ID: 483796
Sample Name:
SecuriteInfo.com.Trojan.Loader.788.32290.4876
Cookbook: default.jbs
Time: 13:52:25
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

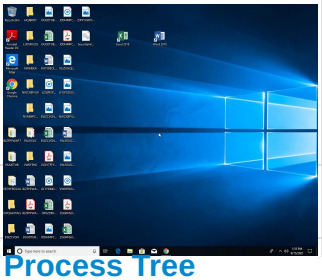
Windows Analysis Report SecuriteInfo.com.Trojan.Load…

Overview

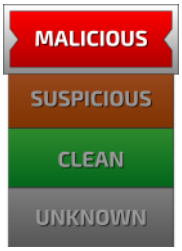
General Information

Sample Name:	SecuriteInfo.com.Trojan.Loader.788.32290.4876 (renamed file extension from 4876 to dll)
Analysis ID:	483796
MD5:	ab4dabb7296c60..
SHA1:	3a71cbe4e689ea..
SHA256:	58d3533e94bd90..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

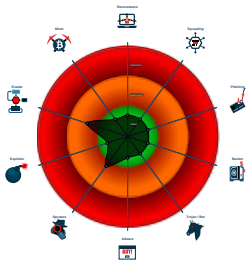


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Monitors certain registry keys / valu…
- 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: 1708 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5248 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3440 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1848 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3440 -s 724 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 2296 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll,uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 780 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2296 -s 716 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1008 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5284 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1008 -s 716 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

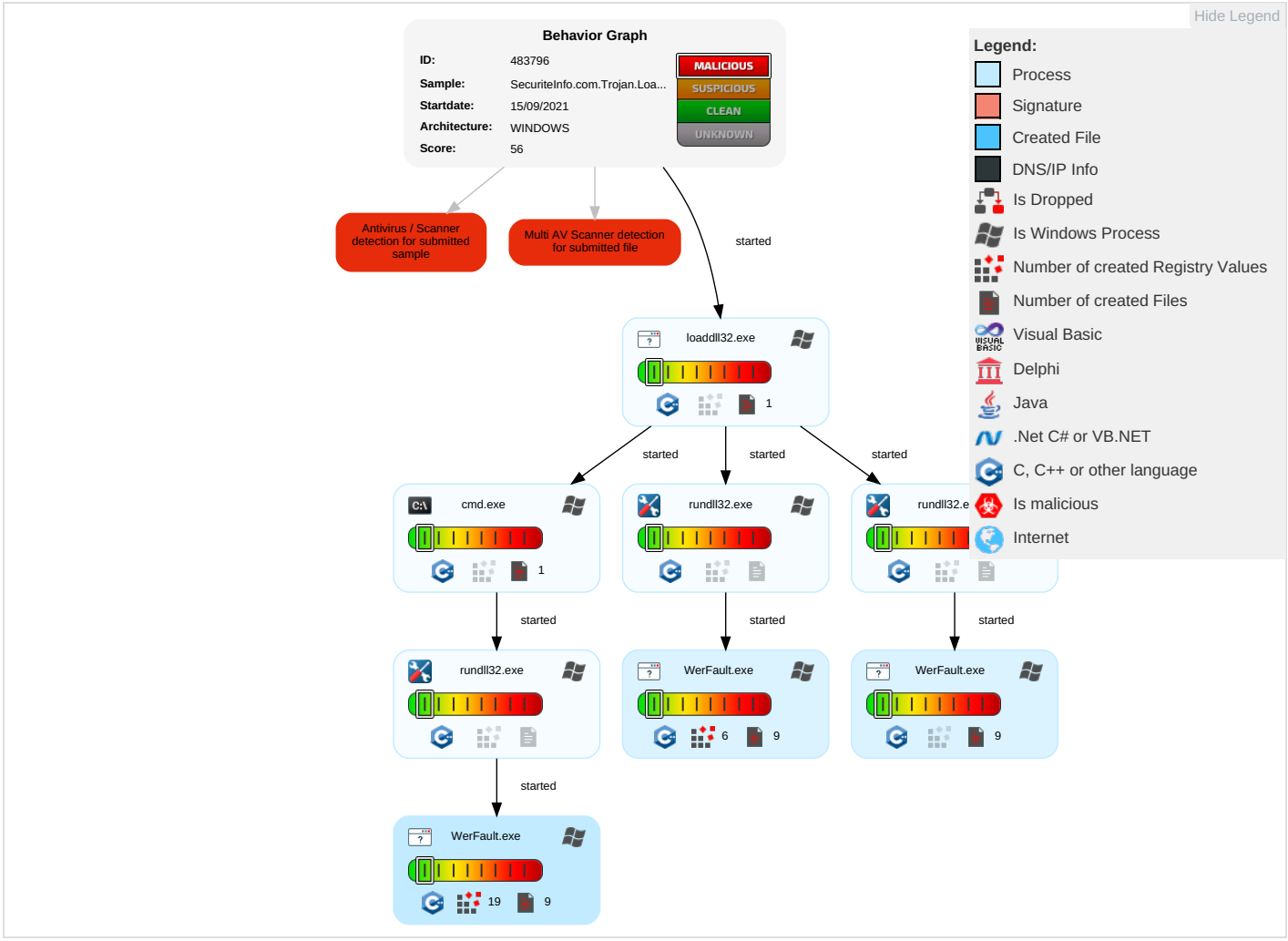
Multi AV Scanner detection for submitted file

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	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph

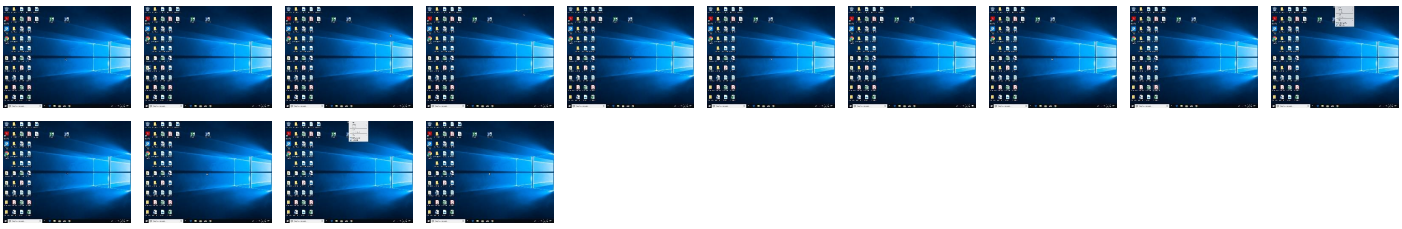
Copyright Joe Security LLC 2021



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.Loader.788.32290.dll	42%	Virustotal		Browse
SecuriteInfo.com.Trojan.Loader.788.32290.dll	75%	ReversingLabs	Win32.Trojan.Spynoon	
SecuriteInfo.com.Trojan.Loader.788.32290.dll	100%	Avira	TR/Injector.nhqlj	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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:	483796
Start date:	15.09.2021
Start time:	13:52:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Loader.788.32290.4876 (renamed file extension from 4876 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:	35
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: 76.6% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:53:35	API Interceptor	1x Sleep call for process: loaddll32.exe modified
13:53:38	API Interceptor	3x Sleep call for process: WerFault.exe modified

Copyright Joe Security LLC 2021

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_70ca6d92bb7cd6d05a398077544511f8e964d76_82810a17_035c146d\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12054
Entropy (8bit):	3.7682059970537845
Encrypted:	false
SSDEEP:	192:RK7ioe0oXuHBUZMX4jed+2/u7sxS274lt7cOj:0iVXmBUZMX4jer/u7sxX4lt7cOj
MD5:	86BD6549A7E27119E4A3E9DDF4A977B7
SHA1:	8CEEA87A087935532EF6FE002D08C88EB5DAC39E
SHA-256:	353D6E6BF581AE9EBC69F8FF3407232DCECBC4E76A014765324702A9E832B4AA
SHA-512:	A7094EEDDC9CC060CDBC03A769C2263B10A33A9884B22FFB6682309D834D27627032CB9BE591C674DAF580DABAEFAD3FB7CE194585B793976BD77C99BF9970B
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.2.1.2.8.1.6.0.0.3.9.8.8.5.....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.=.1.3.2.7.6.2.1.2.8.1.7.2.5.3.9.7.6.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.b.8.5.8.d.2.3.-.e.3.c.e.-.4.0.e.a.-.9.3.2.e.-.9.3.b.e.2.0.3.0.f.5.d.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.f.9.c.c.5.8.c.-.f.3.5.5.-.4.9.2.5.-.b.2.d.c.-.a.b.9.0.5.5.7.c.c.7.a.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.f.8.-.0.0.0.1.-.0.0.1.7.-.b.b.6.3.-.c.3.b.d.7.3.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.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_70ca6d92bb7cd6d05a398077544511f8e964d76_82810a17_07680eef\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12058
Entropy (8bit):	3.7663689980206785
Encrypted:	false
SSDEEP:	192:zjGfie0oXoHBUZMX4jed+W/u7sxS274lt7cp:mfioXQBUZMX4jeL/u7sxX4lt7cp
MD5:	FF49F91FF9717087EC08F0DCDA859EA3
SHA1:	3E30A9E01C88CC8F07D9BEF114468C33AB79CE72
SHA-256:	F05D1D14B55BE37B5657EF2B7343683FA70F6E2D10D24770D4C7EB865BDB3C4D
SHA-512:	C820D689C5BFE807905F62484520F55D398721F15DB710D75CD6449DC735FB21C64F9340A6537DDF09A007558D285CFCB1EEE018662A66593F0C598EC6B9A831
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_70ca6d92bb7cd6d05a398077544511f8e964d76_82810a17_07680eef\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.2.1.2.8.1.6.2.3.9.0.3.8.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.6.2.1.2.8.1.7.4.4.2.1.4.8.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.e.d.2.9.2.9.-.b.9.8.9.-.4.7.4.9.-.a.f.e.0.-.f.9.c.9.f.1.a.0.b.0.2.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.5.8.3.9.d.6.3.-.c.2.3.f.-.4.e.8.7.-.8.7.c.7.-.a.0.7.3.a.0.b.a.e.b.b.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.7.0.-.0.0.0.1.-.0.0.1.7.-.6.e.3.f.-.c.8.b.d.7.3.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.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_70ca6d92bb7cd6d05a398077544511f8e964d76_82810a17_14f41a2a\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12056
Entropy (8bit):	3.7692159594188963
Encrypted:	false
SSDEEP:	192:PiJin0oXpHBUZMX4jed+2/u7sxS274lt7cb:PYiZXZBUZMX4jer/u7sxX4lt7cb
MD5:	E901566F9DEFF5EB99704D6C0D368A45
SHA1:	296E07F22C1CF49446AF6C6751A28A27F655B789
SHA-256:	C5B61422644920ED8A2FD877283BD9017266B8CA87B3089E2AD0C5AA39C5B58D
SHA-512:	0EF020FD7A734B537B475B917593EBA3D590D9F304D4E9B92AC3C37DC15F14A4C01963CD527AF83EF2830BC49738025A475BA20B91DF58053869A66AE9E8EDE
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.2.1.2.8.1.8.5.9.3.8.4.9.5.....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.=.1.3.2.7.6.2.1.2.8.2.0.2.8.1.3.8.3.0.....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.=.b.f.a.d.0.5.3.1.-.3.7.d.9.-.4.3.a.c.-.8.5.1.9.-.d.b.f.f.7.b.b.5.7.b.3.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.=.e.e.7.b.7.8.e.3.-.1.b.7.c.-.4.e.2.6.-.9.4.5.7.-.9.9.2.d.4.6.5.b.7.7.5.4.....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.=.0.0.0.0.0.3.f.0.-.0.0.0.1.-.0.0.1.7.-.3.5.b.f.-.c.9.b.f.7.3.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.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1355.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8350
Entropy (8bit):	3.6936358656587402
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMV476RT6YsG6Gkgmf8eSULCprD89bASsfbgm:RrlsNiMK76l6Yt6Fgmf8eS0ARf5
MD5:	80F1D885C49D9C1EC8A669A5B64AFF0B
SHA1:	62389C2AB6262E29AE4D081F33D3E8F7C70074FD
SHA-256:	B8DFE63CAAF170279CBE2343571827B37FF21B1026B109938080F2CB089CD902
SHA-512:	BEB1E88D158E6334CF561690B90C44F568A3E08DFF8BAE3C709B6BAC914D0E3D5F5976EE2AC78C65A94BA928FC4B4A2B1DB2B5FBD63CA0856A0CFD6642859628
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.>.1.0.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER14EC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.482621902564733
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9sKWSC8BB8fm8M4JCds0MFD9G+q8vjs0+/4SrSWd:uITfKTrSN8Jy9KtyDWWd
MD5:	DF2EBAC1356D5234DBF6BFFEEB831E79
SHA1:	9D4F889F3E18EBA9A3CBF114729448EC223254E4
SHA-256:	78F21DD61CD2CAB39F9E04F62B56FD812B44E38B6A08007C6D25C1060E17D679
SHA-512:	C5B26271E8B4569033F8B5A997A3E7639FD21000927888768E21120E59CDC1ACC5E162091408F1C7E86510151E2A1E40C33E295A4D066435700B34D01211FFC6
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER14EC.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="1168204" />.. <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\WER598.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 20:53:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45656
Entropy (8bit):	2.0950508424754974
Encrypted:	false
SSDEEP:	192:rHJySCjl5KngWoYjOjranVMznIhedXmm7YWo32n/cx:E14gWoYjO0ezgedl7Ykkx
MD5:	B67508136C326CB677E34B3AAC0F2E3E
SHA1:	9C79D30CF3675FAEC5EE7FC81112DE254C0B136C
SHA-256:	4D89A57A9B56A60326412F3212205D0E389B6BAB6E99CFCDAA0FED0CA9CB4EFD
SHA-512:	11487B622919183CF4B9246AECF6F8E3FFBD21B49E12BCB53CBBA992976609584C3EBB3016FF9D9219F7D2095C0FFB4C624ED64035289F3D9B7F8018CED1532
Malicious:	false
Preview:	MDMP..... .....P]Ba.....U.....B.....GenuineIntelW.....T.....K]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\WER682.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 20:53:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	44400
Entropy (8bit):	2.1565002610099397
Encrypted:	false
SSDEEP:	192:Q9jGzCnwipenYYro887/VsnVMznIheF36mXoRwpoZnrAl:YjGzmwipqqtp2ezgeFJXoRwQrAl
MD5:	80CAE7E73B80D05DA2C3A26C20BB81E2
SHA1:	26AC82249A95C87C2C66B1B8087970E18552D44E
SHA-256:	2E3C888DFBD7D838E3AD431B1C15C94C5FCA00667F7EA1122CDF767DC8C69521
SHA-512:	32F21EDE2621035FFEEE78C8F4B06579D64D73025A885BF5C27B0981543BC41ABC82EE388BDE8073EA545AB1951E6B60F2C315DEDDF99388F4F3A10A48BC674
Malicious:	false
Preview:	MDMP..... .....P]Ba.....U.....B.....GenuineIntelW.....T.....p...K]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\WER923.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8350
Entropy (8bit):	3.69247674327344
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiCK6OPQsDe6YsJ6Gkgmf8eSULCprP89bO7sfs6m:RrlsNiv6n6YS6Fgmf8eSQOAfQ
MD5:	1D722310DA0BE6C77B1A583B512CF5E0
SHA1:	465F562C0D0AFA6FC70C511FD71CEC6552EC42F8
SHA-256:	336E2F48B3D17B8ACDF7B2A307357562C43DD1A1E444E5BC6B6B59716F611589
SHA-512:	7F557348979B3A27C521ED5CA166CDEEF1AF6D1417E2D0EBA35282F627613E7A8E32D35B225ABE38468955DB2CA66CB0BCB36A9E376F76DE5890D0FC4E330D5
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.>.2.2.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CF.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):	8354
Entropy (8bit):	3.693517483856706
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+76yPQJ6Yon69gmf8eSULCpr589bO3sfh6m:RrlsNii676YY69gmf8eSWO8fd
MD5:	3C9941FD1111189E866CE851CB48BCF5
SHA1:	756CE3AA51FD855CF3EC6EC742F67C187BC0B816
SHA-256:	6D903703B561E450D699A37BE1B3CFED440BDDDB7CBBFA193382A77640DC75E5
SHA-512:	19FB44B078A279DCE10994883690980E7B350C065016BEB5DDB24EDEEFC3747D428FA15D12D7C6C6F240BBEE0A846DDAC9306F1E20E1893CCA427604CEC8A97
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.4.4.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.481897753406463
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9sKWSC8Bpa8fm8M4JCds0MFL+q8vjs0dEzn4SrS1d:uITfKTrSNzJyyKtWDW1d
MD5:	01311CAD72C0BC8B0D021426C1971DD5
SHA1:	0C79FCB1CAFEC26B639CFED9713730687693FC2B
SHA-256:	F83F36E2796F7C4DBFA72217987C73581C3FD0E3E17CCF4F7C18ABADB4DE1C66
SHA-512:	CF78EF0988774A1444E862E7DD29F5452434FB4593D9F6E0A5ECF50B5EAB5A5BB603F8476FF7B5771B94A534A0586E7D6084A1B377E6E9EE114FEB5124F12B00
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="1168204" />.. <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\WERA9B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.479597922489219
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9sKWSC8BR8fm8M4JCds0MFKG+q8vjs0Ln4SrSXd:uITfKTrSNwJyGKtzDWXd
MD5:	65E8BF104530B0174CAB4EBA03F0A7F8
SHA1:	0897C25B30107CD27C06E20625DA6D2D3AF8F9D8
SHA-256:	07DA9F76FC3473D8FC60D5661583AF0494EAD0965D4DB9178971154B4899C95C
SHA-512:	3E0F3366B89301017B71A82E398B8A950DDE37D1DC1308E1FFD4339975F8464CC195278FC721AC8E275832D7DF0378052414B10D50B4D432AC4B82009422BEF5
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="1168204" />.. <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\WERFAA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 20:53:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48384
Entropy (8bit):	2.0046509514616377
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAA.tmp.dmp	
SSDEEP:	192:lrXzU1AeWpMvnVMznlhe+X8Atfrq0ElzUQEs:gXzm5WpM/ezge+s+f+0EdUs
MD5:	B05604691E9562343EC1EE6E756758B4
SHA1:	2E1E973EACEF5BF0E7FB4D65D943B41F3B5E06D1
SHA-256:	1313D1C545BC25DA739DBE36796D3FB92D6A1DA037D29DBDF4BBC3E5257B9779
SHA-512:	6DE0B8FD5A28D00BB2D15D2226E71B1B9CE0EDA5C11AD22C439C0A8C506DA430B8494474E935861955F1D75B4DF7F01902BB5BC1763747BE7C3F55C704886D
Malicious:	false
Preview:	MDMP..... .....S]Ba.....U.....B.....GenuineIntelW.....T.....N]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..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.612809244096079
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.Loader.788.32290.dll
File size:	6144
MD5:	ab4dabb7296c60f618a8bba9ec194659
SHA1:	3a71cbe4e689eab68fb642bb94a4995102b03a9d
SHA256:	58d3533e94bd90a6aaff46e76f8f264f63aebd84ea246ab5074a32457e3ba39b
SHA512:	ec791043f95ca06804aed549d3f6414a2605ad85ba7e1d06fd14357a9bd5234ed60cb4f28d89fcc6680801ee8cae2282cdb7c79927d830e15ad9753c8e356b75
SSDEEP:	96:/an1ASk3NDZ+tCiq5RSKKgHCgQNLJ2L8ipKvrD3:/dgqTSHg+d2LKjD3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sA.....Rich..... PE..L...O..`.....!.....

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:	0x6090924F [Tue May 4 00:16:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6

General

Subsystem Version Minor:	0
Import Hash:	68cb0529e8a62fbcd192ffb1ba826877

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x694	0x800	False	0.46533203125	data	5.07347132918	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x98e	0xa00	False	0.4578125	data	4.64118874162	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x354	0x200	False	0.1171875	data	0.557168346014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, 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: 1708 Parent PID: 2416

General

Start time:	13:53:30
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.Loader.788.32290.dll'
Imagebase:	0xf40000
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: 5248 Parent PID: 1708

General

Start time:	13:53:30
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.Loader.788.32290.dll',#1
Imagebase:	0xbd0000
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: 2296 Parent PID: 1708

General

Start time:	13:53:31
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.Loader.788.32290.dll,uvlcopdlxoed
Imagebase:	0x260000
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: 3440 Parent PID: 5248

General

Start time:	13:53:31
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.Loader.788.32290.dll',#1
Imagebase:	0x260000
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: 780 Parent PID: 2296

General

Start time:	13:53:34
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2296 -s 716
Imagebase:	0x260000
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: rundll32.exe PID: 1008 Parent PID: 1708

General

Start time:	13:53:34
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.Loader.788.32290.dll',uvlcopdlxoed
Imagebase:	0x260000
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: 1848 Parent PID: 3440

General

Start time:	13:53:34
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3440 -s 724
Imagebase:	0x260000
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: 5284 Parent PID: 1008

General

Start time:	13:53:38
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1008 -s 716
Imagebase:	0x260000
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

Copyright Joe Security LLC 2021

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021