IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 9, September 2020

DOI 10.17148/IJARCCE.2020.9913

Cyber Security Threats on the Internet and Possible Solutions

B. A. Obotivere[1], A. O. Nwaezeigwe[2]

Department of Computer Science, Delta State Polytechnic, Oghara, Delta State, Nigeria[1,2]

Abstract: Cyber security is concerned with protecting information, hardware, and software on the internet from unauthorized use, intrusions, sabotage, and natural disasters. The numerous ways in which computer systems and data can be compromised has made cyber security a growing field. Data needing cyber security could be online banking information, medical or financial information, and private photographs. However, cyber security is not always easy to implement as there are threats to cyber security itself. Cyber security threat is any malicious act that seeks to damage or steal data and disrupt digital life in general. This paper analyses and identifies the various threats on the internet and proposes possible solutions to enable internet users keep on guard.

Keywords: Threats, Cyber Security, Internet, Digital Life.

I. INTRODUCTION

The advent of computer technology has had great impact on mankind. Information technology, being an integral part of computer technology has made significant contribution to getting things done easily while handling huge data. Despite the effectiveness of the technology of computing, most trusted stored files in computers, mobile phones, and the internet are susceptible to attacks by hackers and all forms of unauthorized access in the cyberspace and this gives rise to the need for efficient cyber security systems. The most prevalent current example of the application of communications technology is the internet. The internet, since its emergence has evolved into a force strong enough to reflect the greatest hopes and fears of those who use it. With the internet, one could go into the world of real creeps without having to smell them. The internet has changed the way we live, work, study and conduct businesses. It has turned the world into an inclusive village of global connectivity. We can exchange informal chats, messages or conduct real businesses with people on the other side of the planet quickly and inexpensively. The proliferation of personal computers, mobile technology, easy access to the internet, and a booming market for related new communications devices have changed the way we spend our leisure time and the way we do businesses. This technological development has also changed the way criminals commit crimes. Universal digital accessibility now opens new opportunities for the unscrupulous. Computers, related technologies and networks are now being used to harass victims and set them up for violent attacks. Even terrorist activities that threaten all of us have been coordinate and carry out using technology [1].

II. CYBER SECURITY

Cyber security is concerned with making cyberspace safe from cyber threats. The notion of "cyber threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors. As commonly used, the term "cyber security" refers to three things:

- A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and software, including data and information, as well as other elements of cyberspace, from all threats, including threats to the national security;
- The degree of protection resulting from the application of these activities and measures;
- The associated field of professional endeavour, including research and analysis, directed at implementing those activities and improving their quality [2].

Cyber security is also concerned with the understanding of surrounding issues of diverse cyber-attacks and devising defense strategies (that is., countermeasures) that preserve confidentiality, integrity and availability of any digital information [3]. Many cyber security experts believe that malware is the key choice of weapon to carry out malicious intends to breach cyber security efforts in the cyberspace. Malware refers to abroad class of attacks that is loaded on a system, typically without the knowledge of the legitimate owner, to compromise the system to the benefit of an adversary. Some exemplary classes of malware include viruses, worms, Trojan horses, spyware, and bot executables.

Security Threat, Attacks, Exposure and Vulnerability

In order to address security threats on the internet, the system components that make up the internet must first be identified. It is important to understand the system components including all components, devices and services. The principal assets of any system are the system hardware, software, services and data offered by the services [4].

Vulnerability

Vulnerability is a cyber security term that refers to a defect or weakness present in a system itself that allows information security to be exposed to a threats or attacks. There are two types of vulnerabilities: hardware and software. Hardware vulnerabilities are very difficult to identify and fix even if the vulnerability were identified due to hardware compatibility and interoperability while the software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drives.

Exposure

An exposure is a non-universal vulnerability or set of systems that allows attacker to conduct information gathering activities or to hide activities. Such exposure raises the possibility that an attacker might capture the device, extract cryptographic secrets, modify their programming, or replace them with malicious device under the control of the attacker.

Threats

A threat is a malicious act that aims to corrupt or steal data or disrupt an organization’s system or the entire organization. Threats can be derived from two primary sources: humans and nature. Human threats are those caused by people, such as malicious threats consisting of internal or external threats looking to harm and disrupt a system. While natural threats, such as earthquakes, hurricanes, floods, and fire could cause severe damage to computer systems and nobody can prevent them from happening. [5] explained the concept of cyber security threat as a malicious act that seeks to damage, or steal data, and disrupt digital life in general. According to [6], cyber-based technologies are now ubiquitous around the globe. They said criminals, terrorists, and spies also rely heavily on cyber-based technologies to support their objectives. These malefactors may access cyber-based technologies in order to deny service, steal or manipulate data, or use a device to launch an attack against itself or another piece of equipment. Examples of commonly recognized cyber-aggressors include cyberterrorists, cyberspies, cyberthieves, cyberwarriors, and cyberhacktivists.

- **Cyberspies:** Cyberspies are individuals who steal classified or proprietary information used by private or government corporations to gain a competitive strategic, security, financial, or political advantage.

- **Cyberterrorists:** Cyberterrorists are criminals who uses computer technology and the internet, especially to cause fear and disruption. Insurgents, jihadists and transnational terrorist organizations, have used the internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, and a means of communication.

- **Cyberthieves:** Cyberthieves are individuals who steal or engage in illegal cyberattacks from others using a computer for monetary gain. For example, organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a financial account.

- **Cyberwarriors:** Cyber warriors are computer experts who engage in the infiltration or sabotage of information systems, or in the defense of information systems against outside attack, typically for strategic or military purpose.

- **Cyberhacktivists:** Cyberhacktivists are individuals who breaches websites or secured communications systems to deliver political messages including those related to foreign policy or propaganda. Examples include someone who attacks a technology system as a personal challenge (who might be termed a “classic” hacker), and a “hacktivist” such as a member of the cyber-group anonymous who undertakes an attack for political reasons.

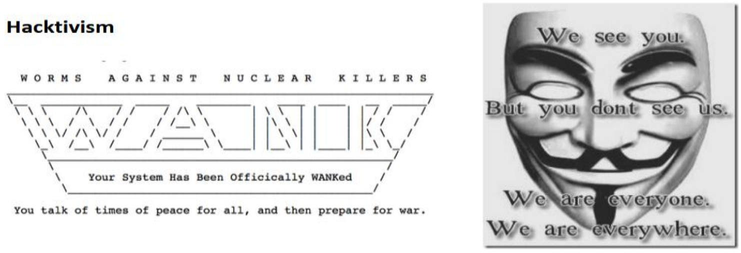

Hacktivism
WORMS AGAINST NUCLEAR KILLERS
WANK
Your System Has Been Officically WANKed
You talk of times of peace for all, and then prepare for war.
We see you.
But you dont see us.
We are everyone.
We are everywhere.

Fig.1: Hacktivism

[Source: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction to the Concept of IT Security.pdf]

Attacks: Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense [4]. Some common cyber-attacks are: physical, access, denial-of-service, reconnaissance, cybercrime and so on.

III. TYPES OF CYBER SECURITY THREATS

The task of keeping up with new technologies, security trends and threat intelligence is challenging but must be performed. In order to protect information and other assets from cyber threats, the following forms of threats are analyzed:

- **Ransomware** is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them. Ransomware is becoming increasingly prevalent: Symantec observed a 500% month-on-month increase in ransom ware in 2013.
- **Malware** or "malicious software," covers any file or program introduced into the target's computer with the intent to cause damage or gain unauthorized access. There are many different types of malware, including viruses, spyware, worms, ransomware, Trojan horses and keyloggers, to name a few.
- **Social Engineering** is a key area where threats are proliferating and where social engineering is carried out (that is, attackers gather personal data about persons of interest via social networks and then use it to make targeted emails more convincing).
- **Phishing** is a type of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information [7].

IV THE TOP 9 CYBER SECURITY THREATS, RISKS OF 2019 AND THEIR SOLUTIONS

The term "Cyber security Threats" can mean many different things to many people. For some, threats to cyber security are limited to those that come through virtual attack vectors such as malware, however, cyber threats are continuously changing. SophosLabs' 2019 Threat Report indicates that: "The threat landscape is undoubtedly evolving; less skilled cybercriminals are being forced out of business, the fittest among them step up their game to survive and we'll eventually be left with fewer, but smarter and stronger, adversaries. These new cybercriminals are effectively a cross-breed of the once esoteric, targeted attacker, and the pedestrian purveyor of off-the-shelf malware, using manual hacking techniques not for espionage or sabotage, but to maintain their dishonorable income streams." [8] analyzed the top 9 cyber security threats that will ruin your day. These cyber security threats are as follows:

1. Human Nature

It has been confirmed that people are the biggest threats to cyber security. These vulnerabilities come from employees, vendors, or anyone else who has access to your network or IT-related systems. More so, a cyberattack or data breach can occur simply because of human error or a lack of cyber security awareness such as using easy-to-guess passwords or falling for phishing emails. For example, hackers frequently use social engineering tactics such as "hacking without code" to get their victims to either provide the information they need or get them to engage with malicious content. So, they may install malware, download data, or perform other dire actions that can pose a potential risk. Whatever the reason, whomever is responsible, the results are the same: Data is stolen, your customers are compromised, and your company's reputation takes a major hit.

Recommended Solution(s): Keeping strong firewalls and antivirus solutions in place is not enough, rather companies should use the services of an in-house or third-party cyber security operations center (CSOC) to stave off these types of cyber security threats for both their overall organizational cyber security and their website.

2. Various Forms of Malware

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Microsoft identifies malware cyber security threats as "malicious software or unwanted software." This malicious software includes backdoors, downloaders, spyware, trojans, worms, and macro viruses. [9] reports that the top 10 Malware in September 2019 are: (i) Zeus, (ii) Kovter, **(**iii) Dridex, (iv) Nanocore, (v) Cryptowall, (vi) Ghost, (vii) Coinminer, (viii) Trickbot, (ix), Ursnif**,** and (x) Bifrose.

Recommended Solution(s): There are many things you can do to safe guard malware-based cyberattacks:

- The use of limited user access and application privileges right.
- The use of reputable antivirus and anti-malware solutions, email spam filters, and endpoint security measures.
- Ensure that your cybersecurity updates and patches are all up to date.
- Ensure that your employees undergo regular cybersecurity awareness training in order to avoid suspicious emails and websites.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

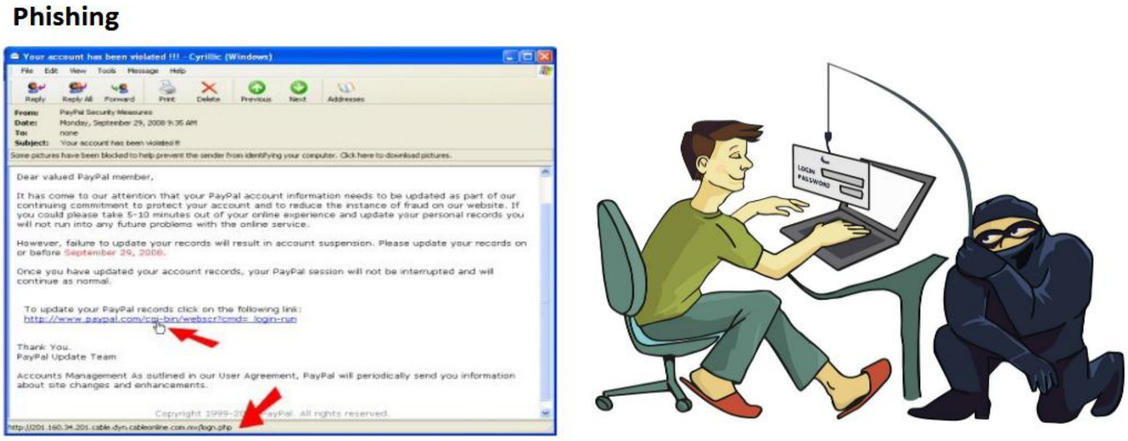
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 9, September 2020

DOI 10.17148/IJARCCE.2020.9913

3. Different Types of Phishing Attacks and Social Engineering

Phishing is a fraudulent attempt to elicit sensitive information from a victim in order to perform some type of action (gain access to a network or accounts, gain access to data, get the victim to perform an action such as a wire transfer, and so on). According to [10], Hushpuppi used cyber-heist to defraud a New York-based law firm.



Phishing

Your account has been violated !!! - Cyrillic (Windows)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
LOGIN
PASSWORD

From: PayPal Security Measures
Date: Monday, September 29, 2008 9:35 AM
To: none
Subject: Your account has been violated !!!

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

Dear valued PayPal member,

It has come to our attention that your PayPal account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before September 29, 2008.

Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal.

To update your PayPal records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
PayPal Update Team

Accounts Management As outlined in our User Agreement, PayPal will periodically send you information about site changes and enhancements.

Copyright 1999-20 PayPal. All rights reserved.

http://201.160.34.201.cable.dyn.cableonline.com.mx/login.php

Fig. 2: Phishing
[Source: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction to the Concept of IT Security.pdf]

Recommended Solution(s): There are several things that you can do to ward off cyber security threats:

- The Implementation of cyber security awareness training for every employee across board.
- The use of reliable email and spam filters.
- The use of email encryption and email signing certificates.
- Emphasize the importance of phishing reporting.
- The running of random phishing simulations.
- The use of HTTPS on your website to create secure, encrypted connections.
- Provision of two-factor authentication.

4. Formjacking

Formjacking is a type of cyber security threat that involves a cybercriminal taking over forms on websites by exploiting their security weaknesses. [11] Informed that two Nigerians Babatunde Adesanya and Akinpelu Abass, cloned the corporate websites of ILBN Holdings BV in order to carry out a scam on Freiherr Fredrick Von Hahn, who represent North Rhine-Westphalia. The goal is to skim and harvest any valuable data that end users submit via the forms. Symantec's 2019 Internet Security Threat report shows that formjacking was on the rise in 2018.

Recommended Solution(s): There are some ways that you can prevent formjacking. These include:

- The running of vulnerability scanning and penetration testing will help to identify any weaknesses in your cyber security defenses.
- The monitoring of outbound traffic from one website to another.
- Using sub-resource integrity (SRI) tags to ensure that files used by web applications and documents do not contain unexpected, manipulated content using hashing.

5. Inadequate Patch Management

Inadequate patch management is a process which leaves gaping holes in your IT security infrastructure. Preferably, patching should be implemented as soon as a vulnerability is detected because they: leave your organization at risk of cyberattacks, lead to remediation which can lead to downtime, cause reputational harm, and make you noncompliant with many industry and regulatory cyber security standards.

Recommended Solution(s): Some of the ways that you prevent inadequate patch management include:

- Making Patch management a priority and not optional.
- Provision of effective patch management is essential to your business and the security of your customers' data.
- Developing and implementing effective patch management policies and procedures will help to reduce the attack surface of your organization stolen data.
- Patching these vulnerabilities in real time through automation makes your cyber security more effective.

DOI 10.17148/IJARCCE.2020.9913

6. Outdated Hardware and Software

It is important to note that all patches are updated but, it is equally true that not all updates are patches. Therefore, keeping your hardware and software assets (components) up to date is vital to the security of your organization's network, servers, devices, data, and customers. If you are using out-of-date technologies, your security defenses will not be able to keep out enemies. The same concept can be applied to your cyber security defenses.

Recommended Solution(s): Some of the ways that you can prevent outdated hardware and software include:

- Develop device management policies for your organization and follow industry best practices.
- Keeping your systems and software up to date will prevent hackers from hacking your information.
- When a manufacturer releases an update, it is necessary to apply it immediately in order to remain secure and out of the reach of cybercriminals.

7. Internet of Things Insecurities

Internet of Things (IoT) connects and networks devices across the world. IoT is popular, and its popularity continues to grow. [12], reports that the number of IoT devices will reach 20.4 billion by the year 2020 and the number seems to increase up to 25 billion by 2025. [13], reported that the Open Web Application Security Project, or OWASP, has released the latest top 10 IoT Vulnerabilities list. These are: Weak, guessable or hard-coded passwords, insecure network services, insecure ecosystem interfaces, insecure default settings, insecure data transfer and storage, insufficient privacy protection, use of insecure or outdated components, lack of secure update mechanisms, lack of device management and lack of physical hardening.

Recommended Solution(s): Some of the ways that you can protect your IoT insecurities threats. These include:

- The use of IoT digital security certificates as part of your PKI infrastructure to facilitate encrypted connections.
- Securing your devices, protecting data and privacy is by securing your IoT.
- To identify any vulnerabilities and potential liabilities

8. Man-in-the-Middle Attacks

Man-in-the-middle (MitM) attacks is an attack where the attack secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. These types of cyber security threats are made by cybercriminals who set up fake public Wi-Fi networks or install malware on victims' computer or networks. The goal of an attack is to steal personal information, such as login credentials, account details and credit card number.

Recommended Solution(s): Some of the best ways to help protect your company, customers, and website from man-in-the-middle attacks include:

- Using HTTPS on your websites is actually required by major browsers such as Google Chrome, Firefox and so on.
- Using HTTPS on your websites by installing SSL/TLS certificate.
- Using Virtual Private Networks (VPNs) on public Wi-Fi can help increase security and create secure encrypted connections.

9. Poor Digital Certificate Management

Digital certificate manager (ACM) allows you to manage digital certificates for your network and use Transport Layer Security (TLS) to enable secure communications for many applications. Expired SSL certificates is a form of cyber security threat that one should be mindful of on the internet. Certificate expiries can happen to any website or business if they are not careful.

Recommended Solution(s): Some of the ways you can prevent poor digital certificate management include:

- Having a few SSL certificates and their corresponding PKI infrastructure will help to facilitates encrypted connections.
- Using Sectigo Certificate Manager (formerly Comodo CA Certificate Manager) is a solution that helps you to mitigate certificate expiry issues by automating rapid certificate renewals, installations, and revocations.

In general, the following measures will assist to curb cyber security threats:

- The use of strong password as part of a good online security. Some of the ways you can make your password difficult to guess include:
- using a combination of capital and lower-case letters, numbers and symbols
- making it between 8 and 12 characters long
- avoiding the use of personal data
- changing it regularly
- never using it for multiple accounts

- using two factor authentications
- Endeavour to limit user access and application privileges. For example, you can:
- control physical access to premises and computers network.
- restrict access to unauthorized users.
- limit access to data or services through application controls.
- The use of security software.
- Ensure that your systems and programs are updated regularly
- Implement cybersecurity awareness training for every one across board.
- The use of intrusion detectors to monitor system and unusual network activity.
- The use of reputable antivirus and anti-malware solutions, email spam filters, and endpoint security measures.
- Provision of a strong firewall in place.
- Using best practices defined in the government's cyber essential scheme [14].

V. CONCLUSION

Like a sniper, the most dangerous cyber security threats are the ones you never see coming. As cyber security threats continues to evolve and become more sophisticated, enterprise IT must remain vigilant when it comes to protecting their data and networks. To do that, they first have to understand the types of security threats they are up against. Having identified and understood in clear terms the various cyber threat to cyber security, caution is a watchword for whoever is on the internet. Nevertheless, cyber security is potentially under the mercies of some common factors as explained in this journal article.

REFERENCES

[1]. S. O. Asakpa, O. T. Adeife, B. A. Obotivere and O. J. Isaiah, "E-crimes on the internet and possible solutions"- 3rd National Conference of the Academic Staff Union of Polytechnics (ASUP) Zone C, Ado- Ewe 2018 at the Federal Polytechnic, Ado Ekiti, 2018.

[2]. M. Duun, A Comparative Analysis of Cyber Security Initiatives Worldwide: WSIS Thematic Meeting on Cyber Security. Geneva, 28 Jun 1 July 2005.

[3]. J. Jang, and S. Nepal, "A Survey of Emerging Threats in Cyber security". Journal of Computer and System Sciences, 80 (2014), 973-993. 2014.

[4]. M. Abomhara, and G. Koien, "Security and privacy in the internet of things: Current status and open issues,". The 2nd International Conference on Privacy and Security in Mobile Systems (PRISMS 2014), Aalborg, Denmark, May 2014.

[5]. T. T. Abi, What is a Cyber Threat?, 2020. [Online]. Available: Http://www.upguard.com/blog/cyber threat

[6]. A. F. Eric, C. L. Edward, W.R John, and A.T. Catherine, The 2013 Cyber security Executive Order: Overview and Consideration of Congressional Research Service Report. 2013.

[7]. P. S. Seemma, S. Nandhini, and M. Sowmiya, "Overview of Cyber Security". International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 7, Issues 11, November 2018.

[8]. C. Casey, The Top 9 Cyber Security Threats that are guaranteed to ruin your day, 2019. [Online]. Available: http://www.thesslstore.com/blog/the-top-9-cyber-security-threats-that-will-ruin-your- day/

[9]. Center for Internet Security (CIS). Top 10 Malware, September, 2019. [Online]. Available: http://cisececurity.org/blog/top-10-malware

[10]. U. William, Hushpuppi Conspired to steal £100 Million from English Premier League club, 2020. [Online]. Available: http://NairaMetrics.com

[11]. BBC News: Nigerian Men arrested over German PPE 'Scam'. Sept. 07, 2020. [Online]. Available: http://www.bbc.com/news/world-africa-54051424

[12]. Gartner, 2019. 7 trends to watch in IoT & cyber security in 2019. http://www.irishtechnews.ie/7-trends-to-watch/

[13]. P. Rentz, OWASP Releases Latest Top 10 IoT Vulnerabilities, 2019. Available: http://www.techwell.com/techwell-insights/2019/01/OWASP-release-latest-

[14]. Common Cyber Security Measures. [Online]. Available: https://Nibusinessinfo.co.uk.htm

[15]. Introduction to Security. Cyberspace, Cybercrime and Cybersecurity. [Online]. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction to the Concept of IT Security.pdf