SHADE MALWARE DETAILS

File Type	PE32 executable (GUI) Intel 80386, for MS Windows
Malware Type	Windows trojan
File name	Csrss.exe / v3x7voxudm.exe
Malicious	**True**
Size (bytes)	1593544
Entropy	7.398055076599121
Encrypted	False
Target Machine	Intel 386 or later processors and compatible processors
Entry Point	158432
Imports	ADVAPI32.dll, KERNEL32.dll, GDI32.dll, USER32.dll
Filetype	Data
MD5	695a0d416cdccad008acb2369b0165a2
SHA1	C9002f65273ac587f5753f50cf61911885d92521
SHA256	Bf32e333d663fe20ab1c77d2f3f3af946fb159c51b1cd3b4b2afd6fc3e1897bb
Architecture	Image_file_machine_i386
Subsystem	Image_subsystem_windows_gui
Administrator privileges	True
Programmed in	C, C++ or other language
Reputation	Low
Entrypoint Section	.Text
TrID	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
SSDEEP	24576:kcDD3THmsmB7K1k52fzgtv0HqIYG3yC3Q1KbeRho7KWU8RKDyAlAY:bTHmsq72zgtv0HYG37bD7KWU8UhV
Imports Hash	3d5653e951869b517f5970bc8af2ea09
Signature	PE (The PE's digital signature is invalid.)
Digitally signed:	True (Signer: AEQATRXK, Issuer: AEQATRXK (The file was modified after it was signed.))
Signature Validation Error	The digital signature of the object did not verify

Functions which are commonly using malware files are identified and are listed below.

The program may be hiding some of its imports:

- GetProcAddress
- LoadLibraryW
- LoadLibraryA

Can access the registry:

- RegOpenKeyExA
- RegQueryValueExW

Uses functions commonly found in keyloggers:

- GetForegroundWindow
- GetAsyncKeyState

Memory manipulation functions often used by packers:

- VirtualAlloc
- VirtualProtect

Malware Description: CSRSS.exe is the executable file of the legitimate Windows OS process, known as Client Server Runtime Subsystem (CSRSS). This is an essential process that handles the majority of the graphical instruction sets of the Windows operating system. However, since it is a common and critical system process, many cyber attackers take advantage of it and release the malicious Trojan program sneaking in the CSRSS.exe name. 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 site.

Malware symptoms

- 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.
- Redirection to untrustworthy or suspicious sites.

To verify the presence of a fake CSRSS.exe File there are two ways. The first is the location of the file. The original, legitimate 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 second way is through Task Manager. Follow these steps:

- Launch Task Manager.
- Under the Process tab, look for CSRSS.exe or Client Server Runtime Subsystem process.
- Right-click on the file and click on Delete.
- If Windows prompts you with a warning box, then it is a legit CSRSS.exe process. If Windows does not show any warning box, then the CSRSS.exe process is fake.

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

YARA STRINGS AND DESCRIPTION

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

YARA RULE FOR SHADE MALWARE

```
 rule ananthuYaraRule{
   meta:
      Description = "Simple YARA rule to detect shade malware"
      Author = "Ananthu.R.krishnan (MT20ACS493)"
      Date = "2021-08-25"
      hash1 = "bf32e333d663fe20ab1c77d2f3f3af946fb159c51b1cd3b4b2afd6fc3e1897bb"

   strings:
      $url1 = "http://www.usertrust.com1" fullword ascii
      $url2 = "http://ocsp.usertrust.com0" fullword ascii
      $url3 = "1http://crl.usertrust.com/"
      $str1 = "AEQATRXK" fullword ascii
      $str2 = "AEQATRXK0" fullword ascii
      $str3 = "The USERTRUST Network1!0" fullword ascii
      $str4 = "UTN-USERFirst-Object0"
      $process1 = "GetProcAddress" fullword ascii
      $process2 = "LoadLibraryW" fullword  ascii
      $process3 = "LoadLibraryA" fullword ascii
      $process4 = "RegOpenKeyExA" fullword ascii
      $process5 = "RegQueryValueExW" fullword ascii
      $process6 = "GetForegroundWindow" fullword ascii
      $process7 = "GetAsyncKeyState" fullword ascii
      $process8 = "VirtualAlloc" fullword ascii
      $process9 = "VirtualProtect" fullword ascii
      $dll1 = "USER32.dll" nocase ascii wide fullword
      $dll2 = "GDI32.dll" nocase ascii wide fullword
      $dll3 = "ADVAPI32.dll" nocase ascii wide fullword
      $dll4 = "KERNEL32.dll" nocase ascii wide fullword

   condition:
      uint16(0) == 0x5a4d and filesize < 5000KB
      and 2 of ($url*) and 3 of ($str*)
      and 6 of ($process*)  and 3 of ($dll*)
}
```

1. ($url*) :- This Strings references a URL Pattern.
2. ($str*) :- This Strings references signature names and interesting strings.
3. ($process*) :- This Strings references the names of Functions which are commonly using malware files.
4. ($dll*) :- This Strings references dynamic link library names.

Ref: https://yara.readthedocs.io/en/stable/writingrules.html