Understanding and Defending Against the Ways Malware Spreads

Introduction

Malware is one of the many security threats to an organization's network. As it continues to grow and vary, it is important for an IT Professional to remain well informed of the various means in which malware might try to infiltrate the network. Threats that utilize the network and spread with or without human intervention are a serious risk. Another vector for the spread of malware comes from attackers utilizing social engineering to increase the odds in their favor that a malicious attempt will lead to a successful infection. Finally, this paper explores ways in which the World Wide Web is leveraged as another channel to spread malware. With each section, the means to defend against that particular threat is also discussed at length.

Exploits Across the Network

The modern world is nothing if not a complex network. The Internet connects over 2.4 billion users, over 34% of the world's population (Internetworldstats.com). Unfortunately, many of those connections are the source of malicious attacks against the rest of us. From the small home wireless network to large corporate Wide Area Networks, preventing malware attacks is paramount. With so much on the line there are far too many exploits across networks that require sophisticated security defense plans.

Worms such as Code Red, Nimda, and Slammer (also known as SQL Slammer) have caused millions of dollars in damage in the past, disabling many government, corporate, and educational networks. Many more were shut down voluntarily as a precaution. A computer worm is a self-replicating program that penetrates a system to spread malicious code. They can utilize networks to send copies of itself to other computers. Some of the harm caused can include the installation of backdoors to allow access to the network by hackers, sending documents via email consuming bandwidth, and the deletion or transmission of files (PCTools.com). Unlike most viruses, worms don't need guidance or another computer program to attach to and can be transported via file sharing, infected websites and attachments. A good example of how a worm sneaks its way onto a network is the Nimda worm or "readme.exe". The worm spread by sending infected e-mail messages, copying itself to computers on the same network, and compromising Web servers using Microsoft's Internet Information Server (IIS) software. (Cnet.com)

A Trojan horse is a non-mobile malware designed to provide unauthorized, remote access to a user's computer by deleting a system file and taking on the system file's name. Trojan horses can turn a computer into a zombie computer or bot, stealing data, keylogging and installing more malware and allowing crackers to control the compromised computer simply by searching for computers on a network using a port scanner and finding ones that have already been infected with a Trojan horse. Forms of Trojans specifically dangerous to networks are Trojan Downloaders and Droppers. Droppers often carry several unrelated pieces of malware that can be different in behavior. They are a type of malware archive of different malicious code. They can include a joke to distract the user from the real purpose, the background installation of code, adware or 'pornware' programs. Most droppers are written using VBS or JavaScript and are thus easy to write and perform multiple tasks. Downloaders are much smaller than Droppers and are used to install malicious code on a victim machine and can also be used to download constant new versions of malicious code, adware or 'pornware' programs. Downloaders are also commonly written in script languages such as VBS or JavaScript. They also often exploit Microsoft® Internet Explorer vulnerabilities. (Securelist.com)

Another network threat is called a zero day vulnerability, meaning a hole in a software application that the vendor is unaware of, which is exploited by hackers before the vendor becomes aware of the issue. The attacks can include infiltrating malware, spyware or allowing unwanted access to user information. Once the vulnerability becomes known, a race begins for the developer, who must protect users. Examples of zero day attacks include the Code Red worm, the Mac Flashback, and Back Orifice/Netbus (PCtools.com).

As mentioned previously, email attachments are a grave threat for the transport of malware. One of the most damaging examples was the Melissa virus. The Melissa virus flooded corporate networks with e-mail messages. The huge amount of e-mail it created forced some companies, including Intel and Microsoft, to shut down their e-mail servers. Melissa was a macro virus, or a computer virus written in the same macro language used for software applications like word processor, releasing a chain of events in conjunction with the application. The virus launched when a user opened an infected Microsoft Word document sent as an e-mail attachment. Users were duped into opening the attachment because the e-mail, usually had the name of someone the recipient knew and a subject line saying, "Here is the document you asked for... don't show anyone else ;-)." When it was an attachment, the virus was sent to the first 50 names in the user's address book. Copycats such as the love letter virus also spread quickly as a Visual Basic script attachment to an e-mail message with a provocative subject line. It also took the names from the Outlook address books of infected PCs to infect more victims. To take a strong stand against this type of malicious attack, the government prosecuted the writer of the Melissa virus, who was convicted and sentenced to 20 months in federal prison for unleashing the virus that caused more than $80 million in damage (PCWorld.com).

Defending Against Threats Across the Network

To combat these many malware threats, larger organizations protect their networks through the use of firewalls. As opposed to static packet filter firewalls or stateful packet inspection firewalls, application proxy firewalls inspect application content in the traffic that travels between clients and servers using an HTTP proxy program on an application proxy firewall. All major firewall vendors have protocols for working with antivirus servers. When a firewall inspects a package it checks its policy rules base, determining if the object should be passed to the antivirus server. The antivirus server filtering goes beyond viruses, searching for worms, Trojan horses, phishing, spam, rootkits, malicious scripts and other malware. If the antivirus server does not drop the object it is returned to the firewall to be passed on or direct to the recipient.

A paper by J.V. Antrosiom from Wake Forest University, states that existing malware defenses based on fingerprint or signature technology which look for a type of network behavior or specific code is vulnerable because new variants of worms can bypass the malware defense by changing their signature or fingerprint. He proposes a new defense system that consists of three components: security authentication, quarantine system, and a policy manager. In contrast to user authentication, security authentication detects and characterizes the vulnerabilities of the machine. This new type of authentication is necessary because an authenticated user can unknowingly bring an infected machine into a secure network. Therefore, the new defense is particularly effective at preventing the spread of malware inside a local network where traditional firewall systems are no longer effective.

Social Engineering

Social Engineering, as a means to spread malware, has evolved over the years to become one of the most frequent vectors used for successful infections. Social engineering is the manipulation of an individual to lead them to a particular action or to share information that should otherwise be kept confidential. When it comes to spreading malware, most encountered social engineering attempts are simplistic though complex ruses are becoming more frequent as they prove successful.

Social engineering can be as simple as lying and deceiving a victim. It can also be quite elaborate by creating a scenario and building legitimacy with the intended target. A reasonable request to one person in an organization might allow a social engineer to use them or the information they provided to build a believable story for a different person. Building the scenario in social engineering, for example, lying to a secretary and telling them that you are working with their boss and need certain information, is called pretexting. A manipulation using pretexting makes the story more difficult to detect as a scam and tends to make it more likely that a target will comply with the manipulator. Instead of using a vulnerability or hacking a network, a social engineer aims to get individuals within the organization to use their access rights to do their bidding, which could include installing malware.

Trojan horse malware, mentioned previously as a threat across the network, is also a social engineering attempt to infect computers with malware. It spreads by seeming to be a desired program. It employs social engineering to infect victims by getting the end-user to execute the program even though it is malicious. Convincing a user to run a file could be as simple as using the right file name, such as patch.exe as was the case with NetBus, an infamous Back Orifice tool (Podrezov, A., & Hypponen, M.). Other Trojans might disguise themselves as popular free applications such as Firefox or VLC and rely on SEO or use advertising to be the first search result instead of the legitimate product (Hamilton, J.). While the Trojan might still install the desired program, it could install other malware during the process to log keystrokes, show ads, or join the computer to a botnet.

Some people may let their guard down when it comes to their email but it is another technology that social engineers can use to try manipulating a person. A phishing email is an email that seeks account details like usernames, passwords, or credit card numbers while disguising itself as a legitimate email. These could be very generic emails spammed to millions of people at a time in the attacker's hopes that enough people will respond to make the effort profitable. Phishing emails might be disguised as an email from popular websites or big businesses like banks, eBay, PayPal, Hotmail, and others. In order to make phishing emails even more believable, a social engineer might use a URL shortener to obscure the destination of a link, typo squat on a similar URL, or make use of subdomains. The difference between an address like paypal.com and paypa1.com (with a 'one' instead of the 'L') could be indistinguishable with the right font or go unnoticed if the victim is not paying close attention.

A more targeted phishing attack is called spear phishing. It might use information relevant to a person or organization to make it more believable. Valuable details to build a sophisticated attack can potentially be found on social networks, the company website, or from a separate, previously compromised account. A phishing email might request account information as a reply, direct a user to a website, or request that the recipient download an attachment. Malicious PDFs or Microsoft Office files exploiting zero day vulnerabilities have been used recently to infect computers with malware (Adobe Security Bulletin). These malicious attachments might then take advantage of vulnerabilities in their program to install malware on the target computer (Global Research & Analysis Team, Kaspersky Lab).

Not all social engineering efforts are direct manipulation attempts. Some just take advantage of natural interest in free objects or people's curiosity. USB drives might be used in a targeted attack on an organization. An attacker could leave a malware-laden USB drive in the parking lot. A well-meaning person might find it on their way into the office and plug it in to investigate what files are on it. The attacker that planted the drive could have it configured to install malware using an autoplay exploit. They could also place infected files on the drive with an invoking name like '2013 salary list.xlsx' to entice the victim to execute them manually. USBs could be infected with a rootkit with the capability to email private information outside of the organization, against company policy. Penetration tests frequently use this to test for employees inserting unknown devices or any devices into company computers (Goodchild, J.). This attack is commonly referred to as baiting.

Social engineering started off as a psychology term. Crossing over to malware, social engineering has embraced one of the most driving forces of human psychology, fear (Lavasoft News - Understanding Social Engineering). Scareware is the term for malware that presents false information to a user to drive them to pay for software or download further software in an attempt to fix the falsely-claimed problem. By planting redirect code on popular websites, creating websites on breaking news, or buying ads known as malvertising, victims are unknowingly led to websites that may display a realistic-looking report that their computer is infected or the site may have malicious code to install a fake anti-virus which will similarly try to convince the victim that they need to purchase the "full" version of the fake program in order to deal with the problem.

The scareware tactics are over a decade old, when computer users easily bought into security panic following the Blaster worm (Wallace, B.). Building on scaring people, ransomware takes the infection a step further. Ransomware is malware that infects a computer and holds the computer or data hostage until a payment is made. One popular family of ransomware are variants of the FBI virus which launches at startup to prevent any other action from being taken that shows a message supposedly from the FBI (or other government agency). The message states that the FBI is aware of the user's illegal actions and that a fine must be paid. Whether the motivation is either a guilty conscience or fear of losing access to their computer, victims may make a payment to the scammer instead of disinfecting the computer. This can net the attacker millions of dollars with the scam (AFP.).

Perhaps the most direct social engineering approach to spread malware is the fake technical support phone call. A malicious actor might call a victim and claim to be from Microsoft, Apple, or another technical company (James, P.). The scammer then works to convince the victim of their legitimacy and the need for the phone call. They might direct the user to a standard system file or registry key and then claim that that file's existence is a side effect of being infected with a virus. The attacker insists if the victim will allow them to remotely control their computer, they can remove the claimed infection. Once granted remote access, the malicious person will then proceed to install malware, a fake anti-virus program, or delete crucial system files to help illustrate their claim that a computer is infected (Krebs, B.). At this point, the scammer will conclude their "assessment" of the situation and will state a price that must be paid in order for them to remotely service the computer which may still not actually cure the problem.

Defending Against Social Engineering

Social engineering is one of the most difficult vectors to guard against. Since an attacker manipulates a user into performing the desired task, many security safeguards are useless to prevent inadvertent infections. The attacker does not need a user name and password cracked in order to compromise an otherwise secure network if that information can be simply requested.

While antivirus and other security programs can prevent identified, malicious files from residing on an endpoint, they cannot always determine when a user is being manipulated or is performing a legitimate task such as downloading and running software, using email, or accessing various files. Security best practices such as separation of duties can prevent a complete process from being compromised by having multiple users involved. In addition, educating end-users is often a first step to help prevent social engineering. Training users to recognize phishing or other scams can prevent social engineering attempts from succeeding. In addition to raising public awareness, other attempts to deal with the growing number of incidents include legislation, user training, public awareness, and technical security measures. Microsoft cites its SmartScreen Filter blocks between 2 and 5 million attacks a day for users of Internet Explorer versions 8 and 9. (Haber, J.) Legislation may be able to impose a stiff penalty such as imprisonment and a hefty fine in order to discourage the manipulation of victims with social engineering.

Malware from the Web

While there are many threats facing organizations, from internal risks to natural disasters, none are perhaps as pervasive and as numerous as attacks that take place over the web. These days, self-serving attackers are taking advantage of the scalability of operations that the Internet provides with participation in unscrupulous money-making schemes which lie at the heart of many attacks. From identity theft to schemes where advertisers will pay for clicks, less than ethical publishers will find illegal means to acquire those clicks and traffic in order to make a quick buck, often times at the expense of a user's personal security.

With the continual maturation of the Internet, more and more services are being hosted online which means more of our personal information is online than ever before. White Hat Security says that the web layer is "…the number one target for malicious online attacks". (Grossman, 2007) Services like DropBox host millions of people's personal documents, and Apple's iCloud hosts people's photos all across the web. With all of this, it's easy to understand how malware from the web can be an increasingly important factor for IT security specialists to monitor.

One of the more popular web threats facing companies and individuals alike is cross-site-scripting (XSS). Grossman's security report states that XSS is the most likely threat a user can experience, which outlines the need for safeguarding your websites and users against these kinds of threats.

XSS works on unprotected pages when an attacker injects malicious scripts in to a web page that accepts user input. The malicious code is often injected browser-side from the attackers system. Let us consider a scenario in which a website has a search function that uses a standard HTML input form field. The behavior of many internal site searches is to show a search results page that says something to the effect of "Results for [search query]" thus repeating the searcher's input. An unprotected form would be vulnerable to an attacker injecting HTML in to the page that could potentially harm the visitor. They may put a hyperlink instructing the user to download an executable or they may overwrite the contents of the HTML page to show something else. The danger is especially high, since the visitor would not typically have any reason to distrust a link from a reputable website.

The fact that this code is implemented in an otherwise trustworthy website makes these attacks especially dangerous since users will typically not think to mistrust sites they frequent and have had positive experiences with in the past. All it takes is one unsecured form and the script will have open rein to a user's cookies, session ID's and any other information contained within your browser. Additionally, the contents of the HTML page may be overwritten to suit the needs of the attacker. XSS is clearly a threat and organizations should do their best to verify that the threat is mitigated by taking proper security measures against these sorts of threats. Defense against XSS is attained by making sure that data is not accepted from untrusted sources without escaping it first.

Another type of threat facing organizations is that of drive-by downloads. The perimeter is getting harder and harder to secure not only because of organizations needing to adopt BYOD (Bring Your Own Device) policies but also because more and more of the Internet needs to be accessible for employees to conduct their business. This means relaxing firewalls and letting more traffic through which also increase the likelihood of a successful attack.

A drive-by-download can occur either as a result of an XSS attack, or by simply visiting a site that has hidden the malicious intent of the download behind a rather innocuous message. Often times it appears in the form of a warning message from an antivirus program in an attempt to get the user to take action. Google has even reported that in 2007, one in ten websites was hosting a drive-by download file. (University, 2013) While both drive-by downloads and XSS are both serious threats to organizations, the effects are typically not as wide in magnitude as some recent intrusions in to systems that have taken place in the past several years.

Perhaps the most damaging and impactful of attacks occurs between enterprise level organizations and even between nations. The complexity of worms has reached a point where governments are investing heavily in what amounts to cyberwar in efforts to hinder nuclear research and acquire intelligence about foreign nations. In fact, the US's top intelligence officials declared in March of 2013 that cyberwar is the single biggest threat to the US's security, beyond even Al Qaeda. (Dilanian, 2013) The most famous example of this recently has been the Stuxnet worm that was launched in 2009 in what is believed to be a joint effort between Israel and the United States. The Stuxnet worm targeted centrifuges at the Natanz uranium enrichment plant in Iran (Zetter, 2013) that reportedly set their ability to create a nuclear weapon back by three years.

Due to the nascence of such attacks, the international rules governing what constitutes an "attack" are not well agreed upon. Some see these as acts of force while others, a part of espionage that has been going on in the non-technological world for years. One thing is for certain, though: it can be very easy to disavow the actions of an individual or group, but the fact that nearly everything online leaves a digital trail there does appear to be a higher likelihood of tracing given attacks back to their originator. However, proving a connection may be difficult. For instance, the US knows that a record-breaking number of attacks are originating from China, however the government will disavow any involvement in them.

While the purposes of the US and Isreal's joint-venture were more or less harmless to the average citizens of Iran, cyberwar has the potential to wreak havoc on citizens. A nation's entire financial systems, transportation systems, and power grids are all connected now and the takeover by a malicious attacker could lead to devastating outcomes.

Defending Against Web Threats

The securing of systems from cyberwar goes beyond simply installing firewalls and setting up VPN tunnels. Physical and electronic security systems must be in place in order to prevent intruders from either acquiring access to protected areas or sending a worm or other information-based attack. An all-encompassing security architecture needs to be in place to safeguard against cybercrime: one that encompasses all facets of information security, both physical and electronic.

It's clear that malware from the web covers all spectrum of criminal ranging from smalltime hackers looking for a quick buck to global efforts in espionage and terrorism conducted by nations and guerilla groups. There are numerous ways to safeguard against these, but IT security professionals will need to continually hone and update their skills and knowledge to reduce the risk of an event occurring.

Security against web threats requires a commitment to an environment of security by an organization. An IT governance board should have rules governing the proper use, storage, transmission of confidential information as well as proper filtering and firewalls in place for incoming traffic.

Ingress filtering conducted via a firewall can help drop potentially malicious packets. A firewall should be protecting all internal systems from external threats. It is also a good idea to have egress filtering to make sure that no threats are originating from within the organization. Firewalls and filters will prevent a lot of the SPAM emails containing hacked websites or phishing attempts, but users must still be aware of attempts at gaining access to their system.

In addition to firewalls, physical security is important and should be taken into consideration. An attacker that has gained access to an Ethernet port may set up a wireless access point allowing him connection to internal networks. Sweeps should be conducted regularly to safeguard against such threats.

Ultimately there is no end-all solution for web security management. The numerous points of entry require a persistent commitment to information security to maintain any hope of preventing web attacks. A well planned firewall architecture with proper filtering and packet evaluation along with physical security measures serve as a good base for starting a culture of IT security that can be built upon and evolved over time.

Conclusion

Defending against malware and people with malicious intents can become a cat-and-mouse game. For example, antivirus definitions are being updated at an increasingly frequent pace to try to keep up with the growing variety of malware that exists. In this paper we examined threats over the network, social engineering risks, and malware that leverages the Internet to spread and infect more users. While the paper discussed many defense measures that may be implemented to improve security, there will always be malicious actors looking for a new angle to take advantage of as long as there is a benefit or profit to be had. For that reason and the rapidly changing nature of technology, it is important for IT Professionals to understand and continue to grow their knowledge on the numerous threats to their networks that exist.

References

AFP. (n.d.). Spanish Police and Europol Bust Global "Ransomware" Operation. *SecurityWeek.Com*. Retrieved April 10, 2013, from http://www.securityweek.com/spanish-police-and-europol-bust-global-ransomware-operation

Adobe - Security Advisories: APSA13-02 - Security Advisory for Adobe Reader and Acrobat. (n.d.). *Adobe*. Retrieved April 10, 2013, from http://www.adobe.com/support/security/advisories/apsa13-02.html

Antrosiom, J.V.; Fulp, E.W., "Malware defense using network security authentication," Information Assurance, 2005. Proceedings. Third IEEE International Workshop on, vol., no., pp.43,54, 23-24 March 2005

Dilanian, K. (2013, March 12). Cyber-attacks a bigger threat than Al Qaeda, officials say. *LA Times*.

Global Research & Analysis Team, Kaspersky Lab. (n.d.). The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor. *Securelist*. Retrieved April 10, 2013, from https://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor

Glossary - Securelist. (n.d.). Securelist - Information about Viruses, Hackers and Spam. Retrieved April 11, 2013, from http://www.securelist.com/en/glossary?glossid=189275905

Goodchild, J. (n.d.). Social Engineering: Anatomy of a Hack. *CSO Online* . Retrieved April 13, 2013, from http://www.csoonline.com/article/479038/social-engineering-anatomy-of-a-hack

Grossman, J. (2007). *WhiteHat Website Security Statistics Report.* Santa Clara.

Haber, J. (n.d.). SmartScreen Application Reputation in IE9. *IEBlog - MSDN Blogs*. Retrieved April 10, 2013, from http://blogs.msdn.com/b/ie/archive/2011/05/17/smartscreen-174-application-reputation-in-ie9.aspx

Hamilton, J. (n.d.). Is Your Firefox Genuine? Phishing at its Phinest!. *404 Tech Support*. Retrieved April 10, 2013, from http://www.404techsupport.com/2010/01/is-your-firefox-genuine-phishing-at-its-phinest/

James, P. (n.d.). AppleCare Overwhelmed by Calls About Fake Antivirus. *Intego Mac Security*. Retrieved April 10, 2013, from http://www.intego.com/mac-security-blog/applecare-overwhelmed-by-calls-about-fake-antivirus/

Krebs, B. (n.d.). Aghast at Avast’s iYogi Support. *Krebs on Security*. Retrieved April 10, 2013, from krebsonsecurity.com/2012/03/aghast-at-avasts-iyogi-support/

Lemos, R. (n.d.). 'Nimda' worm strikes Net, e-mail. Technology News - CNET News. Retrieved April 13, 2013, from http://news.cnet.com/2100-1001-273128.html

Panko, R. R. (2010). Corporate computer and network security. Upper Saddle River, NJ: Pearson Prentice Hall, c2004..

Rosencrance, L. (2002, May 1). Melissa Virus Author Sentenced. PCWorld. Retrieved April 13, 2013, from http://www.pcworld.com/article/97964/article.html

University, C. (2013). Drive By Download.

What is a Computer Worm?. (n.d.). PC Tools. Retrieved April 12, 2013, from http://www.pctools.com/security-news/what-is-a-computer-worm/

What is a Zero-Day Vulnerability?. (n.d.). PC Tools. Retrieved April 12, 2013, from http://www.pctools.com/security-news/zero-day-vulnerability/

World Internet Users Statistics Usage and World PopulationStats. (n.d.). Internet World Stats - Usage and Population Statistics. Retrieved April 12, 2013, from http://www.internetworldstats.com/stats.htm

Zetter, K. (2013, March 25). *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*. Retrieved from Wired: http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/