Detection and Prevention of System against Cyber Attacks

Prof. Gargi Shah
Professor
Department of Computer Engineering
Vadodara Institute of Engineering & Research, Waghodiya, Vadodara, India

Abstract— It is important to take security measures to protect your computer information, reduce identify theft, and prevent from malicious cyber-attacks. With cyber-attacks on the continuous rise, people need to understand and learn ways to prevent from these attacks. Cyber-attack is an important factor to be considered if one is to be able to protect oneself from malicious attacks. Without proper security measures, most computer technology would hinder home users more than such technologies would help. Knowledge of how cyber-attacks operate and protective steps that can be taken to reduce chances of its occurrence are key to increasing these security measures. The purpose of this paper is to inform home users on the importance of identifying and taking preventive steps to avoid cyber-attacks. Throughout this paper, many aspects of cyber-attacks will be discuss: what a cyber-attack is, the affects of cyber-attack for home users, different types of cyber-attacks, methodology to prevent such attacks; home users can take to fortify security of their computer.

Key words: Cyber-Attacks, Home User, Prevention, Security, Intruder, Hacking, Denial of Service

I. INTRODUCTION

A Cyber Attack is an attack initiated from a computer against another computer or a website, with a view to compromising the integrity, confidentiality or availability of target and the information stored in it. Cyber Attacks, in a way, can be broadly considered to be a part of Cyber Crime. An attack to commit a Cyber Crime can be called as a Cyber Attack!

It has three distinct factors: (1) Attack or an illegal attempt to (2) gain something from and (3) computer system. A system is a collection of units that work collectively towards a common goal. Thus, whether it is a single or a collection of computers – offline or online (websites/intranets), it is a system as they work to facilitate something or the other. Even a single computer has many components that work together for a common goal and hence is called a computer system.

The main factor is illegal access to such a system. The second factor is target system. The final factor is gains to the attacker. It should be noted that illegal access must have a motive to compromise the target system, in a way that the attacker gains something, such as information stored in the system, or the total control of the system.

II. TYPES OF CYBER ATTACKS

There are many methods of Cyber Attacks from malware injection to phishing to social engineering to the internal stealing of data. Other advanced but common forms are DDoS Attacks, Brute Force attacks, hacking, holding a computer system (or a website) for ransom using direct hack or Ransom ware. Some of them have been listed below:

1) Gaining, or attempting to gain, unauthorized access to a computer system or its data.
2) Disruption or denial of service attacks (DDoS)
3) Hacking a website or mal-facing the site
4) Virus or malware installation
5) Unauthorized use of a computer for processing of data
6) Inappropriate use of computers or applications by employees of a company, in a way that it harms the company.

Fig. 1 below shows the increasing different types of cyber-attacks.

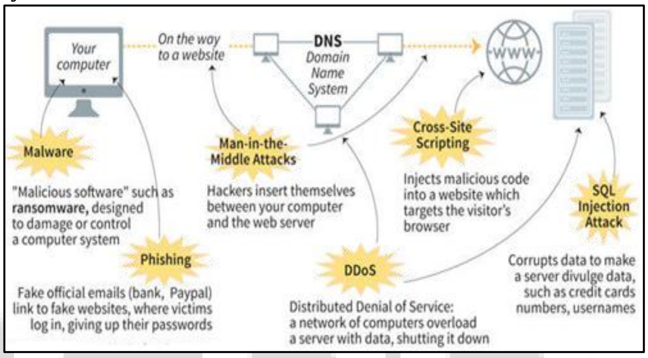

Fig. 1: Types of Cyber Attacks

III. CYBER-ATTACKS RESPONSE

Prevention is always better than the cure. The same applies to the field of IT when it comes to protection against Cyber Attacks. However, assuming that your computer(s) or website(s) were attacked, even after taking all the precautions, there are certain common general response steps laid down:

1) Did the attack really happened or is someone calling in to play a prank;
2) If you still have access to your data, back it up;
3) If you cannot access your data, and the hacker is demanding ransom, you may want to consider approaching the legal authorities
4) Negotiate with the hacker and regain the data
5) In case of social engineering and employees misusing their privileges, checks should be conducted to determine if the employee was innocent or acted deliberately
6) In the case of DDoS attacks, the load should be mitigated to other servers, so that the website comes back online as soon as possible. You may rent out servers for a while or use a cloud app so that costs are minimal.

IV. PREVENTION OF CYBER ATTACKS

In this digital era and increase use of the technology makes it tremendously important to secure our data/information. More data is being transmitted over network and stored in computer today. Nowadays the sophistication of the attacker increases day by day but intruder knowledge remains same as shown in figure 2. Therefore it is very beneficial to be educated and use tools to prevent from such cyber-attacks. Although cyber-attacks cannot be stopped completely; their effectiveness can be limited.

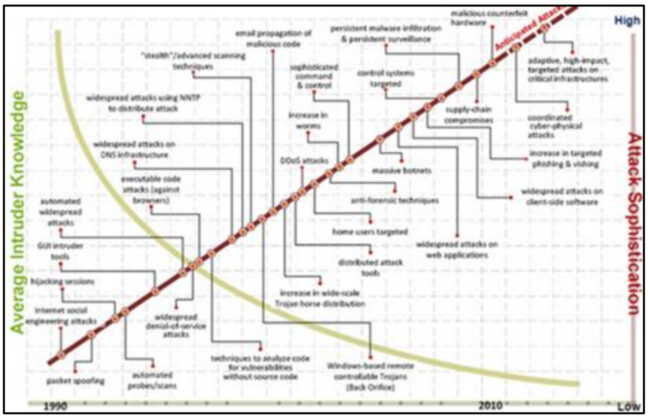

Fig. 2: Average Intruder Knowledge vs. Average Sophistication

Following the steps given will give a much higher level of security for valuable information.

1) Make sure you've got a super strong, unique password. In other words, ensure that your password is difficult to guess. One way to come up with a creative password is to brainstorm a random sentence. Take the first letter of each word in that sentence and use that acronym as the base for your password.
2) Don't use the same password for multiple services. Using the same term for all of your passwords leaves your entire digital life vulnerable to attack. This means that if a hacker has one password, he or she has all of your passwords.
3) Enable two-factor authentication. Many services, including Google, offer two-factor authentication for logging into your account. Instead of simply entering a username and password to log in, the website will prompt you to enter a code sent to your smartphone to verify your identity.
4) Apply software updates when necessary. Apple, Google, and Microsoft typically include security bug fixes and patches in their most recent software updates. So don't ignore those annoying prompts and keep your software up-to-date.
5) Carefully read the permissions before installing apps. This is one of the most prominent ways in which malicious apps can gain access to your personal information. These types of issues have been especially present in the Google Play store. A lot of apps ask for a lengthy list of permissions, and that doesn't mean they're all ill-intentioned. But it's important to be aware of the types of information your apps are accessing, which can include your contacts, location, and even your phone's camera.
6) Check the app publisher before installing. There have been numerous instances in which scammers have published apps in the Google Play store posing as another popular app. For example, in late 2012 an illegitimate developer posted an imposter app in Google Play pretending to be "Temple Run." A quick look at the publisher shows that the app comes from a developer named "apkdeveloper," not the game's true publisher Imangi Studios.
7) Avoid inserting hard drives and thumb drives you don't trust into your computer. If you find a random USB stick, don't let your curiosity tempt you to plug it in. Someone could have loaded malware onto it hoping that an interested person was careless enough to insert it into their device. If you don't trust the source, you're better off not putting your computer at risk.
8) Make sure a website is secure before you enter personal information. Look for the little padlock symbol in front of the web address in the URL bar. Also, make sure the web address starts with the prefix https://. If these things aren't there, then the network isn't secure and you shouldn't enter any data you wouldn't want made public.
9) Don't send personal data via email. Sending critical information such as credit card numbers or bank account numbers puts it at risk of being intercepted by hackers or cyber-attacks.
10) Keep an eye out for phishing scams. A phishing scam is an email or website that's designed to steal from you. Often times, a hacker will use this email or website to install malicious software onto your computer. These web entities are designed to look like a normal email or website, which is how hackers convince their victims to hand over personal information. Phishing scams are typically easy to spot, but you should know what to look out for. Many of these emails contain spell errors and are written in poor grammar. Here's a great example of a standard phishing email from Microsoft's security blog as shown below in figure 3.

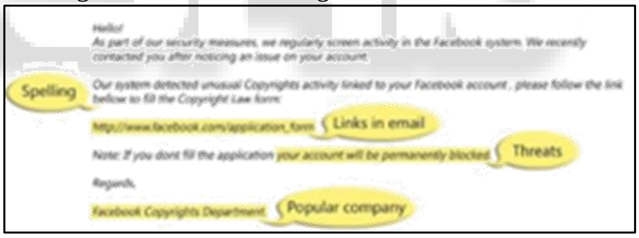

Fig. 3: Microsoft's Security Blog

11) Avoid logging into your important accounts on public computers. Sometimes you've got no choice but to use a computer at the coffee shop, library, or local FedEx. But try not to do it frequently, and make sure you completely wipe the browser's history when you're finished.
12) Back up your personal files to avoid losing them. You should keep a copy of all important files in the cloud and on some sort of hard drive. If one of them gets hacked or damaged, you'll still have a backup copy.

V. CONCLUSION

In conclusion, it’s very essential to educate home users on how to make better decisions and understand the risk associate with cyber-attacks. The key to deter cyber-attacks, with the information given we as a whole can reduce the effects of cyber-attacks. Governments across the globe need to take legal action and enact laws to protect citizens from these threats. The threat of identity theft and fraud is severe enough to warrant the necessity of educating every home user. If the effects of cyber-attacks are not at least contained partially; these threats have the capability to undo all the positive impacts computer technology has on society. Cyber-attacks are always changing and new methods can always be discovered. However, this should not deter users from at least enacting some steps to protect valuable information. User's knowledge, awareness and responsibility are the best defence against any kind of cyber-attacks regardless of government action. There are many different ways to protect data other than just the methods given. Being informed about these threats will hopefully reduce chances of such threats or even encourage others to discover preventive methods of their own.

REFERENCES

[1] Savita Mohurle and Manisha Patil; "A brief study of Wannacry Threat: Ransomware Attack 2017"; International Journal of Advanced Research in Computer Science; Volume 8, No. 5, May-June 2017; ISSN No. 0976-5697
[2] MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, "A novel method for recovery from Crypto Ransomware infections",Computer and Communications (ICCC), 2016 2nd IEEE International Conference.
[3] Haydar Teymourlouei; "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users"; World Academy of Science, Engineering and Technology; Volume 9, No. 3, 2015
[4] Stone, D. (2015). "Detecting Cyber Attacks. Retrieved from Everyday Life" - Global Post: http://everydaylife.globalpost.com/detecting-cyberattacks-30915.html
[5] Schwarz, C. D."5 ways to prevent a personal cyber attack." Retrieved from http://hereandnow.wbur.org/2014/12/26/cybersecurity-sony
[6] Musil, S."Cyber crooks use DDoS attacks to mask theft of banks' millions"Retrieved from CNET:http://www.cnet.com/news/cybercrooks-use-ddos-attacks-to-mask-theftof-banks-millions/ ; 2013, August 21
[7] The wall street Journal, America.www.wsj.com