

The State of Malware

Daniel B. Owen

Middle Tennessee State University

Abstract

Malware, broadly defined as any type of malicious and probably secret software, has been an issue in the personal computer (PC) industry since at least the mid 1980s. This paper outlines the current state of malware with an emphasis on non-viral malware such as spyware, adware, worms, Trojan horses, keystroke loggers, dialers, and browser hijackers. Viruses are mentioned only as a comparison point where appropriate. This paper reviews the types and behaviors of malware, infection methods and mitigation techniques. It also outlines a methodology for further research to discover practices in common use among corporations.

Malware is broadly defined as any type of malicious and probably secret software (Weiss, 2005). Malware has been an issue in the personal computer (PC) industry since at least the mid 1980s (Schmidt & Arnett, 2005). In 1986, two brothers released the Brain virus into the wild. This was the first publicly distributed virus for the PC (Schmidt & Arnett, 2005). Most early viruses were boot sector infectors and spread over a matter of weeks as floppy disks were shared between computer users (Keller, Powell, Horstmann, Predmore & Crawford, 2005). Malware has evolved from the early viruses most of which seem minor by modern standards to numerous threats that range from information disclosure to complete takeover of the affected system (Henry, 2005; Shukla & Nah, 2005; Stafford & Urbaczewski, 2004; Thompson, 2005; Weiss, 2005; YOUNGHWANG & KOZAR, 2005).

This paper will outline the current state of malware with an emphasis on types of malware that have superseded or built upon the viruses of the 1980s and 1990s. Virus infection is a major current malware issue but will be ignored in this paper since, unlike other forms of malware, viruses have been extensively covered in previous studies. Where appropriate, viruses will be mentioned as a comparison point.

This paper will start with a look at the types and behaviors of malware found in the modern enterprise. Next, the problems associated with malware will be discussed. The methods of malware infection will be reviewed. Then, mitigation techniques will be reviewed. Consumer studies have been undertaken but mitigation techniques in the enterprise have been less fully examined. The final portion of the paper will be a proposed research methodology outlining an investigation of techniques currently being employed by security professionals in the enterprise environment.

Types of Malware

There is a wide variety of software that fall under the heading of malware and unfortunately, experts often disagree about whether a given type of software should be classified as malware. For this reason, this paper will start with a definition of the types of malware that will be discussed. In order to concentrate on types of malware that are almost universally accepted as malicious, some common software types that are often identified as malware will be defined but will not be discussed.

Web Cookies

Web cookies are files that are placed on a user's computer when visiting a web site. Web cookies were originally intended as a way to allow web sites to hold information about a user as he or she traverses the site. Examples would include merchandise in a shopping cart or a website password. Cookies are used by many web sites for these and similarly benign purposes. Cookies can also be used for tracking the use of a web site, without the user's knowledge (Sipior, Ward, Roselli, 2005). While web cookies are of concern to many people, this paper will not concentrate on tracking cookies due to the large proportion of legitimate cookies used and lack of consensus in drawing a line between legitimate and abusive uses of cookies.

Computer Viruses

This paper will not directly discuss computer viruses in depth, but it is important to establish a precise definition of a virus before discussing other forms of malware. Some forms of malware discussed in this paper may be broadly defined as viruses by anti-virus vendors. A computer virus is a piece of code that is designed to replicate by attaching itself to a host program. The behavior of attaching itself to another file is key to

the distinction of a virus from other malware. A virus also requires some type of user interaction such as running an infected program or opening an infected file. Once a virus is executed it will attempt to spread to other files. Viruses do not rely on system vulnerabilities to spread but instead rely on functionality that is commonly used by other non-malicious software (Ford, 1998).

Worms

Worms are often confused with viruses since they self replicate like viruses. There are a number of distinctions that separate worms from viruses and other malware. Worms are stand-alone applications that do not attach to or infect another file. Worms typically do not rely on a user executing a program instead they rely on vulnerabilities in software to allow them to spread. Worms typically spread across networks without user intervention (Ford, 1998). Successful worms can propagate extremely rapidly. It is estimated that once 10,000 systems have been infected a worm can be said to have reached critical mass. Once critical mass is reached infection rates will increase exponentially, but infection of the first 10,000 hosts can take a long time (Henry, 2005). On the other hand, the Slammer Worm infected ninety-percent of vulnerable systems within ten minutes of its release (Keller et al. 2005).

Trojan Horse Software

Trojan horse software operates differently than advertised. Typically, a Trojan will be advertised as a useful tool such as a browser plug-in but carry additional unwanted malicious code with it. The malicious code may damage the system or open a back door that an attacker can use later to attack the system. Trojan horse applications do

not self replicate (Ford, 1998; Henry, 2005; Keller et al. 2005; Sipior et al., 2005; Weiss, 2005; Younghwa & Kozar, 2005).

A sub form of Trojan horse is known as a Remote Administration Trojan (RAT). A RAT has the same characteristics of other Trojan horse programs but specifically allows control of the system by an outsider. RATs are often installed by exploiting security vulnerabilities in the operating system or web browser when visiting infected web sites (Sipior et al., 2005; Thompson, 2005).

Keystroke loggers

A keystroke logger is a type of software that is designed to record and report keystrokes back to someone other than the computer's user. This type of malware may overlap with any of the previously mentioned types of malware. Keystroke loggers may steal data such as passwords, financial data or any other data entered at the keyboard (Henry, 2005; Sipior et al., 2005; Shukla & Nah, 2005; Stafford & Urbaczewski, 2004; Thompson, 2005; Weiss, 2005; Younghwa & Kozar, 2005). Keystroke loggers are sometimes referred to euphemistically as system monitoring tools (Sipior et al., 2005).

Browser Hijackers

Browser hijackers change a browser's settings. This is often an attempt to increase the number of hits to the publisher's web site or to re-route browser requests through the hijacker's proxy server. Browser hijackers can also be used to gather information about the user without their consent. Finally, browser hijackers may change the user's search functionality within their browser (Shukla & Nah, 2005; Weiss, 2005; Younghwa & Kozar, 2005).

Dialer

A dialer is a piece of software that tries to cause the modem to call expensive toll services such as 900 numbers, international calls, or expensive 10-10-xxx access codes. The author of the dialer gets a portion of the call's proceeds (Stafford & Urbaczewski, 2004; Weiss, 2005). Dialers are often associated with pornographic web sites (Younghwa & Kozar, 2005). As a general rule, enterprises do not have modems in their computers so the billing issues associated with dialer software may not be an a problem but any malware is a concern even if it is not completely successful in its aims.

Spyware

A number of different types of software are commonly referred to as spyware including all of the previously mentioned types of malware with the exception of viruses and worms and some viruses and worms have spyware functionality. This paper will define spyware relatively broadly but use other more exact terms when a more definitive term is appropriate.

Spyware is broadly defined as any software that collects, subverts and reports information about a user without the user's knowledge or informed consent (Awad & Fitzgerald, 2005; English, 2006; Keller et al. 2005; Klang, 2004; Sipior et al., 2005; Stafford & Urbaczewski, 2004; Weiss, 2005; Zhang, 2005). This broad definition of spyware creates a base for describing spyware. Further additions of common characteristics of spyware will narrow the focus of the working definition used in this paper.

Spyware will often employ deceitful tactics in order to hide its installation or existence. Some spyware can be installed by simply visiting a web site that will silently

install software on the visitor's computer (Keller et al. 2005). Another tactic used by some spyware authors is the inclusion of a lengthy and confusing end user license agreement (EULA) that states that spyware will be installed. Some spyware will have a EULA that is 50 or more screens long (English, 2006). Freeware is a common source of spyware (Zhang, 2005) but there is nothing to preclude commercial software from having spyware provisions hidden in the EULA.

A new and disturbing twist on the spyware theme is polymorphic spyware. Polymorphic spyware changes file names, file contents and installation locations each time it is installed. This makes conventional file based anti-spyware software obsolete (English, 2006). This is a technique that was perfected years ago by virus writers (Nachenberg, 1997) so the crossing of ideas between malware authors becomes more obvious.

Adware

Adware is often associated with spyware because both types of software have similarities in function and purpose but they are not the same thing. At its simplest, adware is software that is advertiser supported. The problem with adware is that some cross a line and transform from being advertiser sponsored software to spyware.

What makes malicious adware unique from other forms of malware is that it is advertiser driven. Adware may monitor a user's web browsing habits and report them to a central database or force advertising on the user based on the browsing habits. Some adware may change the way that the browser works or may change default browser settings. Specifically adware may change the user's home page or search settings (Shukla

& Nah, 2005; Stafford & Urbaczewski, 2004). Some adware will initiate popup advertising on the infected computer (Shukla & Nah, 2005; Younghwa & Kozar, 2005).

A common form of adware that can be malicious or benign is the browser plug-in. Plug-ins are software that extend or change the functionality of a web browser. Most adware plug-ins consist of a search toolbar (Shukla & Nah, 2005).

Drive-by Download

A piece of malware that uses drive-by downloading as an infection method will be installed when a user visits a web site (Awad & Fitzgerald, 2005; Shukla & Nah, 2005; Stafford & Urbaczewski, 2004). Any type of malware can take advantage of drive-by installations. All that is required is a way of getting people to come to an infected web site or infecting an already popular site. Third party advertising is a common method used to get drive-by installation code displayed by otherwise legitimate web sites (Shukla & Nah, 2005). Drive by downloads typically take advantage of use of ActiveX commands, browser security issues and parasitic programs (Awad & Fitzgerald, 2005). By definition drive-by downloads are installed without the user's informed consent (Awad & Fitzgerald, 2005; Shukla & Nah, 2005).

Bundleware

Bundleware is simply software bundled with other legitimate software. Bundleware is a common source of both spyware and adware (Shukla & Nah, 2005). Bundleware will often disclose the inclusion of malware in the EULA, but this is not a guarantee. In some cases, bundled software may be installed without any agreement from the end user or warning about what will be installed. Even if the EULA discloses the bundled software, it may do so in a confusing or overly broad manner (English, 2006;

Weiss, 2005). Some software authors see bundleware as a method of receiving payment for their programs (Klang, 2004)

Blended Threats

A blended threat is malware that uses multiple attack vectors to install itself (Gordon, 2005; Keller et al. 2005). Unlike some other forms of attack, blended threats do not require any interaction on the part of the end user. Blended threats specifically look for security weaknesses as a way of spreading. While many forms of malware rely on an end-user running or installing malicious software a blended threat will take attack code for known software vulnerabilities and include it in an automated malware attack. Blending of attack methods makes this type of malware a very efficient spreader. Code Red and Nimda were extremely efficient examples of blended threat malware. In the first half of 2003 over sixty percent of malware submissions were blended threats (Keller et al. 2005).

Rootkit

A rootkit is possibly the most dangerous type of malware currently affecting computer users. A rootkit spreads bits of itself throughout a system giving the “owner” of the rootkit complete access to the system and then hides (Conry-Murray, 2006; Fontana, 2006). Rootkit techniques can also be used as part of the hiding technique used by other types of malware. Some rootkits are even written for hire by professional malware authors to assure that standard signature based malware detection programs do not detect the software (Fontana, 2006). Many experts suggest that the only way to be sure that a rootkit has been removed is to completely wipe the hard drive of the system and reinstall all software from scratch (Fontana, 2006; Hayes, 2006).

The Problem with Malware

The preceding outline of the types of malware will begin to explain why malware is a problem. In this section, additional problems associated with malware will be considered.

Most people discover that they have a malware issue when their system becomes unstable or slow to respond. Microsoft estimates that half of all crashes are caused by spyware (Sipior et al., 2005). At approximately 20% of all support calls, malware infection is the most common reason for calls to Dell's technical support lines (Sipior et al., 2005).

Testing undertaken by Computer Associates showed that malware can have devastating effects on productivity. They found that the addition of a single specific piece of adware increased PC boot time by 3.5 minutes. They also found that the infected machine took almost five times as long to load a web page. (Thompson, 2005) Taken over the number of computer users in a corporation malware has the potential to cause a substantial loss of productivity.

Of particular annoyance to many users is the fact that malware is often difficult or impossible to remove once installed. As mentioned earlier in the case of a rootkit many experts do not recommend even attempting to clean the infection but starting over with a freshly formatted hard drive. For less resilient forms of malware such as generic spyware many times the uninstall process will actually leave certain portions of the system non functional (Stafford & Urbaczewski, 2004). Some companies may include an uninstaller that does not work while others simply do not provide an uninstall option (Shukla & Nah,

2005). Also of concern is that uninstalling the program that brought the spyware onto the system may not remove the spyware (Klang, 2004).

From a corporate standpoint, there is an at least equally troubling issue of liability. For some time, experts have predicted that there will be numerous lawsuits filed against compromised companies used as a staging ground for further attacks (Hancock, 2004). Large numbers of lawsuits have not yet materialized but the risk remains. Similarly, in an effort to mitigate cyber liability risks some companies have added language to their use policy that states that they are not responsible for the loss of personal information if they are hacked regardless of the security of the hacked system (Swartz, 2004). Both liability to customers and unknown third parties must be considered when developing a malware policy.

A number of malware products have been linked to the creation of botnets. A botnet is group of computers referred to as bots or zombies that have been compromised by a third party to gain control over the systems (Henry, 2005). These systems are commonly controlled semi-anonymously via Internet Relay Chat (IRC). It is estimated that more than a million bots are in existence on the Internet (Passmore, 2006). According to Trend Micro's David Perry, single botnets of 60,000 infected machines currently exist (Messmer, 2005a). This gives the "owner" of the botnet a substantial amount of available computing power.

Computers in botnets are often used as part of spam relay networks (Henry, 2005; Stafford & Urbaczewski, 2004; Thompson, 2005). Spam networks can be used as a way of generating income by directly spamming or, more commonly, by renting or selling the

botnet to a spammer. Another use for a spam oriented botnet is the spread of the same or a different piece of malware (Messmer, 2005b).

More disturbing, some botnets are used for Distributed Denial of Service (DDOS) attacks (Henry, 2005; Stafford & Urbaczewski, 2004; Thompson, 2005). DDOS attacks are attacks that flood a target with connections from a large number of different computers under the control of the attacker (Thompson, 2005). Botnets are the common source of the computers used in DDOS attacks. DDOS attacks are extremely difficult to defend against due to the distributed nature of the attack. Blocking DDOS attacks can cause disruptions for large numbers of unrelated visitors without necessarily mitigating the attack (Passmore, 2006). Even very large companies are often incapable of defending against a DDOS attack. For example, Amazon, Microsoft, Yahoo!, CNN and eBay have all been victims of DDOS attacks (Passmore, 2006). While it has not yet been attempted in a court of law, there is still a potential for a victim of a DDOS attack to sue an intermediary company for not taking due diligence to protect their systems (Hancock, 2004).

A major concern for all corporations is the potential loss of proprietary information due to spyware. This is especially true for companies that must comply with regulations relating to data protection such as the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act (SOX) (Hu & Dinev, 2005; Sipior et al., 2005). A breach may lead to legal sanctions if the malware victim is found not to have taken proper measures to protect their systems.

In the cases of malware such as key loggers, RATs and rootkits escalation to other forms of intrusion is a worry. As has been mentioned keystroke loggers can capture

username and password combinations as well as other types of sensitive data. This information may be used as a starting point to a further breach (Stafford & Urbaczewski, 2004).

Rootkits and RATs can actually take this a step further and open a back channel that allows the person controlling the malware to take complete control of the infected system. This gives the attacker as much access to the protected system and attached resources as the user who is logged into the system.

Identity theft is a concern since keystroke loggers will record all information entered at the keyboard. The person who wrote or distributed the keystroke logger may directly take part in identity theft or they may sell the information to a third party who will actually use it (Stafford & Urbaczewski, 2004).

In an information economy the information created or owned by the corporation is often the corporation's most important asset. In a survey undertaken by the Computer Security Institute (CSI) in 2004, 83.3% of companies placed a high value on their digital business data (Keller et al. 2005). Many forms of spyware have the potential to destroy or leak this information. In the same survey, CSI found the total security related cost for mid-to-large companies in 2004 was \$141,496,560. Nearly 40% of those costs were virus related (Keller et al. 2005).

Prevalence of Malware

Malware of all types is a major problem for both corporations and individual users. Dell estimates that 90% of Windows PCs have at least one piece of spyware loaded (Weiss, 2005). A joint AOL and Nation Cyber Security Alliance (NCSA) study found that 80% of the computers they scanned contained some form of spyware or adware

(Gordon, 2005). In a study undertaken by Symantec, they found that 359 pieces of adware were left after surfing popular kid focused web sites (Gordon, 2005). A February 2005 study by Symantec found seventeen pieces of adware and two pieces of spyware after surfing six sports oriented web sites (Gordon, 2005). Additionally large numbers of adware and spyware were found in studies looking at travel and gaming sites (Gordon, 2005). Gartner estimates that 20 million people have installed some form of adware (Gordon, 2005; Sipior et al., 2005). There are over 78,000 different applications designed to monitor and report user activity to a third part (Stafford & Urbaczewski, 2004).

Few studies have been conducted to assess the prevalence of spyware and adware on systems but as the reader can see spyware and adware are both very prevalent in the modern computing environment. The next questions that must be addressed are “How does malware get installed?” and How can it be avoided?”

How Malware Gets Installed

Different forms of malware have different infection vectors. Computer virus and worm infection vectors were discussed earlier in this paper so they will not be discussed here. Due to their relative newness and the fact that they have been studied less thoroughly, infection vectors of spyware, adware and their associated sub types are of particular interest.

One of the most difficult types of spyware installation to avoid is drive-by-installation. As mentioned earlier this is a problem across a wide variety of web site types. Even “trusted” web sites have been found to contain adware or spyware (Shukla & Nah, 2005) so simply avoiding “questionable” sites is not enough to completely mitigate this infection source.

End-users often inadvertently install malware. One major source of both adware and spyware is the user's desire for "free" media that can be acquired using peer-to-peer networks. Some research has even indicated that some people are willing to accept spyware as the cost of the "free" media available from peer-to-peer networks (Weiss, 2005).

Bundleware included with freeware or shareware is another area in which spyware and adware often come in under the guise of something free (Gordon, 2005; Klang, 2004). Freeware and shareware authors will sometimes bundle their software with additional software as a revenue stream (Sipior et al., 2005) and some software is simply written with the sole intent of being the carrier for spyware or adware. Research shows that only 6.4% of end-users say they read EULAs carefully while another 4% read "most" of the agreement (Zhang, 2005) even though it is crucial that end users read EULAs before installing software. Spyware and adware installed along with other software will often be disclosed in the EULA. Although unusual, there may even be an option of installation without the spyware being included in the package (Sipior et al., 2005).

Research has found that some computer systems actually come from the manufacturer with spyware installed (Stafford & Urbaczewski, 2004). In this case, avoiding spyware may be impossible and recovery is the appropriate solution. Not purchasing from companies that load objectionable software is also an option.

Mitigation Techniques

There are a number of malware mitigation techniques in use today. There is not a single product that can be loaded on systems that will make the system malware proof.

There are a number of reasons for this. First, malware is a rather broad topic so no single product is designed to try to eliminate all malware risks. Secondly, the security community has not reached an agreement on what to include in the definition of malware. An example of this is the web cookie. Finally, different products will detect a varied group of malware within their own market segment. This is especially true in the area of spyware and adware which do not have readily agreed upon definitions. For these reasons malware mitigation requires a combination of products and security techniques. Current malware mitigation techniques used in the corporate environment will be discussed in this section.

Up to this point, this paper has intentionally ignored viruses and anti-virus software where possible. Due to the fact that anti-virus software is mature and the theoretical basis for many newer types of anti-malware software, anti-virus software will be discussed in some depth to give a background for other techniques that have followed. Some anti-virus software vendors have added additional functionality to their anti-virus products to mitigate risks posed by non-virus malware.

Most people are familiar with anti-virus applications. One recent survey found that 100% of respondents used an anti-virus scanner and some respondents were even using multiple scanners for additional protection (Keller et al. 2005). This seems to indicate that both home and corporate users are familiar with the need to run anti-virus software to protect their machines.

A signature based anti-virus package can only detect viruses it knows about and historically there has been a problem in training users to update their anti-virus signatures. This continues to be a problem that shows no sign of an immediate solution.

In the corporate world this normally falls on the often already over worked IT staff. Many anti-virus companies have seen this opportunity and created software that will automatically update signatures on a schedule (Keller et al. 2005).

This still results in an inherently reactive anti-virus system. Systems protected by signature based anti-virus software are at risk of being infected by a new virus until the virus has been identified and anti-virus vendors have created and distributed signature files. In the W32.Sober.I outbreak, some anti-virus vendors took as long as 12 hours to create signature files. Once a signature is available, it will take some time for all users of an anti-virus product to update their signature files. Experts state that there is only a two-hour window from the time that a virus is spotted until it reaches critical mass (Henry, 2005). This timing difference is an obvious problem for signature based anti-virus systems.

The use of heuristic or behavior monitoring software is one method of identifying potential viruses before a signature is available. An anti-virus product that uses heuristic scanning will allow code to run in a controlled environment and watch what the software is trying to do. Heuristic software is an improvement for unknown malware detection, but heuristic anti-virus software is only about 90% effective and has a higher false-positive rate than signature based anti-virus software (Henry, 2005).

As with any security initiative, defense in depth is imperative. Some techniques that are not specifically considered anti-malware will, if properly implemented, help to reduce the malware risk. A firewall with a well designed restrictive rule set will help to mitigate some risk by simply disallowing access to vulnerable systems (Henry, 2005). Proper egress filtering at the firewall can also help to keep already infected internal

systems from making a connection to a botnet or from making other potentially undesirable connections (Messmer, 2005b).

A proper patching procedure will help reduce the risk of receiving malware (Stafford & Urbaczewski, 2004). In the cases of both the Blaster and SoBig worms patches that would have prevented infection had been available for at least a month before the attacks. In both cases, millions of infections were allowed by the negligence or ignorance of end users who did not keep their systems updated to a current patch level (Berghel & Hoelzer, 2005).

Both ingress filtering at the firewall and patching are especially useful for worm mitigation due to the automated way that worms spread across networks. Egress filtering of traffic at the firewall may not stop a computer from becoming infected but it will limit the damage once a machine has become infected.

Corporate policy backed by technological force where necessary can also be useful in the fight against malware. End-users should not be allowed to download and install software without a review process from the information technology (IT) department (Gordon, 2005). This will greatly reduce the chances of malware piggybacking on another product being introduced into the protected network. The challenge is that employees may try to find ways around the policy if the IT department is not responsive to requests. To make this policy work the IT department must be able and willing to review software requests in a timely manner. If it is not practical to have all software reviewed by the IT department then end-users must be trained to review EULAs (Sipior et al., 2005).

The use of peer-to-peer networks should be restricted or banned in order to reduce the chance of malware coming into a protected network (Sipior et al., 2005). Peer-to-peer client software is notorious for containing spyware (Kucera, Plaisent, Bernard and Maguiraga, 2005). Peer-to-peer networks introduce a number of vulnerabilities with limited corporate advantage. While these may be acceptable risks for the home environment, most companies will find more risk than reward.

Intrusion Detection Systems (IDS) can be extremely effective in identifying systems that have been infected by malware. IDSes watch network traffic as it passes on the wire and alerts when it identifies something “suspicious.” This can include infected systems phoning home, protected computers attacking other systems or other malware related traffic (Keller et al. 2005). A large portion of fixing malware problems is knowing that there is a problem before it reaches critical mass. An IDS can alert system administrators of the need to investigate a machine before the malware has time to do more damage within the system or the network.

Anti-spyware and anti-adware applications are also available. In many ways, these applications have followed an evolution similar to that of anti-virus applications. These applications are still relatively new and many experts claim that no single application currently on the market is capable of detecting all forms of spyware. Therefore, it is recommended that multiple anti-spyware tools be employed (Arnett & Schmidt, 2005; Sipior et al., 2005; Younghwa & Kozar, 2005; Zhang, 2005).

One issue faced by anti-spyware vendors is that some spyware and adware vendors exist in a gray area. Some spyware or adware vendors’ softwares are questionable from an ethical standpoint and unwanted by the end user but legal. Due to

this issue, some anti-spyware vendors are reluctant to list spyware from quasi-legitimate vendors for fear of being sued (Gibson, 2005; Sipior et al., 2005).

It is estimated that 80% of spyware can be detected by current anti-spyware software (Younghwa & Kozar, 2005). Research shows that between 10% and 40% of Internet users currently use anti-spyware software (Poston, Stafford, Hennington, 2005; Younghwa & Kozar, 2005). This still leaves a large number of systems open for attack. Considering that some spyware cannot be detected by current anti-spyware software taking other mitigation steps in conjunction with the use of anti-spyware software is crucial.

As has been mentioned, different products leave holes at different levels. For this reason a defense in depth at the machine and network level is critical. Given this, many companies will use multiple anti-virus applications. A good solution for anti-virus scanning is to have a scanner at the gateway, a scanner at the e-mail server and a third scanner on the desktop to detect viruses that do not come in via the network. Further, each of these scanners should come from a different vendor so that if one vendor misses a threat hopefully another vendor's product will catch that threat (Henry, 2005). A company will not necessarily follow this exact same equation for other malware mitigation but a similar approach of detection at multiple levels using different products where possible is advisable.

Proposal for Further Research

There is a need for further research to look at what techniques are being used in the corporate world. Once this initial research is completed it will be possible to devise

empirical research that can test which techniques increase overall malware resistance and which do not significantly help or may even make the problem worse.

This question will be evaluated by administering a survey to security professionals who work in a cross section of businesses. The survey will concentrate on the techniques used by companies in the United States. This may limit the utility of the research for those outside of the United States, but there is a concern that implementations will be significantly different across borders and in the interests of a limited scope only respondents working in the United States will be accepted.

For this study, a security professional will be defined as anyone who is responsible for at least a portion of the security within his or her organization. The survey will be limited to security professionals due to the fact that non-security professionals may not have the detailed information necessary to answer the survey accurately and completely. Given the broad definition of security professional used for the survey any respondent who handles malware prevention will be defined as a security professional. Some respondents may not have computer security as a primary description of their job responsibilities but will be defined as a security professional for this study.

The survey will be tested using undergraduate and graduate Computer Information Systems students. The results of this survey will be tabulated and reviewed to assure the clarity and usefulness of the survey instrument. The results of this initial survey will not be used beyond the survey instrument testing phase.

The group that will be used for this survey will be members of the Global Information Assurance Certification (GIAC) alumni e-mail mailing list. According to Stephen Northcutt, President of the SANS Institute, the GIAC alumni list currently has

approximately 500 subscribers. Mr. Northcutt has agreed to allow the used of the GIAC alumni list for a survey invitation (S. Northcutt, personal communication, June 29, 2006). GIAC alumni mailing list members are security professionals that have successfully completed, with honors, one or more of the certification exams administered by GIAC in association with SANS. The SANS Institute and GIAC are both highly respected organizations in the security field and GIAC certifications are considered premier technically oriented security certifications. This is a somewhat self-selected group of professionals due to the fact that the combined SANS Institute training and GIAC certification is costly. Furthermore GIAC certifications have a reputation for being difficult thus reducing the pool of potential respondents. That being said, the limited membership of the GIAC alumni mailing list will assure that only security professionals receive the request to complete the survey.

The call for participants will be e-mailed to the GIAC alumni mailing list requesting potential participants follow a link to a web-based form. This method of requesting participants does introduce some self-selection error into the study but it is believed that this will not be a significant impediment to the research. All participants that complete the survey will be offered a copy of the aggregate results so that they can compare their policies to other participants.

Due to the general reluctance in releasing information concerning security initiatives (Kotulic & Clark, 2004), as little personally identifiable information as possible will be requested of the participants. There is no justification for keeping personally identifiable data that correlates the surveys back to the recipient therefore correlation data will be deleted after all surveys are received and a list of participants

requesting results is created. These safeguards will be explained in the initial message to the GIAC alumni mailing list as part of an attempt to assure members of the safety of completing this survey.

The survey will be broken into several sections. Each section will be presented on an individual web page with multiple questions on each page. The first section will consist of eight questions related to the types of perimeter traffic filtering implemented. Firewall rules are often overlooked when discussing malware prevention but, as this paper has demonstrated, a good perimeter defense is a first step in stopping malware from entering the protected network or mitigating the damage that is done after an infection. The second section looks at a similar question by asking about personal firewall in installations on systems. Systems are broken into nine different groups to differentiate according to purpose as well as operating system. It is believed that there will be a difference in treatment according to perceived vulnerability of different types of systems. The third section of the survey continues to look at underlying security precautions that have an effect on overall malware mitigation efforts. In this section two questions are asked to determine how systems are patched on an ongoing basis. This section is broken down into multiple groups to differentiate along operating system and system purpose lines.

The fourth section asked five broad groups of questions about anti-virus software. The first three questions concentrate on where anti-virus software is installed and whether security in depth is implemented. Question four looks at signature update techniques. Question five investigates whether heuristic scanning is being used and if so how aggressively. The fifth large subsection of questions asks three questions about anti-

spyware software. These are the same as the first three questions asked in relation to anti-virus software.

Section six looks at Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as they specifically relate to malware prevention and mitigation. This is another area that is often overlooked when considering malware mitigation but, as outlined earlier in this paper, can add a substantial level of security. First respondents are asked if they use these technologies and then are asked if they use them to detect or stop five specific malware threats. Section seven asks three questions about spam mitigation. Since spam can be an infection vector it is important to analyze spam mitigation techniques in relation to malware.

Many security experts stress the importance of strong human resource policies as a way of reducing a number of security exposures. Malware exposure can be reduced if proper policies are in place and enforced. In section eight of the survey seven questions are asked to evaluate what policies are in place to assist in malware prevention. Malware can be difficult or impossible to remove from an infected system the final section looks at malware removal techniques to determine what techniques are working for professionals in the field.

A text representation of the proposed survey instrument is included in the Appendix.

Conclusion

As has been demonstrated, malware is a menace that must be mitigated in order for a modern business to operate safely. The malware menace has grown from the early

days when an exceptionally nasty virus might have caused down time or the loss of unprotected data. Modern malware can cause these problems but newer forms of malware also include the possibility of a company being a source of additional internal and external attacks, data theft, financial liability, loss of reputation and a number of other potentially disastrous outcomes.

Even if a company is legally protected from customer lawsuits by their EULA the customer will still have an expectation that their data will be protected. When companies have security breaches that involve the disclosure of sensitive data customers lose faith in that company's ability to protect them and move their business to a competitor. Malware, especially spyware in its numerous forms, can lead to this type of information disclosure. Equally troubling is that a focused attack using malware may also be launched to gain access to sensitive information. Companies must protect themselves from both focused and unfocused attacks if they hope to retain the trust of their customers.

Finally, companies have an ethical responsibility beyond their legal responsibilities. Companies must at least show a good faith effort to protect their systems from malware and other attacks as a method of protecting the online environment as a whole. All entities whether they are individuals or companies have an ethical responsibility to protect themselves when they establish a connection to the Internet. By protecting themselves these entities are protecting other Internet users. A perfect example of this is the DDOS attack. DDOS attacks are very difficult, if not impossible, to defend against since they simply overwhelm the victim's resources. On the other hand, if everyone took on their responsibility to protect their small part of the Internet DDOS attacks could be eliminated because huge bot armies would not be possible.

In order for companies to protect themselves the question that must be asked is twofold. First “What are companies currently doing to mitigate malware risks?” and secondly “Is that enough?” The proposed further research outlined in this paper will answer the first question. The second question can only be partially answered at this time. Further controlled experimentation will need to be undertaken to assess whether the current malware prevention techniques are effective. It is important to assess what is being done in the corporate world before tests that will mirror and evaluate these prevention techniques can be fully devised for the lab.

Malware is without a doubt a menace to modern computing environments, especially environments connected to the Internet. Since connecting networks of computers creates a great deal of good security professionals must find a way to mitigate the malware threat. The proposed research outlined in this paper will be the first step in determining what mitigation techniques are being used in the corporate world and from there it will be possible to empirically evaluate the effectiveness of these techniques.

References

- Arnett, K.P., Schmidt, M.B. (2005, August). Busting the Ghost in the Machine. *Communications of the ACM*. 48(8), 92.
- Awad, N.F., Fitzgerald, K. (2005, August). The Deceptive Behaviors that Offend Us Most About Spyware. *Communications of the ACM*. 48(8), 55.
- Berghel, H. & Hoelzer D. (December 2005). Pernicious Ports. *Communications of the ACM*. 48(12), 23.
- Conry-Murray, A. (2006, March). Who Knows What Evil Lurks?. *IT Architect*. 21(3), 18.
- English, Ed. (2006, January/February). Why You Should Not Play the Numbers Game with Anti-Spyware Vendors. *Information Systems Security*. 14(6), 23.
- Fontana, J. (2006, April 24). Rootkits Aren't Doom - But Keep Up Defenses. *Network World*. 23(16), 20.
- Ford, R. (1998). Malware Briefing. *Computers & Security*. 17(2), 110.
- Gibson, S. (2005, August). Spyware was Inevitable. *Communications of the ACM*. 48(8), 37.
- Gordon, S. (2005, July/August). Fighting Spyware and Adware in the Enterprise. *Information Systems Security*. 14(3), 14.
- Hancock, B. (2004). Law Suits for Cyber Damages Increasing. *Computers & Security*. 20(4), 289.
- Hayes, F. (2006, April 17). Routed by Rootkits. *Computerworld*. 40(16), 58.
- Henry, P.A. (2005, November/December). Firewall Considerations for the IT Manager. *Information Systems Security*. 14(5), 29.

- Hu, Q., Dinev, T. (2005, August). Is Spyware an Internet Nuisance or Public Menace?.
Communications of the ACM. 48(8), 61
- Keller, S., Powell, A., Horstmann, B., Predmore, C. & Crawford, M. (2005, Spring).
Information Security Threats and Practices in Small Businesses. *Information
Systems Management*. 22(2), 7.
- Klang, M. (2004). Spyware - The Ethics of Covert Software. *Ethics and Information
Technology*. 6(3), 193.
- Kotulic, A. G. & Clark, J.G. (2004, May). Why There Aren't More Information Security
Research Studies. *Information & Management*. 41(5), 597.
- Kucera, K., Plaisent, M., Bernard, P., Maguiraga, L. (2005). An Empirical Investigation
of the Prevalence of Spyware in Internet Shareware and Freeware Distributions.
Journal of Enterprise Information Management. 18(5/6), 697.
- Messmer, E. (2005a, October 31). Botnets Turning Into Spyware Enemy No. 1. *Network
World*. 22(43), 10.
- Messmer E. (2005b, Nov 7) Botnets Getting Nastier. *Network World*. 22(44), 1.
- Nachenberg, Carey. (1997, January). Computer Virus-Antivirus Coevolution.
Communications of the ACM. 40(1), 46.
- Passmore, D. (2006, May). DDOS Attack Mitigation: Potential Solutions. *Business
Communications Review*. 36(5), 14
- Poston, R., Stafford, T.F., Hennington, A. (2005, August). Spyware: A View from the
(Online) Street. *Communications of the ACM*. 48(8), 96.
- Schmidt, M.B., Arnett, K.P. (2005, August). Spyware: A Little Knowledge is a
Wonderful Thing. *Communications of the ACM*. 48(8), 67.

- Shukla, S., Nah, F. (2005, August). Web Browsing and Spyware Intrusion.
Communications of the ACM. 48(8), 85.
- Sipior, J.C., Ward, B.T., Roselli, G.R. (2005, Spring). The Ethical and Legal Concerns of
Spyware. *Information Systems Management*. 22(2), 39.
- Stafford, T.F. & Urbaczewski ,A. (2004). Spyware: The Ghost in the Machine.
Communications of the Association for Information Systems. 14, 291.
- Swartz N. (May/June 2004). Viruses on Rise, but Are Companies Liable?. *Information
Management Journal*. 38(3), 18.
- Thompson, R. (2005, August). Why Spyware Poses Multiple Threats to Security.
Communications of the ACM. 48(8), 41.
- Weiss, A. (2005, March). Spyware be gone!. *NetWorker*. 9(1), 18.
- Younghwa, L., Kozar, K.A.. (2005, August). Investigating Factors Affecting the
Adoption of Anti-Spyware Systems. *Communications of the ACM*. 48(8), 72.
- Zhang, X. (2005, August). What Do Consumers Know about Spyware?. *Communications
of the ACM*. 48(8), 44.

Appendix

Malware Survey

E-mail Address _____

What country do you work in? _____

Part I. Traffic Filtering

	Yes	No
Have you implemented a firewall at the perimeter of your network to separate the production network from the Internet?		
Do you filter traffic entering the protected network?		
Do you use a default deny ruleset for incoming traffic?		
Do you filter traffic leaving the protected network?		
Do you use a default deny ruleset for traffic leaving the protected network?		
Do you block Internet Relay Chat (IRC) traffic?		
Do you block instant messaging traffic?		
Do you block peer-to-peer (P2P) traffic?		

Comments:

Part II. Personal Firewalls

Have you installed personal firewalls?	Yes	No	Current Project	N/A
Windows servers				
Linux/UNIX servers				
Mac servers				
Other servers				
Windows laptops				
Windows desktop/workstation PCs				
Mac workstations/laptops				
Linux/UNIX workstations/laptops				
Other workstations/laptops				

Comments:

Part III System Patching

Do you have automated patching for system vulnerabilities?	Yes	No	Current Project	N/A
Windows servers				
Linux/UNIX servers				
Mac servers				
Other servers				
Windows laptops				
Windows desktop/workstation PCs				
Apple Mac workstations/laptops				
Linux/UNIX workstations/laptops				
Other workstations/laptops				

Comments:

What method do you use for patching systems?	Vendor supplied automatic	Third party automatic	Manual Web Install	Manual Download and Install	Not Patched	N/A
Windows servers						
Linux/UNIX servers						
Mac servers						
Other servers						
Windows laptops						
Windows desktop/workstation PCs						
Apple Mac workstations/laptops						
Linux/UNIX workstations/laptops						
Other workstations/laptops						

Comments:

Part IV Anti-Virus Software

Have you installed anti-virus software?	Yes	2 or more	No
At the gateway or proxy			
At the external mail relay			
At the internal mail server			

Comments:

Have you installed anti-virus software?	Yes	No	Current Project	N/A
Windows application servers				
Linux/UNIX application servers				
Mac application servers				
Other application servers				
Windows web servers				
Linux/UNIX web servers				
Mac web servers				
Other web servers				
Windows laptops				
Windows desktop/workstation PCs				
Apple Mac workstations/laptops				
Linux/UNIX workstations/laptops				
Other workstations/laptops				

Comments:

	Yes	No	N/A
Do you use anti-virus scanners from multiple companies			

Comments:

Which of these techniques do you use for updating your anti-virus signatures	Yes	No	N/A
Automatic update on each machine			
Automated update pushed from a central server			
Third party update tool			
Home grown upgrade system			
Manual installation on a predefined schedule			
Manual installation on an as needed basis			

Comments:

Do you use heuristic anti virus scanning? (Choose only one)	Yes
Set at low sensitivity	
Set at medium sensitivity	
Set at high sensitivity	
Disabled due to false positives	
Disabled for other reasons (Please explain in the comments.)	

Comments:

Part V Anti-Spyware and Anti-Adware Software

Have you installed anti-spyware/anti-adware software?	Yes	2 or more	No
At the gateway or proxy			
At the external mail relay			
At the internal mail server			

Comments:

Have you installed anti-spyware/anti-adware software?	Yes	No	Current Project	N/A
Windows application servers				
Linux/UNIX application servers				
Mac application servers				
Other application servers				
Windows web servers				
Linux/UNIX web servers				
Mac web servers				
Other web servers				
Windows laptops				
Windows desktop/workstation PCs				
Apple Mac workstations/laptops				
Linux/UNIX workstations/laptops				
Other workstations/laptops				

Comments:

	Yes	No	N/A
Do you use anti-spyware/anti-adware scanners from multiple companies			

Comments:

Part VI Intrusion Detection/Prevention System (IDS/IPS)

	Yes	No	N/A
Do you use an IDS?			
Do you have IDS signatures loaded to detect viruses?			
Do you have IDS signatures loaded to detect worms?			
Do you have IDS signatures loaded to detect Trojans?			
Do you have IDS signatures loaded to detect spyware?			
Do you have IDS signatures loaded to detect other malware?			
Do you use an IPS in place of or in addition to an IDS?			
Do you have IPS signatures loaded to detect viruses?			
Do you have IPS signatures loaded to detect worms?			
Do you have IPS signatures loaded to detect Trojans?			
Do you have IPS signatures loaded to detect spyware?			
Do you have IPS signatures loaded to detect other malware?			

Comments:

Part VII Spam

	Yes	No	N/A
Do you filter spam at the mail server or mail relay?			
Do you filter spam at the desktop?			
Is malware mitigation a consideration in spam filtering?			

Comments:

Part VIII Policies

	Yes	No	Role Dependent	N/A
Do users have administrative credentials for their own systems?				
Do employees with administrative credentials always or usually log in using administrative credentials?				
Are users allowed to install software on systems?				
Does IT review software before it is installed?				
Is the use of peer-to-peer software limited or banned?				
Is the use of IRC software limited or banned?				
Is the use of instant messaging software limited or banned?				

Comments:

Part IX Malware Removal

Which of these techniques have you successfully used to clean malware infections	Yes	No	N/A
Anti-virus software			
Anti-spyware/anti-adware software			
Anti-rootkit software			
Drive imaging tool			
Reinstallation after formatting the hard drive			
Other methods/tools (Please explain in the comments.)			

Comments: