Patches and Antivirus

[**Introduction**](#_h4n4cki0bki8) **2**

[**Patches**](#_wbgzarx0gtwi) **2**

[**Antivirus**](#_cc232ytnka3t) **2**

[Scanning](#_881o8th7u320) 3

[Virus Definitions](#_gwopadx8fdv3) 3

[Heuristics](#_j38mvh1gk370) 3

[False Positives](#_m49f75pcpljg) 4

[**Conclusion**](#_46uoue6vbaa8) **4**

[**References**](#_d1ri97nxpzjn) **5**

# Introduction

Two important concepts in cybersecurity are the existence of patches and antivirus software. They are incredibly important subjects, but aren’t often thought about. Patches are downright essential in maintaining the security of a system, and antivirus software is vital in the attempt to defend against the myriad viruses that proliferate and infect the internet.

This module will contain a brief overview on patches and antivirus software. Of the two subjects, we will go into much more detail with the subject of antivirus software. Finally, there will be a short game to review and reinforce your knowledge!

# Patches

A patch is a piece of software designed to fix a problem. The types of problems a patch can solve are pretty much any software problem you can think of. For example, some types of problems a patch can fix are: bugs, new features, and (importantly for our purposes) security vulnerabilities. Patches are often used to shore-up the security of a system. As an example of a patch that could affect security, the patch adds a new minimum password length to a system.

As a user, not staying up to date on the latest patches for a system exposes you to the vulnerabilities that have been fixed by the patches. Therefore, not installing the latest patch is usually a terrible idea.

# Antivirus

A much more complicated subject of cybersecurity compared to patches is the concept of antiviral software. The Internet is an enormous interconnected network that has become essential to daily life for most people. However, with that convenience also came the proliferation of malware, hackers, and other computing related threats. Browsers, games, plugins, web apps, phone apps, and more, all are vulnerable to attack from a myriad of attack types, be it malicious code or a malicious person. There are so many viruses and other malicious programs circulating the web that it is impossible for even computer science experts to keep up with them.

Antivirus software was developed to combat this problem. By letting virus detection and prevention be handled programmatically, much more attacks can be prevented than if they were handled by a layman. In the next sections, we will be covering how exactly antivirus softwares prevent attacks.

## Scanning

Antivirus systems handle threats by scanning for them and then stopping their execution. There are several different types of scans an antivirus software can perform. Full System scans go through **everything**, everything on your hard drive, everything on your network, system memory, and any other connected file storage. Quick scans check the commonly used sections of the computer. On-access scans scan files as you open them.

The next few sections go into how exactly the antivirus software detects threats.

### Virus Definitions

There are two main ways in which antivirus programs perform threat detection. The first of those is the use of virus definitions. Basically, a virus definition tells the antivirus engine what to look for. So, if a piece of malware that is found, analysis is done on the code in order to generate a definition. This definition is then patched into the antivirus software so that if that piece of malware enters a user’s computer, then the software will notice it since the code fulfills the requirements of the definition.

### Heuristics

The second method of threat detection is with heuristics. Heuristics are used to detect the malware that has yet to be analyzed. It does this by using signature detection. As an example of a signature, suppose a program you just downloaded attempts to delete every single “.doc” file on your hard drive. A reasonable assumption is that only a piece of malware would be trying to do that. Antivirus programs use heuristics by listening for behaviors that a program shouldn’t be engaging in (signatures) and then putting a stop to those programs.

### False Positives

Virus definitions and heuristics have a very glaring problem, however. They aren’t totally perfect since they rely on signatures and definitions, which allows for “false positives.” To return to a previous example, suppose you downloaded a file called “deleteAllDocFiles.exe” because you wanted to get rid of all “.doc” files on your computer. The antivirus software would flag that file as malware, even though it is working exactly as intended. This would be a false positive. Since antivirus software relies on detecting signatures and stopping files that fulfill certain requirements, they can often flag perfectly normal files as malware.

# Conclusion

And that's about it! Remember, no antivirus software is perfect, so don’t just leave all of your security concerns in their hands.

# 

# References

1. [Patches](https://www.lifewire.com/what-is-a-patch-2625960)
2. [Antivirus Explanation 1](https://www.hackingtutorials.org/malware-analysis-tutorials/how-does-antivirus-software-work/)
3. [Antivirus Explanation 2](https://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/)