Malware White Paper
April 2011

Emerging Trends in Malware - Antivirus and Beyond

One need only listen to the news or read the latest Twitter and media updates to hear about cyber crime and be reminded of the importance of internet and data security. The last few months of 2010 were filled with stories of WikiLeaks and the whistle-blowing website's effect on the security of nations across the globe. This story was just one of many that highlighted the fact that all levels of businesses and individuals, not to mention government agencies, are subject to the necessity of data security and the need to be aware of multi-level cyber threats in 2011 and beyond. While the WikiLeaks site was motivated by publicity and politics, the trend in cyber crime has moved towards financial motivation, which indicates that it will continue to grow and put everyone at risk. Cyber crime is the big bad wolf, concealed in many forms, like the wolf dressing up as the grandmother ready to pounce on the unknowing Red Riding Hood.

This paper will explore the different types of malware surfacing today and some of the solutions available to protect yourself against them. These types of threats go beyond the standard ones of computer viruses and require more protection and, often, more than one type of security software.

Malware and the forms of Malware

Malware, short for malicious software, can encompass a variety of hostile or criminal software. Malware is a term that is an umbrella for multiple threats including computer viruses, worms, trojan horses, rootkits and other unwanted software. It is intended to cause harm to or infiltrate computer systems without the user or owner's knowledge. It can even be disguised as legitimate software and appear to come from an official site. This big bad wolf comes in many forms.

The most common forms of malware are viruses and worms. A virus is a program that has infected software, and, when run, causes the virus to spread to other executables and requires the user to "open" the program, thus activating the virus. A worm is spread automatically, actively transmitting itself to spread over other computers.

The first reported self-duplicating virus occurred 25 years ago and was called the Brain Virus, created by two brothers in Pakistan who were testing loopholes in their company's software, a company named Brain Telecommunication.[1] This type of virus had to be transmitted by floppy disks, which seems antiquated compared to today's modes of malware threats. The Morris Worm, in 1988, was the first known worm malware. Its creator was a Cornell student who was subsequently convicted of computer fraud. This worm slowed computers down or rendered them useless by exploiting vulnerabilities in the network server. Worms continue to pose such a threat today.

Virus: ***a program that has infected software, and, when run, causes the virus to spread to other executables and requires the user to "open" the program, thus activating the virus.***

Harking back to the story of Troy, a trojan horse is a form of malware that hides within another program. Because this type of malware is disguised as something harmless, the user is misled to run it, which leads to attacks, like the ancient Greek warriors leaping out of the trojan horse. This type of malware is often contained in programs that someone would download on a PC, such as music, games, photos or videos. Once a trojan is downloaded, hackers have the ability to access your computer and save personal information.

A rootkit is not the actual malware, but the program used to hide the malware. The rootkit can modify the user's operating system, so that the malware is concealed. Very often, the rootkit comes bundled with other types of malware, such as viruses, etc. Rootkits enable a hacker to store files on your computer and open the opportunity for multiple instances of illegal activity. The level of activity that a hacker can engage in on your computer is frightening and almost unimaginable. The hacker can send information to websites, use credit card information and cause disruption to the user.

Trojan Horse: ***a form of malware that hides within another program. Because it is disguised as something harmless, the user is misled to run it, which leads to attacks.***

A type of malware that affects most computer users is spyware. It is designed to steal information about the computer user. It records the activities and habits of the user; some types can even record keystrokes and information that is typed on websites or other programs. Spyware is used to gather information for certain advertising or for identity theft. It sends information to advertisers who then use it for pop-ups while you are surfing the web.

[1] http://www.pcmag.com/slideshow/story/261678/4-malware/a-brief-timeline

More prevalent Malware threats today

As technology grows and develops, so does the malware. Those trends in technology that influence our lives and effect how we spend our days leave us, as individuals and businesses, open to malicious attacks. Malware is growing the most in the areas of search engines, social networks and mobile devices. We now use the word “google” in our everyday language to describe searching for something online. Even an 85-year-old grandmother has a Facebook page to keep in touch with her family. The mobile phone is now a necessary accessory, like a wallet, to check email, do online banking, buy movie tickets or play a game of Scrabble. While these tools all enhance our lives, they leave us open and vulnerable when unprotected.

Search engines are our go-to sources of information on a daily basis, in our work lives and personal lives, yet they are also a prime target of malware attacks. Search results can be manipulated to draw individuals to malicious pages, and this is done through the ordinary search tools, such as Google, Bing, and Yahoo! Very often, malware is introduced through “malvertising,” faulty advertising that misleads web users and draws them to infected sites. Users’ computers can be infected and personal information stolen.

Spyware: ***malware that is designed to steal information about the computer user. It records the activities and habits of the user; some types can even record keystrokes and information that is typed on websites or other programs.***

In 2010, more than 1 million websites were infected with malware in the fourth quarter of the year, alone. According to Dasient, that was more than double the figures of the previous year.[2] Barracuda, a security provider, recently released its 2010 Annual Security Report, which indicates that attackers are shifting from email spam to targeting the Internet. Among its findings, the amount of malware that appears daily across search engines increased 55 percent from June 2010 to December 2010. Equally disturbing, is that one in five search topics lead to malware, while one in 1,000 search results lead to malware. [3]

Along with advertising infections, an estimated 1.5 million malvertisements per day were served in 2010, according to Dasient. Other prominent targets of malware have been social media and government sites. As of March of 2011, the blogging site, Wordpress, was being hit by denial-of-service attacks. Performance and connectivity problems resulted. A recent White House report on cyber security stated that the number of attacks on government networks increased by 40

[2]Elinor Mills, http://news.cnet.com/8301-27080

[3]http://pr-usa.net, March 7, 2011.

percent last year.[4] PC Magazine's lead analyst for security, Neil Rubenking, finds that government sites may be increasingly vulnerable in this "budget belt-tightening" era. There might not be enough monitoring and updating as a result of reduced funding. [5]

Another area for businesses and individuals to be aware of in the realm of cyber security is mobile malware. Not surprisingly, with the rise of mobile use and applications, mobile malware has also become an issue. According to PC Magazine, mobile malware is becoming ever more sophisticated. The capability of mobile phones to carry out multiple tasks also opens them up to more threats and corruption. Viruses are capable of sending texts, making calls to designated numbers and a variety of other possibilities. In the news most recently, was the malware attack on the Google Android, infecting hundreds of thousands of smartphones, prompting Google to quick action in fighting the attacks and ensuring stronger security in the future.

Prevention and Protection

So, how does a business or an individual protect itself or himself from the looming threats of cyber crime? A first and important step is antivirus protection. Most antivirus programs, if they are reliable, have kept up with growing threats and are more capable than they were just a couple of years ago. Most now include tools to protect against spyware and spam in addition to antivirus, which make them very reliable.

While good antivirus software will protect you against many malware threats, it is important to secure a broad range of protection, one that encompasses more than even a good antivirus program can offer. Protection on many levels is what offers the most security for the business owner and the individual user. A dedicated anti-malware product will often work in conjunction with an antivirus protection, providing the maximum security. An important feature of the antivirus software is that it will unpatch system files. Typically, an anti-malware program will not have that feature but will work alongside the antivirus piece. A reputable anti-malware program will detect, destroy and prevent malware and will detect malware that an antivirus program might fail to identify. Anti-malware programs provide network protection through intrusion detection and prevention. They keep protected data safe and prevent malware from existing on the firewall. The most critical piece to protecting oneself against cyber crime is to be protected on multiple levels and to leave

[4] http://thehill.com/blogs/hillicon-valley/technology, March 22, 2011.
[5] http://www.pcmag.com, November 22, 2010.

nothing to chance. A combination of a firewall along with antivirus and anti-malware software will do that for you. A joint effort of good antivirus and anti-malware will leave the big bad wolf outside, still scheming new points of entry, but incapable of breaking in.