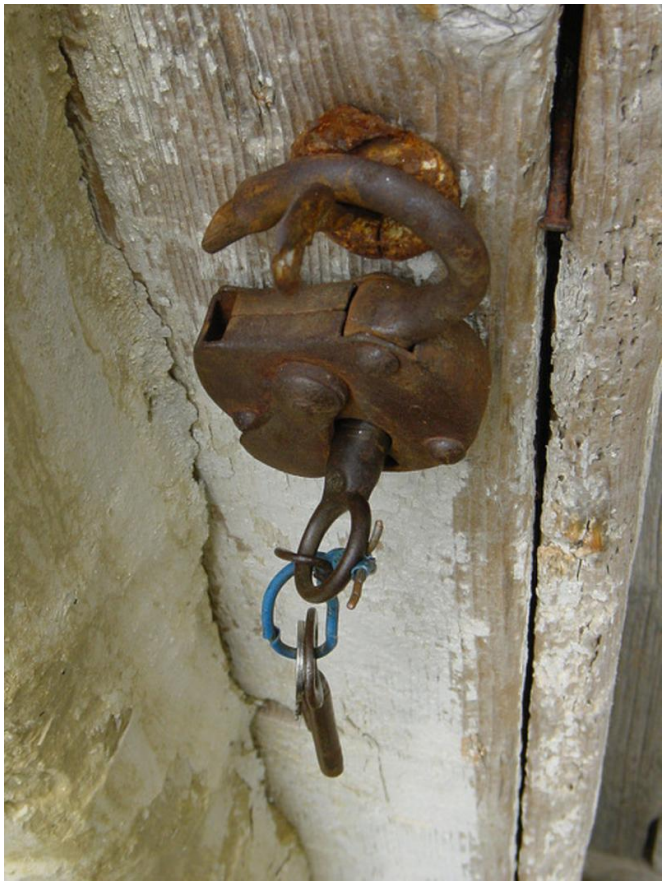
Is it time to uninstall antivirus software?

30 June 2016, by David Glance



Credit: brankomaster/flickr, CC BY

For years everyone has been told that they should run antivirus software on their computer for the best possible protection against the ever growing tide of viruses, trojans and general malware on the Internet.

Now it seems, another security expert is adding his voice to the growing concern that using antivirus software may actually make your security worse, not better. Tavis Ormandy and the Project Zero team at Google has discovered a slew of vulnerabilities with antivirus software from Symantec and Norton. The most particularly worrying vulnerability allows anyone to trigger it by simply emailing a link or a file. Ormandy suggested that the bugs in Symantec's software could be used to crash an entire company's computer network exploit the very software that is supposed to protect them.

Symantec is not the only company that Google Zero has highlighted with security flaws of this kind, other antivirus software from Comodo, ESET, Kaspersky, Fireeye and others have all been found to have similar vulnerabilities in the past. A search of the vulnerabilities database shows hundreds of current issues.

The problems stem from the general complexity of antivirus software, meaning it is hard to write without bugs. But it seems that antivirus companies have also been cutting corners and generally been sloppy in their coding and testing. Symantec in particular had been using open source software packages within their own products but not updating it. Ormandy found packages that hadn't been updated in the last 7 years.

Sloppiness was also the root of Google's discovery last year that Symantec's subsidiary Thawte had been creating fake SSL certificates for domains like www.google.com and google.com and these certificates had subsequently leaked onto the Internet. Fake SSL certificates could be used to fool Internet users that they are visiting a genuine Google site when in fact it was set up by hackers. In this case, an internal investigation by Symantec revealed thousands of fake certificates, some of which were for real domains.

Google is not the first to point out the flaws in security software. Researchers have been identifying problems in most antivirus and other security software for years. The range of different ways that antivirus software can be attacked was the subject of a Black Hat hacking conference presentation as far back as 2008.

Despite everyone in the industry being aware of the problems, security companies it seems haven't paid too much attention.

Antivirus software is very complicated. It has to understand the nature of a very large number of different types of files and the different ways in which these files can be altered to escape detection. In order to efficiently process files that may be being written to a disk or arriving via a web link or email, antivirus software usually runs on the computer with extra privileges. This makes the consequence of attacks on this type of software particularly serious. The counter-intuitive result of this is that antivirus software gives malware writers even greater opportunities for attack on a computer than if the software hadn't been installed in the first place. In security jargon, it actually increases the "attack surface".

Antivirus software companies have attempted to mitigate the potential vulnerabilities in their own software but have balked at doing so in a way that would impact the overall performance of the computer. Google advocates "sandboxing" which is an approach where the antivirus software is run in such a way that it is isolated from the computer operating system and other applications. If it is compromised, it can't affect the overall system. Some security companies are developing antivirus solutions based around this type of approach but so far, it hasn't been adopted widely.

To critics of antivirus software, the issues of reducing the attack surface of these products is moot. One vocal critic, Gunter Ollmann argues that antivirus software is not particularly effective in stopping threats in any case because it is too easily circumvented. He argues that changes to the way that operating systems are developed and improved will provide much greater protection than antivirus software will ever do. Certainly this is true in the case of Apple's mobile operating system which has seen few, if any, problems from malware because of its inbuilt security and highly guarded environment for apps. Increasingly, malware detection and mitigation is being built into newer versions of operating systems like Mac OSX and Windows.

Whilst it may not be worth uninstalling already purchased antivirus software, it is likely that if you are keeping apps and the operating system up-to-date with the latest versions as soon as they are released, adding antivirus software may not bring any additional benefit and may increase the risks.

This article was originally published on The Conversation*. Read the* original article*.*

Source: The Conversation

APA citation: Is it time to uninstall antivirus software? (2016, June 30) retrieved 22 January 2022 from https://techxplore.com/news/2016-06-uninstall-antivirus-software.html