Cyber Crime Varient Activities and Network Forensic Investigation

Giridhar V¹, Prof. Clara Kannmani A², Dr. S. Mohan kumar³
¹Final Year CSE Student, ²Senior Assistant Professor, ³Associate Professor and R&D Co-ordinator, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India

Abstract— The critic’s raise of professionalism advancing technology curves to heights has favored fellow beings but unfortunately gave chance for new hacking methodologies as in course of advancement. the serious and challenging varied threats of cyber crime is sensed and imprinted to motivate as not to be a crucial victim of cybercrime activities, Having made the views about Hazards of it , course of cyber investigations and how they are being tackled. Finally giving an overview about network forensic investigative study, deriving at weighed conclusion in forensic matter.

Keywords—Steganalysis; Paedophiles; Network forensics, Cybercrime activities, password sniffing.

I. INTRODUCTION

Cybercrime cuts across social borders creating a new realm catastrophe making illegal human activities compromising legitimacy of the genuine user. Cyber crime is the major concern for global community. As an impact of modernization, the sensitive statistics of currency and other confidential data marched to computers and databases, though cybercrime is from previous decades, but advancement crimes to flourish competing national and international commerce in masquerading originality.

The rapid growth of internet, not just in terms of incorporating users, but also sophisticating in terms of functionality has allowed entire industries to move their operations, especially money onto internet. The advent of networks set a strategy, merging entire world bringing collaborating user socially. Supporting confidentiality, their by providing feasibility making industries documenting huge database to adapt and fit through communicative transactive internet. But this public networks encouragement has lead prolific growth in criminal activities, availing a virtual view profile. The sole targeting of weighted data computers has necessitated achieving mission of security concentrating vision of tackling attackers. The hackers plan to conquer company’s database acquiring user ids and passwords rupturing the balance of security.

The cybercrime has been part underneath the systematic society from the past. Illumination of globalised social networks unfortunately gave path for cybercrime imprinting hilarious threats in human minds, this flourishment of crime indulged with variant crime taxonomy, which has to be predicted analyzing and finally blocking the variant crime activities.

The sub-branch of forensic which indulge in capturing, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents called Network forensics.

The analysis mechanism in network forensic involves monitoring networks, performing cumulative gathering of data transactions, analyze and inspect internetwork as well as intra network, recognize identity packets and pattern of near future, judge network performance, analyze the traffic through source to destination. To avoid spoofing corresponding activities are concentrated such as replaying of network session, identify different protocols, sessioning and auditing the network, locating the source of any illegal network activities and monitoring network characteristics.

The importance of network forensic and course of investigative life cycle studies indulging several steps of case study. Finally producing the statement of various cyber crimes activities.

II. FORENSICS AND ITS TYPOLOGY

Digital cyber forensics is of two types: Computer forensics, Network forensics

A. Computer forensics

- Computer forensic is a branch of cyber forensics where inspective analysis together with preserving data as evidence, entertaining originality and authenticity.
- Computer forensics is a branch of digital forensic science, where the application of scientific scripts as work to grab the logical/physical evidence.
"application of forensic procedures binding digital evidence" it is a lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is viable, notable and perhaps of evidentiary value as a treasure of fact in managerial, administrative, civil and criminal investigations.

Collection, preservation, and analyzed investigative conclusion on computer related evidence. Attempts to retrieve information even if it has been altered or erased so it can be used in pursuit of detecting criminal.

Computer forensic evidence data recovered must be ensured to be "the data that’s not going to be nightmare for detectives as their by forming pseudo-proof". i.e. data recovered can be inculpatory (favouring prosecution/investigation against suspected criminal) or exculpatory (favouring defendants of case).

Some computer Forensic Capabilities involved for documenting evidence has following steps to be performed.

1. Recover deleted files of investigation
2. Make out what external devices have been attached and what sort of users accessed them
3. Determine what applications ran under these processes
4. Recover web pages and web sites
5. Recover emails and users who read them
6. Recover source and destination of communication
7. Recover chat logs
8. Determine client server and web server using necessary network protocols
9. Determine file servers used
10. Discover document’s hidden history
11. Recover phone records and SMS text messages from mobile devices
12. Recover search web and browser history locations with regards
13. Find malware and data collected forensic capabilities, cross verify them.

B. Network forensics

The branch of digital forensics which deals with analysis of adverse network traffics to avoid intrusions and to avail legal evidence their by reducing cyber crime rate or to abolish hacks.

Relevance of the OSI 7 layer model: Extreme knowledge of protocols, network modules and mechanism involved at each of the seven layers has to be known by network analysts to determine statistics of crime under investigation. The knowledge of OSI layers in forensics lead to effective utilisation of 7 layers with protocols such as TCP, IP etc. to detect bad traffic their by taking action against them.

(XDR) External data representation is a standard data serialisation format usually inferred in computer network protocols. Protocols allow data to be migrated all through computer lane translating data structures or object state into a format that can be stored. This involves conversion of local representation data to XDR called encoding and converting from XDR to the local representation is called decoding. XDR implemented software library function is portable to varied operating systems.

(RPC) Remote procedure call is a protocol where procedure send echo request form a computer at remote site building responsive communications without understanding network details in depth. It makes use of client-server model.

NetBEUI an enhanced version of NetBIOS protocol which is non routable with no intra-network or intra sub-network communication possible

SMB packet way transaction implements sub protocol, where client takes data encapsulates it with smb-transaction forwarding it, as wrapped data arrives at server smb_transaction is taken off, then the raw unprocessed data is passed to function, as the function returns processing raw data its once again encapsulated further forwarding to client for usage.

Ping: (packet internet groper) describe the active users of transactions and to determine whether the destination is alive or not. Often used to test the reachability of a host on an Internet Protocol network and to measure the round-trip time for messages.
NFS (network file system): is a distributive file system protocol allows files to be accessed using the same interfaces and semantics as local files or allows user on a client computer to access files over a computer network. It builds on the open network computing remote procedure call (ONC RPC) system. The NFS is an open standard defined in request for comments (RFC), allowing anyone to implement the protocol.

ICMP (internet control message protocol) is a main protocol of the internet protocol suite. It is used to relay query messages and in informing the error message regards. port no is 7

The UDP (user datagram protocol) uses a simple connectionless transmission model with a minimum of protocol mechanism. its highly profitable. Comparatively slower than other protocol as communicative mechanism involves packet transfer form source to destination in unordered manner with no path. It is a very simple protocol that provides only two additional services beyond IP de-multiplexing and error checking on data. Recall that IP knows how to deliver packets to a host, but does not know how to deliver them to the specific application in the host. its unreliable

MIME (multi-purpose internet mail extensions): is an internet standard that extends the format of email to support text in character set, non textual attachments such as audio, video, images, application programs. This non-textual information is known as hyper media.

SMTP: is an internet standard for electronic mail transmission. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.

TCP: The Transmission Control Protocol (TCP) provides a logical full-duplex (two-way) connection between two application layer processes across a datagram network. Its connection oriented with packet flow following ordered pattern. It’s reliable.

HTTP: hyper text transfer protocol: transactive interaction among web servers and web browsers considering the way of message transmission and formulation.

HTML: hyper text markup language the commanding language to embed structure in an interactive form. A structured hypertext elemental document.

III. COMPUTER CRIME AND INVESTIGATION

Prepare for the forensic examination i.e., typical examinations must guide with ever changing diversified forensic science investigations for fast shaping crimes.

Analyse via communicating to people by making them understand your necessary claims and get suggestions surrounding the case from folks. If you are convicted that the case of in-charge is found to be with sound basement then start assembling your tools to answer the data of questions and to identify the target media.

Examine the target media for safety, collect the data form target media, where the source of info required establishing evidence against crime dwells. In this process, you will be creating an exact duplicate image of the device in question. To do this you need to use an imaging software application. To extract the contents of computer regarding questions, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using.

It is imperative that you follow the directions precisely because this is where the "chain of custody" starts. Make sure that you use a write-blocking tool when imaging the media under investigation. This makes sure that nothing is added to the device when you are creating your image.

When collecting the evidence be sure to check e-mail, SMS, other messengers. so that tenure of work availed in investigation yield a great deal of information.

Examine the collected evidence on the image you have created, documents you find or have been found. Ensuring tools available to help look into open files, encrypted files, and mapped drives and to even analyse network communications, you can look into commercial products and open source products. Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a windows OS, check the registry. Be sure to look into Internet searches pictures that are stored on the target computer.
Many times, criminals will hide incriminating information in pictures and E-mails through a process called "steganography". it is an art of information hiding. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the internet. The hidden message can reside unsuspectingly on a website.

"Steganalysis" is a preventive to the adverse cons of steganography where there by gaining ratings in market of Cyber security. Hiding messages in image data, used by Criminals and even by Non Criminals to send information over internet is quite common. The course of analysis also involve the erased data recovery via essential tools in adaptive to case environment. Finally, report your investigative evidenc MATERIAL back to your respective client which is to be submitted under court of law with a clear, concise testimony.

Organisation’s internal incident response team may have attempted to identify, give caution, resolve the security threats, to predict for recurrent attacks. In such situation network forensics examiner should record the explanations during the initial meeting about how the incident response team became aware of damage at infrastructure and queries, actions, remedies the team took. This gives examiner, the estimate and modifications at security department required for organisations. Possible modifications necessary for that organisation can be derived by answering the questions of security investigations.

Those are, who committed the crime? What did the attacker do while on a computer system or in the network environment? When did the attack occur? Where did the attack occur? Why did the attacker attack? How did the attacker compromise the system or environment? Network forensics examiner determines the possible categorization of the security violation. The following security incident categories, Denial of service, malicious code, unauthorised access, In appropriate usage, Multiple components.

The motto of second stage preliminary analysis is to allow the network forensics examiner to conduct a quick high-level assessment of the security incident to determine a possible outcome among the three - a security incident has occurred, a security incident did not occur, it is not possible to determine if a security incident has or has not occurred. Based on these what next analysed step should be taken care of should be uncovered. at this time, the network forensic examiner identify the various computer, network, and security devices and interfaces that conclude for investigations and that might contain relevant evidence, the device configuration settings, predefined security settings used to enforce security policies, log files of devices, computer- or device-generated paper printout reports etc. are those fields which must be focused on. Devices may contain log information types. The types of Logging Information are Complete Traffic, Session Traffic Alert-Only Traffic, and Statistical Traffic. The log file types are available with configuration and device settings and are depicted with extensions. The complete traffic represents binary capture of ingress and egress network traffic. The session traffic is a part of complete traffic which is used in binary capture of connection oriented only TCP session based network traffic their by reducing the amount of traffic. This impacts end to end connection between source and destination.
Alert-only traffic gives perception about logs generated by network or security monitoring devices as a result of a matched security policy or security violation. Typically, deployed security monitoring agents are implemented across various network groups and the alerts are transferred to a management console for frequent monitoring. Statistical traffic signifies the catalogue or metadata collected while operating with network interfaces.

The third stage being evidence collection to resolve incidents that needs to be tackled with legal proceedings. It’s extremely important to have sound evidence, physical or electronic evidence obtained, called collection procedures which meet legal applicable laws and regulations are to be admitted in court. These computer records are considered as hearsay evidence, such obstacles must be looked out by examiner. The person submitting records at court must prove that the records of the case are authentic and trustworthy. Proper addressing and labelling of all evidence, electronic evidences initially seized must be cryptographically hashed. This process predicts, prevents any possible intentional or accidental modification. Since digital data is volatile examiner should obtain initial network traffic snapshots.

The fourth stage is detailed analysis which is typically performed at forensic laboratories. Examiner at work must commence with conduct that the examiner has legal right to perform a detailed investigation performed by building network analysis framework considering the current adverse impact of traffic. we import STEP mechanism involving segmentation of captured traffic ,tracking packet segments ,end to end review of traffic between organisation of interest to extracts binary-captured traffic, point analysis performed to analyse device based on specific ports.

The fifth stage is preliminary and final reporting where documentation or citation of investigative managed data, submission of those reports and evidences is performed at the court. This stage is of utmost importance as it involves recording every actions and measures taken, starting from pavement of investigation i.e., from security alerts which are time stamped. Documenting with date even for small recurrent changes. The labelling and tagging of document to tighten investigations. To list comments, remedies, omissions as and when required.

The sixth stage being Team Review and Presentation is intended to provide formal review about equipments at investigation and to carve a path of “plan and prepare organisation”.

The seventh stage is depositions which involve the collection of sworn testimony of both sides at judiciary when judge is absent. It is two types – discovery and testimony.

The eighth stage is named to be testimony which consists of two key roles that has to be performed by examiner as he being technical witness showing only the facts as basis for enquiry or as a expert witness, he can conclude and can be opinionative based on experience and deductive, genuine reasoning extracted from the facts which were found during an investigation. Though attested via witnessed client’s counsellor the records are clearly checked again by opposite counsellor. This process of cross checks in between the counsellor of same case leading to qualifying expert witnesses called voir-dire. The case of proxy investigations though being civil or criminal should go under trial process involving- Motion in limine , Empanelling the jury , Opening statements , Plaintiff , Defendant , Rebuttal , Closing arguments , Jury instructions thus giving correct judgement path for all cases.

The ninth stage of forensic examination being containment and recovery, which is to minimise the threats on security indications to full forth performance of organisations during emergency. It is essential to have alerts before the ill-effect of catastrophe makes way to other department’s consistent effort.[12]

V. CYBERCRIME AND ITS VARIANT ACTIVITIES

Cyber crime is defined as “an act or commission of an act that is forbidden for the omission of duty that is commanded by a public law and that makes the offender liable to punishment by the law”

A. Cybercrime against individual

Electronic mail spoofing and online fraud: Spoofed email appears to originate from one source but actually it originates from another source retracing the victims essential details for fraudulent activities.
Phishing: the fraudulent blaming by making an innocent viable for responding to fake emails revealing personal details as being a victim of dubious company which has created the view of reputable companies. An mistrusted entity acts as a trusted entity in electronic communication indulging in fraudulent access of sensitive data exerting adverse effects on social networks.

Spamming: People who create electronic spam are called spammers. It is the abuse of electronic message system.

Cyber defamation: "whoever, by words intended to be read or by hyper media signs or visual representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputations will harm, the reputation of such persons, is said, except in the cases hereinafter expected, to defame the person."

It is a cognizable offense. Libel is written/document defamation and slander is oral defamation.

Software piracy: It is a theft of software through illegal copying of genuine programs or counterfeiting and distribution of products, intended to pass for the original.

Cyber stalking and Harassment: is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.

Pornographic offenses: offensive videos and pictures of sexually explicit conduct creating nuisance in growing minds. "Paedophiles" are people who physically or psychologically coerce minors to engage in sexual activities.

Password sniffing: are programs that monitor and record the name and password of networking users as they login, jeopardizing security at the site.

**B. Cybercrime against property**

- Credit card frauds: credit card number stolen in online databases. Bulletin boards and other online services is the target of hackers.
- payment card industry data security standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent card holder data theft and help to combat credit card frauds.
- Intellectual property crimes: piracy and counterfeiting evolves to be IP crimes. Mechanism of promoting, distributing and selling of products with pseudo proof of genuine trademarks bared well famed companies without their approach or permission.
- Internet time theft: The illegal trespassing through authentic user’s internet data availing, absorbing and accessing it without any intimation to original user.

**C. Cybercrime against organization**

- Password sniffing: password sniffer is a software application that scans, records, directs and redirects by broadcasting them to network interface. It glances to make note of any instance of data packets that contain password via continued checking of outgoing and incoming packets thus involving the mechanism of password sniffing. In brief, every message that a computer on a network interface transmits can be read by all computers which are of same network interface but in practice the recipient computers though notice the message ignores it. Hackers made use of this compromised network interface communication to snatch the passwords.

- Unauthorized access to computers: leads to essential data leakage

- DOS attacks: attempts made to add delay on service needed by the clients at required time. An attack category designed to prevent the authorized legitimate use of networks, systems, or applications by disabling the resource or by saturating the resources bandwidth or capacity their by motivating unavailable resources. [2] explains that DOS denies varied services causing absorption or consumption of scarce resource, destruction of configuration info statics, manipulation of network accessible components etc.

- Virus attack or disseminations of viruses: virus attacks are specific with its attacks pertaining to respective variants. Several types of viruses are- file infector, Resident program infector, Boot sector infector, Multi-partite virus, Dropper Stealth virus, Companion virus, Polymorphic virus, Mutation engine virus. These acquire essential data manipulate it and forward that data after modification, they are also responsible for crashing entire computer systems.

- Email bombing or mail bombs: sending a large number of Emails to the victim to crash victims email account or to make victims mail servers crash.
Salami attack: an intruder of bank insert a program into bank server causing financial crime from the account holders of just deducting negligible amount being unnoticed which may later enhance financial crime called Salami technique.

Logic bomb: are event driven programs created to do something only when a certain event/trigger occurs. Some viruses are termed as logical bombs because they lie dormant all through the year and only become active on a particular date (e.g. Chernobyl virus and Y2K viruses)

Trojan horse: a program designed to trespass or breach the security of a computer system to invade worth of valuable memorandums while ostensibly performing some innocuous, in obnoxious, jejune function.

Data diddling: this attack involves altering raw data just before it is processed by the computer and changing it back after the processing is completed.

Computer network intrusion: the feeble security gives path for unauthorised, malicious hackers to take advantage on network interactive sessions having data related to password, credit cards, bank enquiry etc..

Industrial Spying/Industrial Espionage: spies getting information about product finances, research and development and marketing strategies, an activity known as industrial spying.

Software piracy at organisation level

D. Cybercrime against society

 Forgery: creating bogus duplicative evidence using sophisticated computers, printers and scanners. This is becoming a booming business now a day

 Cyber terrorism: Is an estimated scheme with pre talks via intruder, managing to influence politically, to loot computer program, personal data in bulk demonstrating a mass terror threat or attack over entire network.

 Web jacking: it occurs when someone forcefully takes the control of a website. The actual owner of the website does not have any more control over what appears on that website.

E. Cybercrimes emanating from Usenet groups

New groups in internet giving definitive solutions to illegal or harmful content. It is possible to put Usenet to following criminal case:

 distribution of pornographic material

 distribution of pirated software packages

 distribution of hacking software’s

 sales of stolen credit cards

 sale on stolen data/property

VI. RELATED RESEARCH WORK

Mantesh etal., 2013[4]: The personal and business transactions in competitive current world through secured internet communication with https protocol has been necessitated lifestyle practice. The transaction network security if compromised, to avoid hazards of cybercrime network cyber forensic branches open gates of examination. In this paper author has described overflow mechanism of https analyzer, involving working on raw packets collected from proxy system and perform https analysis on those packets. The main goals of this section are to calculate the session key used for the traffic encryption, decrypt the encrypted HTTPS traffic and produce the forensic result of the traffic. The session keys are calculated on the basis of the initial handshake messages that are used for establishing the SSL session between the client and the server. Author conveys network analysis strategy unveiling Work Flow diagram of HTTPS Analyzer containing Pcap File, Filter HTTPS Packets, and Separate each session of HTTPS traffic. Reorder the packets so that they are incorrect sequential order. Separate the hand shake messages. Identify the cipher suite and protocol version used by this session. Extract the client random server random and encrypted premaster secret. Fetch the private key from the pkcs12 file. Decrypt the encrypted pre master secret. Calculate the master secret. Perform the key expansion. Slice the expanded key into key blocks. Decrypt the data. Reconstruct the file and perform file comparison. Gather the forensic information.

Ikuesan R. Adeyemi etal., 2013[7]:In this paper author reviews the current research in network forensic analysis examining Forensic science as a methodological and correct application of broad spectrum of scientific discipline to answer questions significant to legal system; an interception between technology, methodology and application depicting network forensic as the act (scientific process) of, measuring level of intrusion; investigating source of intrusion, deciphering intrusion intent and vulnerability exploited; or information provision to recover from an intrusion as well as the process of discovering planned intent of network traffic for the purpose of strengthening system security, and culpable evidence presentation. Finally author uncovers distinguishing network forensics and network security.
Sumanjit Das et al.,[5]: The computers and network showing glimpse of technology benefits unfortunately made us hurl under the curve of threat from the deadliest type of criminality termed as ‘Cyber crime. The author categorizes cybercrime to Data Crime, Network Crime, Access Crime etc., he also gives brief description about Theft of Telecommunications Services, Communications in furtherance of criminal On piracies ie., Telecommunications Piracy, hypermedia piracy, Illegal Interception of Telecommunications, Electronic Funds Transfer Fraud, Electronic Money Laundering and Tax Evasion, Electronic Vandalism, Terrorism and Extortion etc., Author demonstrates the impact of cyber crime on varied classes of tenants in toil rich diversified society. Finally upholding adverse effects of cybercrime in future trends.

Elias Raftopoulos ETH Zurich et al., 2013 [6]: The network security system under process has complicated approach of investigating security incidents. In this paper author depicts network analysis as an opaque art involving careful exaction and fusion of evidences derived from security sources, the attentive examination on working of malwares and spywares, exploitation of infrastructural related data and Configuration of the affected network. Author emphasises on collection procedure of evident data, Reconnaissance and Vulnerability Reports, IDS Alerts, Spamming, blacklists etc., the variant malwares negative impact on search engines is described.

VII. CONCLUSIONS

Track records depicts that cyber sensational crimes are wading underneath an organized society, through varied cybercrime activities. The paper enlightens by paving path of investigative studies in network forensics and broadening the view of varied cybercrime activities.

REFERENCES


