Cybersecurity Report

PSCI/BIT/CS 4164

Future of Security

Gisselle Cruz

David Armah Jr

Shashank Gupta

Under the kind guidance of

Dr. Brantly

College of Integrated Science

Virginia Polytechnic Institute and State University Blacksburg, Virginia

September, 2021

Table of Contents

Introduction

About

Hello readers, welcome to our Cybersecurity report. Our team created this report in hopes of educating Virginia Tech students on major cybersecurity related problems and how they are affecting lives all across the world. Throughout the entirety of the report, we will first introduce such problems, then take a look over data we have collected from a variety of different sources, and we will attempt to also analyze and discuss such data,as a way to take an in-depth dive into how impactful such cybersecurity problems have been over the years. These days anyone from governments to just script kiddies with enough time and money on their hands are able to take up hacking into some of the world's largest corporations. Facebook recently had their DNS taken off of the internet for almost an entire day and within 2020 Twitter was able to have some of its highest profile accounts hacked by somebody who basically learned how to use a phone correctly. All it took for someone to run a bitcoin scam on 4 of the biggest twitter accounts was a phone call to pose as a tech support employee who needed to run diagnostics on Twitter in order to trick the people into giving him full control over these accounts. The point being is that cybersecurity is more than just knowing how basic networking structures are, it is understanding how social engineering is used in order to achieve your objectives without them realizing. However, that is not to discount the software that is used in cyber attacks. We will explore different kinds of malware and what social engineering techniques are used to have an actor achieve their objectives despite having systems and people in place to stop them.

About the Authors

David Armah Jr.

A senior at Virginia Tech majoring in Computational Modeling and Data Analytics with a concentration in Cybersecurity/Cryptography, minors in Computer Science and Mathematics.

Gisselle Cruz

A senior at Virginia Tech majoring in Computational Modeling and Data Analytics (CMDA) with a concentration in Cybersecurity/Cryptography, also minoring in Mathematics.

Shashank Gupta

A Computational Modeling and Data Analytics major with a minor in Computer Science and Mathematics and a focus in Cryptography.

About the Class

Future of Security is a capstone class at Virginia Tech taught by Dr. Brantly that helps students identify and analyse real world security threats. These threats can be towards people, organizations, and nations throughout the world. Students in this course use problem solving methods, principals, and decision making tools to respond to conflicts, disasters, or attacks. In this course students are to create a Security Planner which helps the students of Virginia Tech navigate through the web safely, and protect their devices. This report is an explanation of the data visualizations used in the platform.

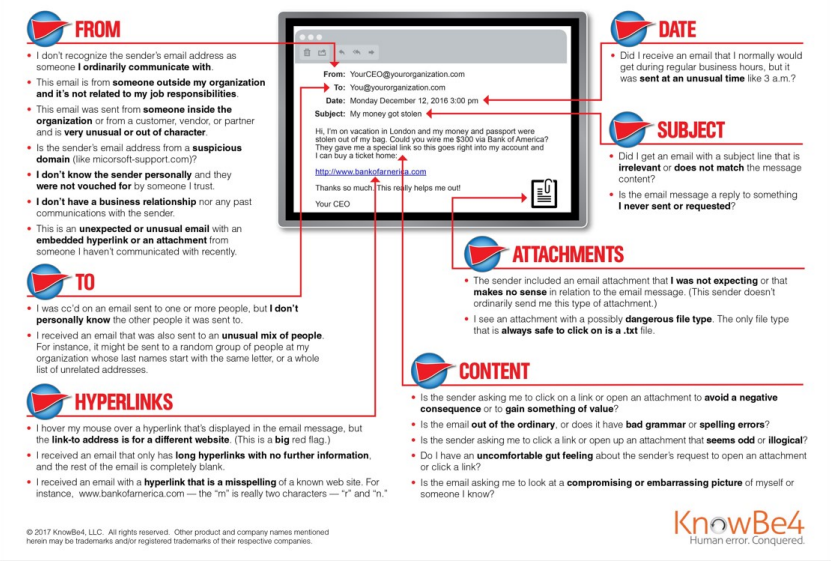
Phishing

What is Phishing?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Common features of phishing scams include eye catching or too good to be true claims of winning a prize of some sort. This can be a flashy image on the side of a website, which may also include some sense of urgency for example a countdown for how much longer the prize will be available. When being sent an email it can be from an unknown sender, which holds a link or attachment that one should not open.

Phishing is the most common ransomware attack vector due to the fact that most phishing attacks come from common things one sees or a known contact.



Example of Red Flags in an Email

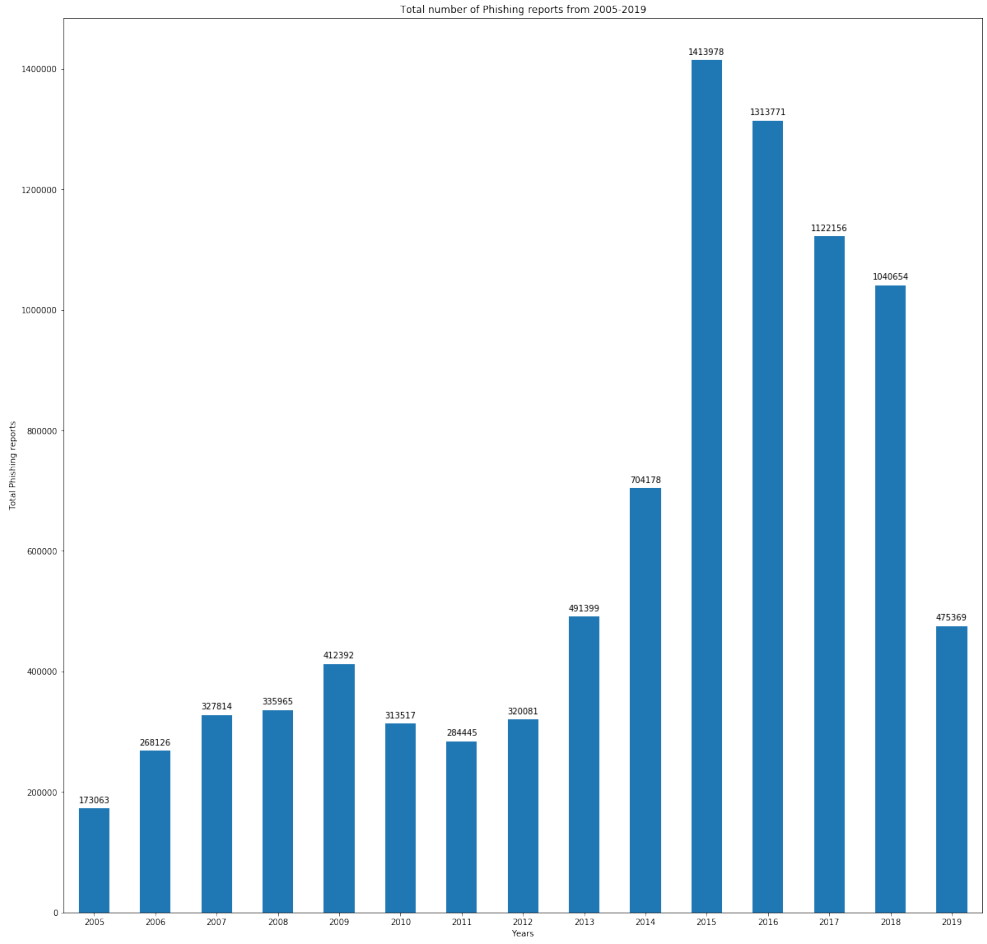


Figure 1: Phishing attacks from 2005-2019

Data Gathered

We were able to gather data from the Anti-Phishing Working Group (APWG). The main goal of APWG is to unify the global response to cybercrime through data exchange, research, and public awareness. The data illustrates the amount of phishing reports there were through the years 2005-2019. As seen on the graph, these numbers go up to the billions.

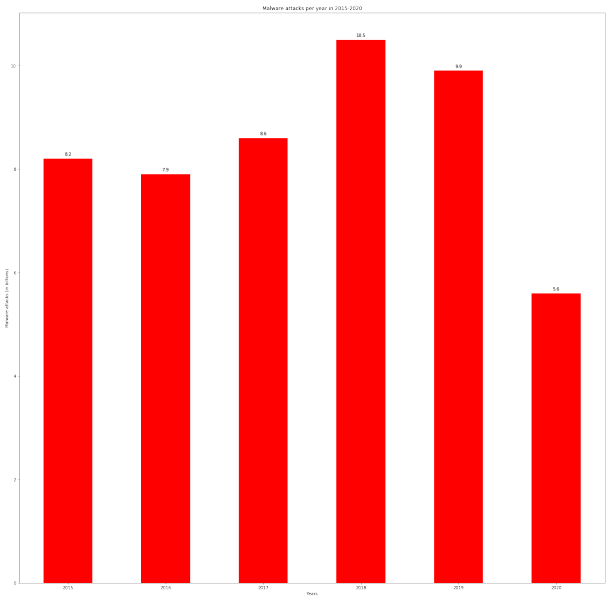
Analysis of Data

Looking at the data we gathered, we notice that the growth of phishing attacks has seen a huge increase from the initial year we collected data in 2005. Going from 170,000 to 14,000,000 in ten years can mean a lot of things. Over the years more and more people got introduced to the ideas of smartphones and started using more technology that would be used day to day. Since this technology was fairly new, most people were not educated on internet safety, this then leads to users clicking mysterious links that were sent to them or on a website. Looking at 2015, this is where phishing attacks peaked. This was because about 85% of organizations throughout the country were victims to phishing attacks. This also makes sense as to why the numbers after 2015 are dropping. The numbers are still significant, but are not as significant as 2015. Organizations learned the effects of phishing and probably tried to mitigate the attacks by teaching employees internet safety.

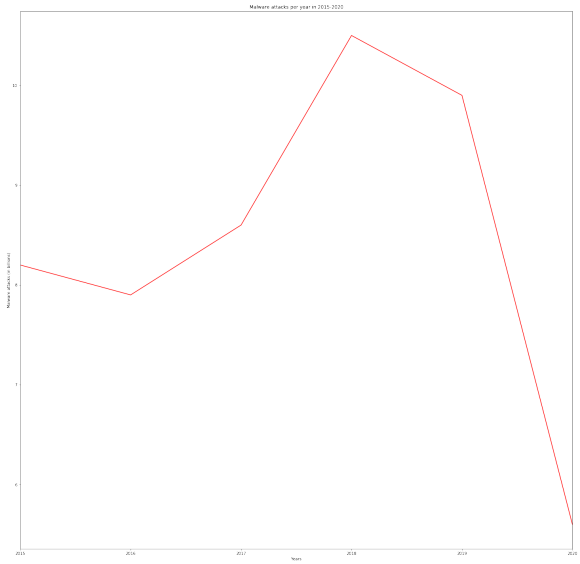
Malware

What is Malware?

Malware stands for "malicious software", this is software that is developed by cybercriminals or hackers to damage or destroy computer systems. In some cases the software is used to steal data from the computer and use it for their advantage. There are seven types of malicious software, Trojan, Worms, Virus, Spyware, Adware, Ransomware and Fileless Malware. Each of these types of malware infect a computer with the intent of retrieving data as quickly as possible before destroying the evidence of infiltration within the computer. When a device seems to work slower than usual, have a loss in disk-space, crashes and freezes, or has unwanted ads on a regular basis, there is a possibility of some sort of malware on the device. When suspicion of malware is on the device one can use antivirus software to help restore the device and remove the malware.



(a) Demonstration as a bar graph



(b) Demonstration as a line graph

Figure 2: Malware attacks in billions from the year 2015 to 2020

Data Gathered

This data was gathered from a study done by Statista based on the SonicWall Capture Labs. This data is based on the number of malware attacks worldwide from 2015-2020 in the billions.

Analysis of Data

Looking at the data we have gathered, malware attacks are still very prevalent in society. Over a 5 billion of malware's happen every year. From 2016-2018, malware attacks were consistently increasing per year, and then in 2019 and 2020, we noticed a significant decrease from the past trend. Although malware attacks have been decreasing as of lately, they still are a very big problem.

Although there was a significant drop in 2020, malware attacks have gone up over time during 2016-2019.

Ways to respond to malware attacks

Data Breaches

What are Data Breaches?

Data breaches are essentially a use of phishing, malware, and other malicious cyber tactics to gain Personal Identifiable Information(PII) or corporate data for the hackers own gain or to cause harm. PII is information like names, date of birth, social security number, email address, telephone number, and banking accounts. [**breach1**] The common causes of these data breaches include having security vulnerabilities that go undetected or unfixed for a long period of time. Human error is also a reason why data breaches occur, this is mostly because of the use of weak passwords or a mistake by someone abusing the systems for personal gain. Another common cause of a data breach is physical theft. Stealing a thumb drive, laptop, phone, or server that holds sensitive information is a way to keep the data and not having to delete it.

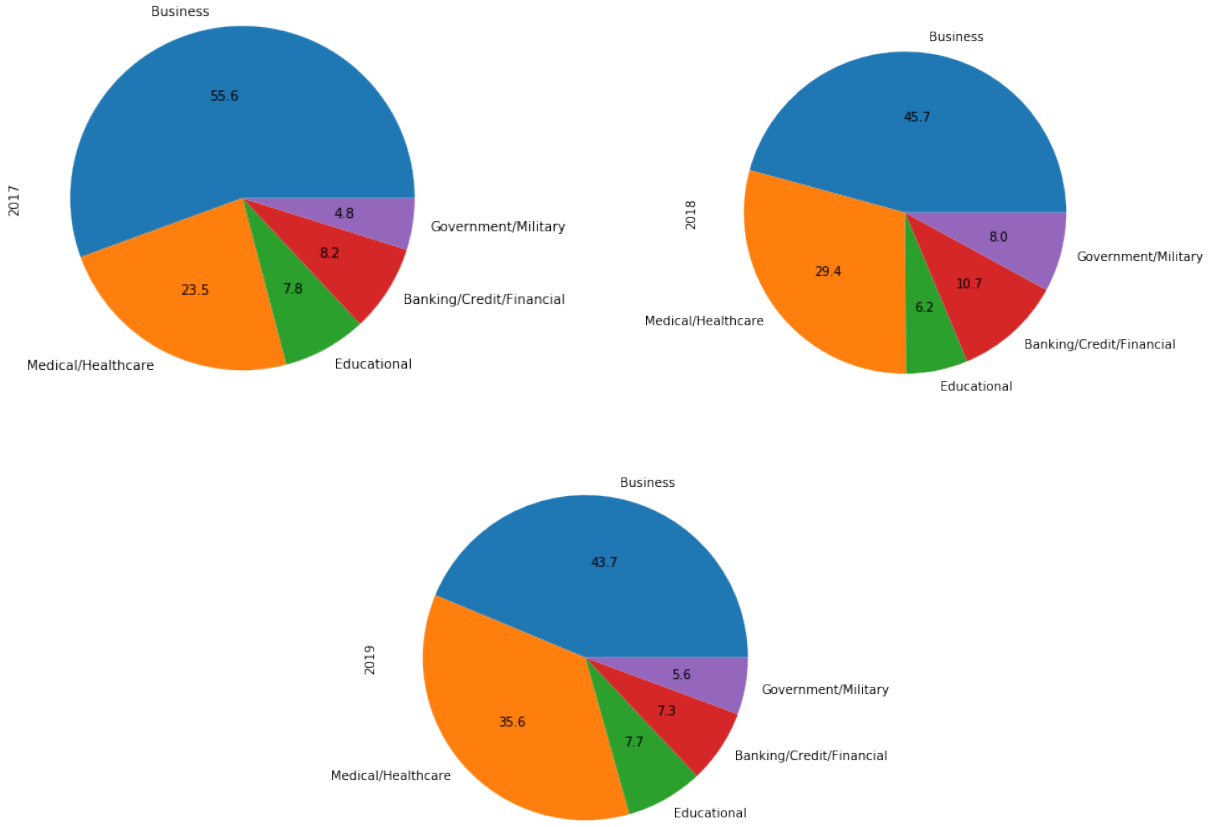


Figure 3: 2017, 2018, 2019 Pie Charts of Data Breaches by Industry

Data Gathered

The amount of data breaches from 2013-2019 were taken from a data base from Statista. This data shows how different industries have had their data breached. Industries such as businesses, Medical/Healthcare, Education, Banking/Financial, and Government/Military.

Analysis of Data

As stated in the gathered data section, there were statistics from 2013 to 2019. For this example we used the latest three years. As shown with the pie charts over the years, there has been a constant rate of data breaches throughout the last three years. Numbers fluctuate, but not as much. Businesses and the Medical industries are the ones who seem to get attacked the most. This may be because they have the most amount of PII. Healthcare and the medical industry are also most vulnerable with their information, millions of health care records have been stolen. Knowing that there are about 31.7 million small businesses in he United States, most small business owners don't know how to protect themselves from data breaches or underestimate the severity of it.

Conclusion

A Look to the Future

Looking into the future, we hope that the numbers of phishing attacks, malware, data breaches, and cyber attacks in general decrease. With more education and awareness of the internet and the dangers of these various cyber security related problems, we will slowly figure out ways to avoid and control the problems entirely. As we have seen with our data, industries get educated more on these unfortunate events and find ways to control it or avoid it. This can be done by training employees about the dangers of clicking a mysterious link, the dangers of having weak passwords, and the dangers of encountering malicious software.