WHITEPAPER

PHISHING IN THE HEALTHCARE POND

GOING BEYOND THE BASELINE OF SOCIAL ENGINEERING

ANDREW HICKS | MBA, CISA, CCM, CRISC
HITRUST CSF PRACTICE DIRECTOR,
HEALTHCARE PRACTICE LEAD, COALFIRE

BRANDON EDMONDS | OSCP, GPEN
SENIOR CONSULTANT, COALFIRE LABS

COALFIRE℠

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

INTRODUCTION: WHO OPENED A CAN OF WORMS?

The weakest link in an information security program is people. Hackers have known this for a long time and have refined the art of social engineering. By convincing someone to do something that isn't in their best interest, malicious individuals are able to launch devastating attacks on organizations.

One method in which the hackers prey on their victims is through *phishing*. This attack vector utilizes electronic communication that appears to be trustworthy. Through this vehicle, hackers attempt to obtain sensitive information about their victims such as credentials, credit card information, and even more coveted protected health information.

The healthcare industry has always been about helping people; however, when it comes to privacy and security, being too helpful isn't always a good thing. Partners Healthcare realized this when a group of their employees fell victim to phishing emails. Hackers were able to convince some of Partners' employees to engage with them through an email on November 25, 2014, allowing the hackers to gain access to the employees' email accounts. This eventually led to the compromise of approximately 3,300 patient records.

In another unfortunate example, Texas-based Seton Healthcare Family, a part of Ascension Health System, became a victim of a compromised protected health information on 39,000 patients when an employee opened an email that turned out to be a phishing scam. This wasn't the first time Seton Healthcare had been breached; in 2013, the health system reported the theft of an unencrypted laptop. Since 2007, they had two additional breaches: one *again* involving a stolen laptop affecting 10,300 patients and a breach by a third-party vendor involving more than 500 patients where member cards were sent to the wrong members.

St. Vincent Medical Group fell victim to a phishing attack targeting employees. A statement posted on their website indicated that they discovered an employee's email account had been compromised around December 3, 2014. As of March 12, 2015, they uncovered the compromised email account that contained personal health information on approximately 760 patients.

With the ease of phishing and the high returns that can be achieved by using this technique, security professionals fear that these types of threats will increase in 2015. With health data becoming more valuable on the black market and the belief that the healthcare industry is not as "up to par" with security as other industries, the healthcare industry will continue to see an increase in attacks. (Source: iHealthBeat)

Research conducted by RSA has identified a phishing attack every minute with a total global cost of $4.5 billion losses in 2014. The U.S. alone has seen an estimated $655 million in losses with 72% of the global phishing attack volume centered on the U.S. *So what can organizations do to protect themselves from falling victim to social engineering attacks like phishing?*

A HOOK, LINE AND SINKER SOLUTION: TRAINING

One course of action an organization can take against social engineering attacks is training. It is essential that employees are made aware of phishing attacks and other tricks that hackers use to convince them to release information that they otherwise shouldn't provide. A good security awareness training program will include topics on social engineering and how to identify phishing-type emails.

Organizations should train their employees on the proper procedures to follow if they receive a suspicious email. Such procedures may include:

- Do not open attachments from unsolicited sources.
- Do not click on links from untrusted sources.
- Validate emails by calling the sender to verify they are the ones that sent the email.
- Trust your gut instincts; if an email looks suspicious, it probably is.
- Never provide account credentials through email (technical personnel should not ask for these types of credentials to be sent through email).
- Some organizations have technical solutions in place to assist with preventing certain emails from coming through, such as spam or emails that are sent externally with internal account names. Employees should know what they need to do in response, such as forward suspicious emails to a certain contact.
- If an employee isn't sure what to do, they should contact their manager/supervisor or someone in their information security department.

Although email is how the world communicates, it is still regarded as an insecure communication channel. Of course, there are solutions that are implemented such as encryption to secure email transmissions; however, employees shouldn't use email to store sensitive information such as protected health information or account credentials.

This type of sensitive information should be stored in more secure locations under more stringent access controls. Organizations need to provide appropriate training and guidance on the expectations of the use (or improper use) of their email solutions, and they should consider running social engineering panels and organizing regular events to determine the effectiveness of their security awareness programs.

SOCIAL ENGINEERING: GOING BEYOND THE BASELINE

Coalfire Labs does a lot of social engineering with the philosophy of going beyond the baseline to deliver the most thorough testing. Traditional social engineering testing involves a mundane process of taking a sample of a population and then attacking those "targets" with some pretext calls or a phishing email to obtain credentials. Metrics are recorded and then reported back in some form of a deliverable, usually a report.

In one example of a standard social engineering engagement, a pretext calling campaign included a target selection of 10 users. We made 10 phone calls and extracted passwords from three of the targeted people. Along with these calls, we delivered a phishing email attack as well, directed to a larger group of 100 users. In response to the phishing email, 12 users submitted their credentials.

In our engagement report, we noted a baseline for that engagement was a 30% fail rate in pretext calls and a 9% fail rate on the phishing campaign (or "success rate" if you look at it the way our penetration testers do). These numbers quantitatively indicate that social engineering is a risk to the tested environment. *However, does this provide a true baseline for measuring risk? Even if repeated annually?*

If it does, then it begs the question, will this be indicative of how the company will truly respond in a real attack situation? We suggest the answer is no for several reasons. The quality of campaign could vary from year-to-year, the person or persons responding to the threat could just be having an off day, recent

events may have influenced the response or any number of other variations could come into play and interfere with the results, skewing the baseline.

Beyond that, the baseline failure percentage rate likely means little to executives – 9% failure on the phishing campaign is 91% success, which on the surface sounds like pretty good performance. *These baseline results show that the organization is somewhat susceptible to a social engineering attack, but does it show impact to business assets? Does this testing prove the incident response team can do their job effectively?*

GETTING BACK TO THE WEAKEST LINK: A PRIME EXAMPLE

More recently than the example above, Coalfire Labs conducted a social engineering campaign at a large financial services institution. We sent out 160 emails and made 30 pretext calls. From all of that, we solicited a single successful response, which was an email. From the traditional, quantitative perspective, this organization has a less than 1% fail rate.

Combine those results with being well protected by firewalls, intrusion-detection-systems, corporate antivirus, a strong patch policy, web content filtering, and email spam protection (all of which we later discovered were indeed in place), and one would construe that the less-than-one-percent failure rate supports the conclusion that this organization has a solid information security program in place. Fortunately, this organization was in support of going beyond the baseline for the phishing campaign. They understood the aforementioned statistical concern – that success is still failure – and asked us to go as far as we could with any access gained. So we did.

1% FAILURE = 100% SUCCESS... FOR THE ATTACKER

The phishing campaign example above included sending malware so that when the single user clicked the link we immediately had access to the system. This shell was launched in memory, undetected by many defense layers, and connected directly into a server in our data center. One click and the game was on. With this shell access we were able to find and "steal" intellectual property, enumerate sensitive company procedures, and exploit additional vulnerabilities in other systems inside their network, ultimately compromising a domain administrator's password. Had we been this organization's actual real-world adversary, we could have easily made this access persistent and gone undetected with unauthorized remote access for an extended period of time. *Sound familiar? It's such a common attack pattern that the industry has termed this an advanced persistent threat (APT).*

PREPARE FOR REAL-WORLD ATTACKS

Simply stated: By going beyond the baseline, we were able to identify a true weakness in a seemingly locked-down environment. These results would have gone overlooked in a traditional-style social engineering campaign. The organization would have most likely seen the 1% fail rate, and considered that an acceptable risk. Instead, our team was able to demonstrate the weakness and tie that to a real-world threat, which provides the organization with ammunition for future training and improvements for implementing stronger security across their architecture.

A baseline social engineering test where failures are recorded and metrics are reported is not enough for preparing your environment for today's attacks. This has been true for recent big-name attacks that have been in the news lately. Successful attacks by real attackers are not going to take a "cookie-cutter" approach, so testing your environment for resilience against such an attack should also not use such an approach. It is time to go beyond the baseline, utilize real scenarios, and tie social engineering testing back to impact against the assets that are at risk.

CONCLUSION

What would the impact to your company's assets be should an employee fall susceptible to a social engineering attack? Do you have people, processes, and technology in place to respond to this sort of attack?

These are the key questions to ask yourself thus providing your organization with the information you need to improve your state of security.

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.

WP_HC_Phishing_091517