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

As the personal computer came to the desk of every house and internet became public, involvement of internet and the communication technology to the human activities have become normal. Since, the economy related things also have become more related to cyber space and open up the space for criminals to execute. Even if the global economy and the world being separated in 1980's now it has become almost a single entity. Since that cyber-crimes become more scalable. In early times there were no rules for cybercrimes too. Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country that has developed laws that allow for prosecution. But in future it definitely going to be a different story as international rules and laws is being accomplished.

Cybercrimes which have been reported are in wide range. One aspect is Cyber terrorism. Cyber terrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources. A cyber terrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. Another category is Cyber extortion. Cyber-extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer protection. An example of cyber extortion was the attack on Sony Pictures of 2014. Financial fraud crimes are also cyber based in present. Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. A variety of internet scams, many based on phishing and social engineering, target consumers and businesses. Dark net markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement. Apart from these online harassment, offensive content also known as cyber-crimes. Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Harassment as defined in the U.S. computer statutes is typically distinct from cyberbullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act. The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be legal. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Investigations and penalties against these cybercrimes as follows. A computer can be a source of evidence. Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a log file. In most countries Internet Service Providers are required, by law, to keep their log files for a predetermined amount of time. For example a European wide Data Retention Directive states that all E-mail traffic should be retained for a minimum of 12 months. There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace, however that is not necessarily a factual basis upon which detectives can solve a case. Different types of high-tech crime may also include elements of low-tech crime, and vice versa, making cybercrime investigators an indispensable part of modern law-enforcement. Methodology of cybercrime detective work is dynamic and is constantly improving, whether in closed police units, or in international cooperation framework. Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison. However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyber offender behavior without resorting to total computer or Internet bans. These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searches by probation or parole officers.

Intelligence under cybercrimes are mostly well organized individuals or groups. They are sophisticated with latest technology as well as money. As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specializing in the sale of stolen content, and so forth. A few of the leading cyber security companies have the skills, resources and visibility to follow the activities of these individuals and group. A wide variety of information is available from these sources which can be used for defensive purposes, including technical indicators such as hashes of infected files or malicious IPs/URLs, as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, on-going access typically requires subscribing to an adversary intelligence subscription service. At the level of an individual threat actor, threat intelligence is often referred to that actor's tactics, techniques, and procedures, as the infrastructure, tools, and other technical indicators are often trivial for attackers to change.

One of the biggest problems in cyber security today is how to manage the volume, velocity, and complexity of data generated by the myriad of IT security tools in a typical enterprise. Feeds from these disconnected tools must be analyzed, normalized, and remediation efforts prioritized. The more tools, the more difficult the challenge. Ultimately, this data aggregation and analysis requires legions of staff to comb through massive amounts of data to connect the dots and find the needle in the haystack. These efforts can take months, during which time attackers can exploit vulnerabilities and extract data. Even if an organization can hire enough qualified resources to perform this analysis, they often misalign remediation efforts by relying on internal security intelligence that lacks context regarding active threats and which specific vulnerabilities they are exploiting. Without taking external threat data and business criticality into account, security teams can focus on mitigating the wrong gaps. In many cases, just reacting to past threats rather than taking a pro-active approach based on predictive analytics to shut the window of opportunity before attackers can take advantage of it.

As cloud use grows, we’re likely to hear about more holes that have already been manipulated in cloud services, similar to those reported recently in consumer tools such as Dropbox and LastPass. At least one of these attacks will eventually be exposed as state-sponsored and this will have a real impact on that particular vendor and competing services. The issue of state-sponsored cyber-attacks will become a growing concern as nations continue to wage cyber warfare in a bid to disrupt competing states and gain a competitive advantage. As well as potential attacks on consumer-grade cloud providers, this trend could also point towards a direct attack on a major security vendor. When you consider the huge amount of investment involved in cyber warfare, it is highly likely that at least one major vendor and a key internet-enabled technology will be exposed as having an open backdoor, vulnerable to malware such as Heartbleed. Whether state-sponsored or not, this vulnerability will undoubtedly be exploited and so will have major repercussions on the security sector and technology industry as a whole. In addition, recent high-profile security breaches, such as the eBay leak, have revealed that a worrying number of attacks can potentially go undetected for weeks or even months at a time. It is highly possible that over the next few years this will be a regular occurrence, with attacks reported on target networks that have been resident for years before being discovered. Ultimately, no one can say for certain exactly where and how cyber-attacks will be carried out. However it is highly likely that the cat and mouse game between the IT industry, governments and cybercriminals will only pick up speed and attention in the coming years. IT security experts will have to contend with more diverse threats than ever before and it is only decisive and continuous innovation that will enable us to stay one step ahead.

REFERENCES for Essay and short notes

https://www.forbes.com/sites/eladnatanson/2018/06/11/mobile-ad-fraud-in-2018-tackling-the-newest-threats/2/#14c241a1204d

https://insights.samsung.com/2018/02/14/mobile-security-threats-what-to-watch-for-in-2018/

https://www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks

https://www.csoonline.com/article/2867407/network-security/shodan-exposes-iot-vulnerabilities.html

https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/

https://www.forbes.com/sites/eladnatanson/2018/06/11/mobile-ad-fraud-in-2018-tackling-the-newest-threats/#5d568d4250f5

https://www.businesswire.com/news/home/20171011005771/en/Dark-Web-Ransomware-Economy-Growing-Annual-Rate

https://securelink.net/resources/trending/will-coin-mining-replace-ransomware/

https://whatis.techtarget.com/definition/vulnerability-and-patch-management

https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerability-and-patch-management/#gref

https://www.pcworld.com/article/144636/guide_patch_vulnerability_management.html

https://www.cylab.cmu.edu/_files/pdfs/news/cybersecurityinthethreetimes.pdf

https://us.norton.com/internetsecurity-mobile-types-of-common-mobile-threats-and-what-they-can-do-to-your-phone.html

https://definitions.uslegal.com/i/internet-security/ 7:08 PM 6/14/2018

https://www.rapid7.com/fundamentals/types-of-attacks/ 11:03 AM 6/16/2018

https://en.wikipedia.org/wiki/Malware 10:52 AM 6/18/2018

https://en.wikipedia.org/wiki/Phishing 11:22 AM 6/18/2018

https://www.acunetix.com/websitesecurity/sql-injection/ 11:36 AM 6/18/2018

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) 11:37 AM 6/18/2018

https://www.techopedia.com/definition/24841/denial-of-service-attack-dos 12:10 PM 6/18/2018

https://www.owasp.org/index.php/Session_hijacking_attack 12:22 PM 6/18/2018

https://en.wikipedia.org/wiki/Credential_stuffing 12:29 PM 6/18/2018

http://www.information-age.com/future-cybercrime-123458380/ 12:39 PM 6/18/2018