What to do when the computer is infected with a virus that fights virtual money?

Experts from Trend Micro recommend users to update the latest operating system patches immediately, as well as upgrade Trend Micro Security version 12 and set up high-level protection.

1. After WannaCry, Petya's "blackmail" malicious code is raging, this is a way to overcome and prevent it
2. How to identify WannaCry malicious code from Vietnam Computer Emergency Response Center (VNCERT)
3. WannaCry is not dead yet, it just attacked Honda and Australia's traffic camera system

Yesterday as Network Administrator reported that thousands of computers in Vietnam were seized by computer vius W32.AdCoinMiner control of computers through online advertising service Adf.ly. After acquiring the right to make the computer, these vius will continue to penetrate through security holes on the software and take control of the user's computer to download hidden payloads, perform money digging work. virtual. When gaining control from the victim's device, in addition to downloading the virtual money payload, the attacker can install other malicious code through their control server to perform spy actions, hitting Information theft and even data encryption to extort money.

According to experts from Trend Micro recommending, to minimize vius infiltration of computers, users need to update the latest operating system patches, as well as upgrade Trend Micro Security version 12 and set up security High-level defense.

In case you suspect your computer has been infected with virtual money microbiology W32.AdCoinMiner, the following measures can be taken:

Step 1 : Before performing any scanning, Windows XP, Vista, and Windows 7 users must disable the first 'System Restore' to be able to scan the entire computer.

Step 2 : During the installation process or different operating system, you will be able to access different files, items, folders or 'registry keys'. If you have found these items in your computer, do not follow these steps. However, there are many computers that do not have these items, so follow the instructions below.

Step 3: Find and delete the Coinminer virus file in COINMINER_MALXMR.AB-WIN64 format.

While searching and deleting this virus file, there will be a few cases such as:

1. The Windows Task Manager may not display all running applications. In this case, users can use another activity tracking application from third parties like Process Explorer to detect malicious files. Users can download Process Explorer here.
2. The second scenario is that Windows Task Manager and Process Explorer are both displayed, but it is not possible to delete them, users should restart the computer in Safe Mode.
3. The third is that Windows Task Manager and Process Explorer do not display this file, users should take the next step.

Step 4: Delete 'Registry Value'.

Note : If you are not careful about modifying the Windows 'Registry', users may experience system problems and cannot recover. Trend Micro recommends that this step should only be done when you know how to use it or request support from the system administrator. Users can consult a few articles about this issue from Microsoft if they want to continue to edit the 'Registry'.

Access by link:

In *HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run*

XMRRUN = '% SystemRoot% WindowsSysWOW64audiodig.exe - c% SystemRoot% WindowsSysWOW64audiodig'

In *HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunOnce*

Wextract_cleanup0 = 'rundll32.exe% System% advpack.dll, DelNodeRunDLL32'% User Temp% IXP000.TMP "

Step 5: Find and delete the files below

Note: Before searching and deleting files, users should turn on the 'Search Hidden Files and Folders' feature in the 'More Avanced Options' section to make sure the files below are not hidden when searching.

% User Temp% IXP000.TMPTMP {random} .TMP

·% User Temp% IXP000.TMPaudiodig

·% User Temp% IXP000.TMPaudiodig.exe

·% User Temp% IXP000.TMPaudiodig.reg

·% User Temp% IXP000.TMPinit.bat

·*% System Root% SysWOW64audiodig*

·*% System Root% SysWOW64audiodig.exe*

·*% System Root% SysWOW64audiodig.reg*

·*% System Root% SysWOW64init.bat*

Step 6 : Finally, users should use Trend Micro Security antivirus software to detect and delete files in the format like COINMINER_MALXMR.AB-WIN64. When detecting infected files, users should delete or completely isolate other files to avoid spreading.

See more:

1. Antivirus software is slowing down your PC
2. Top 10 best Antivirus software in early 2018 for Windows 10
3. Bkav 2018 uses artificial intelligence to detect viruses and protect computers
4. Former NSA hacker turned Kaspersky antivirus software into a spy tool

You finished reading the article "**What to do when the computer is infected with a virus that fights virtual money?**" 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.