SONICWALL

EXECUTIVE BRIEF: 3 THINGS YOU NEED TO KNOW ABOUT PHISHING

Understanding the phisher, the phish and the facts

ABSTRACT

Phishing is still a real threat, and has evolved into dangerous forms such as spear-phishing and whaling. In the past, phishing was primarily viewed as a consumer problem, but today phishing attacks have direct financial and reputational impact on businesses. Targeted attacks are commonly initiated through sophisticated phishing campaigns to harvest credentials or to deliver payloads such as ransomware. Often organizations ignore or minimize phishing assuming for their spam filter alone can detect phishing or that employees can easily tell; neither is true. This paper looks at challenges an organization faces in staying ahead of phishing.

To effectively combat phishing, there are three things you need to understand: The phisher, the phish and the facts.

The Phisher: The spammer's bigger, meaner alter ego

Many organizations treat phishers as "just another spammer" and in some ways, phishing emails do look and act like spam. They come in unsolicited and tend to request something of the recipient such as a purchase, an action or an entry of information. But the similarity ends there.

While spammers send junk mail that is often blatantly spam, phishers cloak themselves in the guise of trusted partner or friend. While the spammer seeks attention, the phisher avoids it, masquerading as a trusted source and using your corporate email system and your employees against you.

While neither the spammer nor the phisher is welcome on your corporate email system, the phisher is by far more threatening. While a little spam might be annoying but acceptable, phishing is totally unacceptable. A single successful instance of email phishing targeted towards your organization could expose your corporate network, corporate data, employees and customers to the criminal or malicious imagination of every hacker and criminal on the web. Even if the hole is patched almost immediately, there might be time enough for the phisher or (more likely) their malicious associates to activate a ransomware attack, or harvest an entire database of customer credit card numbers and destroy your reputation.

The Phish: Phishing, bogus updates and billing fraud

The three most common types of fraudulent emails are phishing, bogus updates and billing frauds.

Phishing

Phishing tries to hook unwary victims by leveraging their confidence in recognized brands and trusted sources. Like their consumer counterpart, enterprise phishing emails also appear to come from trusted sources, such as company management, your IT department or a business partner. They inform the recipient that updated information is needed immediately to keep an account open or maintain network access. They usually include a link to a "spoofed" or fake website. Simply by following directions, the employee unwittingly provides the phisher with

SonicWall research shows that phishing campaigns are the preferred vector for ransomware attacks.

sensitive financial data or network access information. With your corporate network compromised, you may have no choice but to recall and reissue all secure ID badges, check all devices for malicious software and trace all account activity for evidence of unauthorized activity.

Bogus updates

Another form of email attack is the bogus update. Among the most common types of bogus update is the software update. This is a fraudulent email that informs your employees of the availability of new versions of software and sends them to spoofed websites. There, they are asked to verify account information to receive the update and then unwittingly download malicious code. Once downloaded, the malicious code can attack in a number of ways. It can bypass security protocols to obtain enterprise information; damage hard drives beyond recovery; steal email addresses for mass mailings of malicious messages; or infect other users through chat sessions. The key to having an employee detect a bogus update is having a clearly defined and communicated "how your system is updated" policy, so that bogus update emails would never be trusted in the first place.

Billing fraud

Fraudulent billing emails take advantage of the fact that no process or person is perfect. Every day in accounting departments around the world, accounting staffs process billions of dollars in legitimate business payments. When an account falls behind, sometimes a vendor sends an email notice, which in turn prompts someone in accounting to process a payment as directed. Sometimes, to expedite payment, accounting may use a corporate credit card to pay the bill online. By closely mimicking the look and feel of a trusted vendor or partner, phishers use fraudulent billing emails to obtain credit card information, illegal payments or both. In extreme cases, phishers change your processes for electronic invoicing, re-directing all payments to a particular vendor to the phisher instead.

The Facts: Anti-spam and anti-virus solutions alone won't stop phishing

Businesses are well aware that email threats such as spam and viruses can cripple productivity, increase liability and cause IT costs to skyrocket. As a result, they have invested millions of dollars in anti-spam and anti-virus protections.

1. **Myth:** The best way to prevent phishing is to stop phishing emails just as you stop spam – with your spam filter.

   Fact: Phishing emails are specifically created to imitate legitimate emails. They are well written, business-oriented emails from an apparently trusted source–exactly what anti-spam filters must allow into your organization. Some phishing emails carry out this deception so well that they consistently elude spam filters. While it is tempting to equate the two, phishing is not spam. Phishing requires specific analysis, identification, and handling in order to keep it from having a negative impact on your organization.

2. **Myth: Using a URL blocking service will block phishing emails.**

   Fact: A URL blocking service is a list of known phishing websites. The links in an email is tested against this list and if there is a match, the email is a phishing email. This method is good, but slow. Phishers can launch attacks and collect their desired information in just few hours, often before the URL is reported, verified and listed on the URL block list. What is needed is an analysis of the content to help identify it as a potential phishing email. Spam filters are trained to discover spam–that is email that looks bad, what is needed is a phishing filter that looks for email that looks good, but has a few subtle tricks such as URL masking or spoofed sender.

3. **Myth: If phishing detection technology fails, employees can recognize phishing emails.**

   Fact: You cannot count on the abilities of your employees to distinguish legitimate content from its phishing twin. According to one report, 30% of phishing emails are opened and 12% of the attachments in phishing emails are clicked[1].

Conclusion

Phishing is not new and businesses have fought the phisher since the beginning of e-commerce. But just as business practices evolve to keep pace with emerging technology, phishers also adapt to the new opportunities that technology offers, such as ransomware attacks. Nevertheless, by understanding phishing as a distinct and more sophisticated type of email threat, and by seeking solutions designed specifically to stop phishing email, you can protect yourself and your organization.

Learn more about best practices to stop phishing attacks. Read our solution brief, 4 Steps to an Effective Anti-Phishing Solution.

[1] *Verizon Data Breach Investigation Report 2016*

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com