International Journal of Leading Research Publication
IJLRP

© IJLRP | ISSN (O) - 2582-8010
November 2021 | Vol. 2 Issue. 3
www.ijlrp.com

INVESTIGATION OF CYBER CRIMES BY THE INVESTIGATIVE AGENCIES

Ashwani

Research Scholar, Faculty of Law, Tantia University, Sri Ganganagar

ABSTRACT

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both - i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

Cybercriminal activity may be carried out by individuals or small groups with relatively little technical skill. Or, by highly organized global criminal groups that may include skilled developers and others with relevant expertise. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or non-existent cybercrime laws.

Keyword: *cybercrime, computer, network, technical, expertise, malware*

1. HOW CYBERCRIME WORKS

Cybercrime attacks can begin wherever there is digital data, opportunity and motive. Cybercriminals include everyone from the lone user engaged in cyberbullying to state-sponsored actors, like China's intelligence services. Cybercrimes generally do not occur in a vacuum; they are, in many ways, distributed in nature. That is, cybercriminals typically rely on other actors to complete the crime. This is whether it's the creator of malware using the dark webto sell code, the distributor of illegal pharmaceuticals using cryptocurrency brokers to hold virtual money in escrow or state threat actors relying on technology subcontractors to steal intellectual property (IP).

Cybercriminals use various attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest.

Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime. Phishing emails are another important component to many types of cybercrime but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

2. TYPES OF CYBERCRIME

As mentioned above, there are many different types of cybercrime; most cybercrimes are carried out with the expectation of financial gain by the attackers, though the ways cybercriminals aim to get paid can vary. Some specific types of cybercrimes include the following:

- **Cyberextortion**: A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyberextortion is the ransomware attack. Here, the attacker gains access to an organization's systems and encrypts its documents and files -- anything of potential value -- making the data inaccessible until a ransom is paid. Usually, this is in some form of cryptocurrency, such as bitcoin.
- **Crypto jacking**: An attack that uses scripts to mine cryptocurrencies within browsers without the user's consent. Crypto jacking attacks may involve loading cryptocurrency mining software to the victim's system. However, many attacks depend on JavaScript code that does in-browser mining if the user's browser has a tab or window open on the malicious site. No malware needs to be installed as loading the affected page executes the in-browser mining code.
- **Identity theft**: An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal

© IJLRP | ISSN (O) - 2582-8010
November 2021 | Vol. 2 Issue. 3
www.ijlrp.com

that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on darknet markets, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and audio streaming, online auctions and more. Personal health information is another frequent target for identity thieves.

- **Credit card fraud**: An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets, where hacking groups that have stolen mass quantities of credit cards profit by selling to lower-level cybercriminals who profit through credit card fraud against individual accounts.
- **Cyberespionage**: A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages.
- **Software piracy**: An attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringements and patent violations are often associated with this type of cybercrime.
- **Exit scam**: The dark web, not surprisingly, has given rise to the digital version of an old crime known as the exit scam. In today's form, dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts -- essentially, criminals stealing from other criminals.

3. COMMON EXAMPLES OF CYBERCRIME

Some of the more commonly seen cybercrime attacks include distributed DoS (DDoS) attacks, which are often used to shut down systems and networks. This type of attack uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. DDoS attacks are sometimes carried out simply for malicious reasons or as part of a cyberextortion scheme, but they may also be used to distract the victim organization from some other attack or exploit carried out at the same time.

Infecting systems and networks with malware is an example of an attack used to damage the system or harm users. This can be done by damaging the system, software or data stored on the system. Ransomware attacks are similar, but the malware acts by encrypting or shutting down victim systems until a ransom is paid.

Phishing campaigns are used to infiltrate corporate networks. This can be by sending fraudulent emails to users in an organization, enticing them to download attachments or click on links that then spread viruses or malware to their systems and through their systems to their company's networks.

A credentials attack is when a cybercriminal aims to steal or guess user IDs and passwords for the victim's systems or personal accounts. They can be carried out through the use of brute-force attacks by installing keylogger software or by exploiting vulnerabilities in software or hardware that can expose the victim's credentials.

Cybercriminals may also attempt to hijack a website to change or delete content or to access or modify databases without authorization. For example, an attacker may use a Structured Query Language (SQL) injection exploit to insert malicious code into a website, which can then be used to exploit vulnerabilities in the website's database, enabling a hacker to access and tamper with records or gain unauthorized access to sensitive information and data, such as customer passwords, credit card numbers, personally identifiable information (PII), trade secrets and IP.

Other common examples of cybercrime include illegal gambling, the sale of illegal items -- like weapons, drugs or counterfeit goods -- and the solicitation, production, possession or distribution of child pornography.

Emerging trends of cyber-crimes include hacking, identity theft, spamming, phishing and cyber stalking. With these emerging trends in crime, it is high time for the Indian police to revamp and reform investigating methodology for a successful prosecution of such cyber case. The Indian system of policing and criminal investigation is still stuck in the old ways of information gathering and beating out a confession from the suspects. The police force are completely untrained on modern methods of criminal investigation, which requires skills for managing and operating highly sophisticated technologies.

© IJLRP | ISSN (O) - 2582-8010
November 2021 | Vol. 2 Issue. 3
www.ijlrp.com

Several potholes exists within the system due to which a gap continues between reporting of crime, arresting a criminal and finally ensuring successful prosecution of the accused in Cyber Cases. Jurisdiction remains highly debated issue till date as to the maintainability of any suits till date. Today with the growing arms of cyber space the territorial boundaries seems to disappear & the concept of territorial jurisdiction as envisaged under S.16 of Criminal Procedure Code and S.2.of the Indian Penal Code will have to give way to alternative method of dispute resolution.

Police are facing this particular problem as there remains a sense of confusion as to whose jurisdiction the case will fall. Let us take an example; a school teacher finds out that a sum of 30,000 INR was withdrawn from his savings account without his knowledge and permission. The amount withdrawn was from ATM located outside the city limits and some outside the state limits. In these situations, the complainant is faced with a problem of filing the complaint at which jurisdiction. Though S.75 of the Information Technology Act provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

A law regulating the cyber-space has already been enacted by India thought there is lack of any operational manual which describes the methods of conducting an investigation relating to cybercrimes. A SOP (Standard Operating Procedure) has to be set so that the present force can conduct its investigation without any ambiguity.

With the advent of cyber cells at various cosmopolitan cities in India, there is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end. The current staff of cyber cells comprises of a mixture of police officers and IT experts. While additional recruitment is welcome, the effort should be to improve the technical capabilities of the police department as a whole, rather than only the cybercrime cells. Police are quite often handicapped in undertaking effective investigation for want of modern gadgets such as high-capacity data-transfer tools, software's, designed for analysis of phones, tools for recovering passwords using brute force, etc. Forensic science laboratories are scarce at the district level, which can render timely assistance to the investigating Police.

The result is that Police heavily lean towards oral evidence, instead of concentrating on scientific and circumstantial evidence. Though various governments have taken this issue into account in the recent years, a definite example can be taken of Maharashtra government; the Maharashtra government has planned on tackling cyber-crime by deploying 1000 police officers as cyber investigators. The statements/FIRs/reports recorded are not fed to the computer immediately so as to maintain a database because there is no computer network or there is no personnel trained in the job or for want of specific instructions. The benefits of online filing of FIR needs to be implemented to reduce the burden on police.

Network Investigation Tools indicated below are also help investigating agencies to trace digital evidence.

- There is a powerful windows tools available at SysInternals:
- Filemon shows file system activity.
- RegMon shows all Registry data in real time.

Process Explorer shows what files; registry keys and dynamic link libraries (DLLs) are loaded at a specific time. Ps tools are a suite created by SysInternals that includes the following tools.

- PsExec—Run processes remotely.
- PsGetSid—Displays the security identifier of a computer.
- PsKill—Kills processes by name or processes ID.
- PsList—Lists detailed information about processes.
- PsLoggedOn—Displays who's logged on locally
- PsPassword—Allows user to change account pass-words.
- PsService—Enables to view and control services.
- PsShutDown—Shut down and optionally restarts a computer.
- PsSuspend—Allows to suspend processes.
- Tcpdump and Ethereal—Packet sniffers.

4. GUIDELINES TO PREPARE CHARGE SHEET

Inadequate skill in drafting the charge-sheet leads the accused to get away with cybercrime committed by them. Many cases fail before the courts of law just because of

© IJLRP | ISSN (O) - 2582-8010
November 2021 | Vol. 2 Issue. 3
www.ijlrp.com

the defective charge-sheets. Below are few guidelines for investigating officer to include in the charge sheet.

- All the relevant information revealed by the complainants during registering the FIR/course of investigation should be included in the charge sheet along with the search and seizure procedure along with chain of custody and DEC form are also included in the charge sheet.
- It has to be made sure that the necessary information / analysis requested from FSL or forensic examiner are incorporated properly in the charge sheet by including all the technical persons who identified, produced and analysed the digital in the case as witness.
- All the incidents occurred should be in the chronological order of time to establish the crime along with the findings.
- In case of the time stamps like System Time, BIOS Time, Access Time, Log times and Physical Access Time etc; investigating officer has to mention it in a chronological order

5. SUGGESTIVE MEASURES

There is a need to ensure specialized procedures associated with expertise manpower for prosecution of cybercrime cases so as to tackle them on a war footing. It must be ensured that the system provides for stringent punishment of cyber-crime and cyber criminals so that the same acts as a deterrent for others. Presently, most of the offences committed under the Information Technology Act are Bailable with punishment up to 3 years imprisonment. This punishment should be increased to a term which would change the mindset of a cyber-criminal of committing similar and like offences again. Separate bench are required to be constituted for fast tracking of Cyber cases in an effective manner. With the constitution of cyber judges, the law enforcement agencies can prove the merits of their respective cyber cases without any hindrance.

Just like the U.S. Secret Service or the FBI, which provides training to state and local law enforcement officials in cybercrime forensics and related topics, similar programmes can be conducted by CBI, which has its separate cyber cell and a manual for conducting investigation. The methods of the CBI can be used by the Police include close supervision of investigation of the important cases by senior officers and evolving a mechanism so that the investigating officers and Superintendents of Police can get legal advice during the investigation.

Cyber projects like National Cyber Coordination Centre (NCCC) of India, Cyber Attacks Crisis Management Plan of India, Internet Spy System Network And Traffic Analysis System (NETRA) of India, Crime and Criminal Tracking Network and Systems (CCTNS) Project of India, etc. have still not been implemented successfully by Indian government and there is an urgent need to implement these projects in India as soon as possible.

Quick response to the Interpol references and bilateral requests, liberal sharing of forensic technology and more cross-country training exchange programmes besides timely alert can be a major step to curb the cyber menace.

Cyber-crime can only be effectively countered when there is a proper coordination and guidance available from various stakeholders, such as industries, local police as well as the state and central governments. To facilitate such cooperation as well as to give impetus and to govern the effective implementation of various initiatives, we need to have adequately tasked and staffed agencies working at various levels. Indian Computer Emergency Response Team (CERT-In) is the national nodal agency set up to respond to computer security incidents as and when they occur. Some of the activities undertaken by CERT-In toward cybersecurity include coordination of responses to security incidents and timely advice regarding imminent threats, conduct trainings on specialized topics of cybersecurity and development of security guidelines on major technology platforms.

There should be an e-filing system for filing of FIR keeping in mind the digitalization of many government bodies and also to reduce the burden on the victims to approach physically at the police station. Process re-engineering is required to ensure that the current cumbersome procedure of a complainant having to go to a police station to file an FIR is replaced with a single emergency response interface, which can bring the police to the doorstep of the victim in distress. There is a need of a centralized online cybercrime reporting mechanism in India, which provides victims of cybercrime, a convenient and easy reporting mechanism that alerts authorities of suspected criminal or civil violations. Also for law enforcement agencies at the national, state, and local level, there should be a central referral mechanism for complaints involving cybercrime.

In many cases, private corporations have more experience with cybercrime investigations than local police agencies & henceforth, the Police can seek cooperation with private corporations without compromising the security.

© IJLRP | ISSN (O) - 2582-8010
November 2021 | Vol. 2 Issue. 3
www.ijlrp.com

For example in the United States, a privately-led Identity Ecosystem Steering group (IDES) has been established to support the National Strategy for Trusted Identities in Cyberspace (NSTIC) .

A number of police agencies have formed partnerships with computer science departments at local universities. These partnerships not only provide expertise to the police, but also serve as a recruiting tool for students who have an interest in cybercrime and policing. A knowledge hub thus can be established which can also attract students to pursue a career as cyber investigators.

REFRENCE

1. https://www.myadvo.in/blog/cyber-crime-in-india/
2. https://www.ijitee.org/wp-content/uploads/papers/v9i3/K24080981119.pdf
3. https://shodhganga.inflibnet.ac.in/bitstream/10603/286007/12/12_chapter%205.pdf
4. https://www.hg.org/legal-articles/cyber-investigation-how-prepared-are-the-indian-police-37384
5. https://shodhganga.inflibnet.ac.in/handle/10603/7829.