



Phishing Tools Framework

K Sharath Kumar¹, Reddyvari Venkateswara Reddy², Donthi Reddy Akhilesh Reddy³, Gandra Akhila⁴, Nagireddy Mallikarjun Reddy⁵

¹Assistant Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India

²Associate Professor, Department of CSE (Cyber Security) CMR College of Engineering & Technology, Hyderabad, Telangana, India

^{3,4,5} Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT: Since early stage of internet, phishers have progressively utilized conveyance frameworks to trap their casualties into giving over private and individual data. Indeed, after many years of phishing and overwhelming publicizing about, phishing attacks, are still exceptionally beneficial for fraudsters. As phishers create progressively modern assault vectors, companies continue to battle to ensure their customers' individual data. Customers are attentive to "official" mail and address the keenness of the websites they presently interface with as their belief erodes. As numerous phishing campaigns awareness programs were conducted to avoid spam, organizations can make a prescient approach to check the risk of phishing. By understanding the devices and methods utilized by these proficient criminals and analyzing their own security and application shortcomings, organizations may avoid most well-known and effective phishing assault vectors. Information security is also a concern in today's world due to the expanding number of cyber assaults. Programmers have gotten to be specialists at hacking into somebody else's framework and taking their data. One such strategy is called phishing, which includes taking sensitive data such as emails, credit card numbers, cvv number phone numbers, bank account details, usernames and passwords. Phishing could be an online character burglary in which an assailant employs social design strategies to get a victim's individual and account data. This article looks at the advancement of phishing instruments, their diverse categories, and the countermeasures security specialists can take to relieve their effects.

KEYWORDS- Phishing, Vectors, Framework, Burglary, Information, Security.

1. INTRODUCTION

Today, internet was characterized by advanced networking and technological development, and increase of cyber threats, especially phishing attacks, which requires a careful consideration. As internet users were increases every year, the number of attackers and attacks is also increasing. With every attack, a new type of exploit or vulnerability is being discovered. Phishing is a sophisticated fraud tactic that has undergone significant evolution as it plays a major role in today's cybercrime scenarios. Due to its complex nature, it requires a deeper understanding, especially the increase of integration of technology in our daily lives, which makes the need of strong cyber security measures and increased awareness. Recent studies show the importance of phishing attacks, and notable cases illuminate the complex nature of cyber threats. This research is situated within the academic discourse of cyber security, using existing theories and methods to explore the history of phishing. In this way, we can advance and expand existing knowledge by providing insight into never ending evolving cyber-crimes. This study discovers the unexplored areas in the field of phishing attacks and fills critical gaps in our current understanding of phishing attacks. It will provide a comprehensive review of the diversity of today's cyber threats based on phishing, may offer innovative ideas, strategies to strengthen our defence against this complex threat. As we know, humans are the weakest layer in security architecture of a company or organization. In the world of science and technology, the internet has become an integral part of every service and technology. so you can get almost anything in the world through online, which make it a gold mine for attackers. If someone says that they were one hundred percent secured against any attacks, then that company or organization doesn't know that they were being attacked. For every successful exploitation of an attack, there are some common methods that attackers often use, and one of them is social engineering. One out of five successful attacks is performed by social engineering. In social engineering, phishing is a method where an attacker sends a uniform resource locator (URL) that is designed to get sensitive personal data from the victim's infrastructure. Some of the phishing techniques are email phishing, spear phishing, whaling, smishing, vishing, etc. This paper may not only contribute to the specialized talk but also hoists the discourse by putting a solid accent on moral conduct in the interest of cybersecurity excellence. It helps to supplying cybersecurity experts with a significant knowledge on phishing tools. As ever-changing technology makes the attackers and user of internet more complex and a new type of attack is being discovered every second.

Types in phishing

1.1 Email phishing

Email was one of the first communication method that uses internet to communicate with each other. It can also be used to perform attack. In email-phishing, attacker will send the malicious email containing a program or URL to the victim. Whenever victim opens the Mail, the malicious program will execute immediately and sends the sensitive information to the attacker. Most of the email providers filters/blocks malicious domain, even so attackers discover a new technique to bypass these filtering method (e.g., cash, money and rewards are some of the keywords that can be blocked by a email servers. Attackers exploited by using c@sh, m0ney, reward\$ these words to escape the filtering).

1.2 Spear phishing

Another yet, a common form of phishing technique called spear phishing. In this attack the attacker will target a group of people like employees or managers of a certain company. First the selects the targets and do some recon about them and launches the attacks. Spear phishing mainly targets the high valued persons like VIPs, Board Members etc. as these persons plays crucial role in growth of a company, this makes the attack more special and fearsome, one wrong click by any person then it can cause a severe damage to the company. On understanding these forms of attacks one can reduce and minimize the overall attack surface of a company.

1.3 Whaling

Whaling is another form of phishing, which is similar to spear phishing that comes under Social Engineering, it targets the High-profile employees and executives of a company. Its main goal is to trick targets into sharing sensitive data, money, grant special permissions and sensitive trade secrets to the attackers which may benefit to attacker. This form of attack is very rare in phishing, but this attack can cause very serious damages such as reputation, financial and intellectual to the organization (or) company.

1.4 Smishing and vishing

Both smishing and vishing comes under phishing. In smishing, the attacker sends a malicious text message or SMS to victim. When the victim opens a malicious URL and submits the data it redirects the submitted data to the attacker. Vishing is also similar to Smishing, but the attacker sends and uses phone calls, voice messages, and VoIP. It's an easy process but a very effective approach for attackers, here the attackers directly contact with victim and deceive them to reveal sensitive information which benefits the attacker.

2. LITERATURE REVIEW

In a study by Diaz et al. (2020), 1,350 randomly chosen undergraduate students get phishing attacks, which taken to look into user click rates, demographics. The exam included students from a different academic Fields, including engineering, mathematics, the arts, and the social sciences. In the study found that several factors, including age, academic year, college affiliation, phishing awareness, internet usage frequency, and cyber-training, all influenced students' susceptibility. The conclusion that those with higher phishing knowledge are more vulnerable to phishing scams is most unexpected. For these unexpected results, the authors entertain two theories. First, as users have been falling for phishing scams more often, their awareness of phishing may have grown. The people who fell for phishing, might not be as informed as they believed. The least number of clicks came from engineering and IT majors, while older students were more adept at identifying phishing emails and URLs.

Phishing attacks continue to pose a significant threat to users, with psychological studies indicating that various factors will impact a user's ability to resist such attacks. These factors include the security features of the browser and the user's perception of phishing. In a study conducted by (Dhamija et al., 2006) involving 22 participants, it was discovered that phishing websites deceived an alarming 90% of participants, while 23% were forgot their security credentials, such as login status and addresses. A similar study conducted (Alsharnouby et al., 2015) found that only 53 out of 100 phishing websites were detected by participants. The authors were also observed the amount of time spent scanning browser items affects and the ability to detect the phishing. The primary reasons that contribute to users falling to phishing, includes lack of knowledge, understanding, and carelessness, leading them to accidentally open suspicious attachments or to click on fake links that result in malware infections. To mitigate the effects of phishing attacks, it is crucial to prioritize user education and preparation.

Empirical investigations into phishing vulnerabilities have uncovered distinctive gender-specific proclivities. Notably, the female demographic manifests an increased susceptibility attributable to a discernible deficit in technical prowess, contrasting with the male cohort's heightened vulnerability to mobile phishing, underscored by an unwavering reliance on mobile and online services (Getsafeonline, 2017; Hadlington, 2017).

Moreover, a discerned positive correlation between extensive PC engagement and heightened proficiency in phishing detection amplifies the intricacies of this cyber threat landscape (Iuga et al., 2016). Cybersecurity behaviour's, intricately entwined with parameters such as internet addiction and impulsivity, surface as pivotal predictors of susceptibility, as illuminated by the nuanced findings in Hadlington's exploration (2017). The subversion of website trustworthiness, exemplified by surreptitious domain manipulations, introduces a dynamic layer to this complex milieu. Instances where malevolent actors strategically replace letters

with numerical equivalents, as exemplified by the metamorphosis from 'google.com' to 'google.com,' exploit user trust in established online entities with calculated precision (Hadlington, 2017).

In summation, this research accentuates the exigency of bespoke educational interventions. Such interventions, envisioned to endow users with nuanced insights and adept acumen, are tailored to address not only demographic idiosyncrasies but also the intricate behavioural determinants, thereby fortifying resilience against the multifarious tapestry of phishing threats.

3. OBJECTIVE

The objective of this research project is used to develop a customizable phishing framework that will be used for conducting phishing campaigns and also awareness programs to educate, the people on rise, of phishing and their complex nature. Phishing poses significant threat to companies and organizations and humans are the weakest layer of security due to this attacker prefer phishing attacks, these attacks cover 20% of overall cyber threats that happen in an annual year. This framework prioritizes the user interface and customization for different templates and we can add new templates to it. Initially, it contains three types of phishing attacks and we can add other types of attacks to it.

4. PROBLEM DEFINITION

Phishing is a type of social engineering method where an attacker tricks victims into sharing sensitive information, this research project is used to develop an phishing framework, in which it is used for raise awareness about phishing and the damage that will affect to the organization and the employees working for it. This project was mainly focused on user interface, customization and being user friendly to the users. It provides a diverse set of different types of phishing methods and the way that can respond when we deliver the URL to the victims. These methods are solely use to perform a campaign on phishing in a simulated networks or areas within an organization to reduce the risks that posed by phishing.

5. METHODOLOGY

5.1 Installation of IDE

Here, first we have to install the VS Code. Create a new folder called Major Project.

5.2 Installation of XAMPP

It can be used to run the project on local server and config the port as 8080 in control panel

5.3 Config phpMyAdmin

Create a root account in MySQL database, and create a table called victims.

5.4 Setting up API's

getUserMedia API is used is integrate with browser, and Ipinfo needs the api key to use.

5.5 Config XAMPP

Config the sendmail.ini, php.ini files. Set the from email and to email options to our requirements.

5.6 Secure Shell Connection

Establish a new SSH connection to serveo.net Public Servers.

6. IMPLEMENTATION

In this project architecture had three main types of options they are geolocation finder, website cloning, and camera phishing. Here the users can opt/select an option for further process. It is completely web-based project that offers different types and also provides customization for various factors.

6.1 Selection

Here we need to select the type/category of phishing attack, after the successful selection of phishing, it will load a website that URL should be sent to victim.

6.2 Geolocation

Here the webpage contains the JavaScript code whenever the user clicks on the buttons it will loads a function that had a special script which permission prompts of location until the user gives the permission it won't go to next step, after the victim allows the location permission, an asynchronous http request is called to backend program called "login.php" that stores the latitude and longitude into local text file in the server.

6.3 Website Cloning

Whenever the victim clicks the webpage option it will loads another webpage that containing different types of website clones, and user can select a web page to launch the attack. The URL should be sends it to victim and whenever the victim open and enters the sensitive data in the webpage after clicking the submit it will load the original webpage and sending that sensitive data to our server, we can store it into local text file.

6.4 Camera

Whenever the victim clicks on the link the browser displays the permission prompts for camera, if the user grants/allows the camera permission it will sends the encoded captured image to backend server and the server will saves the decoded captured image in png format into local file system.

6.5 Port Forwarding

All the project is developed on a local server to access it across the web. we need to use public server along with port forwarding service the project will run in localhost 8080 port number we can use free serveo.net public server via SSH (Secure Shell) tunnelling which makes the serveo.net as our public or traffic forwarding server.

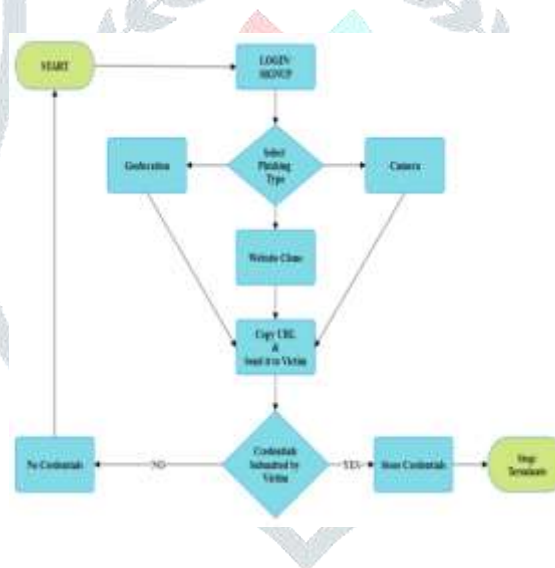


Fig.1 Architecture

6.6 Save Results

All the results will be stored in the local file system into a text file, for images they will be stored in images folder which is in the root folder of the project. The Ip addressed will be stores into a "victims. json" file.

7. RESULT

When generating results from the system, all data will be stored within the local file system as outlined in the project specifications. Textual results will be saved directly into text files. For images, they will be stored within an "images" folder located in the root directory of the project. Each image will be saved in the .png format to maintain consistency.

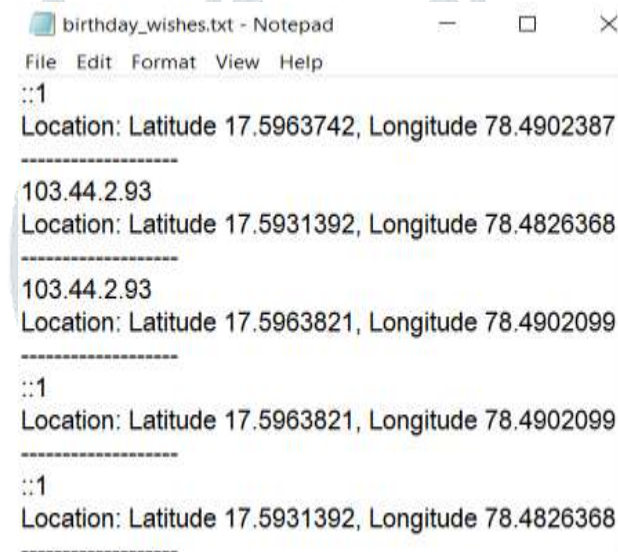
```

usernames.txt - Notepad
File Edit Format View Help
Ip Address: ::1
Date: 2024-02-21
Time: 11:48:03
mediaFire Username: bvasvac@hbjd.sds
password: svchsgsvsgh
-----
Ip Address: ::1
Date: 2024-02-21
Time: 11:48:43
mediaFire Username: bvasvac@hbjd.sds
password: svchsgsvsgh
-----

```

Fig.2 MediaFire Credentials

The fig.2 shows the results of username and password of website clone attack of a victim.



```

birthday_wishes.txt - Notepad
File Edit Format View Help
::1
Location: Latitude 17.5963742, Longitude 78.4902387
-----
103.44.2.93
Location: Latitude 17.5931392, Longitude 78.4826368
-----
103.44.2.93
Location: Latitude 17.5963821, Longitude 78.4902099
-----
::1
Location: Latitude 17.5963821, Longitude 78.4902099
-----
::1
Location: Latitude 17.5931392, Longitude 78.4826368
-----

```

Fig.3 Location Details by Ip Address

The fig.3 shows the results of a location-based output contains Ip Address, longitude and latitude of a victim.

8. CONCLUSION

This research project is successfully achieved its objective by providing the various techniques and the different categories of phishing stacks which makes it a valuable resource to conduct the phishing campaigns and awareness programs on how the real-world phishing attacks are targets the people and the damage that can cause to the organization and the people working for it. This project is not liable to any unethical use it is solely created for pen-testers and security professionals to conduct campaigns and awareness programs.

REFERENCES

- [1] Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *Int. J. Human-Computer Stud.* 82, 69–82. doi: 10.1016/j.ijhcs.2015.05.005
- [2] Getsafeonline (2017). Caught on the net. Available at: <https://www.getsafeonline.org/news/caught-on-the-net/%0D> (Accessed August 1, 2020).

[3] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3, e00346-18. doi:10.1016/j.heliyon.2017.e00346

[4] Iuga, C., Nurse, J. R. C., and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Hum. Cent. Computes. Inf. Sci.* 6, 8. doi:10.1186/s13673-016-0065-2

[5] King Phisher: <https://github.com/rsmusllp/king-phisher>

[6] Social Engineering Toolkit: <https://www.trustedsec.com/resources/tools/the-social-engineer-toolkit-set>

[7] GoPhish: <https://getgophish.com>

