Volume-4, Issue-4, April-2015 • ISSN No 2277 - 8160

Research Paper Engineering

Shifting Trends in Phishing

Prabhanshu Sharma

Dr Kirti Mathur

ABSTRACT

Abstract- This Paper discusses about Phishing attacks and provides practical information on the practice. Common techniques and trends are then discussed, including the growing integration of phishing, spamming, and botnets. Additionally, users awareness is discussed and new trends that have or are likely to emerge are brood over. Finally, we conclude this paper with an overview of the lessons learned and suggestions on its handling.

KEYWORDS : Phishing, Spoofing, Pharming

Introduction

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials [11]. This is done using 'spoofed' email leading consumers to websites designed to trick recipients and pick financial data such as credit card numbers, account usernames, passwords etc. With the increasing shift of people towards e-commerce, the possibility has spawned even more. When a potential victim clicks on a phishing link that has been caught, he is redirected to the original page.

The main strategy followed by the attacker is mass email to their target subgroup. They usually contain enticing offers attracting the victim to visit the phishing website or make an urgent request for the user's personal credentials.

II. Phishing Tools

Phishing attacks rely on simple tools to trick users. [12]The underlying infrastructure to support a phishing scam may be a simple copied HTML page uploaded to a freshly compromised web server and a server side script to process any user input data, or it may involve more complex web sites and content redirection. It is very easy to produce a web site mimicking a target organization, and poorly secured web servers can easily be located and compromised. Even home PC's can make effective hosts for phishing. Attackers are rash and simply select large IP address blocks to scan at random for an exploitable security vulnerability. Spam emails are sent via compromised servers hosted in foreign countries, or via global networks of zombie PCs (botnets), so that they cannot be traced.

To make believe that an email is genuine, phishers:

1) Use IP addresses instead of domain names in hyperlinks.
2) Register similar sounding DNS domains for setting up fake web sites (eg. flipcart.com for flipkart.com).
3) Embed hyperlinks from the real target web site into the HTML contents of an email so that the user's web browser makes most of the HTTP connections to the real web server and a few to the fake one.
4) Obfuscate the fake web site URL as the users skip to notice changes done to a hyperlink and may assume it benign.
5) Configure the fake site to record any input data the user submits, silently log and then forward him to the real web site.
6) Redirect victims to a phishing web site by using
malware to install a malicious Browser Helper Object on their local PC.
7) Use malware to manipulate the hosts file on a victim›s PC that maintains local mappings between DNS names and IP addresses by inserting a fake DNS entry into it.

III. Spawning of Phishing

Phishing spawns through[12]:

Compromised Web servers

Vulnerable servers are scanned with a rootkit and a password protected backdoor is installed.

Port redirection

HTTP request to the compromised web server is re-routed to a remote one in a transparent manner, making the source content location harder to trace.

Botnets

It is a network of compromised computers that can be remotely controlled by an attacker.

Phishers frequently combine the three attacking techniques to provide redundancy and protect their phishing infrastructure by implementing a two-stage networking configuration. Phishers have been found to have a central web server hosting the physical phishing content to attack multiple sites at once and perform parallel mass scanning activity.

IV. Anti-phishing Techniques[4]

These can be categorized as server based and client based. The former are implemented by service providers which include:

1) *Brand Monitoring* in which phished pages are identified for adding to centralized black list.
2) *Behavior Detection* in which each user's profile is identified and used to detect user behavior anomalies.
3) *Security Event Monitoring and correlation* which is done to identify anomalous activity or post mortem analysis following an attack or a fraud.

The late use filters and content analysis at user's end point through browser plug-ins or from email clients.

V. Email giants' action against Phishing

Gmail

In August 2014, Gmail came up with a new tool which dealt with similar looking letters from the Unicode Consortium(UC) that could let spammers fool people. Scanners can exploit the fact that some characters look nearly identical (eg. □, o, and o look nearly identical to the letter 'o') and by mixing them, they can cheat unsuspecting victims. The UC lists such character combinations as «highly restricted.»

Yahoo

Yahoo! Provides few inbuilt anti-spam tools such as Spamguard which employs machine learning to constantly learn and improve filters that block spam and other malicious emails users don't want to see. The user, too, can contribute by clicking on the "Spam" or on "Not Spam" button accordingly. Image blocking is also another offering by Yahoo! which allows to block all images, no image, or only images in messages from contacts.

VI. Best practices for novice users

Users should always have a licensed antivirus and updated browser. Alongside, the users should:

Check the email address of the sender by hovering mouse cursor over the sender name and verifying.

2) Check whether the email was authenticated by the sending domain. The user should make sure the domain seen next to the 'mailed-by' or 'signed-by' lines matches the sender's email address.

Make sure the URL domain on the given page is

correct and click on any image and links to verify that it is directed to proper pages within the site.

Look for the closed lock icon in the status bar

when entering any private information.

Check the message headers. Fig. 1 shows how

one can do so in Yahoo! and Gmail. At Yahoo!, click on "More" and select "View Full Header" option. At Gmail, click on the arrow to the right of reply button and select "Show original" from the options.

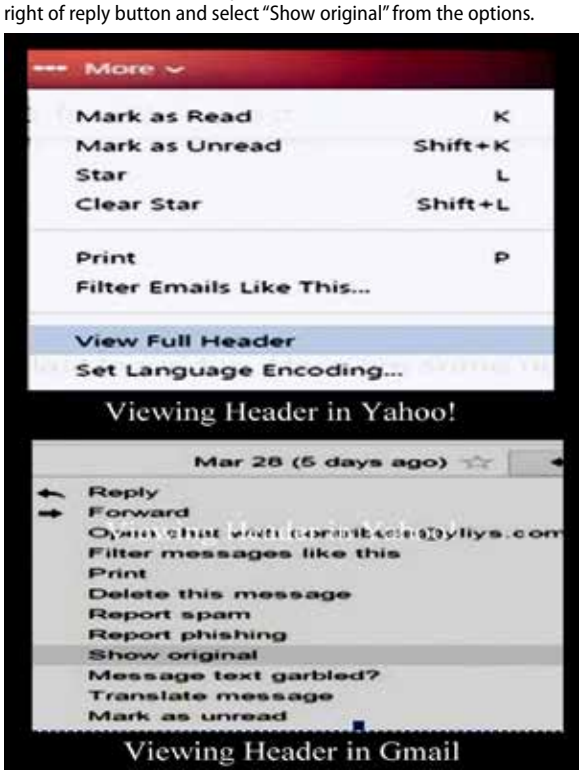

Fig. 1 View Header in Yahoo!/Gmail

If still uncertain, contact the organization from

which the message appears to be have been sent by visiting the official website of the concerned company.

If personal information has been entered in effect

of the phishing message, take quick action by reporting phishing. Fig. 2 demonstrates how to report phishing to Gmail or Yahoo!, for instance.

2FA-Two Factor Authentication for smartphones
Among the web mail service providers, only Gmail and the mailing client Outlook provides this service. It is a way to authenticate mailing account by linking the account to smart phone with the help of Duo Mobile app and then registering trusted devices. Whenever an attempt to login from an unrecognized device is made, a key sent to the registered mobile is asked for and in absence of it the login is disabled.

Fig. 2 Report Phishing to Yahoo!/Gmail

VII. Corporates and Anti-phishing
GFI MailEssentials
It protects email network against email-born viruses and other malware threats using advanced email filtering technologies and up to five antivirus scanning engines and captures spam 99%.

Symantec Online Fraud Management Solution
It offers a multi-pronged technology[10] with an email fraud detection, filtering, and alerting network, online user education against online frauds, free Desktop Security, online customer protection software and a consulting and Assessment Service with established policy.

C. Detect Safe Browsing Software
It gives mechanisms to safely access sites wished to visit by searching for malicious entries in the hosts file, and avoiding pharming attacks[10]. It also allows seeing a historical record of the suspicious activity found during the last 60 days.

VIII. Past experiences in Phishing handling
Below, we mention a few of the significant works that have been done to combat phishing.

SSL/TLS
The Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS), both rely on Public Key Infrastructure (PKI) which allows a mutual authentication of server and client.

PGP
It relies on third parties to sign public keys to attest that a public key belongs to a particular identity. The "web of trust" model relies on individual users to make trust judgments. This allows more flexibility in how authentication decisions are made, but requires a great deal of effort on the user's part to carefully manage keys and to understand the delegation of trust[15].

TRUSTBAR
It is a third party certification approach that requires website logos to be certified[14]. It is used to present credentials from the website, such as logos and icons that have been certified by trusted certificate authorities or by peers using a PGP web of trust.

PASSCODE
This program distributes RSA SecurID devices to AOL members. This device generates and displays a unique six-digit numeric code every 1 minute. To login to AOL website, the user enters his password and the code as a secondary password.

Passmark and Verified by Visa
The user provides the server with a shared secret, such as an image or passphrase along with his regular password. The server presents the user with this shared secret. The user has to recognize it before providing the server with his password.

Synchronized Random Dynamic Boundaries
It marked authenticated windows in the browser and uses a random number generator to set a bit that determines the frequency of border changes in the browser.

7) YURL
Here the browser maintains a mapping of a public key hash to a "petname". When user visits a page through YURL, the browser displays the petname associated with it. An untrusted site can be recognized by the absence of this petname.

VIII. Conclusions and Future work

The recent attacks by the phishes suggest their acquaintance with the changing scenario and knowledge about the latest trends of their target. Till date, no complete solution that mitigates online fraud has been devised. And on top of it with technological advancement, we are being victimized even more on the web. To combat it, a lot more of work is needed. We realize that along with the actions to combat phishing, the developers and users should realize the importance of their being aware of the dos and don'ts to avoid being tricked.

REFERENCES

Gupta. S, Kumaraguru. P(2014). "Emerging | Phishing Trends and Effectiveness of Phishing | Landing Page". arXiv.org, vol 1 [cs.CY]. | [2] Manasrah A., Melhiml L. B., and Anbar | M(2011). "An online model on evolving | phishing e-mail detection and classification | method". Journal of Applied Sciences, Vol 11, | Issue 18, Page No.: 3301-3307. | [3] Berghel H(2006). "Phishing Morngers and | Posers". Communications of the ACM. Vol. 49, | Issue 4, pp 21-25. | [4] Chhikara J., Dahiya R., Garg N., Rani M.(2013). | "Phishing and Anti Phishing Techniques: Case | Study". International Journal of Advanced | Research in Computer Science and Software | Engineering, Vol 3, Issue 5, pp 458-465. | [5] Parno B, Kuo C., Perrig A.(2006). "Phoolproof | Phishing Prevention". In Proceedings of the 10th | International Conference on Financial | cryptography and Data Security (FC'06), | Anguilla, British West Indies. Pp 1-19. | [6] Tally G., Thomas R., Vleck T.V.(2004). | "AntiPhishing: Best Practices for Institutions | and Consumers". McAfee Research, Technical | Report number 04-004. | [7] Easysol Solutions(2009). "Protection Against | Phishing and Pharming attacks". At | easysol.net/ | [8] Symantec Online Fraud Management. | "Mitigating Online Fraud: Customer | Confidence, Brand Protection, and Loss | Minimization". | [9] Watson D., Holz T., Mueller S. "Know you | enemy: phishing" on | honeynet.org/papers/phishing. | [10] Microsoft: Erroneous Verisign Issued Digital | Certificates Pose Spoofing Hazard. Technical | Report Microsoft Security Bulletin MS01-017 | (2001) | [11] Herzberg A., Gbara A(2004). "Protecting | (even) Naive Web Users, or Preventing | Spoofing and Establishing Credentials of | Websites". Technical Report Draft. | [12] Anti-Phishing Working Group, | antiphishing.org/. | [13] Pretty Good Privacy, pgp.com/. | [14] TRUSTe, truste.org/. | [15] Gmai, mail.google.com/. | [16] Yahoo. in.yahoo.com/. |