ANATOMY OF THE ATTACK: PHISHING

Identifying phishing attacks
To prevent data loss
Targeted phishing attacks are on the rise. Not only is spear phishing the most successful starting point for advanced adversaries to utilize to gain entrance to an environment, it also is the most difficult to defend against.

Summary
Phishing poses a real threat to both individuals and organizations alike. Unlike many other types of attacks, phishing primarily targets the person rather than the computer. Because of that, the best defense against phishing is well-informed individuals who know how to identify possible phishing attempts.

What is Phishing?
Phishing is an attempt to obtain sensitive information (like usernames and passwords) by posing as a trusted entity. Phishing attacks can take many different forms including SMS text, phone call, or most commonly, email. There are many different tactics and objectives of phishing attacks, but most follow similar patterns and can be thwarted if identified. Email phishing is the most common technique used by attackers primarily because of its efficiency. Thousands of phishing emails can be sent in the time it would take to make a single attempt via phone. Many of these phishing attacks have been made into easily deployed kits. These kits have proven to be highly successful and pose significant risk to individuals and organizations.

The Attack
Step One. One particular phishing kit that has been highly successful focuses on distributing to users that may be expecting, or regularly receive, documents from someone they know or have communicated with in the past. This kit is extremely effective in a corporate setting affecting both business-to-business (B2B) and business-to-consumer (B2C) situations. This especially effects environments and users that rely on Google Drive. Figure 1 shows an example phishing email from this kit.

Figure 1. shows a phishing email designed to appear to be from a colleague. The email address that was used to distribute was in fact from the associates actual email account. This particular phishing attempt was successful.

Step Two. Once the compromise takes place this particular kit begins to enumerate the victim’s address book and begin redistributing a similar phishing email. Because these new emails are coming from a known source, it is now far more likely the emails will be trusted and the attack will be successful.

Figure 2
Figure 2. shows an email attempting to phish customers of a salesperson. He/she was believed to have.

Step Three. When the ‘CLICK HERE’ link is clicked, the user is then directed to a page similar to Figures 3, 4, or 5. All three of the pages are leveraging Google docs as their primary source to distribute the ‘important document’. These pages are each email provider agnostic, which puts users of any major email provider potentially at risk.

Figures 3-5. show example web pages to which users are directed after clicking on the link in the phishing email. Like the emails, all three are intended to appear to be trusted sources.

Figure 3.
Figure 4.

Figure 5.

**Step Four.** Clicking on one of the icons gives the user an unattractive login form displayed in Figure 5. This would be a trigger for most users to leave the site, but for some, the email coming from a known source is enough for them to overlook this minor discrepancy. This is the overall goal of the phishing attack— to obtain usernames and passwords by appearing to be from a trusted source.

Figure 6.

Figure 7.

Figure 8.

**Conclusion**

Knowledge is the best defense in defending against phishing attacks because they attack the human element rather than the technology. Always be skeptical of emails that deviate from the norm. Although an email may come from someone you know, ensure the content of the email falls in line with what you would expect from that person. Also, keep an eye out for design elements or language that seem 'off'. It is common for phishing attacks to utilize web pages or email templates that were hastily thrown together or use broken English. Finally, never enter your username or password anywhere but the website for which they are intended. For example, you should only enter your username and password for Google drive, Gmail, etc. in a domain that ends in google.com.