ID: 483796
Sample Name:
SecuriteInfo.com.Trojan.Loader.788.32290.dll
Cookbook: default.jbs
Time: 13:58:57
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Trojan.Loader.788.32290.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Jbx Signature Overview 5
AV Detection: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 14
Sections 14
Imports 14
Exports 14
Network Behavior 14
Network Port Distribution 14
UDP Packets 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: loaddll32.exe PID: 6412 Parent PID: 2500 14
General 14
File Activities 15
Analysis Process: cmd.exe PID: 6432 Parent PID: 6412 15
General 15
File Activities 15
Analysis Process: rundll32.exe PID: 6444 Parent PID: 6412 15
General 15
File Activities 15
File Read 15
Analysis Process: rundll32.exe PID: 6456 Parent PID: 6432 15
General 15
File Activities 16
File Read 16
Analysis Process: WerFault.exe PID: 6680 Parent PID: 6456 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
Registry Activities 16
Key Created 16
Key Value Created 16

Analysis Process: rundll32.exe PID: 6708 Parent PID: 6412 16
General 16
File Activities 17
File Read 17
Analysis Process: WerFault.exe PID: 6792 Parent PID: 6444 17
General 17
File Activities 17
File Created 17
File Deleted 17
File Written 17
Registry Activities 17
Key Created 17
Analysis Process: WerFault.exe PID: 6960 Parent PID: 6708 17
General 17
File Activities 17
File Created 17
File Deleted 18
File Written 18
Registry Activities 18
Key Created 18
Disassembly 18
Code Analysis 18

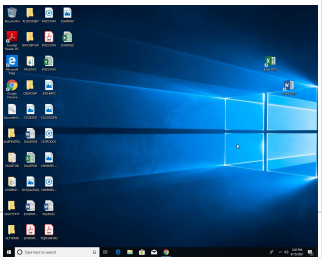
Windows Analysis Report SecuriteInfo.com.Trojan.Load…

Overview

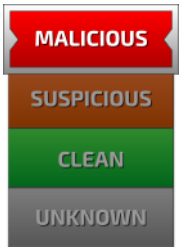
General Information

Sample Name:	SecuriteInfo.com.Trojan.Loader.788.32290.dll
Analysis ID:	483796
MD5:	ab4dabb7296c60..
SHA1:	3a71cbe4e689ea..
SHA256:	58d3533e94bd90..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

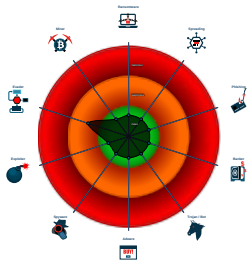


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6412 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6432 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6456 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6680 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6456 -s 724 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6444 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll,uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6792 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6444 -s 716 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6708 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Loader.788.32290.dll',uvlcopdlxoed MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6960 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6708 -s 716 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:

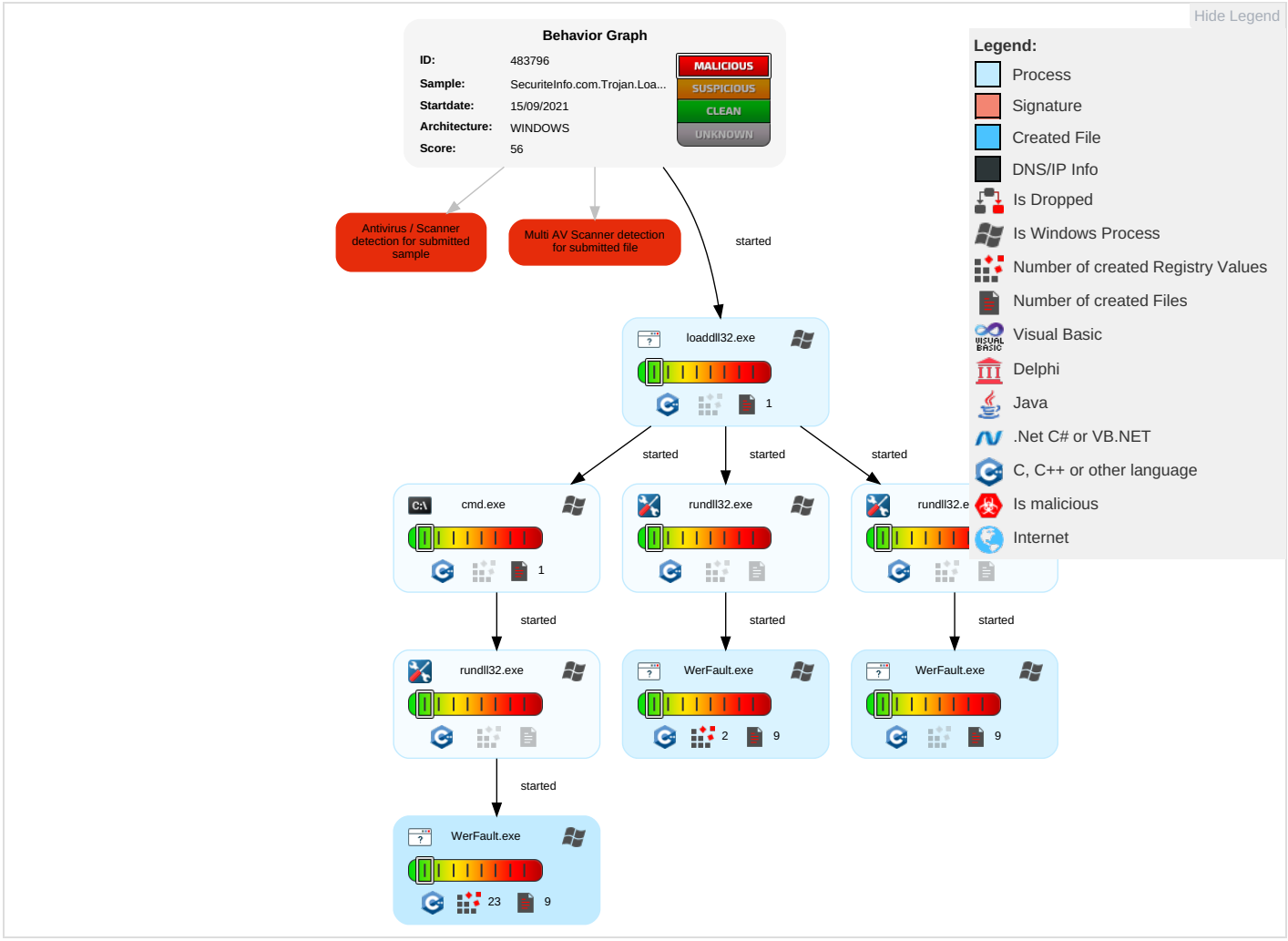
Antivirus / Scanner detection for submitted sample

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	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	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 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



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	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

Source	Detection	Scanner	Label	Link
http://https://watson.telemetry.microsoft	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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:	13:58:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Loader.788.32290.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:	40
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 • 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_69688d2812e06195cef530d1f4e704d7e967697_82810a17_1a0173ec\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):	3.765198868051731
Encrypted:	false
SSDEEP:	192:/VRi10oXiHBUZMX4jed+i/u7s1S274It7cs:9RibX6BUZMX4jeX/u7s1X4It7cs
MD5:	518328E26C8FF6501C25B712A417B90B
SHA1:	AB56DAF80C5F2025748160BE8742A8722D8E90EA
SHA-256:	F200732BD0213631E29DBCC7172110B02255EC643819DA0879B56A10DD060AD8
SHA-512:	76A6CD5B1E2302F14496B34F4A512DE582964DB0433D98FB4B5D8C993A4CECA70EEFA925BD0296D43AFEB8546BFD64637226A03C64D365326862745E82DF643
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.=.1.3.2.7.6.2.1.3.2.0.5.8.1.4.2.3.7.3.....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.=.1.3.2.7.6.2.1.3.2.2.0.7.6.7.3.8.2.4.....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.=.3.0.f.4.1.9.0.7.-.b.d.2.0.-.4.c.a.0.-.9.a.9.9.-.d.8.1.2.c.7.1.4.0.c.e.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.=.6.0.4.d.4.0.2.a.-.2.0.e.a.-.4.7.b.a.-.9.b.8.9.-.0.a.6.b.8.2.7.3.d.e.3.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.a.3.4.-.0.0.0.1.-.0.0.1.6.-.8.9.4.e.-.4.3.a.4.7.4.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_69688d2812e06195cef530d1f4e704d7e967697_82810a17_1b2952a8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12026
Entropy (8bit):	3.767189237668157
Encrypted:	false
SSDEEP:	192:b9Ri/0oXXHBUZMX4jed+q/u7saS274It7c0:ZRiBX3BUZMX4jeP/u7saX4It7c0
MD5:	DF8917A5C9FB0A30491F195D465F903A
SHA1:	1FB1EC02157FF948F19CDB4620E4599A5FE8E009
SHA-256:	B64DF1EF259B4A66E1224AFB99BA39F92A643B96941E62F30FE22A162E11754F
SHA-512:	AC616670F5A9CAD5261B0A68C77B4CE121A1017C2528EA6E17A7E82B4FAE140692BD2600A7B7C8CC975A586767A9728DA9BB7E712B333883F8F1FA398BBF842
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69688d2812e06195cef530d1f4e704d7e967697_82810a17_1b2952a8\Report.wer	
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.=.1.3.2.7.6.2.1.3.2.0.0.2.6.4.9.3.7.9.....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.=.1.3.2.7.6.2.1.3.2.1.1.9.0.5.5.4.9.0.....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.=.e.c.c.2.7.9.3.c.-.3.7.f.b.-.4.3.c.8.-.b.b.5.f.-.c.9.8.2.b.8.1.2.6.2.8.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.3.4.2.9.9.b.1.-.f.d.b.4.-.4.1.b.2.-.b.f.a.9.-.7.6.3.e.2.1.a.1.6.f.c.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.3.8.-.0.0.0.1.-.0.0.1.6.-.a.3.f.8.-.1.b.a.2.7.4.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_69688d2812e06195cef530d1f4e704d7e967697_82810a17_1bb9611f\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):	3.7662107313886293
Encrypted:	false
SSDEEP:	192:8+iF0oXHHBUZMX4jed+q/u7saS274It7cs:5iLXnBUZMX4jev/u7saX4It7cs
MD5:	7216EF1A79D9121B0AB5E270086BEE88
SHA1:	5F84DFF306DF6D5557CFF0E6C9B822814FC028B8
SHA-256:	C79CB51FE3332B4EB0AACB7EC702A97E1DE4618B62D30DB3288E8BCBBE0FCB69
SHA-512:	458A2A407CC706E308E5FAA11B0EC1AFF12731A4A9ECED4483A1B673C235C5D442A1B9F47E24E7D393533BEAAC37EDC640E31966B9166393FFC6EE33833F110B
Malicious:	false
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.=.1.3.2.7.6.2.1.3.2.0.1.7.5.3.8.2.7.3.....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.=.1.3.2.7.6.2.1.3.2.1.5.8.4.7.5.5.4.0.....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.=.f.c.8.f.e.7.d.6.-.9.6.9.6.-.4.3.7.e.-.8.9.4.f.-.6.6.b.b.1.3.1.b.3.e.7.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.=.e.5.6.b.4.f.a.5.-.6.7.6.6.-.4.b.3.0.-.a.c.6.5.-.e.b.b.f.2.a.3.4.6.3.5.5.....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.=.0.0.0.0.1.9.2.c.-.0.0.0.1.-.0.0.1.6.-.2.a.6.f.-.1.5.a.2.7.4.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\WER1DBD.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:00:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45132
Entropy (8bit):	2.133794980071242
Encrypted:	false
SSDEEP:	192:T3dhBD8lDw7L9WPdO1HWtMkuIQLrjW6sHpzUBRkyLnG:pDVL9WPQ42kYLrj6pzILG
MD5:	CB12C62AAC7334EAC7F06D9C23FB0C86
SHA1:	341D3B5C8C0694E6C6FDE79B00141E466683CBC7
SHA-256:	ABC8423DAEFC7E75AEF9696A2E6898B76895029F0C38F5837AA6B75C9FA43665
SHA-512:	291FB4B8DB3F1665C1435D4A0CC0AA6B9F51E9E719AB60827DE257FCE39E1A171C225807BF1C10323204E2E6519498055B58DB40228C1C99FFF677DC7AAE31E
Malicious:	false
Preview:	MDMP..... .....^Ba.....U.....B.....GenuineIntelW.....T.....8....^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\WER2399.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:00:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45260
Entropy (8bit):	2.108116615082561
Encrypted:	false
SSDEEP:	192:soAo0NQqfg0cUD1XA4U6lmWtMkuIQLrD9tEcyPaVhucnuO:jAtNQqIwBsW2kYLrDgcjucb
MD5:	BB5FFC5A63F5286023D8605196EDDED9
SHA1:	9715FEE0055EAA537847CDDD35A1F76C58FFB185
SHA-256:	56E337C0FF7FD28CC050416289FC8990CA2D446DF14D364737AA69932736BB67
SHA-512:	4BFB7A1C2D505CA52F638382841DB858839F6F5EF3C9E6B1DEDAA3E73C553BEBA5A85E397B1D1D24B2FE378286337CDBD159165E0596C6CC5A1BD720DEB57F1C
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2399.tmp.dmp	
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\WER2744.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):	8362
Entropy (8bit):	3.6978936929644113
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicF6nQ6Yw56rgmf8dSRCprv89buisfEVam:RrlsNiu6Q6Yu6rgmf8dSpuhfE5
MD5:	8163946A22BE4A1F5E4078463F1503BB
SHA1:	EB80E48077C2C406C98A35FDB90B8B478E6DE077
SHA-256:	922E92BBB9DF0D7EDAB47414CC1C290785A75DCA2BE7F9BB3A622EF76A7D674A
SHA-512:	B0D76674CF5158CEDA1BA408347C865B156FA6A59CB32654F88EBBBDE0735B07F22696B1C1250F342BD0C6F9FDBBAB3161778F64A23F55717CB1744F23226CC
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.>.6.4.5.6.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D5F.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):	4.484496088298751
Encrypted:	false
SSDEEP:	48:cvIwSD8zspJgtWI9oBKhWSC8Bqa8fm8M4JCdsjMFQ6+q8vjsjGn4SrS4d:uITf7/HSNQJJ4KOkDW4d
MD5:	E92DA7A2372614FEC84E23396FE7844B
SHA1:	E65FE2E3BD50EDDBDA3846155C652B92E12E4927
SHA-256:	CF49DF60679711E376977519EF5856387F0F78CC30AC74F90A364C497DF1BD49
SHA-512:	B8C7395F0760E64993F03EA3F0DBA1FE86E59EE4747411A96C4900467B62C0B23BE3204F4BFF7002D5EA94BA3EA199A2F952CF641AE5B3C4C7527CBB2ADB58A 6
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="1168210" />.. <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\WER326F.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):	8386
Entropy (8bit):	3.6961312652199747
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/z6g7ws6YDx6EBCGgmf8dSRCprO89bYisfqom:RrlsNi76I6Y16EVgmf8dS+Yhfk
MD5:	95C4FB8D38D4A3376BB8D8E0810C14A0
SHA1:	944667E85042FE576A14BE42C8B197F6542FB668
SHA-256:	5AEA9F76927FE1CD3EE1B35EAE7FBF332BC3F5E8678FB7FD3938BE717988B207
SHA-512:	49DA3E0A7AD868D7F1AD879012F700B27DC05B76161437EA1D57EB9421CB7414FE2A8A3856E99EA876C20E2DAC5448A6B4C9275E565962C128F6E757843E66E
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.>.6.4.4.4.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3368.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 21:00:11 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	53904
Entropy (8bit):	1.9317163376928401
Encrypted:	false
SSDEEP:	192:zLGYcAzw0of9QG3Z0xm9894l1rKQXRqedg51Eb0nYT:+YcA0d3Z0wW61rKQbg51TO
MD5:	222EA84DABB55A9C23022E127AD722B5
SHA1:	37D377ADF47C9C5B5104B4FAA287E697101CA796
SHA-256:	AF1F8798531D4998A32EF78A519EF60FB0F85332018A4E2B6B05AEAF20A896F1
SHA-512:	39AB35E76B7E7D21B12A9942A6361A3A7B8AFA1F051735A2B050B6D3DC81924585AB761E2ED9943D9A9EC0F4807B732B4AA343B5AF67855F4E84C7615EDCD3E7
Malicious:	false
Preview:	MDMP..... .....^Ba.....U.....B.....GenuineIntelW.....T.....4....^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\WER3629.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):	4.484975619046288
Encrypted:	false
SSDEEP:	48:cvIwSD8zspJgtWl9oBKhWSC8Br8fm8M4JCdsjMFAEV6+q8vjsjTEfn4SrSpd:uITf7/HSNmJJ66KOTEPDWpd
MD5:	6272F42437363467A46161C9F6274FB9
SHA1:	36AF21588AC46B6CDCFF1614196F30D3263AF206
SHA-256:	144B18529759450654CE183BC39530F56E6ED9A8439305B0FE3A7852ECC5CDE0
SHA-512:	5BBAB021F89A9616D20FA5538AA3349163F9F319A7A42125501385986A951609F3AF68059FEB1583CC2C0ED7C9ADF56BE4DCA1DC598BF28A93636D213A217716
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="1168210" />.. <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\WER4C12.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):	8386
Entropy (8bit):	3.6956392955336814
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNisk6Ww6YD56EBCGgmf8dSRCpr+89bGosfkmim:RrlsNi36R6Y96EVgmf8dSOGbfk6
MD5:	5FE8B652EF9B91DCE555D75606D96F63
SHA1:	8085D34F012562C2F0DF5EAA1C4EF4703BE8A539
SHA-256:	7CBBF839D369430996C40E8ED4451E7CDEB0578282D6ECF28BAC61A1A5B61AD6
SHA-512:	F7CB104AABA14D225C66AAC2909A4F129EC4A443D4DA02E55029F406C3C3C938378C81288E36E658F1D360663F1D02E8DAEC6788B8696D25E87BE2443E5FE11
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.>.6.7.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER502A.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):	4.481480377925222
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER502A.tmp.xml	
SSDEEP:	48:cvIwSD8zspJgtWl9oBKhWSC8BB8fm8M4JCdsjMFmj+q8vjsjTJI4SrSod:uITf7/HSNwJJfjKOT+DWod
MD5:	957712C6CD84465CF2A95E50419F0DB6
SHA1:	F734D33E1D1A1CF2208A8C7242F862533B6A8255
SHA-256:	C62C378E07DCBDA019E71B194B6138F6E6F6FCAB18011E453FD952EE3D42DC44
SHA-512:	9EDC449FF21B070D5818728870732683C28B9B7F907B645324E4360F1B7EA91D65C08F6C08A21C2CFBE8E5EC35AFBCC0CEC3E4679AEAD62B330C4D47650F857
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="1168210" />.. <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):	4.612809244096079
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: 6412 Parent PID: 2500

General

Start time:	13:59:53
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:	0xb80000
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: 6432 Parent PID: 6412

General

Start time:	13:59:53
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:	0x150000
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: 6444 Parent PID: 6412

General

Start time:	13:59:54
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:	0x1b0000
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: 6456 Parent PID: 6432

General

Start time:	13:59:54
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:	0x1b0000
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: 6680 Parent PID: 6456

General

Start time:	13:59:57
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6456 -s 724
Imagebase:	0x160000
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: 6708 Parent PID: 6412

General

Start time:	13:59:58
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:	0x1b0000
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: 6792 Parent PID: 6444

General

Start time:	13:59:58
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6444 -s 716
Imagebase:	0x160000
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

Analysis Process: WerFault.exe PID: 6960 Parent PID: 6708

General

Start time:	14:00:01
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6708 -s 716
Imagebase:	0x160000
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

Disassembly

Code Analysis