International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

A Survey Paper on Identity Theft in the Internet

Guruprasad Saroj[1], Rasika G. Patil[2]

[1]Student, [2]Assistant Professor

[1,2]Bharati Vidypeeth's Institution of Management and Information Technology,

[1.2]Mumbai University, CBD Belapur, Navi Mumbai, Maharashtra, India

How to cite this paper: Guruprasad Saroj | Rasika G. Patil "A Survey Paper on Identity Theft in the Internet" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.969-970, URL: https://www.ijtsrd.com/papers/ijtsrd23966.pdf

IJTSRD23966

ABSTRACT

Identity of any internet user is stole in seconds and the user may not aware about it. There are various tools available in the internet which allow anyone to steal data of any particular user, if he/she is connected to internet. The attacker is not required to have advanced knowledge about the internet technology or how networking works. Identity theft is a tremendous issue for most Internet clients.. This paper is an attempt to make reader aware about how their identity can be theft in the internet. This work expects to expand the mindfulness and comprehension of the Identity thefts that are and related cheats all through the world.

Keywords: *Identity theft, Identity theft techniques:-The harvester, Nmap (Zenmap), Phishing, Google Dork*

1. INTRODUCTION

Identity fraud and character extortion are terms used to suggest to a wide range of wrong doing in which somebody improperly acquires and utilizes someone else's close to home information here and there that includes misrepresentation or trickiness, commonly for monetary increase." as characterized by U.S. Division of Justice. Character criminals take the key bits of the data of client and perform different activity in the interest of the client without knowing him.

2. LITERATURE REVIEW

Identity theft done by many tools which are available on Identity can be steal from any source for eg.

visiting sites,connecting public wifi, bluetooth remain on, downloading content from the internet or visiting any illegal website. Identity can be theft from IP address, website url, Phone number, credit card info, and many more. When user install app in his phone he never read Terms and conditions. After accepting Terms and condition he allows all permission asked be app to allow for better performance. User just want to use the app for some usage, but he doesn't know that he accidentally allow attacker to use his identity. The attacker can now access all of his files, sensitive information, and attacker can set a recorder to record every action done by the user.

3. THE HARVESTER

The Harvester has been created in Python by Christian Martorella. It is a tool which provides us information about e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key server.

This tool is intended to help the entrance analyzer on a prior stage; it is a successful, straightforward and simple to utilize. The sources upheld are:

Google – messages, subdomains Google profiles – Employee namesBing look – messages, subdomains/hostnames, virtual hosts Pgp servers – messages, subdomains/hostnames LinkedIn – Employee names

Exalead – messages, subdomain/hostnames

New highlights:

- Time delays between requests
- XML results export
- Search a domain in all sources

This tool are only allowed to legal authorities of any organization and use of this tool for abuse someone is against the law.

4. PHISHING

Phishing attack depend on more than simply sending an email to victims and hoping that they click on a pernicious connection or open a malevolent attachment, Some phishing scams use JavaScript to place a picture a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be change by using JavaScript.

Phishing efforts for the most part utilize at least one of an assortment of connection control methods to fool unfortunate casualties into clicking, which pass by various names. Connection control is additionally frequently alluded to as URL covering up and is present in many common types of phishing, and used in different ways depending on the attacker and the target.

For example, attackers might attempt to spoof the microsoft.com domain with m!crosoft.com, replacing the letter i with an exclamation mark. Malicious domains may

also replace Latin characters with Cyrillic, Greek or other character sets that display similarly.

One way attackers bypass phishing defenses is through the use of filter evasion techniques. For example, most phishing guards check messages for specific expressions or terms basic in phishing messages - yet by rendering all or part of the message as a graphical picture, aggressors can here and there convey their phishing messages.

5. NMAP

Nmap is outstanding for its data gathering abilities, for example, OS fingerprinting, port count, and administration revelation, however on account of the Nmap Scripting Engine, it is presently conceivable to play out a few new data gathering errands, for example, geolocating an IP, checking if a host is leading vindictive exercises, savage driving DNS records, and gathering substantial email records using Google, among various others.

WHOIS records frequently contain significant information, for example, the enlistment center name and contact data. Framework chairmen have been utilizing WHOIS throughout recent years, and despite the fact that there are numerous apparatuses accessible to question this convention, Nmap substantiates itself priceless on account of its capacity to manage IP extents and hostname records.

Open a terminal and enter the accompanying direction:

$nmap --script whois google.com

6. GOOGLE DORK

Google Dorking is the method for finding vulnerable targets using Google dorks. Google Dorking can return usernames and passwords, email records, delicate archives and site vulnerabilities.

Ethical Hackers use Google Dorking to improve framework security. Black hat programmers utilize this method for unlawful exercises, including digital fear mongering, modern secret activities, and fraud. Google dolts can discover Footholds, sensitive Directories, susceptible documents, inclined Servers, community or Vulnerability information, numerous on-line gadgets, files Containing Usernames and Passwords, touchy on line buying data and Pages Containing Login Portals.

List of Google Dork Queries

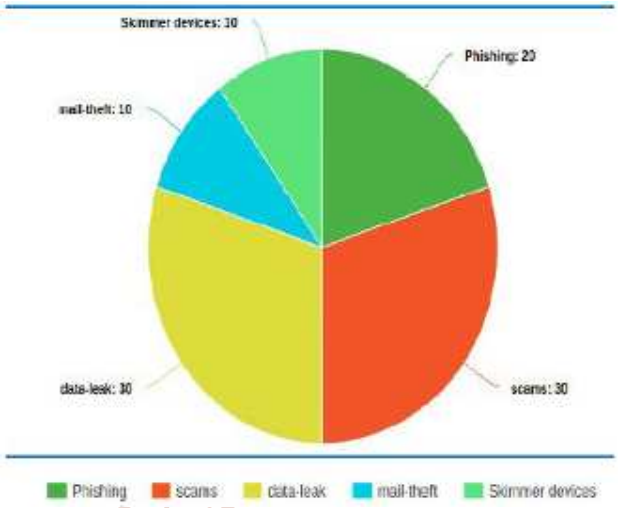
1. Intitle
2. Allintitle
3. Inurl
4. Allinurl
5. Define
6. Site
7. Link

7. Case Study

7.1 Hari, a 27-year-antique funding banker from Bengaluru, has been staying abroad for years. He had a credit score card which he wasn't the usage of anymore nor did he get it cancelled. in the future, he received a name from his bank. He changed into knowledgeable he had exhausted his credit score restriction and the ultimate date to clean his dues became coming nearer. greatly surprised, he realised his financial statistics have been stolen and misused. identification robbery, the most common cyber crime, is obtaining illegally someone's non-public statistics that defines one's identity inclusive of bank account number, Aadhaar variety and credit score card range. The thief can use the stolen statistics to pose as the sufferer for monetary advantage or to commit against the law.

7.2 BENGALURU: Data from caller identity app Truecaller, including names, phone numbers and email addresses of users worldwide, is available for sale on private internet fora, according to a cybersecurity analyst who monitors such transactions.

Data of Indian users, who make up 60-70% of Truecaller's global user base of nearly 140 million, is being sold for about Rs 1.5 lakh (€2,000) on the so-called dark web, the person said. Data of global users is priced as high as €25,000.



8. Conclusion

Every year millions of personal data in india such as mail id,mobile number,Aadhar card information,Pan card information are stolen.Technology has provided us worldwide information,many resources,ease of work and many more benefits but some people and organization use shared data on internet to harm people or theft money or sell that information online. While technology is updated daily in today's world the identity theft or cyber crime are increasing which can be done on minimum scale or maximum scale.

9. References

[1] https://economictimes.indiatimes.com/tech/internet/has-your-identity-been-stolen-heres-what-you-must-do/articleshow/61373168.c ms

[2] https://nmap.org/

[3] https://null-byte.wonderhowto.com/how-to/use-google-hack-googledorks-0163566/

[4] https://www.darknet.org.uk/2012/01/theharvester-gather-e-mail-accounts-subdomains-hosts-employee-names-information-gathering-t ool/

[5] https://www.imperva.com/learn/application-security/phishing-attack-scam/