Example of research paper on trojan horses

Law, Security

Introduction to the problem

The last decade has seen an increased improvement in the technology sector. At every instance, new technological advances are emerging. As technology brings in new, faster and more efficient processes, the security threats also increase, as well. For example, years back, computers were just stand-alone systems not interconnected in any way. With time, there was a need to create systems that would be interconnected through local area connection for ease of sharing information and resources. Further to the technological developments, the world became a global village whereby millions of computers are interconnected across the globe. Interestingly, as the computers shifted from, stand-alone systems to multi networked systems, the security threats emerged with each development (Zittrain, 2008).

The main category of security threats that continue to slow down networks is the malicious ware that includes “ worms, viruses, Trojans, adware and spyware” (Zittrain, 2008). Organizations are made to take up the challenge of doing risk analysis, preventing attacks, dealing with attacks and recovering from the attacks. One of the biggest malware threats in computer technology is the Trojan horse, a malware that causes the system to get prone unauthorized access. The malware does this by posing as a genuine file or a legitimate program, thus tricking the user of a system into believing that it is indeed a helpful program (Spears & Barki 2010).

The following paper describes the issue of Trojan horse virus in the technology context. It gives the background of the study concerning this malicious ware virus, and the statement of the problem. It also describes the

issue of viruses and how recovery from an attack is done. Finally, the paper explains the recommendations regarding the issue of Trojan horses and the conclusion of the research paper.

Background of the study

According to Gozzi, (2000, p. 2), “ a Trojan horse is a malware that masquerades as a legitimate file or helpful program with an aim of allowing a hacker unlawful entry into a computer system.” Once it has collected your info, it is sent to a hacker’s database. The basic difference between a Trojan horse and a virus is that, viruses do replicate, unlike the Trojan horse malware. Also, it does not make copies of itself like the worms do when they attack a system. For a Trojan horse to attack a system, it just aims at gaining remote access through unauthorized access to the system while collecting confidential and private data from the computer. Trojans are of different types. The most common Trojan horse malware are the remote access Trojans, key logging Trojans, backdoor Trojans and IRC Trojans (Backdoors and Trojan Horses, 2002). In most cases, the attacks are done by multiple Trojan horse malware, for example, a computer may be attacked by both a backdoor and a remote access Trojan. Botnets refer to a group of infected computers usually attacked by a combination of three types of Trojans namely the IRCbots, backdoors and remote access Trojans (John et al., 2010). Trojans are used by most attackers as the best method of gaining unauthorized access to confidential information due to their difference from other malware such as viruses. Viruses can easily be cleaned by an antivirus thus making their attack less efficient. However, a Trojan horse cannot be cleaned by the regular anti-virus program; rather the whole infected file

needs to be deleted in order to eliminate the security threat.

According to Gozzi, (2000), the name Trojan horse originated from the Greek Methodology detailing how the Greeks managed to conquer the city of Troy. This was after creating a big wooden Trojan horse that hid a number of Greek warriors. The warriors waited till dark because the enemies could not have suspected that there were warriors in it, and they attacked and destroyed the city, forming the end of the war. The first Trojan (called the Spy Sherrif) horse was detected in the 1980s, and it was noted that the most destructive versions of Trojan horses were able to infect Windows32 files. Over the years, there has been increased emergence of new versions of Trojan horses.

Statement of the problem

The first Trojan horse malware did not damage any file on the computer, rather, it just appeared in the form of pop up warnings that would warn the user of an impending threat (Hughes & DeLone, 2007). The Trojan would then ask the user to click on it so that he or she can install the software needed to prevent such an attack. The users were not quite familiar with this security threat and, therefore, most of them were duped into clicking on the warning. This way, hackers were able to attack, and the Trojan horse was able to spread worldwide, the reason as to why the malware is still so popular today. The main problem with the Trojan horse is the fact that they come as harmless files that users easily may mistake for legitimate files (David, 2011). This is how they were created, and this is their main mechanism of attack to unsuspecting users. The hackers usually allow the Trojan to disguise itself as they plan the best way to enter the system from

afar. The spread of the Trojan horse malware was further fuelled by the then Bulletin Board System, a computer software that allowed the 1980s users to access systems through phone lines. This lead to a further spread of the Trojan horses through files shared, information downloaded and files uploaded in the network. Trojan horses are usually able to clog the memory of an infected computer system, specifically targeting the memory of the operating system (David, 2011).

While, in memory of the operating system, the Trojan causes the production of pop ups that seem to warn the user of software programs that should be installed in the system. Currently, the Trojans are able to violate the user's privacy, yet they are still increasingly becoming common in all computer networks. Trojan horses are on the rise, and in fact they contribute to about 83% of the total malicious ware detected across the globe (Latamore, 2010). Furthermore, the Trojans spread fast across the internet because they are given help by worms by travelling across networks with them. When it comes to botnet, studies show that about 15% of the total computers are included in a botnet, thus showing the extent to which Trojans have affected networks (Latamore, 2010).

Trojan horse and Recovery

It is unfortunate that many people are victims of Trojan horse attacks. Fortunately, there are several measures that an individual or organization can take to recover from a successful Trojan attack (Hughes & DeLone, 2007). For example, if working in an organization as an employee and one finds out that his or her computer has been compromised, the best thing to do is to call IT support department as soon as possible. The IT support

personnel should be notified immediately, so as, to ensure that not much hacking will have been done by the time they start the recovery plan. It is vital to note the IT support instructions that one is given and to follow all the instructions as stated.

It is also extremely crucial to disconnect the computer from the internet once the Trojan horse attack is suspected (Schiefelbine, 2003). This is because the hacker usually accesses the information remotely when one is connected to the internet. By disconnecting the system from the World Wide Web, chances are that the attacker will be cut off from the unauthorized access. This can easily be done by clicking the ‘ disable’ button on the internet connection, or physically unplugging any internet or phone cables on the network.

The next recovery measure would be to back up all the pertinent files from the computer to an external device like a CD because some files may still not be infected (Schiefelbine, 2003). After backing up the documents, it is crucial to scan the computer for all malicious ware, and the scanning must include the operating system. The best way to scan the computer is to use a live CD instead of scanning using the installed anti-virus program since it may be compromised (Won et al., 2009). The next recovery step would be to re-install the operating system and the other programs if the scanning fails. This is the surest way of eliminating the malware because it includes the formatting of the machine. After carrying out the formatting and re-installation of the operating system and the other programs, the other step would be to restore the backed up files, ensuring that they are cleaned up before restoring them (Da-Yu et al., 2011). Before connecting the machine

back to the internet, it is vital to ensure that all protecting is updated to prevent further attacks. There are recommended practices that can then assist in the protection of the system from future attacks.

Recommendations

1. Avoid downloads from unknown sites or unknown people (Grimes, 2008). This is because Trojans are enter systems through downloads.
2. It is advisable to vet whether a file is genuine before opening it even when it comes from a friend. It is crucial to check whether there is a reason good enough for a friend to send a file that one has not asked.
3. Check the file extensions to avoid executable files. This is more so in windows whereby the file extension is often hidden, yet they could be executable Trojans (Latamore, 2010).
4. It is vital to be cautious about typing of commands or following links that have been suggested in the network because that might be a targeting mechanism for Trojan attacks.
5. Change of passwords should be a regular task to keep off remote hackers who could have gained access to the authentications.
6. Keep the software and anti-virus programs up to date
7. Install a firewall that is enabled to keep off malicious ware.

Conclusion

Technological advancements have led to more security threats in computers and computer networks. Malware programs are continuously being designed assist hackers in gaining illegal entry into computer networks. The worst attacks in the world have been caused by Trojan horses, a malware that

poses as authentic files, thus misleading the user into following its instructions. The Trojan horse name is a metaphor signifying a wooden horse created by the Greeks, aimed at defeating the Trojan army. This malware causes losses to individuals and organizations because of the information getting compromised. Recovery can be achieved through some given steps while prevention may be achieved through following the given recommendations. As long as technology advances, Trojans will continue to exist, but, by taking prevention and recovery measures, users can deal will the security threat.

Backdoors and Trojan Horses. By the Internet Security Systems' X-Force. (2002). Information Security Technical Report, 631-57.

David, E. (2011). Trojans: Focus on Trojans – holding data to ransom. Network Security, 20064-7. doi: 10. 1016/S1353-4858(06)70397-X

Da-Yu, K., Shiuh-Jeng, W., & Frank Fu-Yuan, H. (2011). SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases. Computer Law And Security Review: The International Journal Of Technology And Practice, 2652-60

Gozzi Jr., R. (2000). THE TROJAN HORSE METAPHOR. ETC: A Review Of General Semantics, 57(1), 80.

Grimes, R. A. (2008). Protecting the Internet Without Wrecking It: Fixing Web insecurity requires more than a caring community. Boston Review, 33(2), 19-20.

Hughes, L. A., & DeLone, G. J. (2007). Viruses, Worms, and Trojan Horses:

Serious Crimes, Nuisance, or Both?. Social Science Computer Review, 25(1), 78-98.

John, C., Sylvain, L., & Scott, K. (2010). Compromise through USB-based Hardware Trojan Horse device. Future Generation Computer Systems, 27555-563.

Latamore, B. (2010). Cyber Threat Growing More Focused and More Sophisticated. Seybold Report: Analyzing Publishing Technologies, 10(1), 11-14.

Spears, J. L., & Barki, H. (2010). USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT. MIS Quarterly, 34(3), 503-A5.

Schiefelbine, E. D. (2003). Stopping a Trojan Horse: Challenging Pop-up Advertisements and Embedded Software Schemes on the Internet Through Unfair Competition Laws. Santa Clara Computer And High Technology Law Journal, 19499.

Won, K., Ok-Ran, J., Chulyun, K., & Jungmin, S. (2009). The dark side of the Internet: Attacks, costs and responses. Information Systems, 36(Special Issue on WISE 2009 - Web Information Systems Engineering), 675-705

Zittrain, J. (2008). Protecting the Internet Without Wrecking It: How to meet the security threat. Boston Review, 33(2), 7-13.