Malware Details

Malware Type - Windows Trojan

Malware Name: [csrss.exe](https://www.virustotal.com/gui/search/name%253Acsrss.exe)

Malware Description: csrss.exe is a hidden monitoring software that tracks your personal information such as credit card, social security number, ID, email addresses, websites that you surfed or surfing habits, IP addresses etc. This information can be sent to hackers or third parties to damage your computer by sending viruses, spyware, malware or use your personal information for criminal activities or fraud purchases. If its exe, it is a legitimate, also CSRSS.exe executable file is located in the C:\Windows\System32 folder. Any file named CSRSS.exe, which is located in any other folder than this, is undoubtedly a malware or fake file. The fake CSRSS.exe might be hiding anywhere in the system and snakingly spying on users or conducting other illicit activities. Since it disguises itself in the name of a legitimate and safe process, it is pretty challenging to detect the CSRSS.exe trojan. However, the system shows some common symptoms that might confirm the presence of Trojan malware. Here is the list of those indications: CPU usage suddenly rises than usual, the system lags frequently, your browser is bombarded with malicious pop-ups, a random window is opened without the user’s initiation and Redirection to untrustworthy or suspicious sites

MD5 : 695a0d416cdccad008acb2369b0165a2

SHA-256 : bf32e333d663fe20ab1c77d2f3f3af946fb159c51b1cd3b4b2afd6fc3e1897bb

File type : [Win32 EXE](https://www.virustotal.com/gui/search/tag%253Apeexe)

Magic : [PE32 executable for MS Windows (GUI) Intel 80386 32-bit](https://www.virustotal.com/gui/search/magic%253A%2522PE32%2520executable%2520for%2520MS%2520Windows%2520(GUI)%2520Intel%252080386%252032-bit%2522)

TrID : [Win64 Executable (generic)](https://www.virustotal.com/gui/search/trid%253A%2522Win64%2520Executable%2520(generic)%2522)

[Win32 Dynamic Link Library (generic)](https://www.virustotal.com/gui/search/trid%253A%2522Win32%2520Dynamic%2520Link%2520Library%2520(generic)%2522)

[Win16 NE executable (generic)](https://www.virustotal.com/gui/search/trid%253A%2522Win16%2520NE%2520executable%2520(generic)%2522)

[Win32 Executable (generic)](https://www.virustotal.com/gui/search/trid%253A%2522Win32%2520Executable%2520(generic)%2522)

[OS/2 Executable (generic)](https://www.virustotal.com/gui/search/trid%253A%2522OS%252F2%2520Executable%2520(generic)%2522)

File size : [1.52 MB (1593544 bytes)](https://www.virustotal.com/gui/search/size%253A1593544)

Target Machine:Intel 386 or later processors and compatible processors

Entry Point:158432

Creation Time:[2019-02-13 07:46:12](https://www.virustotal.com/gui/search/generated%253A%25222019-02-13T07%253A46%253A12%2522)

Imports: ADVAPI32.dll

KERNEL32.dll

GDI32.dll

USER32.dll

Entropy:7.398055076599121

Filetype:Data

Ref: <https://www.malwarefox.com/remove-csrss-exe/> and https://www.virustotal.com/

Yara Strings and Description

============================

1. This program cannot be run in DOS mode

-> It helps to identify if it is an Windows executable

2.http://ocsp.usertrust.com

-> This String references a URL Pattern

3.http://www.usertrust.com"

-> This String references a URL Pattern

4. Salt Lake City1

-> This String references a Address Pattern

5. kernel32.dll

> The genuine kernel32.dll file is a software component of Microsoft Windows by Microsoft.

> Kernel32.dll is able to monitor applications, record keyboard and mouse inputs, manipulate other programs and connect to the Internet.

Ref: <https://www.file.net/process/kernel32.dll.html>

6. advapi32.dll

the advapi32. dll file, usually located at the Windows\system32 folder, provides advanced Windows API functions related to Windows registry, services, applications and user accounts