John Faria
2/6/2020
Technical Writing
Description Document: Antrivirus Programs

Coding Our Way to Victory Against the Computer Virus

Audience: A student who has taken a computer science class or two and is interested in learning about how awesome security is.

Purpose: To help people with interest in computer science and cyber-security to better understand how antivirus programs work, how they can interact with antivirus software to improve them (perhaps even through their own basic code), and to help get the students interested in the field of cyber-security. This document will be about a basic security tool that someone with a small amount of computer science knowledge should be able to understand and even customize.

John Faria
2/6/2020
Technical Writing
Description Document: Antrivirus Programs

Antrivirus programs are used to help track-down, and delete viruses from a user's computer system. Viruses are malicious unwanted programs that infect your computer, causing damage to the information stored there, and then spread to other computers. Since the beginning of the Internet, software has been sent to and run on computers all the time. Unfortunately, some of the code that is sent to and run on your computer will be malicious, as in it will cause harm to the user generally for the benefit of some attacker. Antivirus programs will search through the files on your computer and look to see if any of them have signatures matching computer viruses. Antivirus software has been popular since the 1990s and the code behind how they work is actually rather simple. By understanding how the antivirus works you can more efficiently use these security tools, and it is even possible to write some of your own basic scripts to take the security of a system into your own hands.

Antivirus programs first emerged in 1987[1] as a response to the first infectious computer viruses that were infecting most computers connected to the internet. Several computer security experts who had learned how to find and remove certain viruses began selling this service, removing these specific viruses from clients' computers. Some security experts learned that they could find computer viruses in a client's file system by looking at the hashes of the files stored on their computer. A hash is a unique string of a few dozen characters generated through mathematical hashing functions. The input of any file into a hashing function will always return the same string of characters, however two files with any difference will generate completely different hashes. Viruses, like all programs on a computer, are stored on that computer in the form of files. The first antivirus program, VirusScan[1], went through all of the files on a computer and compared their hashes to the hashes of known malicious programs. Instead of calling security experts to respond to an infection, a user simply needs to run a program that will search their entire computer for thousands of different viruses that may be hiding in their file system.

In the late 2000s antivirus programs began offering features to help better-protect users from the expanded threats that they were now facing. Malware analysts, who are employed by antivirus companies, continuously researched, reported on, and publicly shared the malicious programs that they found. Some of these programs were actually developed by real companies instead of criminals, and while the offending programs were usually unwanted and did exploit the user, they were not necessarily malicious in nature. These legitimate companies took issue with their software being publicly classified as a virus, so malware analysts created the new classification "potentially unwanted application" to describe these threats. Modern antivirus programs will usually find many potentially unwanted applications and adware on a user's computer, but as these programs are not inherently dangerous the antivirus may not always look for them in order to search more efficiently for other viruses. As the usage of computers evolved and became more complex there became more places that malicious code could be sent to and run on a computer. Instead of becoming installed software on a computer, some viruses began embedding themselves into more complicated programs on the computer that were responsible for running many temporary sub-programs. An example of popular software that is abused in such a way is the web-browser. On the Internet there are many malicious web-pages that will attempt to execute and embed JavaScript code into the web-browser. These viruses will frequently exist as part of the web-browser's execution, lasting until the or the virus has finished executing its payload, or the web-browser is shut-down. The files

1 Sahay, Manish. "Who Invented the Antivirus? A History of Antivirus Software. • The PC Insider." *The PC Insider*, The PC Insider, 17 Aug. 2018, www.thepcinsider.com/who-invented-antivirus-history-timeline-evolution/.

(and therefore the hash signatures) that such temporary viruses leave behind may only be present for a few minutes to a few hours, so an antivirus that is not constantly scanning the computer will be unlikely to stop the virus. To combat temporary viruses, modern antivirus program will run live-protection services that will monitor all currently executing programs, focusing on the files that they create and access. Live-protection has been known to slow-down computers, sometimes severely and is reason that many individuals do not like having an antivirus running on their computer.

Using our knowledge of how antivirus programs work, along with some basic scripting, it is possible for a user who knows some computer science basics to write their own program that will greatly improve the defenses of their computer against viruses. Using the command-line tools that are included with most antivirus programs and a simple scripting language such as Python it is possible to control what directories on a computer are scanned, when this scanning takes place, and what kinds of threats the antivirus program looks for. It is even possible to have the different scans be easily controlled via a programmed interface or simply the processes currently running on the computer. An example of a basic program that you may want to start with is one that will be able to find temporary viruses, while not slowing-down your computer significantly. This could be done by scanning the directories related to complicated programs such as your web-browser, email client, and word processor every few minutes, and then programming a timer to automatically conduct a system-wide scan once every few days. Using antivirus programs and your knowledge of just computer science fundamentals there are many different security features you could program to help defend your computer from viruses.