Instructions for removing fake Antimalware security software

This is one of the most dangerous variants of the WiniSoft series, and is also a copy of the System Veteran malicious application.

QuanTriMang.com - This is one of the most dangerous variants of the WiniSoft series, and is also a copy of the System Veteran malicious application . On the other hand, AntiAid is one of the last versions of this malicious malware, with a lot of graphical interface improvements - Graphical User Interface (GUI):

The main interface of Antimalware

In fact, this is the second time the 'original' author of WiniSoft has improved the dangerous features. With the AntiAid variant, they are inherited and used GUI from TRE Antivirus. This same feature is also being used by other WiniSoft malware streams such as System Warrior or Trust Fighter. In fact, the AntiAid home page is Antiaid.com, and from this source, countless fake applications called Virus Protector have been released. It can be easily 2 main purposes of AntiAid is to try to infiltrate the victim's computer as silently and discreetly as possible and to find ways to let users hook up to buy copyright. Programs like AntiAid regularly work in the system as securely as possible to avoid user detection and security programs.

In essence, AntiAid uses Trojans to infect a victim's computer, they can be extremely cleverly disguised in any form of safety program: flash, codec decoders, live security services. online . When downloaded to your computer, AntiAid will create a lot of fake files in system folders like **C: Windows** and **C: WindowsSystem32** . These first files are actually not harmful, but if not prevented and removed in time, AntiAid will continue to use them to infect and exploit security holes later on. First, the malware will change the registry keys needed to automatically activate the same boot mechanism, then constantly perform the entire computer scan and display error messages based on the files. The report was previously created, such as **newfeat3.chm** . On the other hand, AntiAid continues to "impersonate" the role of the default Windows Security Center application system. At that time, users will meet countless information in the form of popup, security warning . about the status of virus, spyware has penetrated the system, how serious it is . even when the user does not connect. Internet connection. And when you accidentally or intentionally clicked on those messages, you "pulled" more malware and Trojans to your computer.

Some typical signs of computers have been infected with Anti Malware

- All security and security programs available on the computer are blocked, deactivated, even updates are not possible.

- Prevent access to websites with built-in online security tools or services

- Gradually all browsers on the system are paralyzed

- Lock function of system applications such as System Restore, Safe Mode, Task Manager, Registry Editor (only available in SafeMode mode)

- On the Desktop screen will appear many strange shortcuts, when the user clicks on it, will automatically point to the address that was prepared by hackers.

- Automatically change all homepage homepage addresses in the browser

- Every computer activity becomes heavy, slow, even the restart time and speed of Internet connection

- Most cases are infected, the computer will restart itself several times

After analyzing and conducting many tests, security experts of security companies recommend users to use Spyware Doctor with Antivirus program, can also use Trial version, if you buy the version The official rights of the program are better.

Manual removal of Anti Malware

Use Process Explorer () and turn off the following processes: *AntiAID.exe, 2gbk87zj.exe, 8enyqcv1.exe, m6axycx9.exe and uninstall.exe.*

Find and delete the following keys in the Registry:

HKEY_LOCAL_MACHINESOFTWAREAntiAID
HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionUninstallAntiAID
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun '% System% 8enyqcv1.exe'
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun 'm6axycx9.exe'

HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun '% ProgramFiles% AntiAID SoftwareAntiAIDAntiAID.exe -min'
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun 'AntiAID'

Delete all related files and folders in the path *% Program FilesProtection System:*

% Documents and Settings% All UsersStart MenuProgramsAntiAID
% Documents and Settings% All UsersStart MenuProgramsAntiAID1 AntiAID.lnk
% Documents and Settings% All UsersStart MenuProgramsAntiAID2 Homepage.lnk
% Documents and Settings% All UsersStart MenuProgramsAntiAID3 Uninstall.lnk
% Documents and Settings% All UsersDesktopAntiAID.lnk
% Documents and Settings% All UsersStart MenuProgramsAntiAID
% Documents and Settings% All UsersStart MenuProgramsAntiAID1 AntiAID.lnk
% Documents and Settings% All UsersStart MenuProgramsAntiAID2 Homepage.lnk
% Documents and Settings% All UsersStart MenuProgramsAntiAID3 Uninstall.lnk
% Documents and Settings% All UsersDesktopAntiAID.lnk
% Program Files% AntiAID Software
% Program Files% AntiAID SoftwareAntiAID
% Program Files% AntiAID SoftwareAntiAIDAntiAID.exe
% Program Files% AntiAID SoftwareAntiAIDuninstall.exe
% Temp% nss8.tmp
% Temp% nsj3.tmp
% Temp% nsn6.tmp
% Temp% 2gbk87zj.exe
% Temp% 8enyqcv1.exe
% Temp% m6axycx9.exe
c: WINDOWS100849pambotz85.bin
c: WINDOWS1019wo5m65bz.dll
c: WINDOWS10568hack9o5l5z5.dll
c: WINDOWSsystem322901sp55za.bin
c: WINDOWSsystem3229290wozm6795.cpl
c: WINDOWSsystem3229418tro5ez.ocx

And continue to erase the following distribution folders:

c: Documents and SettingsAll UsersStart MenuProgramsAntiAID
c: Program FilesAntiAID Software
c: Program FilesAntiAID SoftwareAntiAID
temp
% temp%

Then, scan the entire system again with Spyware Doctor with Antivirus and CC Cleaner.

On the other hand, you can refer to the features and use the security programs of the following reputable firms: Spyware Doctor with Antivirus, Norton, Trend Micro, Kaspersky, AVG, MalwareBytes or other available security applications of Meta company here.

Good luck!