Malware in Information Security

Jared Dukes

East Carolina University
Malware is directly related to Information Security, and can have a negative impact on both businesses and in household computer uses. Malware includes but is not limited to computer viruses, cookies, Trojan horses, worms, adware, and spyware. Malware is the combination of the words malicious and software together to make the word Malware. All of these effect a computer differently, and it depends on what platform it attacks: Windows or a Mac computer to determine the outcome. Malware is something that hackers or other malware writers or attackers use to shut down or infect computer systems or individual computers. No matter how the malware was spread by the individuals, this is a major problem in the Information Security industry and there really hasn’t been a great way to stop these attacks so far.

One of the biggest threats to computer users on the Internet today is malware. It can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up. Malware programs are usually poorly-programmed and can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak.

Many of them will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean. My paper will detail the different varieties of malware along with basic preventive measures. Later on in this paper, I will examine the removal process and review a set of spyware removers. Although also considered to be malware, programs such as viruses, worms, trojans, and everything else generally detected by anti-virus software will be discussed later on in this paper.

You can get infected by malware in several ways. Malware often comes bundled with other programs (Kazaa, iMesh, and other file sharing programs seem to be the biggest bundlers). These malware programs usually pop-up ads, sending revenue from the ads to the program’s authors. Others are installed from websites, pretending to be software needed to view the website. Still others, most
notably some of the CoolWebSearch variants, install themselves through holes in Internet Explorer like a virus would, requiring you to do nothing but visit the wrong web page to get infected.

The vast majority, however, must be installed by the user. Unfortunately, getting infected with malware is usually much easier than getting rid of it, and once you get malware on your computer it tends to multiply.

Computer viruses which are a form of malware used to be the only main attack that would threaten computers. A virus is a computer code or software program built to maliciously damage your computer files and programs or to corrupt your system. Today malware covers a wide array of attacks which are the most prevalent. Worms are similar to viruses in that they will spread themselves around a network. Worms tend to make copies or duplicates of themselves while spreading around. They also may be able to change their profile to avoid detection. A Trojan horse takes on the appearance of something that is benign, such as an update or adds on to an actual program. Once the Trojan horse is on your computer it may perform harmful functions such as erasing your hard drive or deleting all of your pictures. Similar to Spyware, a Trojan horse may also gather information and send it to a developer.

Adware is similar to spyware in that it sits on a computer generally without the user knowing. Adware specifically refers to programs that contain pop-up advertisements. The subject of the ads is often based on surfing habits of the user. Malware as a whole is defined as “Short for malicious software, malware is a catch-all phrase used to define any program that runs on a computer without the user's knowledge and performs predetermined functions that cause harm.”

If a company or organization is infected with some sort of malware that I’ve discussed then it could spread across all the computers on the network. Developers of Malware prefer to spread
malware across a network because it impacts more computers, which can allow them to get more data to send to developers. If one user from that organization gets malware, they can spread it by sending an email attachment with the malware without even knowing it. Organizations can take some preventative measures however to prevent malware to the best of their ability. Anti-virus protection software does help such as Norton Anti-Virus, Microsoft Security, Essentials, or McAfee. These do not prevent 100% of malware, however it does help to prevent the majority of malware attacks. Also I think it is key that everyone in the organization is using the same anti-virus program because it makes it easier to support for their IT staff in case of a malware infection. Firewalls and routers are also key in securing a network from outside attacks. A good firewall will stop traffic from users outside of the network from gaining access in to the network. Routers can act as firewalls themselves and can provide an extra layer of protection. Also it is very important that if the router is wireless that it is secured and not left unsecured for anyone to join the network without proper credentials.

Users on their home networks are easy prey for developers of malware. Adware is one key form of malware that gets many home users easily to click on and consume malware. Adware is in the form of pop-up advertisements that we all see that are based on the individual users browsing history. For example I really like pizza, if the owner of that malware is able to see that I order pizza online a lot they may send me adware relating to discount on online pizza orders. These adware look legit and it is very hard to tell that they are malware and not a real advertisement. Just like an organization, a user on their home network can help themselves by taking some preventative measures. They too should use anti-virus software that will scan their PC to see if they are infected currently, or hopefully that will prevent the malware from entering the computer in the first place. However developers of malware are getting smarter and smarter and are coming up with new ways where anti-virus software will not detect the malware.
Many users think that there is no way they can get malware with an anti-virus software running but this is not the case. Since malware is becoming harder and harder to detect, a user can have malware on their computer for weeks or even months before they even know it. Once malware is on a computer, I’ve seen many times that a pop-up will pop up asking the user to click on it because it will remove the malware or it wants the user to sign up for its diagnostics service. If they can get the user to sign up for their service to “remove” the malware, then they will get the user’s personal data and sometimes credit card information if the user enters it.

Historically malware hasn’t been around that long. Until the last few years, computer-viruses were the main form of infection that hackers used to attack and infect computes. However the hackers and developers of malware had to get smarter, because the computer industry was making advancements to protect computers from viruses and infections. The hackers always tend to be one step ahead, and usually take the lead and force the industry to step up and make advancements to stay up with them. When the industry does in fact catch up or get ahead of the hackers or developers of malware, many times it is too late and they have already been outsmarted.

The purpose of the first malware which was in the form of worms and MS Dos computer viruses were simply written as pranks or experiments. Young developers wrote viruses to practice their techniques and were meant to be merely annoying not harmful and infectious. In 1999 viruses were starting to surface such as the Melissa virus and the David virus. Both of these viruses were written as pranks but became much more serious than that. The Windows Explore Zip virus was written to delete files off of a computer’s hard disk or to corrupt the file system by writing faulty data to the disk. Before the Internet widespread and became mainstream viruses entered a computer by way of the floppy disks boot sector. As Microsoft Windows platforms become more popular in the 1990’s the spread of viruses became more and more plentiful. It became possible to write macros in the application Microsoft Word
and other Microsoft applications. The macro viruses infected documents and templates rather than applications, but they relied on Microsoft Word because word documents are a form of executable code. Today most malware is written for Microsoft Windows systems, however some are also written for Mac, Unix, and Linux. Worms today work much as they did in the 1980’s, they scan the network and leverage vulnerable computers to duplicate themselves. The spread of worms is very quickly, because no human interaction is needed. One major malware attack is the SQL slammer which infected thousands of computers in a few minutes.

The FBI has been taking a much more visible role in the war on cybercrime this year. Back in June 2011, the Bureau announced its success in shutting down two massive malware rings that resulted in multiple arrests. Now, they’ve helped rid the world of about 4,000,000-bot strong criminal network. As far back as 2008, it was common knowledge in the cyber security business that Esthost the creation of an Estonian company called Rove Digital served a clientele that was largely criminal in nature. What the FBI, Trend, and other security companies didn’t know, however, was that Rove Digital was perpetrating cybercrimes of its own on a massive scale.

With those four million bots managed by more than 100 command and control servers, Esthost admins had plenty of cash-generating power at their disposal. Through poisoned DNS settings, infected computers were directed to malicious domains and served fake antivirus applications galore. If you do a quick search for Rove Digital, you’ll find its name plastered all over numerous questionable software titles.

Now that the details have surfaced, it’s almost maddening that it took so long for the botnet to be shut down. Trend Micro claims to have known who was behind the botnet’s activity since 2006, but that’s the nature of the beast when it comes to complex criminal investigations. Trend reports that the
criminals behind the Esthost network were perpetrating crimes ranging from fraud to selling questionable pharmaceuticals as well as other cybercrimes they refused to discuss in the blog post.

If this had been a comparatively minor operation which was, say, only hijacking browsers and facilitating click fraud it probably wouldn’t have taken so long. But Esthost and Rove were obviously doing some very bad things, and authorities needed to ensure that the crew members arrested in Estonia this week go away for a long, long time. This shows the magnitude of malware attacks and what they could negatively impact across the board. Thankfully the FBI and other organizations are stepping in and trying to eliminate malware attacks wherever they can. As we speak now, I’m sure there are developers trying to develop new malware attacks to shut down systems and get as much information as they can. The information is crucial to them in that it provides a wide array of information from identity information, security, and network information.

One way that malware can enter a system is by way of a process called backdoor. Backdoor bypasses normal authentication procedures. Once a system is compromised, one or multiple backdoors may be installed in order to allow easy access in the future. Once malware is installed on the computer, rootkits can take place, this is the act of hiding or concealing the malware from the list of processes in the system’s list of processes. This is pretty incredible because it makes it very difficult for the user to know that their computer is infected at all. Just think what contributions they would have, if the creators of malware would extend their efforts to actually contributing to the IT world instead of trying to break it down!

Some malware is written for the sole purpose of monetary gain, which in the 1980’s and 1990’s this was not the case. During the 1980s and 1990s, it was usually taken for granted that malicious programs were created as a form of vandalism or prank. Today, the greater share of malware programs have been written with a profit motive either financial or otherwise in mind. This can be taken as the
malware authors' choice to get their control over infected systems and to turn that control into a source of revenue. Spyware programs are commercially produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator. For instance, some spyware programs redirect search engine results to paid advertisements. Others, often called "stealware" by the media, overwrite affiliate marketing codes so that revenue is redirected to the spyware creator rather than the intended recipient.

Spyware programs are sometimes installed as Trojan horses of one sort or another. They differ in that their creators present themselves openly as businesses, for instance by selling advertising space on the pop-ups created by the malware. Most such programs present the user with an end-user license agreement that tries to protect the creator from prosecution under computer contaminant laws. However, spyware EULAs have not yet been upheld in court. Another way that financially motivated malware creators can profit from their infections is to directly use the infected computers to do work for the creator. The infected computers are used as proxies to send out spam messages. A computer left in this state is often known as a zombie computer. The advantage to spammers of using infected computers is they provide anonymity, protecting the spammer from prosecution. Spammers have also used infected PCs to target anti-spam organizations with distributed denial-of-service attacks.

I guess people will try to make a dollar any way that they can today. Some disgruntled employees that have been laid off or fired have been known to implant malware into the system before they leave. I wouldn’t be surprised if some of the developers of malware were disgruntled former employees of a certain company. I think it would be smart for employers to think twice about the fashion that they do lay off their employees.

A common cause of vulnerability of networks is homogeneity or software monoculture. For example, Microsoft Windows or Apple Mac has such a large share of the market that concentrating on
either could enable a cracker to subvert a large number of systems, but any total monoculture is a problem. Instead, introducing in homogeneity which creates diversity, purely for the sake of robustness, could increase short-term costs for training and maintenance. However, having a few diverse nodes would deter total shutdown of the network, and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy would avoid the cost of a total shutdown, would avoid homogeneity as the problem of "all eggs in one basket".

Most systems contain bugs, or loopholes, which may be exploited by malware. A typical example is the buffer-overrun weakness, in which an interface designed to store data, in a small area of memory, allows the caller to supply more data than will fit. This extra data then overwrites the interface’s own executable structure (past the end of the buffer and other data). In this manner, malware can force the system to execute malicious code, by replacing legitimate code with its own payload of instructions (or data values) copied into live memory, outside the buffer area.

Originally, PCs had to be booted from floppy disks, and until recently it was common for this to be the default boot device. This meant that a corrupt floppy disk could subvert the computer during booting, and the same applies to CDs. Although that is now less common, it is still possible to forget that one has changed the default, and rare that a BIOS makes one confirm a boot from removable media.

In some systems, non-administrator users are over-privileged by design, in the sense that they are allowed to modify internal structures of the system. In some environments, users are over-privileged because they have been inappropriately granted administrator or equivalent status. This is primarily a configuration decision, but on Microsoft Windows systems the default configuration is to over-privilege the user. This situation exists due to decisions made by Microsoft to prioritize compatibility with older systems above security configuration in newer systems and because typical
applications were developed without the under-privileged users in mind. As privilege escalation exploits have increased this priority in shifting for the release of Microsoft Windows Vista. As a result, many existing applications that require excess privilege may have compatibility problems with Vista. However, Vista's User Account Control feature attempts to remedy applications not designed for under-privileged users, acting as a crutch to resolve the privileged access problem inherent in legacy applications.

Bottom line is Malware continues to be a problem in the computer world and in the IT industry as a whole. We as consumers and users of technology need to be more aware of Malware and of what actions we can take to better protect ourselves from it. Continuously educating ourselves is the best option that we can do for us and our businesses from the evil that Malware is. I feel that Malware is just the tip of the iceberg along the line of attacks on computers and computer systems. Most likely the attacks on computers will only get worse and more powerful, so the IT industry will be constantly playing catch up to the attacks.
References


