Device Security

Exploring Solutions in User Device Protection

Dylan Dobbins, Donald Ivy, Sahil Kaneria, Matthew Mabrey, Zachary Sparacio

SRS 150-203

Professor Christopher Simber

December 8th, 2018

Introduction

As our software and hardware has advanced and more of our world is pushed online, we have become increasingly vulnerable to the threat of viruses and malware. Consumers often take the safety of their devices for granted, preferring the most convenient option instead of what may best meet their needs. This can potentially leave the consumer worse off, as they may overestimate the abilities of their antivirus and fall victim to easily avoidable malware attacks. This research paper investigate the effectiveness of free and paid consumer-level antivirus\malware offerings, their methods of securing devices, and analyze the trends of new products being released to the public. This paper will provide the basis for determining the most effective solution for a consumer to secure their device. It will also explore the differences between blacklist and whitelist security. The difference between the two is that of an ultimatum: to allow access to everyone except those on a blacklist, or allowing access to a small group on a whitelist. Those two solutions cover two radical ends of a security spectrum, so we will try and find a common ground in the middle, if such a solution exists.

Anti-virus Software

Antivirus software are programs which are designed to prevent malicious pieces of code from running and eliminating them. These software have a virus database which updates regularly. The virus database contains a list of potentially harmful code. During a computer scan, the antivirus software scans files and compares their code with their virus database. If malicious code is found, the antivirus will take action or will ask the user to take action (Comondo). Antivirus software have a long history, dating back to the 1980s (Bradford). The first unofficial antivirus was created in 1983, named the Reaper. This was created in response to the first widespread computer virus known as the "Creeper". Back then, people weren't even aware of the term "virus" until it was coined by an American computer scientist Fredrick Cohen. Since then, technology evolved rapidly and so did the viruses. In response to these growing number of viruses, new software was developed by companies to prevent the replication of viruses and soon after remove most computer viruses. Today's "antivirus software" has evolved to great lengths. It not only deletes computer viruses, but also has built-in firewalls, internet protection, malware protection, etc. The typical antivirus software is responsible for scanning one's computer for commonly found viruses and deleting them, as well as updating its virus database regularly so that its aware of newly created viruses. Antivirus software has come a long way since the 20th century. Infact, companies use them as a money-making tool now. There are several major antivirus companies who try hard to gain new customers for their products. To keep the business alive, antivirus software companies have evolved into not only deleting computer viruses, but also malware, ransomware, spyware, etc. The first results when the term "antivirus" is searched for on Google is a bunch of ads from different software companies trying to sell their 'premium'

antivirus product. However, there are still a variety of cheaper or free antivirus alternatives available in the market. Independent lab testing has shown that free antivirus software is generally as good and as reliable as paid premium antivirus software. But there are still some major differences which sets the two apart. Let's compare two of the most common antivirus software: Windows Defender (which is a free antivirus integrated into Windows 10) and BitDefender Total Security (which charges $140 for three years for five users).

Often times, the single most thing which matters the most is convenience and ease of use. Windows defender integrated into the system and is present by default when windows is installed, whereas BitDefender needs to be installed. This gives Windows Defender the upper hand because the user does not have to do anything once they start using Windows. However, paid antivirus software requires payment and installation. It might not be worth the effort and some users may find the costs to be high. In rare cases, installations might fail and end up creating a multitude of other problems. Both these antivirus products feature a simple and easy-to-use user interface so that the user does not have a big learning curve

Another important factor to consider, especially in today’s internet based world, is the performance of the antivirus software. Windows Defender offers basic protection against viruses for consumer devices and since it's free, its safe to assume that its virus database might not be as up to date as BitDefender’s. BitDefender usually puts more money into R&D and quick database updates. This is proven by tests conducted by the Independent IT- lab institute. Tests show that BitDefender has a perfect score in virus protection. Windows Defender scored slightly lower than BitDefender. However, the difference is not that significant and both of them are still in the upper tier.

For the best protection, BitDefender offers additional security features when you buy its Total security package. They offer additional features like URL checks, password vaults, VPN and online payment protection. These features act as the first line of defense against viruses. Windows Defender, being free, does not offer these features. This definitely gives BitDefender the leading edge. However, some users might argue that these features may not be that necessary and are not worth paying for. In some cases, these additional features might go unused by consumers.

Lastly, another important aspect for antivirus software usage is the consumer support. BitDefender has much better support as they have dedicated customer support lines. While the tech-savvy people don't really need to use the support, there are still plenty of people who don't know how to use or set up the antivirus software. Windows Defender only has an online support website which gives basic information on usability.

In conclusion, it is up to the consumer to choose the best fit for them. To reiterate, independent lab testing has shown that free antivirus software such as Windows Defender do an equally good job when compared to paid antivirus software. But what really sets the paid antivirus software apart is the additional features they provide to enhance the security of one's device; some of them are actually very useful in today's digital world.

Mobile Device Security

While anti-virus and anti-malware are big concerns for our personal computers and laptops, do the same concerns carry over to the smartphones and tablets we carry around every day? The answer is actually quite complicated and needs some explanation. The term "virus" which your average consumer has become quite familiar with, is incorrectly used as a broad term covering any type of malicious software. In reality, a virus is a replicating program that attaches itself to other programs, while malware is the correct term to cover any type of malicious program like spyware or ransomware. The good news is that the replicating viruses that pose a constant threat to our PCs have yet to be detected on our mobile devices. Unfortunately, there is still a possibility of malware getting onto a device, which means consumers can't stop worrying yet.

Android and Apple devices are the two main targets for malware today with other alternatives such as Blackberry and Windows phones not having a large enough user base to be significantly targeted. By far, the most targeted of the two is Android. In fact, according to Olaf Pursche, Head of Communications at AV-TEST, in the F-Secure State of Cyber Security 2017, "There are over 19 million malware programs developed especially for Android, making Google's mobile operating system the main target for mobile malware" (Proske, "Another Reason 99% of Mobile Malware Targets Androids"). This is mainly due to Android's more relaxed stance on security when downloading mobile apps. Unlike Apple's app store which is very selective on what it will allow its customers to download, Android phones easily allow users to change a setting to be able to download APK (Android PacKage) files from unknown sources, meaning anything not from the Google Play Store. This allows fraudulent apps to enter

the marketplace that may disguise themselves as innocent looking apps or offer free versions of normally paid apps. This is why malware overwhelmingly targets Android users opposed to Apple users. It is recommended that Android users only download reputable apps with good reviews from well-known app stores like Google Play.

Although being cautious about the apps you download will reduce the risk of malware getting onto your mobile device there are still other measures that must be taken. Drive-by-downloads, a type of malicious file download that can happen on untrustworthy websites without any actions from the user, require some sort of anti-malware program similar to those we have on our computers. The problem is that a large percentage of mobile device users don't have any security on their device whatsoever. In a Kaspersky mobile security report, they found that only 43% of Apple iPhone users and 53% of Android users use security systems ("Number of the week: 40% of modern smartphones owners do not use antivirus software"). And even in the case of iPhone, their security apps were lacking because iOS makes it impossible to create an app that offers complete protection. Apple's philosophy is that iOS was built from the ground up to be very secure and as such does not need any third party programs to protect it. Because of this, they will not allow comprehensive anti-malware apps onto their app store. This means that the only real market for any type of anti-malware app is on the Android app stores.

There are plenty of options for security in the world of mobile devices, and while some are better than others most follow the same plan of a free base app with a paid subscription to access the more complex security features. In this case, the paid versions are well worth what you're paying for. The free features are often very similar among most apps with the paid security features varying from app to app. For example, the Norton Mobile Security app which

offers call and text blocking, contacts backup, and anti-theft functionality for free with a unique paid App Advisor feature which verifies installed apps and apps on the Google Play store for security and privacy risks. Another example is the CM Security Master app that has unlimited VPN (a service that secures your information from other users on public wifi and disguises your device location from websites) and an ad blocker as it's paid features. While most consumers will opt for the free but limited anti-malware apps Tom's Guide, a popular tech review website that tested and reviewed these anti-malware programs and more, continually found that the best options for security were paid, not free. Their best choice was the paid only app Bitdefender which gave almost perfect malware protection, along with comprehensive privacy-protection tools, and a minimal impact on device performance (Wagenseil, "Best Antivirus Software and Apps 2018"). However while paid apps offer more than their free counterparts, having any app at all is better than nothing.

Overall, while malware is not as widespread on mobile devices as it is on our desktop computers, it is still something to be concerned about. There are threats out there and with an increasing amount of consumers storing more valuable personal information on their mobile devices the threats will only increase. The best action for the consumer is to take precautionary steps in securing their mobile devices such as conscientious app downloads and installing a robust anti-malware.

Peripheral Devices

When a cyber attack or data breach is concerned, the last thing on the mind of an end user is the devices they use daily. Yet, the devices we use to conduct business, and use for fun, are constantly at risk of an attack perpetrated by a malicious actor. This includes a broad scope of devices, but is not limited to keyboards, mice, and USB ports, to name a few examples.

Over the last few years, the time-honored Universal System Bus (USB) standard has been upgraded. Specifically with the introduction of the Type-C connector. Introduced in 2013, the Type-C connector is an evolution of the conventional Type-A connectors seen on computers, mobile device charging plugs, even wall sockets in some homes and businesses. In efforts to reduce the 51,000 tons of electronic waste generated per year at the time("One Mobile Phone Charger for All Campaign - Growth - European Commission."), the European Union launched the campaign for a "common charger" in 2009. At that time, device manufacturers agreed to adopt the Micro USB standard for charging and data transfer. Apple Computer was an exception, continuing to use their 30-pin connector, and later their proprietary Lightning connector for cell phones and tablets. With the advent of USB-C, their campaign has once more been introduced into the conversation, with the EU considering adoption of the USB-C standard. However, with that motion to standardize and rapidly accept a new technology, comes security concerns and growing pains associated with it.

In the age of dependence on devices to stay present in today's connected world, the need for a charge is often prioritized over keeping your data secure. To every user, this may prove to be quite dangerous. In an experiment conducted by San Francisco-based security firm Authentic8 at the 2017 RSA Conference, they offered a free charging station at their booth to

conference attendees, replete with cords and adapters provided by the firm. In their time conducting the experiment, Authentic8 discovered that about 80% of attendees used their charging station without questioning its security (Forrest, "Free charging stations can hack your phone, here's how to protect yourself.").

Through modified microcontrollers in a USB drive or mobile device charging port, a potential attacker is able install malware which copies data from a connected device without the user's knowledge or consent. This phenomenon is known colloquially as "juice jacking." What makes juice jacking possible lies in the way USB works. When a device is connected to a USB port, it attempts to "handshake" with the port - at this point some data is transmitted, usually the device's name, serial number, and vendor name (Forrest, "Free charging stations can hack your phone, here's how to protect yourself."). Since USB is set up as a "two-way conduit", as Authentic8 marketing head Andrew Paik states (Forrest, "Free charging stations can hack your phone, here's how to protect yourself."), it allows for simultaneous data transmission and power for charging; which allows the attacker to copy data from devices connected to the modified USB port.

What seems to be the best avenue for mitigating risk of data falling into the wrong hands? As public charging stations are concerned, an attacker could still gather data from a device. Even if it is set to a power-only mode from the operating system, it still needs to complete the "handshake" between device and USB port, thus it transmits data only to complete that process; though data can be gathered no matter how small the window in time. If a user finds themselves in need of a charge, their best course of action would be to bring along their charging cable and adapter from home, or to purchase a USB battery pack from a retailer. The experiment from

Authentic8 mentioned prior demonstrates, in writer Conner Forrest's own words, that "smartphone owners don't take their security seriously enough."(Forrest, "Free charging stations can hack your phone, here's how to protect yourself") Users conclude that, since their devices are on a platform besides Windows or Macintosh personal computer, their security is guaranteed. Although cybersecurity is a field of constant change, proactive thinking on behalf of the end user will go a long way.

Blacklisting

Looking into some of the components of anti-virus and anti-malware, we stand to see two main listing techniques that are mainly utilized in anti-virus/malware software. These two listings are called blacklisting and whitelisting. Blacklisting is a database that keeps track of details related to malicious or suspicious programs and entities that are not allowed access to a system or network. These suspicious programs can include viruses, spyware, and keyloggers (programs that record keystrokes from user). Theoretically, whether the device be a phone, laptop, or home computer, the suspicious programs should be accounted for in any consumer device. (.FInjan. "Blacklisting vs Whitelisting - Understanding the Security Benefits of Each.") The major concern with these blacklisted programs , which apply to all consumer devices, is that like a physical virus, they can spread to other users, businesses, IP's, or enterprises.

One of the many advantages of blacklisting is that it can identify any malicious programs or malware , thus preventing it any access that can hurt user devices.. For consumers, there is not much upkeep required to prevent this issue, only updating apps and programs (ex.Outlook). Having these apps on auto-update can essentially eliminate any consumer input, allowing for simplicity and safety. However, safety and security relies on both users and the ones maintaining the blacklists. If users do not update (not having auto-updates on), it can make new and improved viruses infect their devices. If the maintainers do not keep their blacklists up to date, they can jeopardize millions of users device safety by making them susceptible to the viruses and malware. Blacklisting is easy to manage by simply adding new programs and entities onto the list to continue user protection.

Blacklisting is flawed in that it can only protect what it knows to be malicious. Attackers

can constantly adapt and find new ways to overcome new blacklists, meaning that many security intelligence agencies must keep up with updates of their blacklists . There is no complete solution yet to this issue with blacklisting, so solutions must constantly keep evolving. About every four seconds, a new piece of malware is contrived , and updates to the blacklist database are essential for users to protect them from these new viruses. (Benzmüller, "In 2017 Every 4.2 Seconds a New Malware Specimen Emerges.")

Whitelisting

Simpler than blacklisting, whitelisting is a list of programs and software that are allowed access, but anything not on the list is denied access. A "zero trust" principle (.FInjan, "Blacklisting vs Whitelisting - Understanding the Security Benefits of Each.") prevents any access, only allowing what the whitelist deems necessary. This can be simple as identifying apps based on file name, size, and directory paths. However, whitelisting can also be complex as how NIST (National Institute of Standards and Technology) utilizes it by combining cryptographic hashing techniques (turning data into unique strings of text. For example, turning the word "Hello" into a encrypted string "f7ff9aeb87b" . . .) and digital signatures linked to the manufacturer or developer of each component of software. Whitelisting can be given a perfect example, since it is already integrated into something almost any user with a device has, an email. More specifically, the spam folder to prevent malicious emails from being sent. The spam folder fillers out suspicious emails just like whitelisting.

There are many benefits to using whitelisting over blacklisting. One of these advantages is allowing access to a small number of programs and entities into the whitelist, which restricts

the use of network and resource access to few people, but can greatly reduce malicious intrusion. It can also help by letting specific applications and software to run, preemptively preventing malware from trying to access user programs and systems. It would also prevent the malware from accessing the user's personal data such as bank account information and important passwords. Whitelisting is actually recommended by NIST by the strong, strict security that it provides. Whitelisting is also used in many industrial and corporate environments. This is mainly due to the fact that companies have more resources to protect, and putting these applications and programs onto a whitelist would ensure the company's protection greater than blacklisting. Overall, this makes the company more secure, more accurate, and minimizes false positives which are errors in some evaluation processes where a condition tested is mistakenly detected. In spam filters, a false positive is a legitimate message mistakenly marked as UBE (unsolicited bulk email), as junk email is more formally known. Another benefit to whitelisting is that it is easily customizable. A user can choose how many or how few programs should be on the whitelist, allowing not only strong protection, but flexibility in security.

As advantageous as whitelisting may be, it can also prove to have a fair share of flaws. More often than not, a standard cybersecurity section IT department that works for a large, valuable company must increase the amount of resources needed to manage the impact of keeping track of valid resources and impacting it's users. The IT department must be kept up to date, but must be wary of user activity and user privileges. They must be careful in not giving user access to inappropriate rights, such as being able to access things that aren't meant to be accessed by the user or take away essential rights to their devices. Since implementing whitelisting requires more managerial attention in terms of impacting end-user productivity, this

requires more management than blacklisting. Implementation and installation for whitelisting can also be a larger task than blacklisting. For how precise it must be refined to find the balance between user access and user protection, more time must be consumed to perfect it's goal of protecting users. The whitelist cannot constrict user access to provide the most protection, but must also not give a user too much access to where they are more vulnerable to malware attacks. This in turn gives users and businesses more control over their resources,while lessening the risk for tampering with assets, such as confidential information that large corporations like Lockheed Martin would not want into the average user's hands.

Greylisting

Whitelisting brings many advantages, because of this there are not many product offerings or alternatives to both blacklisting and whitelisting. That being said, there exists a third known listing, but is much smaller in scope to blacklisting and whitelisting. This third list is known as greylisting, which is another approach to protecting users, but more in the form of specializing in spam prevention and blocking. Greylisting is used to detect if a message of a serving sender is RFC (Requests for Comments) compliant, meaning that the emails are consistent with the internet standards for such documents and mail. (Bjarne, "Greylisting Explained"). Greylisting can be done through temporarily blocking any unknown senders and cache the details of the initial message. If the spammer sends it again, it can essentially catch to see if spam is being conducted.

Future of Anti-Malware

The future of anti-malware technology is uncertain and always evolving. It is a constant back and forth, as new forms of malware necessitate new forms of defense. While it is nearly impossible to outline the future of technology with any form of certainty, there are a few new possibilities on the horizon.

One of the most promising new technologies being utilized against malware is blockchain verification (Pamerleau, "Blockchain: The Future of Cybersecurity?"). The decentralized nature of blockchain creates multiple copies of non-manipulable records of access. Multiple companies are beginning to use this technology to safeguard systems. REMME is using blockchain verification to develop secure single-use passwords, and built their entire business around the security of their methods (Pamerleau, "Blockchain: The Future of Cybersecurity?"). Others are using it to create secure personal profiles that require multiple levels of authentication to be accessed. The main value of blockchain technology is its removal of one of the least secure parts of a network: humans. By automating login information and removing the possibility of human error, blockchain authentication is a promising new frontier of security. Malware cannot intercept passwords when they are securely generated and verified by an entire network of machines per login.

Additional companies are beginning to implement machine learning to analyze threats and develop solutions to them. Though many companies advertise their products as using AI, few, if any, actually use it. Rather, most security companies are using machine learning to train

software to recognize the characteristics and symptoms of specific attacks (Newman, “AI Can Help Cybersecurity - If It Can Fight Through The Hype”).

The adoption of machine learning offers certain advantages and disadvantages. One of the most prominent drawbacks is that the software can only recognize attacks it has been trained for. While the software can always be updated with more data, it leaves enough of a loophole to put some experts on edge about the efficacy of machine learning security. A major advantage of machine learning over traditional antimalware is its method of detecting a threat. While traditional methods of security look for threat specific signatures to determine what is a threat, machine learning scanners hunt for and recognize specific characteristics (Newman, “AI Can Help Cybersecurity - If It Can Fight Through The Hype”). A common shortcoming of traditional antivirus is that a hacker could simply edit enough code within their malware to throw off its signature and be nearly invisible to security programs. Machine learning software analyzes the entirety of the suspected malware and connects several key characteristics to determine if it is a threat. Since building completely new malware is often difficult and time consuming, most hackers build off existing malware to suit their needs. This allows machine learning software to evolve at a far slower pace, since it is easy for a program trained on a wide variety of threats to recognize something slightly new.

Works Cited

Albright, Dann. "Does Your Smartphone Need Security & Antivirus Software?" *MakeUseOf*, 3 Mar. 2016, www.makeuseof.com/tag/smartphone-need-security-antivirus-software/.

Benzmüller, Ralf. "In 2017 Every 4.2 Seconds a New Malware Specimen Emerges." *In 2017 Every 4.2 Seconds a New Malware Specimen Emerges*, 10 Apr. 2017, www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017.

Bjarne. "Greylisting Explained." *Greylisting.org*, 14 Oct. 2016, www.greylisting.org/.

.FInjan. "Blacklisting vs Whitelisting - Understanding the Security Benefits of Each." *Finjan Blog*, Publisher Name Finjan Publisher Logo, 1 May 2017, blog.finjan.com/blacklisting-vs-whitelisting-understanding-the-security-benefits-of-each/

Forrest, Conner. "Free Charging Stations Can Hack Your Phone, Here's How to Protect Yourself." TechRepublic, ZDNet, 16 Feb. 2017, www.techrepublic.com/article/free-charging-stations-can-hack-your-phone-heres-how-protect-yourself/.

Newman, Lily Hay. "AI Can Help Cybersecurity-If It Can Fight Through the Hype." *Wired*, Condé Nast, 27 Apr. 2018, www.wired.com/story/ai-machine-learning-cybersecurity/.

Straub, Jeremy. "With USB-C, Even Plugging in Can Set You up to Be Hacked." The Conversation, The Conversation, Inc., 21 Sept. 2018, theconversation.com/with-usb-c-even-plugging-in-can-set-you-up-to-be-hacked-102296.

Wagenseil, Paul, and Tom's Guide STAFF. "Best Antivirus Software and Apps 2018." *Tom's Guide*, 9 Nov. 2018, 7:15 AM, www.tomsguide.com/us/best-antivirus,review-2588-7.html.

"Another Reason 99% of Mobile Malware Targets Androids." *F-Secure Blog*, 7 June 2018, blog.f-secure.com/another-reason-99-percent-of-mobile-malware-targets-androids/.

"Blockchain: The Future of Cybersecurity?" *Armor*, 16 May 2018, www.armor.com/blog/blockchain-future-cybersecurity/.

"New Books." *Introduction to Computer Ethics*, www.infosectoday.com/Articles/whitelist.htm.

"Number of the week: 40% of our modern smartphone owners do not use antivirus software." *Kaspersky,* 26 Sep. 2012 www.kaspersky.com/about/press-releases/2012_number-of-the-week-40-of-modern-smartphones-owners-do-not-use-antivirus-software.

"One Mobile Phone Charger for All Campaign - Growth - European Commission." The Directorate-General for Internal Market, Industry, Entrepreneurship, and SMEs, The European Commission, ec.europa.eu/growth/sectors/electrical-engineering/red-directive/common-charger_en.

"Should You Worry About Getting a Cell Phone Virus." *Lookout*, www.lookout.com/know-your-mobile/android-virus.

"The State of Cyber Security 2017." *F-Secure Blog*, 15 Oct. 2018, blog.f-secure.com/the-state-of-cyber-security-2017/.

Bradford, Alina. "What Was the First Antivirus Software?" *TopTenReviews*, TopTenReviews, www.toptenreviews.com/software/articles/what-was-the-first-antivirus-software/.

"Test Antivirus Software for Windows 10 - October 2018." *Statistics & Trends Report | AV-TEST*, 23 Nov. 2018, www.av-test.org/en/antivirus/home-windows/.

"How Antivirus Works? | How Antivirus Software Detect Virus." *Comodo Antivirus Blogs | Anti-Virus Software Updates*, Google, 5 Oct. 2017, antivirus.comodo.com/how-antivirus-software-works.php.