International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || PP.01-04

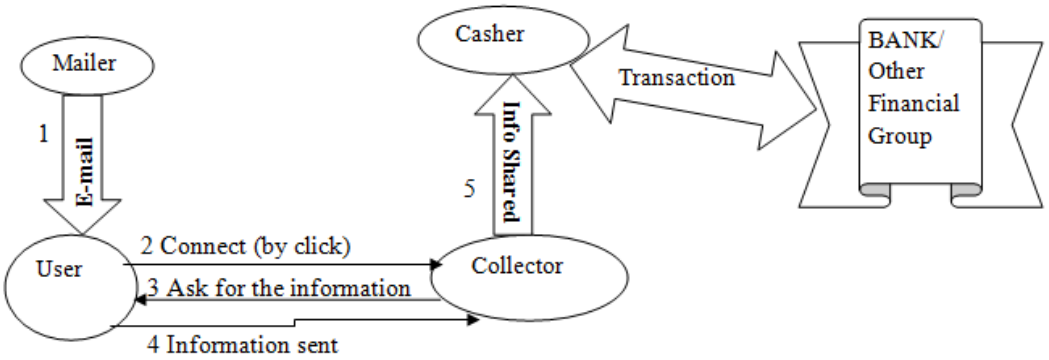
A Statistical Review of Phishing Attack

Tarun Sharma[1], Navdeep Singh[2]
[1]*(Dept. of computer application, CT Institute of Management and Information Technology, Jalandhar)*
[2]*(Department of Computer Science, Trinity College, Jalandhar)*

Abstract: Today, world is moving towards the digitalization. Each and every person on this planet is connected with the internet through one way or another. It is the high time for the cyber attackers to fetch the information of any person with the help of technology. One of the popular cyber attacks is Phishing. Phishing is a type of attack in which a person, also known as phisher, try to retrieve the confidential or sensitive information of an internet user by mimicking e-communication from a renowned organization in automated fashion. In this paper we will review the number of phishing attack in a region and number of people affected by it and later we will discuss about the types of industries affected by the attack.
Keywords: Phishing attack, statistical review, industries affective.

I. Introduction

The word "Phishing" comes in the existence in middle of 1990s, when e-scammers used email as bait to fetch the financial information of legitimate user from the sea of networks (internet). A complete phishing attack needs three role of an attacker: Mailer (Lure), Collector (Hook) and Casher (Catch). The mailer sends the number of deceitful emails to the user, which directs to the fake websites. Collectors handle the fake website, which ask user for the confidential information. At last casher use that information to complete the fraud.



4 Information sent

Fig. 1: Showing the flow of information in phishing

II. Techniques For Phishing Attack

There are many techniques or you can say tools to make fool of the user and fetch the confidential details from the user. Following are the popular trends in this aspect:

2.1 Malware

In this technique a malicious software is send to the user through the e-mail and that particular software install key loggers or screen grabbers on the system of user and then the phishing attack is performed. This usually performs the following tasks:

- Distributed denial of service (DDoS)
- Surveillance
- Redirections for phishing sites
- Installation of other malwares
- Susceptibility scanning and misuse

2.2 Session Hijacking

In this particular attack, attacker monitors the user's activities until an authenticated session with profitable site(according to attacker) is made then the attacker takes over and perform the unauthorized function

like amount transfer etc without the knowledge of user. The most popular method for this is "Man in the Middle Attack".

2.3 URL Beclouding

This method deceives the user from trustworthy site to a malicious site. This is very simple technique but is very effective against the unaware user. In this method attacker can opt any technique to deceive the user:

- HTML Redirection
- Alternate Encoding Schemes
- Analogous Domain Names

2.4 System Reconfiguration Attack

This is very popular and most in use. In this the attacker change the settings on the victim's system without his/her knowledge i.e. attacker can modify the address of an authenticated site with a phishing site. Pharming (DNS based phishing) is one of the types of system reconfiguration attacks.

2.5 Search Engine Phishing

Attacker creates the web pages with some false information (products) and gets them indexed by the search engines and then take the detail of user through order, sign-up or any other activity and later on they use that information to perform the fraud.

2.6 Spear Phishing

This type of phishing usually attack the user with their personal information available on public networks. It can include messages from the topics related to the recipient's role in company, job opportunity, hobbies and any other information from social networking websites. These details make the messages appear more legitimate and have good chances of user to click or download attachments.

Besides these there are many tools or techniques available to perform the phishing attack on user. E-mails, messages and phone calls are the major carriers to perform these attacks. One should be vigilant while surfing through the internet to save him from these attacks.

III. Reports About Phishing

In recent years it has found that phishing attacks are more prevalent in the social engineering. Following are the some stats about the phishing attack:

3.1 Country Wise

Kaspersky labs have provided the data about the percentage of user attacked in the second quarter of 2017(Country wise).

Table 1: Top 10 Countries by percentage of user attacked

S.No	Country	% age of user affected
1	Brazil	18.09
2	China	12.85
3	Australia	12.69
4	New Zealand	12.06
5	Azerbaijan	11.48
6	Canada	11.28
7	Venezuela	10.56
8	South Africa	9.38
9	Argentina	9.35
10	United Kingdome	9.29

From this data it has observed that, Brazil is at the top of the list among the top 10 countries in which users are affected by the phishing attack. Australia added 1.96 p.p to the previous quarter's data and come to the third place and on the other hand the percentage of attack in China has decreased by 7.24 p.p and hence moved to second in the list. In the second quarter, Russia exited the top ten lists with the 8.74% of user attacked. From the last two quarter data, it is conclusive that countries are taking more protective measures to overcome the problem of phishing and on the other hand attackers are working on more sophisticated ways to attack the user.

3.2 Organization Wise

The rating of attacks on different types of organizations is based on detections of Kaspersky Lab's heuristic anti_phishing component. In Q2 2017, the e-payment systems has added 4.8 p.p., the banks and online stores subtracted 2.33 p.p. and 1.31 p.p respectively. The following three sites are ranked top 3 social sites which are attacked in Q2 2017.

Table 2: Percentage of detected phishing links

Organization	% age of detected phishing links
Facebook	8.33
Microsoft Corporation	8.22
Yahoo!	8.01

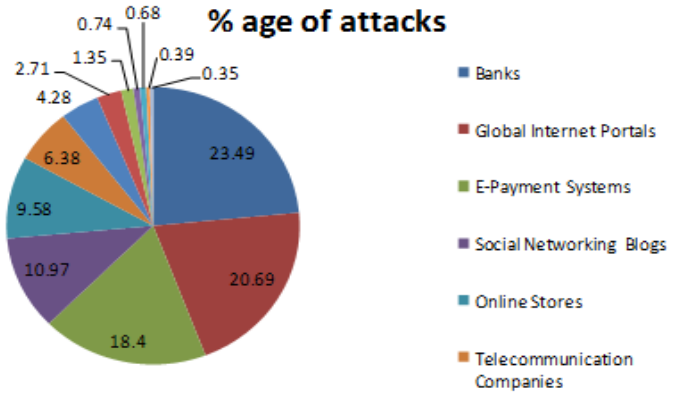


Fig. 1- PIE Chart showing the %age wise attack of phishing on various organizations

In Q2 2017, the average share of spam in global email traffic amounted to 56.97%, which was only 1.07 p.p. more than in the previous quarter. In the second quarter, the most popular malware family was the JS.SLoad (8.73%), with another downloader, MSWord.Agent, in second (3.31%). The Fareit Trojan family (3.29%) rounded off the top three.

3.3 Malware Wise

There are many categories of malware currently active in the third quarter of 2017. The most powerful malware which upset the market and causes some serious losses to the organization is "Ransomware". This type of malware locks away victims' data by encrypting it, then demands a "ransom" to unlock it with a decryption key. Ransomware continued to dominate the threat landscape. New variants emerged daily, development of destructive ransomware persisted, and targeted attacks grew. The following graph shows the overall message volume by a malware.

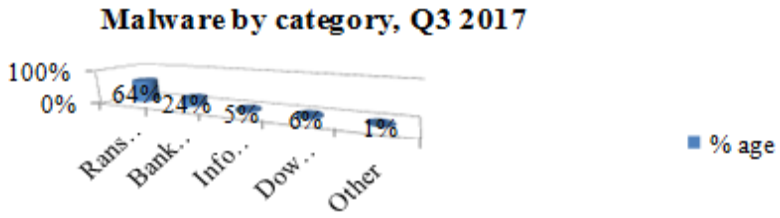


Fig. 2- Showing the category of Malware attack in Q3 2017

IV. Comparison of Industry Targeted

4.1 Email fraud

In email fraud attacks, an email purporting to come from a top executive asks the recipient to wire money or send sensitive information. It doesn't use attachments or URLs, so it can be hard to detect and stop. The following comparison shows which industry is targeted (%age wise) by the e-mail fraud attacks in Q3 2016, Q2 2017 and Q3 2017.

Table 3- Email fraud attacks

Organization type	Q3 2016	Q2 2017	Q3 2017
Manufacturing	31	43	44
Telecommunications	23	38	24
Technology	26	37	41
Financial Services	27	23	24
Government	3	2	6
Education	6	8	13
Business Services	27	28	31

All industries continue to be targeted by email fraud, but attackers did seem to favor organizations with the complex supply chains. Manufacturing companies are targeted more than other industries.

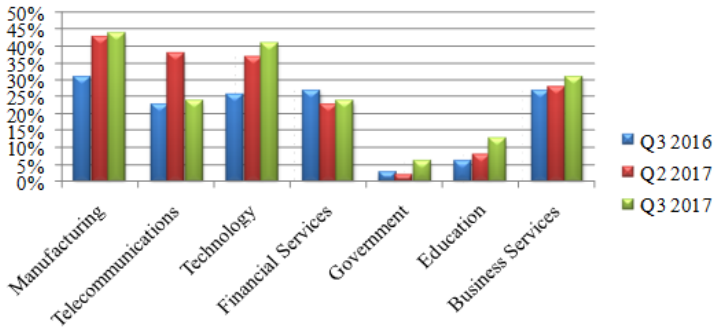


Fig. 3- Average number of email fraud attacks, by targeted industry, Q3 2017 vs Q2 2017 and Q3 2016.

It is very clear from the above chart that manufacturing and technology related industries are more likely to be attacked as compare to other industries. The number of attacks has risen significantly from Q3 2016 to Q3 2017. Many companies are taking many safety measures to secure their data from the attackers.

V. Conclusion

Phishing is a very lucrative activity for cyber attackers. It will never be eradicate. However, it can be reduced by educating the user and performing some up gradations in the system. Users are becoming more aware about the phishing crimes and how to identify the phishing attack. On the other hand, attackers are trying many new ways to fool the user like web obfuscation technique to create the website that is very difficult to differentiate from the legitimate site. This paper has discussed about some of the fishing technologies used by the attacker and showed some data of cyber attack on organizations and the countries. It is clear from the above data that governments and other non-profitable organizations are taking step forward to control the effect of phishing in this advanced era of technology.

References

[1] APWG:[Anti Phishing Work Group] https://www.antiphishing.org/resources/apwg-reports/ Phishing Activity Trends Report, pwg_trends_report_h1_2017.pdf
[2] APWG:[Anti Phishing Work Group] https://www.antiphishing.org/resources/apwg-reports/Phishing Activity Trends Report, apwg_trends_report_q4_2016.pdf
[3] Proofpoint, Inc. : www.proofpoint.com pfpt-us-tr-q317-threat-report_1.pdf
[4] V. Suganya, "A Review on Phishing Attacks and Various Anti Phishing Techniques", *International Journal of Computer Applications (0975 – 8887*) Volume 139 – No.1, April 2016.
[5] Junxiao Shi, Sara Saleem,"Phishing"
[6] Wikipedia: https://en.wikipedia.org/wiki/Phishing
[7] Kaspersky labs:[Kaspersky labs reports on phishing] https://securelist.com/spam-and-phishing-in-q2-2017/81537/
[8] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse," Phishing Attacks and Defenses", *International Journal of Security and Its Applications* Vol. 10, No. 1 (2016), pp.247-256 http://dx.doi.org/10.14257/ijsia.2016.10.1.23.
[9] Jason Milletary, US-CERT, "Technical Trends in Phishing Attacks".