University of Southampton

Msc Cyber Security

Cyber Crime, Insecurity and the Dark Web

Criminology in the future: Horizon Scanning.

Increased web exposure of society is empowering phishing

Author:
Gerard Tio Nogueras

April 30, 2017

1 Introduction

We are going to show the reason companies and individuals should consider spear phishing very carefully and show its rise in our age due to social behaviour. We will start by introducing the relevance of spear phishing in current times by explaining its dangers and the strategies they use. We will follow with the high utility of spear phishing for criminal organisations and the enhancement of spear phishing due to the current behaviour of our society. Our third argument will discuss the future factors that will influence spear phishing. Finally, we will end with ongoing research for countermeasures and personal thoughts on the subject.
Let us start with some definitions and famous examples to validate the importance of the subject.

1.1 Definitions

Phishing: "phishing is a scalable act of deception whereby impersonation is used to obtain information from a target" [1]
Spear phishing: "Phishing attempts directed at specific individuals or companies have been termed spear phishing". The attackers start by gathering as much information from public sources (public registries, social networks, blogs, ...) or from private sources (obtained from previous attacks. Then he will forge a personalised phishing email targeting the victim.[2, 3]
Social engineering: Kevin Mitnick explains in his book that the weakest link in any security system is the person holding the information. Therefore tricking these persons is the key to everything. [4, 5]
Whaling: "Whaling is a type of fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities." "In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company."[6, 7]
Malware: "Short for "malicious software". The effect of malware is to cause something unexpected [...]on your computer.(disrupt computer operation, collect sensitive information, access a private computer system, ...)" [8]

1.2 Famous Examples

To introduce you to the world of phishing here are some famous examples of spear phishing:

- RSA: In 2011, RSA Security firm was targeted by 2 waves of phishing attacks targeting 4 of their employees. These crafted emails were so credible, that one of the employees took it out of his junk box and clicked on a malicious link, giving the attackers full access to the company's network. [9]
- Ubiquity networks: In 2015, employees were tricked into transferring $46.7 million to accounts held by third parties. This was achieved through impersonation of the finance department by creating fake requests from executives thanks to spoofed e-mail addresses and look-alike domains.[9]
- Oak Ridge National Laboratory: In 2011, the lab got targeted by a massive spear phishing attack to 10% of their 5000 employees, faking to be the HR department. 10% of these opened the mail and clicked on the malicious link and unfortunately, 2 computer were not protected properly against these malwares and the attackers used these doors to steal a huge amount of data.[10]
- APT1: APTs are high-level cyber attacks which have as objective to stay in network for long periods of time and steal data continuously. These attacks have the characteristic to start with waves of spear phishing to middle level targets and get a foothold in the companies from there.[11, 12]
- Whaling for political objectives: Using the APT cycle[11] combined with high-level spear phishing targeting politicians during the elections, we gain access to a lot of advantageous information, this is what happened in Hong Kong in 2010. [13]

These examples are here to show how a simple mistake from one employee can compromise entire networks and how wide the range of targets can be.

2 Body

Now that we have introduced the subject, let us dive into the real interest of this essay: current and future social factors influencing spear phishing.

2.1 The power of spear phishing

My first argument will target the reason spear phishing deserves more attention.

Researchers did a study on the effectiveness of spear phishing[19] on users under different conditions by creating 3 types of emails: spam, genuine and spear phishing emails; using 4 types of social engineering approaches: authority(CEO), scarcity(limited by a factor like time or amount), social proof(action already taken by peers) and no strategy; and under different pressure situations. The results showed a high rate of failure when having to detect spear phishing emails in general. The most effective social engineering technique was the authority where the participants were unable to reliably distinguish between spear phishing emails and genuine ones. These results are scary considering the rise of spear phishing because "it doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organisation has if the person behind the keyboard falls for a phish."[16]

2.2 Spear phishing for Criminal organisations

My second argument will target the interest of criminal organisations for this type of schemes.

Since the arrival of organised crime(OC) in the cyber space, we have seen 3 types of trends: Data stealing, transaction-based crimes and actual workings of the internet.[21]
The idea of the acts is always monetization, maximising profit with efficiency. The method that seems to be the most profitable is social engineering because this method is cheap, easy, very effective and allows for a lot of possibilities after a successful entry such as data theft, malware deployment, and a foothold in companies for future attacks. Many of the OC groups have been involved in numerous spear phishing attacks combined with whaling attacks as prime social engineering attacks. Additionally, a tendency for the development of human-based

social engineering is noted because it works in many cases where technological methods fail.
Social networks have changed the game for spear phishing. Social networks, instant messaging and any application involving personal data have become targets for attackers since they directly allow for some type of monetization, but especially because they allow for this types of powerful attacks that are social engineering attacks through the internet: spear phishing. [16, 17]

2.3 Future factors

Finally, my third argument will explain how current society enhances this types of attacks and if any changes are to be expected in the future.
The factors that are expected to influence the future of spear phishing are the following:

- Botnets: One thing is sure is that there will be a widespread use of botnets. Botnets will become more financially driven by attacking all types of digital devices(especially phones which are very unprotected) capturing more data for more sophisticated spear phishing attacks.[21, 15]

- Awareness: As I will go in the counter measures as well, companies are realising that training will be essential. Unfortunately will training be enough against attacks that are going to become more and more tailored?

- Social networks: Privacy rules, encryption, security of all applications with private data will improve, but will the users make use of it? Update their software, update their privacy policies? Training at a younger age will probably be needed to start implementing this for everyone in the future generations.

"Organised criminal activity in cybercrime is predicted to grow and will affect the financial security of online business and cause widespread social harm"[21]
To fight this growing activity we will require a combination of technology and relevant, up-to-date laws and policies as well as the constant reformulation of crime prevention practices. This will require effective partnerships between the state, private actors and multilateral groupings of states, corporations and consumer

groups. Luckily law enforcement, academia and industry are getting better organised (attack reports, information sharing, trends analysing) and there is hope for the future.[16, 21]

3 Conclusion

I will use this space not to sum up my arguments but to hopefully help the readers improve their capacity to protect against these attacks and protect their companies against them.

3.1 Countermeasures

In the field of research there are 2 main topics to counter spear phishing[16, 14, 18]:

- Training: make your employees and the society aware of these types of attacks, and train them to recognise them through games, exercises, presentations, ...
  Some go a bit further and try to create a training that answers today's needs: low cost, pinch the interest of participants and have a high effectiveness[20]

- Make it invisible: If the users can not see the crafted emails, they are protected, therefore there is a lot of research into creating advanced systems of filtering using machine learning and smart recognition of suspicious links to stop them before reaching the user.

"Spear phishing [...] will require equally targeted education and crime prevention efforts"[21]

3.2 Personal thoughts

I am scared. Scared of becoming paranoiac. Because I have already tried my whole life to minimise my web presence but it is almost inevitable. And even if you are almost not present there are high probabilities that someone you are close to in your group of friends, family or work is. One of the reasons I have taken Cyber Security courses is to help our world against this type of attacks by creating a

bigger community of cyber Security and spread knowledge and awareness. Because I think this is the way we will keep our evolving world safe.

References

[1] Lastdrager, E. (2017). Achieving a consensual definition of phishing based on a systematic review of the literature. [online] Available at: https://crimesciencejournal.springeropen.com/articles/10.1186/s40163-014-0009-y [Accessed 19 Mar. 2017].

[2] Fr.wikipedia.org. (2016). Spear phishing. [online] Available at: https://fr.wikipedia.org/wiki/Spear_phishing [Accessed 19 Mar. 2017].

[3] En.wikipedia.org. (2017). Phishing. [online] Available at: https://en.wikipedia.org/wiki/Phishing#Spear_phishing [Accessed 19 Mar. 2017].

[4] Mitnick, K., Simon, W. and Wozniak, S. (2013). The art of deception. Hoboken, N.J.: Wiley.

[5] Mitnick, K., and Simon, W. 2002. The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: Wiley.

[6] Rouse, M. (2014). What is whaling? [online] SearchSecurity. Available at: http://searchsecurity.techtarget.com/definition/whaling [Accessed 19 Mar. 2017].

[7] En.wikipedia.org. (2017). Phishing. [online] Available at: https://en.wikipedia.org/wiki/Phishing#Whaling [Accessed 19 Mar. 2017].

[8] Ed Zaluska, Implementing Cybersecurity - COMP6230. Slides: Malware 1-2.

[9] Brecht, D. (2016). Spear Phishing: Real Life Examples. [online] InfoSec Resources. Available at: http://resources.infosecinstitute.com/spear-phishing-real-life-examples/#gref [Accessed 19 Mar. 2017].

[10] Zetter, K. (2015). Hacker Lexicon: What Is Phishing?. [online] WIRED. Available at: https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ [Accessed 19 Mar. 2017].

[11] Mandiant report, APT1 Exposing One of China's Cyber Espionage Units.2013. Available at https://www.fireeye.com/content/dam/

fireeye-www/services/pdfs/mandiant-apt1-report.pdf [Accessed 19 Mar. 2017].

[12] Techopedia.com. (2017). What is an Advanced Persistent Threat (APT)?. [online] Available at: https://www.techopedia.com/definition/28118/advanced-persistent-threat-apt [Accessed 19 Mar. 2017].

[13] Li, F., Lai, A. and Ddl, D. (2011). Evidence of Advanced Persistent Threat: A case study of malware for political espionage - IEEE Xplore Document. [online] Ieeexplore.ieee.org. Available at: http://ieeexplore.ieee.org/abstract/document/6112333/ [Accessed 19 Mar. 2017].

[14] Bull, D. (2015). The Past, Present, and Future of Phishing and Malware. [online] Available at: https://securingtomorrow.mcafee.com/business/security-connected/past-present-and-future-of-phishing/ [Accessed 19 Mar. 2017].

[15] Roderic Broadhurst and Mamoun Alazab, Spam and Crime, Social engineering and spear phishing. [Online] Available at: http://press-files.anu.edu.au/downloads/press/n2304/pdf/ch30.pdf [Accessed 19 Mar. 2017]

[16] Jason Hong. 2012. The state of phishing attacks. Commun. ACM 55, 1 (January 2012), 74-81. Available at DOI: http://dx.doi.org/10.1145/2063176.2063197 [Accessed 19 Mar. 2017]

[17] Nagy, J. and Pecho, P. (2009). Social Networks Security - IEEE Xplore Document. [online] Ieeexplore.ieee.org. Available at: http://ieeexplore.ieee.org/abstract/document/5210996/ [Accessed 19 Mar. 2017].

[18] Laszka, A., Vorobeychik, Y. and Koutsouko, X. (2015). Optimal Personalized Filtering Against Spear-Phishing Attacks. [online] Available at: http://www.vuse.vanderbilt.edu/~koutsoxd/www/Publications/laszka2015optimal.pdf [Accessed 19 Mar. 2017].

[19] Butavicius et al.2015. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. Australasian Conference on Information Systems. Available at arxiv: https://arxiv.org/ftp/arxiv/papers/1606/1606.00887.pdf [Accessed 19 Mar. 2017]

[20] Schuetz, Sebastian and Lowry, Paul Benjamin and Thatcher, Jason, Defending Against Spear-Phishing: Motivating Users Through Fear Appeal Manipulations (June 27, 2016). 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June 27July 1. Available at SSRN: https://ssrn.com/abstract=2861410 [Accessed 19 Mar. 2017]

[21] Pakistan Society of Criminology. Future Trends in Cybercrime and the Role of Organized Crime. Pakistan Journal of Criminolgy Volume 2, No. 4, October, 2010. Available at http://pjcriminology.com/assets/downloads/PJCVol2No4Oct2010.pdf [Accessed 19 Mar. 2017]

[22] Mamoun Alazab and Roderic Broadhurst, Spam and criminal activity, N. 526 December 2016, Trends and issues in crime and criminal justice, Australian Institute of Criminology, Australian government. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467423 [Accessed 19 Mar. 2017]