Oct 12th, 1:00 PM - 1:25 PM

A World of Cyber Attacks (A Survey)

mubarak Banisakher
mubarak.banisakher@saintleo.edu

Marwan Omar
Saintleo University, marwan.omar@saintleo.edu

Abstract
The massive global network that connects billions of humans and millions of devices and allow them to communicate with each other is known as the internet. Over the last couple of decades, the internet has grown expeditiously and became easier to use and became a great educational tool. Now it can used as a weapon that can steal someone's identity, expose someone's financial information, or can destroy your networking devices. Even in the last decade, there have been more cyber attacks and threats destroying major companies by breaching the databases that have millions of personal information that can be sold online. Cyber-attacks can happen numerous ways and can happen when no one is looking. In this paper we survey several cyber-attacks that has been around and the current ones which will give the readers a quick overview of the finding of this survey. We also arrived at a conclusion that education in this field is very important for companies and individuals to stay safe.

Location
KSU Center Rm 460

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
1- We carefully reading through each sentence to catch errors and have other colleague proof read the paper with a fresh set of eyes.

2- We made a revision as described in the reviewer report.

3- Our goal was to include in this short survey some attacks and not every single one because the paper will be longer than the permitted length as instructed by the conference committee

4- We reviewed the paper and adjusted the abstract and the title of the paper to reflect what we are intended to do.

INTRODUCTION

Technology has changed the way most people live today. It has made us dependent on the devices to get work done, to share information, to set reminders for our busy schedules. Even though there are goods sides to having this technology, there is also a bad side that will not care if it exposes your information or destroy your assets. Attackers often aim at the large corporations for the financial gain or bragging rights, but in order to do that they will target employees by either spamming, phishing or social engineering to gain access the company's database. Most of these attacks are hatched by anonymous hacking groups or individually. Cyber risks have started to pose a serious threat towards the government, businesses and economies around the world.

CATEGORIES OF VARIOUS CYBER ATTACKS

Attackers today have plenty to work with to gain access to information from the million of devices out there. Below are some of the key tools that are being used:

1) **Malware:** According to Neil DuPaul (2012), the name malware is short for malicious software that is used and intended to damage or disable computer systems. Malware is a general term that covers the various types of threats that can happen to device such as viruses, worms, trojans, and ransomware. A virus is a type malware that can replicate itself and spread to other devices connected on the network by attaching itself to various programs and executing when a user launches the infected software programs. A virus can also be used to steal information, create botnets, steal money and render advertisement. Worms work by spreading over the network by exploiting the computer's operating system and causing damage to the network by using the networks bandwidth causing the servers to overload. According to the NATO Review magazine (2013), the first worm to be recognized is the Morris worm back in 1988. The worm used weaknesses from a UNIX system and spread largely by replicated inside the computers to the point of being unusable. Robert Tapan Morris became the first person convicted under the United States computer fraud and abuse act. The trojan horse disguises itself as a normal file or program until it is executed by a user and begins to attack by stealing data such as logins, financial and personal data and can even be used to install more malware to the network. Ransomware has become popular in recent years because this malware can hold a computer or network captive until a ransom is met. This is done by encrypting files on the hard drives or locking down all the systems while displaying a message to pay the creator to remove the restrictions.

2) **Denial of service:** According to the United States Computer Emergency Readiness Team (US-CERT) (2018), a denial of service (DoS) attack occurs when authorized users are not able to access their information systems, devices or network resources due to an attack. Some of the services that would be targeted is email, websites and online accounts. How the DoS works is the host is targeted with a flooding of network traffic to the point of the system crashes and prevents users' access, which can cost a company

time and money to restore. Some of the popular DoS attacks are a Smurf Attack and a SYN flood. In a Smurf Attack, the attacker sends large numbers of Internet Control message Protocol (ICMP) packets with the intent to spoof the victims source IP and broadcast address which causes every computer on the network to send bogus packets to targeted computer which ends up flooding the targets machine. Now the SYN flood attack sends out requests so that it can connect to target server, but never completes the three-way handshake. Because the three-way handshake is not complete this leaves a connection port in an occupied status and will not receive any other requests. The attacker will continue to send out the requests so that the target machine can no longer function.

3) **Phishing:** This attack is used to gather information or steal user data such as login credentials and credit card numbers. Usually this type of attack is sent through email or a fraudulent website that has a victim click on a malicious link that can install malware or ransomware. Or it can trick a victim into giving out personal or financial information and giving the attacker passwords by sending a malicious email to reset your password. Like phishing, Spear phishing targets more specific victims as oppose to the randomness of the normal phishing scam. Then there are phishing attacks that aim towards the powerful or wealthy individuals and that is called whaling attack.

ONLINE ACTIVITIES

Today, most of us deal with online activities such as email, banking, shopping, social networking, gaming, downloading and file sharing. All of these activities make it easier and convenient to enjoy life however, these are the right platform for attackers to exploit and get the personal information from. Let's look into some of these and see how an attacker can succeed and possible ways to deter the attack.

4) **Email:** Email is probably the biggest platform because most people have several email accounts such as work accounts, personal accounts, and educational accounts. In the digital world there are billions of emails being sent and received daily around the world and most have some kind of personal information that can be compromised. An attacker can send email spam, email spoof, and email that can contain malware for user to download. Some countermeasures are to just delete those emails that you don't recognize and don't click on any links that are in the emails.

5) **Net-banking:** This is the second most common platform for an attacker to make there moves. Net banking deals with online transaction, bill payments, loans and credit card payments. Users are able to manage their personal and financial accounts online instead of going into a bank and dealing with employees at specific times and day. Hackers try phishing attacks to get information by sending fraudulent emails from the company asking you to reset passwords or update personal information so that the attacker can gain knowledge and get inside the account. The best measure is to take the time and make sure the website being visited is secure and looks official. Always check to make sure the website uses HTTPS in the URL when dealing with transactions online.

6) **Social Networking:** This platform has been growing in the last decade because we all want to be connected and share thought and ideas. Also, this is a place where you can

share pictures with family and stay in touch with friends and beloved ones. This is where people share their locations and activities they are currently doing which can cause a problem with not only cyber-attacks but also physical security. Attackers can use this for social engineering and can steal identities for their own gain. Social networking sites can be filled with adware and can be easily targeted to gain personal information. The best way to stay safe from being attacked is to make sure you have a very strong password and be careful of who you socialize with and know what is being shared from the website.

LIST OF CURRENT CYBER ATTACKS

Below is a list of the most recent cyber-attacks that have occurred around the world and the details of these attacks.

KOVTER: According to the Center for Internet Security (2018), Kovter was introduced back in March of 2016. It is described as a Trojan that evades its detection by hiding in the registry keys and that can be used as a remote access backdoor. It is being sent through email attachments by some kind of maile spam that contains the malicious office macros. Kovter installs JavaScript as a run key registry value that will automatically run on startup. Once in startup mode, Kovter payload will load into memory and then execute inside a legit process like explore.exe. After installation, Kovter will remove the original installer from the disk and leaving only the malicious registry keys. Kovter has been known to send personal information on the computer to a remote server.

WANNACRY: This started back in May of 2017 and still lives to this date according to the Center for Internet Security (2018). This is a worldwide ransomware attack that targeted Microsoft Windows operating systems by encrypting data and then ask in return ransom payments in Bitcoin cryptocurrency. The attack targeted Windows 7 and Server 2008 clients and when executed the threat would search and encrypt specific filename extensions. It would also append a text file to every file that it encrypted stating the ransom of $300 and a timer of when to pay.

EQUIFAX DATA BREACH: Back in September 2017, Equifax announced that they have been fallen victim of a data breach that affects over 145 million consumers where their full names, social security number, date of birth, addresses, and driver license numbers have been compromised. Not only did it affect US consumers, it also compromised residents from the United Kingdom and Canada. This happened due to the company offering visitors malware that was acting as an update to Adobe Flash, Jeremy Owens (2018). This infected the consumers own personal computers and allowed the attackers to gain even more personal information.

CONCLUSION

With technology rapidly changing, so are the threats that hide in the shadows. Some of the attacks listed can be avoided if you are educated on the types of attacks out there. Some are out of hands but we hope to trust that the companies do the same by educating

and training their employees. With the world constantly trying to connect devices with humans, our personal data is being stored on them and can be exposed if not protected. The internet is not going anywhere anytime soon but what we share and what we do on the global network can cause damage to oneself.

REFERENCES

DuPaul Neil (2012), Common Malware types: Cybersecurity 101. (2012). Retrieved from URL https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

NATO REVIEW Magazine. (2013). Retrieved from URL https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

Understanding Denial-of-Service Attacks. (2018) Retrieved from URL

https://www.us-cert.gov/ncas/tips/ST04-015

Top 10 Malware January 2018. (2018) Retrieved from URL

https://www.cisecurity.org/blog/top-10-malware-january-2018/

Jeremy Owens (2018), The Equifax data breach, in one chart. Retrieved from URL

https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07