Computer threats and resolution

Kevoy Bailey

Saint Leo University

Balbir Bal

Computer threats, security measures and resolutions.

The world of technology that we have all came to know and love today has come from a long way, from a time where we had to do everything manually and take a longer time period to come up with a result to now where all the information and accessibility to information right at our finger tips. In this paper many topics will be covered in regards external threats to the computer system that is software that are malicious in nature which is very harmful to the computer system on a variety of levels depending on the nature of what the software was created to do. Late ninety centuries into the two thousand there has been more advancement into technology that has led to numerous inventions of e-commerce and personal information storage onto their handheld devices that stores. These inventions have created an avenue for criminal elements to take advantage of gathering user's personal information stored electronically but we will discuss further how we can prevent them for happening if our computer system is ever breached. Within this paper there will be a vast amount of discussion on various harmful software programs and the ways how we can prevent exploitation of our personal information.

Let's first look at Spyware. Spyware firstly are software packages that secretly gather information about a user while they surf the internet. These software programs are intelligently designed that they user has no knowledge that their information is being stolen until later on when their debit or credit card has been used to conduct transactions that they user have no knowledge about or in some cases the user's identity if stolen and they either have to pay a lot of money to get their identity back which in most cases are a extensive process to regain their credibility. Spyware can be prevented through the use of antivirus or antispyware software that acts as a barrier to those external entities that wishes to gain individuals personal information. Adware are very similar in nature to spyware software the only difference is that adware collects user's personal information through advertisement that has embedded links that activates when

the user clicks onto the advertising link which then gives external entities access to the user's information. Adware can be prevented by using or installing an adblocker software feature that would intercept advertisement sent by legitimate and non-legitimate sources.

Other means that hackers use to gain web users personal information is by phishing. Phishing involve the process of sending fraudulent emails to web users that seem as if they might come from a legitimate source. There are various types of phishing, some of these may include:

1. Normal Phishing: normal phishing is sometimes referring to as deceptive phishing which normally involves scammers sending out emails in large proportions in the attempt to lure anyone that falls for their tricks. The goal behind the scammers sending these emails are that they scare the user into thinking that an urgent route of action is needed and then they take advantage of the situation. Ways that user can use to spot normal phishing activities by looking for typos, generic greetings and the misspelling of words or letter in the uniform resource's locator. For example, spelling PayPal with two Ls instead of one and so on.
2. Spear Phishing: spear phishing is a specific fraudulent procedure where scammers targets a specific individual or organization. It involves the careful alteration of the spear phishers emails that tend to use more tailored information specifically to have the user think that they have connections with the sender. This is often done through the impersonation of company's employee or an independent contractor in obtaining sensitive information or bank details. Because spear phishing scammers uses social media as their platform to carry out their crime organization must discourage that their employees should not publishing sensitive personal or organizational information on social media.

3. Clone phishing: this the replication of legitimate emails sent to the user email address but then after they receive a similar email that is identical, but the only difference is that the second email that was sent to the user email contains malicious programs. The best way how to protect one's own information is realizing firstly that reputable companies rarely send two emails about the same issue and if the first emailed that was received seem legit then the user should reach out to the company's help desk to query the matter at hand and get to the bottom of the inquiry.

Pharming on the other hand, is a where user is taken to or directed to a fraudulent website with the intention of stealing their personal information without the user's knowledge that any malicious activities are going on. Hackers must use three preliminary steps, these are:

I. A batch script to writes the malicious IP and domain names onto the host files.

II. A joiner that connects the batch file onto another file.

III. A code Obfuscator to help the executable escape detection from anti-virus software.

User can protect themselves from the hackers using pharming programs by installing an antivirus software program packages that prevents the alteration of user files, keep computer updated, check URL, check certification, use a trusted, legitimate internet service provider, check the 'http' address and look for padlock.

A hacking technique that has being use my many hackers to gain information is by using keystroke loggers. These keystroke loggers monitor and record keystrokes via hardware and software devices which is used also my companies to track their employees' activities on the internet. But in the hands of hackers they used this software for malicious purposes, keystroke loggers can be prevented via using specified antivirus and antispyware programs.

Hackers uses various technique to intercept network connection information that is transferred on the clouds between either people to people, people to business or business to business through sniffing and spoofing. Sniffing is the capturing and recording network traffic used by a hacker to intercept information and there are tow main types. Active sniffing which is controlled by a switch that acts as a connection from point to point network devices. This switch control and regulates the flow of data between its ports by actively keeping up with the MAC address of the ports outlined, to capture the traffic between target sniffers actively intercept data traffic from Local area networks which enables sniffing of the data traffic but there are various ways that sniffing activities can be carried out. The second type sniffing is passive sniffing which is done through a hub, the data traffic that passes through the non-switched network are visible by all machines on that segment. Sniffers conduct their operation at a data link layer of that network and data that is sent across the local area network is then sent to each and every machine of that local area network while the sniffers wait patiently for data to be sent in order for them the intercept and capture it.

This research had also led to the recognition of threats that could possible cripple a user's computer system and in some cases require professional help to remove such software programs. One of these specific programs is worms and viruses. Worms and viruses are program codes that are triggered at a specific time and event which attaches themselves to files which can cause severe damage to the system as they are replicated onto various number of other files within the system. The one major difference between a worn and a virus is that, viruses need a host to thrive and survive but on the other hand worms can survive independently without being attached to the host programs. Worms and viruses can also be

preventing through the installation and updating of a task specific antivirus programs consistently scans the system for any abnormalities within the system and solve them.

Another popular threat is logic bombs. These are apart of a group called trojan program which hides malicious programs within legitimate ones such as worms or viruses that is then triggered when a specific condition and time are satisfied to initiate action. The last threat that I will look at is denial of service attacks. This involves the flooding of one's website with hundred of thousand of request with the intentions of overwhelming the system and ultimately causing it to desist from carrying out the tasks that they were created to do. There are two main type of denial of service attacks, Botnet and Telephone denial of service (TDos). Botnets are networks that contains private computer systems which are infected by malicious programs that are controlled as a group without the owner's knowledge, whereas, telephone denial of service uses automated calls that ties up the phone system of the targeted user and create a barrier that prevents incoming and outgoing calls to go through.

So, to conclude there are many other safeguards besides the ones already suggested to protect a computer system on an organizational level. The most important factor that a company should take into account that their employees must be properly trained so that they would be better equipped in handing specific discrepancies of such nature as dealing with hackers, protection of the systems from malwares and follow the guidelines stipulated by organization to extensively secure all data used for business and nonbusiness purposes. The company should seek to conduct its operations on a on an Intranet rather than in the Internet since Intranets are more secured and allows only authorized personnel to have access to confidential information. The use of Virtual private networks is also a very strong mechanism that could help to keep hackers out of a company's system by using encryption

along with other security programs to give access to authorized users. It provides a secure channel that allows for the transmission data between remote users and the company's network. The virtual private network have to key components that helps to protect the system from hackers or unauthorized users, firstly through a firewall that requires the user to provide the required authentication to gain access to the network and secondly, encryption is also very relevant as data that is sent from one computer has to decrypt the data sent which would make it harder for the hackers to make sense of the information if they happen to intercept it. Call Back Modems are also good at providing information on whether the user trying access the system is valid, intrusion detection system is also a secured measure that protects the system from both external and internal access by identifying attack signature, traces patterns and sends an alarm back to the network administrator to prevent denial of service.

Work Cited

1. Beal, V. (n.d.). VPN – virtual private network. Retrieved from https://www.webopedia.com/TERM/V/VPN.html.
2. Sagala, A., Pardosi, R., Lumbantobing, A., & Siagian, P. (2016). Industrial control system security-malware botnet detection. *2016 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*. doi: 10.1109/ic3ina.2016.7863036.
3. Bidgoli, H (2019). MIS9 Management of Information Systems. 9e.
4. Sagala, A., Pardosi, R., Lumbantobing, A., & Siagian, P. (2016). Industrial control system security-malware botnet detection. *2016 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*. doi: 10.1109/ic3ina.2016.7863036.
5. Calderon, P., Hasegawa, H., Yamaguchi, Y., & Shimada, H. (2018). Malware Detection based on HTTPS Characteristic via Machine Learning. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. doi: 10.5220/0006654604100417.