:25
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-FJXE53A16BEA791.13728.dll,FFRgpmdlwwWde
Imagebase:	0xf0000
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: 00000002.00000000.475579943.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6544 Parent PID: 6500

General

Start time:	04:50:25
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-FJXE53A16BEA791.13728.dll',#1
Imagebase:	0xf0000
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: 00000003.00000002.873904073.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 7080 Parent PID: 6476

General

Start time:	04:51:42
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-FJXE53A16BEA791.13728.dll',CheckTrust
Imagebase:	0xf0000
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: 00000009.00000002.874852641.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 7088 Parent PID: 6476

General

Start time:	04:51:43
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-FJXE53A16BEA791.13728.dll',DllCanUnloadNow
Imagebase:	0xf0000
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.00000000.697948285.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000000.716630933.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.758018244.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7100 Parent PID: 6476

General

Start time:	04:51:43
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-FJXE53A16BEA791.13728.dll',DllGetClassObject
Imagebase:	0xf0000
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: 0000000B.00000000.712349151.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000B.00000000.722717692.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000B.00000002.759412743.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7112 Parent PID: 6476

General

Start time:	04:51:43
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-FJXE53A16BEA791.13728.dll',DownloadFile
Imagebase:	0xf0000
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.00000002.756877122.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000000.715578502.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000000.709098090.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7124 Parent PID: 6476

General

Start time:	04:51:43
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-FJXE53A16BEA791.13728.dll',GetICifFileFromFile
Imagebase:	0xf0000
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: 0000000D.00000000.732486689.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000D.00000000.723436557.000000006F021000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000D.00000002.765113573.000000006F021000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5056 Parent PID: 7088

General

Start time:	04:53:08
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7088 -s 664
Imagebase:	0x80000
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 Created

Analysis Process: WerFault.exe PID: 1312 Parent PID: 7100

General

Start time:	04:53:12
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 664
Imagebase:	0x80000
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: 1768 Parent PID: 7112

General

Start time:	04:53:16
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664
Imagebase:	0x80000
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: 5452 Parent PID: 7112

General

Start time:	04:53:21
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 664
Imagebase:	0x80000
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: 5588 Parent PID: 7088

General

Start time:	04:53:21
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7088 -s 664
Imagebase:	0x80000
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: 5440 Parent PID: 7100

General

Start time:	04:53:25
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 664
Imagebase:	0x80000
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: 1536 Parent PID: 7124

General

Start time:	04:53:28
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 664
Imagebase:	0x80000
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

Analysis Process: WerFault.exe PID: 5016 Parent PID: 7124

General

Start time:	04:53:29
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 664
Imagebase:	0x80000
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