Journal of Advances in Science and Technology

Vol. IV, No. VIII, February-2013, ISSN 2230-9659

INTRODUCTION TO THE TYPES OF PHISHING ATTACKS

www.ignited.in

Journal of Advances in Science and Technology
Vol. IV, No. VIII, February-2013, ISSN 2230-9659

Introduction to the Types of Phishing Attacks

Nisha Ahuja[1] Dr. Shewata Rani[2]

[1]M. Tech Scholar, Punjab Technical University, Jalandhar, Punjab

[2]Supervisor

Abstract:- The most recent two decades of network security research have showed that attackers are consistently developing, investigating inventive courses to adventure frameworks, and focusing on new innovations and benefits as they rise. In reality, the widespread utilization of message carried spam and emailviruses; broadband connectivity was accompanied by the ascent of quick self-spreading worms; while the growing utilization of online particular administrations and electronic business came about in refined particular information robbery attacks, incorporating phishing. Such patterns infer that any engineering that achieves a basic mass will pull in the consideration of attackers.

----------♦----------

The Internet is assuming a progressively significant part in today's business and business exercises. Sadly, unfortunate security on the Internet and expansive financial additions furnish an in number cause for attackers to execute such clearly level hazard, yet high-return online tricks. In the year 2004 separated from everyone else, an expected 20 million phishing messages were conveyed, bringing about practically 10 billion dollars in harm . A large portion of the phishing attacks are done by sending substantial volume of unmistakably created messages posturing to start from a real business dominion. These messages are proposed for redirecting the beneficiaries to a disguised site, which shows the same conduct of a real realm, for deceiving the clients to uncover their financial qualified data. Despite the fact that spam filtering strategies could be utilized to battle phishing messages, these countermeasures are not by any means viable as there are an incomprehensible number of promptly accessible instruments that can detour both the factual what's more guideline based spam filters. Additionally, phishers can pick the message beneficiaries by means of social building components.

TYPES OF PHISHING ATTACK

Phishing is a particular type of spam that employs two techniques, deceptive phishing and malware-based phishing. The first technique is related to social engineering schemes, which depend on forged email claims that originate from a legitimate company or bank. Subsequently, through an embedded link within the email, the phisher attempts to redirect users to fake Web sites. These fake Web sites are designed to obtain financial data from victims fraudulently, including usernames, passwords, credit card numbers, or personal information. The second technique involves technical deception schemes that rely on malicious software programs spread through deceptive emails or by detecting and using security holes in the user's computer to obtain the victim's online account information directly. Sometimes, the phisher attempts to misdirect the user to a fake Web site or to a legitimate one monitored by proxies . The current study focuses on deceptive phishing using social engineering schemes. Figure explains the place of phishing email in phishing attack techniques.

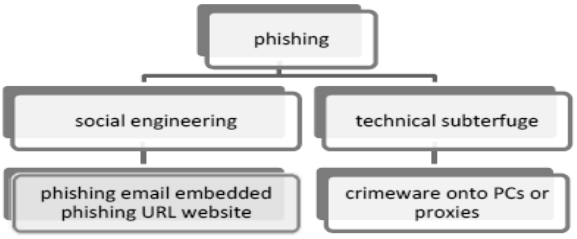

Figure: Types of Phishing Attacks

EVALUATION

We have carried out two experiments to evaluate the effectiveness of UBPD in terms of the two following rates:

	Alice	Bob	Carol	Dave
Reuse	No	No	Yes	Yes
Uniqueness	Strong	Weak	Strong	Weak

TABLE : CHARACTERISTICS OF USER PROFILE

- False negative: The system fails to recognise a phishing attack.

• False positive: The system recognises a legitimate website as a phishing website.

In addition we also search for a useful default threshold value. For both experiments UBPD was modified to not present the warning dialogue, instead it records the phishing score results as well as the URLs for later analysis.

False Negative Rate : From PhishTank and millersmiles we randomly collected 463 recently reported phishing webpages, which target Ebay, Paypal, and Natwest bank. We created four user profiles, which describe four artifical users' binding relationships with the three targeted websites. The four user profiles have different characteristics as shown in Table. 'Reuse' indicates maximum possible reuse of authentication credentials. In this case the user would have same user name and password for Ebay and Paypal. 'Uniqueness' indicates whether the user would use the exact data they shared with a legitimate website at other places. For example if Bob chooses his email address as password then the uniqueness is weak, because Bob is very likely to tell other websites his email address. If Bob uses some random string as his password, then the uniqueness is strong, because this random string is unlikely to be used with any other websites.

We entered the artifical authentication credentials to each phishing webpages. Regardless of the characteristics of the user profile, the detection result is the same for all four users: 459 pages had a phishing score of 1, and 4 had a phishing score of 0. Thus only four pages evaded detection – a 99.14 percent detection rate. Compared to other existing phishing website detection systems, UBPD's detection rate may not be significantly better. Its biggest advantage is that its detection method detects essential characteristics of a phishing attack, namely that phishing web pages request authentication credentials. The details of how users may be manipulated may change with future phishing attacks, but the requesting of such details remains constant. Other detection systems based on the analysis of incoming data will need to adapt and be redesigned for future phishing attacks; UBPD will not.

Detailed analysis confirms that the detection result is determined mainly by the information requested by the phishing webpage. Table shows the classification of the phishing webpages based on the type of information they requested. 92% of the collected phishing webpages asked only for authentication credentials and 7.14% of the collected phishing webpages asked both for personal and authentication credentials.

The four phishing site pages that UBPD neglected to distinguish requested from just individual informative data, for example full name, address, phone number and mother's last name by birth. Actually, they can't be identified by UBPD regardless of what the limit worth is. Then again, it is unrealistic for phishing attacks to request individual informative data without asking for verification qualifications first, since those phishing pages are definitely not introduced to clients when a client chump first lands at the phishing site. Those phishing sites would ordinarily first present the client with a login site page before steering the client to the page that soliciting the individual informative content (none of the four phishing website pages were the greeting page of the phishing attacks). Otherwise such practice might be appeared strange, make potential victimized individuals exceptionally suspicious.

Subsequently, UBPD can catch the phishing attacks and stop clients from indeed, arriving at the phishing website pages that require particular qualified data.

The example size in this examination is impressive and we may have some desire that this might be sensibly characteristic of triumph rate when conveyed 'in the wild'.

False Positive Rate : Five volunteers were furnished with the qualified information required to establish UBPD on their machine. We didn't explictly request that they prepare UBPD with all their coupling relationships, in light of the fact that we needed to perceive how clients might prepare UBPD and what the false positives might be actually if the client has not fittingly prepared UBPD. At the closure of one week, we gathered the consequence log from their machines.

The volunteers were three male and two female science learners. They all utilized Firefox as their essential web browser. They were all consistent Internet clients (in normal over three hours for every day). Therefore the UBPD was initiated a vast number of times and the collaborations that happened throughout the tests secured a wide run of sorts of cooperation.

A different excuse for why we picked those volunteers is on the grounds that they are the most improbable client assembly to fall schmucks to phishing attacks thus we can securely accept they have all cooperated with honest sites. In aggregate the volunteers cooperated with 76 unique sites, sumbitted information to those sites 2107 times, also UBPD ran in location mode just 81 times. Actually all the sites volunteers went to were authentic. On 59 events the phishing score was 0, on five communications gave a score of 0.25, on 13 events the score was 0.5, and the score was 1 on three events.

The phishing score was 1 when clients communicated with three honest to goodness sites (the enrollment pages of videojug.com furthermore surveys.com, and the verification site page of a web discussion). We asked the volunteers what information they supplied to those pages. It appears that the reuse of verification certifications on making

new records is the explanation for why. In this trial, the cautioning dialog is not displayed, as we did not expect to test ease of use. In any case assuming that it does, then the client must settle on choice to prepare UBPD to recall these new tying relationships. To evade the client's perplexity about what is the right decision when the cautioning dialog is introduced, the dialog continuously helps the client to remember the genuine sites UBPD is mindful of, and tells the client that if the client is certain the present site is genuine, and the site is not recollected by UBPD, then they have to overhaul their coupling relationships. This requires no specialized information and ought to be truly simple to comprehend. There are just two decisions gave by the dialog: to overhaul the profile what's more submit the information; or donot send the client submitted information and shut the phishing site page. There is no third decision furnished by the dialog, thusly we drive the client to make the security choice and they can't just disregard the warnings given by the framework.

EMAIL PHISHING

In Email phishing, the attacker sends a fake email which looks like an email from a legitimate source. The email usually contains a link which when clicked on, directs the victim to a fake website whose look and feel are almost identical to the real website. This fake website is used to obtain sensitive information such as user names, passwords, or credit card numbers from the victim. This laboratory exercise is designed to demonstrate how email phishing can be carried out by sending a fake email, and embedding a fake hyperlink in the email. In this laboratory exercise, the victim will not be asked to input sensitive information at the fake website to avoid ethical issues. The detailed laboratory exercise procedure is described below.

There are several ways to send out a fake email: (1) Utilize the services provided by some websites ; (2) Use Microsoft Outlook to send a fake email; (3) Send a fake email through SMTP server using Telnet. Procedures of using the first two methods to carry out phishing are described below.

Sending fake email using a website :

- Go to a website that allows you to send a fake email, for example, www.deadfake.com.
- A form that includes “To:”, “From: ”, “Subject:” and “Message:” fields appears so you can enter information to send a fake email.
- Type in a fake email address in the “From” field. Make sure that the domain name is real. For example, type in jdoe@microsoft.com instead of jdoe@micosoft.com.
- Type in a valid email address (the receiver email address) in the “To” field.
- Enter in a subject in the “Subject” field.
- In the “Message” field, type in the message you want to send to the receiver. To embed a fake link, type a valid URL, for example, www.yahoo.com. Highlight the URL and click on the hyperlink icon. A dialog box will appear to allow you to enter in the actual URL. Enter in www.google.com. This will make the receiver think that he is going to Yahoo.com when he is actually going to Google.com when he clicks on the link.
- Click “Send” to send out the email.

Sending fake email using Outlook 2007 :

- Open Outlook 2007 and click on Tools, then Account Settings.
- Under the Email tab, click on “New” and a new email account window should pop up.
- Select the “Microsoft Exchange, POP3, IMAP, or HTTP” option and click on Next.
- Select the “Manually configure server settings” option at the bottom and click on Next.
- Select “Internet Email” and click on Next.
- On the Internet setting page, enter in a fake name and a fake email address under User Information. Under Server Information, choose POP3 or IMAP as Account Type, input any domain name for Incoming mail server. It does not matter since we are not trying to receive email. For the “Outgoing Mail Server” text box, input your ISP SMTP server (i.e. smtp.earthlink.com) or 127.0.0.1 if you’re able to use your own SMTP server.
- Click on “More Settings”, then click on the “Advanced” tab and make sure the outgoing server is using port 25. Click on OK. Once you get back to the Internet Email Settings window, click on Next, then Finish to complete the setup.
- Click on File, then New, then Mail Message to start composing a new email.
- Click on the Account button and select the fake email account. The account button only show up when you have multiple accounts
- Enter in a valid email of the receiver and a subject.

- Enter in the message you want to send to the receiver. To embed a fake link, click on the Insert tab at the top and then select “Hyperlink”, a dialog box will pop up.

- In the “Text to display” field on the top, enter in www.yahoo.com. In the “Address” field at the bottom of the dialog box, enter in www.google.com. Press OK. This means that when the receiver of the email clicks on the link www.yahoo.com, he goes to google.com instead.

- Click on Send to send the email.

REFERENCES

• Haddad04 Haddad, Ibrahim and Gordon, David. "The Basics of DNSSEC" ONLamp.com, O'Reilly, October 14, 2006.

• Tzanidakis06 Tzanidakis, Manolis. "Creating a sSecure Linux-based Wireless Access Point" Linux.com. July 19, 2006.

• Egilsson07 Egilsson, Einar. "Redirector :: Firefox Add-ons" Mozilla Software Foundation. October 5, 2007.

• N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell. Client-side defense against web-based identity theft. In NDSS, 2004.

• R. Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In SOUPS ’05: Proceedings of the 2005 symposium on Usable privacy and security, pages 77– 88, New York, NY, USA, 2005. ACM Press.

• M. Jakobsson. Modeling and preventing phishing attacks. In Phishing Panel of Financial Crytography, 2005.

• S. H. Ben Adida and R. Rivest. Fighting phishing attacks: A lightweight trust architecture for detecting spoofed emails. Feb 2005.

• W. A. Arbaugh, N. Shankar, and Y. J.Wan. Your 802.11 wireless network has no clothes. In IEEEWireless Communications, 2001.

• P. Bahl and V. N. Padmanabhan. RADAR: An in-building RFbased user location and tracking system. In Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pages 775–784, 2000.

• M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. The Internet Motion Sensor: A Distributed Blackhole Monitoring System. In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS), pages 167–179, February 2005.

• R. Beverly and S. Bauer. The spoofer project: Inferring the extent of source address filtering on the internet. In Proceedings of USENIX Steps to Reducing Unwanted Traffic on the Internet (SRUTI) Workshop, pages 53–59, July 2005.

• R. A. Beyah, C. L. Corbett, and J. A. Copeland. The case for collaborative distributed wireless intrusion detection systems. In IEEE International Conference on Granular Computing, May 2006.

• Bittau, M. Handley, and J. Lackey. The final nail in wep’s coffin. In SP ’06: Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P’06), pages 386–400, Washington, DC, USA, 2006. IEEE Computer Society.

• D. P. Blinn, T. Henderson, and D. Kotz. Analysis of a Wi-Fi hotspot network. In Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling, June 2005.

• N. Borisov, I. Goldberg, and D.Wagner. Intercepting mobile communications: The insecurity of 802.11. In Proceedings of ACM Mobicom, Rome, Italy, July 2001.

• S. Byers, L. F. Cranor, D. P. Kormann, and P. D. McDaniel. Searching for privacy: Design and implementation of a P2Penabled search engine. In D. Martin and A. Serjantov, editors, Privacy Enhancing Technologies, volume 3424 of Lecture Notes in Computer Science, pages 314–328. Springer, 2004.

• J. Cache and D.Maynor. Device drivers. Presentation at Blackhat USA 2006, August 2006.

• R. G. Cole, N. Phamdo, M. A. Rajab, and A. Terzis. Requirements on worm mitigation technologies in MANETS. In PADS ’05: Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, pages 207–214, Washington, DC, USA, 2005. IEEE Computer Society.

• G. Portokalidis, A. Slowinska, and H. Bos. Argos: an emulator for fingerprinting zero-day attacks. In Proc. ACM SIGOPS

• EUROSYS’2006, Leuven, Belgium, April 2006.

• Shannon and D. Moore. The Spread of the Witty Worm. IEEE Security & Privacy, 2(4):46–50, July/August 2004.