WEBROOT®

Phishing 2.0

Why phishing is back as the No. 1 web threat, and how web security can protect your company

Contents

Brought to you compliments of
WEBROOT®

Why Business Needs to Prepare for Phishing 2.0

At one point, it seemed that phishing was receding to the status of a minor issue threatening only naïve consumers. But a new version has emerged, fueled by new cybercriminals and new phishing techniques.

New types of phishing campaigns are particularly worrisome for businesses because:

- They are aimed at businesses (including small and midsize businesses) rather than consumers.
- They evade traditional antivirus and antiphishing products.
- They can fool even security-savvy computer users by using information gathered from social media and other web sources.
- They often target employees with access to the most sensitive information, such as bank accounts, customer lists and intellectual property.

In this white paper we will:

- Summarize the decline of Phishing 1.0.
- Discuss how phishing has turned toward business and become more costly.

- Outline the structure of new Phishing 2.0 attacks.
- Delineate how the new campaigns evade standard antiphishing countermeasures.
- Describe how web security services with real-time antiphishing capabilities can protect against Phishing 2.0 attacks.

The Rise and Decline of Phishing 1.0

Most computer users are familiar with phishing campaigns that broadcast identical emails to thousands of email addresses.

These emails appear to be from banks, online retailers, social networking sites and other widely used websites. They entice readers to go to a website controlled by the cybercriminals and fill in a form or download a file containing a Trojan, keylogger or some other type of malware.

The goal of Phishing 1.0 campaigns is to obtain information that can be used for identity theft, such as user IDs and passwords, Social Security numbers and credit card numbers.

However, information security companies have diminished the effectiveness of standard phishing campaigns through countermeasures that:

- Recognize common phrases used in phishing messages (lexical analysis).
- Flag websites known to send phishing messages and others known to capture information from victims (reputation analysis and blacklists).
- Identify attachments containing known malware (signature recognition).

Also, the number of naïve email users has fallen as accounts of these attacks have circulated in the press.

These factors have limited the potential for financial gain from standard "mass" phishing attacks.

Phishing Activity Turns to Business

The decreasing effectiveness of phishing campaigns against consumers has caused cybercriminals to turn their attention to business — unfortunately with growing success.

According to information security firm RSA, the cost to the global economy in fraud damages related to phishing attacks increased 22% between 2011 and 2012, to $1.5 billion.[1]

The impact has been felt by small and midsize businesses as well as large enterprises.

A recent Webroot survey of U.S. and U.K. firms with 100 to 4,999 employees found that *phishing was the most common web-borne attack in 2012, experienced by 55% of the companies surveyed.*

>> Phishing

Phishing is an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.

TechTarget WhatIs.com

[1] "The Year in Phishing," *RSA*, January 2013: http://www.slideshare.net/emcacademics/rsa-fraud-report-january-2013. Data from RSA and from the Anti-Phishing Working Group indicates that the number of phishing attacks may have peaked in mid-2012 and declined later in the year (see the RSA report and the APWG Phishing Attack Trends Report – 3Q2012 at http://apwg.org/resources/apwg-reports/). However, this is not inconsistent with the rise in the cost of phishing attacks, as more of them are focused on high-value business targets.

>> **For small and midsize businesses, phishing is the most common attack**

Some 55% of companies surveyed experienced phishing attacks in 2012, making it the most common web-borne attack, ahead of keyloggers, website compromises, drive-by downloads and SQL injection attacks.

Webroot survey of 500 U.S. and U.K. companies with 100 to 4,999 employees

The survey also found that:

- Of the U.S. companies, 30% reported the cost of web-borne attacks (including phishing attacks) at $50,000 to $1 million.
- Of the U.K. companies, 27% reported the cost of web-borne attacks (including phishing attacks) at £50,000 to £1 million.

Phishing 2.0: Anatomy of a New Attack

But how have cybercriminals been able to achieve such success attacking businesses, which would seem to be better protected and more security-aware than consumers? The answer lies in the evolution of what can be called Phishing 2.0 — a new breed of phishing campaigns.

We will first look at the basic structure of these attacks, and then examine exactly how they are designed to evade the countermeasures deployed against standard phishing attacks.

Phase 1: Targeting

The first phase of a Phishing 2.0 attack involves profiling a group of potential victims.

There is actually a spectrum of targeting opportunities, ranging from:

- Broad categories, such as "business people who ship packages" and "managers who book business travel," to
- General roles, say, finance executives, engineering managers or members of the legal staff at particular companies, to
- Specific individuals at specific companies.

Phase 2: Reconnaissance

"Reconnaissance" is finding personal information and email addresses of the targeted victims.

For attacks targeting broad categories of victims, it might be sufficient to obtain lists of email addresses from legitimate mail houses or from black market sources of spam addresses. This is because a list of business managers will likely include a reasonable percentage who have sent overnight packages or booked airline reservations for business travel.

For attacks targeting business roles and specific individuals, cybercriminals may need to dig deeper to find names, email addresses and facts about the potential victims. But this is much easier today than in the past.

Company websites, industry and professional association websites, comment sections of blogs and bulletin boards often contain names and titles. Web searches make it relatively simple to find names and email addresses associated with given companies and professions. Social media sites like Facebook, LinkedIn, Google+ and Twitter, as well as video- and photo-sharing sites such as YouTube, Vimeo, Pinterest and Flickr, make it easy to gather names and very detailed personal and professional information.

It is clear that the value of social media has not been lost on cybercriminals. By one estimate, 40% of social media users have been attacked by malware.[2]

>> **Spear Phishing**

Spear phishing is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

TechTarget WhatIs.com

Phase 3: Creating spear phishing emails

The next step is for the cybercriminal to create spear phishing emails. These emails will have two characteristics:

- They will mimic common business and personal emails — without using phrases that could identify them as mass distribution spam.
- They will use details gathered during the reconnaissance phase to make the emails convincing.

If cybercriminals are trying to reach broad categories of potential victims, they will create messages and attachments tailored to attract the attention of those groups. An analysis of the words most frequently found in the file names of attachments in phishing messages include those related to:

- Package delivery and shipping (including "DHL," "delivery," "express," "shipment," "UPS" and "parcel")
- Banking and purchasing (including "Visa Card," "PayPal," "invoice" and "purchase order")
- Airlines and travel (including the names of airlines)[3]

If cybercriminals are trying to reach people in a given role, they might build emails around a top-of-the-mind issue for a specific group, such as an email about new tax legislation aimed at the finance or legal staff.

If the target is a specific individual, the email might contain details gathered from social media sites, including the names of friends and family members, professional affiliations, or even hobbies or recent travel. The email might also purport to be sent by a colleague or friend, or a friend of a colleague or friend.

Cybercriminals have demonstrated considerable sophistication and ingenuity in creating these emails. For example:

- Faculty and staff at several universities received emails seemingly from their IT departments requiring that they send their email credentials to retain access to their university email accounts.
- Twenty individuals at a defense firm were sent an email with an infected PDF file purporting to be an employee satisfaction survey.
- Senior executives of a firm in Australia were sent an email notifying them of a very plausible "commercial litigation subpoena" against the company, with a link to a legitimate but infected legal blog.
- A specific executive was sent, by name, an email purporting to be from the Internal Revenue Service claiming that a criminal tax fraud investigation into the company was under way, with a link to a Trojan.

[2] "40% of Social Network Users Attacked by Malware," *Time*, March 2011: http://techland.time.com/2011/03/23/40-of-social-network-users-attacked-by-malware/.
[3] "Top Words Used in Spear Phishing Attacks," *FireEye*, September 2012: http://www.fireeye.com/resources/pdfs/fireeye-top-spear-phishing-words.pdf.

- A journalist at a press freedom organization received an email from a colleague at a partner organization, with the subject line: "Fw: Journalists arrested in Gambia," and a request in the text to "please review the attachment for more information." The attachment was a .zip file that included a piece of malware disguised as an image file.[4]

In classic phishing fashion, the emails contain links to:

1. A website controlled by the cybercriminal
2. A legitimate website compromised by the cybercriminal
3. A file with a title interesting to the victim, but containing malware

Phase 4: Plant malware on the victim's computer

In some examples of spear phishing, the cybercriminal simply entices the victim to fill out a web form with confidential information like account number, Social Security number or user ID and password.

More commonly, though, the goal is to lure the victim into downloading a malware file, either by clicking on an attachment in the email, clicking on a link in the email that requests a file download, or clicking on a link in a webpage.

However, if there is an unpatched vulnerability in a browser or application on the victim's computer, the cybercriminal can often execute a "drive-by download" merely by luring the victim to a compromised webpage.

Phase 5: Exploit the breach

The cybercriminal is now able to follow up by capturing the victim's keystrokes, finding and exporting files on the victim's computer, or burrowing into the company network using the victim's credentials.

The last approach is the method typically used as part of advanced persistent threats, which are systematic campaigns to capture large quantities of confidential data over a period of time.

Phishing 2.0: Countering the Countermeasures

Let's look now at some of the techniques Phishing 2.0 attacks have used to circumvent the countermeasures that have been largely successful in protecting against standard phishing attacks. These are summarized in Table 1.

Generic versus personalized text

Phishing 1.0 campaigns broadcast high volumes of identical emails. They also made frequent use of disguised links that appeared legitimate in the email text but in fact linked to a completely different site.

[4] These examples were cited in: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf; http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10154/ironport_targeted_phishing.pdf; https://threatpost.com/en_us/blogs/attackers-using-known-trojan-exploits-adobe-zero-day-120811; and http://www.cpj.org/internet/2012/08/dear-cpj-some-malware-from-your-friend.php.

Because so many emails were sent with identical phrasing, antispam and antiphishing programs could easily recognize common wording and often entire emails. In addition, employees could be trained to recognize the suspicious wording and to position the cursor over links to see if they matched the URL shown in the text.

Characteristics of Phishing 1.0 Attacks	Countermeasures	Counter-Countermeasures Used in Phishing 2.0 Attacks
Generic phishing text and disguised links	• Lexical analysis • Train employees to recognize suspicious wording and disguised links	• Simulation of real business emails • Personalized greetings and messages • Obfuscated and shortened URLs
Static sending domains and target websites	• Reputation analysis of domains • Blacklists	• "Throw-away" (limited use) domains • Compromising of legitimate websites
Known malware attachments	• Signature recognition	• Toolkits to morph malware files • Zipped and encrypted attachments
Outbound communication	—	• "Water holing"

But Phishing 2.0 emails are much more difficult to identify through lexical analysis because there are many fewer samples and they mimic real emails sent between business people. The messages may even be unique if they are personalized with information specific to the company and the individual recipient.

Cybercriminals have also learned to obfuscate links by embedding them in buttons ("Submit," "Play," or "Like") and images, and by using short URLs that completely hide the destination website.

Static versus throw-away domains

Phishing 1.0 campaigns were often sent from long-lived domains that could be identified as spam sources in reputation databases. Similarly, websites controlled by the cybercriminals lasted long enough to be identified and included in blacklists used by URL filtering products.

Cybercriminals have developed ways of generating hundreds of domains that may be used only for a single phishing campaign. These websites are far less likely to show up in a reputation database or blacklist. By mid-2012, such "throw-away" domains grew to almost half of all domains used for spear phishing.[5]

[5] Advanced Threat Report – 1H 2012, *FireEye*: http://www2.fireeye.com/advanced-threat-report-1h2012.html., August 2012

Cybercriminals have also developed more effective ways of compromising legitimate websites and using them to foist malware on victims. One technique is to create a pop-up form or a tab that appears on the legitimate website.

Static versus morphing attachments

Attachments used in Phishing 1.0 campaigns were often well-known malware variants. And if they were not well known before the campaign, they became known to antivirus vendors after the campaign was broadcast. Antivirus products were therefore able to identify the attachments as malware either immediately or after the first few victims reported the attack.

Now cybercriminals have developed kits that create hundreds or thousands of the malware files with just enough variation so they can't be identified using standard signatures. In mid-2011, the top 20 malicious attachments accounted for 45% of total attachments used in spear phishing campaigns; by mid-2012, that figure had fallen to only 26%.

Cybercriminals have also become more sophisticated in using encryption (and sometimes double encryption) to prevent some antivirus products from scanning attachments.

A new trick: Water holing

"Water holing" is a technique whereby attackers compromise a website that is known to attract people from a target geographical area, industry or company and set up a drive-by download from that site. Examples mentioned in the press include websites intended for employees of financial services firms, technology companies and government agencies in Massachusetts and the Washington, D.C., area.[6]

Strictly speaking, water holing is not a phishing attack because there is no email component. However, it is a form of targeted attack that can achieve the same results. It is also not hard to imagine that in the future, phishing emails will be used to steer potential prey to these watering holes.

How Web Security Services Can Protect Against Phishing 2.0

Fortunately, there are security products and services that can protect against these new phishing attacks.

Here we will look at the relevant capabilities of one of them: Webroot SecureAnywhere Web Security Service.

1. Restricting the non-business use of social media sites

Webroot SecureAnywhere Web Security Service provides URL and web content filtering features that can prevent employees from visiting websites that are known to contain malware. They can also restrict exposure to sites with a high probability of compromise, such as those related to pornography and gambling. Companies can tailor this filtering based on 83 website categories and subcategories and a database of over 310 million domains.

[6] "Lions at the Watering Hole – The "VOHO" Affair," *RSA blog*, July 20, 2012: http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/.

But the service also provides features that can impede the reconnaissance phase of Phishing 2.0 attacks by preventing employees from visiting social media sites that are not needed for their job function. For example, access to Facebook, Twitter and LinkedIn could be restricted to groups like marketing and human resources that have a business reason to communicate with customers and other outside parties.

Webroot SecureAnywhere Web Security Service can also put employees on guard by flagging suspicious sites in search results — a feature called Scan Ahead.

2. Detecting phishing emails and blocking access to controlled websites

Webroot SecureAnywhere Web Security Service also offers what might be the most sophisticated and efficient antiphishing technology on the market today.

Webroot's real-time antiphishing technology evaluates web traffic to identify phishing sites based on dozens of factors, including source domain, spoofed IP addresses, keywords and patterns in the text, size and type of attachments, the presence of zipped and encrypted attachments, and the presence of disguised, misleading and shortened links.

Webroot SecureAnywhere Web Security Service also evaluates every URL request by scoring each requested webpage for phishing risk. This is done by analyzing the requested page based on the contents of the page and on reputation information of the domain, including the site history, age, location, links and other contextual and behavioral data.

URL scoring is constantly being refined with "machine learning" that adjusts the weight to be applied to the hundreds of factors based on the experience of thousands of customers and millions of Internet users. When necessary, human evaluation is fed back into the machine-learning model to continuously increase accuracy.

These evaluations leverage information in the Webroot Intelligence Network, an online resource with over 100 TB of data on websites, phishing attacks, malware behavior patterns and other security information. This includes information from third-party virus and spam clearinghouses, other security vendors, and a network of spam traps, honeypots and naïve-user simulations designed to observe attacks in real time.

By evaluating websites in real time, Webroot SecureAnywhere Web Security Service provides protection against the use of throw-away domains and water holing.

3. Block malware from phishing messages and infected websites

Webroot SecureAnywhere Web Security Service scans HTTP and FTP-over-HTTP traffic and is 100% effective in blocking known malware before it reaches the company network. It also uses multiple zero-hour heuristic filters to identify new and unknown threats, including many of the morphed files used in Phishing 2.0 attacks.

Summary

Phishing 1.0 campaigns have at least been contained by standard antiphishing and antivirus technologies.

But cybercriminals have developed techniques to target and personalize phishing messages and evade conventional defenses, among other methods, by harvesting personal data from social networking sources, using throw-away domains, compromising legitimate websites, disguising malware files in attachments and creating water holes to attract victims.

The costs of these Phishing 2.0 attacks can be significant — frequently over $50,000 for even small and midsize businesses.

One solution is the Webroot SecureAnywhere Web Security Service, which can limit the amount of personal information employees expose on social media websites, uncover phishing emails and phishing websites in real time more effectively than any other antiphishing technology on the market today, and block both known and unknown malware before it reaches the company network.

About Webroot

Webroot is bringing the power of software as a service to Internet security with its suite of Webroot SecureAnywhere™ offerings for consumers and businesses, as well as offering its security intelligence solutions to organizations that also focus on cybersecurity. Founded in 1997 and headquartered in Broomfield, Colo., Webroot is the largest privately held Internet security organization based in the U.S.

For more information on our products, services and security, visit www.webroot.com or contact us at:

Webroot — APAC
Suite 1402, Level 14, Tower A 821 Pacific Highway
Chatswood, NSW 2067 Australia
Tel: +61 (0)2 8071 1900

Webroot Headquarters — USA
385 Interlocken Crescent, Suite 800
Broomfield, Colo. 80021 U.S.A.
Tel: +1 800 870 8102

Webroot International — EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2 Ireland
Tel: +44 (0)870 1417 070

