E/15/280

Premathilaka M.P.U

The vicissitude of Cyber Crime Threat Landscape: The past, present and the future

Cybercrime is any criminal activity that involves a computer, networked device or a network. Cybercriminals use a number of attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest. With the advance of technology, number of cybercrimes as well as the powerfulness of it increases day by day. Therefore, we can discuss about cyber crime threat landscape in past, present and future.

Cybercrime's origins are rooted in telecommunications, with "hacker" culture as we know it today originating from "phone phreaking," which peaked in the 1970s. Phreaking was the practice of exploiting hardware and frequency vulnerabilities in a telephone network, often for the purpose of receiving free or reduced telephone rates. Cybercrime as we currently think of it began on November 2, 1988 when Robert Tappan Morris unleashed the Morris Worm upon the world. Much like Dr. Frankenstein, Morris did not understand what his creation was capable of. This type of self-replicating program had never been seen before outside of a research lab, and the worm quickly transformed itself into the world's first large-scale distributed denial of service (DDoS) attack. Computers worldwide were overwhelmed by the program and servers ground to a halt. Although Morris quickly released the protocol for shutting the program down, the damage had been done. In 1990 first virus was created. From here on, viruses went, well, viral. Melissa and ILOVEYOU infected tens of millions of PCs, damaging email systems worldwide with little clear objective. At the turn of this century, we began to see a new era of malware emerge as email gave hackers a fresh access point. The infamous ILOVEYOU worm infected 50 million computers in 2000, corrupting data and self-propagating by exploiting a user's email contacts. Given that the infected emails were coming from an otherwise trusted source, it forced many consumers to gain perspective on cybersecurity for the very first time.

If we consider about modern Cyber crimes most of the modern cyber crimes are based on money. In 2018 IOCTA report states the list of dominant online attacks. Those are Ransomware, malware, data breaches, payment card fraud, cryptocurrency, cryptojacking. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. There is a trend of drone-based attacks now a days. SensePost Security in London developed technology called Snoopy that was mounted on a drone, and then hacked into mobile devices from the air to obtain data. In present lacking of cyber security knowledge among people also affects to these cybercrimes.

In future with the technological advance cyber crimes would be unavoidable. Here are the most pressing cybersecurity issues in future.

Advanced phishing kits: Four new malware samples are created every second. Phishing remains one of the most successful attack vectors due to its speed, as most phishing sites stay online for just four to five hours. Users only report 17% of phishing attacks, and it is seen as a low-risk type of activity. As a result, today only 65% of all URLs are considered trustworthy. This puts a strain on both the consumer and any enterprise with an online presence. It predicts that 2020 will be known for advanced phishing attacks, due to the number of new phishing kits available on the dark web. These kits enable people with only basic technical knowledge to run their own phishing attacks. With more tools available, phishing will become an even more dangerous attack method.

Remote access attacks: Remote attacks are growing in number, as well as becoming more sophisticated. One of the main types of remote access attack in 2018 was cryptojacking, which targeted cryptocurrency owners. Another popular type of attack threatened perimeter devices. According to our threat intelligence database, remote access attacks are among the most common attack vectors in a connected home. Hackers target computers, smartphones, internet protocol (IP) cameras and network attached storage (NAS) devices, since these tools usually need to have ports open and forwarded to external networks or the internet.

Attacks via Smart phones: One of the most common attack vectors to smartphones are related to unsafe browsing (phishing, spear phishing, malware). More than 60% of fraud online is accomplished through mobile platforms, according to RSA, and 80% of mobile fraud is achieved through mobile apps instead of mobile web browsers. As most people use their phones to manage financial operations or handle sensitive data outside the security of their home network, this becomes a prominent threat. The fact that users typically hold all their information on their phone, and that smartphones are now used for two-factor authentication - one of the most widely used cybersecurity tools - increases the security risk if the device is lost or stolen.

Vulnerabilities in home automation and IoT: The consumer Internet of Things (IoT) industry is expected to grow to more than seven billion devices by the end of 2020, according to Gartner. Many consumers do not see IoT devices as a vulnerability, because a significant portion of them do not have a user interface. This could lead to issues understanding what kind of data the device collects or manages. However, IoT devices are not only collecting valuable user data. They could become an entry point for an attacker or tool to launch a distributed denial-of-service (DDoS) attack. IoT devices are not secure by design, because putting a focus on security would significantly increase manufacturing and maintenance expenses.

In future Machine learning cyber attacks could be a huge problem. We know that machine learning is one of the best technologies for data processing. That's why hackers target the machine learning to make it one of the cyber threats. They use its faster behavior against its cyber protection ability. Through machine learning, hackers can attack and hack all the information before you can even discover the attack. So, basically, they are taking its advantage by using it against itself.

In future attackers' target could a physical infrastructure. For example, media channels, power grid, and transportation networks. This type of cyber-attack has the potentiality to cause extensive disaster. Detecting this type of sophisticated criminals is too tough for any organization although they are trying their best.

Another huge Cyber Security Challenge is Artificial Intelligence Malware. And the interesting part is it's self-aware and can think in various ways. AI applications come with a lot of advantages, but the problem is all those advantages come with some disadvantages also.

IoT Internet of things is a blessing to us, but it's an extraordinary blessing to criminals nowadays. Most of us use different types of smart devices. Thanks to IoT, we can now connect all our devices to each other. It reduces a lot of complexity. Now you can handle and control all of your devices from anywhere using just your phone. With the modern innovation, you are continuously plugged in. That's getting you away from the cyber protection. Criminals can hack one of your devices and then it can have access to your entire information; both personal and professional. They can use the internet of things for the DDoS attack. It will make them take down the whole system based on the internet. And also, in future it could be possible to hack human body also. Wearable tech isn't yet commonplace, but many people believe that we're on the verge of the technology's boom. If smart watches, contacts, shirts and who knows what else take off and become connected to the Internet, that could give hackers the ability to intrude into people's lives more intimately than in the past. Trend Micro claimed in a recent report that wearables could allow hacks against the human body in large frequency by 2020.

REFERENCES

1. https://www.director.co.uk/12370-2-cyber-attacks-the-past-present-and-future/
2. https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/
3. https://www.govtech.com/security/Scary-Possibilities-for-Cybercrimes-Future.html