The Five W's of Malicious Software Attacks

By: Christina M. Freeman

What is Malware?

Malicious software or malware is “any software that gives partial to full control of your computer to do whatever the malware creator wants”. The main purpose of malware is to infect and spread to create havoc. (How to Protect Against Malicious Software) Malware can interrupt computer operations, collect sensitive information stored on the system, or gain access to private computer systems. (Malware) It is software specifically written to bring harm to a computer system which unlawfully obtain protected data, delete information or add software not approved by the user. Examples include viruses, worms, Trojan horse, spyware and adware. (Malicious Software)

Malware can be code, scripts, active content or other software and can be disguised as legitimate website interface or official correspondence. For example, a user may receive an e-mail from a bank they do business with. The e-mail can look legitimate with official logos and common phrases from that institution, however, the e-mail can have malware embedded in it and the user can easily execute the malware, thinking they are just doing business with their bank. (Malware) The damage caused by malware can vary from fairly innocuous to very destructive. Malware can claim full control of your machine without you knowing. Most of the time the user must initiate the execution of the malware by clicking on an attachment in an e-mail or going to a website that will install software on the machine. Specific types of malware, adware and spyware, embed themselves in the machine, watching and collecting information on what the user does and then acts on that information. (How to Protect Against Malicious Software)

According to a white paper published by Global Knowledge, four of the top ten security threats where related to malware. Number six in their list is malicious attachments. “E-mail attachments are convenient for distribution of documents, images, and other files. However, they are also common distribution vectors for malicious code”. The seventh in the list is phishing, “Often the e-mails are crafted to look similar to official messages from a known entity, like an e-commerce site, social network site, or a financial service site”. Number nine on the list of the top security threats is Drive-by downloads of malicious code, “malicious code execution is conducted through some form of auto-executing script code”. The final security threat on the list is Pop-ups, “if you end up clicking on their content or sometimes even attempt to close them, you could trigger a malicious code infection”. (Stewart)

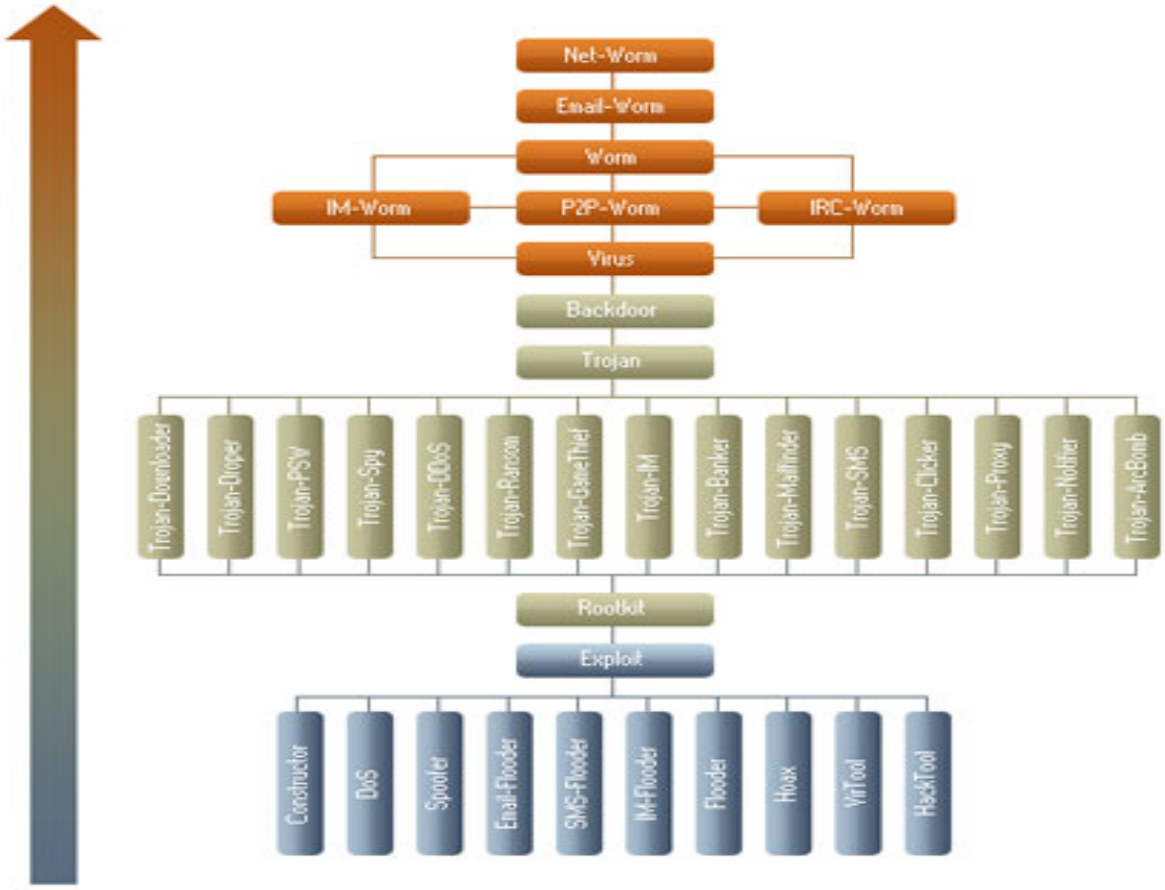
Specific forms of malware include:

- Virus – A replicating computer program designed to infect your computer programs and files, change the way your computer operates or can even stop your computer from working. (Computer Virus information)
- Worm – A self-replicating virus whose sole purpose is to use up system resources. Worms typically do not alter files but it will reside in memory and duplicate itself. Users usually are not aware they have a worm because they will use parts of the operating system that are automatic and are only noticed when the system slows because the replication consumes too many system resources. (Worm)
- Trojan horse – Commonly referred to as Trojans, it is a type of malware that allows the attacker unauthorized, remote access to a user’s computer. Trojans do

not replicate like viruses and worms, but they can be an avenue for viruses being installed on a user's computer. Trojans can allow an attacker to turn a user's computer into a "zombie computer", allowing the attacker to steal sensitive data, installing additional malware, etc. Trojans currently account for the majority of known malware found on the web. (What is a Trojan Virus?)

- Spyware – A software program that is secretly placed on a user's computer through a virus or other type of download. The purpose of Spyware is to gather information about the user or company relay it to advertisers or other interested parties. (Spyware)
- Adware – Free software that a user may download and is supported by advertisements. Commonly, users are not aware of the adware programs, but see it regularly. For example, the toolbar on the web browser or desktop include features that will allow you to search the Web or your hard drive. We use these toolbars to organize shortcuts on your desktop and bookmarks for your favorite web pages. Adware is free to use, but will require you to watch some sort of advertisement when the program is open. Most of the time adware is safe, however sometimes adware can serve as spyware and collect personal data from your hard drive and record patterns of use, like the websites visited or keystrokes. Then the spyware can send the information to another computer. (Adware) Because adware is often referred to as spyware, marketing firms, the general recipients of the adware information, reject their software being referred to as spyware, so more recently, adware is being referred to as "potentially unwanted programs" (PUP). (Spyware)
- Phishing – Sending an e-mail to a user falsely claiming to be a valid company or authorized entity in an attempt to scam the user into providing personal information which will be used to harm the user. (Phishing)

Experts classify malware by the following diagram. Malware that is classified as the least threatening is in the lower part of the diagram and malware that is the most threatening is in the upper part of the diagram. (Malware Classifications)



The most dangerous malware out there combines the above and will create havoc on a user's computer. All malware is dangerous, but some can create more damage than other.

- Overwriting Viruses – Viruses that cause certain types of files to be deleted, sometimes even the entire hard drive contents. The purpose of these viruses is to overwrite the original file with the malicious code, therefore since it has been overwritten, it cannot be recovered.
- Ransomware Trojans – These Trojans infect a user's computer and encrypt the files on the system. Then the attackers demand money from the user in order to obtain the encryption key.
- Password Stealers – Trojans that infect a system and steal login IDs and passwords for the network, e-mail, games and financial sites.
- Keyloggers – A Trojan that monitors and logs the user's keystrokes, and sends the file to a remote attacker.
- Backdoors – A Trojan that provides remote access to a system that has already been compromised. The attacker then has full access to the user's computer and

can take any action as if they were sitting at the computer. Having this access can allow an attacker to install additional malware, steal passwords and gain any additional personal information.

- Rootkits – Allows the attacker to have full access to the system and is able to hide all files and folders it uses.
- Bootkits – Infects flash BIOS, which allows the malware to be loaded on the system at start-up, even before the operating system is loaded. This is possibly the most dangerous because it is almost impossible for the normal user to detect or remove. (Landesman)

When did Malware come into existence?

Malware may be a relatively recent term and new to some people, however, malware is not new at all; we just hear more about it today. It could be because the media is more prevalent in reporting cyber threats and arrests as they relate to malware, but also, given the increased number of attacks, more computer users have been affected by malware in some way. (History of Malicious Programs)

The first computer virus actually came into existence before the personal computer became available to the public. In 1971, a malware virus called Creeper was written and controlled in a lab for the sole purpose to see if it could replicate itself. Then in 1982, the first piece of malware was created outside of the lab. Elk Cloner was created and released on Apple II computers by floppy disk. Finally in 1987, the first destructive virus, Jerusalem, attacked the DOS world and deleted many programs.

Phishing came into existence in the early 90s and the Melissa I Love You malware came about in 1999. Melissa I Love You was a Microsoft word attachment to an e-mail and spread to millions of computers through e-mail messages. The program sent itself via e-mail to everyone in the user's contact list. Finally, the first worm was fairly recent, in 2004. The worm, Sasser traveled across the Internet affecting millions of computers without the use of e-mail as the mechanism for infection. (Malware Virus: When did it Begin?)

Who Creates Malware, where does it come from?

Malware is created by many different types of people, groups and organizations for many purposes. Historically, malware, specifically viruses and Trojans, were created by students, often after they had just learned a new programming language and curiously tried to create a new program. Sometimes that creation was successful and sometimes not, but with the number of "how-to" sites available on the Internet, anyone can learn very easily how to write a simple virus. (Who Creates Malware and Why?) At first, people may create malware just to see if they can. Starting off with simple programs that can be fairly innocuous, malware creators gain confidence and if the program works, their self-esteem is increased and they develop a feeling of power and accomplishment. After the first rush, they may want to determine how a newly created program will react in the networking world, they release the program and if it has the desired affect it just fuels the need to create more. Once people have gained the experience and mastered the programming of simple viruses, they can be very dangerous and they create an even bigger and

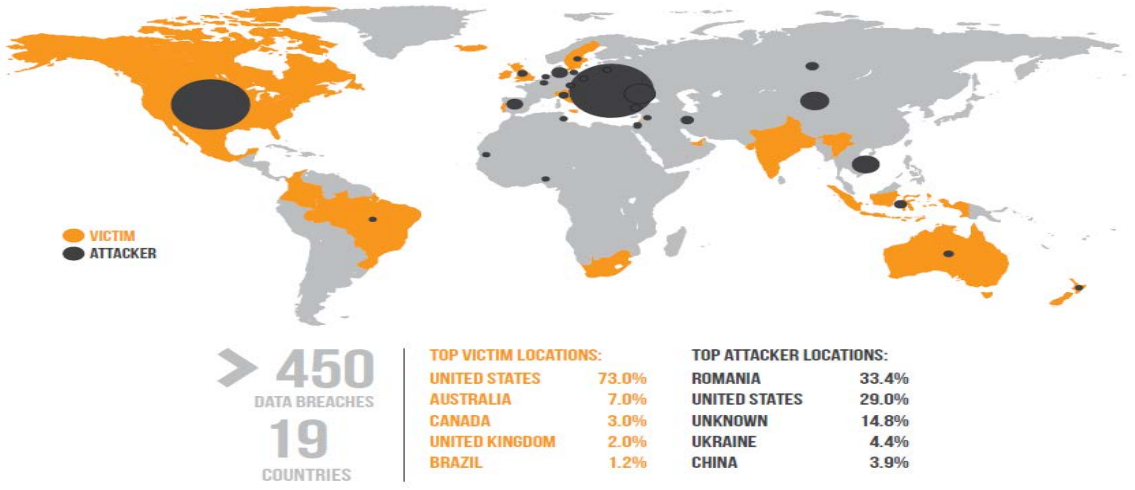
better program and can eventually create extremely dangerous malware with the purpose of causing harm. Malware creators do not just decide one day to cause massive harm to an organization or individual, it is a growing skill that is fueled by pride.

Given this, malware has evolved in the last decade. It is no longer simplistic scripts created by students, spammers and identity thieves. Groups of highly trained programmers have replaced the simple crooks and students. These groups target political organizations, organized crime and government agencies. What began as mischief by curious students has evolved into criminal activity by organized groups and even governments. (Ledin)

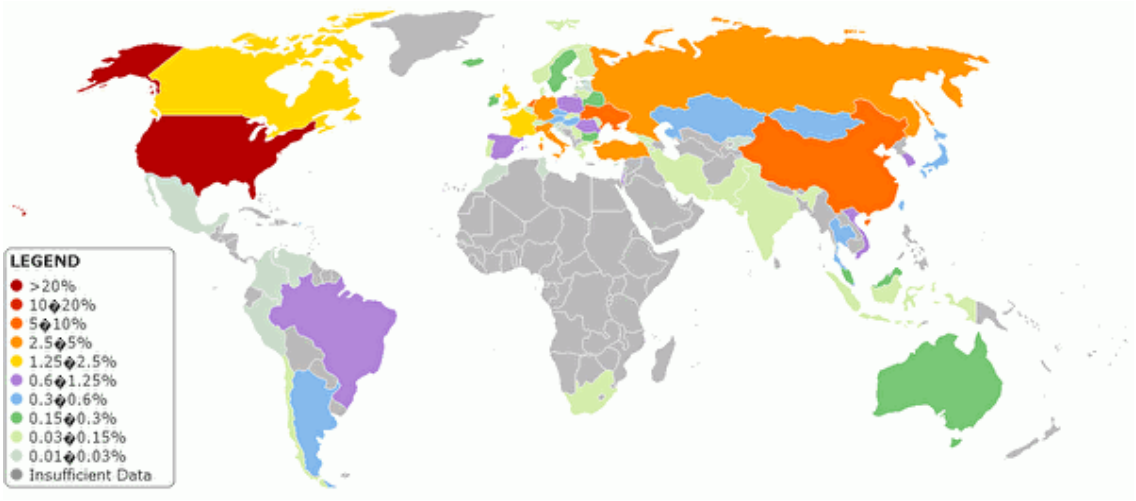
Today there are three types of offenders that create malware. “There are organized criminal gangs who are out to steal your money. There are hacktivists, who are trying to draw attention to a political or social cause. And there are governments.” The government will use malware both inside and outside their own country. Law enforcement may use spyware to gather information on criminals for investigation purposes and some countries may use spyware in order to monitor their citizens. Governments spy on other nations by targeting important organizations, usually by taking advantage of external weaknesses in the network. (F-Secure Research Labs)

An article published in eWeek highlights security threats facing all enterprises. Number three on their list is political hactivism, which is politically motivated hacking. Expert’s state political hactivism is on the rise because there are many easy targets available. “Some, such as social engineering threats that fool employees into downloading viruses, have been around for years and aren't fading away. But an increasing number of companies are falling victim to hacktivism, a phenomenon most CIOs have only started to think about counteracting. But the biggest problem is simple stupidity.” (Preimesberger)

In 2012, attacks originated in 29 different countries. Romania is well known for criminal activity and is the location that has the largest percentage of originating attacks with more than 33 percent of all attacks. The United States follows with 29 percent of originating attacks. This same report identifies the United States as the location with the most victims at 73 percent of all victims. (2013 Global Security Report)



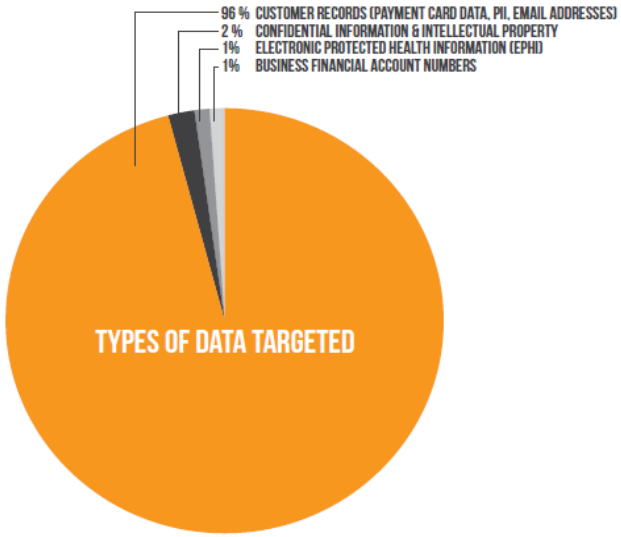
As recent as October 2013, statistics show the United States is number one location where most malicious code being hosted. (Malware Statistics)



What are they seeking, from whom and why?

Most people who create malware are attempting to gather or steal private and personal information about someone or something in an effort to cause harm to someone or some organization. These people, or attackers, are creating programs that attack another user's computer to obtain personal, confidential or sensitive data. Attackers can attempt to access information for many reasons, something as simple as petty theft could be a motive. They may want network access without paying for it so they may steal a user's login and password using a Trojan. An attacker could steal a user's information in order to resell for profit.

Statistics tell us that in 2011 and 2012 the primary data type targeted was cardholder data at 96 percent of all data targeted. Cardholder data is bought and sold in the underground marketplace for fraudulent transactions. (2013 Global Security Report)



A group of attackers, often referred to as hackers, purposely seeks and exploits weaknesses in computer systems and networks. Hackers intentionally create malware programs to steal information such as codes to bank accounts. They can create viruses and Trojans that illegally use resources of the infected computer to obtain a monetary benefit or attack other computers via the infected one. One of the most common attacks over the Internet is for hackers to use Trojans to steal credit card and bank account information. Hackers will use malware to provide an image or identical web-page window to a user via e-mail that duplicates a bank or credit card company, requesting login and password information. (Who Creates Malware and Why?)

Malware doesn't just spread via e-mail. With the popularity of social networking, malware can spread even faster through interconnected networks. The infection of one person on a social networking site can impact all the people they are connected to. Attackers are aware and are using this avenue to spread dangerous malware. (Sood)

In another form of attack, someone will set up networks to be used as a dedicated computer designed to e-mail spam in mass. By sending these spam e-mails from infected computers attackers become anonymous and the spam travels quickly from multiple infected computers. This makes it very difficult to "black list" or trace back to the real people responsible. Thus the person doing the attacking never gets caught.

In addition to stealing personal user information, attackers can switch their focus to stealing a company's proprietary information. Any company that may have possession of valuable information, such as billing companies or banks, are susceptible to attack because attackers are trying to access financial information, illegally transfer funds or possibly obtain proprietary technical documentation. (Who Creates Malware and Why?)

What do we do?

The first step to combatting malware is education. "We cannot protect ourselves from what we do not know. We must not remain stuck in a weak, purely reactive, defensive mode." We need to understand and know what malware looks like so we can anticipate and be prepared for what may come our way. According to some experts, "Detecting and arresting malware and its launchers won't be easy unless we ramp up on all fronts, especially education". (Ledin)

There are steps a user can take to avoid malware and lessen the effect it can have on the user's network.

1. Prevent malware with smart online behavior. Avoid downloading and installing software or any program from a person or site that is not familiar, including websites, e-mail, physical media, pop-up windows, other software and file-sharing services. (Phelps)
2. Install and employ some type of malware detector to identify malware on a computer. The best approach is to use a signature-based malware detector, which uses a list of malware signatures and if part of a program matches a signature in the database, the program is flagged as malware. (Preda)

3. Ensure software is up-to-date. An outdated operating system, browser, anti-virus and anti-malware solution and spam filter can be deadly to a computer. (Phelps)
4. Install and maintain pop-up blockers and firewalls.
5. Do not use file-sharing or peer-to-peer services like Kazaa, Morpheus, iMesh, etc. for music, games, movies or software.
6. Use Firefox browser with the pop-up blocking feature turned on, it is much faster and safer for Internet use. (De Argaez)

In addition to steps a user can take, an organization that is infected with malware needs to follow a predetermined incident response plan. This plan should include:

1. Preparation – Establish policies, identify and assign responsibilities, encourage relationships with key players for communication, develop kits with all necessary supplies and call lists, develop the Incident Response Team and practice.
2. Identification – Identifying what is causing the incident by performing malware analysis, which requires an understanding of how the malware functions so that defenses can be built to protect systems and networks from that malware.
3. Containment – Remove infected systems from the network without turning off the power.
4. Eradication – Clean-up process begins by rebuilding systems and performing vulnerability analysis.
5. Recovery – Previously infected systems will be placed back into production and monitored for re-infection.
6. Lesson Learned – Complete documentation and present any findings or issues to management.

Following a formal plan can benefit an organization in recovering from a malware incident and lessen the impact. It can also help ensure the incident will not happen again. (Distler)

Summary

Contracting malware is not a question of if it will happen, but it is a question of when it will happen. We must know what we are looking for and be aware of what dangers are out there in order to protect ourselves from the ever evolving world of malware. We can educate ourselves and ensure our systems are protected with malware fighting software, however, attackers are continuously testing the limits of malware detection software in an attempt to defeat discovery. It is a continuously evolving game of cat and mouse, as security professionals develop programs to combat malware and close off points of access, attackers develop more sophisticated attacks. As new malware is developed and new exploits are executed, we must continue to develop new ways to combat it and strengthen our resolve to fight against malware and the creators of malicious software.

Bibliography

How to Protect Against Malicious Software, n.d. *ucla.edu*, Retrieved on September 24, 2013 from http://www.seas.ucla.edu/security/malware.html

Malware, n.d. *Wikipedia.org*, Retrieved on September 24, 2013 from http://en.wikipedia.org/wiki/Malware

Malicious Software, n.d. *Techpedia.com*, Retrieved on September 24, 2013 from http://www.techopedia.com/definition/4015/malicious-software-malware

Stewart, James. (2011). Ten Current Security Threats for Individuals. *Global Knowledge*, Retrieved on September 24, 2013 from http://www.redteamusa.com/PDF/10%20SecurityThreats2013.pdf

Computer Virus Information, n.d. *webroot.com*, Retrieved on September 24, 2013 from http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses

Worm, n.d. *Searchsecurity.techtarget.com*, Retrieved on September 24, 2013 from http://searchsecurity.techtarget.com/definition/worm

What is a Trojan Virus?, n.d. *pctools.com*, Retrieved on September 24, 2013 from http://www.pctools.com/security-news/what-is-a-trojan-virus/

Spyware, n.d. *Searchsecurity.techtarget.com*, Retrieved on September 24, 2013 from http://searchsecurity.techtarget.com/definition/spyware

Adware, n.d. *TechTerms.com*, Retrieved on September 24, 2013 from http://www.techterms.com/definition/adware

Phishing, n.d. *Webopedia.* Retrieved on September 24, 2013 from http://www.webopedia.com/TERM/P/phishing.html

Malware Classifications, n.d. *usa.kapersky.com*, Retrieved on September 24, 2013 from http://usa.kaspersky.com/internet-security-center/threats/malware-classifications

Landesman, Mary. Most Damaging Malware, n.d. *About.com*, Retrieved on November 23, 2013 from http://antivirus.about.com/od/virusdescriptions/tp/worstvirus.htm

History of Malicious Programs, n.d. *SecureList*, Retrieved on November 19, 2013 from http://www.securelist.com/en/threats/detect?chapter=77

Malware Viruses: When did it Begin?, n.d. *hubpages.com*, Retrieved on November 15, 2013 from http://perrya.hubpages.com/hub/Malware-Viruses-When-Did-It-Begin

*Sood, Aditya and Enbody, Richard. (2011). Chain Exploitation – Social Networks Malware. *ISACA Journal, 1*, 1-6

Who Creates Malware and Why?, n.d. *SecureList*, Retrieved on September 24, 2013 from http://www.securelist.com/en/threats/detect?chapter=72

*Ledin, Jr. George. (2011 February). Inside Risks, The Growing Harm of Not Teaching Malware. *Communications of the ACM. 54 (2),* 32-34

F-Secure Research Labs. (2013, March 27). Gov't malware: Why and how it's used, and is it cyber-war? *Digital News Asia*, Retrieved on September 24, 2013 from http://www.digitalnewsasia.com/insights/govt-malware-why-and-how-its-used-and-is-it-cyberwar%3F

Preimesberger, Chris. (2012, June 11). Security: Security Threats Facing All Enterprises: Top 10 Issues That Need Attention, *eWeek*, Retrieved on September 24, 2013 from http://www.eweek.com/c/a/Security/Security-Threats-Facing-All-Enterprises-Top-10-Issues-That-Need-Attention-226329/

2013 Global Security Report. *Trustwave*, Retrieved on November 24, 2013 from http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Malware Statistics. (October 2013) *Trustwave*, Retrieved on November 24, 2013 from https://www.trustwave.com/support/labs/malware-statistics.asp

Phelps, Justin. (2010, November 16). How to Avoid Malware. *PC World*, Retrieved on November 22, 2013 from http://www.pcworld.com/article/210891/malware.html

*Preda, Mila; Christodorescu, Mihai; Jha, Somesh and Debray, Saumya. (2007 January). A Semantics-Based Approach to Malware Detection. *Proceedings of the 2007 POPL Conference, 42(1),* 377-388

De Argaez, Enrique, n.d. *Internet Coaching Library*, Retrieved on November 22, 2013 from http://www.internetworldstats.com/articles/art053.htm

*Distler, Dennis. (2007, December 14). Malware Analysis: An Introduction. *SANS Institute 2007*, 1-66