IJCAT - International Journal of Computing and Technology, Volume 7, Issue 10, October 2020
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

A Study of Battles Against Cyber Crime Out of The Trenches

[1] Oluwatobi Akinmerese; [2] Olamide Kalesanwo

[1] Computer Science, Babcock University, Ilishan Remo,
Ogun State, Nigeria

[2] Computer Science, Babcock University, Ilishan Remo,
Ogun State, Nigeria

Abstract - Recent Information Technology (IT) solutions have undoubtedly brought about societal transformation. Several advancements in IT has facilitated several daily activities such as online transactions and connecting with other people. The heavy dependency on the internet and the rapid growth in the cyberspace has resulted in proliferation of cyberattacks. Attacks such as data breach, privacy invasion, ransomware, malware. Despite several attack prevention mechanisms and resource availability of even big IT firms, cybercriminals still find a way to leverage on vulnerabilities and strike a blow to these organizations. Cyber crime is one associated with the most serious of these issues and even its apparent growth in recent times demonstrates clearly how brand-new technologies create new chances for criminal activity. This article gives a brief overview of cyberattacks stating recent attacks on big organizations while discussing mitigation approaches.

Keywords - *Cyberattacks, Computer Security, Cybercriminals, Cyberspace.*

1. Introduction

The advancements in computing, computing technologies, and computing solutions have seen drastic rise in dependability of humans on computing devices. These device, technologies and solutions drive our everyday life. Public and private organizations, small-scale and large-scale businesses as well as individuals leverage on the ease and comfort these technologies bring. More than half of the world's population makes use of the internet-based technology everyday and almost every day [3]. Many of these technologies participate and play major role in the cyber space. Cyberspace refers to an environment where communication among computing devices occur and are facilitated. It allows digitized information to be created, stored, and exchanged over computer networks. Over the years, the cyberspace has undoubtedly grown at a rapid pace thanks to the digital revolutionization. This revolutionization has propelled the world via social networks, cloud computing, artificial intelligence, internet of things, automated processes, online transactions, to mention a few. However, the progression in digitalization results in growth in cyber activities which opens several windows of opportunities for cybercrime. Cybercrime can be referred to as a criminal activity that utilizes computers or computing devices in the cyberspace for theft. Cybercrime could result in loss of funds, privacy intrusion, disruption in services, cyber terrorism to mention a few. Cybercrime can be carried out by individuals or organizations for personal gain, political reasons, publicity, power, and revenge [5]. The bulk of cybercrime is an assault on data concerning people, companies, or governments[6].The fight against cybercrime needs a comprehensive and robust approach. It is imperative that law enforcement agencies, government and even individuals adequately investigate and prosecute cyber criminals [1].

The list of cybercrime is fast growing and some of them include; network intrusion, dissemination of computer viruses, other existing crimes that can be carried out with the use of computer or computing devices, identity theft, cyber bullying, human trafficking, terrorism, privacy intrusion, internet fraud, Automated Teller Machine (ATM) fraud, file sharing and piracy, forgery, child pornography, hacking, spam, e-mail hacking, and sabotage. Cybersecurity and cybercrime can hardly be divided in the interconnected and internet driven environment that we have presently. It plays an important role in the development of information technology as well as internet services. Ensuring the safety of internet users has become integral in the development of new systems and services[7]. Privacy and security of data should be the priority security measure that any organization considers. This article evaluates and analyzes recent cyberattacks on top organizations, strategies used to mitigate and recover from the attacks, as well as its implications. In achieving this, four sections are presented. Section 1 discuss the introduction giving an overview of cyberattacks. Recent attacks on top organizations were covered the section 2 while section 3 elaborates on the strategies that can be used to mitigate these attacks. The conclusion is showcased in section 4.

2. Recent Cyberattacks on Top Organizations

The outbreak of the COVID-19 pandemic has forced many institutions and organization to resolve into remote business operations thereby increasing cyber activity. There has been a drastic rise in the number of data breaches and over 81 global companies have reported data breaches and over 80% of the data breaches have occurred because of stolen data or brute force attack [8].Currently, the pandemic has given cyber criminals an avenue to exploit and launch highly sophisticated cyberattacks on every industry. In the first six months of 2020, numerous Fortune 500 businesses were hit by major data breaches in which hackers sold information containing account passwords, personal documents, private and financial details stolen from these organizations.This year, nearly 16 billion records have been unveiled. In comparison, in the first quarter of the year 2020, 8.4 billion records were exposed! In contrast with the first half of 2019 during which 4,1 billion records were exposed, this figure is a 273% rise relative to the first half of 2019 [8].

Twitter, a social media platform was breached when the twitter accounts of high-profile US citizens like Elon Musk, Barack Obama, Bill Gates, and Joseph Biden were verified. The cyber criminals were able to reset the user passwords, post fake tweets from these accounts and offered to send $2000 for $1000 sent to a specified Bitcoin address. According to Twitter (2020), “the attack on July 15, 2020, targeted a small number of employees through a phone spear-phishing attack. This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems”[2].

Marriott International which is an American multinational hospitality company disclosed a security breach that impacted data of more than 5.2 million hotel guests who used their company’s loyalty application. Hackers stole login codes from two Marriott personnel accounts who had access to customer details about the hotel chain's loyalty program. They used the information about a month before the violation was found to siphon off the data.Hackers may have stolen credentials from their workers either by credential stuffing or phishing, according to the Marriot. Earlier in late 2018, the hotel giant also announced a data leak in which up to 500 million guests were involved [9].

As a result of the “work from home policy” invoked due to Covid-19 outbreak, Zoom became the most widely used video conferencing application [10]. The application became vulnerable to various security threats and eventually became a victim of the data breach.

In the first week of April 2020, the news of “500,000 stolen Zoom passwords available for sale in dark web crime forums” shook the application users. It was reported that more than half a million Zoom account login credentials were up for sale and some of the accounts’ credentials were given away for free. In fact, some of the login credentials were sold for less than a US cent each. Along with account login credentials, victims’ personal meeting Uniform Resource locators (URLs) and HostKeys were available too. The leaked account’ details belonged to financial institutions, banks, colleges, and various organizations[8].

Hackers claim they have accessed the personal data of 80,000 Covid-19 patients in New Delhi.

This attack was done in protest against Delhi Government’s approach towards the healthcare personnel. This is not the first breach of security to occur during the pandemic: in May a French hacker claimed he could access the location data of over 100 million people using the government’s Covid-19 tracing app[11].

Kingston’s Royal Military College is one of four military training schools in Canada. On July 2020, there was an incidence of cyberattack on the University’s online network.

The Online network was temporarily disabled and seem like core systems of the institution were hit. The malicious software that crippled the core system exploited a security hole to install itself and thereafter encrypt the content of the disks rendering it inaccessible and unreadable.

In preventing further spread of the infection, the institution had to turn off everything thereby crippling activities on the school [12].

Data breach of 18 companies were exposed on hacker’s forum. The data breach exposed databases of these companies. Over Three hundred and ninety one million user records were exposed [13]. Table 1 shows a list of the companies and the number of records that were exposed.

Table 1: List of companies that were breached and number of records exposed.

S/N	*Company*	Number of User Records
1	Appen	5.8 Million
2	Chatbooks	15.8 Million
3	Dave	7 Million
4	Drizly	2.4 Million
5	GGumim	2.3 Million
6	Havenly	1.3 Million
7	Hurb	20 Million
8	Indaba Music	475 Thousand
9	Ivoy	127 Thousand
10	Mathway	25.8 Million
11	Proctoru	444 Thousand
12	Promo	22 Million
13	Rewads1	3 Million
14	Scentbrid	5.8 Million
15	Swvl	4 Million
16	True Fire	602 Thousand
17	Vakinha	4.8 Million
18	Wattpad	270 Million
Total Number of User Records breached		391,648,000 **(391 Million, 648 thousand)**

Over 500GB of data has been claimed to the stolen from the Microsoft's private Github repository. The attackers gained full access to the software giant's private repositories. However, is has been stated that the information leaked does not call for any alarm [14].

Recent attacks on these big companies is an indication that cyber criminals are always attempting new means to strike a blow. Despite the ever-improving mitigation techniques and cybersecurity approach, there is need to access every means and vulnerability that can be exploited by attackers. The next section highlights some of the mitigation techniques that are used to curb these constantly stemming attacks.

3. Mitigating Against Cyber Attacks

The ever changing approach attackers use to launch cyberattacks calls for the need to have an ever evolving cyber security approach as well. Cybercrime is rising and new technological frameworks for tackling the growth of cybercrime are in-efficient. This suggest that more preventive measures are needed[4].Cyber security is used to refer to tools, technologies, training as well as practices that are used to protect network systems, devices, software programs, information and data from attackers or unauthorized access. Due to the wide range of attacks (some of which include attack on data, attacks on network, attacks on software program) there are diverse types of cyber security approaches. However, based on some of the reported cases in earlier section, the cybersecurity approach that will be discussed are;

Data Loss Prevention: This is a mechanism that ensures that sensitive data are not being transmitted outside the private network. This technique is used by several organizations to ensure that vulnerabilities are not present on the network and sensitive data are not leaked intentionally or unintentionally by staff and users of the data in the network. The network administrator is aware of what data is being transmitted by users. By using monitoring, detection and blocking techniques, sensitive data are scanned and are prevented if need be from being transmitted.

Intrusion Detection and Prevention Systems:These are systems that monitor the network system to detect and prevent any form of intrusion or anomaly in the network behavior. These systems are able to identify and weed out malicious programs and also detect social engineering schemes that sway users into revealing sensitive information. These systems also help in preventing malware attacks and SQL injections that can be used to access enterprise databases [15].

Encryption of Data:Encryption is the act of scrambling and encoding data to avoid readability and accessibility from an unauthorized third party. The encryption uses a special key to encode the data and only the authorized party with the required key can make meaning of the data. With this technique, even if an attacker lays hold of the information, it will be meaningless except he has the key to unscramble the cyphered text. Cyphered texts are the result of the scrambled or encrypted data while the process of converting the encrypted or cyphered text into readable form using the authorized key is known as decryption. Encryption can be used to protect data at rest (data sitting in the data storage) or data in transit (Data actively used or transferred). Adequate security management on databases will limit attacker's access to data in databases.

Regular Vulnerability assessment Test: This is a process of identifying and evaluating the security vulnerability in an organization. It allows organizations respond quickly to potential and existing threats. Regular vulnerability assessment reduces the chance off attackers preying on vulnerabilities.

Regular update of software and patch installations: Regular installation of software updates and patches also reduce the risk of cyber attacks.
User Orientation: Users of the organization's network (mostly employees) should be educated and trained about security awareness to help them identify and combat cyber threats.

4. Conclusions

Computer security is not only a technological defense strategy, it is also regarding people. Individual users, private sector as well as federal government needs a basic understanding of cyber threats and how to recognize them. On one hand, advancement in innovation has actually brought a lot greater efficiency: traffic jams eliminated, pollution lowered, more affordable expense of transport and even more. It is indeed a golden age. Then a Computer attack jeopardizes the main network. The systems that co-ordinate all transportation shut down, bringing an entire city to a sudden halt, crucial services stop working, and turmoil ensues. Any organization could be attacked. It is important to always be ahead of cyber attackers so as to avoid losing sensitive information.

References

[1] S. Rajeyyagari and A. S. Alotaibi, "A study on cyber-crimes, threats, security and its emerging trends on latest technologies: influence on the Kingdom of Saudi Arabia", International Journal of Engineering & Technology, vol. 7, no. 23, 2018, pp. 54. Available: 10.14419/ijet.v7i2.3.9969.

[2] "Twitter", Twitter.com, 2020. [Online]. Available: https://twitter.com/TwitterSupport/status/1289000138300563457?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1289000208701878272%7Ctwgr%5E&ref_url=https%3A%2F%2Fwww.theverge.com%2F2020%2F7%2F30%2F21348974%2Ftwitter-spear-phishing-attack-bitcoin-scam. [Accessed: 26- Sep- 2020].

[3] A. Kovacevic, N. Putnik and O. Toskovic, "Factors Related to Cyber Security Behavior", IEEE Access, vol. 8, 2020, pp.125140-125148. Available: 10.1109/access.2020.3007867.

[4] Z. Liu, "A Cyber Crime Investigation Model Based on Case Characteristics", International Journal of Digital Crime and Forensics, vol. 9, no. 4, 2017, pp. 40-47. Available: 10.4018/ijdcf.2017100104.

[5] M. Watson, "5 Reasons Why Cyber Criminals Attack - IT Governance UK Blog", IT Governance UK Blog, 2020. [Online]. Available: https://www.itgovernance.co.uk/blog/5-reasons-why-cyber-criminals-attack. [Accessed: 26- Sep- 2020].

[6] "cybercrime | Definition, Statistics, & Examples", Encyclopedia Britannica, 2020. [Online]. Available: https://www.britannica.com/topic/cybercrime. [Accessed: 26- Sep- 2020].

[7] G. Marco, Understanding cybercrime, 2nd ed. ITU publication, 2012.

[8] P. Dutta, "5 Biggest Data Breaches of 2020 (So Far) - Security Boulevard", Security Boulevard, 2020. [Online]. Available: https://securityboulevard.com/2020/08/5-biggest-data-breaches-of-2020-so-far/#. [Accessed: 26- Sep- 2020].

[9] K. Bowen, "Credential Stuffing: the Culprit of Recent Attacks", Infosecurity Magazine, 2020. [Online]. Available: https://www.infosecurity-magazine.com/blogs/credential-stuffing-recent-attacks/. [Accessed: 26- Sep- 2020].

[10] K.Boyarsky, "The 10 Best Video Meeting Apps", Owllabs.com, 2020. [Online]. Available: https://www.owllabs.com/blog/best-meeting-apps. [Accessed: 26- Sep- 2020].

[11] J. Wallen, M. Stephens, D. Penna, J. Kelly-Linden, M. Field and A. Gulland, "Hackers obtain Covid-19 patient database in protest at treatment of Indian health workers", The Telegraph, 2020. [Online]. Available: https://www.telegraph.co.uk/global-health/terror-and-security/hackers-obtain-covid-19-patient-database-protest-treatment-indian/. [Accessed: 26- Sep- 2020].

[12] S. Butler-Hassan, "Motives unclear as cyber attack shuts down RMC network", Kingstonist News - 100% local, independent news in Kingston, ON, 2020. [Online]. Available: https://www.kingstonist.com/news/motives-unclear-as-cyber-attack-shuts-down-rmc-network/. [Accessed: 26- Sep- 2020].

[13] S. Turner, "386 Million Records from 18 Companies Leaked for Free", Fighting Identity Crimes powered by EZShield, 2020. [Online]. Available: https://www.fightingidentitycrimes.com/18-companies-368-million-records-data-breach/. [Accessed: 26- Sep-2020].

[14] S.Gurubaran, "Microsoft's GitHub Account Hacked - 500 GB Of Microsoft Data Exposed", GBHackers On Security, 2020. [Online]. Available: https://gbhackers.com/microsofts-github/. [Accessed: 26-Sep- 2020].

[15] "Intrusion Detection & Prevention | Systems to Detect & Prevent Attacks | Imperva", Learning Center, 2020. [Online]. Available: https://www.imperva.com/learn/application-security/intrusion-detection-prevention/. [Accessed: 01-Oct- 2020].

Authors -

Oluwatobi Akinmerese bagged his MSc. in Information Technology in the year 2016. He was also awarded a bachelor's degree in Electrical/Electronics Engineering in 2009. He currently works as a Lecturer in Crawford University, Igbesa, Ogun-state. He is currently on his doctoral studies at Babcock University, Ilishan-Remo, Ogun State. His research interests includes Cyber Security, Computer Networks and Telecommunication.

Olamide Kalesanwo is a PhD holder in the field of Artificial Intelligence. His research interest spans beyond AI and also covers fields such as information security and Data Science. He has several publications t his name. He is a member of Nigeria Computer Society (NCS) and Data Science Nigeria (DSN).