WHITE PAPER:
FRAUD ALERT: PHISHING

White Paper

Fraud Alert: Phishing — The Latest Tactics and Potential Business Impacts – Phishing White Paper

Symantec™

Norton™ SECURED
powered by Symantec

Fraud Alert: Phishing — The Latest Tactics and Potential Business Impact - Phishing White Paper

CONTENTS

Introduction

As one of the top cyber crime ploys impacting both consumers and businesses, phishing has remained a consistently potent threat over the past several years. In fact, the cumulative number of phishing attacks recorded in 2011 represented a 37 percent increase over 2010.[1]

You no longer need to be a sophisticated hacker to commit fraud on the Internet. Anyone who is motivated can join in, thanks to the off-the-shelf phishing kits provided by a thriving cyber crime ecosystem. Cyber criminals are even migrating to a new business model known as Malware-as-a-Service (MaaS), where authors of exploit kits offer extra services to customers in addition to the exploit kit itself.[2]

The impact on a business can be quite severe. RSA estimated in its October 2011 Fraud Report that the worldwide losses from phishing attacks cost more than $520 million in the first half of 2011 alone.[3] Whatever the threat – whether employees or customers have been phished, or the company Web site compromised – phishing is something to be taken very seriously. Organizations need to stay current on the latest methods employed by cyber criminals, and proactively take steps to protect themselves from fraud.

This fraud alert highlights the current growth and trends in today's phishing schemes, the potential impact on companies, and insight into how businesses can apply technology to protect themselves and their customers.

Phishing Knows No Limits

Phishing – the act of luring unsuspecting people to provide sensitive information such as usernames, passwords, and credit card data via seemingly trustworthy electronic communications – is a serious threat for both consumers and businesses. In the decade since phishing arrived on the scene, this fraud method has been growing rapidly, with one estimate citing approximately 8 million daily phishing attempts worldwide.[4] In 2011, one in every 300 emails transmitted over the Web was related to phishing.[5]

The Anti-Phishing Working Group (APWG) reported at least 112,472 unique phishing attacks globally in the first half of 2011 in 200 top-level domains.[6] Although representing a much larger number than the 42,624 attacks that the APWG observed in the second half of 2010, it was somewhat less than the record 126,697 observed in the second half of 2009, when the Avalanche botnet was on the loose. Still, 79,753 unique domain names were used in these attacks – the highest number since 2007 (see Figure 1).

[1]"RSA: October Fraud Report," RSA, October 2011.
[2]" Symantec iDefense 2012 Cyber Threats and Trends," Symantec. 2012.
[3]"RSA: October Fraud Report," RSA, October 2011.
[4]"Counterfeiting & Spear Phishing — Growth Scams of 2009," Trade Me, Infonews.co.nz, March 2, 2009.
[5]"RSA: October Fraud Report," RSA, October 2011.
[6]"Global Phishing Survey 1H2011: Trends and Domain Name Use," Anti-Phishing Working Group.

The increase is attributed to two emerging trends: Chinese phishers have been registering large numbers of domain names, and hackers instigated a massive campaign against servers hosting multiple domains.

Basic Statistics

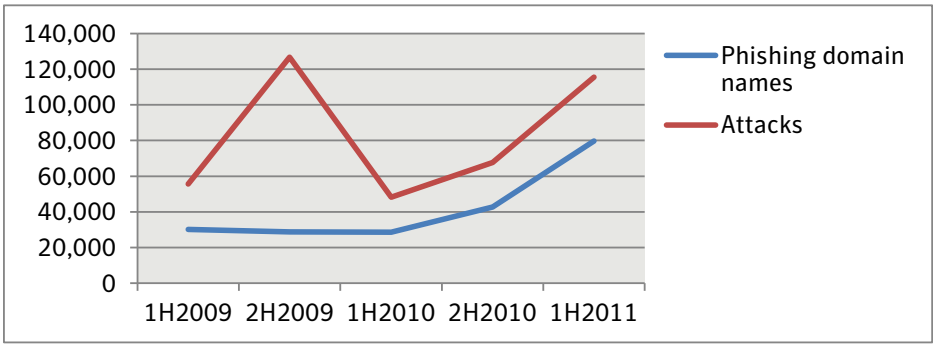

*Figure 1: Phishing attacks and phishing domain names continues trending up.**

Chinese Phishers Increasingly Aggressive

Attacks by Chinese phishers were up significantly in the second half of 2010 and the first half of 2011.[7] Indeed, Chinese phishers were responsible for a full 70 percent of all malicious domain name registrations worldwide. In the first half of 2011, Chinese phishing attacks increased by 44 percent over the second half of 2010.[8]

Shared Virtual Server Hacking Explodes

Although hackers are always coming up with new phishing schemes, this one is actually an old – albeit obscure – one that has been successfully revived. In this attack, a phisher breaks into a web server that hosts large numbers of domains and places the phishing site content on every domain, so that every web site on that server displays the phishing pages. In this manner, phishers can infect thousands of web sites simultaneously. The APWG identified 42,448 unique attacks that used this strategy – a number representing 37 percent of all phishing attacks globally.[9]

Spammers Continue To Take Advantage Of Holidays And Global Events

In the run-up to Christmas in 2011, spammers spoofed a number of legitimate retailers, offering Christmas "deals" on a range of products. There were a large number of phishing campaigns relating to the 2011 Japanese earthquake, the "Arab spring" movement, and other notable global happenings. After the usual onslaught at Valentine's Day, anti-phishing experts expect to see a plethora of emails leading up to Summer Olympics in London.[10] Spear phishing attacks, although less in the news than in previous years, notably increase during holiday periods when businesses' security operations tend to be understaffed. That way, the cyber criminals' operations have a greater opportunity to succeed. However, this seems to be less the case between the Christmas and New Year's holidays. One possible explanation is that while security teams may be only lightly staffed, there are also significantly fewer employees working, so fewer opportunities for targeted users to open malicious attachments.

[7]Ibid.
[8]Ibid.
[9]Ibid.
[10]"Symantec Intelligence Report," Symantec, January 2012.
* Source: APWG.

Phishing that Plays on Economic Fears

Today's economic turmoil delivers unprecedented opportunities for criminals to exploit victims. For instance, popular scams include phishing e-mails that look like they are coming from a financial institution that recently acquired the target victim's bank, savings & loan, or mortgage holder.[11] The large amount of merger and acquisition activity taking place creates an atmosphere of confusion for consumers, exacerbated by the dearth of consistent communications with customers. Phishers thrive in this type of situation.

Blended Phishing/Malware Threats

To increase success rates, some attacks combine phishing with malware for a blended attack model. For instance, a potential victim receives a phishing e-card via e-mail that appears to be legitimate. By clicking on the link inside the e-mail to receive the card, the person is taken to a spoofed Web site which downloads a Trojan to the victim's computer. Alternatively, the victim may see a message that indicates a download of updated software is needed before the victim can view the card. When the victim downloads the software, it's actually a keylogger.

Phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations such as financial institutions, online retailers, and e-commerce merchants) in order to obtain sensitive information such as account numbers, userids, and passwords.

Another type of Trojan that enables phishers to capture sensitive information is a redirector. Redirectors route end users' network traffic to a location where it was not intended to go.

Man-in-the-Middle SSL Stripping

Back in 2008, a new type of malware was introduced that allows cyber criminals to spoof an encrypted session. This is a variance on the standard man-in-the-middle (MITM) attack that criminals use to access passwords or sensitive information passing unprotected over the network.

Texting and Mobile Phone Phishing Scams

Posing as a real financial institution, phishers are using SMS as an alternative to e-mail to attempt to gain access to confidential account information. Known as "smishing," the typical scam informs the mobile phone user that the person's bank account has been compromised or credit card/ATM card has been deactivated. The potential victim is directed to call a number or go to a spoofed Web site to reactivate the card. Once on the site, or through an automated phone system, the potential victim is asked for card and account numbers and PIN numbers.

How Phishing Could Impact Your Business

While the financial industry continues to be a primary target for phishers, it's certainly not the only sector vulnerable to attack. Auction sites, payment services, retail, and social networking sites are also frequent targets. The APWG also reports a massive increase in attacks aimed at cell phone providers and manufacturers. In short, no business or brand is inherently safe.

[11]"FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A Phish-erman's Special," www.ftc.gov

Phishing attacks that pose as a company's official Web site diminish the company's online brand and deter customers from using the actual Web site out of fear of becoming a fraud victim. In addition to the direct costs of fraud losses, businesses whose customers fall victim to a phishing scam also risk:

- A drop in online revenues and/or usage due to decreased customer trust
- Potential non-compliance fines if customer data is compromised

Even phishing scams aimed at other brands can impact a business. The resulting fear caused by phishing can cause consumers to stop transacting with anyone they can't trust.

Protecting Your Business

While there is no silver bullet, there are technologies that can help protect you and your customers. Many of the current phishing techniques rely on driving customers to spoofed Web sites to capture personal information. Technology such as Secure Sockets Layer (SSL) and Extended Validation (EV) SSL are critical in fighting phishing and other forms of cyber crime by encrypting sensitive information and helping customers authenticate your site.

Security best practices call for implementing the highest levels of encryption and authentication possible to protect against cyber fraud and build customer trust in the brand. SSL, the world standard for Web security, is the technology used to encrypt and protect information transmitted over the Web with the ubiquitous HTTPS protocol. SSL protects data in motion, which can be intercepted and tampered with if sent unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware.

To help prevent phishing attacks from being successful and to build customer trust, companies also need a way to show customers that they are a legitimate business. Extended Validation (EV) SSL Certificates are the answer, offering the highest level of authentication available with an SSL Certificate and providing tangible proof to online users that the site is indeed legitimate.

EV SSL gives Web site visitors an easy and reliable way to establish trust online by triggering high-security Web browsers to display a green address bar with the name of the organization that owns the SSL Certificate and the name of the Certificate Authority that issued it. Figure 2 shows the green address bar in Internet Explorer.

The green bar shows site visitors that the transaction is encrypted and the organization has been authenticated according to the most rigorous industry standard. Phishers can then no longer capitalize on visitors not noticing they are not on a true SSL session.

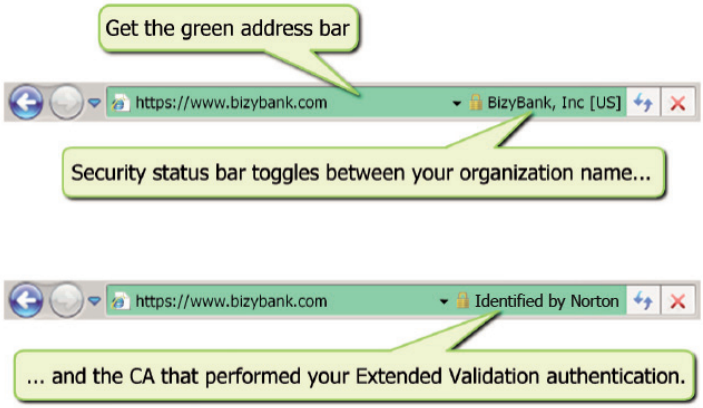

Figure 2. The Green Address Bar Triggered by an EV SSL Certificate.

While cyber criminals are becoming adept at mimicking legitimate Web sites, without the company's EV SSL Certificate there is no way they can display its name on the address bar because the information shown there is outside of their control. And they cannot obtain the legitimate company's EV SSL Certificates because of the stringent authentication process

Consumer and Employee Education

In addition to implementing EV SSL technology, businesses should continue to educate their customers and employees on safe Internet practices and how to avoid cyber fraud. Teach them how to recognize the signs of a phishing attempt, including:

- Misspellings (less common as phishers become more sophisticated)
- Generic greetings instead of personalized, urgent calls-to-action
- Account status threats
- Requests for personal information
- Fake domain names/links

Also educate your customers and employees on how to recognize a valid, secure Web site before they provide any personal or sensitive information by:

- Looking for the green bar
- Making sure the URL is HTTPS
- Clicking on the padlock to match the certificate information with the Web site they intended to go to

Education is a key component of building the trust necessary to overcome phishing fears. By helping your customers understand how to confirm they are safe on your Web site, you can grow revenues, differentiate your offering, and/or benefit from operational savings by moving more transactions online.

Phishers: Tough, Shape-Shifting Cyber Adversaries

Phishing will continue to evolve into new forms, while attempting to take advantage of human behaviors such as compassion, trust, or curiosity. Protecting your brand and your business from phishing requires constant diligence, but pays rewards beyond reduced fraud losses.

By educating and protecting your customers with the highest levels of protection provided by EV SSL Certificates, your business can help ensure that customers have greater confidence in your online services. By demonstrating leadership in online security, you can broaden your market appeal and in doing so, generate new revenue streams.

For the most current information on global phishing trends, please visit the Symantec Monthly Intelligence Report.

Glossary

Certificate Authority (CA) — A Certificate Authority is a trusted third-party organization that issues digital certificates such as Secure Sockets Layer (SSL) Certificates after verifying the information included in the Certificates.

Encryption — Encryption is the process of scrambling a message so that only the intended audience has access to the information. Secure Sockets Layer (SSL) technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive information from electronic eavesdropping.

Extended Validation (EV) SSL Certificate — Requires a high standard for verification of Secure Sockets (SSL) Certificates dictated by a third party, the CA/Browser Forum. In Microsoft® Internet Explorer 7 and other popular high-security browsers, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

HTTPS — Web pages beginning with “https” instead of “http” enable secure information transmission via the protocol for secure http. “Https” is one measure of security to look for when sending or sharing confidential information such as credit card numbers, private data records, or business partner data.

Secure Sockets Layer (SSL) Technology — SSL and its successor, transport layer security (TLS), use cryptography to provide security for online transactions. SSL uses two keys to encrypt and decrypt data — a public key known to everyone and a private or secret key known only to the recipient of the message.

SSL Certificate — A Secure Sockets Layer (SSL) Certificate incorporates a digital signature to bind together a public key with an identity. SSL Certificates enable encryption of sensitive information during online transactions, and in the case of organizationally validated Certificates, also serve as an attestation of the Certificate owner’s identity.

More Information

Visit our website

http://www.symantec.com/ssl

To speak with a Product Specialist in the U.S.

1-866-893-6565 or 1-650-426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

Symantec™

Norton™ SECURED
powered by Symantec

UID: 030/02/14