CYBER SECURITY MADE EASY

OWN IT. SECURE IT. PROTECT IT.

Olawale Hassan

CYBERSECURITY MADE EASY

OWN IT. SECURE IT. PROTECT IT.

Olawale Hassan

To the poor and the busy who helped make this a success anyway

-@wallehazz

Contents

Introduction

Thank you for picking this book. I have had a thrilling and insightful experience researching and writing it and I hope you find it enlightening.

Cybersecurity Made Easy is my first book and I see writing on cybersecurity issues not only as an overdue necessity but also as a responsibility. We've come to find ourselves in a world where our dependence on technology cannot be overemphasized; our lives literally depend on it, our financial institutions, transport system, medical establishments. However, like every scientific and technological breakthrough that has contributed to human civilization, there will always be a downside – if it is not kept in check. Albert Einstein's relativity theorem, for example, has been applied to various fields of science and more specifically in nuclear power plants to power homes and industries. Significantly, however, the same theory played a vital role in building the atomic bombs dropped on Hiroshima and Nagasaki during the second world war. This points to the fact that technology, like the proverbial double-edged sword, with the capacity to make our lives easier could, in a matter of seconds, make it unbearable when not properly regulated.

About This Book

Cybersecurity Made Easy is your guide to identifying common cyber threats and protecting your digital identity and assets against such threats. This book intends to bridge the gap between the “not so tech savvy” and IT professionals. As a result of this, the first chapter has been dedicated to introducing the reader to the fundamentals of IT so if you find it too basic, don't hesitate to skip to the next chapter.

I hope this book will, at the very least, make the end users understand the threats and security issues that come with the ease and convenience of the internet.

Who is meant to read this book?

it wouldn't be an exaggeration to say “everyone should grab a copy” since we are in the digital age with everyone having one form of digital presence or the other. However, to be more realistic, you should read this book if:

- You have one form of digital identity or the other.
- You are a paranoid internet user who is very much concerned about your online safety and data privacy.

- You own or work in an institution or organization with devices plugged into the internet.
- You are an IT professional who needs to carry the executives along.

Chapter Overview

Part I

Chapter 1: This chapter titled “Getting Started” introduces you to the fundamentals and functionalities of the internet as well as the definition of common terms in information technology. If you are new to IT, this is the place to start

Chapter 2 covers the fundamentals of cyber threats.

Chapter 3 covers the concept of Cybersecurity, the CIA triad as well as data privacy regulations

Part II

The second part of the book focuses on the common cyber threats against individuals, small businesses and large organizations. Each chapter entails definitive guide to a threat, its mode of operation, countermeasures and case studies of real-life incidences of such threat.

Part I

Chapter One:

Getting Started

To fully understand cyber threats and appreciate the importance of cybersecurity as well as the need for it, you need to first understand a few concepts about the internet. These concepts are the bolts and nuts holding the internet in place.

The internet has transformed the world from an analog to a full-fledged digital arena; there is absolutely no aspect of life that it doesn't touch. Undoubtedly, it's the fastest means of information gathering and dissemination, with billions of interconnected devices communicating with one another and transmitting one form of data or the other through social media, blogs, and other web services. It’s a world on its own.

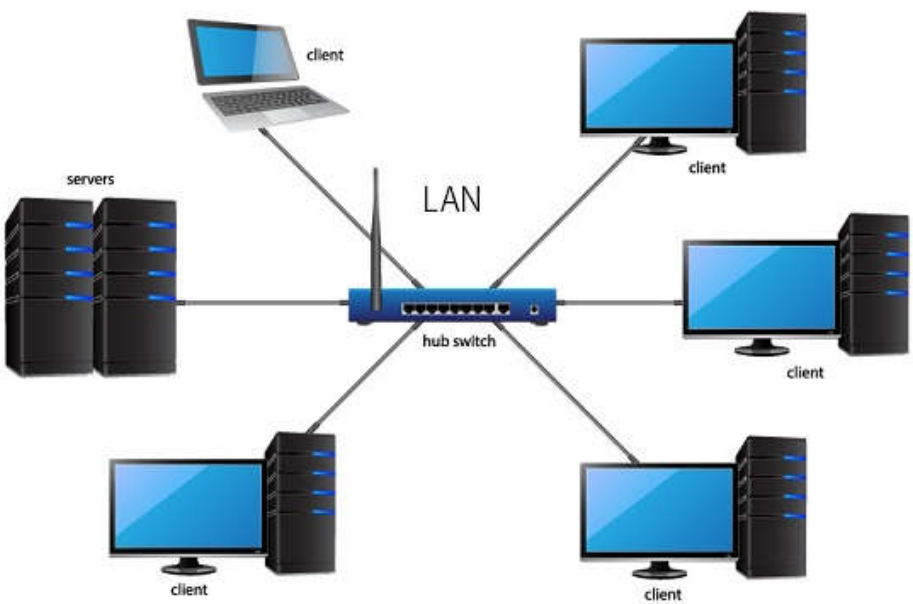
Types of Networks

A network is a connection between two or more computers either by cable or wirelessly, created in order to share resources such as expensive hardware, software, services, and files.

Unless an attacker has physical access to a computer, it would be impossible to compromise it or exploit any vulnerability it might have. In order to hack a system remotely, it has to be a node on a network, be it in the same building or halfway across the globe. There

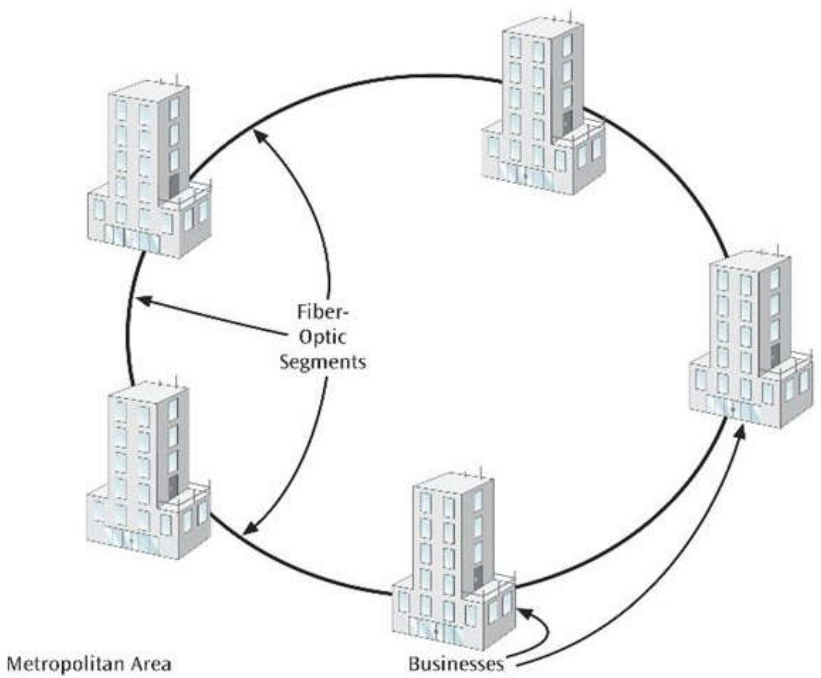
are different types of networks, classified in terms of their magnitude.

Local Area Network (LAN): A LAN network is a collection of locally connected computers and devices such as printers and scanners that depends on a network device called switch to communicate and share services. This type of network is commonly used by small offices and organizations mostly in a single building.



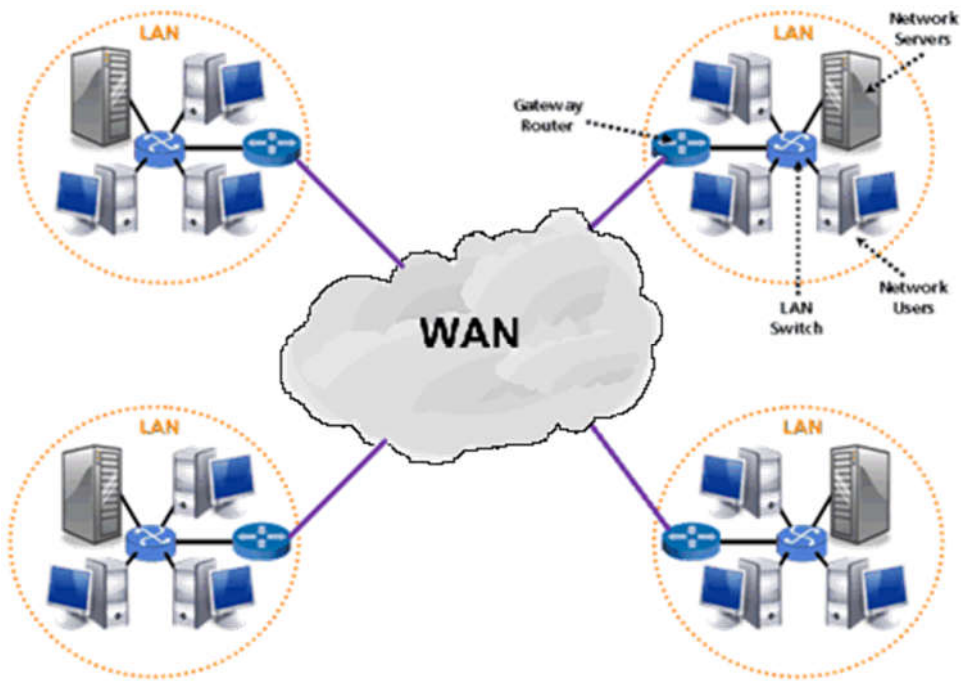
Source: Gomintekno

Metropolitan Area Network (MAN): A MAN network is a computer network interconnecting device in a geographical region of the magnitude of a metropolitan area. Though similar to a LAN network, it spans across an entire city or campus and is usually created by forming multiple LANs.



Source: https://slideplayer.com

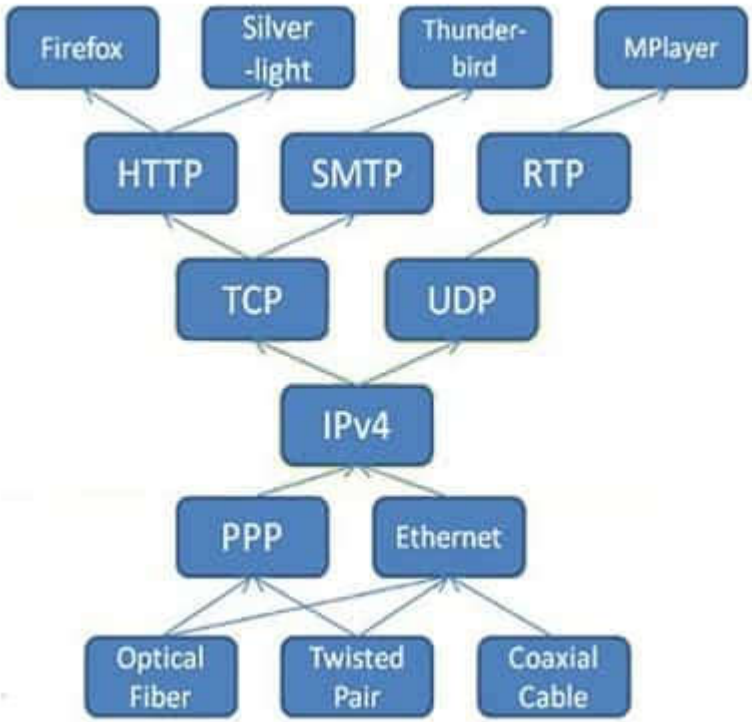
Wide Area Network (WAN): This network is a collection of interconnected LANs that span across long distance like different cities and geolocations. They are wider than MAN and as a matter of fact, the internet is the largest WAN network. WAN networks are owned by large corporations and governments.



Source: medium.com

Network Protocols

Just as different human cultures have their own ways of greeting and communicating like shaking, kissing on the forehead or both cheeks, and doing it wrong could mean you'll have a short and unpleasant stay as a visitor, the same thing applies to our networked devices. In order for interconnected devices of different vendors to communicate and run flawlessly, there are certain established rules on which processes run. These rules are called protocols. Protocols make sure that no matter how dissimilarly manufacturers build their product and devices, they will still communicate fine since the protocol makes them follow some similar guidelines. Examples of these protocols are TCP/IP internet protocol, the TCP and UDP transport layer protocols

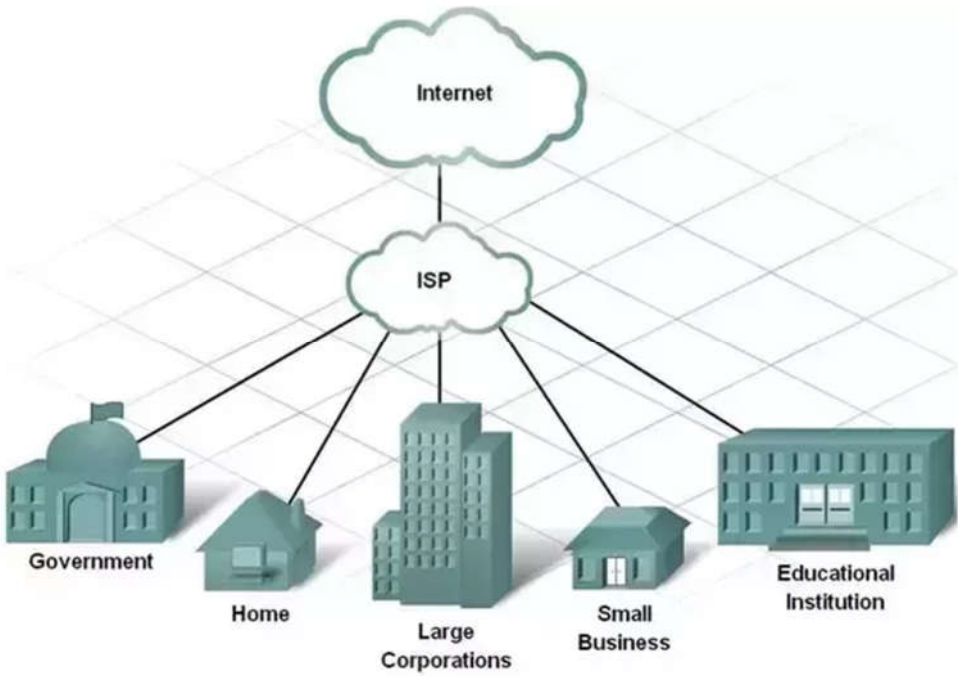


Source:TricksWay.com

ISP

In order to connect to the internet and start surfing the web, sending those emails and booking that flight ticket, you need an ISP to provide you with internet connections. An ISP (Internet Service Provider) is any organization that provides services for accessing the

internet. Services provided by ISPs include internet access, domain name and internet transit.



Source: https://www.quora.com

IP Address

An IP address is a unique 32-bit address that is automatically assigned to every computing device such as smartphone, iPad and personal computers in order for such device to be identifiable over the internet.

The IP address is a 32-bit number divided into four octets with each octet separated by a dot. Each octet has values ranging from 0-255 representing 8-bits of numbers the first version of the IP address scheme is called IPv4 is with some 4 billion (232) addresses and is of the form xxx.xxx.xxx.xxx, for example, 192.168.10.44. An Ipv4 address is divided into two parts, the network portion, and the host portion. An Ipv4 address' host part and network part can be identified simply by finding what class of IP address it is.

We are fast running out of Ipv4 IP addresses as many devices are coming online daily. In order to combat this issue, a new generation of IP addressing which is the Ipv6 has been implemented. However, an in-depth discussion of Ipv6 is beyond the scope of this book.

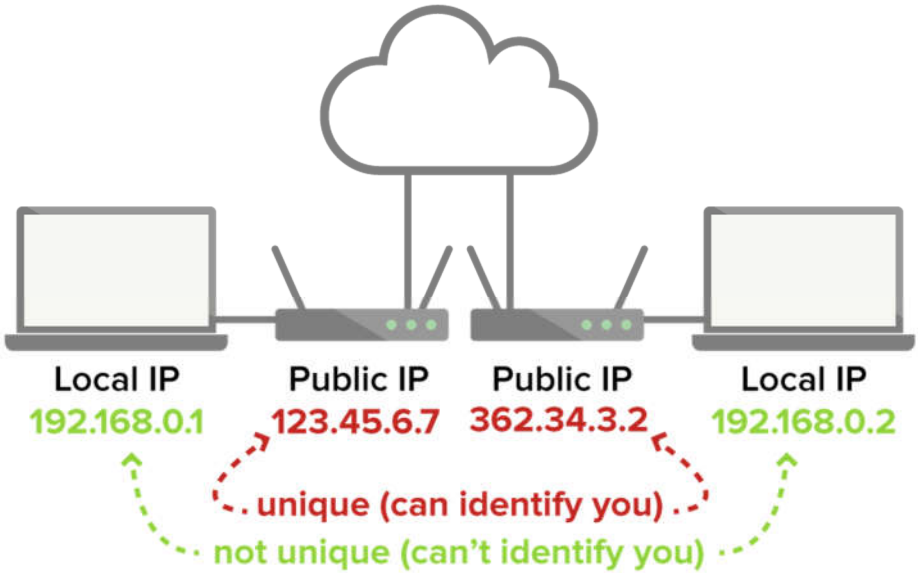
Types of IP Addresses

One way of classifying IP addresses is by the duration assigned by the ISP. Usually when an IP address is allocated to a user, it is commonly leased and tends to expire after a period of time. However, IP addresses are classified into two types depending on whether you are a large business enterprise running a web service that needs to have a static IP address so users can easily find you or just a normal internet user who doesn’t care much about what IP address is assigned to them or when it expires.

Static IP addresses: this is a permanent IP addresses assigned to an organization or individual by the ISP. Organizations that run web services needs to have a static IP address so users can easily reach them without issues.

From a security perspective, having a permanent IP address can make an organization easy to find and attack but there are certain techniques and software like firewalls, IDS and IPS that prevents, or at least mitigates, the effects of an attack.

Dynamic IP Addresses: A dynamic IP address, unlike the static IP address, is a temporary address that changes periodically and can be assigned to any user. Apart from static IP addresses assigned to organizations on request, other internet connected devices such as smartphones, laptops and IoTs have IP addresses assigned dynamically.



Source: https://www.expressvpn.com

The Internet

The internet is the largest network of interconnected LANs and WANs. It's a global system of various unified computer networks belonging to government bodies and private organizations. This fact indicates that though managed, the internet doesn't belong to any central authority and cannot be shut down as a whole although organizations and governments may decide to pull the plug. This action only affects a minuscule section of the entire internet. Of course the internet is just a combination of connected computers and network devices communicating with one another and its real

strength lies in the complexity of various services and applications (like online shopping, social networking, email services, video/audio conferencing, online gaming and ecommerce, to name a few) running on it.

Chapter Two:

Cyber Threat

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

In the last few decades, the world's most valuable resource has been oil and that had greatly improved the economy of oil-producing countries through revenues, aiding job creation and strengthening international bonds but today the world is looking for alternatives to fossil fuel and adopting renewable sources of energy like wind and solar. Now the world's most valuable resource is data, be it raw or refined. Data holds priceless details and information about an individual, organization, competitor and national government. Hence the quote "data is the new oil".

Just as challenges like oil spillage and gas flaring occurs in the oil and gas sector, there are certain challenges facing the digital world as well. The most challenging being data protection and privacy.

Cybercrime is a global problem that is almost as old as the internet itself. It poses a threat to individual's personal data and identity and

even more threat to large corporations, governments, and institutions worldwide as single cyber-attack could send an organization into oblivion.

Now with technology changing so fast, cybercrime and cyber-attacks are becoming more sophisticated than ever before with malicious hackers forming crime rings and creating stronger security-proof tools and techniques. These cybercriminals attack individuals for different reasons be it for personal gain, to sell trade secret to competitors, protest against the government actions or inactions or just for the fun of it and that's where cybersecurity comes in but before going into cybersecurity, we need to understand what cyber threats are.

Cyber Threat

A cyber threat is a malicious action attempted or carried out against an individual, government or organization in order to steal, damage, manipulate data or utilize the resources of such body in carrying out more attacks.

Sources of Cyber Threats

Like any kind of attack, there is always a motive; either to settle old scores or for personal gains. Some of the most common sources of cyber-attacks are:

Disgruntled Employee (Insider Threat): Cyber-attacks that originates from an insider are far more devastating and severe as the attacker always know a lot about the internal operations of the organization. An employee with opinions or perceptions different from that of the organization can go rogue, attack the organization from the inside and sell trade secrets to competitors. The story of Christopher Grupe is a good example to cite. Talking about the danger of a disgruntled employee, Grupe was a systems administrator for the Canadian Pacific Railway (CPR). In December 2015, he was suspended for subordination and when he returned to work, was informed he's been fired, effective immediately. Convincing the boss to let him resign instead, he used the time frame to access the company's networks, delete essential files and removed some admins' accounts and changed the password of others. After he was gone, the network began acting intermittently, and system admins found out they have been locked out and unable to attempt repairs. They eventually got in by rebooting and Grupe got a year in prison.

Terrorists/hacktivist: Sometimes, cyber-attacks originate from terrorist groups, rebels or Hacktivist who hack government facilities and public infrastructures such as power grids, power plants and websites to protest against certain action by the government and as a result persuade the government to do their bidding. A case study similar to this is that of 18-year-old Kane Gamble. By simple social engineering, Gamble gained access to data of top US intelligent officials including then-chief of the CIA, John Brennan; then-Director of National Intelligence, James Clapper; and Obama's deputy national security adviser, Avril Haines. Gamble was sentenced to two years in prison by a UK court. The Judge said Gamble engaged in "Politically motivated cyber terrorism" and this is just one of many cases of cyber hacktivism.

Cyber Crime groups: These are organized cyber groups who hack for the financial benefit alone. These are the ones who majorly attack banks and other financial institutions. This group is also responsible for conniving with internet fraudsters in scamming individuals, performing identity theft and swindling companies.

Comment Crew is a Chinese hacking group, also known as the Shanghai Group. Many believe they're responsible for a number of China's alleged cyber-attacks since 2006. One of their biggest, although not so well-known, successful hacking attempt was on the company Coca-Cola. They sent a malicious email from what looked

like Coca-Cola's CEO to the company's deputy president. Once opened, malware smoothly downloaded onto his computer. Thus giving the hackers full access to everything he typed, through the installation of a keystroke logger. The hackers had access to sensitive files for a whole month before the FBI informed Coca-Cola of the breach.

Competitors: Competition may get so bitter that a company may launch a cyber-attack against a rival company, not necessary to kick them out of business but to either steal product blueprints or organizational secrets so as to have the upper hand in the market.

A lot more was going on when Dejan Karabasevic left his job at clean-energy company AMSC to work for a Chinese wind-turbine company Sinovel. While at AMSC, Karabasevic has had access to company's proprietary technology for wind turbine efficiency. Karabasevic didn't just got a job offer from Sinovel, he was recruited by the company which was one of AMSC's largest customers. He was asked to bring the software with him and when he left, he had secretly downloaded the code to an offsite computer. After implementing the code, Sinovel retrofitted its wind turbines with it, thereby saving itself $800 million price tag which would have otherwise been charged by AMSC. The theft was later detected and the estimated loss was more than $1 billion in shareholder equity and almost 700 jobs.

National Governments: The act of a government launching a cyber-attack against the facilities of another government is referred to as cyber warfare. This could be as a result of a government finding the policies or actions of another government threatening. A good example of such cyber-attack is the Iran's Nuclear Centrifuge sabotage by the Stuxnet malware.

Effects of Cyber Attacks

There are many effects that cyber-attacks have on individuals, organizations and government bodies. Some may be harmless while most are life threatening.

Psychological: One of the effects of a cyber-attack is that it leaves the victim psychologically imbalanced and exasperated. For instance, an individual whose bank account was hacked and had his credit card used in the purchase of firearms on the dark web. Apart from the financial crises, he could also be arrested if the transactions are traced back to his account.

Another scenario is an individual having his/her identity stolen either by being impersonated or as a result of one of his/her social media accounts being hacked. This clone could use the victim's identity for malicious purposes such as tricking the victim's friends

into making fund transfers to his account or posting socially unacceptable messages.

Economic: The economic effects of cyber-attacks are always devastating either for individual, financial institutions or government. In late 2013, a large retailer store, *Target*, sustained a massive cyber-attack that led to the loss of almost 70 million customers' credit card information and other data. The aftermath was costly. On the day it went public with news of the breach, *Target* lost US$ 890 million in market value. The firm subsequently spent $100 million on improvements to its IT system and other tech upgrades. This doesn't include that fact that companies that get attacked faces sanctions by the government and are also fined as a result of the attack.

When government infrastructures are attacked then it's not always business as usual as the effects are seen on the stock market as well as in the economic situation of the nation.

Reputation: Trust is hard to earn, but easy to lose. When a financial establishment gets attacked then there is a high probability of it loosing not just its customers but also its reputation and reliability, and for this reason, most cyberattacks and data breaches are not reported and are only known by the concerned party.

Chapter Three: Introduction to Cybersecurity

With increase in cyber-attacks on government infrastructures, organizations and individuals, it is apparent that cyber threat is no more an issue for cybersecurity experts only but one that involves everyone and requires that all hands be on deck. We all have roles to play in the cyber-sphere and even though cyber threats cannot be completely eliminated, they can be mitigated.

Cybersecurity

As earlier mentioned, cyber threats are on the rise and their effects and aftermath are disastrous. Besides, with the adoption of new techniques by cyber criminals, cyber-attacks are becoming more threatening and sophisticated. To make matters worse, we now have the Advanced Persistent Threat (APT) which is the use of continuous hacking techniques to gain access to a computer network and remain hidden for a long time before finally striking or eventually being discovered.

In order to keep up with evolving threats and attacks, there is a need to create cybersecurity awareness. But what is cybersecurity?

Cybersecurity also referred to as information security can be defined as the practice of protecting personal data, systems, mobile devices,

IoTs and networks from all forms of digital attacks including but not limited to theft, damage and manipulation. Cybersecurity is comprised of a set of tools, methodologies and best practices designed to protect these assets.

In an organization, the people, processes and technology must all complement one another to create an active resistance from cyber-attack. An effective cybersecurity technique has several layers of defense spread across software, processes, computers and networks.

Source: https://www.lookingglasscyber.com

The Cybersecurity Triad

"CIA" to cybersecurity professionals doesn't mean the Central Intelligence Agency, rather in cybersecurity, CIA is a model used by security experts in the development of security policies and to help people think about various parts of cybersecurity.

A deep understanding of the cybersecurity triad is important in building more secure and robust software, web application and services as well as give your network framework a touch of resilience against the rising tide of cyber threats.

Then what does the CIA stands for?

C – Confidentiality

I – Integrity

A – Availability

Confidentiality

At the early stage of the internet and world wide web (www), most of the information on the internet were just static documents and were free for all who could access them but in today's world, with increase in confidential and vital information such as sensitive personal

details, trade secret and military strategies being stored and transferred between networks online, there comes the need to secure these data from unauthorized access.

Confidentiality deals with ensuring that only individuals who should have access to a piece of data are the ones that actually do. This means safeguarding data from unauthorized access and preventing data breach within the organization. Some common means of managing the confidentiality of data include data encryption, requiring password and login credentials, and setting file permissions on a Unix based system.

Integrity

The only thing that could be more threatening than having your confidential asset accessed is for them to be modified or worse deleted. Consider a nuclear power plant undergoing a cyber-attack and having its control unit hacked and tweaked by the attacker to run at maximum capacity, this slight modification could have a devastating effect and lead to emission of radioactive substances into the environment.

This is why integrity is important in cybersecurity and it means protecting data and infrastructure from any form of modification and

deletion by an unauthorized individual. Unintentional modification of such data by an authorized individual should be reversible.

Availability

Finally, the last of the triad is availability. Having your services and applications secured and free of modification isn't enough as they need to be accessible to the right people at all time. That means your organization should be resilient in the advent of a DDoS attack and be able to withstand other forms of cyberattacks that threatens the availability of the services provided by your organization.

Source: https://www.lbmc.com

Data Privacy & Data Protection

Not all cyber threats emanate from the black hat hackers, script-kiddies or the gray hat hackers for that matter. Poor data policies or deliberate trading of users' personal data on the part of trusted companies can also be a form of threat to an individual's digital privacy. How many times have you looked up an ailment online or chatted with a friend about a product and before you know it the only advertisements coming your way are about what you looked up or were discussing? Could this be a coincidence?

Data privacy is the aspect of information security that has to do with what data of an individual is collected, how such data is handled in transit, as well as how and with whom such data is shared.

Data Privacy Regulation

Fortunately, policymakers and government agencies are understanding the need for data privacy regulations as more and more social media companies are being sued over breach in privacy of users and organizations. An example was Washington DC, Attorney General Karl Racine suing Facebook for letting political consulting firm *Cambridge Analytica* access data from some 87 million Users who have an account with it.

General Data Protection Regulation (GDPR)

The GDPR is a data privacy regulation passed by the European Union Parliament in May 2018 to protect EU citizens' personal data. It doesn't matter where your organization is based as long as you have an EU citizen data in your possession, then the GDPR applies to you.

Violating the regulation could cost your organization up to 2% or 4% of your total global revenue or 10 million euro or 20 million euro, whichever is greater.

In summary (the list is pretty long and way beyond the scope of this book), to be free of sanctions from the EU concerning breach in GDPR:

- Consent should be sought before using an individual's data.
- Users' personal data should be up to date and correct.
- There should be transparency on how such data is going to be used.
- More than necessary data shouldn't be collected in other words, collect what you need.
- Stale and irrelevant data should be properly disposed and deleted.
- Personal data should be secure and encrypted while in rest.

- Users should have access to their data in your possession on demand and when requested users' data should be deleted.

Nigeria Data Protection Regulation (NDPR)

The NDPR was a data protection regulation issued by Nigeria's National Information Technology Development Agency (NITDA) in January, 2019. The regulation applies to all residents of Nigeria, citizens of Nigeria in diaspora as well as all organizations controlling or processing personal data of Nigerians. Many of the regulations in the NDPR emulates that of the EU's GDPR, however, the regulation states that any entity that violates the users' privacy rights will be liable to pay a fine of 2% annual gross revenue or 10 million Naira, whichever is greater or a fine of 1% or 2 million Naira for an entity dealing with less than 10,000 data subjects.

More countries and institutions are coming up with their own data privacy regulations to protect their citizens' and clients' vital credentials from misuse and theft like HIPPA (Health Information Privacy and Portability Act) for health care and GLBA (Gramm-leach Bliley Act) for financial institutions.

Part II

Back in November 1988, Robert Tappan Morris, son of the famous cryptographer Robert Morris Sr., graduate student at Cornell who wanted to know how big the internet was – that is, how many devices were connected to it. So, he wrote a program that would travel from computer to computer and ask each machine to send a signal back to a control server, which would keep count.

The program worked well – too well, in fact. Morris had known that if it traveled too fast there might be problems, but the limits he built in weren't enough to keep the program from clogging up large sections of the internet, both copying itself to new machines and sending those pings back. When he realized what was happening, even his messages warning system administrators about the problem couldn't get through.

His program became the first of a particular type of cyber-attack called "distributed denial of service," in which large numbers of Internet-connected devices, including computers, webcams and other smart gadgets, are told to send lots of traffic to one particular address, overloading it with so much activity that either the system shuts down or its network connections are completely blocked.

One thing you have to keep in mind the next time you surf the internet is that "the internet was not designed with security in mind". Of course, the internet still remains vulnerable to security breaches and it always will, the problem with the internet is that privacy and

security have been "bolted on". The internet with more than 3 billion users was never designed to be a secured system. "It was designed to be an open and fault-tolerant system" as said by Mikko Hypponen.

The unpredictability and insecurity of the internet only mean one thing, we will never get rid of cyber threats. Cyber threats are just like bugs and it doesn't take a seasoned developer to know that removing a bug only introduces another. Though the issue of a cyber-threat cannot be completely eradicated, it certainly can be mitigated by first knowing what a particular cyber threat is; secondly, knowing how the bad guys use this threat against you and lastly protecting yourself and your infrastructures against such threat.

In this part of the book, I explained the major and prevalent cyber threats, how these threats are weaponized against a user or system and how to protect yourself.

Chapter Four

Phishing Attack

I choose this as the first form of cyber threat to discuss due to the high rating it gets from security experts and the urgency with which it needs to be addressed. As a matter of fact, the moment you get the gist of this threat, put down the book (I know you don't want to but you have to) and perform a rigorous assessment on your accounts and systems to make sure you are not yet a victim.

Phishing is a form of social engineering where an attacker tries to appear legit in order to steal sensitive data and information from an unsuspecting user either by sending a link through mail or cloning a genuine website and tossing a bait to see who bites. Your whole network and physical infrastructure could be brought down in no time as a result of a phishing attack so you need to be on the lookout.

A phishing attack is the mother of all attacks as it could be the very payload in a cyber-attack as well as it could just be a vector component. There are different types of phishing attacks and they come in all shapes and sizes.

Clone Phishing

This used to be the common form of phishing until the other types showed up. That doesn't in any way mean it's no more effective as it's

still very well common on the internet and is getting add-ons and more sophisticated.

This type of phishing attack is one where an attacker clones a genuine and legit website like a bank portal, e-commerce website and then registers and hosts the fake website with a domain name similar to that of the genuine website (a process referred to as email spoofing) for example a legit website with domain name www.thisisreal.com could be clone-phished to something like www.thisisreel.com, www.thsisreal.com. Common victims to this form of phishing are people who are unconscious of what they are typing into the address bar of their browser.

Spear Phishing

Spear phishing is a form of phishing where an attacker aims an email with a link to a cloned or malicious website, virus, or ransomware executable file. It could also be an attached file. Most cyber-attacks are of this form but still get at staffs and employees as the sender's email address looks legit and genuine. Sometimes they find their way into your inbox and not the spam folder. Many large organizations and corporation with sophisticated security measures and elite security experts still fall for this attack.

Whale Phishing

Whale Phishing attack is similar to spear phishing with the only difference being that it's targeted on high profile employees such as the CEO himself, the CFO or even ironically the CSO. Targeting the head of an organization means targeting the organization as a whole since he has vital information concerning his business and employees. The magnitude of this form of phishing could be devastating and beyond remedy as sensitive information, trade secret, upcoming products and infrastructural blueprints gets exposed.

You can never be too careful when it comes to protecting yourself against phishing attacks. In order to know how to protect yourself against this form of attack, you need to know how it works.

As earlier stated, clone phishing is getting more difficult to detect as it is getting more sophisticated. Malicious hackers now use Greek letters that look similar to the English alphabets in order to be able to convince the victim that the website is genuine. How is this possible? When you register a domain no one else can use it as it has to be unique. But the tricky part is that digital characters may look alike, they, in fact, are unique and an attacker would utilize this feature to deceive his victim. So you may be looking at the address

bar with www.facebook.com displayed but in fact the letter "o" is the Greek alphabet "Omicron" with Unicode code U+03BF.

Source: https://www.totalhipaa.com

(in-depth discussion is beyond the scope of this book).

Phishing greatly on human psychology. An attacker will feed on human ignorance, emotion and greed to get them to click on

obviously suspicious links and even go to the extent of downloading an attached file.

Countermeasures

- One of the signs that an email has been laced with a form of phishing payload is that it arrives in the spam folder. Web servers nowadays have spam filters that automatically send emails from suspicious email addresses or addresses reported as spam to the spam folder. Simply disregard any mail from unknown and unexpected source especially when such mail contains an attachment.
- A genuine mail will probably address you by your first name, be wary of any email with "dear customer", "dear user" etc.
- Be on the lookout for spelling and grammatical error. A malicious hacker won't probably put much effort into this as much as any serious corporate organization would.
- If the email content is too good to be true, then it probably is. Nothing is free especially in the IT world; when someone is offering you a deal, look before you leap.
- The most effective technique you can employ to mitigate phishing attack in your organization is sensitizing your employees on

cybersecurity. Most people are oblivious of this threat or any other threat for that matter. Also sponsoring IT staffs to attend cybersecurity seminars and conferences to brush up their knowledge and other employees'.

- You can have your company implement a spam filter software which detects suspicious file attachments in emails. It also contains a database of known phishing email addresses, websites and IP addresses.
- Implement encryption for all your company's sensitive data. Best case scenario if you or one of your staffs eventually fall victim to phishing, all stolen data will be useless to the attacker.
- Hover over a link before clicking on it to make sure you are being directed to the intended website.

Canadian University Phished

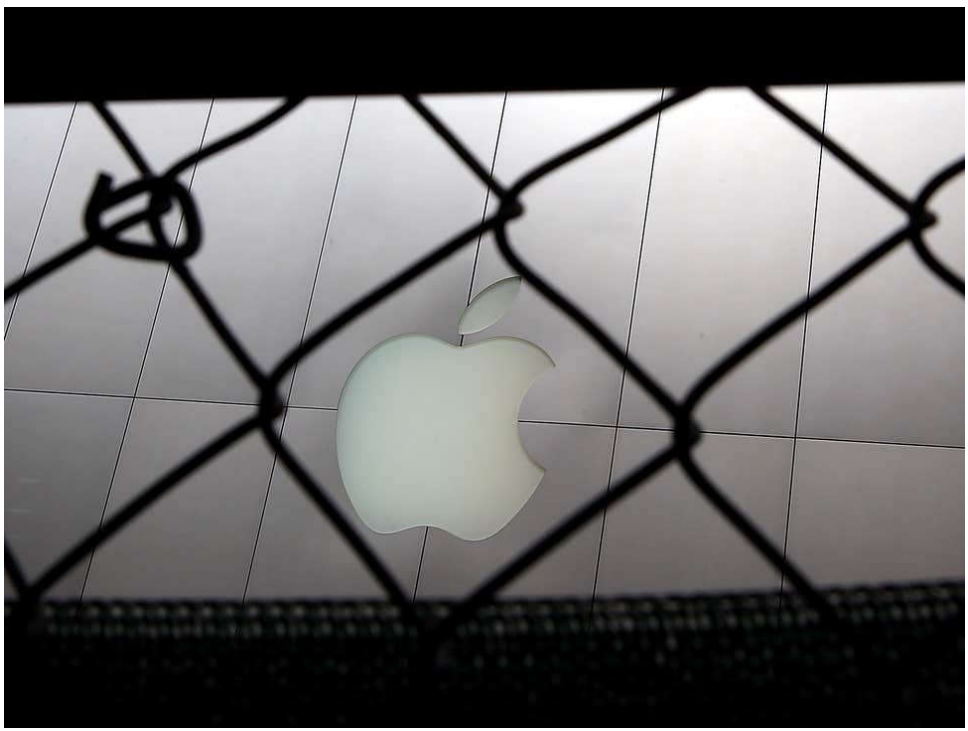
Source: https://www.bbc.com/news/world-us-canada-41116177

A Canadian university says staffers unwittingly lost $9.5m (C$11.8m; £7.5m) in an online phishing scam. Fraudulent emails convinced staff at MacEwan University that one of its clients was changing its bank account details. Staff then paid money into the fraudulently created account. The University, in Edmonton, Alberta, is auditing its business practices. Police have traced most of the funds to accounts in Hong Kong and Montreal, but no charges have been laid. The scam came to light when the real client complained of non-payment.

https://www.bbc.com/news/world-us-canada-41116177

August 2017

Apple ID Expiry Scam



Source: https://www.independent.co.uk

Apple users are receiving phishing messages designed to trick them into handing over their Apple ID passwords and other pieces of personal information. People hit by the scam usually receive an unsolicited message which claims to come from Apple, urging them

to immediately change their Apple ID password before it expires. Victims are then directed to an unofficial but legitimate-looking website like AppleIDLogin.co.uk, where they are asked to input their username and password.

https://www.independent.co.uk/life-style/gadgets-and-tech/news/apple-id-password-expired-expiry-text-website-scam-phishing-a6991126.html

April 2016

Phishing Attack Breaches Data of 30,000 Memorial Hospital Patients

Source: https://www.healthdatamanagement.com

An employee of Memorial Hospital at Gulfport, Mississippi fell victim to a phishing attack, which breached the data of 30,000 patients for more than a week in December. On December 17, officials discovered an unauthorized party gained access to an employee email account on December 6. The account was immediately secured, and an investigation was launched to

determine the scope of the incident. The investigation determined the patient data contained in the emails included names, dates of birth, health data, and or information about services received at MHG. For a limited number of patients, Social Security numbers were included in the breached data.

https://healthitsecurity.com/news/phishing-attack-breaches-data-of-30000-memorial-hospital-patients

December 2019

Chapter Five

Malware Attacks

Malware is a portmanteau word for *mal*icious soft*ware*. Malware is a piece of program written by a hacker with malicious intent of extracting sensitive data ranging from a user's computer or smart device to encryption of organization's vital document. There are different types of malware each with its own function and feature.

Ransomware

Ransomware also called scareware is a type of malware that encrypts and locks down a computer system. The malware is programmed to display a message instructing the victim to pay a certain amount as ransom in order to get the key to the encryption, Usually, a timer comes with it giving the victim an ultimatum and threatening to permanently delete the files if the ransom (usually in form of cryptocurrency) is not paid on time.

Virus

A virus is another type of malware. It's a written computer program which attaches itself to a genuine file and when triggered by an event specified by the coder it executes itself and like a biological virus

replicates itself destroying the affected files and rendering them useless.

Worm

This is a type of malware similar to a virus with the only difference being that a worm doesn't need to be triggered by any event to start deploying its payload. Once a worm gets into a vulnerable system or network infrastructure it starts replicating itself instantly.

Trojan

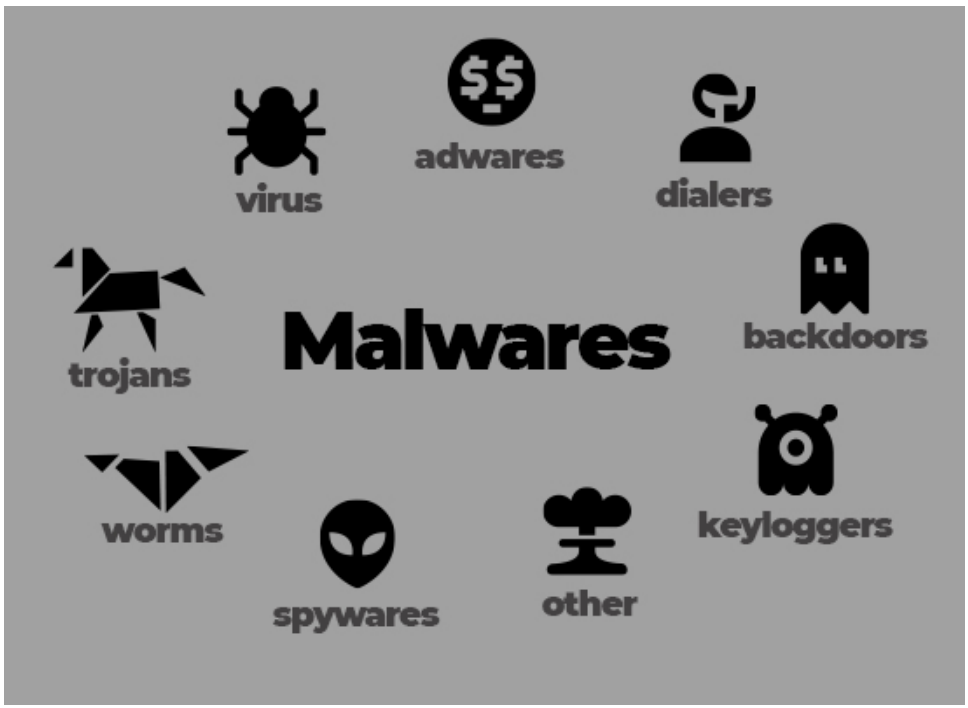
Also referred to as rootkit and named after the "*Trojan horse*" of Troy. This form of malware is very similar to that of Greek history. It is a computer program that appears legit and harmless but underneath is a malicious piece of software which when executed can have a devastating effect on the host system or network. Trojans usually create a backdoor on the affected system opening a portal for more damages; it could be in form of a game, or even worst even an antivirus software.

Adware

Not necessarily malicious or dangerous to the affected system, adware is a form of malware that typically bombards the infected system with advertisements of all kind, it has no perilous effect except for the fact that its pop-ups are irritating and annoying.

Spyware

Exactly what it sounds like, spyware is a piece of malware that hides itself on your system and spy on you, gathering the victim's sensitive data, taking screenshots, recording sounds, taking webcam images and sending it back to the hacker. A good example of spyware is a keylogger which records every keystroke and sends it back to a master source.



Source: https://enterprise.comodo.com

The most common way a malware is contracted is through the internet and clicking on malware-laden email attachment. Some malicious websites have JavaScript code snippet that execute the moment the web page finish loading meaning your organization's network could be compromised simply by one of its employees visiting a malicious website so you are more likely to get infected by a malware by clicking on links, downloading games, installing new toolbar or customized system theme from untrusted websites.

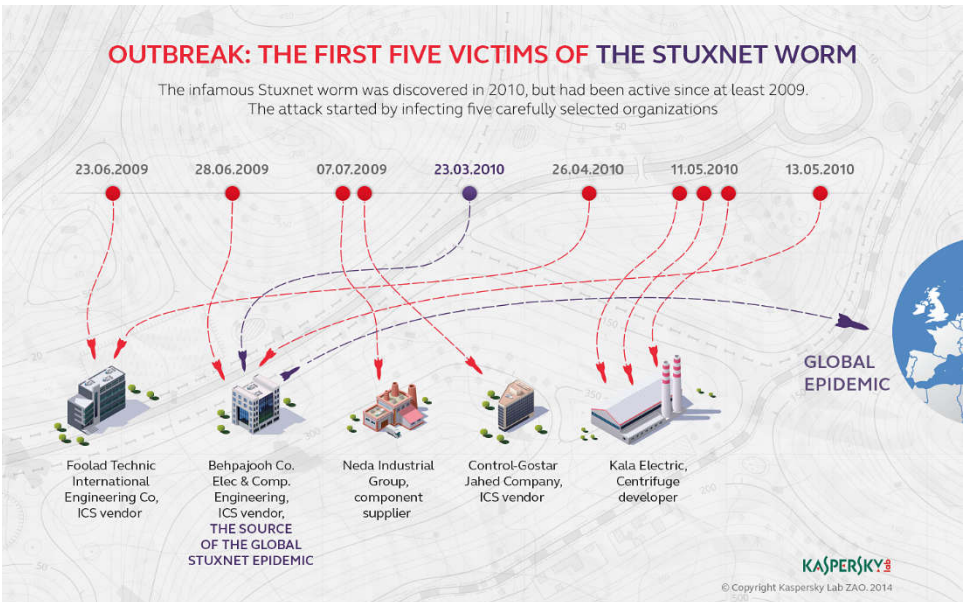
Likewise, you can get malware infection on your system or network by installing counterfeit computer software through an infected optic drive or flash drive.

Countermeasure

- When it comes to malware, human psychology always happen to be a key factor. More than half of malware infections requires human intervention to propagate, either having to click on a link or opening a file. To mitigate and curb cases of malware infections, organizations need to create awareness among their employees by organizing seminars and conferences.
- The next most important way to protect against or remedy a malware infection is to install an efficient antivirus software and keep it up to date at all time. I can't overemphasize the importance of antivirus software as it basically serves as a wall between your infrastructure and malware. Each malware has its own predefined technique of infecting and damaging its target's computer and data, these trails left behind by malware are called signatures and are what antivirus vendors use in counter-attacking malware infections and creating more sophisticated antivirus software.

- Strict security policies should be implemented both technically and administratively to avoid incidents of employees visiting malicious websites or inserting infected flash drives into the organization's system.
- If your home or office network recently recovered from a malware attack then it is highly recommended that you change passwords, pin codes and other sensitive data that the malware might have possibly had access to.
- Always have a routine backup of all vital data on your systems, it could vary from daily backup schedule to monthly backup. But the most important thing to keep in mind is that malicious malwares are getting more sophisticated and you never can tell when the next WannaCry will be launched.
- Don't be too good a Samaritan to the extent of inserting a flash drive you found in the lobby, parking lot or elevator into your system or office computer with the intention of finding the rightful owner.

Stuxnet Ramsomware Attack



Source: https://securelist.com

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It generated a flurry of media attention after it was discovered in 2010 because it was the first known malware to be capable of crippling hardware and because it appeared to have been created by the U.S. National Security Agency,

the CIA, and/or Israeli intelligence. Stuxnet reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the malware to target facilities including water treatment plants, power plants, and gas lines.

Stuxnet was a multi-part malware that traveled on USB sticks and spread through Microsoft Windows computers. The virus searched each infected PC for signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct.

https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/what-is-stuxnet.html

Uncovered in 2010, dates back to 2005.

WannaCry Attack

Source: https://en.wikipedia.org

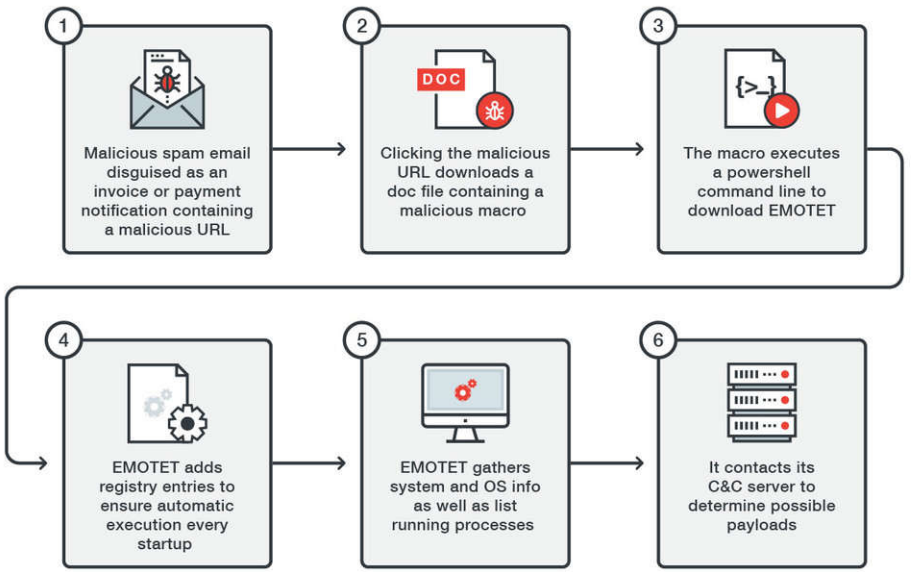
WannaCry is a ransomware attack was first seen in May 2017. Cyberattack by the WannaCry ransomware was a worldwide event which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an

exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was in organizations that had not applied these patches or were using older Windows systems that were no longer supported by Microsoft. WannaCry also took advantage of installing backdoors onto infected systems.

https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

May 2017

Emotet Banking Trojan



Source: https://www.njhomelandsecurity.gov

Emotet is a Trojan that is primarily spread through spam emails (malspam). The infection may arrive either via a malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. Emotet may try to persuade users to click the malicious files by using tempting language about "Your Invoice," "Payment Details," or possibly an upcoming shipment from well-known parcel companies.

Emotet has gone through a few iterations. Early versions arrived as a malicious JavaScript file. Later versions evolved to use macro-enabled documents to retrieve the virus payload from command and control (C&C) servers run by the attackers.

https://www.malwarebytes.com/emotet/

July 2014.

Chapter Six:

Social Engineering

As human, there are times when emotions such as love, fear, happiness get the better of us. In those circumstances, we tend to make *irrational* decisions under duress and this is the basic human psychology. This phenomenon is what social engineering attack exploits. A good example of this form of cyber-attack is the scamming technique used by Nigerian cyber criminals locally called *yahoo-yahoo*.

Social engineering is a form of cyber-attack where an attacker takes advantage of human emotion in making their target give up sensitive data like card details, password or company's secret information.

Pretexting

Pretexting is a form of social engineering technique where an attacker exploits human desire to trust. The attacker, usually a fraudster, builds an aurora of ingenuous trust and atmosphere of security in order to make his prey share private information or transfer funds. Pretexting takes a great deal of effort on the part of the attacker as a slight suspicion from the target could render the attack unsuccessful.

For example, after performing thorough investigation and research on a target company and discovering that although the company has

many branch offices, employees from one branch don't actually know much about employees from another branch. Taking advantage of this knowledge, an attacker could visit one of these branch offices, present fake, but convincing, documents claiming to be assistant manager of another branch and the next minute before suspicion is raised, he's already having tea with the manager of the branch.

Vishing

Vishing, coined from the words: voice and phishing is a form of social engineering attack where an attacker employs the use mobile phone to persuade his target into giving him sensitive personal data such as bank account details, security clearance code, or even residential address. Of course, an attacker would have done his homework before making the call so there is a high probability of his target falling for the con. Imagine receiving a phone call from an individual claiming to be from the Fedral Inland Revenue Services which he accurately stated that you visited a day before; he didn't ask for much, just your email address in order to send you monthly digest to keep you up to date on various activities by the agency, but from a cybersecurity standpoint, one of the most sensitive data a person could possess is your email address. With it, an attacker could perform further reconnaissance on you or your company.

Tailgating

This is another form of social engineering where an intruder follows (tailgates) an employee of a company into a restricted area that needs security clearance to pass through. In order to seem convincing, the intruder may intentionally carry heavy contents and as a compassionate being, the employee is likely to hold the door which usually requires a biometric identification to pass through for the intruder. The intruder now has access to sensitive company assets after gaining entrance into the facility.

Reverse Social Engineering

In this form of attack, you actually end up contacting the intruder. How so? An attacker could send you a mail claiming you have won a prize and that you should contact the number in the mail to redeem your prize.

Countermeasures

- As earlier stated, most social engineering attacks scale through due to human psychology. You can spend millions on security solutions such as firewalls, IDS, IPS but without creating a solid social engineering awareness among employees, your infrastructure is likely to get hit by a cyber-attack.
- As an individual, challenge unfamiliar and suspicious personalities in your institution. It's a 50/50 game so you can get the upper hand by asking further questions concerning a stranger's claim.
- Have your trash disposed-off by professional bodies or create a shredding area within your premises. You shouldn't be surprised that sensitive credentials are usually found in dumpsters.
- Always confirm that calls are from the acclaimed sources. With the advent of deep fake, it easy for attackers to mimic voices of key players in an organization and issue fraudulent commands.
- Don't let greed get better of you. Turn down offers that are sugar coated and too good to be true because it probably is.

Etherum Social Engineered

Source: http://giftout.co

Several people lost thousands of dollars in cryptocurrency after the Ethereum Classic website was hacked in 2017. Using social engineering, hackers impersonated the owner of Classic Ether Wallet, gained access to the domain registry, and then redirected the domain to their own server. Criminals extracted Ethereum cryptocurrency from the victims after entering a code on the website that allowed them to view private keys that are used for transactions.

https://gatefy.com/posts/7-real-and-famous-cases-social-engineering-attacks/

July *2017*

Ubiquiti Breached

Source: https://www.hellotech.com

Ubiquiti Networks, a manufacturer of technology for networking, lost almost $40 million dollars, in 2015, after a phishing attack. It's believed that an employee email account was compromised in Hong

Kong. Then, hackers used the technique of employee impersonation to request fraudulent payments, which were made by the accounting department.

Date reported: August 2015

2016 Election Warm-up

Source: https://gcn.com

One of the most iconic cases of social engineering is the United States presidential election in 2016. Spear phishing attacks led to the leak of emails and information from the Democratic Party that may have influenced the result of the election resulting in Donald Trump's

victory over Hillary Clinton. Hackers created a fake email from Gmail, inviting users, through a link, to change their passwords due to unusual activity. Fraudsters then had access to hundreds of emails containing sensitive information about the Clinton campaign.

https://gatefy.com/posts/7-real-and-famous-cases-social-engineering-attacks/

2016

Chapter Seven: Man in The Middle (MITM)

When it comes to protecting your personal or organization's sensitive credentials from hackers while in transit, then a man in the middle attack is a must know for you.

A man in the middle attack is a form of cyber threat where an intruder intercepts communication between two parties and monitors or manipulates the exchanged information for malevolent intent.

In a man in the middle attack, an attacker pretends to be both the client and the server, they both think they are communicating with each other but in reality, every data sent to the client from the server passes through the attacker where it gets manipulated and vice versa.

Evil Twin

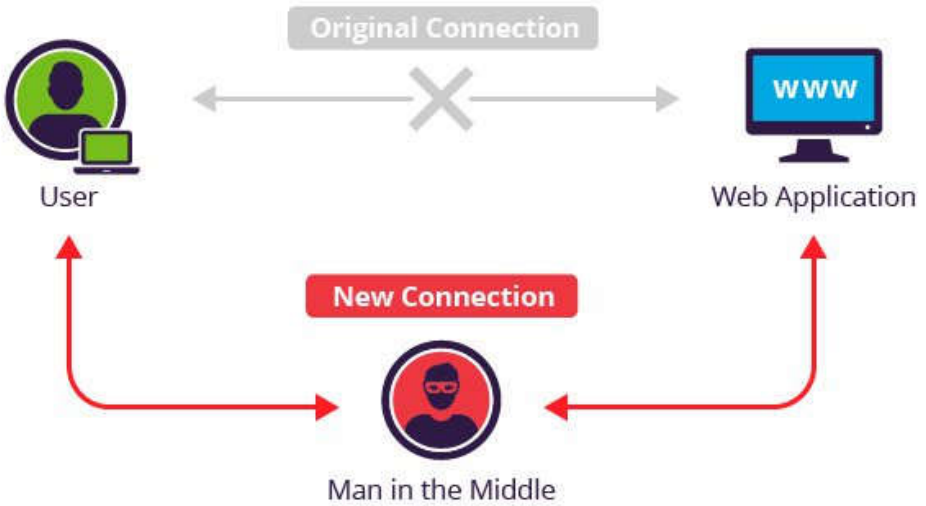
Also known as Wi-Fi eavesdropping, this is a form of a man in the middle attack where a malicious hacker creates an open Wi-Fi network to lure unsuspecting victims into connecting and thereby intercepting their connection and collecting every sensitive data transferred during their connection. This form of a man in the middle attack is usually common in areas where people get free Wi-Fi connections like malls, airports and cafes.

IP Spoofing

IP spoofing is a form of cyber-attack in which an attacker disguises as a legitimate user that is allowed in a network. Some organizations have a way of restricting access to services and vital documents by allowing only certain IP address ranges through the firewall. In order to overcome this restriction, an attacker spoofs an IP address from the address range and sends requests to the server, which in return reply those requests thinking it originated from an authenticated user.

Sniffing

This is a passive form of a man in the middle attack where an attacker connects to a network in order to grab sensitive data being transmitted by unsuspecting victims as they flow through the air or cable by using already made packet sniffing software such as Wireshark Ettercap and the likes.



Source: https://mind42.com

Countermeasures

- Nothing is free. In other words, *quid pro quo* (something for something). Free and open internet connections in public places are usually not recommended for use as most of them are honeypots created to lure and grab sensitive user data. Avoid them as much as possible.
- When browsing the web and submitting sensitive credentials, it's important to make sure that SSL is implemented by the website being browsed. To know if this security feature is being used, you

can look out for a green lock icon in your browser's address bar or HTTPS protocol in the same area. If this is the case packets moving from your browser to the server will be in an encrypted format and not in plain text so even when these packets are intercepted and sniffed, they will be useless to the attacker.

- Pay close attention to browser warning about a website you are browsing being insecure. Mostly when a man in the middle attack is being used against a user, the attacker tends to redirect the victim to a cloned website.

NSA Disguised Itself as Google to Spy

Source: https://www.motherjones.com

In a Brazilian television report disclosure was made that the NSA had impersonated Google and possibly other major internet sites in order to intercept, store, and read supposedly secure online communications. The spy agency accomplishes this using what's known as a "man-in-the-middle (MITM) attack," a fairly well-known exploit used by elite hackers. This revelation adds to the growing list of ways that the NSA is believed to snoop on ostensibly private online conversations.

https://www.motherjones.com/politics/2013/09/flying-pig-nsa-impersonates-google/

January 2013

Spammed by Comcast

Source: https://wordtothewise.com

Comcast was once using packet injection to push its own ads via Wi-Fi, though, the issue poses no threat other than annoyance. One facet of it is designed to alert consumers that they are connected to Comcast's Xfinity service. Other ads remind Web surfers to

download Xfinity apps, Comcast spokesman Charlie Douglas told Ars in telephone interviews.

The advertisements may appear about every seven minutes or so, he said, and they last for just seconds before trailing away. Douglas said the advertising campaign only applies to Xfinity's publicly available Wi-Fi hot spots that dot the landscape. Comcast customers connected to their own Xfinity Wi-Fi routers when they're at home are not affected, he said.

"We think it's a courtesy, and it helps address some concerns that people might not be absolutely sure they're on a hotspot from Comcast," Douglas said.

https://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/

2014

Nokia Browser Decrypting Traffic

Source: https://www.extremetech.com

In late December 2012, security researchers discovered that Nokia's Xpress Browser was redirecting traffic to proxy servers. They get redirected to Nokia/Ovi proxy servers if Nokia browser is used, and to Opera proxy servers if Opera Mini browser is used. The disturbing part of his report was evidence that Nokia is not just proxying traffic, but actually decrypting the HTTPS traffic. Nokia replied with a statement:

"We take the privacy and security of our consumers and their data very seriously. The compression that occurs within the Nokia Xpress Browser means that users can get faster web browsing and

more value out of their data plans. Importantly, the proxy servers do not store the content of web pages visited by our users or any information they enter into them. When temporary decryption of HTTPS connections is required on our proxy servers, to transform and deliver users' content, it is done in a secure manner.

Nokia has implemented appropriate organizational and technical measures to prevent access to private information. Claims that we would access complete unencrypted information are inaccurate.

We aim to be completely transparent on privacy practices. As part of our policy of continuous improvement we will review the information provided in the mobile client in case this can be improved."

https://freedom-to-tinker.com/2013/01/11/how-the-nokia-browser-decrypts-ssl-traffic-a-man-in-the-client/

December 2012

Chapter Eight:

Password Attack

As a way of ensuring that you are who you claim to be, web applications must utilize certain means of identification and one of them is the traditional password authentication. When it comes to choosing a strong password to protect your online identity and organization's vital credentials, you can never be too careful and to appreciate all those warnings you get on implementing a strict password policy, we will be looking at some common form of password attacks.

Shoulder Surfing

It might come as a surprise that I am adding this trivial form of password threat but most internal compromise of systems occurs as a result of rogue employee shoulder surfing employees with higher security clearance and using their password to sabotage the company's operation.

Password Guessing

This is one good reason why you should never use a default password or a weak one for that matter. Password guessing attack is a type of attack where an attacker attempts to log into a user's account or

organizations infrastructure by trying out different passwords and hoping that one clicks. Usually in order to have access to a portal, applications are designed to acquire both a unique user name or email address and a password. When targeting an organization or individual, a hacker would have already performed reconnaissance on the prey and must have gathered employees' email addresses or usernames, this alone has increased the attacker's chance of a successful attack by half. All s/he needs now is to guess a matching password for one of the emails and he's in!

Same goes for social media accounts and other web applications that require a form of identification such as banking apps and online shopping stores.

There are certain techniques which hackers use to speed up their chances of hitting a matching password. One of them is the use of a dictionary. In this process, a malicious hacker runs a long list of dictionary words against each email address or log in credential and waits to see which one matches. However, there is a tool called Crunch which generates wordlist from a character set. Crunch can create wordlist based on character set specified by the attacker, this gives the attacker the ability to customize the attack payload by inserting strings such as pet names, date of birth, username, terms pertaining to the company thereby making the password guessing process more likely.

Password Cracking / Brute Force

This is a form of password attack where an attacker acquires a password hash either by the use of one of the sniffing tools discussed already in man in the middle attack or having physical access to the system and extracting the encrypted password files i.e. the SAM file in Windows operating system and the /etc/passwd file in the case of a Linux operating system.

In order to decrypt the password extracted, the hacker uses one of the passwords cracking tools such as John the Ripper or Cain and Abel which is available both in the Linux and Windows operating system. Depending on the complexity of the password, the cracking process could take anywhere from a few hours to days, months and even years (yes! Hackers can be very patient, but they know when to throw in the towel too).

When you create passwords, they usually are not stored in plain-text format but rather are encrypted so as to give it extra security. This encrypted format of your password is called the password hash. In order to decrypt, and in other words crack this password, Password cracking software is shipped with a database of common passwords

including dictionary words which are already hashed. So when an attacker runs the cracking tool, it compares the hashed password supplied by the attacker with the ones in its database and the process terminates when a matching password is discovered.

Source: https://null-byte.wonderhowto.com

Countermeasures

Even with the most expensive security gadgets in place, your infrastructure could still be at risk as a result of an employee having access to security clearance they shouldn't in the first instance.

Implementing strong and strict password policies among every employee of the company is essential as a single compromised account could bring the whole organization to its knee.

Best Password Policy

- Employees should be made to change their password frequently, at least once every three months.
- When creating a password, always choose a combination of alphanumeric characters as well as symbols; also try mixing the cases of each alphabet to make it more complex because the more complex a password is, the harder it is to crack. Avoid using first name, pet name, a mix of date of birth or any other general information about you as password. The lengthier the better and hopefully the more it doesn't make sense to you, the harder it will be for a cracker to decrypt.
- Always use a unique password for each of your accounts and never recycle a password. Different web applications spend differently on security; you don't want a situation where a data breach incident in a book club you register to affect your banking account simply because you use the same password across multiple platforms.

- Implement two-factor authentications in your company and enable the feature if it is being implemented by any of your online accounts.

EBay Data Breach

Source: https://www.dailymail.co.uk

The online auction giant, EBay reported a cyber-attack in May 2014 that it said exposed names, addresses, dates of birth and encrypted passwords of all of its 145 million users. The company said hackers

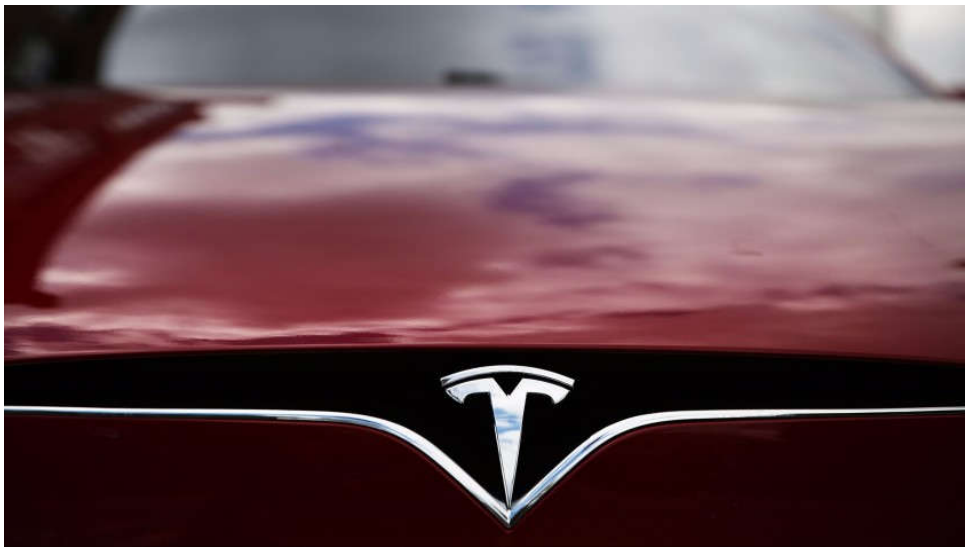
got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database.

It asked its customers to change their passwords but said financial information, such as credit card numbers, was stored separately and was not compromised. The company was criticized at the time for a lack of communication informing its users and poor implementation of the password-renewal process.

https://www.csmonitor.com/World/Passcode/2014/0521/EBay-hit-by-a-cyber-attack-urges-145-million-users-to-change-passwords

May 2014

Rogue Employee



Source: https://www.latimes.com

In 2018, a disgruntled Tesla employee admitted to hacking the company's secret trade information and sharing the data with unnamed 3rd parties. A few days later, Elon Musk sent an email to employees notifying them of the breach and requesting their cooperation and vigilance as Tesla moved forward with its investigation and subsequent lawsuit. As a groundbreaking tech company at the forefront of human innovation, Tesla is no doubt braced for cyber-attacks. A variety of non-malicious hacks have

revealed several of Tesla's security vulnerabilities, but it's this insider attack that set the company on edge.

https://www.reuters.com/article/us-tesla-ceo/tesla-accuses-former-employee-of-hacking-and-transferring-data-idUSKBN1JG2OV

June 2018

Fitness App Breached

Source: https://www.bizjournals.com

In February 2018 Under Armour's MyFitnessPal App experienced one of the biggest data breaches in history when an unauthorized party accessed the company's data stash. The user names, email addresses and scrambled passwords of over 150,000,000 app users were stolen. The breach was discovered on March 25th and users were notified to change their passwords four days after that. The type of data that was breached is considered moderate and the breach was discovered relatively fast. Under Armour gets credit for hashing the passwords and processing credit card information separately; two actions that prevented this breach from spiraling to a whole new level of disastrous. To date, the entity behind this breach has not yet been identified.

https://thycotic.com/company/blog/2018/07/31/the-6-most-disturbing-data-breaches-in-2018-so-far/

February 2018

Chapter Nine:

DDoS Attack

With thousands of devices such as AIs (artificial intelligence), IoT devices and more business networks joining the internet daily, it's becoming more difficult for organizations and institutions to protect themselves and withstand DDoS (distributed denial of service) attacks when they become targeted.

A DDoS attack involves a single system bombarding a single target server with overwhelming packets till it's impossible for legitimate users to access the target service while DDoS on the other hand is a type of cyber-attack where an attacker directs massive packets of incomplete connection requests from many botnets to a single server or network infrastructure with the aim of making the services provided by the system unusable for legitimate users.

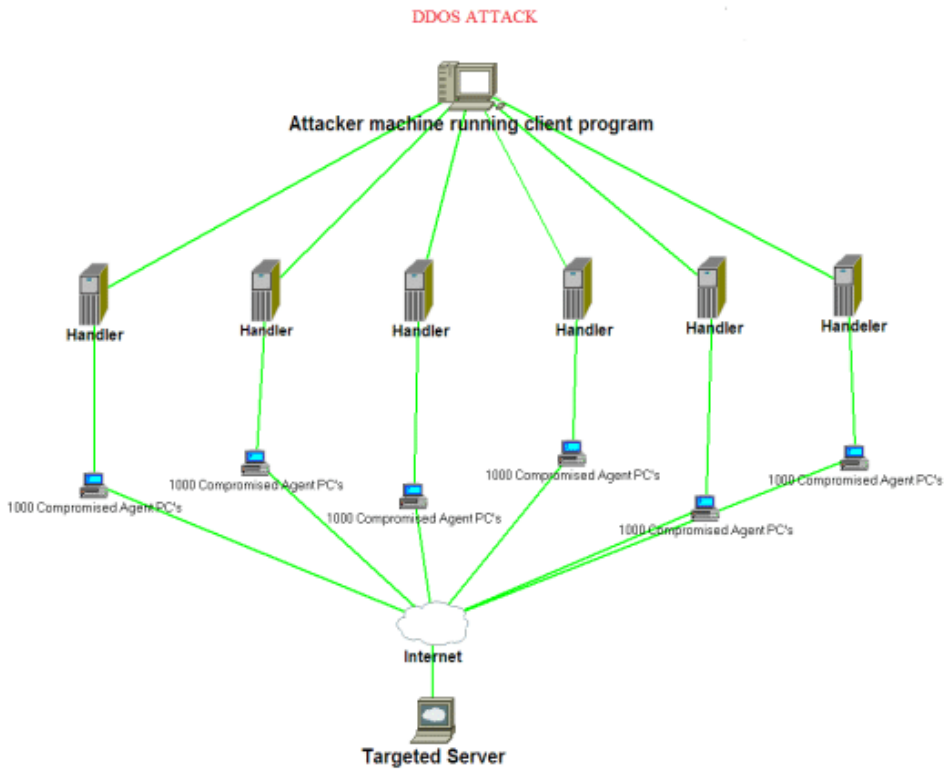
To launch a DDoS attack, a malicious hacker begins by exploiting a security vulnerability in one computer called the *master* from which s/he then infects hundreds or thousands of computers and networks depending on the scale of the attack with malware by exploiting yet another vulnerability in each of these computers which remains hidden and unknown to the system owners. These hacked computers called botnet then wait for commands from the master. In order to perform a DDoS attack the attacker runs a control command from the master computer to all the bots. A typical attack would be to send enormous SYN requests from the bots to the target server.

Volumetric Attack

This is a form of DDoS attack where the malicious hacker utilizes the combined strength and resources of each bot in consuming the bandwidth of the target by bombarding it with malformed packets. This form of attack exploits flaws in the network and transport layers of the OSI model which is the SYN, SYN/ACK and ACK TCP connection format called the three-way handshake.

Application Attack

Application attack is the most sophisticated form of DDoS attacks as they focus on web applications. Also referred to as layer seven attack.

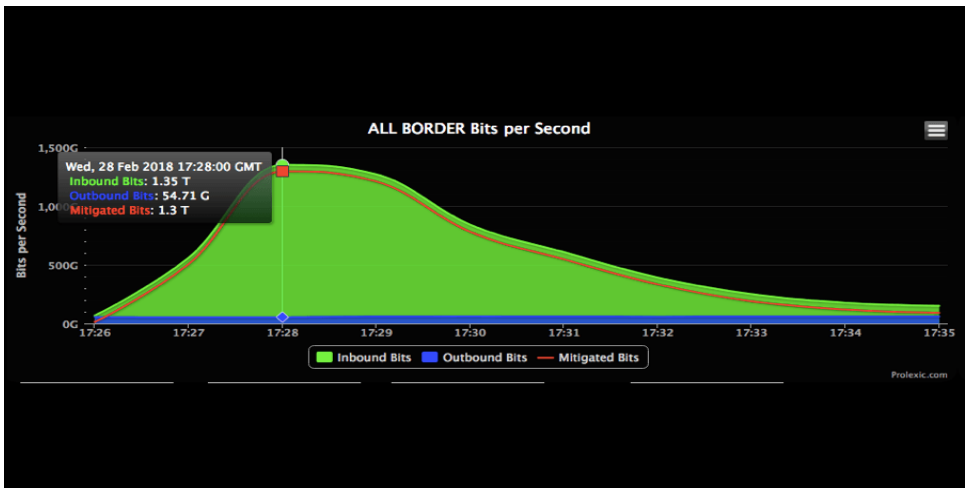


Source: https://www.researchgate.net

Countermeasures

- For a large and medium scale business enterprise, you should consider DDoS-as-a-Service. This service delivers an enhanced environment for your business with the main difference between this and other cloud services being that it provides larger bandwidth and more flexible cloud service to withstand any possible DDoS attack.
- Consider installing both Intrusion Detection system (IDS) and Intrusion Prevention System (IPS) on your network in order to automatically detect and prevent strange packets and network anomaly.
- Even with that new and shiny Intrusion Prevention system, you shouldn't rely totally on automated detections but you should also understand warning signs by manually observing incoming traffic and fishing out seemingly malicious packets. Some symptoms of a DDoS include network slowdown, continuous ping request from a specific IP address in the case of DDoS attack and total website inaccessibility and shutdown.

GitHub Hit



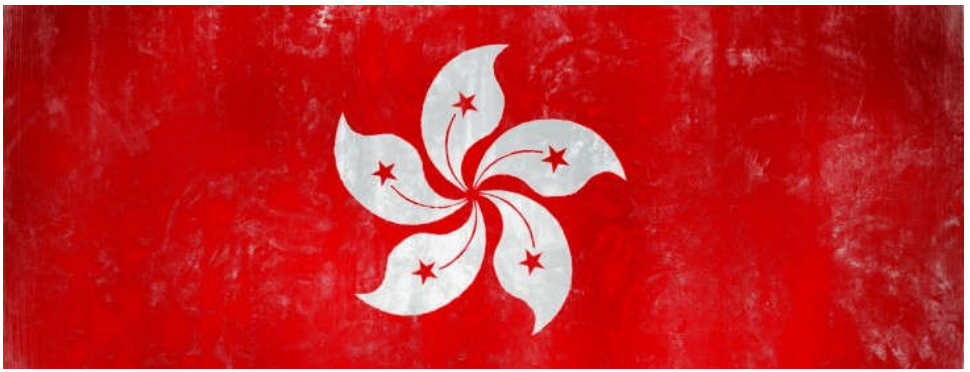
Source: https://fossbytes.com

On Feb. 28, 2018, GitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

February 2018

The Popvote DDoS



Source: https://thenextweb.com

The PopVote DDoS attack was carried out in 2014 and targeted the Hong Kong-based grassroots movement known as Occupy Central. The movement was campaigning for a more democratic voting system.

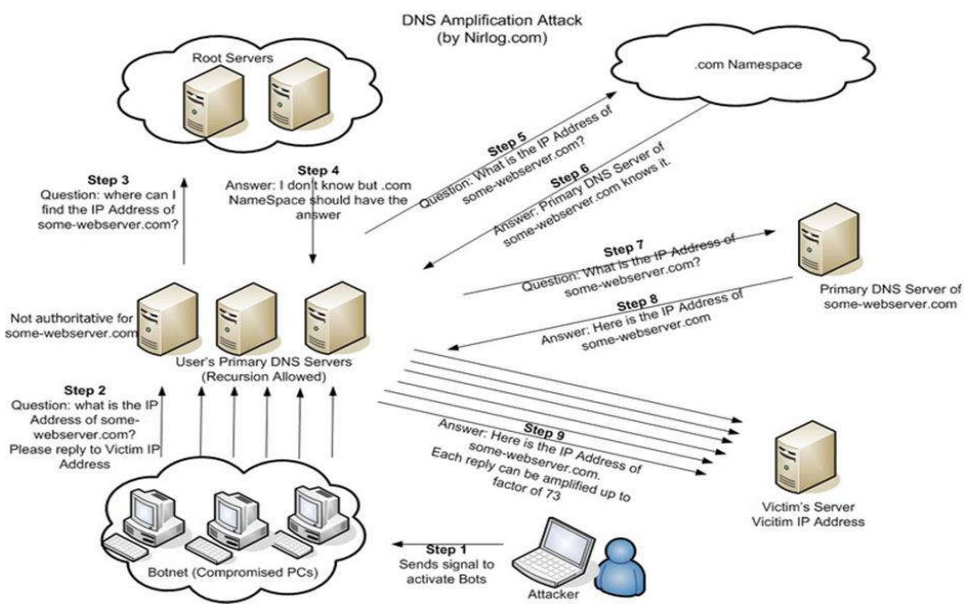
In response to their activities, attacker(s) sent large amounts of traffic to three of Occupy Central's web hosting services, as well as two independent sites, PopVote, an online mock election site, and Apple Daily, a news site, neither of which were owned by Occupy Central but openly supported its cause. Presumably, those responsible were reacting to Occupy Central's pro-democracy message.

The attack barraged servers with packets disguised as legitimate traffic and was executed with not one, not two, but five botnets. This resulted in peak traffic levels of 500 gigabits per second.

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

August 2018

Spamhaus Attacked



Source: https://resources.infosecinstitute.com

In 2013, a DDoS attack was launched against Spamhaus, a nonprofit threat intelligence provider. Although Spamhaus, as an anti-spam organization, was threatened and attacked, this DDoS attack was large enough to knock their website offline, as well as part of their email services.

Like the 2014 attack on CloudFlare mentioned above, this attack utilized reflection to overload Spamhaus' servers with 300 gigabits of traffic per second.

The attack was traced to a member of a Dutch company named Cyberbunker, who seemingly targeted Spamhaus after it blacklisted Cyberbunker.

https://krebsonsecurity.com/2013/04/dutchman-arrested-in-spamhaus-ddos/

March 2013

Jargon Buster

Domain name: An Internet domain name is a unique name of an organization or person on the Internet. The name is combined with a generic top-level domain (gTLD), such as **.com** or **.org**. For example, **www.google.com**

Firewall: The primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network.

Hacker: contrary to the widely known definition, a hacker is someone who uses computer and networking skills to overcome technical problems. In the hacker community, a hacker with mischievous intent is called a “malicious hacker” or simply a cracker. Also, the term gray-hat hacker refers to a hacker hired by a company to find flaws in their systems and prescribe ways to mitigate the effects while a black-hat hacker not only hacks a system without authorization but also does with ulterior motives.

Hash: A hash is just a way to represent any data as a unique string of characters. You can hash anything: music, movies, your name, or this article. Metaphorically speaking, hashing is a way of assigning a “name” to your data. It allows you to take an input of any length and turn it into a string of characters that is always the same length. Obviously, there are many methods (algorithms) to do this.

IDS: Intrusion **D**etection **S**ystem, a Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack. Intrusion detection is very tricky. Too much analysis can add excessive overhead and also trigger false alarms. Insufficient analysis can overlook a valid attack.

IoT: Connecting the physical world to a computer or mobile device via the Internet. Internet of Things (IoT) includes home appliances, door locks, doorbells, thermostats, lighting, sleep monitors, security cameras, fitness bands, as well as sensors for traffic monitoring.

IPS: Intrusion **P**revention **S**ystem, a software that prevents an attack on a network or computer system. It is a significant step beyond an intrusion detection system (IDS). Whereas an IDS passively monitors traffic by sniffing packets at a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It is thus capable of blocking the attack in real time.

OSI Model: (**O**pen **S**ystems **I**nterconnection model) The International Standards Organization's OSI model serves as a standard template for describing a network protocol stack.

Packet: A block of data transmitted over a packet-switched network, which is the common architecture of all local area networks (LANs) and widest area networks (WANs) such as the Internet. Packets are mostly

TCP/IP packets, because TCP/IP is the global networking standard. The terms frame, packet and datagram generally refer to the same entity

Payload: In the analysis of malicious software such as worms, viruses and Trojans, payload refers to the software's harmful results. Examples of payloads include data destruction, messages with insulting text or spurious email messages sent to a large number of people.

Salt: In cryptography, a random number that is added to the encryption key or to a password to protect them from disclosure.

Script kiddies: An amateur who tries to illegally gain access to a computer system using programs (scripts) that others have written. Although they may have some programming skill, script kiddies do not have the experience to write their own programs that exploit vulnerabilities. Malicious codes are freely available on the Web. Script kiddies also tend to be indiscriminate and may try to compromise any computer on the Internet they can reach.

Three-Way Handshake: The TCP three-way handshake in Transmission Control Protocol (also called the TCP-handshake; three message handshake and/or **SYN/SYN-ACK/ACK**) is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network.

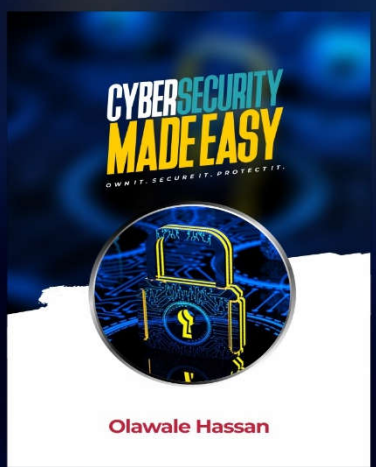
TCP/IP: Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) The most widely used communications protocol. TCP/IP prepares and forwards data packets over a network such as Ethernet. It is connected-oriented and

communicating devices needs to first perform the three-way handshake before connection is established.

UDP: A connectionless, unreliable delivery network protocol which unlike TCP doesn't perform the three-way handshake and are usually used in streaming audio video, voice over IP (VOIP) and videoconferencing.

Unicode: A character code that defines every character in most of the speaking languages in the world. Unicode supports more than a million code points, which are written with a "U" followed by a plus sign and the number in hex; for example, the word "Hello" is written U+0048 U+0065 U+006C U+006C U+006F.

about THE BOOK



Cybersecurity Made Easy is your guide to identifying common cyber threats and protecting your digital identity and assets against such threats. This book intends to bridge the gap between the “not so tech savvy” and IT professionals.