Malware Detection and Removal: An examination of personal anti-virus software

Patryk Szewczyk
Edith Cowan University

Murray Brand
Edith Cowan University

Malware Detection and Removal: An examination of personal anti-virus software

Patryk Szewczyk & Murray Brand
SECAU Security Research Centre
Edith Cowan University
Perth, Western Australia

Abstract

SoHo users are increasingly faced with the dilemma of applying appropriate security mechanisms to their computer with little or no knowledge of which countermeasure will deal with which potential threat. As problematic as it may seem for individuals to apply appropriate safeguards, individuals with malicious intent are advancing methods by which malicious software may operate undetected on a target host. Previous research has identified that there are numerous ways in which malware may go undetected on a target workstation. This paper examines the quality of malware removal programs currently available on the market, which consumers may use whilst utilising the Internet. The research suggests that current anti-virus products, whilst able to detect most recently released malware, still fall short of eliminating the malware and returning the system to its original state. The paper does not compare or disclose potential flaws within each product; rather it depicts the current state of anti-virus products.

Keywords

INTRODUCTION

It has been argued on numerous occasions that access to the Internet can be beneficial from a financial, social, recreational and educational perspective. As a result, the number of individuals acquiring Internet access in Australia alone is steadily increasing. The population in Australia as of August 2008, was just over 21 million, and of those, just under seven million households had Internet access (ABS, 2008). This is equivalent to approximately 33 percent of the national population. Unfortunately, individuals may be unaware of the threats that household computers may be susceptible to whilst using the Internet. Evidence suggests that at any given moment, approximately 90 percent of households worldwide may have some form of malware on their computer (Schmidt & Arnett, 2005, p.68).

A recent malware infection affected the International Epilepsy Foundation server which was subjected to a malware attack (Anonymous, 2006, p.2). The resultant outcome saw visitors machines infected with malware which would display fast-paced flashing images causing seizures. More recent malware infections have resulted in the target machine joining a collective botnet and used for malicious purposes, including identity theft and Distributed Denial of Service (DDoS) attacks. A new malware trend, namely 'ransomware' is encrypting documents, emails, pictures and music on the target host (Bridges, 2008). The aim of this class of malware is to extort money from the victim by offering to decrypt the contents of the victim's computer once the lump sum is paid. Malware affecting consumers is reaching all realms of the online world. Malware is increasingly targeting users of games such as World of Warcraft in an attempt to capture keystrokes during the login process, with the intent to steal in-game currency, inventory or accounts (Bridges, 2008, p.18).

Whilst each anti-virus vendor is continually promoting their product and releasing updates (signatures) on an almost daily basis, consumers are still falling victim to malware attacks. One of the threats facing consumers is the constant evolution and revolution of malware. Secure Computing (2008) reported a constant increase in malware propagation over the Internet towards the end of 2007. The analyst's team stated that "… Microsoft Windows continued to see a steady increase in exploits while decreases were seen on other platforms…" (Secure Computing, 2008). This quote emphasises that SoHo Microsoft Windows based hosts are still the predominant targets for attacks, whilst sabotage and attempted control of the infected host appears to be the main focus of each attack. This creates a dilemma because users must possess the knowledge and skills to safeguard and protect their computers from potential online threats.

The various penalties associated with malware development could include financial penalties and/or employment termination. As a result, there are various methods by which malware may go undetected by employing anti-

forensic techniques to avoid detection and analysis (Brand, 2007). Detection avoidance may be achieved by data destruction, data hiding, and data contraception. Alternatively, malware may also go through a set of analysis avoidance methods including: exploiting flaws in analysis tools, system destruction when undergoing analysis, production of false disassembly listings, and subversion of dissembler heuristics. These anti-forensic methods are discussed in detail in Brand (2007, pp.1-8). Whilst numerous vendors discuss the advantages of their product in relation to malware removal, the anti-forensic and anti-avoidance techniques present a new challenge and hence as a result, not all malware may be detected during a system scan. A concept often overlooked by performance testing of anti-virus software is examined in this paper, by attempting to determine if recently released malware is detected and successfully removed from a Microsoft Windows based computer system.

Network based malware takes advantage of vulnerabilities on computers to install malicious software directly, or can initiate its download from an external, malicious site. The malware is generally packed, and the installation process usually involves a sequence of installing multiple files in the system directory, together with the creation and modification of registry keys, resulting in the creation of new malicious processes that are initiated each time the computer is started. Packing malware provides not only a method of compressing multiple files and installation instructions into a single file but also an opportunity to avoid signature detection. Most anti-virus software will simply detect that a file is packed and warn the user that the file is suspicious. The packed malware generally consists of multiple files which are then copied to various locations in the Windows System directory with the hidden attribute set and provided with file names that very closely resemble legitimate file names to provide additional camouflage. Registry changes can include disabling anti-virus and firewall software and the Microsoft Windows update mechanism. Auto start capabilities are generally changes made to the registry to ensure that the malware is activated each time the computer is restarted. Security settings are often changed in Internet Explorer so that more malware can be downloaded from sites without warnings displayed to the user.

METHODOLOGY

The paper depicts the current state of popular anti-virus products in relation to detection statistics provided by a third party malware analysis group.

Preparation

The test system was comprised of an IBM Pentium 4, 3.0GHz standalone workstation with 1GB of RAM. The chosen host operating system was Microsoft Windows XP Professional running Virtual PC 2007 as the virtual machine environment. In turn, the virtual image consisted of Microsoft Windows XP Professional with Service Pack 3 and all recommend updates from Microsoft up to and inclusive of August 19th 2008. All network connectivity was removed, resulting in the test machine being isolated from other workstations on the network.

Anti-virus Products

The top ten anti-virus products were downloaded from the Internet according to recommendations made by third parties (CNET, 2008; Top Ten Reviews, 2008). Locating a list of top products was based on a process that a SoHo user may utilise to compare and contrast available anti-virus products. As a result the top ten products were located by using the search terms "anti-virus review" and "top 10 antivirus" in Google and are presented in Table 1 below.

Table 1 Anti-virus products tested

Anti-Virus Product	Version
Avast	4.8
AVG	8.0.169
Bitdefender	2008 build 11.0.8
Eset Nod32	3.0.672
F-Secure Anti-Virus 2008	8.00 build 103
Kaspersky	8.0.0.454
Norman	-
Norton	2008 build 10.0.0.359
Panda	2009
Trend Micro	8.910

Product Testing
Each anti-virus product was installed independently on a separate baseline virtual machine image with all updates being applied to the product up to and inclusive of August 26th 2008. Utilising Regshot (Regshot, 2008), a *snapshot* was taken of the registry, the %\Windows and %\System directory of the operating system prior to the malware executing, after the malware had been installed (to monitor changes to the system files), and after the malware had been *supposedly* removed by the anti-virus product. Each malware specimen was executed on the baseline image via two methods:

1. Whilst the anti-virus product was disabled and all subsequent monitoring agents terminated.

2. Whilst the anti-virus product was enabled and hence providing consistent system monitoring.

Results were gathered as to whether each anti-virus product was successfully able to detect the malware specimen, eliminate the malware and all associated malicious files from the system, and return the system and associated system files to their original state.

Malware Specimens
Seven malware specimens were used in the course of this research. The following results were extracted from reports generated by the online malware analysis service Anubis (International Secure Systems Lab, Vienna University of Technology, Eurecom France, & UC Santa Barbara, 2008) and from Virus Total (2008). Table 2 below lists the malware signatures of the specimens as determined by the Ikarus anti-virus software. Names assigned to malware can vary widely between products. This can also include different detection results for the same malware specimen by numerous anti-virus products.

Table 2 Virus signature of specimens assigned by Ikarus

Sample	Virus Signature (Ikarus)
A	Net-Worm.Win32.Allaple.a
B	Trojan-Downloader.Win32.Small.hib
C	Trojan-Downloader.Win32.Small.hib
D	Trojan-PWS.Win32.OnLineGames.kil
E	Backdoor.Win32.Rbot
F	Backdoor.Win32.Rbot.cgu
G	Virus.Win32.Rbot.DCY

Specimen Justification
The malware specimens selected for the research have varying detection rates amongst numerous anti-virus products. Table 3 displays the detection rates for the specimens after submission through Virus Total to thirty-six different anti-virus products. Whilst an anti-virus product may make it to the top ten by third party reviewers it may not actually detect and/or eliminate the malware from an infected host. As depicted by Virus Total, malware specimen F and G appear to have a 100 percent detection rate amongst all current anti-virus products, whilst specimen C has the lowest detection rate.

Table 3 Virus Total Anti-virus detection rates

Malware Specimen Detection Rates						
A	B	C	D	E	F	G
94.40%	86.11%	69.44%	97.22%	94.40%	100%	100%

The malware chosen for testing encompasses varying degrees of sophistication and anti-avoidance techniques which any reputable anti-virus product should be capable of removing. Table 4 displays the varying, high level, functionality of the malware specimens which could include creation of files in the system directory, changing security settings in Internet Explorer, download of executable code, configure auto-start capabilities and joining of an IRC network.

Table 4 Sophistication of malware specimens

	Malware Specimen						
	A	B	C	D	E	F	G
Creates files in the Windows system directory	Yes	Yes		Yes	Yes	Yes	Yes
Changes security settings in Internet Explorer		Yes	Yes	Yes	Yes	Yes	Yes
Downloads executable code		Yes					
Autostart capabilities		Yes		Yes	Yes	Yes	Yes
Joins an IRC network		Yes			Yes	Yes	Yes

The number of malicious files and registry entries created is dependent upon the intention of malware. Table 5 below depicts the number of changes made by the malware specimens used in this research to the registry and to the file system as well as the number of services changed and processes created. A significant number of changes are made by each malware specimen. A malware removal process could be expected to remove the malicious programs, associated files and registry entries by detecting the presence of the malware through some combination of heuristics and signature matching. However, this technique is dependent upon an analyst having first analysed the malicious software to extract its signature and determination of the changes to the file system and the registry the malware makes.

Table 5 Malware characteristics

		Malware Specimen						
		A	B	C	D	E	F	G
Registry Keys	Created	5	0	2	0	8	4	2
	Modified	10	21	0	10	41	53	11
	Deleted	0	0	0	0	0	1	0
Files	Created	2	7	4	2	0	1	4
	Modified	12	13	24	8	3	5	11
	Deleted	0	2	2	2	1	1	1
Services Changed		1	0	0	0	0	0	0
Processes Created		1	0	1	1	0	1	3

Testing
The experimentation was aimed at mimicking the process that a SoHo user would use when installing and using an anti-virus product. As a result, the default settings were used for each and every product as recommended by the vendor during the install process. During the detection and elimination of malware stage, the steps taken by the vendor were also used to remove the malware from the system. If a system scan needed to be conducted, the depth of the scan was dependent on the recommend scan type outlined by the vendor. Whilst a "recommended" scan may not detect or eliminate malware as would a "deep scan", it is the purpose of this paper to mimic the actions taken by a SoHo user in dealing with a malware infected computer system.

RESULTS

In order to protect the vendor of each anti-virus product, names of the product are not used when describing the quality of a particular anti-virus product. Rather, each product is referred to as Product 1 through to Product 10 and does not relate to the order of the products presented in Table 1.

Table 6 depicts the malware specimens presented in Table 2 and whether or not they were detected by the anti-virus product. In this instance, the anti-virus product had been disabled and any monitoring capabilities of the product were terminated also, hence preventing the malware from being detected on install. The malware had been executed and the anti-virus product had been resumed. Product 6 and 7 were able to detect the malware immediately upon activation with a warning box appearing, notifying the user that a virus had been detected. The research suggests that although the products tested have made it to the top ten list, they are still not capable of detecting malware (specimen C) which has been propagating throughout the Internet for a long period of time.

Table 6 Malware Specimens Detected

Product	Malware Specimen						
	A	B	C	D	E	F	G
1	✔	✔	✘	✔	✔	✔	✔
2	✔	✔	✘	✔	✔	✔	✔
3	✘	✔	✔	✔	✔	✔	✔
4	✔	✔	✔	✘	✔	✔	✔
5	✔	✘	✘	✔	✔	✔	✔
6	✔	✔	✔	✔	✔	✔	✔
7	✔	✔	✔	✔	✔	✔	✔
8	✔	✘	✘	✔	✔	✔	✔
9	✔	✔	✔	✘	✘	✔	✔
10	✘	✔	✔	✔	✘	✔	✔

Each anti-virus product provides constant system monitoring to potentially prevent malware from installing itself, whilst the anti-virus product is active. Whilst numerous vendors promote their product with the added feature of "real time monitoring", the research suggests that these monitoring capabilities are far from effective. As presented in Table 7 the detection capabilities of the malware have improved in contrast to the previous detection rate. However, the top 10 anti-virus products have clearly not detected malware which has been available for a long period of time. In most instances when the malware was transferred from a CD to the virtual machine image, most anti-virus products immediately detected the binary instantly and confirmed whether it should be quarantined or deleted. From the products which detected the malware, there was no method by which to make an exception and hence allow the malware specimen to be installed, hence providing good reaction and detection capabilities.

Table 7 Malware specimens detected during install

Product	Malware Specimen						
	A	B	C	D	E	F	G
1	✔	✔	✘	✔	✔	✔	✔
2	✔	✔	✔	✔	✔	✔	✔
3	✘	✔	✔	✔	✔	✔	✔
4	✔	✔	✔	✔	✔	✔	✔
5	✔	✘	✘	✔	✔	✔	✔
6	✔	✔	✔	✔	✔	✔	✔
7	✔	✔	✔	✔	✔	✔	✔
8	✔	✔	✘	✔	✔	✔	✔
9	✔	✔	✔	✘	✔	✔	✔
10	✘	✔	✔	✔	✘	✔	✔

Table 8 depicts whether the malware had been completely removed from the computer system utilising the didactic instructions provided by the vendor. The blank spaces depict those products which could not detect the malware and hence were not able to remove it either. It was discovered that whilst a product may detect and potentially eliminate a piece of malware from a computer system – that there are always remnants which remain on the system after the malware has been eliminated.

Table 8 Malware elimination

Product	Malware Specimen						
	A	B	C	D	E	F	G
1	✗	✔		✗	✔	✔	✔
2	✗	✔		✔	✔	✔	✔
3		✔	✔	✔	✔	✔	✔
4	✔	✔	✔		✔	✔	✔
5	✗			✔	✔	✔	✔
6	✔	✔	✔	✔	✔	✔	✔
7	✔	✔	✗	✔	✔	✔	✔
8	✔			✔	✔	✔	✔
9	✔	✔	✔			✔	✔
10		✔	✗	✔		✔	✔

As is demonstrated by Table 8, those products which were able to detect the malware were not necessarily able to eliminate the malware from the host. It was soon discovered that malware specimen C was significantly problematic for most anti-virus products. Whilst the product claimed to have removed the product, and in some instances needed the host to be restarted – following this didactic process discovered that the malware would re-appear as soon as the system was restarted.

CONCLUSION

The research in progress effectively examined the state of the top ten claimed anti-virus products available to consumers. From the research conducted, the most effective anti-virus product included Kaspersky Anti-Virus and BitDefender Anti-Virus. This strongly conforms to the results and reviews provided by the third party websites which detailed their most highly recommend anti-virus product. Whilst numerous factors may be important when choosing an anti-virus product including ease of update, support and the user interface – it is however the opinion of the authors that the effectiveness of a product in detecting and removing the malware is the most prevailing factor.

From a SoHo perspective, the research suggests that naïve or uneducated users will continue to fall victim to the numerous, predominant threats found on the Internet. Whilst many products do provide instructions by which the user should follow to eliminate the malware, it appears that in many instances that these instructions are not clear. This research re-iterates the issue of how difficult it is for a SoHo user to protect themselves when not only are the product instructions unclear in the steps needed to remove malware, but furthermore when the product itself is not able to remove the malicious content in the first place.

REFERENCES

ABS. (2008). 8153.0 - Internet Activity. Retrieved August 1, 2008, from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

Anonymous. (2006). Attackers target epilepsy site. Network Security, 2006(4), 2.

Brand, M. (2007). Forensic Analysis Avoidance Techniques of Malware. Paper presented at the 5th Australian Digital Forensics Conference, Edith Cowan University, Mount Lawley Campus, Western Australia.

Bridges, L. (2008). The changing face of malware. Network Security, 2008(1), 17-20.

CNET. (2008). Antivirus - Reviews. Retrieved August 20, 2008, from http://www.cnet.com.au/tag/reviews/antivirus.htm

International Secure Systems Lab, Vienna University of Technology, Eurecom France, & UC Santa Barbara,

U.S. (2008). Anubis: Analyzing Unknown Binaries.   Retrieved October 4, 2008, from http://anubis.iseclab.org/

Regshot. (2008). Regshot.   Retrieved August 25, 2008, from http://sourceforge.net/projects/regshot

Schmidt, M. B., & Arnett, K. P. (2005). SPYWARE: A Little Knowledge is a Wonderful Thing. Communications of the ACM, 48(8), 67-70.

Secure Computing. (2008). Secure Computing's Trends in Email, Web, and Malware Threats Retrieved August 3, 2008, from http://www.securecomputing.com/index.cfm?skey=1739

Top Ten Reviews. (2008). AntiVirus Software Review 2008.   Retrieved August 20, 2008, from http://anti-virus-software-review.toptenreviews.com/

Virus Total. (2008). Virus Total.   Retrieved October 4, 2008, from http://www.virustotal.com/en/virustotalf.html

COPYRIGHT