International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-4, Issue-1, January 2018 Pages 01-02

A Review Paper on Phishing Through E-Mail

Monika Nishad

***Abstract*— We cannot imagine a day without a computer especially without Internet. E-Mail plays a vital role in communication globally for communication and sharing of data as well. Now a day the word phishing is known to some people but still a huge amount of people who does not know about this word.It is the most common way to perform cyber-crime by cyber-criminal. This paper present overview about phishing email attack, its classification and preventing approaches.**

***Index Terms*— Phishing, Cyber-crime, Cyber-criminal.**

I. INTRODUCTION

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life; on the other hand it also increases the need for security measures too. Phishing is a con game that uses to collect personal information from unsuspecting users.This is similar to Fishing, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. But the hook inside it takes the complete fish out of the lake.The word 'Phishing' initially emerged in 1990s. The early hackers often use 'ph' to replace 'f' to produce new words in the hacker's community, since they usually hack by phones. The word phishing means to maintain a fake website of any reputed company and ask the member of that website to update their personal information in order to remain active their IDs. Phishing is a cyber-crime and the person who performs such type of activity is called cyber criminals. Spooled e-mails are sent to a set of victims asking them (usually) to upgrade their passwords, data accounts, etc. Calling the victims on the phone, classic social engineering techniques are used by phishers.

II. HISTORY

1980s

A phishing technique was described in detail in a paper and presentation delivered to the 1987 International HP Users Group.

1990s

The term 'phishing' is said to have been coined by the well-known spammer and hacker in the mid-90s, Khan C Smith.[43] The first recorded mention of the term is found in the hacking tool AOHell (according to its creator), which included a function for attempting to steal the passwords or financial details of America Online users.

III. LITERATURE REVIEW

1. Phishing emails pose a serious threat to electronic commerce because they are used to defraud both individuals and financial organizations on the Internet.
2. According to an ecrime trends report , phishing attacks are increasing at a rapid rate. For example, phishing in Quarter 1 (Q1) of 2011 grew by 12% over that in Quarter 1 (Q1) of 2010.
3. A survey by Gartner [6] on phishing attacks shows that, approximately 3.6 million clients in the US alone had lost money to phishing attacks and total losses had reached approximately US$ 3.2 billion Dollar. The number of victims increased from 2.3 million in 2006 to 3.6 million in 2007, an increase of 56.5%.
4. Email has been an online 'killer application' utilized by people, businesses, Governments and different organizations for the needs of communicating, sharing and distributing data ..
5. He has mentioned that it is possible to detect phishing web pages by evaluating the visual similarity of web pages. Visual assessment approach, semantic assessment approach, human computer interaction enforcement, and web page originality verification.

6. He has mentioned that He illustrated and explained CRM114 usage for small-, medium-, and large-scale enterprises (for filtering up to one million client email accounts). He presented the internals of a system using CRM114, implementing the concept of Internet postage known as the CAMRAM. He described a unified model of spam filtration followed by all the spam filters currently available in the market.

IV. CLASSIFICATION OF PHISHING ATTACKS

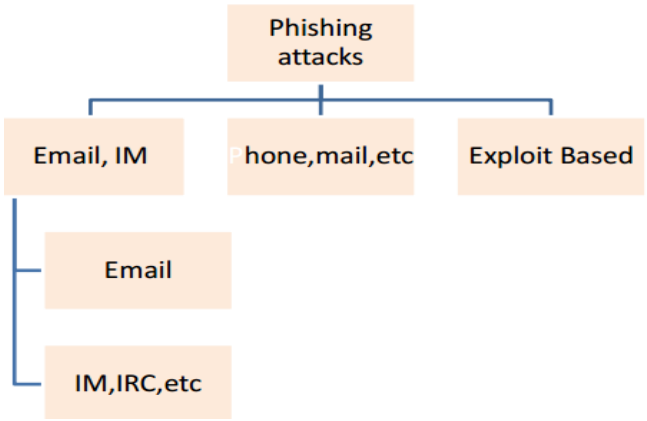
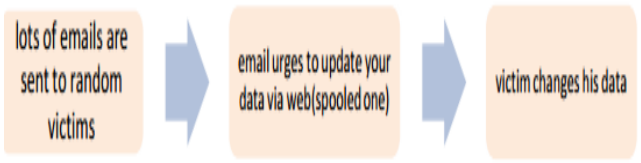


Figure- Types of attack [2]

Monika Nishad, Computer science, Shri Shankaracharya Group of Institution, Bhilai, Durg , India

V. EMAIL PHISHING PROCESS



VI. PHISHING ATTACK STAGES

Phishing attacks involve several stages:

• The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.

• The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.

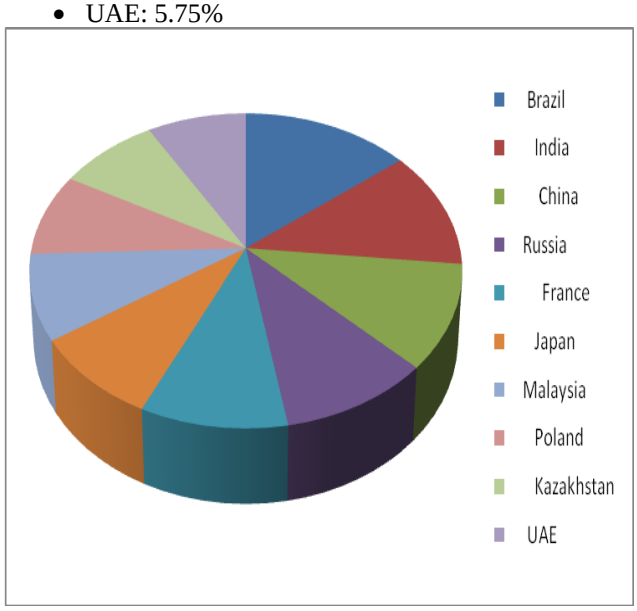
• The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source

. • Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.

• The attacker harvests the victim's sensitive information and may exploit it in the future.

Here is a look at a breakdown of the attacks that occurred in 2015 by what country the victim lived in

- Brazil: 9.74%
- India: 8.3%
- China: 7.23%
- Russia: 6.78%
- France: 6.54%
- Japan: 5.93%
- Malaysia: 5.92%
- Poland: 5.81%
- Kazakhstan: 5.79%
- UAE: 5.75%



VII. REPORT PHISHING

Whenever user finds a particular webpage as spam one he can report the phishing on following websites:

Businesses and consumers can file phishing reports with the following organizations:

Anti-Phishing Working Group
http://www.antiphishing.org

Digital Phishnet
http://www.digitalphishnet.org/

Federal Trade Commission
http://www.consumer.gov/idtheft/

Internet Crime Complaint Center (a joint project of the FBI and the National Collar Crime Center)
http://www.ic3.gov

Trend Micro Anti-Fraud Unit
antifraud@support.trendmicro.com

VIII. CONCLUSION

While surfing to the internet most of the users who are inexperienced falls victim to phishing activity. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users.As communication mode in this IT era is EMAIL. All kinds of communication made must be ensured. To address this problem we have given an awareness to let the common people about the Phishing issues and its consequences. Many researchers have provided various solutions to find, prevent and avoid phishing. We are on the process of developing new method which overcomes all the demerits of the existing phishing solutions. In addition to providing new solutions it is very important to give the awareness of this issue.

REFERENCES

[1] AmmarAlmomani, B. B. Gupta, SamerAtawneh, A. Meulenberg, and EmanAlmomani., A survey of phishing email filtering techniques, IEEE communications surveys & tutorials, vol. 15, no. 4, fourth quarter 2013

[2] Ian Fette, Norman Sadeh, Anthony Tomasic, Learning to Detect Phishing Emails, Track: Security, Privacy, Reliability, and Ethics WWW 2007.

[3] JingguoWang,TejaswiniHerath,RuiChen,ArunAishwanath, and H. RaghavRao, Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email," IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, VOL. 55, NO. 4, DECEMBER 2012.

[4] AmmarALmomani; B. B. Gupta; Tat-Chee Wan; AltyebAltaher; SelvakumarManickam, Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection "Zero-day" Phishing Email, Indian Journal of Science and Technology, Vol: 6 Issue: 1 January 2013 ISSN:0974-6846

[5] Dr.anthonyyingjiefu in Ph.D thesis titled "web identity security: advanced phishing attacks and counter measures-2006.

[6] "Fighting Spam, Phishing and Email Fraud" by Mr.ShailendraChhabra..