Alex Hearne Hearne 1

1 March 2020

INFO 460

Professor Waggoner

Security Research Paper (Anti-Malware/Anti-Virus)

Anti-virus and anti-malware software have long been used to prevent attacks caused by viruses and malware. Computer malware is malicious software designed to harm a device. Malware is the term that is used to describe all different types of software that could harm a device, including viruses, trojans, spyware, worms, etc. A computer virus is a type of malware that executes itself on a computer by inserting unauthorized code onto a device. Once this unauthorized program has been executed, this device is now “infected.” Anti-virus/anti-malware software was created to minimize the possibility of one’s device becoming infected with malware.

Anti-malware or anti-virus software works in a variety of ways. One way this software works is through behavior monitoring. If a file shows signs of suspicious behavior, anti-malware software will scan the file, and then determine whether this file is a threat based on signatures. All viruses or malware contain signatures, which are essentially “fingerprints of a virus” (*Computer Hope*). Every virus or malware contains a fingerprint, which allows it to be identified as a virus. If the file is determined to be a threat, the user will be notified. Another aspect that anti-malware introduces is sandboxing. Sandboxing essentially puts suspicious files into a “sandbox,” which places the file in isolation. Then, the software will further analyze the file and determine if it is a threat. Essentially, sandboxing allows the anti-malware software to separate

Hearne 2

potentially malicious software from applications to prevent damage on a device (*Comodo*). Finally, once a piece of software has been identified as malware, the anti-malware software will then remove it from the device to prevent execution and thus prevent infection of a device. Unsurprisingly, this software must continuously be updated to account for new viruses that have been created which can bypass the anti-virus software (*Yusuf*).

Anti-malware and anti-software applications address a variety of security concerns, including unauthorized access to personal information, files, restoration of corrupted data, protection from spam, and likely the most important: money. Anti-malware and anti-virus software can detect these harmful programs before infecting a device, and thus protect sensitive information and prevent loss of money, specifically from companies.

Anti-malware and anti-virus applications address two aspects of the CIA triad, integrity and confidentiality. Integrity addresses the “protection of data from deletion or alteration from any unauthorized party” (*Forcepoint*). Confidentiality refers to the protection of access to information and data from unauthorized parties. Essentially, anti-virus and anti-malware software will protect the integrity of a device’s data, meaning the authenticity of it, and the confidentiality of the data, meaning the unauthorized access of this data. The two main ways that this is done is through sandboxing and behavior monitoring, which I mentioned above. Discussing these two aspects of the CIA triad brings about the conversation of what is at risk if one does not implement anti-virus or anti-malware software.

The security risks of not using anti-virus or anti-malware software are quite numerous. One security risk is access of personal information, such as social security numbers, addresses,

Hearne 3

insurance policy numbers, bank account numbers, etc. Another security risk is lost data, which heavily applies to companies and businesses. “One employee clicking a malicious link can infect your entire computer system with a destructive virus that can shut down your network, wipe your hard drives, and spread to other companies and clients through the internet” (Chron). Money loss is one of the most important security risks. Time spent dealing with an infection from a virus or from malware can translate to massive amounts of money lost, simply because time spent dealing with the infection is time spent not making money. One more threat associated with not implementing anti-virus or anti-malware software is server hijacking (Chron). “An unprotected business can serve as a threat to others. One reason hackers attack systems is to take them over for their own uses” (Chron). Once the system has been compromised, the hacker can implement a variety of malicious acts that can cost a company monumental amounts of money.

Two contemporary anti-virus and anti-malware products that are in use today are Avast and Kaspersky. Kaspersky is an anti-virus/anti-malware program developed by Kaspersky Lab. Kaspersky is one of the leaders in today’s anti-virus/anti-malware industry. It holds approximately 6.7% of the worldwide market share (Danchev). It is compatible with Microsoft Windows, macOS, and Linux. However, the Linux version is generally only available for businesses. Kaspersky is generally designed for personal usage, not necessarily for businesses. Kaspersky uses real-time protection, detection and removal of harmful malware, and removal of rootkits (software tools that allow a user to gain control of a device without detection). The cost of Kaspersky varies, depending on the number of devices one wishes to protect. Three

Hearne 4

devices cost approximately $90 per year, five devices costs $100 per year, and the family package (20 devices) costs $150 per year (Nadel).

Avast is a cross-platform of internet security applications, which includes anti-virus/anti-malware applications. Avast is also the leading anti-virus and anti-malware program, with a worldwide market share of 17.4%. (Danchev) Avast is compatible with Microsoft Windows, macOS, Android, and iOS. Avast essentially contains a variety of anti-malware and anti-virus software. Avast provides protection using mainly sandboxing and behavior scanning. Quite surprisingly, Avast is a free application. Nonetheless, one can opt for the Pro version of Avast, which includes some added benefits, like sandboxing and SafeZone Browser. SafeZone Browser essentially blocks ads, secures personal information via sandboxing and behavior scanning, and helps one to stay anonymous while accessing the internet. The Pro version of Avast is highly recommended if more advanced security measures are desired. A one-year subscription is $35, a two-year subscription is $70, and a three-year subscription is $105. This is quite cheap when compared to Kaspersky anti-virus. (Avast Pricing)

Overall, anti-virus and anti-malware applications aid in protection by covering the confidentiality and integrity aspects of the CIA triad. There is no anti-virus/anti-malware application that is one-hundred percent effective, however. Nonetheless, most of these applications will adequately provide protection of personal information, data, devices, etc to warrant a purchase. In today’s digital age, anti-virus and anti-malware software is arguably essential, especially for large companies that risk large amounts of money.

Works Cited

“Avast Pricing 2019: Ultimate Review Price for Each Product.” *Thinkmobiles*, thinkmobiles.com/blog/antivirus-avast-pricing-ultimate-review/.

Danchev, Dancho. “Which Is the Most Popular Antivirus Software?” *ZDNet*, ZDNet, 27 June 2012, [www.zdnet.com/article/which-is-the-most-popular-antivirus-software/](http://www.zdnet.com/article/which-is-the-most-popular-antivirus-software/).

“What Is Anti Malware?: How Anti Malware Software Works?” *Comodo Enterprise*, 30 Nov. 2018, enterprise.comodo.com/what-is-anti-malware.php.

“What Is the CIA Triad?” *Forcepoint*, 26 Feb. 2020, www.forcepoint.com/cyber-edu/cia-triad.

“Confidentiality, Integrity, and Availability.” *MDN Web Docs*, developer.mozilla.org/en-US/docs/Web/Security/Information\_Security\_Basics/Confidentiality,\_Integrity,\_and\_Availability.

Nadel, Brian. “Kaspersky 2020 Review.” *Tom's Guide*, 28 Feb. 2020, [www.tomsguide.com/reviews/kaspersky](http://www.tomsguide.com/reviews/kaspersky).

Yusuf, Muchelule & Neyole, Wanjala & Jacob, Misiko & Muchelule, Yusuf & Neyole, Jacob. (2017). Review of Viruses and Antivirus Patterns Software & Data Engineering Global Journal of Computer Science and Technology: C Review of Viruses and Antivirus Patterns. Journal of Computer Science and Technology. 17.

“What Is a Virus Signature?” *Computer Hope*, 26 Apr. 2017, www.computerhope.com/jargon/v/virus-signature.htm.