Does Anti-Virus Software Do All That It Promises? Probably Not.

An Analysis of Antivirus Software

Christina King

Tufts University
COMP 116 | Prof. Ming Chow
December 13, 2019

Abstract

A virus is a type of malware, but 'anti-virus software' is a misnomer because these systems now claim to protect against many types of malware. Most security professionals recommend using some software of this kind, but does it actually protect users from all types of malware? Is it better than nothing at all? Some experts claim that it can actually make your computer less safe. As we explore these topics in this paper, I will discuss signature- and heuristic-based anti-virus software, how well each works, and what else you can do to ensure security of your data.

Thesis

Anti-virus software is all but useless, and people cannot depend on it to protect their devices and data. Although, the spread of this information could make people feel less safe, the public deserves to know that their security is at risk. The only way anything will change is if it is common knowledge that there is a problem here.

To the Community

The effectivity and value of antivirus is a topic that I am very curious about. Why do people use this software and how well does it really work? Personally, I have never used an antivirus software to protect my computer from malware, and I used to embarrassed by this. It felt like I was leaving my computer unprotected by judging whether links and downloads were safe myself, but I never made the time to download or research this software until now. Through the research that I've done for this paper, I've learned that the answer is not what I expected. Perhaps anti-virus does more harm than good.

The topic of anti-virus software is very important because the threat of malware is growing at an alarming rate. According to a Sam Cook, a data journalist, ransomware payments total to

about 1 billion dollars every year. Many people depend on it to protect their security and privacy, but no anti-virus can, or should, ensure that it will do that. Another reason that this needs to be discussed is to come to a consensus on whether to spread this information about the threat to our online security or if it is better for people to think that they are protected.

Background Information

When you look at the marketing and promises on many anti-virus products, they have very strong claims of protection and safety. For example McAffee claims that it provides "comprehensive internet security" ("Antivirus Software & Security Suite").

There are two main types of anti-virus software. The first that came onto the market was signature-based in 1986 in response to the Vienna virus ("History of Malware"). Many antivirus software still use this method of detection. The second type is heuristic-based. The first of its kind, the Flu Shot, showed up later in 1987 ("Technology & Practice Guide").

The difference in these types of software is in the algorithms that they are each based on. The signature-based algorithm compares the signatures or hashes of potential malicious software with that which is already known. This requires that software has access to a lot of data about already known malware. Heuristic-based algorithms, however, use more generalized rules to determine whether a program acts similarly to the way known malware tends to act. This generalization allows it to flag software that isn't exactly like something that we have seen before.

Although heuristic based software can in theory identify malware it has not encountered previously, a signature based algorithm usually cannot. As discussed above the keys of the potential malware have to be the same as a known piece of malware. This allows for a huge vulnerability. If a hacker changes a small bit of the code in a virus, maybe not even altering its performance, the algorithm will probably no longer be able to recognize it. Hackers also make

viruses that are polymorphic so they change as they spread, evading detection even if antivirus software learn its signature.

Most of the antivirus software on the internet use a combination of these methods to classify potential malware. Often, using machine learning to learn malicious signatures and rules for heuristics.

Comparison

Heuristic-based antivirus software might sound more reliable because it looks at the behavior of the potential virus rather than the signature, so it can in theory recognize a virus if there are added comments or slight changes implementation. According to an article in the International Journal of Advanced Research in Computer Engineering and Technology, heuristic-based algorithms are vulnerable to false positive whereas signature based are more vulnerable to false negatives (Mujumbar). But in this situation false negatives are worse than false positives because the result of a false negative is downloading malware onto your device.

In most conditions, heuristic based algorithms are somewhat better than signature based for this exact reason. They will still fail if the hacker writes a virus in a new way or changes it enough as will be shown later in the paper. Also the performance depends a lot on the quality of the heuristics.

Experiment to Test Methods of Common Antivirus Software

If signature based engines are so easy to surpass, big antivirus providers wouldn't use this, right? To test the idea that slightly changing a virus will trick these systems, I did a small experiment. VirusTotal, currently owned by Google, is an aggregation of antivirus software to which a user can upload files in order to check if it is malicious. The idea is that if these antivirus engines that VirusTotal uses are behavior-based, inputting the file to VirusTotal without

comments will give the same outputs as after adding comments. Adding comments changes its signature. A signature based system might not catch the malware after making this change.

To do this, I created a script that would be caught by virus total using MSFVenom and inputted this file into VirusTotal. 25/58 of the engine caught it, meaning many of these engines believe this code to be malicious. Next I Base64 decoded the script, added a lot of comments, and encoded it again. When I saved and submitted it to VirusTotal, only 5/58 recognized it as malicious. Some of the engines that could not withstand this change were McAfee, Avast, and Sophos, antivirus software that many people depend on.

From this, it seems that a lot of the common antivirus software that VirusTotal utilizes applies signature based algorithms because they were not able to detect the malware when its signature changed from the comments. Also they are outdated and no longer helpful in protecting our security and privacy from malware attacks. Perhaps some of the antivirus software that did not catch the malware with comments do use heuristic-based, but I would expect that they would detect that the behavior is the same with or without comments.

Analysis of Malware Effectiveness Data

In a journal article called "On the effectiveness of malware protection on Android," the authors say that they are using heuristic/behavioral based malware classifiers to test detection rates of malware in altered vs. unaltered data. The two figures to the right were used to show the ease at which a person with beginner to moderate coding abilities can evade detection of Android malware from heuristic/behavior based malware classifiers. Many of the

Test Case 2: Unaltered Malware (Reference Values for Test Case 1)

	1	2	3	4	5	6	7	8	9	10	Total
avast	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
AVG	✓	–*	✓	✓	✓	✓	–*	✓	✓	✓	8/10
BitDefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
ESET	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
F-Secure	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
Kaspersky	✓	–	✓	✓	✓	✓	✓	✓	✓	✓	9/10
Lookout	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
McAfee	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
Norton	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
Sophos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10/10
Trend Micro	✓	✓	✓	✓	✓	✓	–	✓	✓	✓	9/10

Table 3.2: Detection rates for Test Case 2, which serve as reference values for Test Case 1 (–* denotes that the sample has been detected as aggressive adware, not as malware)

programs were seen by the antivirus engines as less likely to be malware after alteration. In the article, they explained that altering the malware mostly included changing variable names and adding print statements. This is not very much more complex than adding comments in the signature-based algorithm approach.

Test Case 1: Altered Malware

	1	2	3	4	5	6	7	8	9	10	Total
avast	✓	–	✓	✓	–	✓	✓	–	✓	–	6/10
AVG	–	–*	–	✓	–	✓	–*	–	–	–	2/10
BitDefender	✓	–	–	✓	–	✓	✓	–	–	–	4/10
ESET	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	9/10
F-Secure	✓	–	✓	✓	–	–	✓	✓	✓	–	6/10
Kaspersky	✓	–	–	✓	–	–	✓	–	–	–	3/10
Lookout	✓	–	–	✓	–	✓	✓	✓	✓	✓	7/10
McAfee	✓	–	–	✓	–	–	–	–	–	–	2/10
Norton	✓	–	–	✓	–	✓	–	–	–	–	3/10
Sophos	–	–	–	–	–	–	–	–	–	–	0/10
Trend Micro	✓	–	–	✓	–	–	–	–	✓	–	3/10

Table 3.1: Detection rates for Test Case 1 (–* denotes that the sample has been detected as aggressive adware, not as malware)

According to the authors, "The weakness lies in the lack of sufficiently effective heuristics and behavioral analysis" (Fedler 24). Although this study was done in 2013, and I am sure these classifiers have improved, so has malware and the techniques to avoid them. Heuristic-based classifiers are definitely not even close to perfect. It is clear from this data that even the most popular antivirus software is relatively easy to evade. Action is required to protect ourselves from attacks because antivirus software will not do it.

Additional Problems with Antivirus

Besides its lack of effectiveness, there are a few other drawbacks to using antivirus software. The first is a false sense of security. It is a common misconception, as I have said above, that antivirus can protect you, so many people are not as careful when it is installed on their computer.

Another reason why it might not be wise to use it is that this software is often not secure itself—allowing for attackers to access your data and devices through vulnerabilities in the antivirus. Referring to these vulnerabilities, Tavis Ormandy, a Google Project Zero researchers says, "They affect the default configuration, and the software runs at the highest privilege levels possible." This means that if there are vulnerabilities, attacks can cause really devastating effects.

Next Steps

Delete your antivirus. Or if you don't have one, don't download one. It is infinitely more effective and cost effective to take other steps rather than using antivirus software. These include backing up your computer to mitigate loss, updating and patching software on your computer, and being mindful of what you click on and download.

The next thing you should do is tell people. Although the knowledge that your antivirus isn't protecting you might make people feel less safer, hackers already know that it doesn't work. Spreading the word is the only way to make big changes and get people to focus on security more.

Conclusion

From my research, I found that generally antivirus software is not effective. As Bruce Potter says in an article published the IEEE Security and Privacy Journal, "making malware-ridden documents that fly past up-to-date antivirus products is incredibly simple (57)." I was able to surpass a large portion of those on VirusTotal by adding comments to a piece of otherwise classified malicious code.

Some may say, "Why not use antivirus software in addition to taking these other steps just in case it catches something?" This might be true, but there are other problems with antivirus software like a false sense of security and added vulnerabilities. There are things you can do to protect yourself though. The public deserves to know that their security is at risk, so voice this to whomever you can. The only way anything will change is if it is common knowledge that there is a problem here.

Works Cited

"Antivirus Software & Security Suite" *Trusted Anti-Virus, Identity Management, and Privacy Protection for Every Device You Own | McAfee Total Protection*, www.mcafee.com/consumer/en-gb/store/m0/catalog/mtp_521/mcafee-total-protection.html.

Baggett, Mark. "Effectiveness of Antivirus in Detecting Metasploit Payloads." *No Think*, 6 Mar. 2008, www.nothink.org/metasploit/documentation/metasploit_payloads.pdf.

Balci, Ege. "Art of Anti Detection 1 – Introduction to AV & Detection Techniques." *Pentest Blog*, 13 Feb. 2017, pentest.blog/art-of-anti-detection-1-introduction-to-av-detection-techniques/.

Chung, Emily. "Could Antivirus Software Make Your Computer Less Safe? | CBC News." *CBCnews*, CBC/Radio Canada, 9 July 2016, www.cbc.ca/news/technology/antivirus-software-1.3668746.

Fedler, Rafael, Marcel Kulicke, and Julian Schütte. "On the effectiveness of malware protection on Android." Fraunhofer *AISEC*, 2013.

"History of Malware." *Viruslist.com - 1987*, Kapersky Lab, 2007, web.archive.org/web/20071107040723/http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311150.

Mujumbar, Ashwini. "Analysis of Signature-Based and Behavior-Based Anti-Malware Approaches ." *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)* , vol. 2, no. 6, June 2013.

Ormandy, Tavis. "How to Compromise the Enterprise Endpoint." *How to Compromise the Enterprise Endpoint*, Google Project Zero, 1 Jan. 1970, googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html.

Potter, Bruce. "Necessary but Not Sufficient." *IEEE Security & Privacy Magazine*, vol. 8, no. 5, 14 Oct. 2010, pp. 57–58., doi:10.1109/msp.2010.157.

"Technology & Practice Guide." *Flu Shot for Computer Viruses*, web.archive.org/web/20140826115405/https://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/tsp97flushot.html.