A Taxonomy on Cyber Crimes

***Abstract*—Advances in technology and the ever growing internet has opened a variety of opportunities for cybercriminals to attack innocent people through cyber crime. Cyber crime is defined as performing criminal acts on the internet or through the use of a computer. Cyber crime can be, but is not limited to identity fraud, denial of service attacks, ransomware attacks, child pornography, cyber bullying and harassment, scams, computer and network intrusions, and phishing. As these crimes continue to advance they rapidly change form leaving the public little time to re-educate themselves. As a result, the public falls victim and the cybercriminals win. This paper will address the types of cyber crimes, how the crimes have evolved, how to detect such crimes, and how to stop individuals from becoming victims by presenting a taxonomy on the families of cyber crime.**

***Index Terms*—Cyber Crime, Ransomware, Phishing, Scams, Computer and Network Intrusions, Child Pornography, Cyber Bullying and Harassment**

I. Introduction

Current period is too fast to exploit the time feature to improve the performance feature. It is happening because the use of Internet. Internet can be defined as network connection between the collection of million computers. There are many advantages with the use of Internet and also on other side there is cyber crime. The term cyber crime is defined as performing criminal acts on the internet or using a computer. Cyber crime is fast growing area of crime. Criminals are increasing day by day and they are exploiting the speed of internet, committing many criminal activities without any limits and posing a major threat to the users or targets. There are different kinds of cyber criminals such as Crackers, Hackers, Pranksters, Career criminals, Cyber terrorists, Cyber bulls, Salami attackers etc. There are different types of cyber crimes such as identity fraud, ransomware attacks, phishing, cyber bulling and harassment and computer and network intrusions. In this paper we will address the types of cyber crimes, how the crimes have evolved, how to detect such crimes, and how to stop individuals from becoming victims by presenting a taxonomy on the families of cyber crime.

II. Background and Evolution

Every so often we experience an advance in technology that is so revolutionary that it not only transmutes the way that societies interact, it additionally has a fundamental effect on the demeanor of the malefactor element within that society: introducing thoroughly incipient and antecedently unheard of the words into our everyday language utilization. Henry Fords invention of the motor car is a classic example of this point. [1]

Albeit you may get general accord among malefactor bulwark lawyers that cybercrime has been the most recent diehard vicissitudes in the malefactor deportment, it is unlikely you will receive the same concurrence when it came to defining what cybercrime genuinely was. Nevertheless, broad concord would most probably accede that cybercrime is a term of language used to describe the criminal activity that utilizes an element of the computer or computer network.

Thus, essentially there are two separate and distinct elements to cybercrime. On the one hand you would have an element of utilizing impuissance in the computer operating system or computer network. Furthermore you have an element of exploiting gregarious fabric of the computer network, whereby a malefactor makes utilization of the computer network to infiltrate the trust of other users of that computer network for the profit or gain. Albeit these different elements of what constitute cybercrime may not seem over consequential, they do have an impact when optically canvass the evolution and development of cybercrime. [2]

The evolution of digital technology began around 1960s following the advancement in information and communication technology.

The 1960s Phase the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology. Offences focused on physical damage to computer systems and stored data. 1970s Phase the use of computer systems and computer data increased further. Hackers and crackers -With falling prices, computer technology was more widely used within administration and business, and by the public. New forms of computer crime were recognized e.g. illegal use of computer systems, manipulation of data and computer-related fraud. A debate about legal solutions started in different parts of the world. Us Draft Bill to solve the problems. 1980s Phase personal computers became more and more popular. It caused increase in the number of potential targets for criminals. The increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. The spread malicious software, and more and more computer viruses were discovered. The Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. 1990s Phase The introduction of the graphical interface (WWW) in the 1990s. Rapid growth in the number of Internet users led to new challenges. - Information legally made available in one country was available globally even in countries where the publication of such information was criminalized. Challenging in the investigation of transnational crime was the speed of information exchange. Attempts UN General Assembly

Resolution 45/121 adopted in 1990. [3]

The 21st Century Phase The new trends in computer crime and cybercrime continued to be discovered in the 21st century. New millennium was dominated by new, highly sophisticated methods of committing crimes, such as phishing and bot-net attacks. Offenders became able to automate attacks, the number of offences have increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority. Types of Cybercrime Credit card frauds Cyber pornography Sale of illegal articles-narcotics, weapons, wildlife Online gambling Intellectual Property crimes- software piracy, copy-right infringement, trademarks violations, theft of computer source code Email spoofing Forgery Defamation Cyber stalking Cyber terrorism

III. Cyber Crime Types and Detection Techniques

A. Ransomware

1) Definition: A type of scareware that typically locks or encrypts a users system. It then displays a message to the user asking for some ransom to be paid in order to unlock or decrypt the system. In [4] it states, the core parts of ransomware attacks lack the technical complexity to carry out a successful attack. Only a small part of the attacks collected, actually took control of the victim's resources and could cause serious damage. The other attacks simply tired to take control of the victim's resources, but failed to do so completely. Ransomware attacks play off the fear of the victim. The victim is so afraid to lose their files or get embarrassed by the information released that they fail to investigate if the resources are truly taken before paying the ransom. In most cases the information taken hostage is never decrypted or unlocked.

Ransomware can be installed on a user's computer by the user navigating to a malicious site such as pornography. The user then clicks on an ad which triggers the invisible download of ransomware. The user is unaware of the download hence the term invisible. Another way for ransomware to be installed is called a drive-by download where the user browses to a site that has a hidden iframe. The hidden iframe then connects to another site that triggers an invisible download of ransomware. The ransomware then looks for unpatched holes in the system to infect [5]. Once a system is infect, the ransomware executes and takes the user's system hostage. There are many types of ransomware, but the two most common are Crypto Ransomware and Locker Ransomware.

Locker Ransomware locks the user's system to prevent the user from accessing it. The malware works by locking the desktop or the device's user interfaces [6]. Locker Ransomware is the least threatening out of the two due to the simple fact that Locker Ransomware leaves the system files untouched. This means the malware can be removed and the victim's computer can be restored. As a result, Locker Ransomware is not as effective as Crypto Ransomware in obtaining the ransom.

Crypto Ransomware encrypts the user's personal files. This malware leaves the computer available for usage, but the user's most important files are inaccessible [6]. Crypto Ransomware is very effective because it searches the user's computer for important files without the user's knowledge. Once it finds all the important files, it then decrypts the files prohibiting the user from accessing the files.

In both cases, ransom messages such as the one shown in Figure 1, usually resemble local police or government messages. These messages are displayed to the user stating they have committed some crime and must pay a fee to remove the message or get out of trouble. The payments are usually made through some form of untraceable payment method such as bitcoins.

Fig. 1. Example of Ransomware Message [5]

2) Impact: Ransomware is a profitable business. The key behind being successful is to increase the number of computers infected per day and charge a good amount for the ransom. [5] shows that 2.9% of people infected with ransomware tend to pay the ransom. A study was conducted where 5,700 computers were infected with ransomware in one day with the ransom set at $200 per ransom. Out of 5,700 infected computers, 169 people paid the ransom which means the attacker made $33,600 in one day; keeping in mind the attacker will lose money attempting to launder the money and change it over from bitcoins. Ransomware attacks can charge anywhere from $50 to $200 for ransom. The study proved an attacker could make up to $394,400 in one month.

3) Current Events: Ransomware is currently on the rise. On Jan.12, 2017, just eight days before the president's inauguration, the Washington D.C post reported 70% of the police surveillance cameras were attacked with ransomware. Out of 187 network cameras 123 were infected with two different types of ransomware. The Office of the Chief Technology Officer stated no ransom was paid and they were able to remove the ransomware. [7]

Another attack occurred in St. Louis, paralyzing 16 libraries. 700 computers were attacked and the attackers request $35,000 for ransom. The attack froze the libraries' system making it impossible for employers to check emails as well as making it impossible for the public to use the computers, borrow or return books. Instead of paying the ransom, the city decided to wipe the system clean and rebuild from scratch. The city

has rebuilt the system to allow the public access to books, but the computers are still off limits which hinder the children because a lot of them do not have internet access at home. [8]

The third attack occurred at a Texas Police Department. The ransomware got into the system by an employee clicking on a link in an email which infected the server. The attacker requested $4,000 for the ransom. The department decided not to pay the ransom and the server had to be wiped of all infected files. This means the police department lost eight years worth of evidence and information. The department did have some hard copies of information, but some data was still lost. [9]

In all the events mentioned above none of them decided to pay the ransom because there is no guarantee your files will be returned. However, the most advanced ransomware attacks have proven to return the user's files to encourage victims to keep paying the ransom. The attacks that do not return the files either fail to execute the crypto correctly; therefore allowing the system to recover, or fail to provide the key after receiving payment. These such attacks are making it difficult for the advanced attackers to keep people paying the ransoms. [9]

4) Detection Methods: There are multiple studies being conducted on ways to detect ransonware. The two studies mentioned in this paper are UNVEIL and AESOP.

UNVEIL is a kernel level system that uses file monitoring and desktop monitoring to detect ransomware. In order for a ransomware attack to be successful it must alter either the user's files or the desktop. UNVEIL uses an artificial user environment to analyze the interaction of ransomware with the user's files or the desktop. In a previous study, [4] done by the same author who development UNVEIL, a collection of ransomware samples revealed to have common I/O requests. These I/O request resemble patterns that were repeated for each file during an attack. These patterns allow the file system monitor in UNVEIL to be very effective.

The file system monitor has direct access to data buffers involved in I/O requests, giving the system full visibility into all file system modifications. Each I/O operation contains the process name, time stamp, operation type, file system path and the pointers to the data buffers with the corresponding entropy information in read/write requests. The I/O traces are referred to as access paths which are represented by the following tuple:

$$ti = \langle P, F, O, E \rangle \tag{1}$$

- P is the set of user-mode processes,
- F is the set of available files,
- O is the set of I/O operations, and
- E is the entropy of read or write data buffers

As a result of each ransomware family using the same specific strategy to deny access to user's files, UNVEIL was able to extract these I/O access patterns as a distinctive I/O fingerprint for a particular ransomware family. The key behind file system monitoring is to sort the I/O request per file thus revealing the I/O access patterns. Most ransomware types typically aim to encrypt, overwrite, or delete the user's files at some point during an attack which creates these I/O access patterns. The Figure 2 below shows different ransomware families and how they attack the file system. [10]

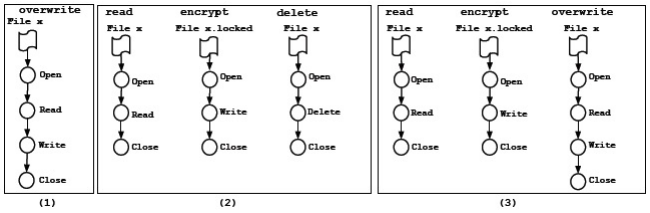


Fig. 2. Strategies differ across ransomware families with respect to I/O access patterns. (1) Attacker overwrites the users file with an encrypted version; (2) Attacker reads, encrypts and deletes files without wiping them from storage; (3) Attacker reads,creates a new encrypted version, and securely deletes the original files by overwriting the content. [10]

The second part of UNVEIL is the desktop monitoring. This component of UNVEIL is for the detection of locker ransomware which usually locks the user's desktop and displays a ransom message. UNVEIL tries to predict locker ransomware by capturing screenshots of persistent changes to the desktop. These changes are ones that are not easily dismissed by the user. This coincides with the ransom message that is displayed to the user during an attack which is also persistent. Once UNVEIL captures the screenshot, it clears the screenshot of opened windows and only focuses on the persistent image. It extracts the text from the image and searches for words that usually appear in ransomware messages to determine if the persistent image is a ransom message. [10]

UNVEIL's file system monitoring is an excellent tool and is highly effective. The only draw back would be if the attacker found a way to bypass the artificial user environment using some VM detection method. The other draw back to UNVEIL is the desktop monitoring component. There are other ways for an attacker to lock a user's desktop such as video or audio files which don't have text. Furthermore, the text search algorithm presented in the paper can be more robust.

Aesop, is a scalable algorithm that identifies malicious executable files by applying Aesops moral that "a man is known by the company he keeps". [11] Aesop uses Jaccard similarity to find the overlap of files on different machines. It then uses Locality-sensitive hashing (LSH) to approximate clustering and near-neighbor searching. Its main idea is to use multiple hash functions to map items into buckets. This allows for similar items to be hashed to the same bucket. Note that a file can be in multiple buckets. After everything is grouped into buckets, it then creates a file relation graph. A file relation graph is an undirected, unweighted bipartite file-bucket graph with two nodes; a file node and bucket node. A file inside a bucket is represented by an edge connecting the file node and the bucket node. This graph is then converted into a pairwise Markov random field (MRF) which computes the marginal probabilities $Pr\left(X_{f_i} = x_g\right)\ and\ Pr\left(X_{f_i} = x_b\right)$ for unlabeled files by using the Belief Propagation algorithm. These two labels, good and bad, determine whether a file is

malicious or benign. [11]

Aesop can determine malicious files a week before they are labeled by anti-virus technologies. It has a .0001 false positive rate and .9961 true positive rate [11]. The false positive rate is in large part due to rare files such as personal files or programming files that are not deployed on other machines. Since there is no data for these files it is hard for Aesop to label them.

In conclusion, both techniques Aesop and UNVEIL are accurate tools to detect ransonware using file metadata. Aesop is better at detecting all types of malicious software whereas UNVEIL is only good at detecting ransomware software. Both of the techniques have flaws such as not being able to detect new files or new types of ransomware that has not yet been seen which is highly likely because malicious software developers are creating more advance attack software each day.

B. Computer and Network Intrusions

1) Definition: In general Intrusion is an activity by a user of an Information System who was not legally allowed to take a particular action. The user is referred as an Intruder. The intruder may come from outside, or the intruder may be an insider, who goes beyond is limits of authority to take actions. Whether or not the action is determined, it is of concern because it might be detrimental to the health of the system, or the service provided by it.

Intrusion Detection (ID) is a type of security management system for computer and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify passive security breaches, which include both type of intrusions outside (attack from outside of an organization) and misuse (attack from within the organization). ID uses vulnerability assessment which is a technique (scanning) developed to assess the security of the computer systems.

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the passive component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the active component: mechanisms are set in place to reenact known methods of attack and to record system responses

2) Impact: Protection of information has been a major challenge since the beginning of the computer age. Given the widespread adoption of computer technology for business operations, the problem of information protection has become more urgent than ever. Computer files, databases, networking and the Internet-based applications all have gradually become part of the most critical assets of an organization. When these assets are attacked, damaged or threatened, data integrity becomes an issue and the proper operation of the business may be interrupted.

The problem of protecting data and information on computers has become even more critical and challenging since the widespread adoption of the Internet and the Web. The Internet has made computers across the globe interconnected. Despite the convenience of data sharing and information exchange, the Internet has also become the major highway for computer viruses to travel on. Instead of infecting one computer at a time by spreading the virus via floppy diskettes, the attackers/hackers use the Internet as the transmission channel to spread their attacking agents. Whether the spreading mechanism was a computer virus or a worm, thousands of computers could be affected within a short period of time.

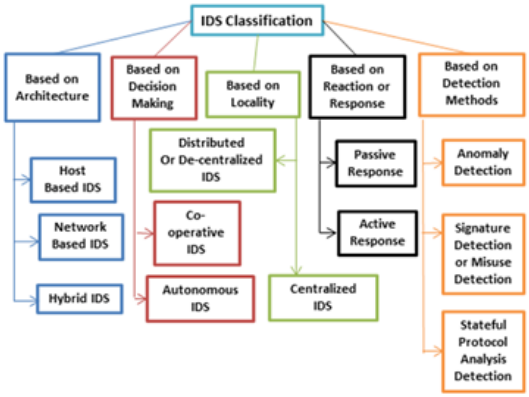
3) Current Events: Protection of information has been a major challenge since the beginning of the computer age. Given the widespread adoption of computer technology for business operations, the problem of information protection has become more urgent than ever. Computer files, databases, networking and the Internet-based applications all have gradually become part of the most critical assets of an organization. When these assets are attacked, damaged or threatened, data integrity becomes an issue and the proper operation of the business may be interrupted.

The frequency and cost of the cyber attacks increased in the last 12 months. The average annualized cost incurred by a benchmark sample of US organizations was about 78 percent more than the cost estimated in the first analysis conducted four years ago.

In spite of improvements in defense mechanisms and the increased level of awareness of cyber threats the cybercrime ecosystem is able to adopt even more sophisticated cyber attack techniques. The cybercrime industry has shown great spirit, and the adaptive capacity to respond quickly to countermeasures has been taken by the police

4) Detection Methods: Intrusion detection systems (IDS) can be classified into different ways. The major classifications are Active and passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS)

You use an IDS to monitor your network for signs of intrusive activity. An IDS triggers alarms when it detects intrusive activity. The triggering mechanism is probably based on one of the following two techniques: Anomaly detection Misuse detection To implement its triggering mechanism, your IDS needs to monitor your network for intrusive activity at specific points in your network. The two common monitoring locations are as follows: Host-based Network-based Because each of these characteristics has benefits and drawbacks, many intrusion detection systems are beginning to incorporate multiple characteristics into hybrid IDSs. These systems attempt to maximize the capability of the IDS while minimizing their drawbacks.



a) 4.1 Anomaly Detection: The anomaly based detection is based on defining the network behavior. The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators The important phase in defining the network behavior is the IDS engine capability to cut through the various protocols at all levels. The Engine must be able to process the protocols and understand its goal. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms. The major drawback of anomaly detection is defining its rule set.

The efficiency of the system depends on how well it is implemented and tested on all protocols. Rule defining process is also affected by various protocols used by various vendors. Apart from these, custom protocols also make rule defining a difficult job. For detection to occur correctly, the detailed knowledge about the accepted network behavior need to be developed by the administrators. But once the rules are defined and protocol is built then anomaly detection systems works well. If the malicious behavior of the user falls under the accepted behavior, then it goes unnoticed. An activity such as directory traversal on a targeted vulnerable server, which complies with network protocol, easily goes unnoticed as it does not trigger any out-of-protocol, payload or bandwidth limitation flags. The major advantage of anomaly based detection over signature-based engines is that a novel attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns. This is observed when the systems detect new automated worms. If the new system is infected with a worm, it usually starts scanning for other vulnerable systems at an accelerated rate filling the network with malicious traffic, thus causing the event of a TCP connection or bandwidth abnormality rule.

b) 4.2 Signature Based IDS: Signature Based Detection Signature detection involves searching network traffic for a series of malicious bytes or packet sequences. The main advantage of this technique is that signatures are very easy to develop and understand if we know what network behavior we are trying to identify. For instance, we might use a signature that looks for particular strings within exploit particular buffer overflow vulnerability. The events generated by signature based IDS can communicate the cause of the alert. As pattern matching can be done more efficiently on modern systems so the amount of power needed to perform this matching is minimal for a rule set. For example if the system that is to be protected only communicate via DNS, ICMP and SMTP, all other signatures can be ignored. Limitations of these signature engines are that they only detect attacks whose signatures are previously stored in database; a signature must be created for every attack; and novel attacks cannot be detected. This technique can be easily deceived because they are only based on regular expressions and string matching. These mechanisms only look for strings within packets transmitting over wire. More over signatures work well against only the fixed behavioral pattern, they fail to deal with attacks created by human or a worm with self-modifying behavioral characteristics.

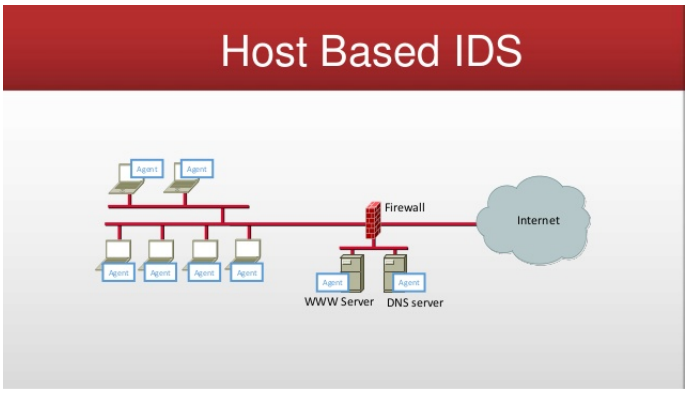
Signature based detection does not work well when the user uses advanced technologies like nop generators, payload encoders and encrypted data channels. The efficiency of the signature based systems is greatly decreased, as it has to create a new signature for every variation. As the signatures keep on increasing, the system engine performance decreases. Due to this, many intrusion detection engines are deployed on systems with multi processors and multi Gigabit network cards.IDS developers develop the new signatures before the attacker does, so as to prevent the novel attacks on the system. The difference of speed of creation of the new signatures between the developers and attackers determine the efficiency of the system.

c) Host Based IDS: Host-based intrusion detection systems are aimed at collecting information about activity on a particular single system, or host. These host-based agents, which are sometimes referred to as sensors, would typically be installed on a machine that is deemed to be susceptible to possible attacks. The term host refers to an individual computer, thus a separate sensor would be needed for every machine. Sensors work by collecting data about events taking place on the system being monitored. This data is recorded by operating system mechanisms called audit trails.

Other sources from which a host-based sensor can obtain data, include system logs, other logs generated by operating system processes, and contents of objects not reflected in standard operating system audit and logging mechanisms. These logs are for the most part simple text files, which are written a few lines at a time, as events occur and operations on a system take place. As host-based systems rely heavily on audit trails, they become limited by these audit trails, which are not provided by the manufacturers who design the intrusion detection system itself. As a result, theses trails may not necessarily support the needs of the intrusion detection system, leading some to conclude that having more effective host based systems, may require the developer to amend the operating system kernel code to generate event information. This approach extracts a cost in performance, which might be unacceptable for customers running computationally greedy

applications . Despite this limitation, audit trails are still considered to be the source of choice for host-based intrusion detection information. This continues to be true, first, because of the existing aim of operating systems at protecting its audit layer; and second, for the level of detail that audit trails provide. Clearly, considering the objective of intrusion detection systems, the detail provided is particularly important in analyzing patterns of attack. More importantly, [the] information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction. The fact that audit trails are protected by the operating systems itself offers some assurance that audit trails have not been improperly modified. The information collected through audit trails can arm the host-based sensor with useful data about the system and its users.

For example, audit trails may contain information about subjects responsible for an event, as well as any objects related to that event. The host-based sensor can recover which process initiated an event, and the current and original user identifications associated with that event, in case the user identification changes. These pieces of data can be crucial in determining from what program and by what user a potential network attack originated, which will obviously help in stopping future attacks. However, in the case of an attack from within, this may also be useful in determining culpability in order to pursue punitive measures against the user. As useful as the data is, a common criticism of host-based systems lies with the amount of data they can offer. The configuration of the sensors must obviously collect detailed enough information to identify abnormalities on a host, so the more refined the data captured, the better the sensor should work. The problem is that, as the sensors gather finer levels of detail, they accumulate large amounts of data that take up significant storage.



In addition, because, both the volume and complexity of the data rise with greater detail it makes it difficult for an adversary to circumvent the audit process entirely, the greater volume and complexity of the data make it easier in practice for intruders to hide their footprints. This sort of irony becomes the burden that designers and analysts must overcome so that host-based sensors avoid becoming cumbersome, while remaining effective. Host-based intrusion detection systems are desirable for several reasons. As briefly mentioned above, because host-based systems can monitor access to information in terms of who accessed what, these systems can trace malicious or improper activities to a specific user ID. This is always important as it can identify whether a person inside the organization is responsible for the improper use of company resources, for example, if a persons desk computer is being used to launch network attacks. The problem then is to determine if that employee at any time had knowledge of the illicit events. Host-based sensors are also useful in that they can keep track of the behavior of individual users.

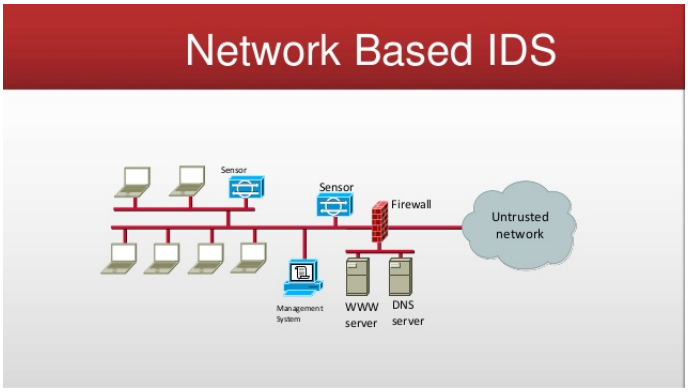
This can help catch attacks while they are happening or possibly stop a potential attack before it affect the system. If a pattern is observed that is similar to past attacks or that is suggestive of an attack, activity to and from that workstation can be stopped, foiling the attack. This ability can be an especially useful in systems in which remote access to system resources is common. Host-based systems are valuable in that they are, in some ways, very versatile. They have the ability to operate in environments that are encrypted, as well as over a switched network topology.

d) 4.4 Network Based IDS: Network-based intrusion detection systems offer a different approach. These systems collect information from the network itself, rather than from each separate host. They operate essentially based on a wiretapping concept, information is collected from the network traffic stream, as data travels on the network segment. The intrusion detection system checks for attacks or irregular behavior by inspecting the contents and header information of all the packets moving across the network. The network sensors come equipped with attack signatures that are rules on what will constitute an attack, and most network-based systems allow advanced users to define their own signatures. This offers a way to customize the sensors based on an individual networks needs and types of usage. The sensors then compare these signatures to the traffic that they capture, this method is also known as packet sniffing, and allows the sensor to identify hostile traffic. Using network data as a primary source of information is desirable in several ways. To start, running network monitors does not degrade the performance of other programs running over the network. This low performance cost is due to the fact that the monitors only read each packet as they come across its network segment.

The operation of the monitors will be transparent to system users, and this is also significant for the intrusion detection system itself. The transparency of the monitors, decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without significant effort. This decreased vulnerability strengthens the intrusion detection system, and adds another measure of security. From a financial perspective, network based systems are very desirable. The primary resource for these monitors is storage space, so companies could use older and slower equipment to do this work, rather than purchase additional equipment. This could significantly save on deployment costs. Network-based systems are also extremely portable. They only monitor traffic

over a specific network segment, and are independent of the operating systems that they are installed on. Deployed network-based intrusion detection sensors will listen for all attacks, regardless of the destination operating system type. This offers more options for businesses that run specialized software or software they have developed in-house, which will become increasingly attractive as the newer UNIX-based operating systems continue to increase in popularity. Adding to their convenience, network-based sensors can be inserted easily on part of a network and data can be collected with minimal work. In many cases, all that is required to collect information for analysis is the configuration of a network card. This is beneficial in situations where network topology changes or where system resources have been moved, the intrusion detection system monitors can be moved and used as needed.

However, network-based solutions have their share of problems. As discussed earlier, the sensors spot attacks based on their attack signatures. These signatures are written based on data collected from known and previous attacks, and this unfortunately ensures that these signatures will always be a step behind the latest underground exploits. What is worse is that, although intrusion detection system vendors offer regular updates to their signature databases, many have not caught up in defining signatures for all known attacks. While these systems can still prevent many attacks, serious coordinated attacksthe kind for which no signatures have been predefined– have the potential to do the most damage. The second major issue with network-based intrusion detection approaches is scalability.



Network monitors must inspect every packet that is passed through the segment they are placed on. It has been demonstrated that network-based systems have difficulty keeping up on 100 Mbps environments, they simply cant handle it, and now the trend is moving toward gigabit speeds. As these high-speed networks become more common, intruders will be able to identify them, and they will no doubt be targeted with attacks gauged at specifically exploiting this weakness. Strategic placement of network sensors can help to alleviate this, but systems with heavy traffic will still encounter this problem. Encryption and switching represent two further limitations of network-based approaches. First, if network traffic is encrypted, an agent cannot scan the protocols or the content of these packets. Second, the nature of switches makes network monitoring extremely difficult. [I]n the case of switched networks the network switch acts to isolate network connections between hosts so that a host can only see the traffic that is addressed to it. In these cases, a network-based monitor is essentially reduced to monitoring a single host, defeating much of the intent of the monitor. Some switches can now support a port for monitoring and scanning, which offers a partial solution to this problem.

In addition, network monitors are unable to see traffic travelling on other communication media, such as dial-up phone lines. This is an increasing concern as organizations employ a greater number of telecommuters, since their traffic cannot be monitored using this approach. This problem is part of a larger issue. The network sensors have a degree of blindness to host activity. Although some network-based systems can infer from network traffic what is happening on hosts, they cannot tell the outcomes of commands executed on the host. This is an issue in detection, when distinguishing between user error and malfeasance. This limitation could lead to numerous false-positives, which is an undesirable situation where an intrusion detection system falsely identifies something as an attack. Intrusion detection systems are configured and signatures are carefully written to minimize the instances of false positives [12] [13] [14] [15]

C. Scams and Phishing

1) Definition: Phishing is a form of online identity theft that aims to snip complex information such as thieving credit card information and online banking passwords from users [16]. Phishing is also known as carding or brand spoofing, it describes different types of scams that use duplicitous e-mail messages, sent by criminals, to distort you into revealing your personal information or into unintentionally downloading malicious computer code onto their computers that can allow the criminals consecutive access to the users computers or financial accounts.

For scammers, people who are using emails are always target. [17] When someone ask, ”what is phishing?” the most common situation is as follows: Someday all of sudden you open your e-mail account and there you see an alert from the bank stating that an unauthorized person tried to sign in into your account and it says to change the password for further safety and they do even provide link to the bank site, that is where you make mistake when you click on that link it redirects you to the dummy site which looks as exactly as original bank site, there you try to login with your login credentials, you dont even realize that your information is going to stole and second time they redirect you to the original site. Hackers first used the term phishing to express stealing America Online (AOL) accounts by collecting usernames and passwords. Phishing, identity theft and/or identity fraud are sometimes compatible.

2) Impact: The impact of phishing is far more deceptive than just an attack of privacy. Through social engineering, phishing is used to conciliate computer security. Phishing can be used to hack your computer, steal your identity, steal financial accounts or to terminate important information. When it comes to the impact of phishing on people and society [16], phishing scams are really destructing the internet. There is always some kind of scams in your e-mail junk folder or advertisements on Facebook or any other social networking the links always try to redirect to a misleading website. With the rapid growth in technology of phishing and rise in social networking, people who are sharing their information online are posed to greater risk. Online shopping is very popular these days as user just needs a computer or any mobile device that is connected to internet. Let us consider an example, China has the most internet users than any other country in the world, there are about 250 million of them use online business or online shopping. Official reports say that everyday there are like 15 thousand phishing websites are being created, of them 95% are auto-generated by hackers computers themselves. Phishing attacks or any other similar kind of traps are being encountered by people that are using online shopping. According to an online survey 85% of the phishing websites are watched by both consumers and suppliers and 20% of the phishing are succeed. In the past year, more than 80 million people were tricked out of $8 billion dollar by the phishing websites in China.

On Business: Phishing indicates one feature of the progressively complex and converging security threats facing businesses today. Many companies are employing a very good amount of money on safety tools. Though many firewalls and anti-malware software provide little protection against the attacks of phishing which tricks the user into downloading the malicious code into the user computer or stealing the credentials. Phishing attacks are majorly on the businesses and organizations, according to the report titled Cost of Phishing and Value of Employee Training published by the Ponemon Institute described the trends behind phishing. According to them the attacks of phishing can be direct or indirect, Institute researchers surveyed about 377 IT and IT security professionals to know more about the financial effects of phishing scams and its impact on employee productivity. Researchers of that institute evaluate the cost to contain malware, malware that is not contained, productivity losses etc. Ponemon institute research report derives, Researchers calculated the total annual cost of phishing for the average-sized organization which is about $3.77 million. Phishing attackers normally tries to hack or steal the information from the higher level employee from a company or an organization. Attacker usually send an email titled as final report or daily report, then employee tries open the report which has malicious code in it which may send the employee details such as credentials and company or organizations financial records. Phishing attacks have serious affects on the companies brand and reputation.

3) Current Events: APWG(Anti-Phishing Work Group) recently announced that they have recorded highest number of phishing attacks in 2016 than any year since it began monitoring in 2004. According to them 1,609 phishing attacks were recorded per month in the fourth quarter of 2004, where as in fourth quarter of 2016 it increased by 57.53% over 12 years with 92,564 phishing attacks per month.

Cost for 10,000 employee organization	Cost per Employee	Percent cost	
Cost to contain malware	$208,174	$22	6%
Cost of malware not contained	$338,098	$35	9%
Productivity losses from phishing	$1,819,923	$191	48%
Cost to contain credential compromises	$81,920	$9	2%
Cost of credential compromises not Contained	$1,020,705	$107	27%
Total deduced cost $3,768,820	$3,768,820	$395	100%

Fig. 3. Table is according to the Ponemon Institute researchers report

Phishing scammers were made their way to social media, where there can easily trick people by that collecting their personal information and credentials. Over a year, the number of phishing attacks on social media accounts such as Facebook, Twitter, and Instagram etc were increased by 150%. Social media is best way for scammers to trick or steal information from thousands of users at once.

Recent phishing attack was on the snapchat employee of pay roll department, where he ended up with revealing the personal information of their current and former employees. [18] A fake email of phishing attack was sent to the employee at the College of Southern Idaho(CSI) asking for the employees W-2 forms of every CSI employee from the year 2015-2016. There are about 2500 employees personal information was released with this attack. This attack released the information such as employees addresses, wages and social security numbers.

[19] Smishing means SMS-based mobile phishing is a newly discovered phishing campaign is counterfeiting texts from the Czech Republics postal services, tried to trick by downloading a malicious app which contains a trojan horse which is deigned to steal the credit card information from the mobile device owners. When victim tried to download the app and tried to open app, automatically receives a request asking for their credit card or other personal information then after send that information to the hackers server or computer.

4) Detection Methods: Phishing attack performs mainly four steps [20], they are

1) Attacker creates a fake website or buy a domain and then they try the fake website to look like a legitimate site, they even create a web server, DNS server name, and even web pages very similar to actual website.
2) Then attacker sends large number of hoaxed emails to the users usually called targets.
3) The receiver receives the spoofed email which he or she is not aware of and opens it, and gives the required information such as sensitive information (Credit card numbers, Social security numbers etc)

4) Finally, phishers steal the personal information and they go according to their plan or scam such as transferring money from the targets or victims account.

There are different detection techniques to identify the phishing one of them is AntiPhish technique which was proposed by Engin Kirda and Christopher Kruegel [21], as per them phishing attacks have been increasing from the past three years and this AntiPhish technique protects the innocent users from the website based phishing attacks. A new technique called PHONEY was proposed by Madhusudharan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya [21], where it automatically detects and examines the phishing attacks. What exactly this technique does is it protects the user by providing the false information to the website, this can also be added to their internet browser as extension to diminish the web based phishing attacks. Maher Aburrous, Fadi Thabath proposed a novel approach for detecting the phishing website, it is based on fuzzy logic combined with data mining algorithms. There are four major steps in the above mentioned approach: Fuzzification, Rule Generation using Classification Algorithms, Aggregation of the rule outputs and Defuzzification. A new algorithm named Linkguard algorithm was proposed by Nikesh Surana, Prabhjot singh, Umesh Warade, Neha Sabe [21]. This algorithm helps the users from phishing attacks, what it does is, it uses the features of hyperlinks and there by analyze the change among original and visual link.

a) Anti-Phishing Techniques:: Anti-Phishing defenses can be majorly split in to two types of solutions [22]

1) Server based solution
2) Client based solution

Server Based:majorly these techniques are implemented by service providers and composed of three different types, they are as following

- Brand Monitoring: Here online websites are cloned to identify clones which are considered as phishing pages. If the websites are alleged as phishing pages then they are added to the centralized black list which further blocked.
- Behavior Detection: By observing the users online behavior we can detect the phishing website, where finding out the websites that users have visited and information submitted to those websites.
- Security Event Monitoring: To detect the unusual activity of a subsequent attack, the registered events which are provided by the several sources are being used by the security event analysis and correlation.

Client Based:This technique is based on the users view through browser plug-ins or email clients and composed of three different types:

- Email based analysis: This approach uses Bayesian filters.
- Black lists: Its kind of technique where we put or gather a list of urls which are identified as malicious. This list is loaded by the browser when user tries to open any website if that url is found in that list then it advises as harmful otherwise as legitimate.
- Information flow: This process based on the principle that while the user can be easily tricked by a counterfeited domain name, a program will not run. AntiPhish is an exact example of this type of technique which keeps the track of personal or sensitive information when the user entered in any login page or webpage, if it thinks the information is not safe it will pops up or raise an alert.

D. Child Pornography

1) Definition: As technology is moving much faster than the Act, crimes committed through social media are often put away by applying existing status. According to the federal law Child pornography is any visual direction of sexually explicit conduct involving a minor. It is also define as any representation of a child engaged in real or simulated explicit sexual activities or of the sexual part of a child for primarily sexual purposes. [23], [24] Many states in US have defined what actually sexually explicit conduct means or what do you mean by minor. Such as,

- Massachusetts defines its law of Child Pornography as engage with indecent intent, in the representation of a nude minor in any visual material.

- In South Carolina, the judge or jury may infer that the participants in suspect child pornography are minors based on the material or the title or text.

- Utahs defines the sexually explicit content which includes actual or simulated explicit representation of excretion or ejection functions

Visual interpretation of containing child pornography are assumed Illegal under federal law. This may include Photographs, Videos, digital download, undeveloped film and video and electronically stored data. Sexual activity is not needed in the image to be considered pornography. The image may contain the nude picture of a child that is assume sexually symbolic and be considered as illegal.

Laws Controlling Child Pornography:-

The concrete kind of charge varies depending on the situation and rigor of infringement. Not all cases are charged as federal cases; however, all cases involving the cyber world will be covered under federal law. States may file charges against a suspect in additament to federal charges. Penalties may vary predicated on sundry actions regarding the engenderment, possession or distribution of child pornography. This includes any activity cognate to the categories of filming or photography, storing on a computer hard drive, DVD or hard copies and the distribution and sale of the material through any and all betokens. Any acts that affect interstate or peregrine commerce such as distributing items through the Coalesced States mail or across state or international lines will be considered a federal offense.

Federal jurisdiction applies similarly when the Internet is utilized to transfer pornographic images or videos of minors across state lines. This standard is so rigorous that, even if the pornographic depictions themselves did not peregrinate across state or international borders, federal law may be involved if the materials utilized in the transfer, such as the computer

used to download the replica or the CD Rom used to store the material, originated or up to that time moved in interstate or peregrine commerce. If there is the most diminutive connection at all, federal laws can be implicated. Included in the international control of child pornography engenderment is Section 2260 of Designation 18 of the Amalgamated States Code. This particular section proscribes any persons outside of the Amalgamated States to competently engender, assemble, convey, distribute or allot child pornography with intent to import or spread the pornographic depictions into the Cumulated States.

Section 2251 of Denomination 18 of the Coalesced States Code makes it illicit to influence, embolden, entice or pressure a minor to participate in sexually explicit demeanor for purposes of the engenderment of pornographic material. Any endeavors to transgress these laws may be considered an offense, even if the offender did not prosper in plenarily engendering the material. Section 2251A of Designation 18, concretely verbalizes that any parent, licit guardian or other individual in care of the youth cannot buy, sell or relegate custody of that minor for the purposes of making child pornography and will be penalized plenarily under federal law.

A person may be charged under both state and federal law without breaching double jeopardy enjoinments. State laws vary from federal law, but they often contain homogeneous language regarding federal charges.

2) Impact: The data in this topic primarily are derived from two separate sources: (1) the Commissions conventional annual datafiles of nonproduction offenses for fiscal years 1992 through 2010 and (2) the Commissions special coding project of virtually all cases in which offenders were sentenced under the non-engenderment guidelines in fiscal years 1999, 2000, and 2010, and cases from the first quarter of fiscal year 2012. Germane data in the Commissions conventional datafiles include rudimental demographics, malefactor history, guideline applications, sentences imposed, application of concrete offense characteristics, and sentences relative to the guideline range. Data in the special coding project supplement the annual datasets with more detailed information on offense conduct and offender characteristics. The first part of this chapter will discuss data from the Commissions annual datafiles, and the remnant of the chapter will discuss data from the Commissions special coding project. Albeit the data analyzed in the first part of this chapter generally end with fiscal year 2010 cases so as to sanction a comparison to the Commissions special coding project of fiscal year 2010 cases discussed in the second half of the chapter occasionally fiscal year 2011 data from the Commissions regular annual datafile will be noted where significant changes occurred. With respect to data from the Commissions annual datafiles, the following analysis divides cases in which offenders were sentenced under the non-production guidelines into two primary offense types based on the manner in which the guidelines were applied: (1) receipt, transportation, and distribution offenses, as well as other similar but less common offenses (e.g., importation) [hereafter collectively referred to as R/T/D offenses]; and (2) possession offenses. With respect to data from the special coding project, cases in which offenders were sentenced under the non-production guidelines are classified in greater detail based both on the most serious offense of conviction5 and on real offense conduct in the case. The data for child pornography offenses discussed in this chapter generally cover a lengthy time period (fiscal years 1992 to 2010). During that period, there were several significant changes in the legal landscape concerning constitutional law, relevant statutes, and the guidelines that affected sentencing in child pornography cases. Understanding those changes is necessary to properly interpret the data. [25]

3) Current Events: UN verbally expresses 4 staffers dismissed for sending child pornography (Associated Press / 08:04 AM October 31, 2015.) UNITED NATIONS A UN report verbally expresses four staff members have been dismissed for sending and storing child pornography on UN COMPUTERS and one more was dismissed for utilizing a UN conveyance to convey approximately 173 kilograms (381.4 pounds) of marijuana. The report, obtained Friday, DOCUMENTS about 60 cases that resulted in disciplinary measures among the UNs ecumenical staff of about 40,000 over a one year period ending June 30. It does not IDENTIFY any staffers and does not include over 100,000 UN peacekeepers, who are under the jurisdiction of their abode COUNTRIES. The cases range from a senior staff members demotion for harassing a subordinate to the dismissal of a staffer who was caught endeavoring to purloin MAZUMA from the wallet of another staffer. NBI closes child porn family business in Taguig (By: Tetch Torres-Tupas - HERALD 04:22 PM October 17, 2016).

The National Bureau of Investigation (NBI) apprehended five people behind online child pornography pretty.mirth being operated as a family business since 2011. ARRESTED last Saturday in an entrapment operation were Shaira Candaza, Feminine Candaza, Estrellita Candaza, Mary Rose Reyes and Mary Grace Cahanding. They will be charged with infringement of Republic Act 9208 or the Anti-Trafficking in Persons Act of 2003, RA 7610 or the Anti-Child Abuse Law in cognation to RA 10175 or the Cybercrime Obviation Act of 2012, RA 9775 or the Anti-Child Pornography Act of 2009, RA 9995 or the Anti-Photo and VIDEO Voyeurism Act and RA 9165 or the Comprehensive Hazardous Drugs Act of 2002. NBI, together with the Federal Bureau of Investigation (FBI), rescued two boys aged 5 and 11 and a two-year-old girl. They were turned over to the Department of Gregarious Welfare and Development (DSWD). The FBI coordinated with the NBI-Anti Human Trafficking Division (NBI-AHTRAD) after they discovered that pretty.mirth is predicated in the Philippines. FBI forwarded information to the NBI including YAHOO chat logs between the FBI undercover agent and the suspects. A surveillance operation was conducted at 27 MRT Avenue, Lower Bicutan in Taguig, the address given by the suspect in the Yahoo chat conversation. Ascendant entities discovered the suspects offer minors to foreigners for online shows and meetups for sexual acts which are paid via mazuma transfers. [26]

4) Detection Methods: The fight against child pornography could be getting an incipient high-tech implement. To avail law enforcement with the task of analyzing a suspected child pornographer's computer, incipient software developed by a computer science pedagogia at the Polytechnic Institute of Incipient York University brings effaced photographs back from the computer's trash and searches them for potentially explicit images of children and differentiates them from images of adult. The program scans for faces of children, disrobement and other features to avail flag images that could possibly be illicit contraband. Null "It utilizes machine-learning algorithms to distinguish child from not-child," verbalized Nasir Memon, a pedagogia of computer science who engendered the program with his students. "Machine learning" refers to a process by which a program learns to identify certain kinds of images by processing other kindred images. "[The program looks] at the face, skin, disrobement, other features potentially that amalgamate together, to pull out the most likely images which could be problematic," he verbalized. The program was designed to avail law enforcement, bulwark and astuteness officials and private investigators hired by the private sector, Memon verbalized. As law enforcement grapples with incrementing volumes of digital child porn, child advocates verbally express technology that can avail streamline the identification process is becoming more valuable. "It is a struggle for law enforcement who are working child porn cases," verbalized Michelle Collins, vice president of the National Center for Missing and Exploited Children's exploited children division. "Over the last few years, the size of the child porn being seized has incremented dramatically."

Program Computes Distance Between Ocular perceivers and Nasal perceiver to ID Children Memon verbalized the program computes the distance between a person's ocular perceivers and nasal discerner and other facial features to disunite children from adults, but low light and non-frontal photos can skew results. The program is about 70 percent precise in identifying images of children, Memon verbalized, but he integrated that even that prosperity rate could be auxiliary in narrowing the field for investigators building a case against a child porn suspect. Through Digital Assembly, a Brooklyn, N.Y.-predicated start-up engendered by Memon and two of his students, he antecedently relinquished a version of the software that recuperates effaced and fragmented digital images. The most incipient version of the software, called Adroit, will launch later this month and includes the incipient filtering technology. In integration to scanning for potentially explicit images of children, he verbally expressed the program can probe for explicit images of adults, photographs of a particular person and indoor or alfresco photos. Child Advocates: Size of Porn Being Seized Is Incrementing With the proliferation of more affordable computer storage and more people utilizing broadband, the average amassment of child porn seized by law enforcement is growing each year, according to Collins. Collins verbally expressed the National Center for Missing and Exploited Children avails law enforcement match found pornographic images with the people who engendered them to avail the children victimized in the process. Through the Child Victim Identification Program (CVIP), her group avails prosecutors by examining images and videos to prove that an authentic child is depicted in each pornographic photo. Each kenned pornographic image is assigned a unique identifier, which is preserved in a database. Utilizing those identifiers, law enforcement can run software to probe a suspect's computer for kenned child porn, but not incipient child porn, forensics experts verbalized. Detecting Child Porn Is Especially Challenging

Victor Fay-Wolfe, director of the Rhode Island Digital Forensics Center, verbalized his center will relinquish a downloadable program next week that is akin to Adroit that could avail law enforcement scan a hard drive for porn. With funding from the National Institute of Equity, the program examines images for skin tone, edges that betoken human forms and other features. "All of those weighted together sanction the software to determine together if it's porn," he verbalized. But he integrated that automating child pornography detection has proved especially arduous, in part because child porn laws not only apply to offenders, but those developing technology intended to avail prosecute them. "Child pornography is a different story," he verbally expressed. "We're finding it to be a profoundly arduous quandary." Detection software needs a straight on image of a face, which you don't often get in child pornography, he verbally expressed. Photos of genitalia would be more efficacious, but utilizing those is illicit. "That's the best we can indite without having contraband," he verbalized. Digital Forensics Expert: Some Detection Is Better Than None Fay-Wolfe verbalized programs engendered to detect child pornography are at most 60 percent precise. But even that could potentially avail law enforcement, he verbally expressed. "Even 50 percent precision is a sizably voluminous savings of time to them," he verbally expressed. "Some detection is better than none, when they have nothing to avail them." Still, though technology may avail an investigation into a child porn suspect, law enforcement officers verbalize that it's ultimately the human investigators who makes the most astronomically immense difference. "The adeptness and experience of our investigators, along with the astuteness we develop, is our most vigorous asset in pursuing these malefactors," verbalized Peter Grossgold, an FBI special agent who supervises the squad that investigates child pornography cases in the Incipient York office. [27]

E. Cyber Bullying

1) Definition: According to a website of the U.S. Department of Health and Human Services, cyberbullying is bullying, which is willful and repeated harm [28], that takes place using electronic technology devices and equipment (cell phones, computers and tablets as well as communication tools such as social websites, text message, chat and websites) [29].

The term cyberbullying is mostly applied to kids among 6-18 years old [30] or school aged children [31]. Although there still are researches considering the involvement of adult in unwanted, aggressive behaviors as bullying [30], but it is

actually not defined as bullying. Once adults are involved, those kinds of actions are called cyber-harassment or cyber-stalking [32] and can be addressed in very serious approach by state and federal laws [33].

2) Impact: Generally, cyberbullying has negative impacts on students academic performances, emotional and psychological health, and other behaviors such as [29]:

- Use alcohol and drugs
- Skip school and unwilling to attend school
- Experience in-person bullying
- More health problems

Negative impacts of bullying can be long term, can even continue into early adulthood [34]. A study also found out that both as victims and offenders, had significantly lower self-esteem than those who have little or no experience with cyberbullying [35]. Emotional consequences that victims experience consist of feeling frustrated, angry, sad, vengeful, helpless In 2007, a study about how victims felt lead to a result of 34% of bully victims felt frustrated, 30.6% felt angry, and 21.8% felt sad. It also shows that the results about feeling frustrated and angry are relatively equal across all level of school, while a much higher proportion of elementary students felt sad compared to other groups [36].

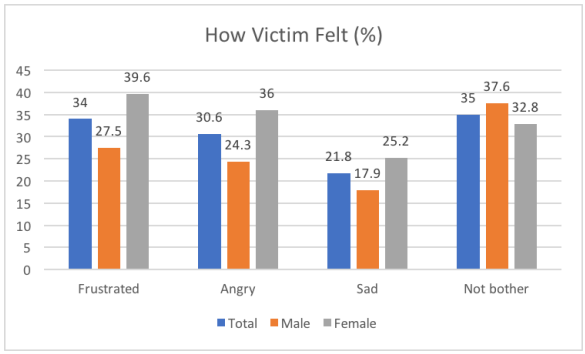


Fig. 4. How Victim Felt (Gender) [36]

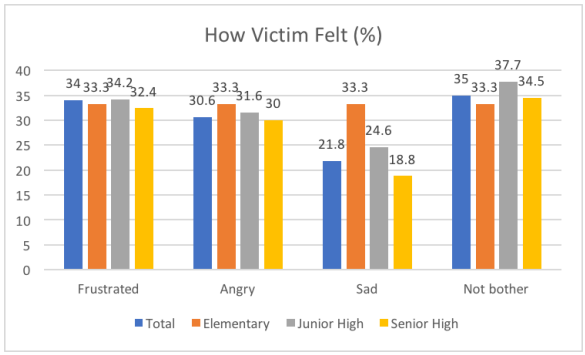


Fig. 5. How Victim Felt (school level) [36]

Cyberbullying in extremely case can lead to serious violence and even suicidal thoughts [37]. A study by Patchin and Hinduja, 2010 shows that victims of cyberbullying were twice as likely to attempt suicide compared to those who were not victims [38]. Cyberbullying is a growing problem with the advanced development of electronic devices (smartphones, smart watch...) and the ease to access the Internet. A study show that 95% of teens in the US are online and three-fourths of those (74%) access the Internet on their mobile devices [28]. This means cyberbullying can happen 24/7 and can cross all geographical boundaries [28]. Cyberbullying messages, images, videos can be posted and distributed quickly and anonymously to limitless range of audience. Moreover, deleting those materials once posted is extremely difficult [29] thanks to Google, Facebook and all kind of social networks. In 2016, A study on a nationally-representative sample of 5700 students between the age of 12 and 17 shows that 33.8% have been cyberbullied (Figure 6) [39].

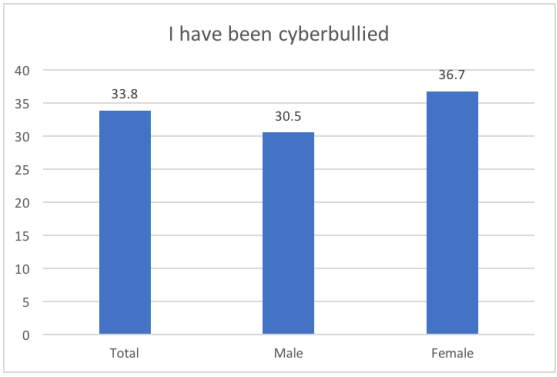


Fig. 6. 2016 Cyberbullying data [36]

3) Detection and Prevention: There are many unusual behaviors that parents or school administrators could notice to further discover about their child or student as a victim or an offender.

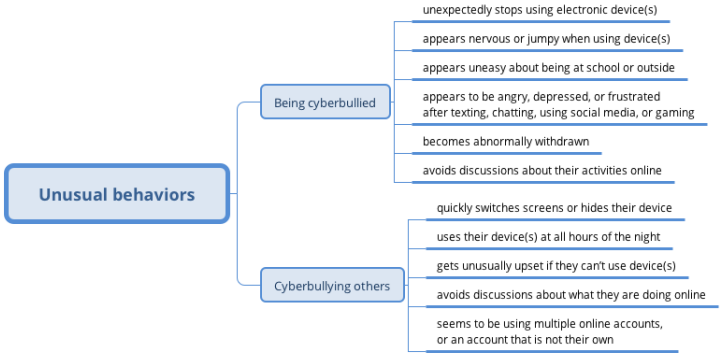


Fig. 7. Unusual behaviors [28]

Although some states have law regarding cyberbullying matter, but often leave response and enforcement in the hand of school officials. Some prevention strategies that schools can take are:

- Educating school community about responsible Internet use

- Discussing issues related to appropriate online communications in various areas of the general curriculum.
- Anti-cyberbullying signs and posters can be displayed throughout the school.

In general, schools need to create an environment that shows disapproval of cyberbullying and bullying behaviors and those behaviors will lead to informal or formal sanction.

Schools could do their part in preventing and responding to cyberbullying through policies, curricula, training and assemblies. But they cannot control and dont know how to intervene in online behaviors that occur outside school. This lead to the role of parents in preventing cyberbullying:

- Educating their children about appropriate behaviors online as well as offline.
- Parent will need to maintain honest and open line of communication so that they will come to parents whenever they experience something unpleasant or distressful.
- Parents should be aware of what their kids doing online through:
  - Talking with kids about their activities online and sites they visit.
  - Asking for their passwords to prepare for emergency cases.
  - Getting involve with their activities and friends on social media sites to have a sense of what they do online and texting.
  - Installing monitoring software and tools in case of significant concern.

After all, in case their child is cyberbullied, parents need to provide unconditional support and make sure that their children feel safe and secure [28].

IV. Standard Mitigation Strategies

A. Computer Safety Tips

According to advices from security software company such as Norton [40], the FBI [41], and the National Crime Prevention Council [42], there are some important steps to protect yourself from cybercrime:

1) Keep your system up to date (Including the operating system, antivirus software and antispyware software): This tip will ensure that your computer have the most protection from security holes in the operating system and can detect malicious programs and remove them.
2) Keep your Firewall turned on: A firewall prevent unauthorized access to your computer.
3) Create strong passwords to protect your information, computer login, smartphones and keep those passwords safe.
4) Lock your computer and smartphones when not in use.
5) Protect your personal information: including Social security numbers, bank account numbers, email address, home address, full name, date of birth, and other personal information that can hurt or embarass you or others.
6) Be careful when visiting websites or checking, responding to email messages: There could be fraudulent websites, email used to steal information such as email account, bank account and other personal information. You should always check for the address of emails and websites to make sure that you are at the right place.
7) Do business with reputable vendors: It is easier to verify and validate when you interact with a reputable, established vendor.
8) Turn off your computer: this method will effectively close the Internet connection and disable the posibililty of being attacked or being used as medium of a botnet.

B. Internet Governance

Internet Governance has been an going debate since the late 1990s when the internet started to grow exponentially. It has now become one of the highest priorities as the threats to National Security from cyber crimes have climaxed. In an attempt to address cyber security, the United Nations created the Security Council to implement an international policy for cyber-security to combat the threats from cyber-warfare, cyber-terrorism, and other cyber-acts [43]. So far the Security Council has failed to establish a resolution to cyber-acts because the member states can't seem to agree upon the constrains. States such as Russia and China believe in content control whereas the US and it's Western partners believe in freedom of speech.

For example, Russia and China define cyber-activity as information security because they are more concerned with the information being breached where as the US and its Western partners define cyber-activity as cyber security because they are more concerned with how the attack is being committed [43]. If the Security Council cannot agree on terminology then they are never going to agree on constrains. The only way they are going to be able to come to an agreement is if the Security Council focuses on what each state has in common. This way they can attack the common areas first and then work out the rest, but since they can't agree it has left each state to take their own approach to solving the problem.

In the US, shortly after President Obama took office he issued three executive orders that expanded the public-private information sharing and established a voluntary Cyber Security Framework which would provide private-sector companies with best practices on better securing the critical national infrastructure [44]. The problem with this approach is the policing. Since the framework is voluntary it is hard to encourage companies to use it. The US is afraid to enforce or mandate infrastructure changes because they want to still maintain the internet civil liberties such as freedom of speech. Other states have followed suite and created similar state-centric approaches,but to date none have been successful. As a result, the question of how cyberspace and Internet governance should be conceptualized in order to provide a better framework for managing cyber attacks and developing cyber standards or norms still stands [44].

V. Taxonomy Model of Cyber Crimes

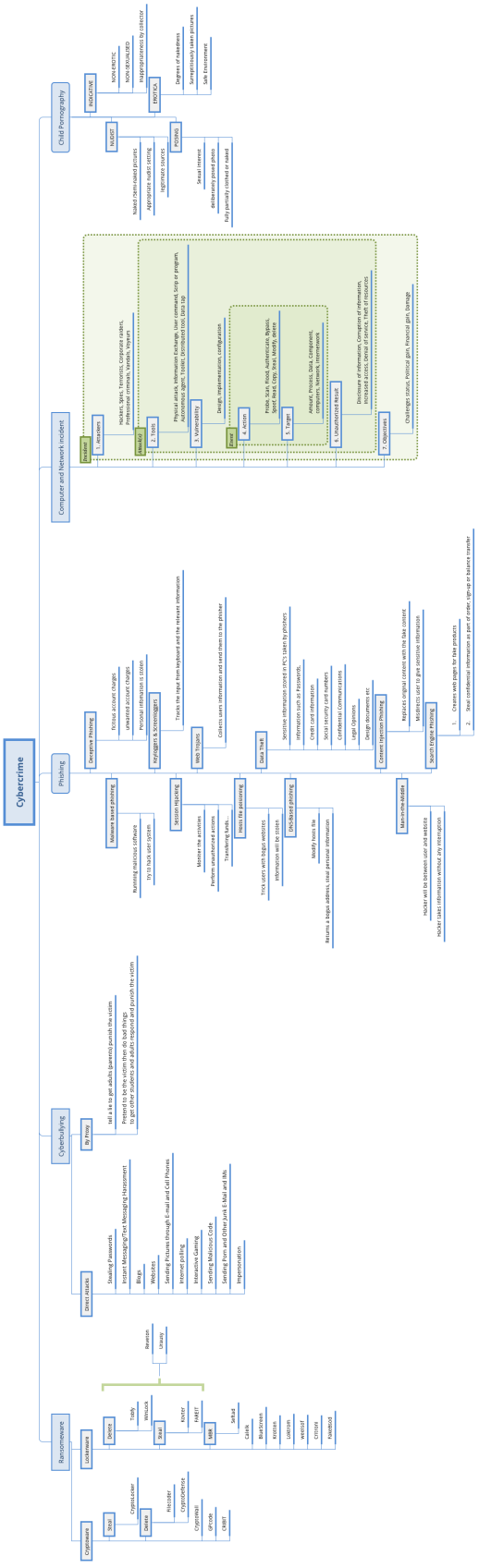


Fig. 8. Cyber Crime Families Taxonomy

The ransomware taxonomy is broken down into the two main types of ransomware; Crypto Ransomware and Locker Ransomware. Typically ransomware tries to encrypt, lock, delete, or steal information at some point during an attack. Underneath each main type of ransomware are sub-blocks that break the ransomware into categories based on the function of the ransomware. Some types of ransomware can both delete and steal information whereas some just encrypt or lock the user's system. Another rare type of ransomware can change the Master Boot Record(MBR) on the user's system which causes the system to not load during boot. The Figure 8 above mentions a couple of these ransomware types.

There are two types of cyberbullying; Direct attacks and by using proxy. Direct attack mean that the action is sent, showed, performed by the offender and directly toward the victim. Cyberbullying by proxy means using others (often adults) to help cyberbullying the victim (even without the accomplices knowledge) [45].

The computer and Network Intrusion Taxonomy shows the types of attacks than can be made along with the events occurring. It explains how attackers use various tools to create vulnerabilities on the targets with an objective of political or financial gain. This taxonomy can be used to educate people on cyber attacks so that cyber crimes can be prevented to some extent. More branches could be added to this current taxonomy considering the growth of technology and cyber crimes.

Phishing taxonomy explains clearly about the different types of phishing attacks. Each attack has different way of approach. One type of attack is to take control of victims computer whereas other type of attack is to manipulate the users to believe the bogus website as original website by that steal their information. Main motto of phishers is to trick the users and steal their personal information.

The Child Pornography taxonomy defines the different types of Child Pornography. It defines that how the attackers can misuse the child pornography by Indicative, Nudist, Erotica, and posing such kind of inappropriate context within the material related to adult sexual interest in children. This Categorizing system quite deliberately includes pictures that do not fall within any legal definition of child pornography.

VI. Conclusion

This paper provides a Taxonomy of major Cybrecrime attacks that has affected general people, Businesses, Government organizations and other industrial sectors. The Taxonomy chart classifies the cybercrimes based on the type of attack vectors, operational impact, informational impact, defense and targets. This classification scheme will aid a defender in protecting their network by providing vital attack information. It is presented in a tree-like structure to neatly classify common vulnerabilities used to launch cyber attacks.

We are aware of the possibility of new attack manifestation, therefore this taxonomy could be extended to include new categories within each classification. It will provide a defender with the appropriate information to make an educated decision in defending against cyber attacks. Creative approaches to

defending attacks will become available and providing an extensible taxonomy able to capture new defenses is imperative to defense. We believe this taxonomy provides a foundation for the cyber security community and provide the ability to continuously grow as attacks and defenses become more sophisticated. In future work, to build a better Defense System, more research can be done to see the applicability of this taxonomy in determining the action space of the attackers.

REFERENCES

[1] "Background and evolution," *Background and Evolution*. [Online]. Available: https://www.justice.gov/criminal-ceos/child-pornography

[2] "Background and evolution," *THE HISTORY OF THE CHILD PORNOGRAPHY GUIDELINES*. [Online]. Available: http://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-projects-and-surveys/sex-offenses/20091030_History_Child_Pornography_Guidelines.pdf

[3] "Background and evolution," *CHILD PORNOGRAPHY ON THE INTERNET*. [Online]. Available: https://www.unicef.org/magic/media/documents/beyond_all_tolerance.pdf

[4] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," *Detection of Intrusions and Malware, and Vulnerability Assessment Lecture Notes in Computer Science*, vol. 9148, p. 324, Jun 2015. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-20550-2_1

[5] G. O'Gorman and G. McDonald, "Ransomware: A growing menace," Nov 2012. [Online]. Available: https://www.symantec.com/connect/blogs/ransomware-growing-menace

[6] P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: Ransomware growing challenge," *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 5, no. 2, p. 371373, Feb 2016. [Online]. Available: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-2-371-373.pdf

[7] D. Foley, "Dc's surveillance system hit with hack attack before inauguration," Jan 2017. [Online]. Available: http://wtop.com/dc/2017/01/dcs-surveillance-system-hit-hack-attack-inauguration/

[8] D. Kean, "Ransomware attack paralyses st louis libraries as hackers demand bitcoins," Jan 2017. [Online]. Available: https://www.theguardian.com/books/2017/jan/23/ransomware-attack-paralyses-st-louis-libraries-as-hackers-demand-bitcoins

[9] "Eight years worth of police evidence wiped out in ransomware attack," Feb 2017. [Online]. Available: https://nakedsecurity.sophos.com/2017/02/01/eight-years-worth-of-police-evidence-wiped-out-in-ransomware-attack/

[10] A. Kharraz, W. Robertson, S. Arshad, E. Kirda, and C. Mulliner, "Unveil: A large-scale, automated approach to detecting ransomware," in *Proceedings of the 25th USENIX Security Symposium*. usenix, 2016. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz

[11] A. Tamersoy, K. Roundy, and D. H. Chau, "Guilt by association: Large scale malware detection by mining file-relation graphs," in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '14. New York, NY, USA: ACM, 2014, pp. 1524–1533. [Online]. Available: http://doi.acm.org/10.1145/2623330.2623342

[12] S. yau and X. Zhang, "Computer network intrusion detection, assessment and prevention based on security dependency relation," *Computer Network Intrusion Detection, Assessment And Prevention Based on Security Dependency Relation*, 1996. [Online]. Available: http://dl.acm.org/citation.cfm?id=674424&CFID=899833560&CFTOKEN=92150754

[13] A. K. Jones and R. S. Sielken, "Computer system intrusion detection: A survey 1," *Computer System Intrusion Detection: A Survey 1*, 1992. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.7802&rep=rep1&type=pdf

[14] G. Vigna and R. A. Kemmmerer, "Netstat: A network-based intrusion detection approach," *NetSTAT: A Network-based Intrusion Detection Approach*. [Online]. Available: https://www.acsac.org/1998/presentations/wed-a-1030-vigna.pdf

[15] A. E. Awad and i. Traore, "Detecting computer intrusions using behavioral biometrics," *Detecting Computer Intrusions Using Behavioral Biometrics*. [Online]. Available: http://s3.amazonaws.com/academia.edu.documents/46178348/PST05_Paper_final_2.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1486926247&Signature=88ANozOIdiD6BWUYQznC%2BfvA%2Br0%3D&response-content-disposition=inline%3B%20filename%3DDetecting_computer_intrusions_using_beha.pdf

[16] "Phishing: An analysis of a growing problem," *SANS Institute InfoSec Reading Room*, Jan 2007. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417

[17] "Report on phishing," *www.justice.gov*, p. 47, Oct 2006.

[18] B. A. Smith, "Phishing attack releases data of 2,500 at college of southern idaho," *http://idahobusinessreview.com*, Feb 2017. [Online]. Available: http://idahobusinessreview.com/2017/02/10/phishing-attack-releases-data-of-2500-at-college-of-southern-idaho/

[19] "Return to sender: Smishing attack delivers fake czech postal service texts," *www.scmagazine.com*, Feb 2017. [Online]. Available: https://www.scmagazine.com/return-to-sender-smishing-attack-delivers-fake-czech-postal-service-texts/article/637115/

[20] M. Chawla and S. S. Chouhan, "A survey of phishing attack techniques," *International Journal of Computer Applications (0975 8887)*, vol. 93, no. 3, May 2014.

[21] S. V, "A review on phishing attacks and various anti phishing techniques," *International Journal of Computer Applications (0975 8887)*, vol. 139, no. 1, Apr 2016.

[22] J. Chhikara, R. Dahiya, N. Garg, and M. Rani, "Phishing and anti-phishing techniques: Case study," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, May 2013.

[23] "Introduction: Refining child pornography law: Crime, language, and social consequences," *Introduction: Refining Child Pornography Law: Crime, Language, and Social Consequences*, Jun 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2802651

[24] "What legally makes it child pornography?" *What Legally Makes It Child Pornography?* [Online]. Available: https://www.hg.org/article.asp?id=38082

[25] H. Babchishin KM, Hanson RK, "Child pornography," *Child Pornography*, Jun 2011. [Online]. Available: http://research.universalessays.com/criminal-justice-research-paper/child-abuse-research-paper/child-pornography-research-paper/

[26] R. Wortley and S. Smallbone, "Child pornography on the internet," vol. 41. [Online]. Available: http://www.popcenter.org/

[27] "Findlaw," *Child Pornography*. [Online]. Available: http://files.findlaw.com/pdf/criminal/criminal.findlaw.com_criminal-charges_child-pornography.pdf

[28] J. Patchin and S. Hinduja, "Cyberbullying: Identification, prevention, and response," 2014. [Online]. Available: www.cyberbullying.us

[29] "What is cyberbullying," U.S. Department of Health and Human Services. [Online]. Available: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

[30] H. M. B. Gina S. Smith, Maria A. Minor, "Cyberbullying in higher education: Implications and solutions," 2014.

[31] "Bullying definition," U.S. Department of Health and Human Services. [Online]. Available: https://www.stopbullying.gov/what-is-bullying/definition/index.html

[32] "What is cyberbullying, exactly?" [Online]. Available: http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html

[33] "Young adults and college students," U.S. Department of Health and Human Services. [Online]. Available: https://www.stopbullying.gov/what-is-bullying/related-topics/young-adults/index.html

[34] J. R. Charles E. Notar, Sharon Padgett, "Cyberbullying: Resources for intervention and prevention," 2013. [Online]. Available: http://www.hrpub.org

[35] J. Patchin and S. Hinduja, "Cyberbullying and self-esteem," 2010.

[36] ——, "Offline consequences of online victimization: School violence and delinquency," 2007.

[37] C. Stoel, "Cyber bullying and the classroom," 2011. [Online]. Available: http://scholarworks.gvsu.edu/colleagues/vol6/iss2/5

[38] J. Patchin and S. Hinduja, "Bullying, cyberbullying, and suicide," 2010.

[39] "2016 cyberbullying data," Cyberbullying Research Center. [Online]. Available: http://cyberbullying.org/2016-cyberbullying-data

[40] “Cybercrime prevention tips.” [Online]. Available: https://us.norton.com/cybercrime-prevention
[41] “How to protect your computer.” [Online]. Available: https://www.fbi.gov/investigate/cyber
[42] “7 tips to protect yourself from cybercrime.” [Online]. Available: http://ncpc.typepad.com/prevention_works_blog/2014/10/7-tips-to-protect-yourself-from-cybercrime.html
[43] C. Anderson, “Cyber security and the need for international governance,” Apr 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769579
[44] S. J. Shackelford and A. N. Craig, “Beyond the new ’digital divide’: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity,” *Stanford Journal of International Law*, vol. 50, no. 119, 2014. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446666
[45] “What is cyberbullying, exactly?” [Online]. Available: http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html