International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 2, January-February 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Comparative Analysis of Phishing Tools

Sudhakar P[1], Dr. Uma Rani Chellapandy[2]

[1]Student, [2]Associate Professor,
[1,2]Department of MCA, Jain deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

A phishing attack is the type of social engineering which Cybercriminals use to manipulate people to collect sensitive information. With today's available technology phishing can be launched even with smartphones in a few clicks. Setting up and operating a phishing attack is fast, inexpensive, and low risk with no expert knowledge anyone can launch an attack. many originations have suffered losses from phishing. Phishing is the most common social engineering attack which contributes more than 75 percent of all security breaches.

This article examines and compares various phishing tools which can simulate phishing attacks to give people real-life phishing attack experiences and make people aware of the risk and train how to respond.

KEYWORDS: *Phishing, toolkits, social engineering, cyber awareness*

How to cite this paper: Sudhakar P | Dr. Uma Rani Chellapandy "Comparative Analysis of Phishing Tools" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-2, February 2022, pp.1451-1453, URL: www.ijtsrd.com/papers/ijtsrd49446.pdf

IJTSRD49446

1. INTRODUCTION

As the number of internet users is increasing over time, cybercrimes are also increasing due to the lack of cyber security awareness in the users. End-user cyber security awareness relates to how well they understand the cyber security threats that their networks face, the risks they pose, and the security best practices that may be used to guide their behavior.

In Phishing an attacker sends bogus messages to a human target in order to fool them into exposing sensitive information or installing malware on their machine. Phishing attacks have become more sophisticated, allowing the attacker to monitor everything the victim does while on the site and bypassing any further protection levels. A phishing attack can be launched by anyone with minimum knowledge which makes it a dangerous and most common threat.

Internet users need to be trained about these types of attacks and also need to be thought about how to respond to the attacks.

A phishing toolkit is a platform with pre-configured or customized phishing tests, that allows us to conduct (simulate a real-time phishing attack) and control every part of a phishing awareness campaign.

In this paper, different types of phishing tools are compared where the description and features of each tool are explained followed by a comparison chart. The user can choose the best tool among them.

2. INVESTIGATION TOOLS

2.1. Gophish

Gophish is a web-based toolkit developed with go-language that enables pentesters to conduct real-world phishing simulations. The main objective of this tool is to make it Affordable and Accessible to everyone. It is an open-source application

Features:

- Multiple Campaign
- REST API
- supports Windows, Linux, and Mac OSX
- GUI
- Real-time result reports

2.2. King phisher

It provides a complete suite with graphical user interface to launch and manage Phishing Campaigns

that imitate phishing attempts in the real world to exercise and prepare end-users how to respond to such attacks. King Phisher has the ability to run a variety of campaigns parallelly.

Feature:
- Run multiple phishing campaigns parallelly
- For a more credible appearance, send an email with included photos.
- Supports 2fa capturing
- Captures Geolocation
- API
- GUI

2.3. SET tool kit

The Social-Engineer Toolkit is a CUI-based toolkit. It contains a huge collection of browser exploits and allows creating custom payloads, it is a powerful pen-testing tool.

Features:
- free and Open Source
- supports Linux, and Windows.
- Supports integration with custom modules.
- provides many attack vectors

2.4. Evilginx2

bypassing multi-factor authentication is the main feature of this tool, this is one of the best tools available on the internet. As the man-in-the-middle, Evilginx2 collects all access tokens along with usernames and passwords. This feature of extracting access tokens makes it outstanding than other tools. By extracted tokens, an attacker can break any kind of multi-factor authentication enabled on the user's account.

Features:
- Access token capturing

2.5. Hidden Eye

The hidden eye is a simple to use phishing toolkit that enables the integration of various modules such as keylogger, custom templets, data collectors. It consists of preloaded social media templates which are ready to integrate with other modules.

Features:
- All the sites are mobile compatible.
- Keylogger
- Fake security templets
- 2FA capturing

2.6. Social phish

Social phish is a simple open-source basic level Phishing Tool. It is simple than Social Engineering Toolkit. It consists of preloaded popular social media templates such as Facebook, Instagram, Google, Microsoft, etc. also providing the option to create and use a custom template.

Features:
- open-source tool.
- written in bash language.
- Supports Ngrok,serveo.net tunneling.

3. COMPARISON TABLE

Phishing tools	Go phish	King phisher	SET tool kit	Evilginx2	Hidden Eye	Social phish
Open-source	√	√	√	√	√	√
Multiple phishing campaigns	√	√		√		
GUI	√	√				
Report generation	√	√				
Geo-location		√				
Capture 2fa tokens		√		√		
API	√	√				
Keylogger					√	
OS						
Linux	√	√	√	√	√	√
Mac	√		√		√	
Windows	√	√		√		
Android			√		√	√

4. FUTURE SCOPE

Even using additional security mechanisms like multi-facture authentication is useless when the user is not aware of basic security elements. Every user on the internet should be aware of cyber-attacks and their risk. Educating Internet users on common threats is important to successfully fight against cyber threats. A company security posture will be good enough until the employees are well aware of cyber threats. As social engineering type of attacks focuses on human nature to breake into information system. It is necessary to exercise the employee with emerging threats that are sophisticated enough to exploit human behavior.

5. CONCLUSION

Social networking sites is one of the most common platform where all categories of people use, which makes it huge threat surface for phishing attack.

In this paper, the differences between some phishing tools are listed along with a comparison chart. There are many tools available on the internet with different features. Selecting the right tool based on the criteria depends on an individual user.

6. REFERENCES

[1] http://en.wikipedia.org/wiki/Internet_security_awareness

[2] https://getgophish.com/

[3] https://github.com/rsmusllp/king-phisher

[4] https://github.com/kgretzky/evilginx2

[5] https://github.com/yevgen2020/HiddenEye

[6] https://github.com/xHak9x/SocialPhish