Anatomy of a Phishing Attack

Introduction

Through access logs and other resources lent from the target bank's web hosting company, we were able to produce the anatomy of this phishing attack.

Attackers working from Romania had been planning this day for over 2 weeks. On the morning of August 26, 2005 a computer system in Bledsoe County, Texas, belonging to the K-12 school system's library, was used as a launching point to distribute hundreds of phishing emails. The message requested private customer information such as social security, credit card, and personal identification numbers. A compromised server in Brazil had been staged by these attackers with a mock-up of the bank's real web site to collect the data.

By the early afternoon, phishing email recipients around the globe were viewing the message in their inboxes. As an act of good faith, some readers who were not even customers of the targeted bank, reported the suspected fraud. Shortly after 13:00 hours EST, the fraudulent site had been removed by the Brazilian CERT. However the attackers in Romania noticed quickly and re-built their fake web site within forty-five minutes.

As of Monday August 29, the second incarnation of the fraudulent web site has also been taken offline – thanks to the efforts by several high profile take down teams working over the weekend. Yet, as a result of several key flaws in the attacker's deployment methodology, this report is able to accurately quantify the number of potential customers affected (viewed the message), number of potential customers victimized (submitted data), the distribution profile of email services (ie Hotmail, Yahoo, etc), the hours during which the attack was most widely viewed, and the countries from which those emails were viewed

We were also able to learn several key characteristics about the attackers, including country of origin, potential motives, planing timeline, and staging areas. Furthermore, we can identify at least five other institutions (eBay, PayPal, Washington Mutual, LaSalle Bank, Sky Online) targeted by the same techniques and code. We quite possibly even have obtained high resolution photographs of the attackers. If this is true, and we may never know for sure, then we would also have their hacker nicknames, Yahoo Messenger screen names, locations of residence, birth dates, and pictures of their family and friends.

At the time of this writing the phishing attempt is getting almost no attention and we know of only one user who submitted data to the phishing form (not even necessarily *correct* information) and that is being researched by the bank. For an attack to have been planned 2 weeks in advance, launched globally, and monitored consistently to only result in one possible victim, we could safely label this phishing attack as highly unsuccessful.

We would like to invite you to enjoy this report and share with us your questions and concerns. Please read carefully and with as much attention to technical detail as possible. The events which seem negligible at first glance are the ones that pull this puzzle together.

Note: When times are discussed, unless otherwise noted they are done so in 24-hour format, Eastern Standard Time. The time in Romania is +7 hours of EST.

Note: We refer to the attacker sometimes as singular (he) and sometimes plural (they). The truth is – we don't know if there was more than one attacker, much less the gender.

Note: The Appendices contain just as critical information as the other sections. Do not skip the Appendices because they appear lengthy.

Reconnaissance, Staging, and Testing

The obvious first step in a phishing attack, or any attack for that matter, is the process of gathering information on the target. We know for a fact, methodology to be revealed later, that the attacker worked primarily from an IP address of 81.181.196.115 and that this machine is located on a Romanian net block.

We have a unique view into this phishing attack. We have the web server's access logs as far back as mid-July 2005 and can easily search for any access from the 81.181.0.0/16 range.

Sure enough, on August 11 at 06:45, the user at 81.181.196.115 visited the bank's real home page and then quickly left. We believe that this event marks the beginning of the attacker's interest in the bank. The plans to launch an attack against the bank were formulated several minutes before or very shortly after the following log entry was made:

```
81.181.196.115 - - [11/Aug/2005:06:45:17 -0400] "GET / HTTP/1.1" 200 19637 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

Unless visiting from a net block other than 81.181.0.0/16 (which would make it almost impossible for us to know), the attacker did not come back until August 23. At 08:21, the user visited the home page once more, and quickly left. By this time, most of the planning and staging has likely been completed. The attacker probably came back to update their copy of the web site with any details that the real site had implemented since the 11th.

```
81.181.196.115 - - [23/Aug/2005:08:21:42 -0400] "GET / HTTP/1.1" 200 19637 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

On August 24 at 20:14, the web site was visited by a second Romanian IP address, but made only this single request to the web server.

```
81.181.45.38 - - [24/Aug/2005:20:14:12 -0400] "GET / HTTP/1.0" 301 300 "-" "-"
```

At 20:14 EST, it is just past 5 AM in Romania. Note there is no referrer string (one of the empty "-" entries), meaning the user was not browsing a web site prior to accessing the bank's real home page. Furthermore, there is no User Agent (ie browser type), which is normally hard coded into the browser application's software. Perhaps the most interesting characteristic of this log file entry is the 301 status code and the HTTP 1.0 version being used.

The bank's real web site sends back a permanent redirect command for the visiting browser to address it's request to the HTTPS (SSL secured) version of the web site. Apparently the user on the other end of this connection does not have an SSL-enabled browser (it didn't follow the request), making it likely to have been an old command line, text based browser or custom script.

This event is very strange and currently unexplained. The hits on August 11 and August 23 showed a user from the same IP address visiting the home page from the same browser, in the early afternoon. Now we see a user visit the site from a different IP address, with what is most likely not even a GUI browser and is old enough to request HTTP 1.0 protocol by default. On top of all this, it occurs in the middle of the night and for seemingly no good reason.

All is quiet on the 25 of August, likely while the near final web site mock-up was being fine tuned (we learn later that there was *nothing* fine about this deployment). Around 05:00, the attacker visits the bank's real home page from the primary IP address of 81.181.196.115. Concurrently, a new address (81.181.175.28) steps into the picture and accesses nearly the exact same content as the primary.

Then, at 08:08, the user at 81.181.196.115 pulls up the bank's personal-banking.php page without ever

going to the home page first (as if clicked from a bookmark). The critical factor in this log entry is the referrer string of secure-activ.html:

```
81.181.196.115 - - [26/Aug/2005:08:08:29 -0400] "GET /personal-banking/personal-
banking.php HTTP/1.1" 200 22867
"http://200.213.21.5/menu/imagens/www.obfuscated.com/secure-activ.html" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

If you don't understand the significance of this referrer, think about it in human interaction/networking principles. Your friend Bob gives you Allison's number. When you call Allison for the first time, you explain that you got her number from Bob. Bob is the referrer; Bob is the person you were talking to right before calling Allison. Back to the log file – this user's browser was on a page named secure-activ.html, at the specified path above, hosted on the server located at 200.213.21.5 *just before* accessing the bank's personal-banking.php page.

This proves that as early as 08:08, the phishing site was online, publicly accessible, and programmed to link back to the real site upon submission to the data form. One other factor provides some insight into the attacker's methodology and planning routines. At 08:08, the fraudulent web site was still under construction. The URL in the referrer string shows that secure-activ.html resided in a directory on the server named “www.obfuscated.com,” however this was edited to just “obfuscated” before the attacker began distributing emails with the URL embedded into them.

In the moments following 08:08, the attacker made the decision to change that URL above, and then sent himself a test email. As early as 08:17, the attacker was viewing the phishing email from his primary computer:

```
81.181.196.115 - - [26/Aug/2005:08:17:10 -0400] "GET /images/logo.gif HTTP/1.1" 304 -
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

81.181.196.115 - - [26/Aug/2005:08:19:00 -0400] "GET /images/logo.gif HTTP/1.1" 304 -
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

81.181.196.115 - - [26/Aug/2005:08:22:16 -0400] "GET /images/logo.gif HTTP/1.1" 304 -
"-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

We were able to single out these three particular requests because they were completely out of spec from normal browsing patterns and occurred consecutively. Over the 5 minute period (08:17 – 08:22), the remote computer requested the same file, which happens to be the bank's logo, 3 times in a row. Furthermore, this was a direct request, it was not pulled down as a result of the logo being embedded in another web page that the browser requested. What could cause this type of behavior?

The answer is that this image on the real bank's web site is linked to from within the phishing email. Anyone who views the email, upon their email client rendering the message, will end up fetching the logo.gif file - and *only* the logo.gif file.

Keep in mind that the testing we refer to is occurring on two machines: both 81.181.196.115 and 81.181.175.28 are producing similar entries in the real bank's access logs. At 08:45, the .28 address hits logo.gif from a Yahoo mailbox:

```
81.181.175.28 - - [26/Aug/2005:08:45:45 -0400] "GET /images/logo.gif HTTP/1.1" 304
"http://us.f304.mail.yahoo.com/ym/ShowLetter?box=Inbox&MsgId=3914_12240882_134332_127
9_1029_0_4793_2572_450994382&Idx=0&Search=&PRINT=1&ShowImages=&YY=62069&order=down&so
rt=date&pos=0&view=a&head=b" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)"
```

Shortly thereafter, the attacker at .28 does a few very strange things. First, he connects to the site looking for Frontpage extensions and then submits a completely empty form to the bank's contact page.

```
81.181.175.28 - - [26/Aug/2005:09:02:15 -0400] "POST /_vti_bin/shtml.exe/_vti_rpc
HTTP/1.1" 403 310 "-" "MSFrontPage/5.0"
```

```
81.181.175.28 - - [26/Aug/2005:10:14:55 -0400] "POST /cgi-bin/FormMail.pl HTTP/1.1"
200 914 "https://www.obfuscated.com/contact/contact.php" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1; SV1)"
```

These are likely efforts to find weaknesses in the server itself or scripts on the legitimate web site. Based on the 403 status code of the Frontpage requests, we know the attacker did not gain access to this service. Likewise, based on the 914 byte return from the FormMail submission, we know the attacker didn't fill out any of the fields (the return page echoes back the entered data and 914 bytes is the empty template).

From this point on, we see no more access from the .28 address.

The Ironwindow Incident

Continuing in time line fashion, it's somewhere between 10:15 and 10:25.

Two interesting events are forthcoming in the next few minutes. At 10:27, the .115 primary address accesses the bank's security.php page. Likely they are looking for notices of detection from the past few days or to review the bank's previous security warnings. At 10:30, we then see this address access logo.gif from a completely new referrer:

```
81.181.196.115 - - [26/Aug/2005:10:30:46 -0400] "GET /images/logo.gif HTTP/1.1" 200
3006 "http://ironwindow.org/obfuscated.htm" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1)"
```

The “what” is easy, but the “why” is unclear. It's a URL that points to a primitive copy of the HTML code used to build the phishing emails. A few clues indicate that this is simply a template used by the Romanian crew. For instance, much of the email is still customized for LaSalle Bank:

```
<a target="_blank"  href="http://www.antoq.com/lasell/index.html" >
https://www.obfuscated.com/personal-banking/personal-banking.php</a></span></b><br>

<img alt="Member FDIC" hspace="0"
src="http://www.lasallebank.com/templates/images/fdic_home.gif"  border="0"
width="19" height="15">
```

Likewise, a bundle of the code is still customized for the last phishing attack against eBay:

```
<form target="_blank"  method="POST"
action="http://mail.yahoo.com/config/login?/ACTIUNEAIS">
<input type="hidden" size="30" name="id" value="124">
<input type="hidden" size="30" name="mailuser" value="EMAILADDRESSIS">
<input type="hidden" size="30" name="ebay_user_id" value="test">
```

Without a doubt, the system hosting www.antoq.com was compromised by these attackers and used as the staging grounds for a phishing attack against LaSalle bank and eBay in the very recent past. At the time of this writing, www.antoq.com no longer resolves and is has been removed from many of the Whois databases. However, Miller's Miles archives a phishing report against Washington Mutual, which used to reside at http://www.antoq.com/wamu/index.html [1]. Likewise, MCSE forums archives one against PayPal, also hosted on what used to be www.antoq.com, [2].

The attackers are so sloppy that they have practically told us which other institutions they have been targeting. It's also obvious that they don't know a thing about HTML: the closing </form> tag is actually written *after* the closing </html> tag. You also may notice 3 large submit buttons in the body of the circulating email labeled 124, EMAILADDRESSIS, and test. These are actually remnants from the eBay phishing exploit, and the attackers didn't remove that section of HTML from the code.

We will revisit the paths uncovered by the Ironwindow incident, however it provides no further information relevant to this section. We currently have no idea why the .115 primary computer accessed this URL during this phishing attack. We believe it may have been an accident – one of the most costly

accidents the attackers could possibly have made, short of mailing us their drivers license and a signed statement of guilt.

Public Release of Phishing Emails

Back to the time line, phishing emails have been publicly released. The time between 10:31 and 10:35 marked the beginning of email distribution. The first occurrence of logo.gif being accessed from an email inbox, by someone other than the Romanians, was at 10:35:53 by someone with a Hotmail account:

```
200.x.x.x - - [26/Aug/2005:10:35:53 -0400] "GET /images/logo.gif HTTP/1.1" 200 3006
"http://by14fd.bay14.hotmail.msn.com/cgi-bin/getms
g?msg=MSG1125066943.7&fti=yes&curmbox=F000000001&a=89b6804c5d5cfbddaf7d07179605471346
f3eeb0d3d07a10ff54f6a6ab61a174" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)
```

Reporting and Seeking Assistance

Incredibly, less than 15 minutes after the email distribution began, a non-member of the bank, reported the fraud. The reported email was forwarded from an Earthlink account, which means the first person to view the phish (using Hotmail) was not the first person to report it. This report came in at 10:42, not even a minute after this log file entry:

```
69.x.x.x - - [26/Aug/2005:10:41:12 -0400] "GET /images/logo.gif HTTP/1.1" 200 3006
"https://webmail.pas.earthlink.net/wam/msg.jsp?msgid=3008&folder=INBOX&x=815176418"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

At 12:13 an email was sent to the Brazilian CERT – the ISP for the compromised server hosting the fraudulent web site.

```
The server which IP address 200.213.21.5 is hosting files used in a phishing attack
against a financial institution in the United States.

The offending files are located at http://200.213.21.5/menu/imagens/obfuscated/
```

Then, more important things surface, like the first user to make a submission to the fraudulent web site:

```
216.x.x.x - - [26/Aug/2005:12:43:29 -0400] "GET /personal-banking/personal-
banking.php HTTP/1.1" 200 22867 "http://200.213.21.5/menu/imagens/obfuscated/secure-
activ.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

We have no way of knowing who this user is and what data they submitted – if any. It could be someone completely naive who filled out the form in entirety; or it could be someone who just wanted to get a good laugh and see where clicking 'submit' would lead. Quite possibly, the user entered something crazy, or simply left the form blank, because less than 10 minutes later the attacker made a submission himself. We initially thought the attacker was checking to see if the exploit was still online and in working order, however on second thought – why would the attacker need verification if someone had just submitted data less than 10 minutes ago? Is the attacker troubleshooting?

```
81.181.196.115 - - [26/Aug/2005:12:52:16 -0400] "GET /personal-banking/personal-
banking.php HTTP/1.1" 200 22867 "http://200.213.21.5/menu/imagens/obfuscated/secure-
activ.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

Initial Recovery Reactions

On the time line we're at about 12:55. By 13:00, There is now an attention-grabbing warning on the home page of the real bank's site as well as the personal-banking.php page (which is the first thing a user would see if they submit data to the fraudulent form). Once again, the attackers made the mistake of redirecting browsers to the legitimate live web site after submission. This is great because the bank is allowed the opportunity to throw up a flag right in the face of anyone who submits and let them know what just happened.

At approximately 13:06 PM, the Brazilian CERT takes the phishing web site offline.

```
Security-Embratel - Ticket

Sirs,

As requested the URL was removed.

--
Internet Security Team
Network Operation Center
EMBRATEL - BRAZIL
```

The Reprise Campaign

The attackers aren't ready to give up yet. As soon as 13:45 the fraudulent web site is back online, restored with the original files. The Brazilian CERT is contacted once again, with information of the bounce back. The time line events from this point on are not substantial. Staffing of the service providers in Brazil on weekends is noted as an extremely limiting factor by the take down teams. Perhaps the attackers launched the exploit on a Friday for this very reason (I never said they were dumb, just that they made a lot of mistakes).

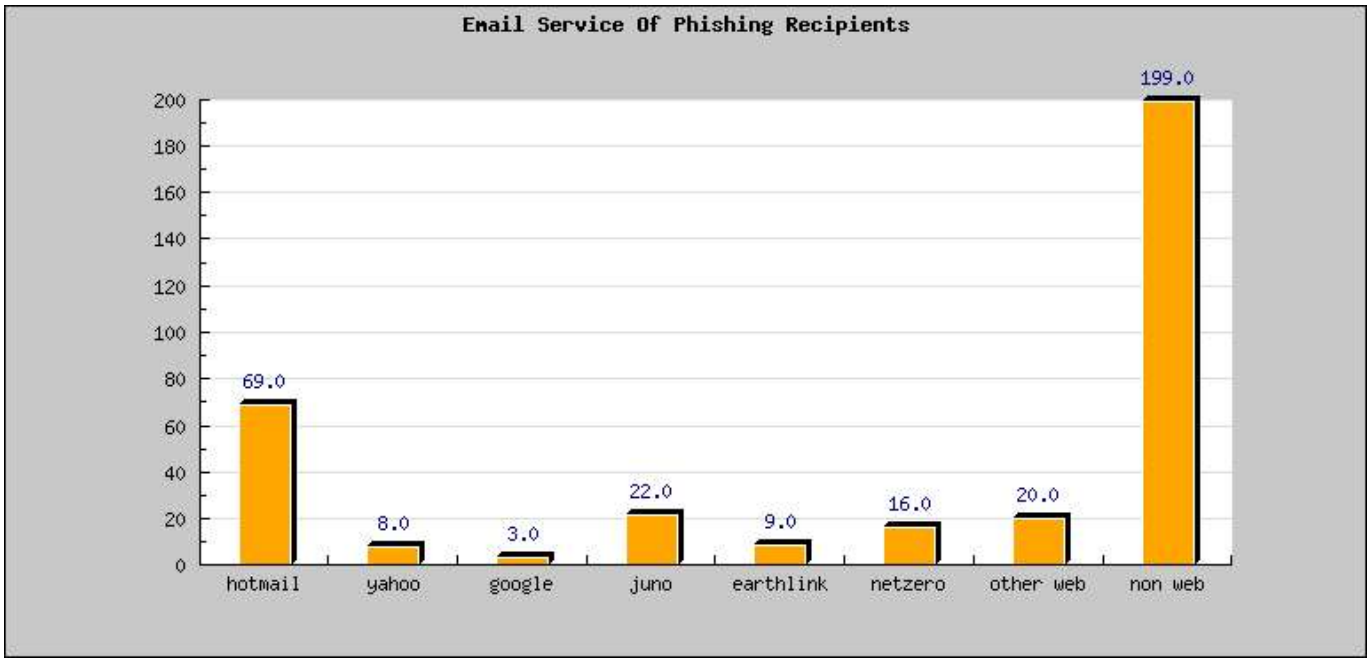
Meanwhile, we have a lot more to tell.

Classification of Phishing Recipients

As previously mentioned, anyone who views the email, whether by web mail clients or MUAs like Outlook, will produce an entry in the legitimate web server access log. These hits will be unique and easily distinguishable from normal users who access the logo as part of normal browsing. The difference is that the email recipients will only produce one access log entry - the image itself, with either no referrer entry or an entry that identifies the web mail client used to view the email. Furthermore, legitimate access of the bank's logo should only occur as a result of browsing the web site pages on the legitimate site, which would produce an access log entry with a referrer of www.obfuscated.com. On that assumption, we can extract the list of IP addresses which accessed logo.gif *without* a referrer of www.obfuscated.com.

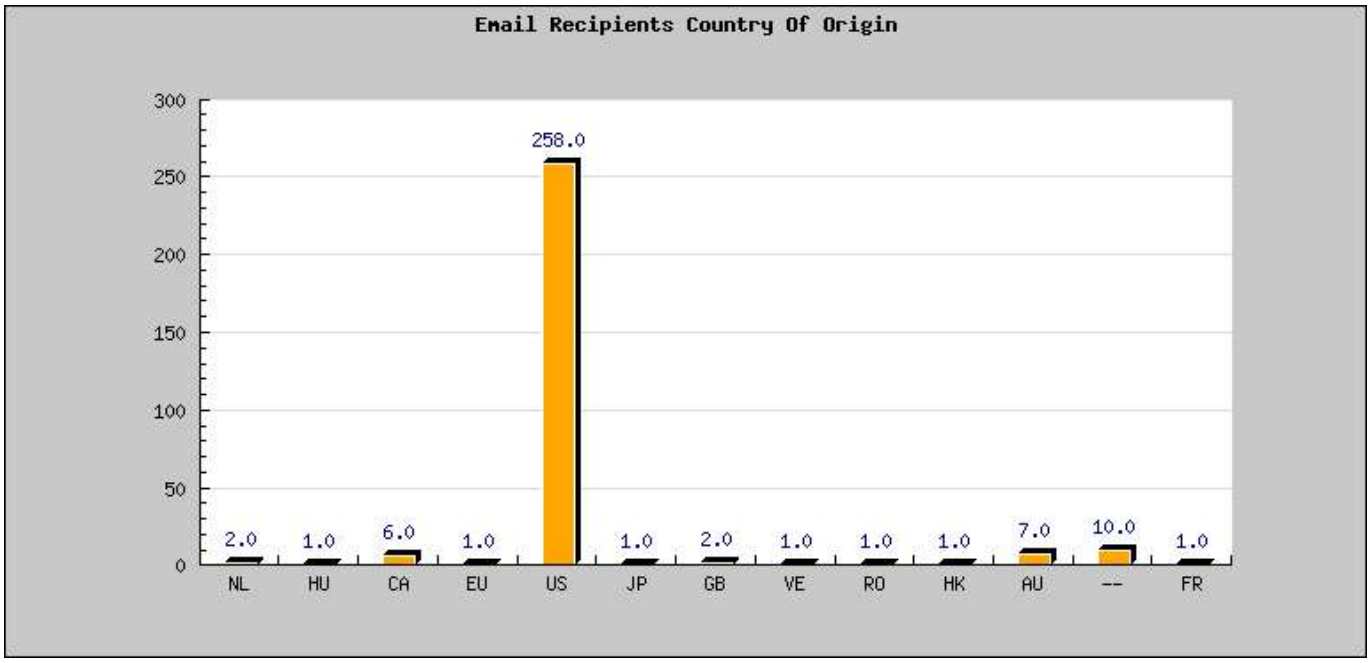
Based on the referrer strings in these access logs, we can build a profile of the email services used by recipients of the phishing email.

To view the Perl and PHP scripts used to generate the data, view Appendix C – Data Analysis Scripts.



One aspect of this attack that we still do not know is – how did the attacker's harvest this list of email addresses? Was it a randomly generated list, taken from other records online, or did they have some other source? We may never know, but this profile may help with correlation in the event that we do come across some possibilities in the future. This question is brought up again in the Unanswered Questions.

The next graph shows a profile of countries in which the email recipients viewed their message. Users in at least 12 unique countries were exposed to this phishing attack, with the majority being in the United States. Ten addresses were either unknown or not able to be resolved correctly (signified by the "--" country code).

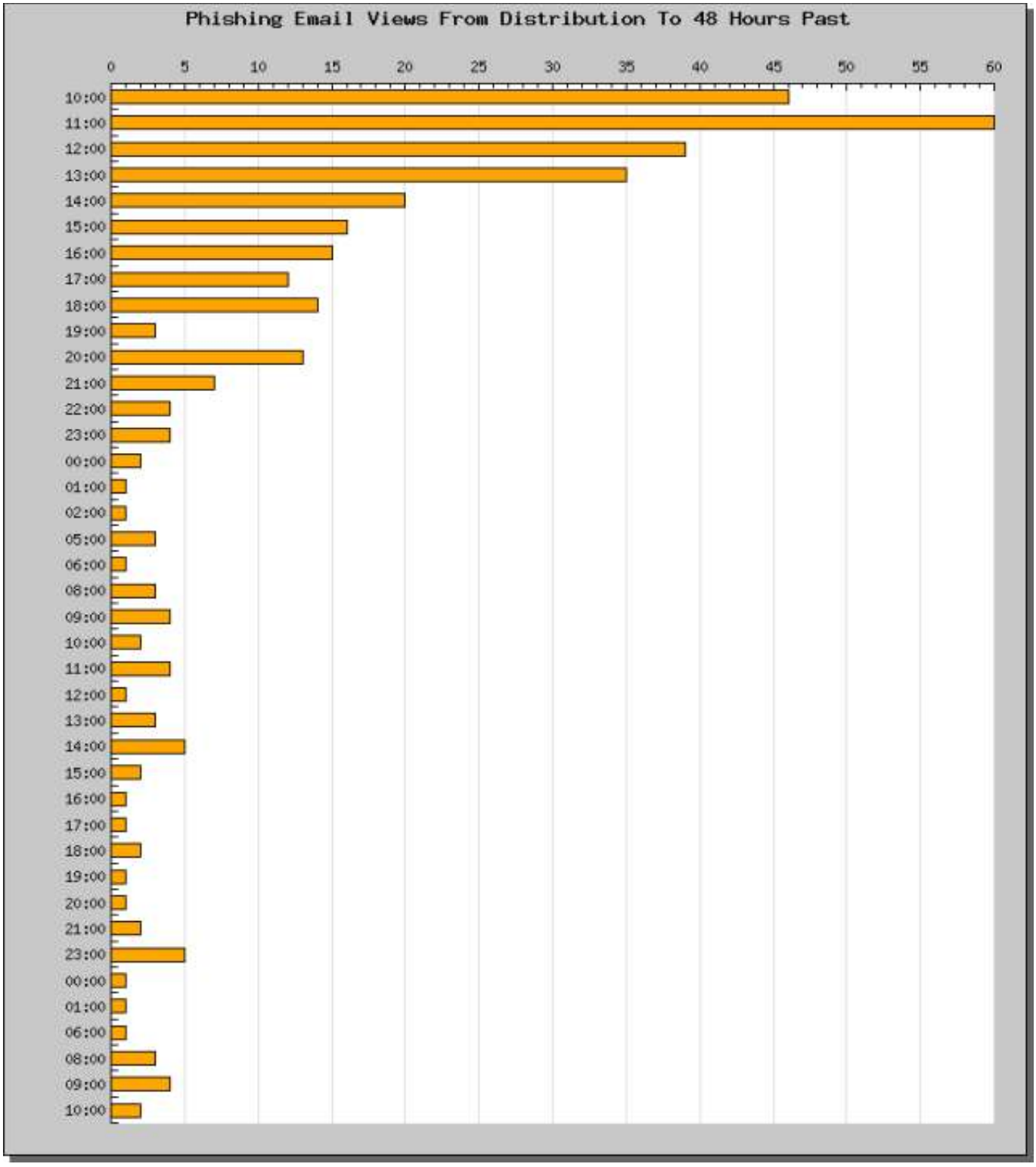


Resolution of these addresses was done using the Geo::IPfree module for Larry Wall's Perl coding language.

Legend:

```
NL, Netherlands
HU, Hungary
CA, Canada
EU, Europe
US, United States
JP, Japan
GB, United Kingdom
VE, Venezuela
RO, Romania
HK, Hong Kong
AU, Australia
FR, France
```

The final graph shows the phishing email's popularity, from the hour it was released to 48 hours later.



Timeline begins at 10:00 EST on August 26 and traces through 10:00 EST on August 28. Null hours are not shown (if there were no hits, the hour is not represented on the vertical axis). We know via other means that the first phishing emails were released at 10:30 (give or take) on the 26th. The data in this graph correlates with this fact. The number of hits during the August 26 work day were high, and began to trail away around 5 and 6 PM EST. Throughout the remainder of the weekend, between zero and five users per hour viewed the email (world wide). There have not been any additional submissions to the secure-activ.html form.

Sites and References

[1]. http://www.millersmiles.co.uk/report/782

[2]. http://www.mcse.ms/archive177-2005-6-1679884.html

[3]. The Romanian Wikipedia http://ro.wikipedia.org/wiki/Pagina_principal%C4%83

[4]. The Romanian Google Engine http://www.google.ro

[5]. Online Romanian Dictionary http://www.castingsnet.com/dictionaries

[6]. An archived copy of the phishing email template on a French bulletin board, before it was actually turned into a template by the Romanians (only available via Google cache):

http://64.233.161.104/search?q=cache:0RB_bfdow2kJ:newffr.com/viewtopic.php%3Fsess_id%3Dc7f98aaa49e745d3c083737875c69d3b%26forum%3D26%26topic%3D8670+%22%3Cinput+type%3D%22hidden%22+size%3D%2230%22+name%3D%22ebay_user_id%22+value%3D%22test%22%3E%22&hl=en

Appendix A – Whois Records

81.181.196.115, The Romanian Primary

```
inetnum:      81.181.196.0 - 81.181.197.255
netname:      SC-WORLDNET-COMUNICATII-SRL
descr:        SC WorldNet Comunicatii SRL
descr:        Str. Babadag Nr 14, bloc 8 Parter.
descr:        Tulcea, Romania
country:      ro
admin-c:      LS2095-RIPE
tech-c:       LT849-RIPE
status:       ASSIGNED PA
mnt-by:       AS3233-MNT
mnt-lower:    AS3233-MNT
mnt-routes:   WORLD-MNT
notify:       hostmaster@rnc.ro
changed:      hostmaster@rnc.ro 20050105
source:       RIPE

person:       Laurentiu Simion
address:      Valea Ialomitei, Nr 1A, Bl
address:      C18a, Sector 6 ,
address:      Bucuresti.
phone:        +40-723-606000
e-mail:       laur@world-net.ro
nic-hdl:      LS2095-RIPE
notify:       lucian@worldnettl.ro
mnt-by:       WORLD-MNT
changed:      lucian@worldnettl.ro 20040702
```

```
source:       RIPE

person:       Lucian Timofanovici
address:      Str Babadag Nr14, Bloc 8 ,
address:      Parter
phone:        +40-724-302000
e-mail:       lucian@worldnettl.ro
nic-hdl:      LT849-RIPE
notify:       hostmaster@rnc.ro
mnt-by:       AS3233-MNT
changed:      hostmaster@rnc.ro 20040702
source:       RIPE

% Information related to 'LS2095-RIPE'

route:        81.181.196.0/23
descr:        WorldNET
origin:       AS12752
mnt-by:       WORLD-MNT
changed:      lucian@worldnettl.ro 20050127
source:       RIPE
```

200.213.21.5, The Brazilian Capture Server (www.dnsstuff.com)

```
inetnum: 200.213.21.0/26
aut-num: AS4230
abuse-c: GSE6
owner: Braum & Lucas Ltda
ownerid: 003.223.376/0001-53
responsible: Claudio Luis Braum
address: Travessa Natal, 43,
address: 96825-160 - Santa Cruz do Sul - RS
phone: (51) 3711-1478 []
owner-c: CLB266
tech-c: TCV
created: 20001023
changed: 20001023
inetnum-up: 200.213/16

nic-hdl-br: CLB266
person: Cláudio Luís Braum
e-mail: c_mudras@hotmail.com
created: 20030119
changed: 20030930

nic-hdl-br: GSE6
person: Grupo de Segurança Internet da Embratel
e-mail: abuse@embratel.net.br
created: 20001005
changed: 20001005

nic-hdl-br: TCV
person: Tiberius Cesar Galhardo de Vasconcellos
e-mail: galhardo@adinet.com.uy
created: 19981126
changed: 20050205

remarks: Security issues should also be addressed to
remarks: cert@cert.br, http://www.cert.br/
remarks: Mail abuse issues should also be addressed to
remarks: mail-abuse@cert.br
```

200.213.21.5, The Brazilian Capture Server (www.whois.sc)

```
inetnum: 200.128/9
status: allocated
owner: Comite Gestor da Internet no Brasil
ownerid: BR-CGIN-LACNIC
responsible: Frederico A C Neves
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR
```

```
phone: +55 11 9119-0304 []
owner-c: CGB
tech-c: CGB
inetrev: 200.128/9
nserver: A.DNS.BR
nsstat: 20050825 AA
nslastaa: 20050825
nserver: B.DNS.BR
nsstat: 20050825 AA
nslastaa: 20050825
nserver: C.DNS.BR
nsstat: 20050825 AA
nslastaa: 20050825
nserver: D.DNS.BR
nsstat: 20050825 AA
nslastaa: 20050825
nserver: E.DNS.BR
nsstat: 20050825 AA
nslastaa: 20050825
remarks: These addresses have been further assigned to Brazilian users.
remarks: Contact information can be found at the WHOIS server located
remarks: at whois.registro.br or at http://whois.registro.br
created: 19950104
changed: 20020902

nic-hdl: CGB
person: Comite Gestor da Internet no Brasil
e-mail: blkadm@NIC.BR
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR
phone: +55 19 9119-0304 []
created: 20020902
changed: 20050621
```

208.182.x.x, The Bledsoe County Library Computer

```
OrgName:    State of Tennessee Department ofEducation
OrgID:      STDO
Address:    710 James Robertson Parkway
Address:    7th Floor
City:       Nashville
StateProv:  TN
PostalCode: 37243
Country:    US

NetRange:   208.182.0.0 - 208.183.255.255
CIDR:       208.182.0.0/15
NetName:    TEN-NASH
NetHandle:  NET-208-182-0-0-1
Parent:     NET-208-0-0-0-0
NetType:    Direct Assignment
NameServer: NS1.ENA.COM
NameServer: NS2.ENA.COM
Comment:
RegDate:    1999-06-21
Updated:    2003-04-16

AbuseHandle: ARA15-ARIN
AbuseName:   Abuse Role Account
AbusePhone:  +1-615-312-6200
AbuseEmail:  abuse@ena.com

NOCHandle: NOC115-ARIN
NOCName:   NOC
NOCPhone:  +1-615-312-6200
NOCEmail:  hostmaster@ena.com

TechHandle: LC682-ARIN
TechName:   Cothron, Lisa
TechPhone:  +1-615-532-2818
TechEmail:  lisa.cothron@state.tn.us
```

```
OrgTechHandle: NOC115-ARIN
OrgTechName:   NOC
OrgTechPhone:  +1-615-312-6200
OrgTechEmail:  hostmaster@ena.com
```

Appendix B – Key Players Timeline

This timeline is directed at the key players in the exploit. There are three Romanian IP addresses used in planning and staging the attack. Their steps are outlined below.

```
August 11
  81.181.196.115
    visits home page, leaves
August 23
  81.181.196.115
    visits home page, leaves
August 24
  81.181.45.38
    visits home page with http 1.0 browser, gets http 301
    fails to follow perm. https redirection
    probably using a text based or custom cli client w/o ssl
August 26
  81.181.175.28
    05:13:57 accesses home page, leaves
    05:34:19 accesses home page, leaves
    05:53:14 goes directly to personal-banking.php
    from then until 06:17:29, gathers a lot of the other pages (ie locations.php,
      etc)
    08:22:48 visits home page, follows link to personal banking login
    08:45:21 accesses logo.gif ONLY from yahoo mail referrer string
      the attacker is testing their email, by sending the phish to their own yahoo
      email account (3x more times before 10:23:14)
    09:02:13 attacker visits site with new referrer (frontpage 5.0) looking for
      shtml.exe
    10:14:55 atacker clicks submit on the bank's contact us form, 914 bytes returned
      to browser (empty form)
  81.181.196.115
    05:19:05 accesses home page, leaves
    08:08:29 goes directly to personal-banking.php WITH REFERRER of secure-activ.html
    08:16:07 accesses home page, leaves
      between 08:17:10 and 08:22:16 accesses logo.gif 3 times through a !webbased
      MUA (no referrer)
    08:23:57 visits home page, leaves
    08:27:27 goes directly to personal-banking.php
      from then until 08:29:24 accesses logo.gif 3 times through a !webbased MUA
      (no referrer)
    08:30:41 goes directly to personal-banking.php
      from then until 08:38:45 accesses logo.gif 3 times through a !webbased MUA
      (no referrer)
    08:38:45 accesses logo.gif from yahoo webmail inbox
      from then until 08:55:28 accesses logo.gif about 5 times each through non
      web based MUA and also via yahoo web mail
    from then until 10:27:42 does general browsing of the web site pages,
      security.php in particular, (probably looking for notices)
    10:30:46 accesses logo.gif from http://ironwindow.org/obfuscated.htm (this is
      critical)
    12:52:16 goes directly to personal-banking.php WITH REFERRER of secure-activ.html
      (testing again)
```

Appendix C – Data Analysis Scripts

This Perl script accepts web server access logs as input and produces a profile for email client (based on referrer), country code (based on IP address), and day/time of the visit. It also outputs code to cut and

paste into graphing library functions.

```
#!/usr/bin/perl

use Switch;
use Geo::IPfree;

sub numerically { $a <=> $b; }

# popular clients we want to quantify

@known_clients = ('hotmail', 'yahoo', 'google', 'juno',
  'earthlink', 'netzero');

open(A,"email_client_logs.txt") or die "no file: $!";

while(<A>) {
  ($ip,$date,$refer) = split;
  next if ($ip =~ (/^81\.181\./);
  # only take unique addresses, but count the total
  $addr{$ip}++; $samples++;
  if ($date =~ /\[((\d){2})\/Aug\/2005:((\d){2})/) {
    $daytime{$1}{$3}++;
  }
  $refer =~ s/\"//g;
  # blank refer as result of non web based email client
  if ($refer =~ /^$/ or $refer =~ /^\s?\-\s?$/) {
    $other_nonweb++;
  }
  else {
    LOOP: foreach $i (@known_clients) {
      if ($refer =~ /$i/) {
        $clients{$i}++; $recognized++; next LOOP;
      }
    }
  }
}
close(A);

$other_web = $samples - ($recognized + $other_nonweb);

#
# prepare to output client email level data
#

print "\nEmail Client Profile...Coming Up...\n\n";

foreach $i (@known_clients) {
  print "$i = $clients{$i}\n";
}
print "other (web) = $other_web\n";
print "other (non web) = $other_nonweb\n";

print "\nWhy don't you just go ahead and cut cut and\n",
"paste this into jpgraph, mmmmkkkay?\n\n";

$graph_client_name = '$clients=array(';
$graph_client_numb = '$databary=array(';

foreach $i (@known_clients) {
    $graph_client_name .= "\"$i\",";
    $graph_client_numb .= "$clients{$i},";
}

$graph_client_name .= "\"other web\",\"non web\"";
$graph_client_numb .= "$other_web,$other_nonweb";

$graph_client_name .= ');';
$graph_client_numb .= ');';

print "$graph_client_numb\n";
print "$graph_client_name\n";
```

```
#
# prepare to output country level data
#

print "\nCountry Profile...Coming Up...\n\n";

foreach $i (keys %addr) {
  ($country,undef) = Geo::IPfree::LookUp("$i");
  $co{$country}++;
}

foreach $cc (keys %co) { print "$cc = $co{$cc}\n"; }

print "\nIf you could just go ahead and paste this too,\n",
"that would be greeaaat. Thanks...\n\n";

$graph_country_code = '$country=array(';
$graph_country_numb = '$databary=array(';

foreach $cc (keys %co) {
  $graph_country_code .= "\"$cc\",";
  $graph_country_numb .= "$co{$cc},";
}

$graph_country_code .= ');';
$graph_country_numb .= ');';

print "$graph_country_code\n";
print "$graph_country_numb\n\n";

#
# prepare to output daytime level data
#

print "View By Day/Hour Profile...Coming Up...\n\n";

$graph_daytime_code = '$daytime=array(';
$graph_daytime_numb = '$databary=array(';

foreach $a (sort numerically keys %daytime) {
  foreach $b (sort numerically keys %{ $daytime{$a} }) {
    $graph_daytime_code .= "\"$b\",";
    $graph_daytime_numb .= "$daytime{$a}{$b},";
    print "$a/$b:00 - $daytime{$a}{$b}\n";
  }
}

$graph_daytime_code .= ');';
$graph_daytime_numb .= ');';

print "\nHow about that report?\n\n";

print "$graph_daytime_code\n";
print "$graph_daytime_numb\n";
print "\n\n";
```

This is one of the three graphing functions. It takes the input of the script above and produces a JPEG image with the plotted data.

```
<?

include "../jpgraph/src/jpgraph.php";
include "../jpgraph/src/jpgraph_bar.php";

// Some data
$databary=array(59,25,4,21,9,11,22,226);
$clients=array("hotmail","yahoo","google","juno","earthlink","netzero","other
web","non web");

// New graph with a drop shadow
$graph = new Graph(768,368,'auto');
$graph->SetColor("white");
```

```
// Use a "text" X-scale
$graph->SetScale("textlin");

// Specify X-labels
$graph->xaxis->SetTickLabels($clients);
$graph->xaxis->SetTickLabels($clients);

// Set title and subtitle
$now = time();
$graph->title->Set("Email Service Of Phishing Recipients");

// Use built in font
$graph->title->SetFont(FF_FONT1,FS_BOLD);

// Create the bar plot
$b1 = new BarPlot($databary);
$b1->SetColor("white");
$b1->SetFillColor("orange");
$b1->value->show();
$b1->SetShadow();

// The order the plots are added determines who's on top
$graph->Add($b1);

$graph->Stroke();

?>
```

Appendix D – Secure-activ.html Source Code

This is a sample of the Secure-activ.html page for proof of another targeted organization.

```
<!--
 HTML Name:             retail_sign_on.HTML
 Version:               4.5.71 - 50
 Change Activity:
 Date           Flag            Description
-----------------------------------------
        NA      C                       Created
10/06/2003  M_10062003_PPK   Xtn in progress changes
-->
<HTML>
<!-- Lotus Domino Web Server (Release 4.6a - Nov 13 1997 on AIX) -->
<!-- Style Sheet related changes - 11/14/2003 --><HEAD>
<TITLE>Sky Online Personal Banking</TITLE>
<style>
<!--
    *  {font-family: Arial, Helvetica, sans-serif; font-size:10pt; }
-->
</style>
</HEAD>
```

Unanswered Questions

1. We don't know why the Romanian primary visited the template at ironwindow.org during the morning of August 26.

2. We don't know why the template from ironwindow.org has unused form tags and submit buttons. We can only speculate sloppiness and lack of experience with HTML on the attacker's part.

3. We don't know the significance of the “http://mail.yahoo.com/config/login?/ACTIUNEAIS” strings in the ironwindow.org template.

4. We don't know how the attackers harvested the list of emails to which they wanted to distribute the phishing emails.

5. We don't know how the attackers became interested in this bank in the first place.

6. We don't know how many other institutions (besides the 5 already identified) that this group has targeted or who they plan to attack in the near future.

7. We don't know what the enroll.php script does with the data submitted to secure-activ.html. Presumably it emails it off to the attackers or stores it locally on the compromised server for the attackers to fetch. An archived copy of the "obfuscated" directory would really help with this.

8. We don't know a breadth of things about the attackers themselves, but the Ironwindow incident, we hope, is going to reveal more than enough.

Zona-Garii and the Ironwindow

Through the attacker's sloppiness and our attention to detail, we have what we believe to be a legitimate lead into who these people really are. It all started with the Romanian primary address visiting the phishing template off the root directory of ironwindow.org. This URL was not distributed in the emails, thus there is no reason to believe anyone other than the attackers, who staged it themselves, would have any idea where to find this page. Furthermore, we do have correlation with the user's source IP, which matches that of the address used to conduct reconnaissance on the real bank's web site.

It has crossed our minds that ironwindow.org and it's associated party is an innocent bystander, but we're convinced this is not the case. This site is simply used for the attacker to preview the appearance of the phishing email before sending it out. It makes perfect sense for the attackers to compromise an innocent server for which to host the fraudulent site, but would it make sense to go through the trouble of compromising another site just to see what the email will look like through a browser? We think that through pure laziness and desire for convenience, the attackers threw this template up on a site that they readily and normally have access to.

At this point, there is a high degree of speculation and circumstantial evidence. We aren't going to prove guilt with a theory or two about who owns some web site. That's when we found the pictures. Ironwindow's main attraction is a gallery of photographs, many of which reveal some interesting facts that correspond with our expectations.

In the background of an image entitled alecu.jpg, we identified a map of the Romanian territory:

In the background of an image entitled mkdir-iron.jpg (Iron is believed to be a nickname of one of the involved persons), we identified a calendar with the Romanian language. Noiembrie in Romanian is obviously November in English.

In an image entitled CucuBau.jpg, three boys stand in front of a vehicle which displays the license plate and Romanian emblem:

In an image entitled ana0.jpg, a female poses for the camera, but with a Romanian flag on the wall behind her:

Next, a series of computer screen shots show a large amount of information. They reveal the Yahoo Messenger screen names, preferred nicknames, and popular IRC channels. The channel is #Zona-Garii, a term displayed on the top of the Ironwindow home page. Some of the key players seem to be Cosmin (cosminhack), Iron (adryanproject), Cimino (catalin_mr_cimino), jamelia_89, strumphitzu, and rona_ioana.

We also see shortcuts to Yahoo mail on the desktops of these screen captures. When the phishing email was being testing, it was done so via Yahoo inbox. Despite the millions of Yahoo users, this is just another factor in the overall equation that seems to make perfect sense.

The images are entitled AncaIt.jpg, curuLuSoarec, jpg, RonaWebcam. jpg, ursurupetot.jpg, and tare.jpg, respectively. Once again, only snippets are shown here – Appendix Z.iv has the original images.


rona}{ (rona_ioana) -- Instant Message
Conversation Edit View Contact Help
Webcam Games Voice Send File Photos Conferen
rona}{ - View My Webcam
rona}{: ejti ?
iron: ada
rona}{:
iron:
rona}{: dc ejti pe invisible?>
iron: ma ascund de lume


Cimino (catalin_mr_cimino) -- Instant Message
Conversation Edit View Contact Help
Webcam Games Voice Send File Photos Confer
Cimino -ADRIAN - TRENUL VIETII www.lunch.org/p
BUZZ!!!
iron: camu.
Cimino : ce draq te mint pa tine
Cimino :
Cimino 's status is now "ADRIAN - TRENUL VIETII ww
Cimino : ce draq te mint pa tine


adryanproject - Invisible to Everyone
Messenger Address Book
Add IM Text Chat
-=[*iron SeedS*]=- (12/144)
amy4u - Invat!Nu deranjati! [nothing] 04:00
Asterix
Baby_me - Cream & C.R.B.L - Nu din prima seara
cosmicom2000 -
D3n3m0na - Be cool instantly!
DJ-VLAD - 50 CENT - In da club
Doina - hm... traiasca vacanta, ca mai e mult pana la ea
Gyovanni - Be cool instantly!
Impal3r - Cacatu de Cupidon cand A vrut sa traga in mi
iulio - Be cool instantly!
slash
Vik
Yahoo! Help (1/1)
YahooHelper


mIRC - [#zona-garii [...
My Webcam (jamelia_...
cosmin (cosminhack) ...
iron (adryanproject) ...

I'm convinced the operators of Ironwindow.org are Romanian, though still nothing proves their involvement in the phishing attacks. Is it all just a big coincidence? These young people definitely fit the hacker stereotype. The setting for many of these photographs is a small computer lab or around one of the user's desktop computers. If nothing else, these images prove that the lifestyles of these people would support their ability to plan and execute phishing attacks and other forms of online computer crime. Once again, they aren't guilty – yet.

There is some unexplained code in Ironwindow's home page:

```
<INPUT TYPE=HIDDEN NAME=pwd VALUE="SoulS">
```

We don't have any clues as to the reason this code exists on the page, but for what it's worth it is documented here anyway. There also seems to be some affiliation with the www.coiuldefier.com web site, which is no longer available for whatever reason:

```
PAGINA IN MEMORIA www.coiuldefier.com R.I.P. Last Up Date 22.06.2005
```

Perhaps this was a previous site operated by this group of Romanians, but they were unable to hold onto it. Has someone already shut them down once? The term “fier” in the Romanian language translates to “iron” in English, however the full “coiuldefier” is slang for “hard dick.”

Exploring other venues, we did a search for cosminhack, one of the user's Yahoo Messenger screen names. We found this user has an account on antiproxy.com, but more importantly – we found the user's personal home page. What used to be www.cosminxp.ro has moved and exists at www.cosminxp.tk, a TLD country code specifying Tokelau – a small island in the South Pacific Ocean.

On Cosmin's home page, he asks that any suggestions about the site be sent to CosminHack@Yahoo.com. Hey Cosmin, are you ripping off banks in the United States or are we barking up the wrong tree? Wrong tree? I thought you'd say that...

```
--===Mica Descriere======---
Nume : Cosmin
Data nasterii : 08.06.1986
Locul nasterii : Braila
Adresa : Soseaua Focsani no.57
Telefon : +402396***** & +40722******
E-mail : CosminHack@Yahoo.Com CosminXp@CosminXp.Tk Cosmin@ForzaRapid.Ro
Scoala : Liceul "Grigore Moisil" Braila
Profil:Tehnica De Calcul (Computere Telefonie Mobila Si fixa)
Zodia : Gemeni
Pasiuni : Fotbal ,calculatoare ,muzica etc.
...:::In curand mai multe vor fi:::...
```

On the download section of Cosmin's page, he lists his favorite hacking tools, some of which we are already familiar with as a result of previous run-ins with Romanians (we got to analyze a large subset of Romanian hacking in Honeynet.org's Scan of the Month 34). Cosmin likes Radmin, PsyBnc, and IPScan.

Enough picking on Cosmin for now. Iron's email address appears to be adryanproject@yahoo.com, retrieved from his member information on a public forum. We currently have no additional information on this person or the other members of the Romanian group.

Last but not least, if Cosmin and the Romanian group are not responsible for these phishing attacks, I give them my sincere apologies for false accusation. I will revise this document immediately upon receiving reliable information on their innocence.