Bringing the Fight to Them

Exploring Aggressive Countermeasures to Phishing and other Social Engineering Scams

---

Allen Zhou

Comp116 Final Paper

Abstract

Phishing is the illicit practice of using social engineering to steal credentials or money from Internet users, or as a gateway to infect the victim's machine with malware [1]. The general approach to phishing and other social engineering scams has been essentially reactionary, built on educating users to avoid scams or constructing systems to filter out phishing messages, rather than actively fighting those who perpetrate the attacks. However, starting in the early 2000's, niche communities of Scambaiters supplied an alternative and more active approach to disrupting *419* phishing schemes. Scambaiters are individuals who intentionally engage in contact with phishers and online scammers in order to waste their time and resources [2]. However, as phishing schemes today become increasingly intelligent, targeted, and damaging, it is important to explore more aggressive approaches to combating phishing, techniques akin to scambaiting. This paper will begin by delving into a brief history of phishing. We will then look into how phishing has evolved in the modern day, taking advantage of machine learning tools used in conjunction with social platforms. Finally, we will explore today's research in aggressive approaches for fighting traditional phishing, and urge more development in how we combat phishing on social media platforms.

Introduction

The term "phishing" was first coined in 1992 when malicious actors using AOL began posing as system administrators, asking the users of the service to confirm billing information or account details [3]. Soon, with the rise of email and other networks of mass distribution, phishing attacks grew exponentially [1]. Early phishing scams were often identifiable through their poor grammar, shoddily built websites, and terrifyingly urgent subject matters (Your Bank Account

Has Been Compromised!) Perhaps the most famous of the early phishing attacks is the Nigerian 419 scam, which take its name from the section of the Nigerian Criminal Code that outlaws it [4]. These scams usually arrives as an out-of-the-blue email from some overseas individual, seeking help to transfer money out of their country. They promise the receiver of the email a hefty reward if followed through with, and all they have to do is pay a "trusted" organization a small amount in order to secure the success of the transfer. Though these *419* schemes still live on, buried in our email's spam folders, these older phishing techniques have been largely superseded by a host of more cunning and destructive tactics. Clone phishing replicates a previously sent legitimate email that holds either a link or some file attachment, and replaces the payload with some malicious content, while claiming that it is an updated version of the previous email. Spear-phishing takes advantage of information gathered about a victim to craft phishing schemes specifically for a target. Whaling is one form of Spear-phishing that is directed at especially high profile targets who have access to valuable data, like an administrator or business executive [3].

To the Community

When I refer to today's response to phishing attacks as "reactionary," I am referring to the general practices of advising internet users to not click on unsolicited links and to not provide sensitive information to entities that they are not 100% sure are legitimate. This is all reliant on the victim's own intuition being the last line of defense. Phishing represents a billion dollar criminal industry that is built on exploiting the average internet user's lack of security knowledge [1]. Thus, it is important to consider whether the general reactionary approach to phishing is appropriate for today's complex and dangerous Internet. This paper will weigh the viability of

more active approaches to combating phishing, as well as discuss the ethicacy of aggressive approaches that can be considered hacking back.

Modern Day Phishing

Phishing has gradually become more and more sophisticated over the years. Many schemes are no longer based on simply blasting a generic email at as many users as possible and hoping for one victim out of a million targets. Instead, hackers are developing phishing techniques that are contextually aware in order to improve click-through rates, and thus increase the revenue of these scams. Even more alarming, by using machine learning technology, hackers have made their Spear-phishing scalable, meaning the attacks will have the large scale nature of broad phishing attacks, with the precision of Spear-phishing.

In research performed by John Seymour and Philip Tully, they showed through an automated phishing prototype they call *SNAP_R* how machine learning and social engineering can be combined to create customized phishing messages for susceptible targets on Twitter [5]. First, the model is able to discover targets by pulling from the Twitter API and determining which users are high value and likely to fall for a phishing scam. It then uses a combination of Markov models and Long Short-Term Memory neural networks in order to generate a tweet with a malicious link that the user would likely be interested in. *SNAP_R* also has the wherewithal to send the tweet when the target is most likely to be active on Twitter. Seymour and Tully found that this model more than doubled the success rates of large-scale phishing attacks, and was comparable to manual spear-phishing campaigns. Since we know that similar models are already deployed and are performing these attacks today, this shows that phishing is becoming more of a

problem on today's Internet, and that being cautious on traditional phishing platforms like email is not enough.

Advanced Scambaiting

As the success rates and severity of phishing attacks rise, so to has the methods of fighting it. What we can call "advanced Scambaiting" begins to step away from the playfulness of simply wasting the phishers time, to actually actively attacking the phisher, and is more along the lines of what security researchers call "hacking back." As early as 2008, reports of a social engineering scam known as the tech support scam began cropping up in the United States [6]. These scams typically see a scammer cold calling a victim, informing them that they work at Windows or Microsoft, that their computer is vulnerable, and that it can be fixed if given remote access. Of course, when given remote access, they will install keyloggers, malware, backdoors, or direct the victim to a fake site, where they will be asked to enter their credentials [6]. To fight back, some take advantage of an exploit in Ammyy Admin, a remote desktop software that scammers often use [7]. The exploit is available as a module on metasploit and allows arbitrary code to be ran on the scammer's computer once the Ammyy Admin connection has been established [8].

From an ethical and legal perspective, hacking back as a general practice is dangerous and illegal. In October of 2017, Georgia Congressman Tom Graves introduced the Active Cyber Defense Certainty Act (AC/DC Act) which would allow victims of cyber attacks to execute vigilante justice, which would likely include the use of the Ammyy Admin exploit [9]. If legalized, it is not hard to imagine how the lines for what constitutes a cyberattack and what counts as reasonable retribution becoming blurred. Furthermore, in scenarios where a botnet is

being used, we run into the attribution problem where a hack back might hurt some other innocent party, and not the hacker themselves. The AC/DC act was not passed, but this does provide a reminder that when proposing aggressive solutions to phishing, they must still operate ethically.

Action Items

In order to both ethically and effectively combat phishing aggressively, we can begin by looking at a solution proposed by Robbie Gallagher at ShmooCon 2016 called Honey-Phish [10]. Inspired by old-school Scambaiters, Honey-Phish works by automating replies to phishing emails, and contain a message and then a URL to Gallagher's own phishing website. If clicked on, the website logs as much information about the phisher as possible, including IP, operating system, and web browser, and reports it back to Honey-Phish [11]. The messages themselves are constructed using a Markov Chain, inputted with text from Reddit's financial forums, making the generated emails a convincing reply. Although Gallagher's implementation of Honey-Phish ends here as a data aggregation tool, it is a small jump to use this as a tool to mark IP's for possible criminal activity, and given enough evidence, blacklist the IP or use it track down the source of the attacks. Another model proposed by John Brozycki called Phish Feeding is incredibly reminiscent of Scambaiting in that it is based on intentionally interacting with the scammer. The idea is that once a phishing website is found, saturate its results and thereby its profit by pumping it full of realistic looking, but fake credentials and information [12]. There are a number of benefits to doing this: the value of the real data is decreased, the phisher is wastes their time with fake data, and there is more time to try and shut down the site. Additionally, "honey tokens" can

also be submitted, which can be later tracked and help law enforcement find the perpetrator of the phishing attack [13].

Besides the development of the honey pot and phish feeding solutions, we should also look to obstruct access to the tools that allow phishing to be so easy. PhishLabs' 2013 white paper suggests several methods, such as shutting down the mailer programs that support email based phishing, and the websites that host the phishing kits that phishers download and use for their scams [14].

Conclusion

As phishing attacks have taken to social media and become more dangerous and effective, new tools must be developed to counteract them. Reactionary approaches to phishing have not been effective in slowing the rise of phishing attacks, nor its profitability. There exists a precedent for success in more aggressive countermeasures, but more must be developed to combat phishing on social media, while staying within the bounds of ethics and the law. Today's cyberspace is an increasingly complex space, which requires complex solutions to crimes perpetrated on it.

References

[1] Elledge, Anthony. "Phishing: An Analysis of a Growing Threat." *SANS Institute InfoSec Reading Room*, www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417.

[2] *Welcome to the 419 Eater*, www.419eater.com/html/letters.htm.

[3] KnowBe4. "General Phishing Information and Prevention Tips." *Phishing.org*, www.phishing.org/.

[4] Australian Competition and Consumer Commission. *Nigerian Scams*. 4 Jan. 2018, www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams.

[5] Seymour, John, and Philip Tully. "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter." www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf.

[6] Arthur, Charles. "Virus Phone Scam Being Run from Call Centres in India." *The Guardian*, Guardian News and Media, 18 July 2010, www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres.

[7] Weeks, Matt. "Exploiting Ammyy Admin – Developing an 0day." *Thoughts on Security*, 11 Sept. 2014, www.scriptjunkie.us/2014/09/exploiting-ammyy-admin-developing-an-0day/.

[8] Scriptjunkie. "Exploit." *Exploits Database by Offensive Security*, 13 Sept. 2014, www.exploit-db.com/exploits/34647/.

[9] United States, Congress, *Active Cyber Defense Certainty Act*. 2017

[10] Szczys, Mike. “Shmoocon 2016: Phishing for the Phishers.” *Hackaday*, 17 Jan. 2016, hackaday.com/2016/01/16/shmoocon-2016-phishing-for-the-phishers/.

[11] Gallagher, Robbie. *Honey-Phish*. bitbucket.org/rothga/honey-phish/src/3361fb40ffcf?at=master.

[12] Brozycki, John. “Phish Feeding: An Active Response to Phishing Campaigns.” *SANS Institute InfoSec Reading Room*, pdfs.semanticscholar.org/presentation/beb4/ddd72bca8052cd05c1766fd7682e36f979c5.pdf.

[13] Spitzner, Lance. “Honeytokens: The Other Honeypot.” *Symantec*, www.symantec.com/connect/articles/honeytokens-other-honeypot.

[14] PhishLabs. “How to Fight Back against Phishing: A Guide to Mitigating and Deterring Attacks Targeting Your Customers.” info.phishlabs.com/hs-fs/hub/326665/file-558105945-pdf/White_Papers/How_to_Fight_Back_Against_Phishing_-_White_Paper.pdf?t=1517337371521.