IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 13, Issue 1, January 2023, ||Series -I|| PP 53-57

Recent Fraud in Cyber Forensics.

Abraar Khan[1], Dhwaniket Kamble[2], Dr.Mohan Awasthy[3], Poulomi Kha[4],Akshada Jagtap[5], Shreyash Navale[6], Abhishek Mane[7], Shubham Sarang[8], Shriti Kashmirkar[9],Diksha Bhalerao[10]

[1] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[2]Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University,Maharashtra, Navi Mumbai-410210, India.
[3] Principal of Bharati Vidyapeeth Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[4] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University, Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[5] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University,Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[6] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University,Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[7] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University,Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[8]Department of Information Technology, Student in Bharti Vidyapeeth Deemed University,Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India.
[9] Department of Information Technology, Student in Bharti Vidyapeeth Deemed University,Department of Engineering and Technology, Maharashtra, Navi Mumbai-410210, India
[10] Department of Computer Science and Engineering, Faculty of Bharti Vidyapeeth Deemed University, Maharashtra, Navi Mumbai-410210, India.

Received 10 January 2023; Accepted 26 January 2023

Abstract: Cyber-attacks are becoming more frequent and severe. When an attack occurs, the attacked enterprise responds with a series of predetermined actions. One of these actions is the use of digital forensics to aid in the recovery and investigation of data from digital media and networks. Cyber Forensic Investigation entails the collection and analysis of digital data to prove or disprove whether an internet-related theft occurred. Previously, computers were only used for storing large amounts of data and performing numerous operations on them, but these days they have expanded and occupied a prior role in crime investigation. The selection and use of forensic tools is critical to solve these cyber-related problems. The developers created it for better research and faster investigation.

Keywords: Cyber Forensic, Malware, SQL Injection, Phishing, Whaling

I. INTRODUCTION

Know-days people's lives and jobs have surely been transformed by the digital era. However, the lustre of digital technology is being eroded by a wave of cybercrime that jeopardises end-user privacy and data. The alarming growth in cybercrime has become a major source of concern for cyber experts. In this bleak environment, digital forensics has emerged as a benefit for cyber professionals, proving to be an efficient method of analysing cyber-attacks [1]. Cyberattack or crimes is the most critical issue that has a considerable influence on the economics of enterprises, particularly those that operate online. Cybercrime, often known as computer crime, is the criminal use of computer equipment and networks to accomplish other goals, such as fraud. The internet is the primary source of all of these activities [1]. Due to this the economy loss affects all sectors, including the government and traditional enterprises. The development of software application tools/computer forensics tools is the most promising technological breakthrough in digital forensics. Data storage platforms range from industrial machine controllers to autonomous devices, personal computers, mobile devices, computer networks, cloud-based systems, and servers. There are numerous types of digital forensics tools available on the market, one of which is to preserve the original file or data after the data is recovered from these devices, so that they can be compared with the original data and ensure that the extracted date is not contaminated or tampered with. There are certain fundamental concepts to keep in mind while utilising digital forensic tools. When data is gathered, it should not be changed. People who use digital forensic tools should keep detailed records of their activities. Furthermore, access to the original document should be controlled to avoid any tampering or modification of the evidence.

Digital forensics is a field of forensic science concerned with the recovery and study of evidence discovered in digital devices, frequently in connection with computer crime. Computer forensics is often referred to as cyber forensics. It entails using computer investigation and analytical tools to solve a crime and give evidence to back up a claim. It is the process of locating, conserving, analysing, and presenting digital evidence in a way that is legally admissible. It is relatively simple to investigate the evidence utilising cyber forensic techniques.

II. METHODOLOGY

FRAUDS REGARDING CYBER FORENSICS

Some of the frauds we're going to study about are:-

2.1.Malware:- Malware are nothing but a program which is specifically designed to harm one's computer or personal devices.[1][2] Malware includes computer viruses, spyware and other malicious program. Let us look at one of the Malware example:-[2]

1.2.Spyware(Key Logger):- Key logger is a type of malware that can be installed onto your computer by connecting an infected external device. The attacker installs the key-logger and as soon as you startup your device all of the keys that you've pressed are recorded and all of the data is shared to the attacker. This is a breach of your sensitive data and attacker can easily obtain all of your accounts login information and credit card details.

1.3Ransomware(Case-Study):-CovidLock, ransomware, 2020

In case to recent events, while the lockdown was set in covid,many people had created applications that would give live information about covid-19. Many of the hackers had taken advantage of this situation and started creating apps which had malware in them. In some of the cases, People who had downloaded this apps were injected with a malware that encrypted whole of their storage. Then these hackers would ask for ransom money to free their private data.

2.Phishing:- The goal or the main motive for the phishing attack is to steal the sensitive data like "credit and login information" or to install malware on the victim's machine (it happens through email). These attacks are the practice of sending fraudulent communications that appear to come from a reputable source. The particular email is send by the trusted sender/user to fool the victim, he or she is coaxed into providing confidential information, often on a scam website [4]. Sometimes the malware is also downloaded onto the targeted computer. Phishing types:-

2.1 Smishing:**-** according to FBI phishing is the most common type of cybercrime in 2020 -241,324cases in 2020 and in 2019 :-114,702 cases when a hacker send a message to trick victims to hand over sensitive information to hackers or to install viruses, Trojans, or ransomware**.**

2.2 Spear phishing**:-**it is personalized and more targeted form of phishing the target is on a specific individual, hackers know about the victim. In this the professionally designed email comes from trustworthy Sources.

2.3 Whaling:-it is more targeted than spear phishing , the target aims.at seniors executives like CEO/CFO. Whaling emails looks like believable when they appear to come from trusted partners.

2.4 Phishing(Case-Study):**-** Hackers stealing Github accounts using fake CircleCl notifications. Github is warning of an ongoing phishing campaign that started on sept 16 and is targetting its users with emails that impersonate the CircleCI continuous integration and delivery platform. The bogus message inform recipients that the user terms and privacy policy have changed and they need to sign into their Github account to accept the modifications and keep using the services. CircleCI using the links like circleci.com or its sub-domains, underlines the notice from CircleCI.

3.SQL-Injection Attack:-SQL is used to query, operate and administer data system such as Micro-soft, SQL server, Oracle and so on. One of the most common attack is the SQL injection attack[6]. A successful SQL injection exploited can read sensitive data from backend database it can also be modified or delete data or execute administration operations. Some time it can even issue comments to the operating systems.

Types of Sql Injection Attack are:-

3.1 Authentication Bypass**:-**Here in the last attacker log on to an application without applying valid username and password.

3.2 Information Discloser:-Here it is use to obtain sensitive information from a database.

3.3 Compromised Availability of data:- Here compromised data integrity involves altering the content of a database to either Web-page or insert malicious content.

3.4 SQL Injection (Case-Study):-BQE Software's BillQuick Web Suite versions earlier than 22.0.9.1 allows SQL injection that gives rise to an even more serious remote code execution (RCE) risk.

The CVE-2021-42258 vulnerability was patched on October 7 (PDF) but a number of systems nonetheless remain vulnerable.

Huntress Threat Ops team reports that the vulnerability was exploited to get initial access onto the systems of a US engineering company prior to a ransomware attack.

Active exploitation

BQE boasts a user base of 40,000 of mostly small to medium-sized organizations worldwide, and the need for those behind the curve of patching or remediating this actively exploited vulnerability could hardly be more pressing.

The vulnerability enables blind SQL injection via the application's main login form. this opens the door to both stealing data from vulnerable systems without authentication (by dumping SQL database contents) as well as planting malicious code, a detailed technical analysis by Huntress outlines:

With help from our partner, we were able to recreate the victim's environment and validate simple security tools like sqlmap easily obtained sensitive data from the BillQuick server without authentication.

Because these versions of BillQuick used the sa (System Administrator) MSSQL user for database authentication, this SQL injection also allowed the use of the xp_cmdshell procedure to remotely execute code on the underlying Windows operating system.

4. DDOS(DENIAL OF SERVICE):-Description of attack

A DDoS attack remains one of the most effective ways of forcing a website to shut down. In DDoS attacks, sites (or specific pages) become inundated by an overwhelming load of requests, making it so that the server on which the website is hosted is no longer able to accept more requests.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. How to identify a DDoS attack, The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable.

4.1 DDOS(CASE-STUDY):-RECENT DDOS ATTACK ON, SPOTIFY, GITHUB, REDDIT, INSTAGRAM, SOUND CLOUD

Twitter, SoundCloud, Spotify, Shopify, and other websites have been inaccessible to many users throughout the day. The outages are the result of several distributed denial of service (DDoS) attacks on the DNS provider Dyn, the company confirmed.

An attack against a DNS host service appears to be a change of tactics, causing disruption for some of the largest sites in the world as opposed just to taking one offline

we learned that the reason why my Spotify and millions of other user's online activity was interrupted was because of the Mirai botnet

Botnets have become an increasingly prevalent cyberweapon, one that uses malware to enslave network-connected devices to form a massive malicious network that begins to flood website servers with terabytes of garbage traffic, crippling them under the strain.

This is known as a distributed denial of service (DDoS) attack. What makes the Mirai botnet unique is that instead of relying on computers, the malware targets devices on the Internet of Things (IoT), such as the network cameras, digital video recorders, control panels and automation devices that represent a fast-growing product segment of many SIA members.

5. XSS(Cross-Site Scripting):-Cross site scripting is type of injection attack in which malicious scripts from the side of attacker are injected to the user website. Where XSS attack will happen when an attacker or hacker uses a web application to send malicious code normally in the browser side script to different end at the user. This type of attack will occurs anywhere where the web application uses input from a user and an output will generate without validating it.

A attacker can use XSS to send malicious script to unsuspecting user. The Target user browser has no way to suspect that the script should not to be trusted, but it will execute the script because the browser thinks the script came from the trusted source, then the malicious script can access any cookies and session tokens or other sensitive information like user database that used with that site.

5.1 XSS(Stored):- In stored XSS the script that is executed on the web-application will be stored there until and unless it is cleared. Stored XSS is high risk vulnerability as the script is stored on the web-application and if any other user tries to access the same link, he can get affected with the stored XSS.

By this method the script which was targeted for a single user can affect many of the users that visit the same link. HenceStored XSS is a valid threat to the web-application.

5.2 XSS(Reflected):-In reflected XSS the script that is executed on the web-application will be reflected there the time it is executed. Reflected XSS can help the attacker to get the session cookie of the victim by sending him an infected link. By getting the session cookie the attacker can hijack the session of the user.
5.3 XSS(DOM):-In DOM-BASED XSS the Javascript that is executed on the web-application will be reflected there the time it is executed. To execute DOM-Based XSS we need to create a source file which will carry the JavaScript Payload.
5.4 XSS(Case-Study):-The security flaw, tracked as CVE-2022-39239, allowed an attacker to bypass the source image domain allow list by sending specially crafted headers, causing the handler to load and return arbitrary images. Because the response is cached globally, the image would then be served to visitors without requiring those headers to be set.
Therefore, an attacker could achieve XSS by requesting a malicious SVG file with embedded scripts, which would then be served from the site domain.
A vulnerability in Netlify could allow an attacker to achieve either persistent cross-site scripting (XSS) or full-response server-side request forgery on any supported website.
Netlify is a web development platform that also offers hosting and serverless backend services for websites.
Researchers found that Netlify was open to XSS attacks due to a cache poisoning vulnerability.

III. RESULT AND DISCUSSION

The study of all these works in the domain is to acknowledge you about that recent-frauds which are happening in are day to day life.Valuable to the digital forensics' community as tools improve, created, they promote the development of close-knit communities of developers who provide regularly updated and patched or maintained code, bug patches, and extensive documentation

IV. CONCLUSION

The study in this report shows that digital forensics in cybersecurity necessitates more broad and rigorous research, both academic and industry-focused. Because digital forensics is a very broad and broad topic in and of itself, international authorities must stimulate study in this sector as well as hardware development in order to detect and mitigate technological and functional concerns and obstacles. To begin with, digital forensics are often Including tool development. After scrutinizing whether these tools were maintained after development, I found that many were not. when you refer to Quality of comments in the source code found. The problem lies with the fact that in most cases, tool development is not the focus of the research, but rather a by-product. With a combined lack of coding standards, limited testing, disparate repository locations and poor documentation, it is unlikely these tools will ever be widely adopted by the digital forensic community.

REFERENCES

[1]. Abhishek Kumar Pandey, Ashutosh Kumar Tripathi, Gayatri Kapil, Virendra Singh Current Challenges Forensics in Cyber Security, [Internet] January 2020

[2]. Anitta Patience Namanya, Andrea Cullen, Irfan U. Awan, Jules PagnaDisso "CASE STUDY The World of Malware: Overview Bradford, UK [Internet] September 2018

[3]. Ike Vayansky, Sathish Kumar Coastal Carolina University "CASE STUDY Phishing- challenges and solutions" [Internet] January 2018 From- (PDF) Phishing – challenges and solutions (researchgate.net)

[4]. Vahid Kaviani J, Parvin Ahmadi Doval Amiri, Farsad Zamani Brujeni, NimaAkhlaghi, Modification data attack inside computer systems: a critical review, November 2020, Available from:https://www.researchgate.net/publication/345142006_Modification_data_attack computer system in a critical review

[5]. Mohd Amin Bin MohdYunus, Muhammad Zainulariff Brohan, NazriMohdNawi, Ely Salwana, Review of SQL Injection: Problems and Prevention, June 2018, Available From:https://www.researchgate.net/publication/325940419 Review of SQL Injection Problem and Prevention

[6]. Sonakshi, Rakesh Kumar, Girdhar Gopal, "CASE STUDY OF SQL INJECTION ATTACKS", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, ISSN: 2277-9655, pp 176-189, 2018, India. Balakrishnan Subramanian, An Overview of Autopsy: Open-Source Digital Forensic Platform, May 2020, Available From: https://datascience.foundation/sciencewhitepaper/an-overview-of-autopsy-open-source-digital-forensic-platform-1

[7]. Fahdiaz Alief, Yohan Suryanto, Linda Rosselina, TofanHermawan, Analysis of Autopsy Mobile Forensic Tools against Unsent Messages on WhatsApp Messaging Application, November 2020, Available From: https://ieeexplore.ieee.org/document/9251876

[8]. David Ng’ang ‘a Njuguna, John Kamau, Dennis Kaburu "CASE STUDY A Review of Smishing Attacks Mitigation Strategies

[9]. Prashant Saurabh, Amrit Jay Kumar Roy, Role of Cyber Forensics in Investigation of Cyber Crimes, 2021, Available: https://www.ijlmh.com/wp-content/uploads/ROLE-OF-CYBER-FORENSICS-IN-INVESTIGATION-OF-CYBER-CRIMES.pdf

[10]. AmiruddinAmiruddin, HafizhGhozieAfiansyah, Hernowo Adi Nugroho,Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8,2021, Available from: https://ieeexplore.ieee.org/document/9699337

[11]. SecurityScorecard [Online]. Available:https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation

[12]. Sakshi Singh, Suresh Kumar, Qualitative Assessment of Digital Forensic Tools, 2020, Available from: https://www.trp.org.in/wp-content/uploads/2020/11/AJES-Vol.9-No.1-January-June-2020-pp.-25-32.pdf

[13]. Balakrishnan Subramanian,An Overview of Autopsy: Open-Source Digital Forensic Platform, May 2020, Available From: https://datascience.foundation/sciencewhitepaper/an-overview-of-autopsy-open-source-digital-forensic-platform-1

[14]. Muthu Dayalan, Cyber Risk, The Growing Threat,[Internet] November 2017; Available From: https://www.researchgate.net/publication/320753018_Cyber_Risks_the_Growing_Threat

[15]. Sushmita Chakraborty, Praveen Kumar, Dr Bhawana Sinha “Case Study A STUDY OF DOS ATTACKS, DANGER AND ITS PREVENTION May2019 From:- https://www.researchgate.net/publication/335757374_A_STUDY_ON_DDOS_ATTACKS_DANGER_AND_ITS_PREVENTION

[16]. Nagarjun, PMD,AU - Shakeel, Shaik “Case Study Cross-site Scripting Research: A Review International Journal of Advanced Computer Science and Applications

[17]. Prashant Saurabh, Amrit Jay Kumar Roy, Role of Cyber Forensics in Investigation of Cyber Crimes, 2021, Available: https://www.ijlmh.com/wp-content/uploads/ROLE-OF-CYBER-FORENSICS-IN-INVESTIGATION-OF-CYBER-CRIMES.pdf

[18]. https://www.ncsc.gov.uk/guidance/phishing

[19]. https://portswigger.net/web-security/cross-site-scripting

[20]. https://www.bleepingcomputer.com/news/security/hackers-stealing-github-accounts-using-fake-circleci-notifications/

[21]. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9146148

[22]. https://developer.mozilla.org/en-US/docs/Glossary/Cross-site_scripting

[23]. https://www.avast.com/c-ddos

[24]. https://en.wikipedia.org/wiki/Malware

[25]. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Abraar Khan, et. al. "Recent Fraud in Cyber Forensics." *IOSR Journal of Engineering (IOSRJEN)*, 13(1), 2023, pp. 53-57.