



Phishing Lures
infectionvectors.com
April 2005

Overview

Phishers continue to use obfuscation tricks to hide the true nature and location of their web sites. One of the more common in recent months is known as Blinder, a JavaScript function that throws a small pop-up window onto the screen in hopes of covering the actual URL displayed in the browser with a phony one. Blinder is described in more detail at <http://www.infectionvectors.com/malagents/blinder.htm>. This report examines one phisher's use of such tactics and the breadth of the business behind phishing.

Bank On It

The following email was received by infectionvectors.com; it purports to be a security update alert from Bank of the West. Bank of the West is a large California-based institution.



We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank.

Hoping you understand that we are doing this for your own safety we suggest you to update your information, this will maintain your account updated.



The Strength To Help You Do More.

The email looks fairly convincing, however, like many scams it contains an oddly phrased sentence, "Hoping you understand that we are doing this for your own safety we suggest you to update your information, this will maintain your account updated." Nonetheless, given the volume of most spam-delivered fraud attempts, this one will likely catch a few Bank of the West customers. Within the source of the email is the address of the actual website as well as the location of a few of the images used in the message. See below for code from the email (this snippet edited for space, no content was changed beyond removing carriage returns/tabs except where noted):

```

<a target=3D"_blank" href=3D"http://213.252.80.82/ls/index.html">
  <img alt=3D"wamu.com"
src=3D"http://www.sierramadrenews.net/biz/bank=
ofthewest/images/logo.jpg" border=3D"0"
width=3D"194" height=3D"62"></a>
  [edited content here]
  <span class=3D"text"><font face=3D"Verdana">W</font><font
face=3D=
"Verdana" style=3D"font-size: 9pt">e are glad to
  inform you, that our bank has a new security
system. The new updated technology will ensure the security of your
payments through our bank.<br>
  <br>
  Hoping you understand that we are doing this
for your own safety we suggest you to update your information, this
will maintain your account updated.</font></span><br>
  <br>
  <a href=3D"http://213.252.80.82/ar/update.htm">
  <img id=3D"imgSignUp" alt=3D"sign up now"
src=3D"https://mortgag=
e.unionplanters.com/upmb/resource/images/regions/b_login_alt.gif"
align=3D=
"right" border=3D"0" name=3D"imgSignUp" width=3D"68"
height=3D"21"></a><br=

```


Note the use of other bank sites (wamu.com and unionplanters.com, also the victims of phishing scams recently) for graphic files as well as the address of the server used to stage the fake login page. When a user clicks the "Log In" link, they are directed to a fake version of the Bank of the West's website which uses the Blinder trick mentioned above.

Bank of the West | - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://213.252.80.82/ar/update.htm>

<https://www.bankofthewest.com/BOW/home>

BANK OF THE WEST  [PERSONAL](#) [SMALL BUSINESS](#) [COMMERCIAL](#) [ABOUT US](#)

Online Banking

Former Union Safe Deposit Bank customers now joining Bank of the West can get information on [frequently asked questions](#).

News Bulletin

March 10, 2005 | Bank of the West is introducing itself to the many new communities it now serves - resulting from its acquisition of Community First Bank - by offering a checking account program with a "furry" twist. [More](#)

Confirm Your Identity

Full Name:

ATM/Debit Card Number:

Expiration Date: month year

CVV2:

PIN Number:

E-mail Address:

We are asking you this to make sure you are the real owner of this account.

Take note of the fact that the Trojan is unsuccessful at guessing the correct location of the address bar and covers links on the “bank’s” website, immediately raising red flags to users. Consider, however, how good the site would look if instead of an IP address, the Blinder-created pop-up/URL inhabited the address bar.

The site that an unsuspecting (or suspecting researcher) is one of many hosted by the phishers in question at the same address. For the period of March 30, 2005 through April 9, 2005, reports of scam sites at 213.252.80.82 (see below for registration information) include:

MBNA Scam:

http://groups-beta.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/10d5d3d7c63752b9/71b6da8324035ffb?q=213.252.80.82&rnum=2#71b6da8324035ffb

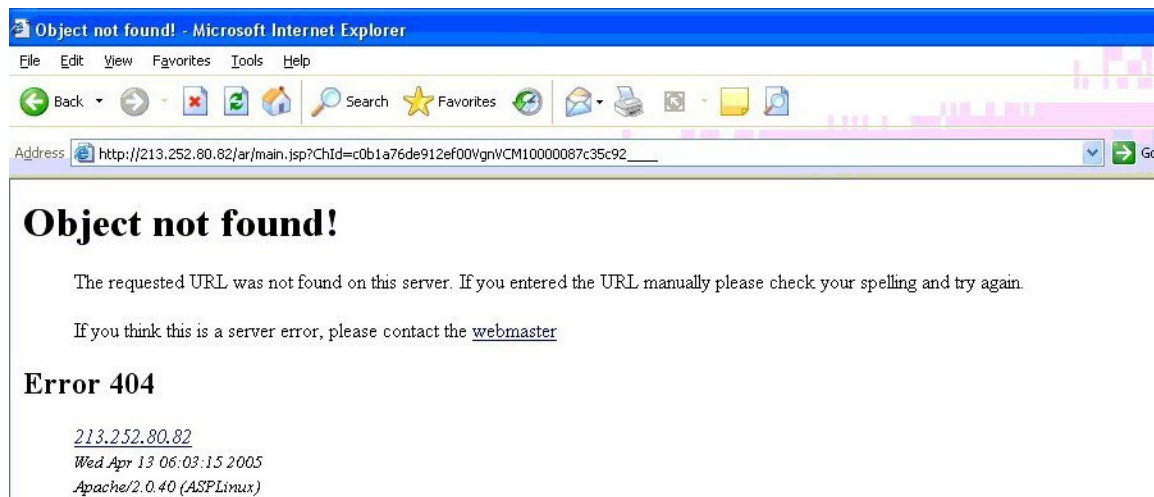
ebay Scam:

http://groups-beta.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/2269c0806b568a24/eccd4fa34e748ab9?q=213.252.80.82&rnum=3#eccd4fa34e748ab9

Regions Bank Scam:

http://groups-beta.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/4c2495ae8599be28/609c81cad9c7d056?q=213.252.80.82&rnum=1#609c81cad9c7d056

The phony Bank of the West site was created by Microsoft's FrontPage 5.0 (presuming the HTML tags in each are accurate) like the email that was blasted out to users everywhere. The Blinder script is immediately recognizable at the top of the source for the web page, guessing the correct location for the pop-up and inserting the "bankofthewest.com" entry. The rest of the site looks much like the real bank’s page, with the exception that the criminals did not ensure that links worked correctly.



As shown above, the hyperlinks do no lead to other phony pages or to the actual site (as many phishers have done) but to real error pages indicating the links are invalid. This is

possibly the result of standing up so many iterations of the phishing scam on the server; certain details are simply not worth the time/resources required. There is a return on investment calculation for every business; those attracted to these scams are probably not going to check the rest of the links on the page.

The HTML of this page also reveals a routine that asks for credit card data that is not used in the current iteration of the scam and a page that exists as the “index” for the site. Following the URL provided in the HTML to the index page for the site, one can observe another of the scams established on the server. Initially, a Regions Bank scam is tipped off by the page title: "Regions - Customer Details Confirmation." Another version of Blinder can be seen in this code as well.

Lifted from the index page, an IP address registered to Chile, possibly indicating the last location of this page’s contents:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">  
<!-- saved from url=(0027)http://164.77.195.251:87/r/ -->
```

Bank of the West

The subject of this report, Bank of the West, like all online financial institutions is wrestling with phishing daily. One credit to the bank is a very informative consumer protection page that they host at:

<http://www.bankofthewest.com/BOW/main.jsp?ChId=9d1825494ae10010VgnVCM100007fc35c92>

Their page provides a good definition of phishing, ways to identify fraud, and links to resources such as the FDIC Phishing Alert page. This type of response is only one level of a fraud prevention and mitigation plan, but is a very good start that every business should employ.

Appendix: Additional Information

WHOIS Information for 213.252.80.82

Russian Federation (high) [City: Moscow, Moskva]

% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See <http://www.ripe.net/db/copyright.html>

inetnum: 213.252.80.0 - 213.252.80.255
netname: RMT-EXCHANGE-10
descr: RMT Exchange subnets
country: RU
admin-c: RMTL1-RIPE
tech-c: RMTL1-RIPE
status: ASSIGNED PA
mnt-by: RM-TELECOM-MNT
changed: *****@rmt.ru 20010910
source: RIPE

route: 213.252.64.0/18
descr: DELEGATED CIDR BLOCK
descr: RMT
origin: AS5523
mnt-by: RM-TELECOM-MNT
changed: *****@rmt.ru 20010503
source: RIPE

role: RM Telecom Network Operations Center
address: RM Telecom NOC
address: 17a, Boutlerova str.,
address: 111342, Moscow
address: Russia
phone: +7 095 3330322
phone: +7 095 3330422
fax-no: +7 095 3330422
e-mail: *****@rmt.ru

trouble: -----
--

trouble: RM Telecom NOC is reachable 09:00-21:00 on MSK working
days.

trouble: -----
--

trouble: For problems with routing contact (5 x 12):

trouble: RM Telecom Network Operation Center:

trouble: - *****@rmt.ru

trouble: - +7 095 932-88-80

trouble: - +7 095 939-58-77

trouble: -----
--

admin-c: EGK11-RIPE
tech-c: EGK11-RIPE
tech-c: NVB10-RIPE

tech-c: AML9-RIPE
nic-hdl: RMTL1-RIPE
remarks: http://www.rmt.ru/
mnt-by: RM-TELECOM-MNT
changed: *****@rmt.ru 20030522
source: RIPE

WHOIS Information for 62.193.231.125 (sender of email):

inetnum: 62.193.224.0 - 62.193.239.255
netname: AMEN-EUROPE-NETWORK
descr: AMEN European Network
descr: For Spam/Abuse requests please send mail to
*****@amenworld.com
country: FR
admin-c: AN1108-RIPE
tech-c: AN910-RIPE
status: ASSIGNED PA
mnt-by: AMEN-MNT
mnt-lower: AMEN-MNT
mnt-routes: AMEN-MNT
rev-srv: ns1.amenworld.com
rev-srv: ns2.amenworld.com
notify: *****@amen.fr
changed: *****@amenworld.com 20040130
source: RIPE

route: 62.193.228.0/22
descr: AMEN Networks
origin: AS28677
mnt-by: AMEN-MNT
notify: *****@amen.fr
changed: *****@amenworld.com 20040607
source: RIPE

role: AMEN NOC
address: AMEN - Agence des Medias Numeriques
address: 12/14, rond-point des champs elysees
address: 75008 Paris, France
phone: +33 8 92 55 66 77
e-mail: *****@amen.fr
nic-hdl: AN910-RIPE
admin-c: AN1108-RIPE
tech-c: AN1018-RIPE
tech-c: AN1019-RIPE
notify: *****@amen.fr
mnt-by: AMEN-MNT
changed: *****@amen.fr 20030826
changed: *****@amen.fr 20031114
changed: *****@amen.fr 20040908
source: RIPE

person: Gorun RENAULT
address: AMEN - Agence des Medias Numeriques
address: 12/14, rond-point des champs elysees

address: 75008 Paris, France
phone: +33 8 92 55 66 77
fax-no: +33 1 40 87 76 89
e-mail: *****@amen.fr
nic-hdl: AN1108-RIPE
mnt-by: AMEN-MNT
changed: *****@amen.fr 20031114
source: RIPE
notify: ****@amen.fr