Cis assigntment #2

Malware and its Effects Malware is a make up term that refers to malicious software. These are software that are created by individuals and designed to attack computer systems for the creators benefit (Szor, 2005). Malware has been in existence for almost as long as computers have and have been one of the greatest enemies of software developers as they are designed to find points of weakness in order to gain entry into a host computer and thus serve as a means of revealing the imperfections that exist within the various programs that have been designed by computer companies (Parikka, 2007). There are different types of Malware present in the market and they are used by their attackers to perform different activities. Some of the malware present in the wolrd of computers to day include:

Viruses – These can be said to be one of the oldest malwares that have been present in the world of computers (Brodkin, 2013). Viruses are programs that have been designed to replicate themselves so as to spread from computer to computer causing havoc wherever they infect. They affect the computers they infect in a number of ways including changing the behavior of the computer, erasing data and stealing information that may be stored on the computer.

Viruses embed themselves onto other program files in the computer and are activated when the user attempts to open the infected file (Brodkin, 2013). They can be spread through a downloaded file that contains the virus which is transferred from one computer to another.

Trojans – These malware is named after the Greek mythology of the Trojan horse due to their innocent appearance to the user so as to avoid suspicion of the actual danger that they yield (Brodkin, 2013). Once they are activated however, they are able to achieve a number of attackers on the Personal

Computer such as causing continuous irritations such as unrelated pop up windows to more harmful acts such as the deletion of programs and the creation of backdoors into the computers files.

The fact that Trojans present themselves as harmless programs make them harder to detect and a user may be more vulnerable to this form of malware. Remote Access Trojans (RATs) are those that can create a backdoor system that allow the hacker access to one's computer and is even able to send commands via root access capabilities (Brodkin, 2013).

Backdoors – These are programs that are designed to allow the creator undetected access to a computer system once they have been installed. Backdoors can be used by hackers to steal information from a server undetected and are similar to Remote Access Trojans in their functionality (Brodkin, 2013). The main difference between RATs and other backdoors is that RATs have a user interface available to the hacker.

Information Stealers – These are malware designed to steal important information from a computer system undetected (Brodkin, 2013). The information may include things like passwords, restricted data and other private details meant for the computer owner only. Examples of information stealers include desktop recorders, memory scrapers and keyloggers.

Ransomware – This can be considered to be one of the most destructive malware available as they are designed to hold the computer owner hostage by taking control of their PC and threatening to delete important files or even the whole machine unless financial compensation is paid to the creator in exchange for having the " problem solved" (Brodkin, 2013).

Botnets – This malware does not exactly directly affect the computer and turns a user's desktop into their own task dog and a hacker is able to use to

perform various functions that may bring about monetary gain (Brodkin, 2013).

The main prevention of these malware consists of the various antivirus programs that are available in the market today (Parikka, 2007). However, developers of these malware continue to discover new ways of avoiding them and the best strategy to prevent infection would be to avoid downloading any suspicious documents onto your computer as well as avoid entry into suspect sites as these are the main gateways that are used by these malware.

References

Brodkin, J. (2013). Viruses, Trojans, and worms, oh my: The basics on malware.

ARS Technica.

Retrieved on February 8, 2013 from:

http://arstechnica. com/security/2013/02/viruses-trojans-and-worms-oh-my-the-basics-on-malware.

Parikka, J. (2007). Digital Contagions. A Media Archaeology of Computer Viruses,

Peter Lang. New York. Digital Formations-series

Szor, P. (2005). The Art of Computer Virus Research and Defense. Boston: Addison-

Wesley.