ID: 483798
Sample Name:
SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll
Cookbook: default.jbs
Time: 14:01:58
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

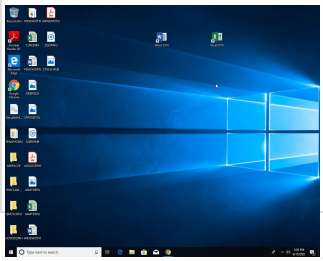
Windows Analysis Report SecuriteInfo.com.Trojan.Agen…

Overview

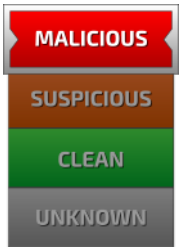
General Information

Sample Name:	SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll
Analysis ID:	483798
MD5:	4b59be3cef04547.
SHA1:	bed0d3a622ca55..
SHA256:	b7ca395f51df95b..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

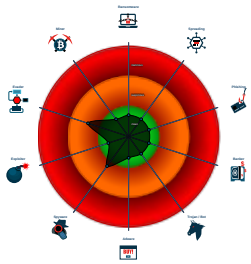


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Creates a process in suspended mo…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6680 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6812 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6780 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6200 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6780 -s 816 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6820 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll,uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4312 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6820 -s 804 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6192 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll',uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5780 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6192 -s 804 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

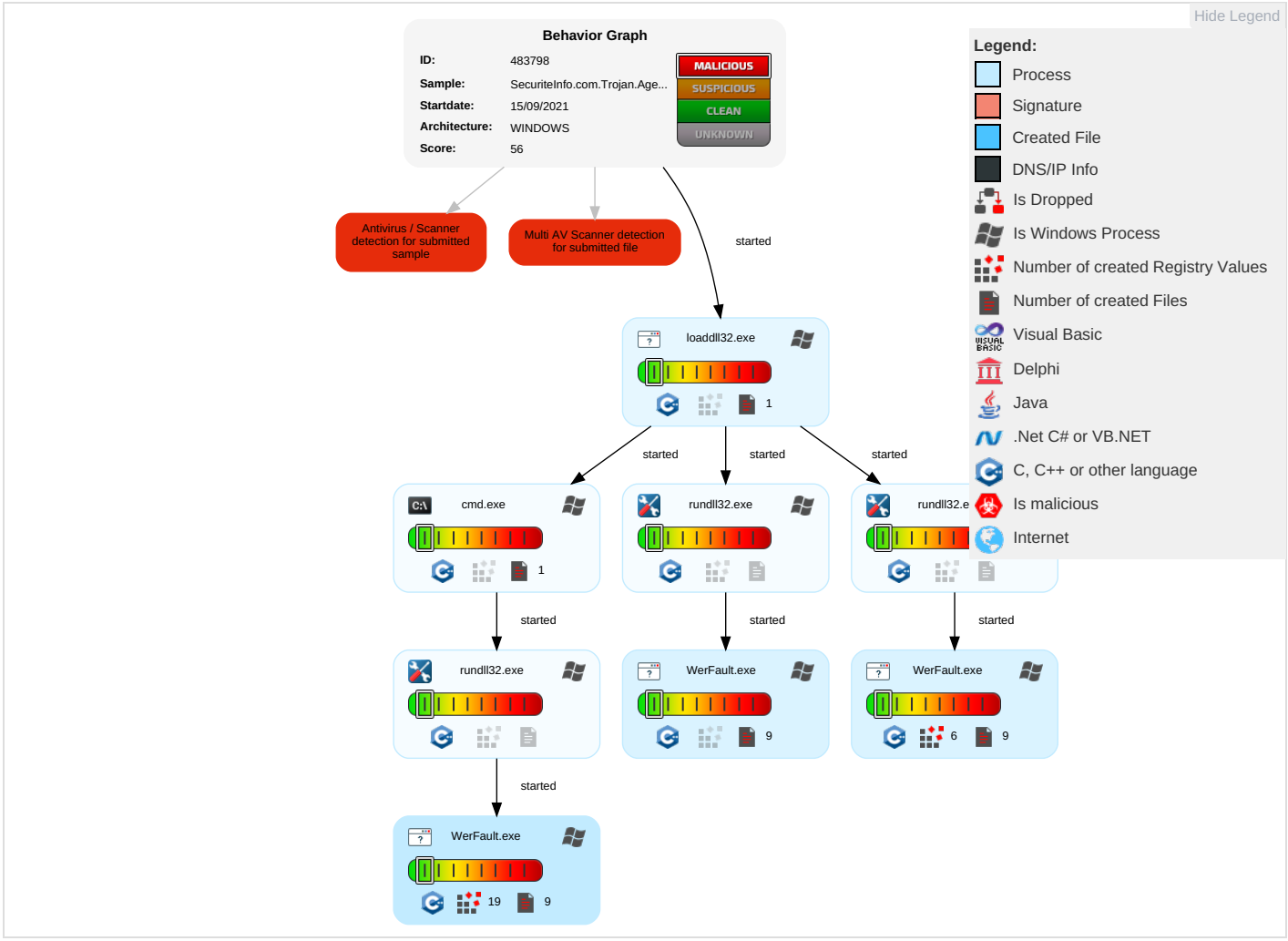
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

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	Rundll32 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone 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 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

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.Agent.FHBA.20741.dll	63%	Virustotal		Browse
SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll	29%	Metadefender		Browse
SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll	75%	ReversingLabs	Win32.Trojan.Spynoon	
SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll	100%	Avira	HEUR/AGEN.1142362	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
4.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
4.0.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
3.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
4.0.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
9.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
9.0.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
9.0.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1142362		Download File
3.0.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1142362		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483798
Start date:	15.09.2021
Start time:	14:01:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	33
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:	mal56.winDLL@12/12@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 68.5% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d7875efe6eda25dedf35b4fc2e3f4edb5b4f3df8_82810a17_109fc28b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13858
Entropy (8bit):	3.765844462426622
Encrypted:	false
SSDEEP:	192:fmi/0oXXHBUZMX4jed+IqZnB/u7sfS274ItWcQ:uiBX3BUZMX4jeCJB/u7sfX4ItWcQ
MD5:	3ED7A7984B1D72B471DA0E7043463509
SHA1:	F8E074A9E2622E57ECE0CF307301B4A1637FCDFF
SHA-256:	4C6EE35311A4BF6998CDE482DC65BF2028D130DBAADD43D7621C07CD5ED3CF44
SHA-512:	65E8EBE25FA190C22D52B7300DB3708775E3AD1F7048ABF0BEEAD6418E424E73C015AE6A82CA59EF7CF3AACA0C218377D1374302544123B87B887B31EDFE9D 9
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.=.1.3.2.7.6.2.1.3.3.8.1.3.1.0.0.8.2.6.....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.=.1.3.2.7.6.2.1.3.3.8.2.7.0.0.7.1.5.0.....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.=.a.6.1.e.e.f.2.0.-.5.f.b.5.-.4.f.0.c.-.9.8.a.0.-.d.a.9.d.6.7.6.9.9.0.4.6.....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.=.8.5.c.b.2.b.1.7.-.8.0.2.f.-.4.7.8.3.-.9.6.0.8.-.8.7.e.8.d.7.f.5.f.1.5.9.....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.a.a.4.-.0.0.0.1.-.0.0.1.7.-.b.9.8.b.-.e.c.0.e.7.5.a.a.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_d7875efe6eda25dedf35b4fc2e3f4edb5b4f3df8_82810a17_16d3cd0a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13862
Entropy (8bit):	3.7646929532943063

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d7875efe6eda25dedf35b4fc2e3f4edb5b4f3df8_82810a17_16d3cd0a\Report.wer	
Encrypted:	false
SSDEEP:	192:fs50MiZ0oXTHBUZMX4jed+RGWGg/u7sfS274ltWc/:k59iXXTBUZMX4jeiQg/u7sfX4ltWc/
MD5:	F70484AB94473D4572E660A7CDEC2795
SHA1:	7549F5212B9530CB66073143B7FCB0AD43624D2B
SHA-256:	FB628AC0351E983C91DBC6E5EEE080F8F51C049B515F37DC89E15A1884CD1F75
SHA-512:	9FFEA32902A227EB3169CCD11D224862AEB2619991355DD0FA559DE989B472BD01AFFFF405461A1B902BED772070F5B60CEF7AAA941A8A0D7C43463654C616E
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.=.1.3.2.7.6.2.1.3.3.8.4.7.9.5.4.0.2.9.....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.=.1.3.2.7.6.2.1.3.3.8.5.7.9.5.3.8.8.4.....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.=.5.2.2.5.b.4.5.6.-.5.c.0.2.-.4.d.9.e.-.9.d.a.0.-.b.5.d.3.1.0.1.2.7.3.3.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.0.9.9.9.b.7.1.-.8.8.1.d.-.4.9.6.5.-.a.d.5.1.-.9.a.7.6.e.a.3.3.c.3.e.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.3.0.-.0.0.0.1.-.0.0.1.7.-.d.2.1.2.-.f.a.1.0.7.5.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d7875efe6eda25dedf35b4fc2e3f4edb5b4f3df8_82810a17_187fc375\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13862
Entropy (8bit):	3.765531692970136
Encrypted:	false
SSDEEP:	192:nril0oXxHBUZMX4jed+Vbu5w/u7sfS274ltWcb:rirXBBUZMX4jem8w/u7sfX4ltWcb
MD5:	957DD93B52A93018BA848FEE95FEA520
SHA1:	88CE3424BAA4C3D818FB3D33DF9DD157840F1196
SHA-256:	8F901762659EE347A4D1683D92173C0067CE1E55813CC87D7BA75F03A8DDDCB7
SHA-512:	98DB885B24869E2468AFCE0E21B78A7B68F7EC270938ED3FDC3E143214845C372A7CCA45A078B4C528B62420ADEF8CE9562A69193F292985A27B670332AD59D(
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.=.1.3.2.7.6.2.1.3.3.8.1.3.2.8.9.3.5.6.....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.=.1.3.2.7.6.2.1.3.3.8.2.6.8.8.3.0.2.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.5.0.a.b.e.d.1.-.6.1.b.2.-.4.1.0.4.-.b.e.c.0.-.7.3.3.2.f.5.9.a.d.3.7.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.1.b.c.7.7.f.4.-.7.c.2.b.-.4.1.8.c.-.8.3.c.7.-.4.c.5.f.c.0.1.7.9.7.6.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.a.7.c.-.0.0.0.1.-.0.0.1.7.-.9.e.b.e.-.f.1.0.e.7.5.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB905.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:03:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49126
Entropy (8bit):	2.111260583968291
Encrypted:	false
SSDEEP:	384:gL3EHVMwYt78K7k64Ran3V0qzJjz/nSqp:a3+YB8K7+O3VzJjz7
MD5:	F9449304824785877700 7EA2C9EE9FA6
SHA1:	8A7E40F6AD4B29BE6B3762FFEAFB3B7347F379CF
SHA-256:	97670F13F9C4EADEB8F3D31F3720C4C6161F30E9418A9840335C7F26D3C43AE8
SHA-512:	772C91D8C4F08299A6FDA1A3BF41B36C128BB6A2EF98EB1823541F7716AFCD0266F6CEEA03D3C895F5F222214CFED54C758CBBF7CC27C3118F77A1202F06F6E3
Malicious:	false
Preview:	MDMP..... ....._Ba.....U.....B.....%.....GenuineIntelW.....T....._Ba.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB915.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:03:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	57762
Entropy (8bit):	1.9592582376729129
Encrypted:	false
SSDEEP:	384:Rpt2zLdB1A+Zt4MBIWsUF7KP40gDrb3Wh:Rpt2+wyMBIWczgDrDi
MD5:	EA863139A89FE4F931D481EB01F3244C
SHA1:	D1808A00D230A2293FE72EB6033A61E26BB7229C
SHA-256:	CFD4B6413BF2C181C48AF487D9395B33BA2565467EFFB45906DA5A1E28F230B9

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB915.tmp.dmp	
SHA-512:	162A2C67F4FBC7B14405F78040B7324B922DAC869B312717684AE5746E849A491BC5D932796EC27E43A8DAD2CE0F2737E46B77B20CE79D32EDE386737CEADF8
Malicious:	false
Preview:	MDMP..... ....._Ba.....U.....B.....,&.....GenuineIntelW.....T.....|...._Ba.....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..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBCFE.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):	8290
Entropy (8bit):	3.695839717179838
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNisQ6q6Y++6sRgmfT+S/iCpr189bkCsfyMm:RrlsNiL6q6Yn66gmfT+SgkBfo
MD5:	FB5B8ACCD619A3FF97F03654874A37B3
SHA1:	0C756F2BB9F3AD96310CC04D8CE57729B09973AF
SHA-256:	A90A7490683D9E2E5AB00109446C74789766BB5BBA6503DAAE44F67B305848C2
SHA-512:	05612436B5209DCCBC2A5E805EEF718EBBBC8B4D8E081064895299D63B28FA2146BC2E66FDE0A0C0DFDD7CD76FE5C01962DF1441409C0CCC1FD85CC0DB91C D4
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.>.6.7.8.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD1D.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):	8310
Entropy (8bit):	3.6978120602526583
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihX6F6YCB63xogmfT+S/iCprD89bkQsf0oMm:RrlsNix6F6YE63+gmfT+S2kjfv
MD5:	C6D06049A05B964C8D7B6E9CAA8784FC
SHA1:	D725016E2A8E21A728C84CC01EDB2367A7488247
SHA-256:	800A8497ECCA8A4F4E9434439BA40A9FF0E4A43E3B7656AC6920529E6935D918
SHA-512:	89D058B8DCBAE02CF0D882EB7D6A762490C25CA915DA6940CCC1441E72D9FAA9092B6B0957D9AD3F9EB9D574753448A14A80E91DEFF5499BE3D83DDE7B60D 4F
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.>.6.8.2.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDAB.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.495306608627608
Encrypted:	false
SSDEEP:	48:cvIwSD8zsAJgtWI9dZWSC8B88fm8M4JCdsEZFoSV+q8/OU34SrS1d:uITfG2oSNHJ65O3DW1d
MD5:	95FFC24C14BD85C56BAEE2690A42D640
SHA1:	013CA3D91F6AF76CC443C22E4EF2286278CE5446
SHA-256:	2D12673FD19B5E2E5F4BD5E46A2E8C7049B5923FDE211096539C086CC02DCF8B
SHA-512:	260165E57DB7E87906AC18510F6FC6C3048794AD29F52F8472174B669E1471A41A2CFC5BA508833297B015DB26BA35A64E7518CB9C813C5FBF82D9037F4C2349
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDAB.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="1168213" />.. <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\WERBDCA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.493595461455166
Encrypted:	false
SSDEEP:	48:cvIwSD8zsAJgtWI9dZWSC8Bkw8fm8M4JCdsEZFHJ+q8/OUN4SrSchd:uITfG2oSN+NJ6NONDW4d
MD5:	F05BBAA43305E52C22B638C626429CEE
SHA1:	ADC413FB15971738D63DA3242A76A928736BA744
SHA-256:	BFFA763BD4699F69457D08DEDCF25380D22DB564F7B611F848DCEE4E1554C254
SHA-512:	37D59A8D1C016A13ABB0AC6A84EFFA0313FC1A87A64283B7C7290B6EA8AB8F30B5AE2C943F364DD39B5B9FEBF21790A5FE6DA648AA9E4484340C4D17A70868B5
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="1168213" />.. <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\WERC6A2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:03:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48630
Entropy (8bit):	2.168934706666154
Encrypted:	false
SSDEEP:	192:ITtFi69fjyWtTrIjapH4PxS8Klx3AgyWuXH7PnF3Mw:48UfjyWtTrIGt78KlxwgfaTBMw
MD5:	D293DE3E6419791ACB3147D0BDBD74EA
SHA1:	F89CBE2F1FAE2AA59F75B1D52F7ECCC63F24123A
SHA-256:	663682751B538AB7631488CB3CB65F1BFC95EAA5C9A8B79563B60E4C8146E708
SHA-512:	42A8ACB1C2AB0C2D7476FC72599304487483850A4DE51A9D849CD5D5F7E516AC20041181B796D80A595D0A00AB6DA83F051607D6397D0B99C57951C3B123426(
Malicious:	false
Preview:	MDMP..... ....._Ba.....U.....B.....%.....GenuineIntelW.....T.....0...._Ba.....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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC991.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):	8310
Entropy (8bit):	3.699034045450217
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5C6j6YC363xogmfT+S/iCprL89b7nbsf/50Opm:RrlsNic6j6Yi63+gmfT+Su7ngf/5Q
MD5:	DC602782E7176C4B002E00452DD2C391
SHA1:	3DE11A877794EE73A58FEDA02B54D3499AC2A54F
SHA-256:	90F82B5A981B11C582F567F432CBF5BE871D4ACBA3070F787CC820E7FA628953
SHA-512:	582FD700461F563582D52EC19C608BC5DD874BBF92E1016AA0BFA40971B6C42362686DBF039B371629A3CDC963605903D56A80139C8D3CC461EF4E8272127635
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.>.6.1.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.491960778876212
Encrypted:	false
SSDEEP:	48:cvIwSD8zsAJgtWI9dZWSC8Bz8fm8M4JCdsEZFy6+q8/OU7n4SrSWd:uITfG2oSNGJ6u6OjDWWd
MD5:	78390C2962AC5FEFE7967D1C6A1A3F96
SHA1:	F91E534E18D6D057D14D35DD2F44D0894FCFF98D
SHA-256:	73C05159ECCD1C8CD938CE71B9E7D731A323EA2A6E2E301A726397FC3608D9CC
SHA-512:	9BEB07049740E0C566EE7C386896708378F1E54D3409B7D679E59AC8F36FD360A934F97B53AEA73AB2B30BF9211958D0C550FB5D32B2956DC3875A9902967D42
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="1168213" />.. <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" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.102957541893627
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.Agent.FHBA.20741.dll
File size:	4608
MD5:	4b59be3cef04547514828f8c6443ae20
SHA1:	bed0d3a622ca55a914ceaf885ebc2fb419e8a9eb
SHA256:	b7ca395f51df95bd3d5b5b4a30a5c2381a9893f0d66aff011d605319d5c0ea7d
SHA512:	5aabf0b4b62e7ec664cc0787eac599fb507b2d79a9967e94244fedecbfd42205de00f29c567679e50247293e0067549e2a6c4b37fa943bf7609df2aa598383eb
SSDEEP:	48:iswv7jh9qy/njLFg2jSzhqh+hQaFLi/vMTaplZcCIIISwFlJfzm7W475d2:/wLqyHFgURgb+NUwFlJfzmW47r2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O0K..^...^...^..E_...^..._...^..GZ...^..G^...^..G\...^.Rich..^.....PE..L...a..`.....!..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, NX_COMPAT
Time Stamp:	0x60931161 [Wed May 5 21:42:57 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	8b1a65dc59feff9ba4c412ec478b377b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d6	0x400	False	0.498046875	data	4.58066088703	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x840	0xa00	False	0.41171875	data	4.11239200133	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6680 Parent PID: 5716

General

Start time:	14:02:56
Start date:	15/09/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll'
Imagebase:	0x970000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6812 Parent PID: 6680

General

Start time:	14:02:56
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.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: 6820 Parent PID: 6680

General

Start time:	14:02:56
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll, uvlcopdlxoed
Imagebase:	0x9e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6780 Parent PID: 6812

General

Start time:	14:02:57
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll',#1
Imagebase:	0x9e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: WerFault.exe PID: 4312 Parent PID: 6820

General

Start time:	14:03:00
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6820 -s 804
Imagebase:	0xf90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 6200 Parent PID: 6780

General

Start time:	14:03:00
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6780 -s 816
Imagebase:	0xf90000

File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: rundll32.exe PID: 6192 Parent PID: 6680

General

Start time:	14:03:00
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Agent.FHBA.20741.dll',uvlcopdlxoed
Imagebase:	0x9e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: WerFault.exe PID: 5780 Parent PID: 6192

General

Start time:	14:03:04
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6192 -s 804
Imagebase:	0xf90000
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

Disassembly

Code Analysis