CO325 – Assignment

E/14/317

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

Before moving on to the depth of the topic it is essential to have an informed idea about what is meant by the term cybercrime and which crimes falls under it and not.

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.

Now let's look at the text book definition of what cybercrime is. Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Most cybercrime are attacks on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life. We are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

An important aspect of cybercrime is its nonlocal character. Actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Convention on Cybercrime was

signed by 30 states. The convention came into effect in 2004. Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes, were proposed in 2002 and came into effect in 2006. In addition, various national laws, such as the 'USA Patriot Act' of 2001, have expanded law enforcement's power to monitor and protect computer networks.

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or governments deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism. That is, the use of the Internet to cause public disturbances and even death. Cyberterrorism focuses upon the use of the Internet by non-state actors to affect a nation's economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyberterrorism has grown dramatically. Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number. Taxes are collected on the basis of each citizen's Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual's Social Security number affords the opportunity to gather all the documents related to that person's citizenship (i.e., to steal his identity. Even stolen credit card information can be used to reconstruct an individual's identity) Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide. Cybercrime is clearly, however, an international problem.

In 2015 the U.S. Bureau of Justice Statistics (BJS) released a report on identity theft. The BJS report showed that while the total number of identity theft victims in the United States had grown by about 1 million since 2012, the total loss incurred by individuals had declined since 2012 by about $10 billion to $15.4 billion. Most of that decline was from a sharp drop in the number of people losing more than $2,000. Most identity theft involved small sums, with losses less than $300 accounting for 54 percent of the total.

Internet related frauds are another growing threat which schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or "419," scam. The number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires "laundering" to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

In 2002 the newly formed U.S. Internet Crime Complaint Center (IC3) reported that more than $54 million dollars had been lost through a variety of fraud schemes. This represented a threefold increase over estimated losses of $17 million in 2001. The annual losses grew in subsequent years, reaching $125 million in 2003, about

$200 million in 2006, close to $250 million in 2008, and over $1 billion in 2015. In the United States the largest source of fraud is what IC3 calls "non-payment/non-delivery," in which goods and services either are delivered but not paid for or are paid for but not delivered. Unlike identity theft, where the theft occurs without the victim's knowledge, these more traditional forms of fraud occur in plain sight. The victim willingly provides private information that enables the crime, hence, these are transactional crimes. Few people would believe someone who walked up to them on the street and promised them easy riches, however, receiving an unsolicited e-mail or visiting a random Web page is sufficiently different that many people easily open their wallets. Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime. South Korea is among the most wired countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. Japan has also experienced a rapid growth in similar crimes.

E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the freedom of speech in a liberal democratic polity. Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

One of the most significant problems in shutting down spammers involves their use of other individuals' personal computers. Typically, numerous machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control. Such machines are known as zombie computers, and networks of them, often involving thousands of infected computers, can be activated to flood the Internet with spam or to institute DoS attacks. While the former may be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been deployed in efforts to blackmail Web sites by threatening to shut them down. Cyber experts estimate that the United States accounts for about one-fourth of the 4–8 million zombie computers in the world and is the origin of nearly one-third of all spam.

E-mail also serves as an instrument for both traditional criminals and terrorists. While libertarians laud the use of cryptography to ensure privacy in communications, criminals and terrorists may also use cryptographic means to conceal their plans. Law-enforcement officials report that some terrorist groups embed instructions and information in images via a process known as steganography, a sophisticated method of hiding information in plain sight. Even recognizing that something is concealed in this fashion often requires considerable amounts of computing power; actually decoding the information is nearly impossible if one does not have the key to separate the hidden data.

Sometimes e-mail that an organization would wish to keep secret is obtained and released. In 2014 hackers calling themselves "Guardians of Peace" released e-mail from executives at the motion picture company Sony Pictures Entertainment, as well as other confidential company information. The hackers demanded that Sony Pictures not release *The Interview*, a comedy about a CIA plot to assassinate North Korean leader Kim Jong-Un, and threatened to attack theatres that showed the movie. After American movie theatre chains canceled screenings, Sony released the movie online and in limited theatrical release. E-mail hacking has even affected politics. In 2016, e-mail at the Democratic National Committee (DNC) was obtained by hackers believed to be in Russia. Just before the Democratic National Convention, the media organization WikiLeaks released the e-mail, which showed a marked preference of DNC officials for the presidential campaign of Hillary Clinton over that of her challenger Bernie Sanders. DNC chairperson Debbie Wasserman Schultz resigned, and some American commentators speculated that the release of the e-mail showed the preference of the Russian government for Republican nominee Donald Trump.

Sabotage

Another type of hacking involves the hijacking of a government or corporation Web site. Sometimes these crimes have been committed in protest over the incarceration of other hackers; in 1996 the Web site of the U.S. Central Intelligence Agency (CIA) was altered by Swedish hackers to gain international support for their protest of the Swedish government's prosecution of local hackers, and in 1998 the *New York Times* Web site was hacked by supporters of the incarcerated hacker Kevin Mitnick. Still other hackers have used their skills to engage in political protests. In 1998 a group calling itself the Legion of the Underground declared "cyberwar" on China and Iraq in protest of alleged human rights abuses and a program to build weapons of mass destruction, respectively. In 2007, Estonian government Web sites, as well as those for banks and the media, were attacked. Russian hackers were suspected because Estonia was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.

Sometimes a user's or organization's computer system is attacked and encrypted until a ransom is paid. The software used in such attacks has been dubbed *ransomware*. The ransom usually demanded is payment in a form of virtual currency, such as Bitcoin. When data are of vital importance to an organization, sometimes the ransom is paid. In 2016 several American hospitals were hit with ransomware attacks, and one hospital paid over $17,000 for its systems to be released. Defacing Web sites is a minor matter, though, when compared with the specter of cyberterrorists using the Internet to attack the infrastructure of a nation, by rerouting airline traffic, contaminating the water supply, or disabling nuclear plant safeguards. One consequence of the September 11 attacks on New York City was the destruction of a major telephone and Internet switching center. Lower Manhattan was effectively cut off from the rest of the world, save for radios and cellular telephones. Since that day, there has been no other attempt to destroy the infrastructure that produces what has been called that "consensual hallucination," cyberspace. Large-scale cyberwar (or "information warfare") has yet to take place, whether initiated by rogue states or terrorist organizations, although both writers and policy makers have imagined it in all too great detail.

In late March 2007 the Idaho National Laboratory released a video demonstrating what catastrophic damage could result from utility systems being compromised by hackers. Several utilities responded by giving the U.S. government permission to run an audit on their systems. In March 2009 the results began to leak out with a report in *The Wall Street Journal*. In particular, the report indicated that hackers had installed software in some computers that would have enabled them to disrupt electrical services. Homeland Security spokeswoman Amy Kudwa affirmed that no disruptions had occurred, though further audits of electric, water, sewage, and other utilities would continue.

With the advent of almost every new media technology, pornography has been its "killer app," or the application that drove early deployment of technical innovations in search of profit. The Internet was no exception, but there is a criminal element to this business bonanza—child pornography, which is unrelated to the lucrative business of legal adult-oriented pornography. The possession of child pornography, defined here as images of children under age 18 engaged in sexual behavior, is illegal in the United States, the European Union, and many other countries, but it remains a problem that has no easy solution. The problem is compounded by the ability of "kiddie porn" Web sites to disseminate their material from locations, such as states of the former Soviet Union as well as Southeast Asia, that lack cybercrime laws. Some law-enforcement organizations believe that child pornography represents a $3-billion-a-year industry and that more than 10,000 Internet locations provide access to these materials.

The Internet also provides pedophiles with an unprecedented opportunity to commit criminal acts through the use of "chat rooms" to identify and lure victims. Here the virtual and the material worlds intersect in a particularly dangerous fashion. In many countries, state authorities now pose as children in chat rooms. Despite the widespread knowledge of this practice, pedophiles continue to make contact with these "children" in order to meet them "off-line." That such a meeting invites a high risk of immediate arrest does not seem to deter pedophiles. Interestingly enough, it is because the Internet allows individual privacy to be breached that the authorities are able to capture pedophiles.

Hacking is another form of important cyber security violation that we had not mentioned before.
While breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music, video, or child pornography—what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network? The story of hacking actually goes back to the 1950s, when a group of phreaks (short for "phone freaks") began to hijack portions of the world's telephone networks, making unauthorized long-distance calls and setting up special "party lines" for fellow phreaks. With the proliferation of computer bulletin board systems (BBSs) in the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to "hacking" corporate and government computer network systems.
Although the term *hacker* predates computers and was used as early as the mid-1950s in connection with electronic hobbyists, the first recorded instance of its use in connection with computer programmers who were adept at writing, or "hacking," computer code seems to have been in a 1963 article in a student newspaper at the Massachusetts Institute of Technology (MIT). After the first computer systems were linked to multiple users through telephone lines in the early 1960s, *hacker* came to refer to individuals who gained unauthorized access to computer networks, whether from another computer network or, as personal computers became available, from their own computer systems. Although it is outside the scope of this article to discuss hacker culture, most hackers have not been criminals in the sense of being vandals or of seeking illicit financial rewards. Instead, most have been young people driven by intellectual curiosity; many of these people have gone on to become computer security architects. However, as some hackers sought notoriety among their peers, their exploits led to clear-cut crimes. In particular, hackers began breaking into computer systems and then bragging to one another about their exploits, sharing pilfered documents as trophies to prove their boasts. These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks.

The scale of hacking crimes is among the most difficult to assess because the victims often prefer not to report the crimes—sometimes out of embarrassment or fear of further security breaches. Officials estimate, however, that hacking costs the world economy billions of dollars annually. Hacking is not always an outside job—a related criminal endeavor involves individuals within corporations or government bureaucracies deliberately altering database records for either profit or political objectives. The greatest losses stem from the theft of proprietary information, sometimes followed up by the extortion of money from the original owner for the data's return. In this sense, hacking is old-fashioned industrial espionage by other means.
One of the largest known case of computer hacking was discovered in late March 2009. It involved government and private computers in at least 103 countries. The worldwide spy network known as GhostNet was discovered by researchers at the University of Toronto, who had been asked by representatives of the Dalai Lama to investigate the exiled Tibetan leader's computers for possible malware. In addition to finding out that the Dalai Lama's computers were compromised, the researchers discovered that GhostNet had infiltrated more than a thousand computers around the world.

In previous paragraphs we have discussed about the history of cyber-crimes and trends. However there is no need to tell you that cyber-crimes, obviously, gets more sophisticated and complex each month, let alone each year. There does seem a trend towards manual attacks from talented cyber criminals who have thorough bread understand about concepts behind the cyber space then use such knowledge to exploit vulnerabilities. The reason for this is likely because automated cyber-attacks are now much better understood by malware analysts and security network professionals. However, just as soon as they solve a bunch of attack payloads and signatures, so come along another armada of new cyber-attacks tools and persistent threats. Therefore, so far the fight against cyber-crimes has been a defeating fight. The reason for this is that there is a huge gap

between the numbers of cyber vulnerabilities turned in to cyber-attacks Vs the professionals who have enough knowledge to fight against them. Moreover still in third world countries the rules and regulations against cyber-crimes are not at its strongest. Crime is a crime and cyber technology is the latest super tech weapon criminals got. A person can be a victim of a cyber-crime launched even from the other side of the world. It's unpredictable, untraceable. Learning what to do and not to do is the best we can do. So finally, be ready the next victim is may be you.

Summary report on Internet Security

Introduction

The Internet has revolutionized the way people live today. Activities ranging from access to information to entertainment; financial services; product purchase and even socializing all seem to take place online. Due to its wide coverage and pervasive information collection, millions of people are relying on the Internet for almost all kind of activities. And with frequent usage, they have also come to trust the Internet to provide a gateway for personal, home and office convenience. The basic simple structure of the Internet based on a host of backbones and host servers, however makes it vulnerable to many risks. The hosts vary from supercomputers to personal computers using different types of hardware and software. The common link in all of these hosts is the TCP/IP (Transport Control Protocol/Internet Protocol). This language again is based on simple functionality that is if a host has TCP/IP then it can easily connect to other computers that have same backbones and operating systems. This open technology not only expose the Internet to numerous security risks and pitfalls but it also becomes the real issue for its users. This is because attacks on IP is possible; IPs do not perform robust mechanisms for authentication for packets of data that come onto the Internet. Without the authentication mechanism any data packet may claim it originates from certain address but there is no sure way to check the claim of the data packet. Since there is no check for such criminal activities, Internet crime and security breaches continue to rise along with the evolution of the Internet.

Spoofing and Session Hijacking

One of the most basic and common security breaches is when a host claims to have an IP address of another host. This kind of attack is called spoofing. Considering the different router access control lists of different systems are connected to the Internet, the only way for receiving computers to recognize its data packet is through the IP address. An attacker may devise and use techniques to spoof IP address and send packets to a host that require certain actions which may be harmful. In addition some applications allow logins on IP address which open the server/host to great risks if the IP address is known to attackers.

Denial of service

Between the years 2000 and 2002, sixty percent of UK companies have suffered security breaches while eighty five percent of the US companies suffered from network breach costing some $10 million in damages. This only shows that the number of incidents of security breach is increasing and as the Internet spread far and wide, it would also bring with it more threats and risks for breaches. Apart from the physical security, the Internet is also threatened by software breaches. Denial of Service or DoS is one of the instances of security breach.

Encryption

Encryption is a method of changing plain text messages from its original composition by replacing or rearranging the letters and numbers and converting the composition into an indecipherable format. This method uses a mathematical algorithm and a key for encryption. The length of the key is measured in bits which determines the weakness of the encryption program. The encryption key may be 40 bits in length but it

will generate 1 billion possible keys or combination. For this reason encryption creators use long strings to increase security level

Phishing

Related to information theft there is a trend on the Internet whereby web pages are replicated using the same information and encryption as the original website. The user unaware of the fact that they have arrived at a wrong address willfully enter personal and financial information. This is called phishing. According to Sandi Hardmeier (2004) phishing refers to "creating a replica of an existing Web page in an attempt to fool a visitor into providing personal, financial, or password information." The hackers behind the phishing technique can send out email to claim that they are from legitimate business or government organization, and require users to enter personal identification numbers, passwords, credit card information or social security numbers that would ultimately allow them to use the information to access funds from the user's account.

Virus, worms and Trojans

According to Michael Durkota (2005) of US-CERT "Trojan horses are one of the most malicious programs to infect any computer. Even though there are different kinds of removal tools available on the internet, the chances of identifying the right program for the specific Trojan is difficult and by that time the virus would have infected the whole computer." (Durkota 2005) Internet users are exposed to the Trojans easily as it target online users who are connected to the Internet (network of networks). A computer that does not have an anti-virus program is likely to become infected with Trojans horses especially through emails and internet explorer. Some of the measures for preventing Trojans from entering by not opening unsolicited attachments in email messages; unsolicited links; using updated anti-virus software; use an internet firewall and keeping the system patched.

How to Prevent Internet Security breaches?

Antivirus Software

From time to time one reads of malicious bugs and viruses like Melissa and Love Bug that run in email script and target the users by entering their systems and destroy programs etc. One of the reasons why bugs and viruses easily access users' system is due to the fact that these target Microsoft products such as Internet Explorer and Outlook Express The most common interface among consumer IE is not only vulnerable to attacks but it is also being targeted by perpetrators. Outlook for example is a weak tool as it automatically opens email as read when a user clicks on a new email. As a result the virus is triggered even when the user attempts to delete the unsolicited email by clicking on it. But eventually a virus will get close to you, if not actually destroy data and thus rob you of hours of hard work." For this reason there is more reason for taking precautionary measures for virus attacks.

Digital signatures

One of the most important and critical aspect of digital communication is that the Internet does not offer secure transmission. Online email sessions especially are being hacked and emails read a regular basis. Hackers can sniff open sessions and acquire passwords in text form; they may hack into corporate accounts through scanning tools for generating passwords protected email accounts etc. To counteract these instances of security breach, digital signatures have been created through Public Key Infrastructure or PKI. The PKI is basically a digital data transmission tool for secure Internet interaction. The PKI relies on encryption comprising

of keys to protect the digital information. The integrity and confidentiality of the digital information is ensured as it is only accessible by the intended receiver.

Digital Certificates

Digital certificates are one of the most widely used security techniques. They are provided by third party certification authority that verifies the applicant's identity and generates certificate for legal transactions. The certificates ensure that the electronic message such as credit card information and other personal details are not tampered during transmission on the Internet. The digital signatures rely on encryption algorithm for scrambling and unscrambling of the same. The two most common security protocols in digital certification is SSL (secure sockets layer) by Netscape and SET (secure electronic transaction) by Visa International. These have been developed to ensure that credit card users' security when they are trading online.

Firewalls

One of the most commonly used methods of security measures for the Internet is firewall. Firewalls have maligned with bad reputation for not implementing security policy at the network level. In reality firewalls do provide certain level of protection and help organizations to enhance specific machine security. Not only are this but firewalls easy to use, cost efficient and not complex to install. A firewall basically operates on multilevel security by first erecting a wall between the network that is the private network and the Internet. The firewall then monitors the traffic with specific characteristics and allow it to pass through gateways to the user machine. When digital traffic does not comply with the firewall criteria, then the information cannot pass through the gateways thus preventing unauthorized traffic such as viruses and bugs from entering into the computer.

Conclusion

Computer security is a serious issue and has grave implications such as unauthorized access to the system, destruction of information and damages in monetary terms. Security vulnerability is subject to how weak the network is and how sensitive it is to security needs. A corporate intranet is vulnerable to the external environment as it has to be connected to partner or customers to complete transactions. Security vulnerabilities arises when the weak link result in problems and extensive damages to the users.

Proper and effective network security provides the following,

- Accountability--proof that an intended transaction indeed took place.
- Confidentiality--protection of confidential information from an eavesdropper.
- Integrity--assurance that the information sent is the same as the information received.
- Authority--assurance that those who request data or information are authorized to do so.
- Authenticity--assurance that each party is who they say they are.

From the above report it has been observed that hackers tend to attack users and corporations based on the weak infrastructure rather than the software and tools they use. Infrastructure makers like Microsoft often rely on similar platforms and typologies. Even the security measures used to detect malware, viruses, bugs and spyware are based on the same logic of seek and destroy. It does not actually address the problem of technological platform. Similarly, most hackers target Microsoft products and applications and hence devise programs to destroy the application software and users accordingly.

However, the major concern is not to increase the number of tools, techniques or methods but rather to design an effective infrastructure that discourage potential attackers. Even with the latest technologies corporations are being victimized on a regular basis upon various reasons including espionage, greed, monetary gain, or revenge etc. At an individual level, users are being victimized because hackers are keen on studying user behavior, invade privacy, mischief or simply to beat the challenge of having control over the online user. These instances only indicate that with the development of new technologies, even newer technologies will be devised to counteract the security measures.

Short Notes

1. **Evolution of Malware**

In 1982, Elk Cloner was written to infect Apple LLC's operating system. Attached to a game, it infected the Apple's boot sector and spread by "cloning" itself to new disks introduced to the system. Once the virus was triggered, it would display a poem explaining how Elk Cloner was copying itself throughout the victim's machine and that it wouldn't be easy to reverse its effects. A year after the first personal malware was found "in the wild," the term "computer virus" was coined to refer to a malicious program written to destroy data or to corrupt systems. As time moved on, the computer virus branched off into many different categories, each meant to define how it acted.

Malware learned the art of evasion and as a result, antivirus software became a growing business. By the end of the 1990s, the Internet was circling the globe. In the early 2000s, more aggressive social engineering strategies came into play. The "I Love You" worm, aka "Love Letter," was considered the most damaging worm of its time, infecting millions of computers worldwide merely 15 minutes after its release.The issue of computer infection became so paramount that the world started to see authorities making arrests for computer crimes. In 2001, Jan de Wit was arrested after he authored the worm known as the Anna Kournikova worm that spread quickly by tricking recipients into believing that the email they had just received contained a photo of Anna Kournikova.

By the mid-2000s, there were more than a million known computer worms circulating around the Internet. Email spam was becoming big business as malware authors stood to make serious cash by blasting out unsolicited email, spam, and getting just a percentage of users to buy their goods or click on links. The idea of governments and militaries using malware as a new weapon was at first only a theory. This changed with Stuxnet in 2010 (and spin-offs later that year including Duqu and Flame). The world had proof that state-sponsored attacks were a reality.

Cryptolocker and its spinoffs, CryptoWall and CryptoDefense, (all ransomware) made their first appearances around September 2013. Cryptolocker employed strong encryption to scramble nearly every file on its targets, making them impossible to recover without the unique, private key used to encrypt them. Even if the Cryptolocker infection was successfully removed, the files would remain encrypted and unusable. This instantly made many of its victims aware of the importance of a reliable backup strategy.While technology and personal habits mature with each new cyberattack, the threats lurking around the corner do the same at a seemingly uneven pace. Because we can't predict exactly what's ahead, here is a reminder of the best practices that will keep users and systems safe in the face of ever-changing and always evolving malware:

- Remain vigilant; don't let your security practice become complacent
- Add layered security measures
- Only use trusted sites
- Have a reliable backup strategy

2. Web Threats

A web threat is any threat that uses the World Wide Web to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets. Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking. Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected client, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected client may also become a vector to deliver phish attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

3. Mobile Threats

Like viruses and spyware that can infect your PC, there are a variety of security threats that can affect mobile devices. We divide these mobile threats into several categories: application-based threats, web-based threats, network-based threats and physical threats.

Downloadable applications can present many types of security issues for mobile devices. "Malicious apps" may look fine on a download site, but they are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes. Application-based threats generally fit into one or more of the following categories:

- Malware is software that performs malicious actions while installed on your phone. Without your knowledge, malware can make charges to your phone bill, send unsolicited messages to your contact list, or give an attacker control over your device.
- Spyware is designed to collect or use private data without your knowledge or approval. This stolen information could be used for identity theft or financial fraud.

- Privacy Threats may be caused by applications that are not necessarily malicious, but gather or use sensitive information than is necessary to perform their function.
- Vulnerable Applications are apps that contain flaws which can be exploited for malicious purposes. Such vulnerabilities allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, or download apps to your device without your knowledge.

Because mobile devices are constantly connected to the Internet and frequently used to access web-based services, web-based threats pose persistent issues for mobile devices:

- Phishing Scams use email, text messages, Facebook, and Twitter to send you links to websites that are designed to trick you into providing information like passwords or account numbers
- Drive-By Downloads can automatically download an application when you visit a web page. In some cases, you must take action to open the downloaded application, while in other cases the application can start automatically.
- Browser exploits take advantage of vulnerabilities in your mobile web browser or software launched by the browser such as a Flash player, PDF reader, or image viewer. Simply by visiting an unsafe web page, you can trigger a browser exploit that can install malware or perform other actions on your device.

Mobile devices typically support cellular networks as well as local wireless networks (WiFi, Bluetooth). Both of these types of networks can host different classes of threats:

- Network exploits take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.
- Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the WiFi access point.

Mobile devices are small, valuable and we carry them everywhere with us, so their physical security is also an important consideration.

4. IoT Exposed

Everyday appliances and 'smart' devices that are connected to the internet are part of what is known as the Internet of Things (IoT) - a vast array of internetworked 'things' ranging from domestic appliances to buildings and vehicles. According to reports from publications such as Smart
Company, The Guardian and The New York Times, the 2016 distributed denial of service (DDOS) attack harnessed IoT devices such as web cameras, baby monitors, and digital video recorders to launch enough traffic to overwhelm the targeted websites.

Smart fridges, smart TVs, even smart kettles can be exploited and used against you or against someone else. Like the 2016 attack, these devices can be co-opted into a 'botnet' - a network of computers enlisted to deliver a DDOS attack without the knowledge of the owner - to bring down other networks. Your smart devices can also be hacked to use connected cameras to spy on families. Typically, the owner of the device has no way of knowing when it has been compromised. Unprotected devices can also provide a backdoor to your network, leaving your business or personal data exposed.

The types of internet-connected devices targeted for exploitation are generally unlikely to be protected by security software in the same way as personal computers, smartphones and tablets. Attackers can use software to locate devices that are secured only by factory-set default usernames and passwords. These

settings are typically not changed, or cannot be changed, by manufacturers or home users and are easy for attackers to identify, guess or break.

But there are steps we can take to reduce these risks.

- Whenever possible, change any default passwords on the device to a secure and private password. If unsure, look up how to change the device settings on the manufacturer's official website or contact their customer service centre. Learn how to create and remember strong passwords.
- Often devices collect a lot of information (usage patterns and house hold activity) and have cameras and microphones. Make sure you read the terms and conditions/operating instructions for the device and understand what happens to any collected data.
- Make sure your business's wireless network is properly secured. Learn how to protect your network.
- Ensure your software updates are set to apply automatically on your device. Learn about updates.
- Follow all instructions when installing and configuring the settings for the device.

5. Ransomware, coin mining and underground economy

The idea of using a decentralized electronic payment method that relies on cryptographic proof, known as a cryptocurrency, has existed since at least 2008 when an anonymous author using the pseudonym 'Satoshi Nakamoto' published a paper outlining the Bitcoin concept. Although Bitcoin was reportedly used to purchase goods for the first time in May 2010, serious discussions of its potential as an accepted form of currency began in 2011, which coincided with the emergence of other cryptocurrencies. There were approximately 1,370 cryptocurrencies as of December 2017 with new currencies added every day, although many cryptocurrencies cannot be mined. The price and volatility of popular cryptocurrencies surged in late 2017

During 2017, the cryptocurrency market grew nearly 20-fold, reportedly increasing from approximately $18 billion to more than $600 billion (USD). Those gains amplified threat actors' interest in accessing the computing resources of compromised systems to mine cryptocurrency. Secureworks incident response (IR) analysts responded to multiple incidents of unauthorized cryptocurrency mining in 2017, and network and host telemetry showed a proliferation of this threat across Secureworks managed security service clients. Financially motivated threat actors will continue to use malware infections to deploy cryptocurrency mining software for as long as it remains profitable.

Compared to complete loss of availability caused by ransomware and loss of confidentiality caused by banking trojans or other information stealers, the impact of unauthorized cryptocurrency mining on a host is often viewed as more of a nuisance. However, the cumulative effect of large-scale unauthorized cryptocurrency mining in an enterprise environment can be significant as it consumes computational resources and forces business-critical assets to slow down or stop functioning effectively.

6. vulnerabilities and Patching

Vulnerability management is a pro-active approach to managing network security. It includes processes for,

- *Checking* for vulnerabilities: This process should include regular network scanning, firewall logging, penetration testing or use of an automated tool like a vulnerability scanner.

- *Identifying* vulnerabilities: This involves analyzing network scans and pen test results, firewall logs or vulnerability scan results to find anomalies that suggest a malware attack or other malicious event has taken advantage of a security vulnerability, or could possibly do so.

- *Verifying* vulnerabilities: This process includes ascertaining whether the identified vulnerabilities could actually be exploited on servers, applications, networks or other systems. This also includes classifying the severity of a vulnerability and the level of risk it presents to the organization.

- *Mitigating* vulnerabilities: This is the process of figuring out how to prevent vulnerabilities from being exploited before a patch is available, or in the event that there is no patch. It can involve taking the affected part of the system off-line (if it's non-critical), or various other work-around.

- *Patching* vulnerabilities: This is the process of getting patches usually from the vendors of the affected software or hardware and applying them to all the affected areas in a timely way. This is sometimes an automated process, done with patch management tools. This step also includes patch testing,

References

- https://www.businesswire.com/news/home/20171011005771/en/Dark-Web-Ransomware-Economy-Growing-Annual-Rate
- https://www.webopedia.com/TERM/M/mobile_security_threats.html
- https://hackernoon.com/threats-to-your-mobile-device-security-938467bcab3f
- https://en.wikipedia.org/wiki/Web_threat
- https://usa.kaspersky.com/resource-center/threats/web
- https://unifaceinfo.com/docs/0906/Uniface_Library_HTML/ulibrary/webSecurityThreats_A3799D56DFF59A0A23793CE3BCC7FEA4.html
- https://www.wired.com/brandlab/2016/12/cylance-evolution-malware/
- https://discover.cisco.com/en/us/acr/evolutionofmalware
- https://en.wikipedia.org/wiki/Internet_security
- https://www.symantec.com/security-center/threat-report
- https://www.symantec.com/security-center/threat-report
- https://www.britannica.com/topic/cybercrime/Spam-steganography-and-e-mail-hacking
- http://www.bankinfosecurity.asia/webinars/future-trends-in-cyber-crime-assessing-preparedness-law-enforcement-to-w-1327