KEYHOLDER

Неотдавна семейството на изнудваческите зловредни кодове (от типа на Cryptolocker) беше попълнено от нов член – Keyholder (Ключодържател). Заразяването с него става чрез кликване върху зловреден линк, отваряне на заразени приложения към електронни съобщения, изтегляне на нелицензиран софтуер и др. След като компютърът бъде заразен с Keyholder, при пускането му на екрана се появява страница със заключен катинар и всякакъв достъп до функционалностите на компютъра става невъзможен (например, четене и копиране на файлове, сърфиране в Интернет и др.). От време на време на екрана се появяват заплашителни съобщения от името на правоприлагащи органи, с които, под претекст че са нарушени някакви норми на поведение в онлайн пространството (изтегляне на пиратски софтуер, детска порнография и др.), се искат суми, срещу които компютърът да бъде отключен.

Добрата новина е, че експертите, които са търсили начини за противодействие срещу Keyholder, вече предлагат средства за обезвреждането му. При един от подходите се зарежда конкретна програма, която сканира компютъра и го изчиства от инфекцията. Другият подход включва последователност от действия на експерта, който избирателно изчиства конкретни файлове. Тези действия са различни в зависимост от версията на Windows (XP, Windows 7, Windows 8) и от използвания браузър (Internet Explorer, Google Chrome, Mozilla Firefox). По-надолу са дадени последователностите на действията и за двата подхода.

Метод 1. Премахване на Keyholder с помощта на SpyHunter

Антивирусното приложение SpyHunter може да се изтегли от http://www.pcspywarekiller.com/spyhunter.php
Използването му е лесно и автоматично като антивирусна програма.

Метод 2. „Ръчно“ премахване на KeyHolder

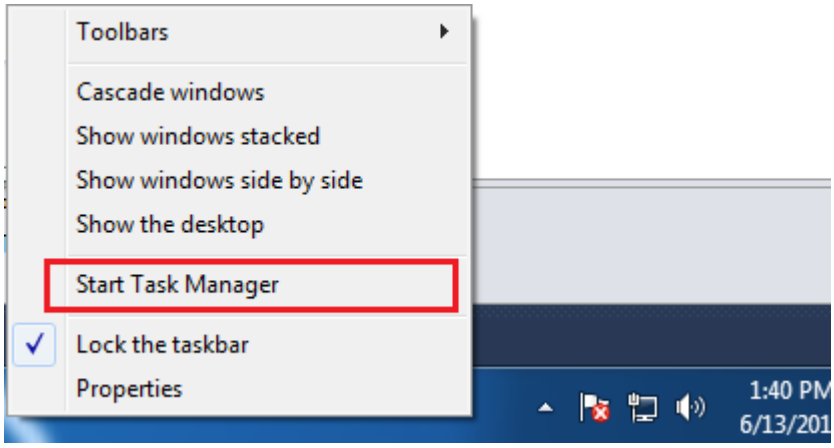
При MS Windows 7

СТЪПКА 1: Стартиране на компютъра в режим Safe Mode with Networking

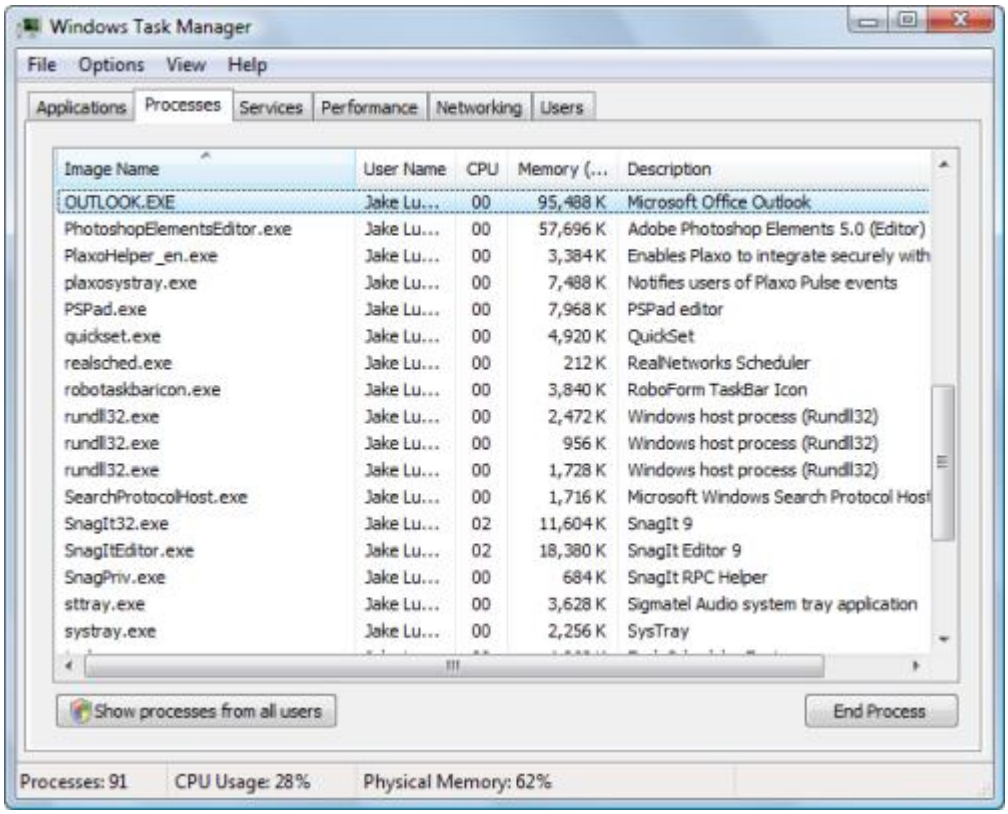
Рестартирайте компютъра, като задържите бутона F8. На екрана се появява Advanced Boot Options. Използвайте бутоните със стрелки Up-Down на клавиатурата, изберете опцията “Safe Mode with Networking” и натиснете Enter, за да продължите.

СТЪПКА 2: Спиране на съответните процеси

Отворете Task Manager, като кликнете с десния бутон на мишката върху лентата със задачите (Taskbar) и изберете "Start Task Manager".

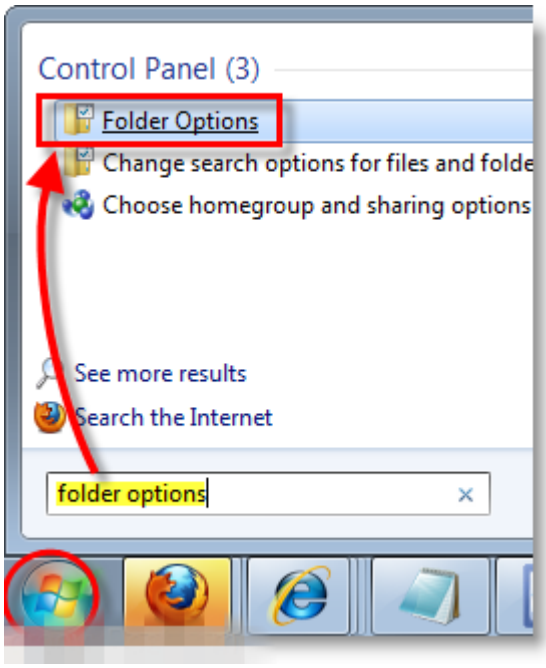


Когато се появи диалоговият прозорец на Task Manager, отидете на таба Processes и кликнете бутона End Process, за да прекратите процесите на троянския кон.



СТЪПКА 3: Показване на скритите файлове и папки

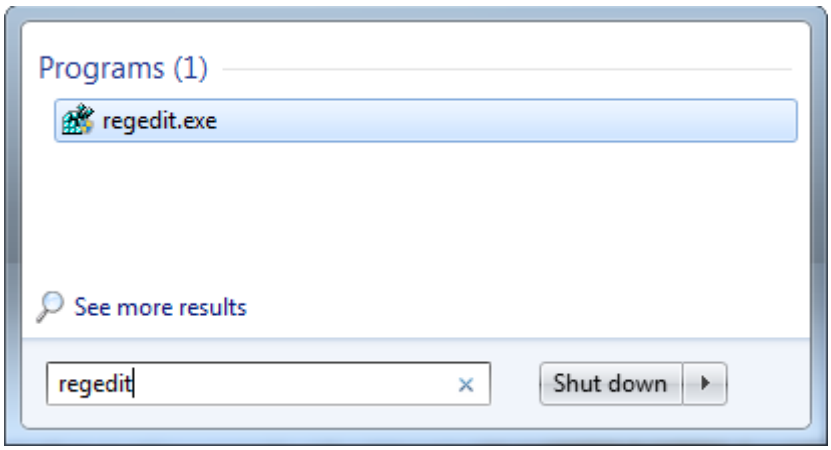
Кликнете върху менюто Start, напишете “folder options” в лентата за търсене и изберете върху “Folder Option” в резултатите на търсенето.



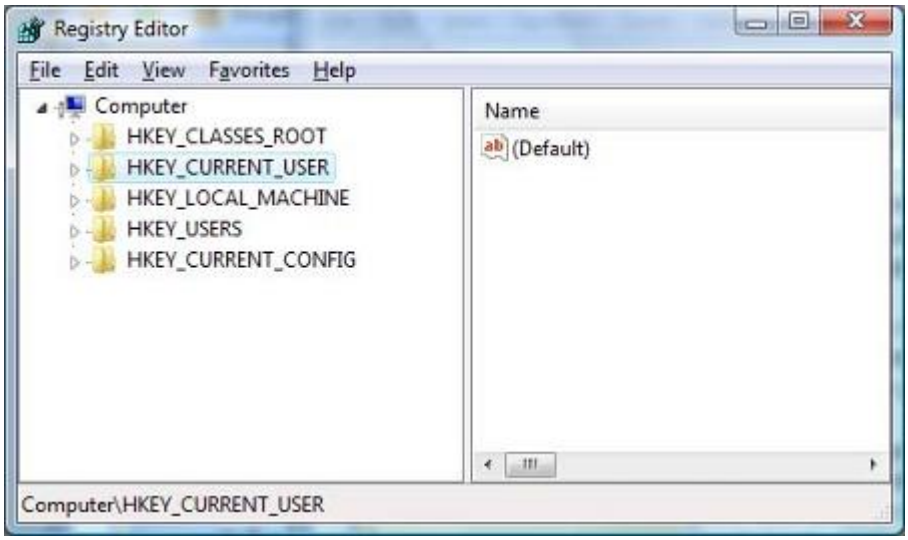
Във Folder Options, кликнете върху таба “View” и в “Advanced settings”, изберете опцията “Show hidden files, folders и drives” и забранете опцията “Hide protecting operating system files (Recommended)”. След това потвърдете с бутона OK.

СТЪПКА 4: Заличаване на вписванията в Registry Editor

Отидете в меню Start, напишете "redegit" в кутията за търсене и кликнете върху "regedit.exe" в списъка на резултатите от търсенето.



В Registry Editor, намерете и отстранете всички вписвания, свързани с троянския кон.



HKEY_LOCAL_Machine\Software\Classes\[Trojan horse name]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\[Trojan horse name]

СТЪПКА 5: Заличаване на файловете, свързани с троянския кон

Отидете на диск C, намерете и заличете всички файлове, свързани с Троянския кон.

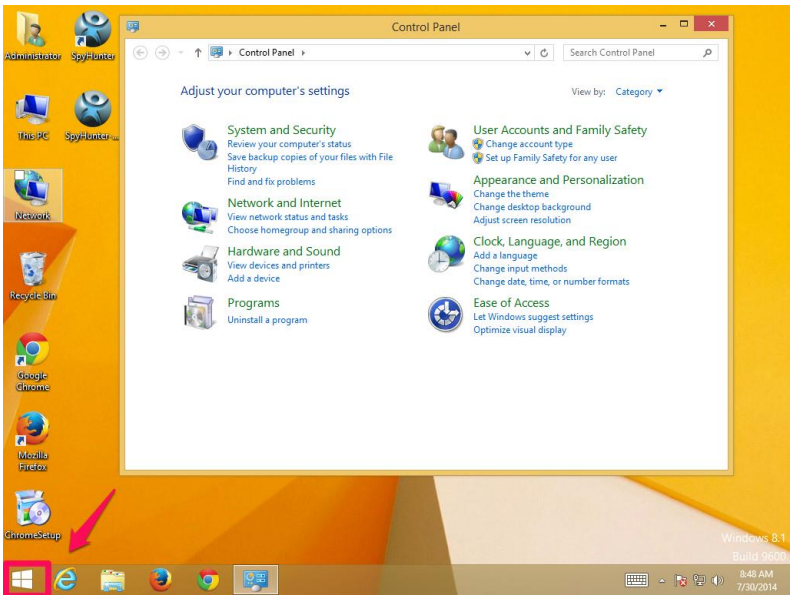
%Temp%\[Trojan horse name]
%AppData%\[Trojan horse name]
%LocalAppData%\[Trojan horse name]
%LocalAppData%\[Trojan horse name].exe
%CommonAppData%\[Trojan horse name]

СТЪПКА 6: Рестартиране на компютъра

При MS Windows 8

СТЪПКА 1: Деинсталиране на KeyHolder от програмата Add & Remove

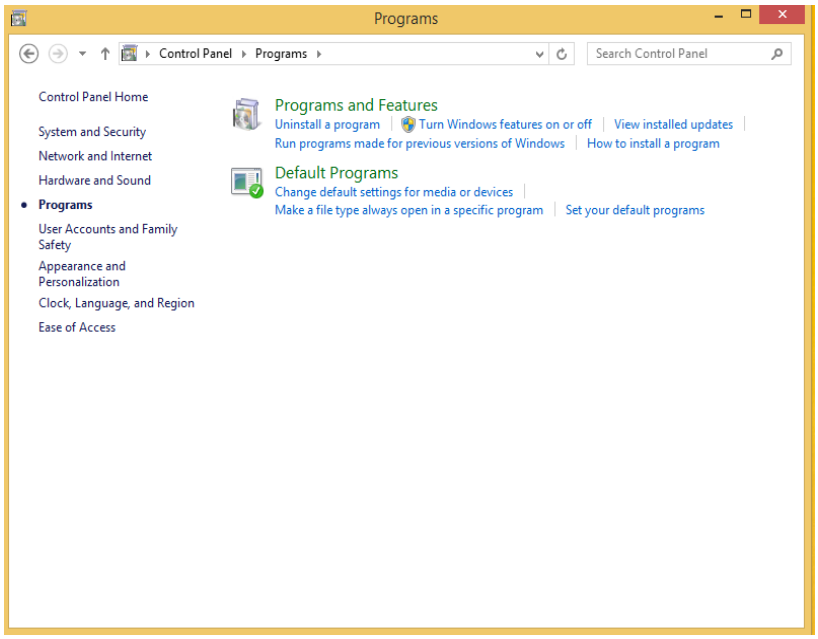
1. Натиснете бутона Start.



2. Кликнете върху Control Panel.

3. Кликнете върху Program.

4. Кликнете върху Uninstall a program.



5. Намерете KeyHolder в списъка и изберете Uninstall.

6. Натиснете бутона Apply и след това бутона OK.

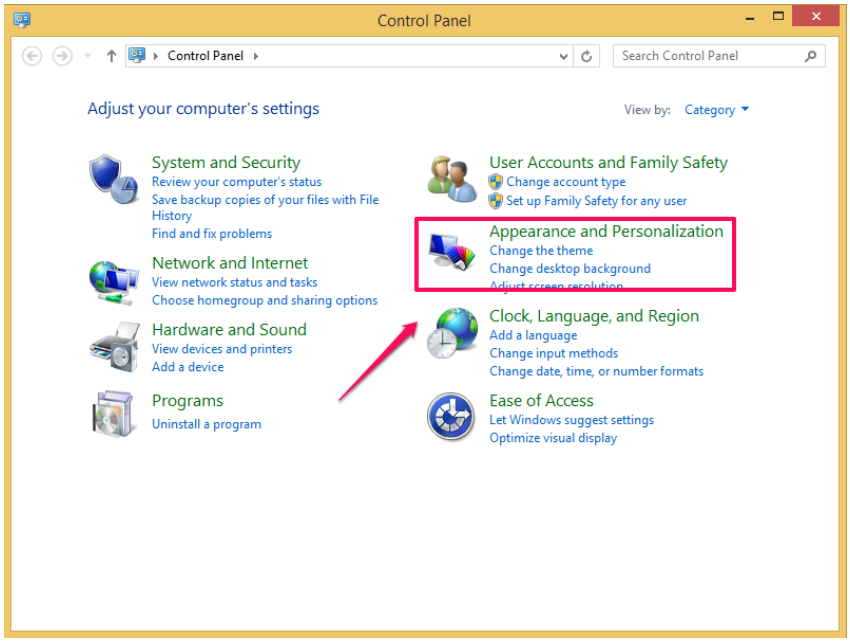
СТЪПКА 2: Показване на всички скрити файлове

1. Затворете всички програми, за да излезе десктопът.

2. Кликнете върху бутона Start.

3. Изберете Control Panel.

4. Когато Control Panel се отвори, кликнете върху Appearance and Personalization.



5. Под категорията Folder Options, кликнете върху Show Hidden Files or Folders.

6. Под раздела Hidden files and folders section изберете радио бутона Show hidden files, folders, or drives.

7. Махнете отметките от чекбокса на „Hide folder merge conflicts“ и „Hide protected operating system files“.

8. Натиснете бутона Apply и след това бутона OK.

9. Заличете всички файлове, свързани с KeyHolder.

Video Shows: https://www.youtube.com/watch?v=7NsF409JIno

СТЪПКА 3: Изчистване на всички бисквитки от засегнатите уеб-браузъри

Тъй като KeyHolder е в състояние да използва бисквитките за проследяване и следене на интернет активността на потребителите на компютъра, желателно е всички потенциални бисквитки да бъдат изчистени. Функции за изтриване на бисквитите има във всички популярни браузери. При нужда от помощ можете да ползвате посочените по-долу линкове:

За Google Chrome:

Video Shows: https://www.youtube.com/watch?v=gsQTJhciius

За Mozilla Firefox:

Video Shows: https://www.youtube.com/watch?v=NfjnS7JSdqU

За Internet Explorer:

Video Shows: https://www.youtube.com/watch?v=E5FK1eZKlx0

За повече информация:

http://www.spywareremovepro.com/keyholder-removal-tutorial-to-get-rid-of-keyholder-from-your-pc/
http://www.pcspywarekiller.com/how-to-remove-keyholder-completely-from-your-computer/