Spear Phishing - The New Face of Phishing

Sudhir Shashidhar, Research Fellow, IIT Kanpur

Abstract

Over the last ten years, spear phishing was used mainly by espionage groups sponsored by different world states to delude high-ranking people by deceiving them to disclose specific information precious to the attackers. But recently, their strategy has changed and specialists wondered why they troubled to "spread crypto ransomware or banking trojans to the masses when a single scam e-mail could do the trick?" (Godin, 2016) This article investigates the answers to this question, the main ingredients that turn a cyber attack into a successful spear phishing and some protective ways against this sweeping wave of cybercrimes.

Phishing vs. spear phishing

A traditional phishing email usually appears like a serious warning message sent by a legitimate organization, such as a bank or a commercial institution, to customers about their account that seems to have been compromised. People are tricked to provide their personal information via email or SMS and the defendant uses them especially for financial purposes. This is considered to be the least complicated version of identity fraud, but more sophisticated ways are the new fashion today.

One of them is the presence of malicious attachments that make people download and install malware on their computers, leading to confidential information being stolen and sent to unknown destinations. Also there are links that direct people to fake websites, which are perfect replications of the real ones. This is another misleading and intricate way to get personal details and then keep the victim as long as possible unaware of the fraud. (Clough, 2012, p. 193)

The spear phishing attacks are very difficult to detect, but very easy to succeed. Once the victim opened or downloaded an apparently innocent file attachment, the malware is installed immediately and it opens the access of a malicious remote user to the compromised device.

What differentiates spear phishing from other regular phishing attacks is the fact that it is directed to carefully selected individuals, like those who may represent the weakest link in the security system. But this requires a lot of research, investing time and money, figuring out numbers, names and personal details, having a perfect knowledge of that person's social

environment. This is the job of elite hackers, as the common hackers hate intricate attacks. However, these forms of phishing are the most costly.

The last two years revealed an increased number of incidents known as "CEO email scams". Assuming the identity of leading people in a company, the perpetrators send emails to other employees requesting for sensitive information, payments approval, wire transfers, etc. The target employees are those working in human resources, security and financial departments. "It's not a new tactic, but it is one that is becoming increasingly popular; according to the FBI, businesses have racked up more than $2.3 billion in losses to targeted phishing attacks since 2013" (Barber, 2016).

Main ingredients

The reason of using spear phishing instead of ordinary phishing attacks is that most targeted people are working in domains like business and government, where downloading from the Internet is not an in-site accepted habit. So that, an email coming from an executive is more credible and has more chances to get the desired answer. Using someone's information as a bait, the perpetrators get access to case sensitive information, but also to all the contacts that person has ever had.

The research paper published By Trend Micro in 2012, *Spear-Phishing Email: Most Favored APT Attack Bait* revealed that the most common file types attached to an email are disguised as either .ZIP or .RAR documents, because .EXE are usually detected by security systems and they seem dubious even to the recipient. The statistics show that more than 90% are file attachments, while the most common alternative is tempting the victim to open links and download malicious files from there.

Information availability is another major ingredient, because it facilitates access to insiders and their personal details. In his two studies on cybercriminals organizations, Richet report that this could be a major reason behind so many spear phishing attacks directed to government, activist groups and financial industries. The more information shared on their websites, the more attacks directed to them (Richet, 2013). Another major flaw that helps phishers is that millions of personal information and connections are placed under the control of one single organization, like in the case of the Internet marketing company Epsilon. Its server breach in 2011 exposed users' personal information, their online shopping habits, their relationships with different organizations and so on. Moreover, the attack is not only context-aware but also is capable of extrapolating for information that the phishers don't yet have (Richet, 2012).

Called *collaborative spear phishing* in Shashidhar and Chen's study (2015), this effect is analyzed from the perspective of success probability of a phishing attempt. The authors proposed some metrics and the Steganography security model to evaluate the success of a phishing attack,

but also the phishing detection algorithms. Consequently, they discovered that the collaborative spear phishing is by far the most successful and subversive way, because hackers use collaborative filtering to gain access not only to personal information, but also "potential accounts that an individual may have with organizations using information that he already possesses" (Shashidhar and Chen, 2015, p.20).

Prevention and protection

The most common way recommended by specialists is the user education. Barber (2016) informs companies that there are some evident signs that indicate an email could be a spear phishing attack. When the greeting is different from the usual one, the tone of writing is very formal and out of place, the request addressed to the recipient seems weird and inconsistent with the hierarchical structure of the company, then it is highly recommended that the receiver of that suspicious email should ask for more directions.

Besides that, another typical yet more strategic defense is the filtering of malicious emails. If the filtering threshold is set too high, non-malicious emails could also be removed; if the threshold is too loose, then "different users have different levels of carefulness and different potential to cause damage." (Laszka, Vorobeychik and Koutsoukos, 2015, p.1) and it could result in surprising and unexpected breaches.

Starting from the assumption that any organization has an email classifier that scores the level of maliciousness, this study introduces two factors: *false negatives* ("when a malicious email is below the threshold") and *false positives* ("when a non-malicious email is above the threshold") (Laska et al., 2015, p.2). Using these two referential concepts, the authors propose a personalized filtering threshold modeled as a Stackelberg game, where the company is able to adjust the threshold accordingly and to find an optimal defense strategy. From their perspective, the attacker's best response is worthless compared to the challenging struggle to find the defender's best strategy.

In a subsequent study published in 2016, the same authors applied the model mentioned above on strategic thresholds and found out a coordination problem between different independent users and the externalities they could impose upon one another. These interdependent security problems were scarcely addressed in other studies, but they are very significant due to the resulting effect: "filtering decisions by some may result in others being targeted" (Laszka, Lou, Vorobeychik, 2016, p.1).

Laszka et al. (2016) took into account both malicious non-targeted emails (spam and phishing) and malicious targeted emails (spear phishing). The authors were concerned about the strategic dynamics of email filtering thresholds on short-term and long-term processes. They used *Stackerlberg multi-defender equilibrium* concept for the short-term analysis and the *Nash equilibrium* concept for the long-term. One remarkable thing they found while applying these

equilibria was that they are socially optimal. In other words, although the users act selfishly when making decisions and even if the attacker always offers the best response, the strategies used are still able to minimize the damages and losses.

Conclusion

Spear phishing is here to stay for a long time, because it is the most favorite vector for targeted cyber attacks. As long as the users continue to fall prey to them and the phishers continue to be difficult to spot, this will be the major game of those elite hackers who love to exploit the weak links in a security system. Finally, while email filters and strategic thresholds add layer after layer of protection against cybercrimes, it is pointless to ask the *if* question. Rather, the most appropriate questions that filtering technology tries to answer are *when* and *how*.

References

Barber, Richard (2016), Modern Spear Phishing is a Security Wake-Up Call. Retrieved April 26, 2016, from http://ww2.cfo.com/cyber-security-technology/2016/04/modern-spear-phishing-security-wake-call/

Clough, Jonathan (2012), *Principles of Cybercrime.* doi: http://dx.doi.org/10.1017/CBO9780511845123

Godin, Dan (2016), Crypto ransomware targets called by name in spear-phishing blast: Once the domain of espionage, personalized scams embraced by profit-driven scammers. *Ars Technica.* Retrieved April 26, 2016 from http://arstechnica.com

Laszka, Aron, Vorobeychik, Yevgeniy & Koutsoukos, Xenofon (2015), Optimal Personalized Filtering Against Spear-Phishing Attacks. *Association for the Advancement of Artificial Intelligence* (www.aaai.org). Retrieved April 26 2016 from http://www.vuse.vanderbilt.edu/~koutsoxd/www/Publications/laszka2015optimal.pdf

Laszka, Aron, Lou, Jian & Vorobeychik, Yevgeniy (2016), Multi-Defender Strategic Filtering Against Spear-Phishing Attacks. *Association for the Advancement of Artificial Intelligence* (www.aaai.org). Retrieved April 26, 2016 from http://aronlaszka.com/papers/laszka2016multi.pdf

Richet, J. L., & Telecom, E. M. (2012). How to Become a Black Hat Hacker an Exploratory Study of Barriers to Entry into Cybercrime. In *17th AIM Symposium*.

Richet, J. L. (2013). From Young Hackers to Crackers. *International Journal of Technology and Human Interaction (IJTHI)*, *9*(3), 53-62.

Shashidhar, Narasimha & Chen, Lei (2015), An Indistinguishability Model for Evaluating Diverse Classes of Phishing Attacks and Quantifying Attack Efficacy, *International Journal of Security* (IJS), 9 (2), 15-23

Trend Micro (2016). Spear-Phishing Email: Most Favored APT Attack Bait. Retrieved April 26, 2016 from http://www.trendmicro.com/