UNIVERSITY OF CENTRAL FLORIDA

FRONTIERS IN INFORMATION TECHNOLOGY

COP 4910

CLASS FINAL REPORT

Abstract

This report brings together the final papers presented by the students in the Frontiers in Information Technology class, COP 4910 during the Spring-2015 semester. In addition, it is worth mentioning that this semester the students attended 76 talks and each student gave 4 presentations. In each talk they had to present the technical aspects of the selected topic along with its social impact, ethical aspects, and professional impact.

Antivirus Software

Final Paper

Nick Kirby
COP 4910
University of Central Florida
Spring 2015

Joseph Ululati
COP 4910
University of Central Florida
Spring 2015

***Abstract*— The purpose of this research is to explore various topics regarding antivirus software, including: an introduction to the technology, technical aspects, professional impacts (careers), social impacts, and the ethical issues associated with the technology. The first phase of this research involves an introduction to antivirus software, followed by an overview of detailed technical aspects associated with this technology. This information is presented in the second phase to show the influence as well as the importance this technology has in today's society. This research also provides valuable professional information regarding the application and development of careers in the realm of antivirus software. Evaluation of antivirus software, the related technology, and the place this technology holds in society will prove beneficial in the overall understanding and protection of individuals and corporations alike in the new digital age.**

I. INTRODUCTION

Many threats that have been developed within the past decade have incorporated many advanced techniques to avoid detection and prevention. A few of these techniques include pseudo-randomized domain command and control servers, bidirectional channel communication, obfuscation and encryption, custom kernel modules/ drivers, and custom virtual file system containers. Some of the malware that have implemented many of these techniques within the past decade include: the Storm botnet, Conficker, Stuxnet, Duqu, Flame, CryptoLocker and Regin. This research will primarily focus on antivirus software developed in order to detect, search for, and prevent the narrow scope of cyber attacks that include computer viruses, worms, Trojan horses, and adware/spyware [1]. This research will go over valuable professional information regarding the development, implications, and future of antivirus software in general.

Section 1 has given a brief introduction to antivirus and virus technology, history, and the importance antivirus solutions in today's society. In section 2 we discuss technical aspects of antivirus software, followed by professional impacts (careers and required education) in section 3. We further discuss the important social aspects and ethical issues related to antivirus software in sections 4 and 5 respectively and then finishing with a conclusion in section 6.

II. TECHNICAL ASPECTS

Antivirus solutions are extremely complex and sophisticated software packages designed to detect and prevent the execution/spread of malicious code. In the past before the dawn of the internet, most of the antivirus solutions at the time existed on physical media and thus were updated only seldomly. In addition, the technology at the time only used a basic dictionary-based search scheme. Present day antivirus software mainly consists of five different detection methods: dictionary approach, heuristic approach, beginning approach, and the sandbox approach.

The first detection approach is known as the dictionary approach. In this scheme, antivirus engines scan through files looking for code sections, which are then compared to signatures of existing viruses/malicious code in a database. If the antivirus engine finds a match, it then has the option to either delete the file, quarantine it, or attempt to repair the file by carving out and removing the existing malicious code [4].

The second detection approach is known as the heuristic approach. This approach focusses on the behavior aspects of a system rather than searching for and comparing possible virus/malicious code signatures. In this scheme, the antivirus engine establishes a baseline of system activity and will then monitor the system for any deviations of that activity [5]. This approach is preferred over the dictionary approach when

concerned about new threats because new the database definitions are not always up to date with the latest as well as unknown threats. When using the heuristic approach, many new previously unknown threats can be found by monitoring system activity, as well as identifying encrypted or packed threats. There are two main downsides to using a heuristic detection method. First, if the system is already compromised before the antivirus engine can establish a baseline, the activity from the malicious software may become part of the baseline rather than measure of deviation. Secondly, often time's legitimate software can cause a system to deviate from its standard activity [6]. This can many times lead to false positives, or legitimate software being flagged as malicious. It is also important to note, that if too many false positives arise, users may get used to ignoring the warning messages even when the antivirus engine detects an actual threat.

The third detection approach is known as the beginning approach. This approach uses a variation of the heuristic based method in order to detect an opposing threat. In this method, the antivirus engine will intercept suspected virus code before it reaches the executable. Antivirus software will then emulate the beginning portion of the code and will then determine if the emulated actions are along the lines of malicious intent or not (usually determined by heuristic baseline). This method is generally good at detecting malicious, polymorphic malware since often times the methods or instructions that induce the change are one of the first actions this type of malware completes.

The fourth detection approach is the sandbox detection approach. This approach is one of the more modern methods antivirus engines use and consists of various uses of virtualization and cloud based technologies. In this method, antivirus engines emulate the entire host's operating system (either in the cloud or in a compact virtual container on the local machine) and run the suspected malware in the emulated virtual machine. The results are then aggregated and a decision is determined by the antivirus engine based on the execution of the suspected malware.

The fifth and final detection method is known as the real-time detection approach. This approach is very similar to, and is often an extension of the heuristic detection method and utilizes a number of advanced technologies to monitor the host system in real time. In this method, antivirus engines use kernel and user mode hooking in order to monitor and intercept suspicious API calls [7]. For example, registry and thread/process API calls are very closely monitored by antivirus engines. These antivirus engines use hooking techniques in order to be able to monitor and restrict which resources are available to a specific process, such as specific modules or DLL's [4].

Modern antivirus solutions have adopted many other techniques and technologies in order to protect the end users. Most antivirus solutions come packaged with a software defined firewall, which often incorporates IDS/IPS abilities to capture and monitor network traffic leaving and entering the machine. New antivirus solutions come with a variety of backup services, scheduled scanning, vulnerability scanning, password managers, secure file deletion, parental controls, white and black listing, phishing detection, virtual keyboards, safe-mode emulation, and optional recovery tools.

III. Professional Impacts

The professional impacts of antivirus software are firmly rooted in the future. Due to the fact that antivirus software is the main, and often times only, line of defense against malware and viruses, developers need to move as fast as possible to keep up with the every-growing list of harmful files and worms being created by devious minds. This technological "arms race" essentially puts antivirus development in a constant state of growth, new jobs are being created every day, and more people to do the current jobs are sought after as well. As is the case with most software, the majority of the jobs needed for development fall into the Computer Science field rather than our IT area, but post-production upkeep and improvement give way for IT analysts and admins to step in and shine as well.

3.1 Marketing

For the majority of the population, the market of antivirus software is in the form of "freeware", or free-to-download software, available on the respective company's website. Another prominent marketing method some companies are utilizing are that upon buying a new computer, a user is offered a free 30-day trial of a given antivirus software that was bundled with the purchase. This "bundling" is likely the leading factor that leads to Security Essentials securing the top share of number of customers having real-time protection, as can be seen in the image below.

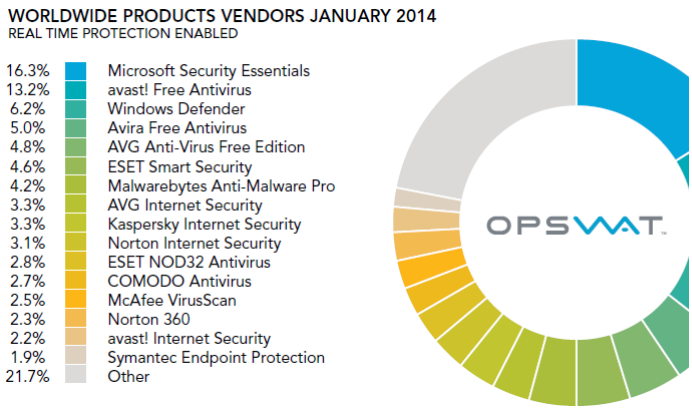

Fig. 2. Market share of various protection products.

A select few internet service providers also make use of this "bundling" method by partnering with a chosen antivirus company and giving their customers access to this partnered company's services that they would, under normal circumstances, have to pay for.

3.2 Careers

Among the many careers that are being offered pertaining to antivirus software, we will be featuring two relatively predominant positions that we feel are most integral to the creation of a successful antivirus. One of those jobs is that of the Antivirus Software Developer. This position is essentially the person who writes, runs, and develops the code needed for the initial creation of the software. Oftentimes companies will hire developers that have experience in writing code for full programs in their past, due to the extent and size of what an antivirus program should be. Virtually every large-scale development company (Microsoft, Symantec, Avast, etc.) is looking for new and more developers to aid their effort, and in fact the career market expects the annual pay for this position to increase by 22% by the year 2022 [8]. The current pay for this position sits at an average of $93,000 per year.

The second position is of the Penetration Testing Software Engineer. This specific type of analyst's job is to review, analyze, and modify programming systems done by the developers, including encoding, testing, debugging, and installing to support and improve any weak points that may be found during testing. Many times, these engineers will create self-made viruses to pit again the antivirus to asses detection and handling of the software. This position is just as essential as the developer itself, and the career market seems to expect well over 27,000 new Penetration Testing Software Engineer positions to open by 2022. People with this career on average have a salary of $85,000 per year [9].

3.3 Education

As previously stated, the career field relevant to antivirus software seems to benefit those studying Computer Science rather than Information Technology, but surely having a degree in IT will not turn a hopeful applicant completely off to any and all antivirus software positions. Specifically, the Antivirus Software Developer requires quite a bit of CS background to be considered and/or be successful. The vast majority of listings call for at least a Bachelor's degree in CS, with a Master's in Software Development or Programming preferred. If the applicant does not happen to have the elusive Master's degree, entry-level developer positions exist. Whichever route is taken, a software developer must be very well-versed in many programming languages, the most prominent being C++, PHP, and HTML for antivirus software specifically.

As for the Penetration Testing Engineer, a Bachelor's degree in IT or any technological field is sufficient. The only other major skill that companies ask an applicant to be educated in is being fluent in C++ for both Windows and Linux operating systems. This is most likely due to the software needing to be tested on any and all platforms it could possibly be used on [9].

Table 1. Potential Career Outlooks

Career	**Education/Experience**	**Salary**
Ativirus Software Developer	BS/MS in CS, or 4+ years exp	$72,000-$90,000
Penetration Testing Software Engineer	BS in any technical fied, or 4+ years exp	$85,000

IV. Social Impacts

Normally, when one thinks of the finer aspects of antivirus software, being socially impactful is not a main idea. In today's day and age, anything and everything can have an impact on our social collectiveness, and antivirus is no exception. A prime example of this is the creation of Immunet in 2009. The company (who also called their software Immunet) ventured to make an antivirus that checks downloaded files against a directory of viruses and malwares that can be updated and shared between common "friends" on a social network. Not only does this software specialize in protecting users against the type of malware that is being increasingly spread through mediums like Facebook and Twitter, but it uses these same mediums to send and share data about these viruses and malware to fellow users to also have Immunet. Their hope is to eventually connect as many people through Immunet as possible to create an exponentially stronger

database, but it does not seem to have grabbed the footing that they hoped [10]. The use of social media somewhat humanizes antivirus software, and puts the act of improving more on the shoulders of the users.

V. Ethical Issues

It was mentioned in a previous section that penetration testers will sometimes create their own viruses or malware to test the software. The ethical problem with this procedure is two-fold; these manually created viruses, much like living organisms, always have the chance of escaping the testing field and harming outside systems, and it is supposedly not even an effective way of doing heuristics testing in the first place. In addition to this, if this method of testing for unknown viruses is a relatively ineffective, then it causes many to question the need to take the chance of such danger at all. [11]

VI. Conclusion

Antivirus software is proving to be just as important of a piece of a computer's software as the operating system itself with the ever-growing strength of malware and viruses infecting users through more and more mediums. The truth is that all the antivirus needs of a normal household can be met with a quick and easy free download from any of the top trusted names, and doing so can do nothing but help. Antivirus software has many types of detection methods and algorithms for differing kinds of malware, which allows for creativity and expansion in the career field that is currently exploding with very high pay as well. In its relatively short history of existence, antivirus software has evolved greatly, and can only improve with further usage and input/report-sending habits of users worldwide.

References

[1] Criddle,Linda. Http://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software. N.p., n.d.

[2] Donchenko, Igor. "History of Computer Viruses." History of ComputerViruses. http://www.antivirusworld.com/articles/history.php. N.p., n.d. Web. 22 Feb. 2015.

[3] Y. Yiming, A. Clementi, P. Stelzhammer. "Free Antivirus and Its Market Implementation". BoD – Books on Demand, Oct 2014

[4] Hodges, Vernon, and Shawn O'donnell. "Method and system for providing automated updating and upgrading of antivirus applications using a computer network." U.S. Patent No. 6,269,456. 31 Jul. 2001.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[7] North, Max M., Roy George, and Sarah M. North. "Computer Security and ethics awareness in university environments: A challenge for management of information systems." Proceedings of the 44th annual Southeast regional conference. ACM, 2006.

[8] Bureau of Labor Statistics. "Software Developers" Occupational Outlook Handbook. U.S. Bureau of Labor Statistics, 8 Jan. 2014. 22 Feb. 2015. http://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm#tab-1

[9] Indeed Jobs. "Antivirus Software Jobs". Antivirus Software Jobs. N.p., n.d. Web. 22 Feb. 2015. http://www.indeed.com/q-Antivirus-Software-jobs.html

[10] Lemos, Robert. "Antivirus Protection Gets Social". MIT Technology Review. Technology Review. 21 Aug. 2009. 22 Feb.2015. http://www.technologyreview.com/news/414997/antivirus-protection-gets-social/

[11] Hashimoto, Gilberto Tadayoshi, Pedro Frosi Rosa, and Jayme Tadeu Machado. "A Security Framework to Protect Against Social Networks Services Threats."Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on. IEEE, 2010.