A Study on Cyber Crime Threat Intelligence

1st Ambati Bhargav
dept of Electronics and Communication
KGRCET
Hyderabad, INDIA
bhargavambati@kgr.ac.in

***Abstract*—In the circle of data innovation, digital protection assumes a basic part. In this day and age, safeguarding data has become quite possibly the most troublesome errand. When we consider network safety, the primary thing that strikes a chord is "cyber crimes," which are on the ascent at a disturbing rate. Different legislatures and organizations are finding an assortment of ways to battle cyber crimes. Regardless of many advances, network safety stays a significant issue for some individuals. This paper centers around the issues that digital protection faces in the cutting edge period. It additionally conceals the most to-date data on network protection strategies, morals, and patterns that are changing the essence of network safety.**

***Index Terms*—Cyber crime, Cyber security, Network security**

I. Introduction

The present man can send and get any sort of information, whether it's an email, a sound or video recording, with the press of a button, yet has he at any point thought about how safely his information is being sent or shipped off to the other individual with no data being spilled? Cyber security is the arrangement. In this day and age, the Internet is the fastest developing framework. Numerous new innovations are changing the substance of mankind in the present mechanical climate. Be that as it may, due to these new innovations, we can't safeguard our own data as effectively as we would like, and accordingly, cybercrime is on the ascent. Since in excess of 60 percent of general business exchanges are presently conducted on the web, this region requires an elevated degree of safety to guarantee straightforward and productive exchanges. Thus, digital protection has turned into a hotly debated issue. The extent of network protection reaches beyond tying down data in the IT business to incorporate an assortment of different areas, for example, the internet and cyber space.

Cloud computing, portable figuring, E-business, web based banking, and other state of the art innovations all require an elevated degree of safety. Since these advancements contain touchy data about an individual, their security has turned into a need. Improving network protection and defending significant data foundations are basic to the security and monetary prosperity of any country. Making the Internet more secure (and safeguarding Internet clients) has turned into a vital part of both new assistance advancement and unofficial law.

The battle against cybercrime requires a more exhaustive and secure procedure. Considering that specialized measures alone can't forestall any wrongdoing, police really should be given the apparatus they need to research and indict cybercrime appropriately. Numerous nations and state-run administrations are currently sanctioning solid digital protection regulations to stay away from the deficiency of touchy information. Each individual should be taught network safety skills to shield themselves from the increasing number of cyber crimes.

II. CYBER SECURITY

The protection and security of information will generally be top security needs for any firm. We currently face a daily reality such that all data is put away in computerized or digital structure. Clients can draw in with loved ones in a protected climate on long range informal communication destinations. Digital hoodlums would keep on focusing on informal communication locales to acquire individual information from home clients. While utilizing virtual entertainment, yet in addition while utilizing a bank, an individual should accept all essential security insurances.

- **Network Security**
  The execution of both equipment and programming procedures to get the organization and foundation from undesirable access, disturbances, and abuse is known as organization security. Successful organization security supports the assurance of an association's resources from an assortment of outside and interior dangers.
- **Cloud Security**
  Cloud security alludes to the production of secure cloud designs and applications for organizations that utilization AWS, Google, Azure, Rackspace, and other cloud specialist co-ops. Assurance against different perils is guaranteed by compelling plan and environmental setting.

CYBER CRIMES			
Types of Attacks	2018	2020	Percentage
Fraud	2439	2490	42
Spam	291	614	11
Malicious Code	353	442	25
Cyber Harassment	173	233	35
Denial of Services	122	101	12
vulnerability Report	44	111	76
Total	3581	5592	88

All above examination of Cyber Incidents enlisted to Cyber999 in India among January and June 2018 and 2020 shows the network protection risks. Safety efforts are growing couple with the ascent in wrongdoing.

III. CYBER CRIME

Cyber crime is characterized as a crime carried out utilizing a PC and an organization. It's conceivable that the PC was utilized to carry out a crime or that it was the expected objective. Whenever private data is caught or revealed, whether legally or lawfully, there are various protection concerns.

Cybercrime is carried out by both legislative and non-administrative elements on a worldwide scale, including secret activities, monetary robbery, and other cross-line crimes. Cyberwarfare is a term used to describe cybercrime that crosses worldwide lines and includes the activities of something like a country state.

A. Cyber Terrorism

Since mid 2001, government authorities and data innovation security specialists have noticed an impressive flood in Internet troubles and server tricks. Government offices like the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) are turning out to be progressively worried that such interruptions are important for a planned exertion by digital fear based oppressor unfamiliar knowledge administrations or different gatherings to plan potential security openings in basic frameworks. A digital psychological oppressor is somebody who utilizes a PC based assault against PCs, organizations, or the data put away on them to scare or propel an administration or an association into propelling their political or social objectives.

B. Cyber Extortion

Cyberextortion is a wrongdoing including an assault or danger of an assault combined with an interest for cash or another reaction as a trade-off for halting or remediating the assault.Cyberextortion assaults are tied in with accessing an association's frameworks and recognizing points of shortcoming or focuses of worth. Cybercriminals request installment through noxious action, for example, ransomware, which is the most widely recognized type of cyberextortion. They likewise utilize disseminated disavowal of-administration (DDoS) assaults and take secret corporate information and take steps to uncover it.

C. Cyber Warfare

A digital assault or series of strikes against a nation is in some cases alluded to as digital fighting. It can cause ruin on government and regular citizen framework, as well as hinder fundamental frameworks, hurting state and even passing. Digital fighting is the work of computerized assaults against an enemy state fully intent on making comparable harm conventional fighting and additionally upsetting basic PC frameworks. Specialists differ on what comprises digital fighting and whether something like this exists.

D. Cyber Crime Analysis

A PC or other actual gadget is characterized as an apparatus used to perpetrate digital crime. It alludes to criminal activity brought out through PC networks disregarding standards and guidelines as well as regulations. Distinguishing robbery, harm, exchange extortion, hacking, and programming protection are altogether instances of digital crime.

A crime includes a PC and an organization. The PC might have been utilized in the commission of a crime, or it could have been the objective. Cybercrime might compromise an individual or a country's security and monetary well-being.

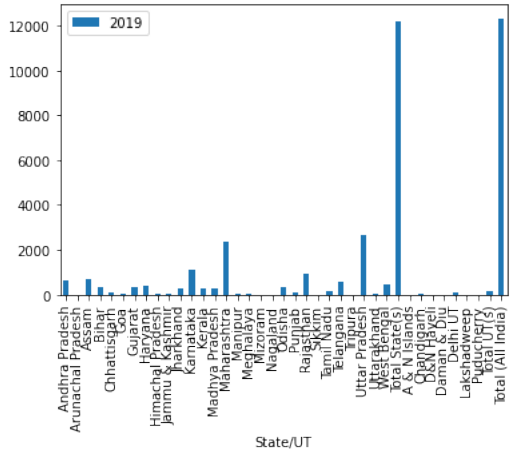

Fig. 1. Cyber Crime in 2019 State wise

Starting at 2019, Delhi had the most elevated crime percentage. Designated messages, or lance phishing, is accounted for by organizations to be utilized in 91% of fruitful information breaks and 95% of all venture organizations.

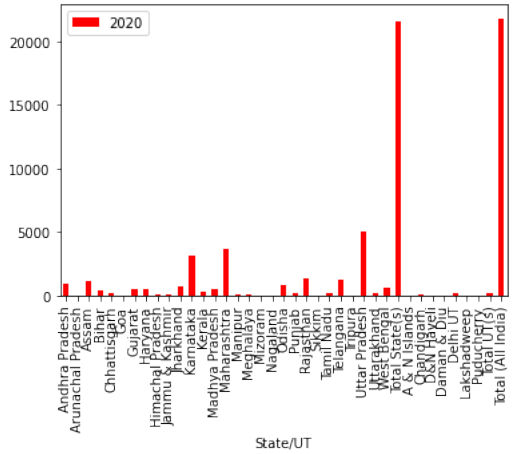

Fig. 2. Cyber Crime in 2020 State wise

Uttar Pradesh is the top region by number of cyber crimes in India. As of 2020, number of cyber crimes in Uttar Pradesh

was 11,097 that accounts for 22.25 percentage of India's number of cyber crimes.

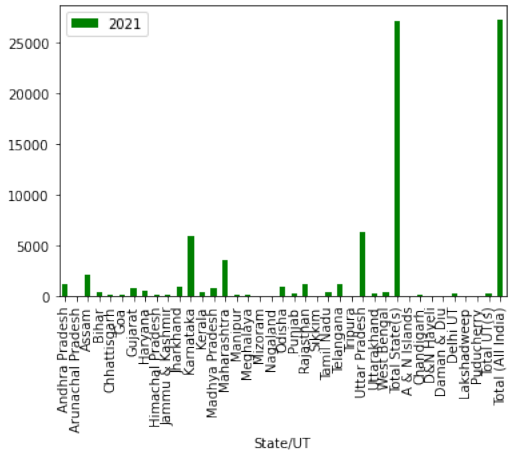

Fig. 3. Cyber Crime in 2021 State wise

Only one of every eight cybercrimes reported in the city in 2021 has been solved. According to police records, 6,423 cybercrime cases were reported last year and only 787 (12%) have been solved. Police said 5,479 or 85% of the cases are still under investigation or undetected as of now.

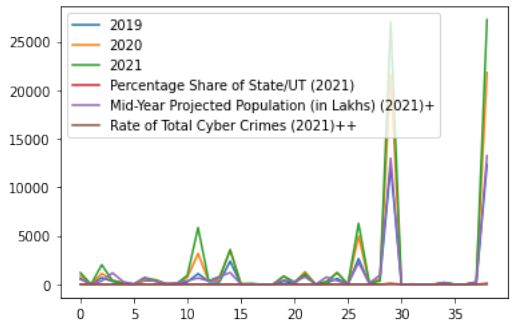

Fig. 4. Overall view of Cyber Crime

Cyberattacks have long been a target for computers such as desktops and laptops. They've also grown into devices that may fit in the palms of our hands or even around our wrists, and the cybersecurity dangers that come with them and their platforms have expanded as well.

IV. TYPES OF CYBER CRIMES

A. Hacking

Hacking is the demonstration of distinguishing and taking advantage of safety defects in a PC framework or organization to acquire admittance to individual or organization information. Utilizing a secret phrase breaking method to get admittance to a PC framework is one illustration of PC hacking.

PCs have turned into an absolute necessity for working an effective business. It isn't to the point of having separate PC frameworks; they should be organized to speak with outside firms. This makes them helpless against hacking and the rest of the world. Framework hacking is characterized as the utilization of PCs to submit false demonstrations, for example, extortion, attack of protection, robbery of corporate/individual information, etc. Consistently, digital wrongdoing costs numerous organizations a large number of dollars. Organizations should protect themselves from such dangers.

B. Methods to prevent Hacking

- **Encrypt Files While Storing and Transferring**
  Continuously encode any urgent Microsoft records that you share with others or store on your gadget, USB, or cloud stage. The expression "encryption" alludes to the method involved with utilizing numerical systems to "lock" information utilizing a cryptographic key. To protect plaintext information from undesirable gatherings without a validation key, encryption scrambles it and renders it ambiguous.

- **Use Browser Extensions to Block Malicious Sites and Harmful Downloads**
  Various free program augmentations monitor destructive and phishing destinations and boycott them. To use them, you'll have to introduce these program augmentations ("additional items" for Firefox) to keep hackers under control and forestall hacking.

- **Install a Strong Anti-Malware Program**
  Even though it should go without saying, some users require a gentle reminder to use antivirus and anti-malware software. This form of protection software scans your device on a regular basis and removes dangerous malware. They will also notify you if you visit a spammy or harmful website or download a damaged file from the internet.

- **Scan PC Manually**
  Some advanced varieties of malware are undetectable by firewalls and security tools. To avoid hacking, it's a good idea to keep an eye on your device manually.
  Check your C: drive on a regular basis, particularly folders like C:/Program Files, C:/Program Files (x86), and all TEMP folders. Keep an eye on the Downloads folder as well. If you come across any weird products that you haven't downloaded yet, conduct some research on the internet to discover more about them. If the files are no longer needed or are linked to malicious behaviour, delete them.

- **Enable Encryption Using BitLocker for Windows**
  Your hard disc will be encrypted with this technology. No one can attack you by stealing data from the hard disc if your Windows PC is stolen or sold without

wiping the memory (note: always erase the memory before selling a device!). It also includes a USB drive encryption feature.

- **Enable Two-Factor Authentication (2FA)**
  Alongside your standard passwords, 2FA gives an additional a level of safety. Each time you sign in to your record or complete an exchange, you'll get a one-time secret phrase (OTP), secret code, or an enchanted connection to your enlisted portable number or email address. Empower 2FA with any of your banks, charge card organizations, or other specialist co-ops quickly!

- **Never Log in Third-Party Platforms**
  Next on our rundown of ways of abstaining from hacking is to try not to connect accounts. At the point when you go to login into another stage, you might be given the choice of utilizing your current records, like Facebook, Gmail, LinkedIn, etc. These settings ought not be utilized. Utilize your email address or telephone number all things being equal, or physically finish up the login structure (don't be lethargic).

- **Never Share Information via HTTP Sites**
  Take a gander at the location bar when you open a site. The site is running on HTTP, which is an uncertain convention, in the event that you see "Not secure" or an interjection image all around or triangle. This implies that any delicate information sent between your program and the site's server isn't gotten, making it simpler for programmers to take your own and monetary information.

- **Recognize Signs of Fake or Malware-Infected Websites**
  Certain individuals buy space names that look like notable area names however contrast marginally in spelling or high level areas. Contingent upon the circumstance, this is alluded to as cybersquatting or typosquatting.

- **Recognize Fake vs. Legitimate Software and Applications**
  Whenever you introduce programming on your gadget, you allow it to transform it and access your information. It's an unsafe activity since you're in a bad way on the off chance that the maker has vindictive expectations or the item contains infections!

- **Recognize Phishing Emails**
  As per FireEye, one out of each 101 messages is malevolent! Malware is spread by email connections or by diverting you to vindictive sites. Some cybercriminals utilize mental stunts to inspire you to share individual data.

V. PEN TESTING

Entrance testing is a reenacted programmer attack on an application determined to decide the seriousness of any current defects. Rather than Vulnerability Assessment, which essentially identifies and records generally existing weaknesses in your site, Penetration Testing centers more around how every one of these imperfections could be taken advantage of exploits.

A. Methodology for Website Penetration Testing

- **Information Gathering:**
  During information gathering, the pentester searches the website's backend for fingerprints. It usually includes information such as the server's operating system and CMS version.
- **Exploitation:**
  The purpose of the final phase of exploitation is to take advantage of any vulnerabilities uncovered in the previous phase. To weed out erroneous positives, this is frequently done manually. Exfiltrating information from the target and maintaining persistence are also part of the exploitation phase.

B. Information Gathering

- **NMAP**
  It is a program that sends bundles and examinations the responses to observe has and benefits on a PC organization. Nmap has various apparatuses for investigating PC organizations, like host disclosure and discovery of administrations and working frameworks.

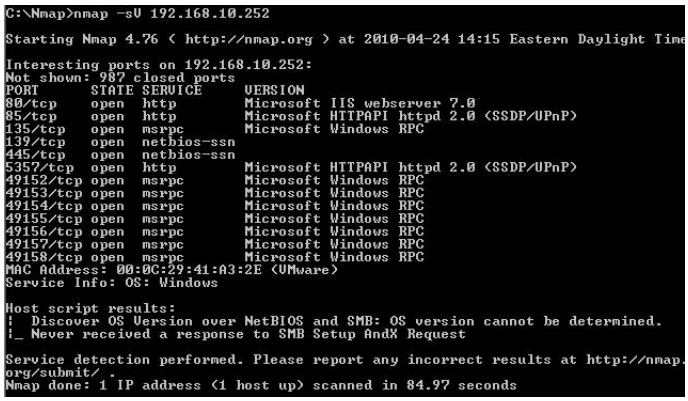

Fig. 5. NMAP

- **The Harvester**
  While some programmes, such as NMAP, capture information in a black box, others, collect Open Source Intelligence. OSINT is data about your target that is available in the public domain, such as Whois registration information, company emails, and so on. This information is useful while performing website penetration testing. It's all over the internet, on sites like Google, Whois, and so on. As a result, the harvester gathers information from many sources and provides you with a one-stop shop.

Fig. 6. Harvester

C. Exploitation

- **Nikto**
  Nikto is an apparatus that sweeps for weaknesses in north of 270 distinct sorts of servers. It can look for 6700 server misconfigurations in depth.However, Nikto's disadvantage is that it is very loud and oftentimes creates misleading up-sides. Moreover, Nikto's firewall avoidance techniques are ghastly. It can, in any case, find success when matched with one more Kali Inundator (to evade IDS).

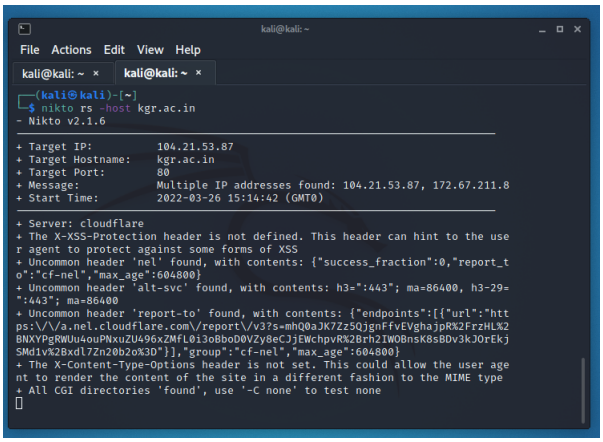

Fig. 7. Nikto

- **Metasploit**
  When it comes to target exploitation, the Metasploit framework is nearly an industry standard. Nmap can also be used by Metasploit to undertake recon. There are a myriad of exploits to select from if you identify any flaws. At long last, match your adventure to a fitting payload and you're all set. Metasploit additionally offers a wide scope of post-double-dealing instruments. Quick 7 possesses Metasploit, which is written in Ruby. Practically all verification of-ideas for notable zero-day weaknesses have been refreshed as Metasploit modules.

Fig. 8. Metasploit

CONCLUSION

PC security is a tremendous subject that is turning out to be more important on the grounds that the world is turning out to be profoundly interconnected, with networks being utilized to complete basic exchanges. Digital crime keeps on separating in various ways with each New Year that passes. So does the security of the data. The most recent and troublesome innovations, alongside the new digital instruments and dangers that become visible each

REFERENCES

[1] IEEE Security and Privacy Magazine –IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[2] Priyanka Datta,"A Technical Review Report on Cyber Crimes in India",International Conference on Emerging Smart Computing and Informatics (ESCI),IEEE,India, 2020
[3] Grace Odette Boussi," A Proposed Framework for Controlling Cyber-Crime", 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),IEEE, India, 2020
[4] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M. "On the effectiveness of machine and deep learning for cyber security", 10th International Conference on Cyber Conflict (CyCon) pp. 371-390. IEEE,2018
[5] Dawson, J. and Thomson, R., "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", Frontiers in Psychology, 9(JUN), pp.1–12, 2018, doi: 10.3389/fpsyg.2018.0074
[6] Hernández, A., Sanchez, V., Sánchez, G., Pérez, H., Olivares, J., Toscano, K., Martinez, V. (2016,March). Security attack prediction based on user sentiment analysis of Twitter data. In 2016 IEEE international conference on industrial technology (ICIT) (pp.610-617). IEEE.
[7] Praveen Paliwal, "Cyber Crime", Nations Congress on the Prevention of Crime and Treatment of Offenders, March 2016
[8] Buczak, A. L., Guven, E ,"A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys Tutorials, 18(2), pp. 1153-1176, 2016
[9] R. Sabillon, J. Cano, V. Cavaller and J. Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", International Journal of Computer Networks and Comm. Security, vol. 4, no. 6, pp. 165-176, 2016
[10] Adnan Amin at. Al. ," Classification of cyber-attacks based on rough set theory", First International Conference on Anti-Cybercrime (ICACC), IEEE, Saudi Arabia 2015
[11] Le Compte, D. Elizondo and T. Watson, "A renewed approach to serious games for cyber security", 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 203-216,2015
[12] [10] F. Pasqualetti, F. Dorfler and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013
[13] Z. Trabelsi, K. Hayawi, A. Braiki and S. Mathew, Network Attacks and Defenses: A Hands-on Approach, Boca Raton, Florida:CRC Press, 2013
[14] Kshetri N. The simple economics of cybercrimes, IEEE Secur Priv, 4, pp. 33–39, 2006