Trojan-Downloader.Win32.Agent.mee

This dangerous program is a trojan. It is a Windows PE file. The size of the infected file can range from 70KB to 260KB.

Detection date: March 28, 2008

Specifications

This dangerous program is a trojan. It is a Windows PE file. The size of the infected file can range from 70KB to 260KB. It is not compressed and written in Delphi.

Setting

At startup, the trojan copies itself to the " **intetsrv** " subdirectory of the Windows directory with the name " ***lsass.exe*** "

% System% inetsrvlsass.exe

Two " **Hidden** " and " **read only** " attributes are assigned to this file.

To ensure that this Trojan is automatically started every time the system restarts, it will register its executable file into the registry as follows:

[HKCUSoftwareMicrosoftWindows NTCurrentVersionWindows]
"load" = "% System% inetsrvlsass.exe"

This key ensures that the Trojan will be started before the user accesses Windows

The Trojan also creates a unique value, " **izokraSizokras** ", to identify the signal for its presence in the system.

It creates the following registry key:

[HKLMSoftwareMicrosoftInternet Explorerinet.]
"Day" = ""

Work

The Trojan copies itself to all logical drives, removable drives, network drives (writable) as follows:

: MSOCache90000804-6000-11D3-8CFE-0150048383C9lsass.exe

pointing to the drive

It also adds the following file to each root of each drive:

: autorun.inf

This file will launch the trojan executable file every time the user opens the infected drive by clicking directly on the drive.

" **Hidden** " and " **Read only** " attributes are assigned to all files created by Trojans.

Instructions for removal

If your computer does not have an antivirus program updated regularly, or does not have an effective antivirus solution, the following guide will help you delete it:

1. Use **Task Manager** to determine the Trojan's progress

2. Delete the following registry keys:

[HKLMSoftwareMicrosoftInternet Explorerinet.]
"Day" = ""

3. Delete the following registry parameter values:

[HKCUSoftwareMicrosoftWindows NTCurrentVersionWindows]
"load" = "% System% inetsrvlsass.exe"

4. Delete the original Trojan file (the path depends on how the original program infected the system)

5. Delete the following files:

% System% inetsrvlsass.exe
: MSOCache90000804-6000-11D3-8CFE-0150048383C9lsass.exe
: autorun.inf

6. Update antivirus database and perform a "full scan" scan.

You finished reading the article "**Trojan-Downloader.Win32.Agent.mee**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.