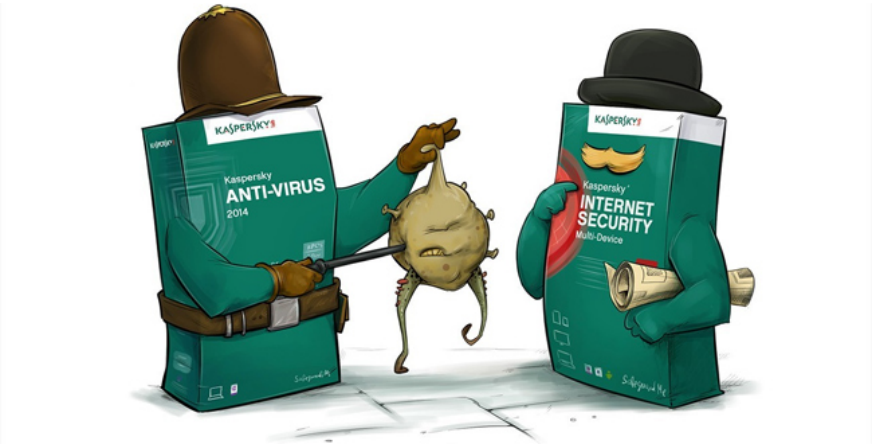
Former NSA hacker turned Kaspersky antivirus software into a spy tool

By knocking out Kaspersky Lab's anti-virus software and turning it into a search engine that benefits from confidential documents, Patrick Wardle, Digita Secutiry's research director and former NSA hacker proved that, sometimes when a security software can still be exploited and become an effective spy tool.

By knocking out Kaspersky Lab's anti-virus software and turning it into a search engine that benefits from confidential documents, Patrick Wardle, Digita Secutiry's research director and former NSA hacker proved that, sometimes when a security software can still be exploited and become an effective spy tool.



Patrick Wardle said that antivirus products have many features in common with the spy code it is looking for. Therefore, he wanted to try to see if this mechanism could be exploited to perform reverse attacks. For example, if an anti-virus software maker wants, either is forced, hacked or for some reason, will they be able to create a symbol to mark and search for confidential documents ?

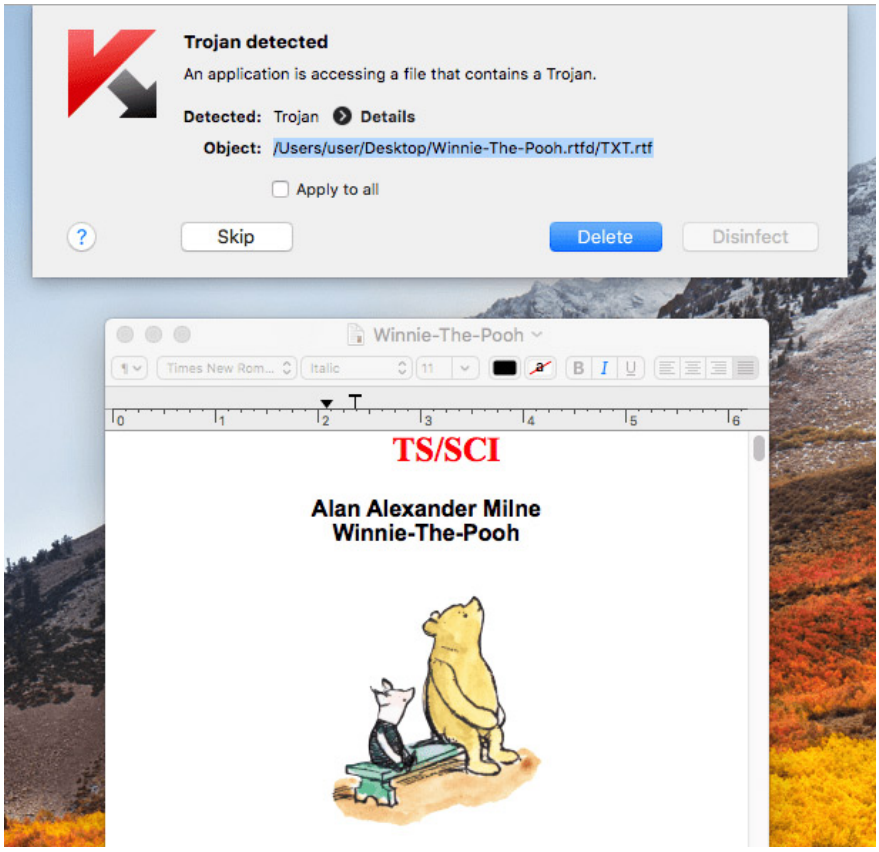
US President Donald Trump signed a bill banning the use of Kaspersky Lab's products and services across all federal agencies in December of last year.

A top-secret report by former NSA employee Edward J. Snowden was released online showing that the NSA has targeted antivirus software (such as Checkpoint and Avast) to collect sensitive information stored in the machines. target since 2008.

Patrick Wardle, Research Director of Digita Secutiry and former hacker of NSA.
To exploit the ability to take advantage of Kaspersky Lab antivirus software for intelligence purposes, Wardle has implemented a reverse process on this software. He wishes to be able to create a Kaspersky Lab insertion symbol to search and detect confidential documents.

The source code for Kaspersky Antivirus is extremely complicated but the signature of Kaspersky malware is easy to update. Wardle realized that this feature could be exploited to automatically scan victim computers and perform spy activities, stealing confidential documents.

Realizing that officials often mark classified documents with Top Secret / TS / SCI (Sensitive Compartmented Information), he added a rule to scan Kaspersky's antivirus program to mark any resource. Do you have a "TS / SCI" symbol?



In order to test this new scanning rule, Wardle added the TS / SCI symbol to the beginning of a document with a content about Winnie the Pooh bear and saved it on his computer. As soon as the text is saved on the hard drive, Kaspersky's antivirus program immediately marks, quarantines it and sends this data to the company for further analysis.

Kaspersky Lab thinks Wardle's research is not correct because all signatures are always open to all users and cannot distribute a specific signature or update the signature for a single user secretly. In addition, the updates are digitally signed so they cannot be faked.

However, Wardle's research also shows us that an antivirus program can be turned into an extremely powerful search engine.

You finished reading the article "**Former NSA hacker turned Kaspersky antivirus software into a spy tool**" 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.