"The Cyber-threat Landscape and its Evolution in the Modern Era"

Abstract

The dependency on the internet has been rapidly growing ever since it was invented in the early 1990s. Hence, it has become extremely important to secure computers and machines, and information stored in them from malicious actors. Computer security, which was once primarily focused on securing physical locations where these machines were kept e.g. data centers, has now evolved into a huge field called Cybersecurity. Each of the subset fields under Cybersecurity focus on protecting different aspects of a system such as software, hardware, network, data and information, and people from continuously evolving cyberattacks. In fact, according to Norton, *"there are more than 2,200 cyberattacks per day. That equates to about one cyberattack every 39 seconds."*. This alarming comparison indicates the frequency of attacks that are being carried out in today's cyberspace. Hence, a company or an organization's first priority should be on securing their IT infrastructure and not take things for granted. This report dives deep into today's cyber landscape and explores a specific type of malware that has been disturbing businesses financially for several years. The report also discusses the differences between cyber attacks and physical attacks in the end.

Part 1:

There are many types of cyber-threats that could pose danger to its victims and even cost them millions financially, depending on the scale, type, or source of the attack. The intentions behind these cyber-threats mainly include monetary gains, spreading a political viewpoint, or carrying out espionage for extracting information. The cyber-threat landscape has been evolving with the rise of new technologies. Some of the common cyber-threats that seem to accomplish the job for attackers include:

- **Malwares** - software programs that are created to carry out various tasks such as corrupting or stealing data, credentials, personal information, or consuming a computer's resources thus making it slower, displaying irrelevant advertisements and popups, spying and tracking user's computer and internet activity, etc. These functions are not carried out by a single program. In fact, each malware is programmed to carry out one or specific set of tasks. Some of them are described below with their specific uses:
    - **Trojan -** a program or software that seems legitimate but intends to harm the computer it is downloaded on due to malicious scripts embedded in its source code.
    - **Ransomware -** a program that takes over a victim's computer, encrypting all its files and data, and asks for a ransom to be paid (via BitCoin mainly) in order to decrypt. This is considered to be a very lucrative attack vector as many people fall victim to it.
    - **Worm -** a self-propagating malicious program that spreads rapidly in a network infecting several devices present in that network. This rapid infection causes networks to slow down. It can also perform various other tasks depending on the way it's programmed.
    - **Virus -** a self-copying malicious program that intends to corrupt a computer and delete its files and perform other such activities. It can aim to exhaust the victim's computer's processing power as well.
    - **Adwares -** programs that continuously show irrelevant and unwanted advertisements and popups on the victim's computer, thus frustrating the user.
    - **Spywares -** softwares that secretly spy and track information, track the victim's computer and internet activities, make use of keyloggers to steal credentials, use webcam and other such functions to gain extensive knowledge about the target and later use it to carry out effective directed attacks.
    - **Bots and Botnets -** a network of infected computers and devices (bots) controlled by C2 servers (Command and Control servers) that can be used to carry out DDoS attacks.
    - **Rootkits -** maliciously-intended hidden program that is installed on a victim's device for hackers to gain unauthorized access (like a backdoor) whenever required.
- **Phishing -** a type of social engineering attack that relies on the receiver (intended victim) falling prey to it and performing the action (required by the attacker) unknowingly. It can involve clicking on a malicious link, downloading malware (thinking it as a normal file), manipulating the victim (using the sense of urgency, authority, scarcity and such tactics) in such a way that he/she gives out the credential and personal information. This is considered a very effective and widely used tactic, if carried out in a planned manner. Moreover, depending on the medium used, it can be further divided into the following types:

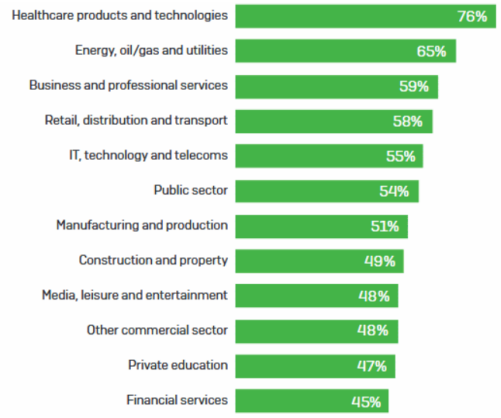
    - **Vishing -** phishing implemented using voice calls as a medium. It can be very effective if used with the 'urgency' tactic that does not give the victim enough time to double think and compels him/her to perform a task or give out the information at the same instance.
    - **Smishing -** phishing carried out through the use of SMS (Short Message Service). It might be either automated or targeted. It demands the user to click on a malicious link or perform some kind of task that will trigger a malicious activity on the device.
    - **Spear phishing -** targeted phishing scam carried out with prior research by the attackers on a company's employees or a group of people.
    - **Whaling -** a type of phishing that targets the so called 'big whales' of a big corporation or organization. They can be anyone ranging from the CEOs to anyone important or highly regarded.
- **Denial of Service or Distributed Denial of Service -** an attack carried out using bots and botnets controlled by a central C2 server. It aims to disrupt the services or ongoing operations of a company and in turn make the machines and servers unresponsive by generating fake traffic.
- **Web application attacks -** attacks carried out on vulnerable websites and web applications by variety of attack vectors such as:
    - **SQL injection -** involves passing SQL code as input parameters on websites to gain sensitive data from the server or database)
    - **Brute force attacks -** trying out different sets of combinations of usernames and passwords in an automated manner to gain unauthorized access to a website.
    - **Man-In-The-Middle Attack -** a hacker intercepts the incoming and outgoing requests and information between the victim's website and the server. The intercepted information could turn out to be potentially crucial for the attacker sometimes.
    - **Cross-Site Scripting (XSS) -** This is one of the widely used web application attacks which requires the user to visit a website after which the programmed malicious function is performed automatically after visiting or by performing an action such as clicking.

These are some of the ways, also referred to as 'attack vectors' in cybersecurity terms, that can be used by people either for malicious means or for testing the strength of security in a company, website, or application. There are attack sources that use these attack vectors for carrying out malicious activities depending on their intentions. These include Criminal organizations, Advanced Persistent Threats (APTs), Terrorists, Hacktivists, Insiders, Spies, Script kiddies, and Nation States. In today's world, everything on the internet is available and can be accessed with the blink of an eye. Everyone has an online presence which can be used for passive reconnaissance (gathering information about a target using open source intelligence before an attack). This can be considered a cyber-espionage on an extremely small scale or level. Moreover, *"Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks."* (Introduction to Information Security by Cengage Learning, page 17). This explains the fact that personal information of anyone is extremely important and needs to be secured. Many technologically advanced nations such as the USA, China, Russia, Israel, North Korea, and Iran are rumored to be undergoing information warfare, whereby these countries are spending huge amounts of resources on increasing cyber presence and secretly spying on other nation's digital assets. It is definitely true to an extent. Nation state actors, especially, use this methodology called 'cyber-espionage' to keep an eye on other nations through cyber means and gain crucial information about their developments and key assets. This is effective in a way that unlike using traditional spies, there is negligible risk to their and common people's lives. Since all the data is available digitally, using physical attacks doesn't make sense. Moreover, the majority of the world's population uses the internet nowadays, so it becomes easier for hacktivists to maliciously promote their political point or agenda through social media and news. As far as criminal organizations are concerned, they can use identity-theft and reconnaissance techniques to gain valuable information about the target to carry out an effective operation. The most important reason one might use cyber-attack instead of a physical attack is that using cyber-attack, one can easily cover the tracks and sneak in or out unnoticed, making it harder to track the attacker's identity and their location. Being anonymous on the internet has become easy using a variety of tools (eg. Tor) that are available. In conclusion, performing a cyber attack is comparatively cheaper and safer.

Part 2:

One of the most common security threats is Malware. It's been used so widely and publicized a lot that it's the first thought that comes to mind when talking about cybersecurity. Hence, in this report, I'll be diving deeper into malware, in general, but more specifically into a subtype of it i.e. Ransomware.

Malwares, as described above in part 1, are software programs that are used for malicious purposes such as stealing or corrupting computer data and files, using up and exhausting computer resources and power, tracking user activity, and such tasks. Ransomwares are similar to them in a way that they are also computer programs and intend to hijack a computer i.e. block user access to the computer and encrypt its data and files until a ransom amount is paid by the victim to decrypt back. This is a very lucrative attack vector for attackers. Hence, financial gain is the main intention behind this attack. The primary victims are high-profile individuals, medium-sized corporations and organizations, and hospitals. This is so because the data stored by them is extremely important to them and they cannot afford to lose it or make them end up in the wrong hands. The reason ransomwares don't target big corporations is because of the requirement of having huge resources and skills in order to overcome their security infrastructure and carry out a successful attack. According to Bleeping Computer's article, the healthcare sector has been hit the most by ransomwares historically. As the chart below shows 76% of the total ransomware attacks were targeted towards the healthcare sector. This might be due to the fact that they tend to pay ransoms more easily than others. However, most of the ransomwares, to increase their attack surface and in turn improve the probability of getting paid, attack multiple sectors. Thus, explaining the reason behind such close figures.

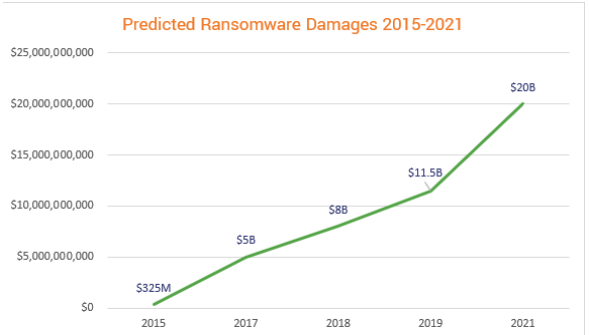


Credits: Statistics provided by Bleeping Computer website

In recent years, ransomware implementations have been evolving, with the main motivation being the same. They are growing in capabilities to encrypt files, evade antivirus softwares and prevent detection. They are becoming so sophisticated that reverse-engineering them has become more difficult.

These ransomwares can be delivered through email attachments (much like in phishing), which when opened or installed unknowingly will infect the computer. Another vector through which it can enter is SMS or social media messages, or popup ads. As soon as it enters the computer, it finds vulnerabilities that can give it root access. After which, the files are encrypted using asymmetric cryptography where the private / decryption keys stay with the hackers.

To indicate how financially destructive ransomwares can be for individuals and businesses, take a look at Security Boulevard's line graph over a period of time from 2015 until now.



Credits: Graph provided by Security Boulevard

According to Security Boulevard, "Cybersecurity Ventures estimates that the global costs will reach $20 billion by next year. This is an increase from their estimated damages of $11.5 billion in 2019 and $8 billion in 2018". The graph indicates that ransomware attacks have been becoming popular and frequent year by year. This is due to the evolving implementations and mechanisms. Moreover, the financial gain from these attacks have been very high for the attackers, which tells that they might want to continue on this proven method.

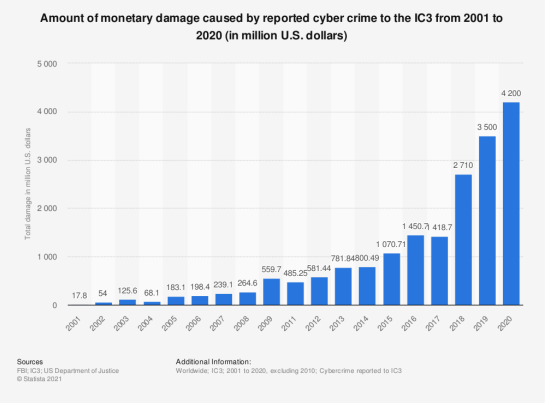
However, companies might want to protect themselves from these attacks as it can turn out to be very damaging for their reputation as well as financially. Some ways they can ensure this are by:

- **Keeping a separate backup** of all files and data so that in case one computer gets infected, there will be a second option and paying the ransom will not be required.
- **Updating** the computer software and system regularly to keep up to date with latest patches.
- **Educating and creating awareness** among employees is crucial for organizations because they might be the weak link in security if anyone becomes a victim of phishing or social engineering attacks.
- Businesses should follow the system of **'least privilege'**. In other words, employees should not be given administrator level access and should only work under required restrictions.

There have been many instances where ransomware attacks have been a major threat around the world financially. One such ransomware was **'WannaCry'** in 2017. It used the worm mechanism to spread itself automatically in a network. The vulnerability it exploited was the Windows SMB vulnerability. It demanded fixed payments in BitCoin, given a time constraint, to help facilitate anonymous transactions. According to Financial Times, *"around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan"*. Another one of the famous ransomware attacks was the **'SamSam'** attack in late 2015. Unlike other ransomwares, SamSam particularly targeted data-rich industries such as education and healthcares to maximize the monetary gain. It made use of brute-force attacks against weak or default passwords, like the Mirai botnet. After which, it tries to perform 'privilege escalation' and take root control of the computer.

Part 3:

Cyber attacks are definitely less riskier or dangerous than physical attacks in the sense that there's less threat to human life since everything is carried out behind the computer screens. However, when speaking in terms of effectiveness, cyber attacks seem to be very effective especially in today's data-rich world. Though cyber attacks don't have the capability to cause severe physical damage to any infrastructure, there's still a possibility. Attacking an Industrial Control System (ICS) is one such way to cause huge disruptions. However, to successfully do that, skills and resources are required, which is rare to have, if one is not a nation state actor. Below is a graph of the total monetary damage (in millions) done using cyber attacks from 2001 to 2020. However, physical attacks do much harm to life due to weapons and bombings while cyber attacks can do more damage in financial terms.



Regarding the solutions to prevent the increasing cyber attacks, organizations should give importance to their security infrastructure. Moreover, some of the big scale attacks in the past have alerted the world and compelled them to improve their cybersecurity programs and common people have become more aware and conscious on the internet. However, certain rules and regulations are yet to be implemented and brought into action. As a result, due to the lack of this, cyber criminals are finding it easier to escape the repercussions and hence are not afraid. The solutions available nowadays are enough in a way to prevent individual hackers and script kiddies. However, certain organized cyber criminal groups and nation states have the support and ability to research and develop zero-day exploits. They might turn out to be extremely dangerous. Moreover, with constantly evolving technologies, zero-day vulnerabilities are bound to be found in some way or other. The way cyber-threats can play a huge role in cyberwarfare might be by allowing nation state attackers to bypass traditional border defences and cause direct damage to government properties on a cyber level. They might attack Industrial Control Systems and national infrastructures that provide necessary services for the population such as telecommunications, power grid, transportation etc. This could affect the general population indirectly as these are the essential services that people use in their everyday lives. For it to classify as a cyberwarfare, it should be an attack by a nation on another nation on a large scale disrupting the lives of millions of people. As for the prediction of when cyberwarfare is likely to happen, it's already likely happening behind the scenes. Although not in action, technologies and methods are being implemented by government agencies and private organizations in full force to be prepared. However, it's unlikely that such a digital war of large scale will actually take place because of the limited impact.

References

“A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time.” Digital Guardian, 1 Dec. 2020, www.digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

Crane, Casey. “20 Ransomware Statistics You’re Powerless to Resist Reading.” Security Boulevard, 28 Feb. 2020, www.securityboulevard.com/2020/02/20-ransomware-statistics-youre-powerless-to-resist-reading.

Cimpanu, Catalin. “Ransomware Victims Hit on Average by Two Attacks per Year.” BleepingComputer, 6 Feb. 2018, www.bleepingcomputer.com/news/security/ransomware-victims-hit-on-average-by-two-attacks-per-year.

“115 Cybersecurity Statistics and Trends You Need to Know in 2021.” Norton, 9 Aug. 2021, www.us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html.

Jones, Sam (14 May 2017). "Global alert to prepare for fresh cyber attacks". Financial Times.

Learning, Cengage. “Introduction to Information Security”, https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

PGP Corporation, “An Introduction to Cryptography”, 2002, https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf