ID: 510679
Sample Name:
SecuriteInfo.com.Trojan.Win32.Save.a.28377.26991
Cookbook: default.jbs
Time: 04:41:51
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

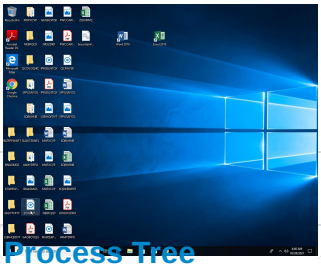
Windows Analysis Report SecuriteInfo.com.Trojan.Win3…

Overview

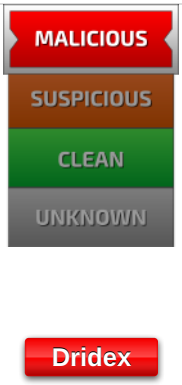
General Information

Sample Name:	SecuriteInfo.com.Trojan.Win32.Save.a.28377.26991 (renamed file extension from 26991 to dll)
Analysis ID:	510679
MD5:	2228471d39760f9.
SHA1:	38b7d35e72c995..
SHA256:	a9238550f705b96.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

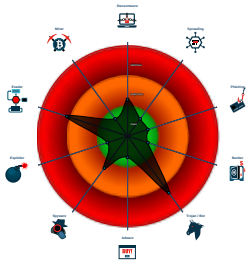


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Creates a DirectInput object (often fo…
- 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 …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6900 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6920 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6940 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6928 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll,FFRgpmdlwwWde MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6284 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',CheckTrust MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6360 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1496 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6360 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 6208 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6360 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6368 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6188 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 3096 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6396 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DownloadFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 492 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5128 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6372 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',GetICifFileFromFile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6756 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 6832 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 668 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
0000000B.00000002.1035624541.000000006E3E1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000D.00000000.987956861.000000006E3E1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000C.00000000.994333944.000000006E3E1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000A.00000002.1035258572.000000006E3E1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0000000A.00000000.993496871.000000006E3E1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Click to see the 10 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.rundll32.exe.6e3e0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e3e0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
12.0.rundll32.exe.6e3e0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
13.2.rundll32.exe.6e3e0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
10.0.rundll32.exe.6e3e0000.2.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

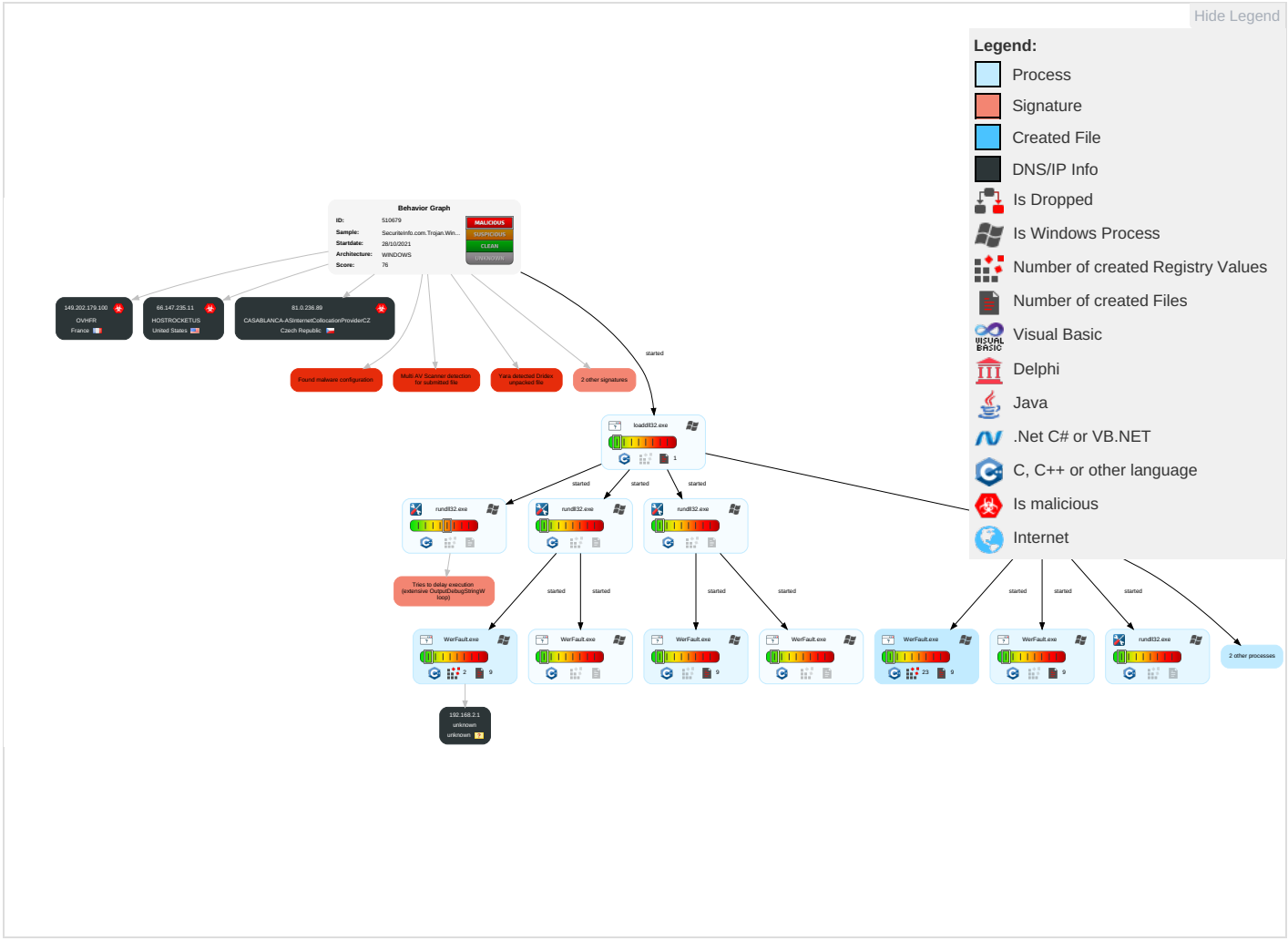
Malware Analysis System Evasion:

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	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 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	Archive Collected Data 1	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 Poir
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

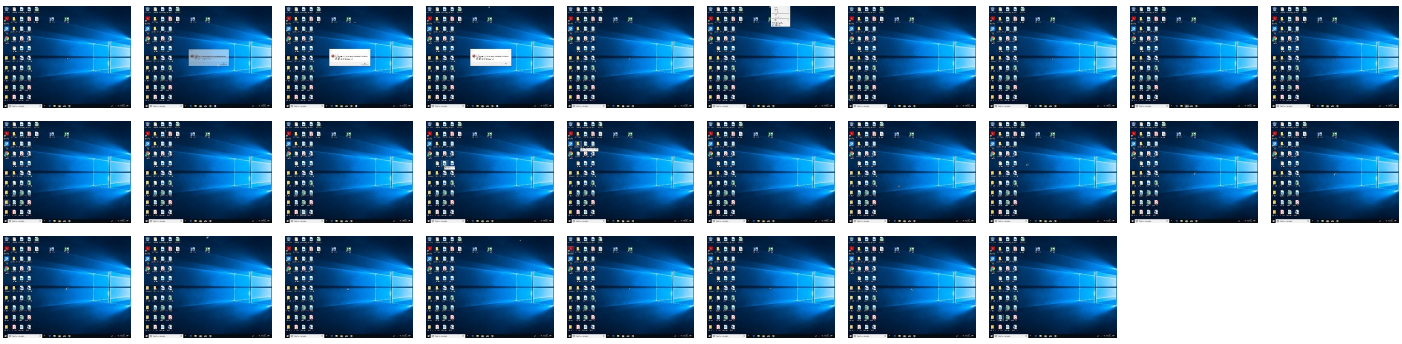
Behavior Graph



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.Trojan.Win32.Save.a.28377.dll	21%	Virustotal		Browse
SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	29%	ReversingLabs	Win32.Trojan.Drixed	
SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.rundll32.exe.a00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.af4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.b94756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rundll32.exe.b10000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.3494756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
8.2.rundll32.exe.ba0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
10.2.rundll32.exe.c30000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.0.loaddll32.exe.29b4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.0.rundll32.exe.b94756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.rundll32.exe.af4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.31d0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
8.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.0.rundll32.exe.c30000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
0.0.loaddll32.exe.b50000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.0.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.0.rundll32.exe.c30000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
10.0.rundll32.exe.4834756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.3494756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.6e3e0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.0.rundll32.exe.5f0000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.af4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.rundll32.exe.d54756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.2.rundll32.exe.4834756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.a00000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.5f0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.0.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.0.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
8.2.rundll32.exe.4a34756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
11.2.rundll32.exe.b10000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.0.rundll32.exe.b10000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.2.rundll32.exe.b94756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rundll32.exe.6e3e0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.0.rundll32.exe.4834756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rundll32.exe.46a4756.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.rundll32.exe.31d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
11.0.rundll32.exe.46a4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.rundll32.exe.46a4756.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.rundll32.exe.a00000.3.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
13.0.rundll32.exe.6e3e0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
10.0.rundll32.exe.6e3e0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
13.2.rundll32.exe.5f0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.7b0000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
12.2.rundll32.exe.6e3e0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6e3e0000.2.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:	510679
Start date:	28.10.2021
Start time:	04:41:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Win32.Save.a.28377.26991 (renamed file extension from 26991 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:	27
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: 95.1% (good quality ratio 91%) • Quality average: 78.6% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 83% • 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
04:43:40	API Interceptor	1x Sleep call for process: loaddll32.exe modified
04:45:33	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.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.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.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.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.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
	2jFfKOEefN.exe	Get hash	malicious	Browse	• 213.186.33.5
	payment advice0272110.exe	Get hash	malicious	Browse	• 54.38.220.85

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_100fb986e1756f46c39bcd29fe4136c1b062e4_82810a17_1812e8eb\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):	0.9147263722763317
Encrypted:	false
SSDEEP:	192:h6a9i80oXnHBUZMX4jed+n/u7sKS274ltWc:p9iaXHBUZMX4jeS/u7sKX4ltWc
MD5:	E7E14D8C061DD05DC23D7E06247D5932
SHA1:	4BBEF54B65651171070EAC7C1584732406BDB9A9
SHA-256:	72F32F940ECCD8629347414C2481CB0FA6614B4AF00A8882998DA74FDF9FAE10
SHA-512:	F820906248994889BEE0469314E2A2AEEA11C39DB496528E5492C61C958BFEE24CF6ED8C091FCD36A1C52FF62C46084B33AEA66D6D0D6ACF5565863F10BDC3AC
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.=.1.3.2.7.9.8.6.2.7.2.1.3.5.7.4.5.9.7.....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.=.1.3.2.7.9.8.6.2.7.3.2.2.1.6.7.7.2.4.....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.=.d.e.0.3.5.9.1.4.-.b.e.6.3.-.4.c.0.4.-.9.e.2.b.-.c.0.8.9.9.8.5.f.d.0.0.8.....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.=.d.9.5.8.9.1.e.0.-.e.c.e.b.-.4.b.1.d.-.8.2.6.e.-.4.a.d.b.0.c.1.6.e.5.0.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.e.0.-.0.0.0.1.-.0.0.1.b.-.9.1.2.e.-.2.b.9.d.a.5.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_23f57899179e2315822a274bdb180af5dd610e5_82810a17_1436f4b3\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):	0.9147510970983889
Encrypted:	false
SSDEEP:	192:m/Ufciy0oXsHBUZMX4jed+n/u7sKS274ltWc:LciUX0BUZMX4jeS/u7sKX4ltWc
MD5:	5FBFD61F5C65BC128B8C50947A20D1A7
SHA1:	4440B407AD28F21566A08A3097F789BA487C85AC
SHA-256:	A0F6E7E599D8AD0A18E6B548AF1CE99293F8DBE73127B86E62CB1DFC39606979
SHA-512:	C33B888DBFE6D21A16CDA6C2483E15076703BD82970E95522EBDB74B79BF4D2AA9E8A486B3BF9399ABF21A6D6A2DAE27B1072C54A160460DF7A61C6A5F97091
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_23f57899179e2315822a274bdb180af5dd610e5_82810a17_1436f4b3\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.=.1.3.2.7.9.8.6.2.7.2.6.2.8.2.6.4.0.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.9.8.6.2.7.3.7.1.2.6.3.4.9.7.....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.=.e.f.4.3.1.6.c.5.-.b.0.c.1.-.4.6.b.d.-.9.6.e.7.-.3.2.b.b.0.4.2.7.3.2.f.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.8.2.a.a.f.2.1.-.e.9.0.4.-.4.d.a.2.-.a.f.6.5.-.6.9.9.0.d.5.0.b.8.5.9.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.f.c.-.0.0.0.1.-.0.0.1.b.-.1.f.f.3.-.6.5.9.d.a.5.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c06c6d9b89f48a8a0e6e4feba1443adadff228e_82810a17_05e6e1d6\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):	0.9148494104496225
Encrypted:	false
SSDEEP:	192:ETiM0oXzHBUZMX4jed+n/u7sKS274ItWc:QiKXzBUZMX4jeS/u7sKX4ItWc
MD5:	E2AFAEE51560E1FF51718BA40A62F62C
SHA1:	AC1339867659160152C5E19070BA2244E4E2A5F6
SHA-256:	C969D1CDC6D94FC001BA102F16126CB0C409F1BED816F85BF7122B205CC7219B
SHA-512:	129B4F7024186A677D8240F191F97CD95ED17CAB39656FDF618D54CC5BDC0C53F4C684239A5ADB796F639337DAE439F5C445FB6C3A03E7CB9F128E2098628C7
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.=.1.3.2.7.9.8.6.2.7.1.8.9.9.7.8.8.5.3.....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.=.1.3.2.7.9.8.6.2.7.2.9.2.4.7.8.4.6.8.....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.=.6.5.d.6.d.7.5.b.-.0.5.b.a.-.4.d.3.b.-.9.7.0.f.-.1.c.2.a.1.3.2.1.5.e.3.6.....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.=.1.a.6.f.d.c.7.4.-.3.2.d.3.-.4.c.e.d.-.b.3.3.6.-.1.f.f.6.e.5.5.2.8.b.3.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.d.8.-.0.0.0.1.-.0.0.1.b.-.a.3.c.3.-.e.f.9.c.a.5.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c3cbf2193d9fa4edd46cb99d95805ff8d68ee663_82810a17_1a5af733\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):	0.9145760292834912
Encrypted:	false
SSDEEP:	192:rXi20oXcHBUZMX4jed+n/u7sKS274ItWc:biwXkBUZMX4jeS/u7sKX4ItWc
MD5:	68BF401C1D1C39E4E4CDF821FE5C2A5E
SHA1:	45C06CEDBB0CE9B1ABA293E7DB922903128B9FDD
SHA-256:	9B28CAA49E2B0D32429C9BBB9AD7BD2973D2A2A1DC1F71ADFBD512F00809129A
SHA-512:	2D24443B11E8404682CB158A54169A1E49FB029CA6D9DA0B58E611541CCB3FD8298736A8A6C6E2272C8850675387783767295DD26734900EF73A32E99F4BE638
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.=.1.3.2.7.9.8.6.2.7.2.7.4.2.6.1.6.5.5.....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.=.1.3.2.7.9.8.6.2.7.3.7.9.7.2.9.9.1.6.....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.=.0.d.2.e.4.8.1.b.-.3.3.9.1.-.4.7.d.1.-.9.4.d.9.-.5.8.d.1.a.d.8.b.9.2.9.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.5.8.b.2.b.d.1.-.3.5.e.9.-.4.5.f.3.-.b.6.7.5.-.4.a.5.3.3.9.b.2.b.9.c.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.e.4.-.0.0.0.1.-.0.0.1.b.-.4.4.d.e.-.9.9.9.d.a.5.c.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA838.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 02:45:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45982
Entropy (8bit):	2.110582099269261
Encrypted:	false
SSDEEP:	192:OgQxOI0eNO5Skb2m0mbEDBv4mlkxoSdyQK6O66CsGTwAhfnDHozDQ/K:35Lb2miVlkFyQ6WsGTHDsDQC
MD5:	882931F51B1B73DC6B62F1EDCB0E3A09
SHA1:	5FFA2B3D9A8F873AF27C5F5C56E2B3C50A845973
SHA-256:	CCEF491401B05B23FCAD05D2217ADD7D3C753D6F5B1BBF68226AC1B870D43B91
SHA-512:	8D0B5AB14E9C95B7ABFC45301999FAE401E2095489C26789C2F20640E3761D6A780D0AAFE60465697FBDF1F559172B2890D0235F61323314648326420E68673E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA838.tmp.dmp	
Preview:	MDMP..... .....za.....(-.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....[.za.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERB132.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):	8334
Entropy (8bit):	3.6941056954487266
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimjU6sYQ6Y9v6VhcgmfTHSf+prRS89bwYsfawm:RrlsNioU6U6Y16LcgmfTHSwrwLf8
MD5:	F453E77E2A7CC2D905D007AED06302D8
SHA1:	087A39420A8465730004ABA1B5FD3F0C393A3C8C
SHA-256:	FE9CEB0E5EFF45686DACB635F46D04B019F71EA3C5D511207834B8FD90A5ADCB
SHA-512:	677142FD2ACD3005B88237C202EEE44854C14A7F1A92BACA6CB68EB406089CB8A3ED97E8DBB64595D42AD3EFA7DB30DB82392EDA90FECC280D55C8634F4C59C
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.>.6.3.6.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB170.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 02:45:24 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46774
Entropy (8bit):	2.0599297130149634
Encrypted:	false
SSDEEP:	192:akiexOux2QvozO5SkbQepjaM5kx8Kdx/032KvW3Jmd7l37n8:3zoq5LbdRkFdx/0xymdF8
MD5:	F92717FDA23E860A6EF7EDAB858200B9
SHA1:	F5F306E9219CB5925A009EDDED35AD89CF4B9286
SHA-256:	2A1A6F10D6E5215DA0C9778E590942AD4BC8F7EB5BB53101976021F209C52517
SHA-512:	DAC7DF1DF44BAE9C6C28FEDEA4AA32381B0AA604BEEE24BBB6D0E12D989DABAE17D6178F79D27F85FA81A82D5CE6796C343B3C7188758368E355D584114E8C06
Malicious:	false
Preview:	MDMP..... .....za.....(-.....T.....8.....T.....&.....0.....U.....B.....GenuineIntelW.....T.....[.za.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERB3F2.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4694
Entropy (8bit):	4.488212192939574
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxJgtWI9XnWSC8BV8fm8M4JCdsRFp+q8/J74SrSAd:uITfD4WSNEJnkDWAd
MD5:	129D66DE96BECA1534E9E3391368E940
SHA1:	703E09F0EA5A23A31C9C4B2F321AAF8872C26947
SHA-256:	892E572C1B606CE700CAA0E3F4839C05CE1ED16CB27620E3AE03C7D2651DBE7F
SHA-512:	B6A370BA81340E418EDBF8BEB6485178D9AC4E25B97C11BD87E609C57E06681C60C3375A8DAC9D876078A9400C01205CD59F7415EFE09BCF400011E5356F8E0
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="1229036" />.. <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\WERC140.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):	8334
Entropy (8bit):	3.6935294774212855
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiOjGC6wu6Y9l6VhcgmfTiSf+prRE89bPHsfjaGlm:RrlsNiAGC6Z6Yv6LcgmfTiSwhPMf+1
MD5:	059631A4291335880F0A32CA284F19E3
SHA1:	873D9320CC9612C8F91488124E9EAD54E7162700
SHA-256:	F765F4D1706FDC7B72ED807FC007C38E1DD6CA2AD60CBF5CE918DA0B5E8365B4
SHA-512:	02DE057A231550C2FC3A0404958CCA39A537C307D6F189B69654883720826A273F02CDA97556729DF1CB231BFDF1D13FD51951827FB0A7376A1BC327E0AB0474
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.>.6.3.6.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4AA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 02:45:29 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	38366
Entropy (8bit):	2.2811286454770294
Encrypted:	false
SSDEEP:	192:DPpdOZg8vTfa+cO5Skb4RsmXlngS/fkxAJkNyJlF/nU:qLr5Lb4pxkwkNyJ3
MD5:	A4758AC6A770AA0391B62614BC23494B
SHA1:	CA97ACA2575F7A8F7CAAF584494DDA812E3A34BD
SHA-256:	2316620D8490C69207C6F0FC45A7BF2B2B652CA46D4B61BD0D34B51FCF8E87AB
SHA-512:	18B5F42A530F45F28214A96B6E2177414278EAD98A4F64A9DDA38C822007DE8D7A3688676F21B8E571DCF2E23C27782DBE3D82D8615424DBEF0D1BAF0BE5B1D
Malicious:	false
Preview:	MDMP..... .....za.....d.....l.....,*.....T.....8.....T.....z.....U.....B.....GenuineIntelW.....T.....\.za.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERC71D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4694
Entropy (8bit):	4.486217981525297
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxJgtWI9XnWSC8Bs8fm8M4JCdsoFJo+q8/JtU4SrStd:uITfD4WSNHJBhDWtd
MD5:	C42E1B4B49B80A03857EC1A009C573A4
SHA1:	594F5586F8D102C354E5140A4749B8DCC0C08641
SHA-256:	244935B6B7A3CB948E377A06324CA482D509C8ACD7CFC2CF208255B79A4F0DAC
SHA-512:	AE5BBCC3CFAD4F0E85022B935FAB20B5BAD61DC927FA022935E7DE8F01B5EFAE3116131540AEA12A00A60A697FCFEA32FA53130323989D0E019CEE69FDFD7E09
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="1229036" />.. <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\WERC91E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 28 02:45:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	38650
Entropy (8bit):	2.2706103473918606
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC91E.tmp.dmp	
SSDEEP:	192:sYjdOZg8vTdiKO5Skbt43gUOB207kxKZFyjW6zAsnT3:sLo5Lbt43IkgFyjPT3
MD5:	EBDD0217FFF159507E8BEEF529E562ED
SHA1:	203E1C4E108A6AA2AFB27C437C3145121A7A1B96
SHA-256:	4E07358FC83CC2578998F36E1C25E1757EA871C23F27F668E2C91B69380B6A98
SHA-512:	8D5D77E28E0622AA2FE6BCD509EFB7A9CED4A5F38AF3FB71F42CE6898A34CC0987F46A1D369BBCD67721806E8F295FBCB7287B3B253864A9FF53D822CAF9E17
Malicious:	false
Preview:	MDMP..... .....za.....d.....l.....,*.....T.....8.....T.....|.....U.....B.....GenuineIntelW.....T.....\.za.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERD2B4.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):	8334
Entropy (8bit):	3.6951960712951584
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiPjG6NJrm6Y9Q6VhcgmfTZSf+pr689bInsfI4m:RrlsNi7G6u6Y66LcgmfTZSAIsfO
MD5:	A965A4E7197B5D5643E437EF1026BF09
SHA1:	42C6C763BCE8FC761AE606F92C8D75CF7E8CF518
SHA-256:	7295FC28007141C32E0081C8E646D560C60C035CECE7710B10A22108415F42A1
SHA-512:	BA89D5173AE8A319CDE1AD969DF3A4851EF3B3C11861E456126B02C3F100B80601C56D58FA25FD039CE46B8E4703C4EA2559455223AB860AD194367C84F4C9C
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.>.6.3.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4694
Entropy (8bit):	4.488959000814019
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxJgtWI9XnWSC8B/8fm8M4JCds5FD+q8/J6S4SrSad:uITfD4WSNGJ9yDWad
MD5:	5BDF284660CF0C76C2F5E2D931FF5D15
SHA1:	90EFD8DF68F09EDC4664C8FD29DC9431D2C4ECCD
SHA-256:	24478D1EE7D78F7A4CA458CB3776F13095CB9F692B37736FC41BC45033597350
SHA-512:	15C7E72F52C948B41D9B7EF8B55F7F52DD4485EB732B0B6843476CF75EA41C964A254E5A529E68D39DBC983274D054D5B8E9B36E9DC05F60B5781399E5ECAD4
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="1229036" />.. <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\WERDCA7.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):	8334
Entropy (8bit):	3.6933352539414077
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilx6iy6Y9k6VhcgmfTNSf+prRw89bD9sflhm:RrlsNiz6X6Y+6LcgmfTNSwND2f6
MD5:	02611AA259B4B5892273F7A9E07C73C4
SHA1:	819643A654BFC05962C24DDFD4F30F88B7F09383
SHA-256:	EFBB016BCA21237A560CBE15F6ADFA5E7E8288F90F751204014AB2A59E7201F4
SHA-512:	81DB23E395748B919AAEBBE35F9E703EC7F5D43F5247FC2ADA2B5C3D8801859B3410F84CC0A41E99AA091E8D533845070A25F4E370B05615A753BA125124655D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA7.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE40B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4694
Entropy (8bit):	4.487676574686123
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxJgtWI9XnWSC8BPs8fm8M4JCdsxFo+q8/Jyu34SrS4d:uITfD4WSNxRJCaDW4d
MD5:	B1AB375C0816154098F60DFD37310902
SHA1:	8DB57959201F5240BBB468EF84C9A3F367EA5C86
SHA-256:	F316047E60C449085851A7C10477F3F53A117BE2AE7CE089FB3ABCEEA6D56E4F
SHA-512:	A007FF2FF06BFFA158B0186CE96DF0052EDF2C56CBBE56B1A4E124A2D8FCF7555FB0B5D7A42009A67D5CE8D295C88DC019CC1BF920D66E3CABBCD0B74A01ADE6
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="1229036" />.. <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):	4.244673068780695
Encrypted:	false
SSDEEP:	12288:RQd7oesqEOTJQ4v7769XyErYnea1cQlFVrIzGRCxAlks9t7W:6d7oesqEOT64v7Yen
MD5:	8C3AB5B1DC5D1ABD9348B10C33895312
SHA1:	47E73434578A58BB370B2174BD5D92B8C25ABDA3
SHA-256:	38DA0FE6DE4F7EFE780FBD799732FF44A32941360219CE41CA266958BB9D73FB
SHA-512:	8BD292301E368F16FD0D1C9C4C7249D9EA957540020619C401AC02B78C44148E0DA3D0631B129C3A372B60520EBF6322E879B95D272C24D649067B1890D1B88D
Malicious:	false
Preview:	regfH...H...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.[u..... ....;Sq..... .....

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):	3.413917876186381
Encrypted:	false
SSDEEP:	384:uT55K5sPv4EgnVVeeDzeD1NKZtjLT8GpwT1L33SYL:GnKkg/eeDzeZNYtjkGpwThSY
MD5:	05273D33251685A4E511B9006999199F
SHA1:	14A5E3BADAAE5071A82B785D0FBA89774AD0AC41
SHA-256:	81830EE13605B6D9302DD08C2709AD2F669DC20C5725470F062A56FCA01E477A
SHA-512:	298C602ED65BBDE9CE4B28E9409CE81640407FDE55B3FC4DD2D433124410FA07DEA73B8DE4C937ED059D6719D79060DDA740D71C02FD016128CE8439A547CC5
Malicious:	false
Preview:	regfG...G...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.[u..... ....=Sq.HvLE.N.....G.....V..zH..W"."s..... ..hbin.....p.\.,.....nk,.3.w..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .3.w..... ....Z.....Root.....lf.....Root....nk .3.w..... .....*.....DeviceCensus.....vk .....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.160195302212999
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.Trojan.Win32.Save.a.28377.dll
File size:	1093632
MD5:	2228471d39760f9a389ac95f71b671a9
SHA1:	38b7d35e72c995ca526e293af9d448a7a8011df6
SHA256:	a9238550f705b9668a390a9e7b9e4dec6a88daec2c8acca19ffa10af328d594d
SHA512:	48d40173dfbc5dd798efbae2252b9599d2dd88b3a9b953e4f7203de79bd272c24b5c914f5b809774d1b3b146b8fd3a12446bc4d5855959eca3229e0a97b7194
SSDEEP:	24576:tjsXggYiykQsMy2GSuCAaimSQws2yyq+YoWEUK6ES0wOyeSGwswWquEQq2GiMcis:m
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	0.381795247396	data	4.41548626837	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0xf4032	0xf5000	False	0.135155253508	data	7.11998014415	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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: 6900 Parent PID: 1364

General

Start time:	04:42:46
Start date:	28/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll'
Imagebase:	0x1110000
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: 6920 Parent PID: 6900

General

Start time:	04:42:47
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.Trojan.Win32.Save.a.28377.dll',#1
Imagebase:	0x11d0000
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: 6928 Parent PID: 6900

General

Start time:	04:42:47
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll,FFRgpmdlwwWde
Imagebase:	0x11a0000
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: 00000002.00000000.781525113.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6940 Parent PID: 6920

General

Start time:	04:42:47
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',#1
Imagebase:	0x11a0000
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: 00000003.00000002.1190711259.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security

Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6284 Parent PID: 6900

General

Start time:	04:43:38
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',CheckTrust
Imagebase:	0x11a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.1189742876.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6360 Parent PID: 6900

General

Start time:	04:43:39
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DllCanUnloadNow
Imagebase:	0x11a0000
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.00000002.1035258572.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000000.993496871.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000000.983061292.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6368 Parent PID: 6900

General

Start time:	04:43:39
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DllGetClassObject
Imagebase:	0x11a0000
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.00000002.1035624541.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000B.00000000.984417816.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000B.00000000.993970485.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6396 Parent PID: 6900

General

Start time:	04:43:40
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',DownloadFile
Imagebase:	0x11a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000000.994333944.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000000.984331787.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000002.1038712080.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6372 Parent PID: 6900

General

Start time:	04:43:40
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll',GetICiffileFromFile
Imagebase:	0x11a0000
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.00000000.987956861.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000D.00000000.1005884089.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 0000000D.00000002.1038939767.000000006E3E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 1496 Parent PID: 6360

General

Start time:	04:45:17
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6360 -s 664
Imagebase:	0x2b0000
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: 6188 Parent PID: 6368

General

Start time:	04:45:19
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -s 664
Imagebase:	0x2b0000
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: 6208 Parent PID: 6360

General

Start time:	04:45:22
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6360 -s 664
Imagebase:	0x2b0000
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: 492 Parent PID: 6396

General

Start time:	04:45:22
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 664
Imagebase:	0x2b0000
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: 3096 Parent PID: 6368

General

Start time:	04:45:22
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6368 -s 664
Imagebase:	0x2b0000
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: 5128 Parent PID: 6396

General

Start time:	04:45:23
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 664
Imagebase:	0x2b0000
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: 6756 Parent PID: 6372

General

Start time:	04:45:26
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 668
Imagebase:	0x2b0000
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: 6832 Parent PID: 6372

General

Start time:	04:45:28
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 668
Imagebase:	0x2b0000
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