Banking Scam Revealed

by Secure Science Corporation

last updated November 13, 2003

1 Overview

Not all people that send undesirable email (spam) are the same. Their motives differ as greatly as their toc document uncovers a spam gang who seeks to acquire your banking information, and the response from o Citibank.

This document describes the unique bulk-mailing tool used for recent rash of financial email scams. These s such as Citibank, Wells Fargo, Halifax Bank, eBay, and Yahoo. Only one specific spam gang uses this tool fo spam gang started slow with only a few members, but has increased in both gang membership and spam v

All emails and headers are provided unmodified with the following exception: all personal information has b identity of the recipient. These modifications are denoted with bold and underlined typeset. Every effort ha data format without disclosing personal information. For data taken from the public domain, such as newsg from open forums, no effort has been made to modify the data or protect the publicly disclosed recipient.

2 The Citibank Scam

With the growth of online banking comes online fraud. These schemes vary from web sites that "look" like t email asking for personal banking information. At first glance, the email below (Fig. 1) looks like just anoth fraud schemes.

Figure 1: Sample Citibank Scam

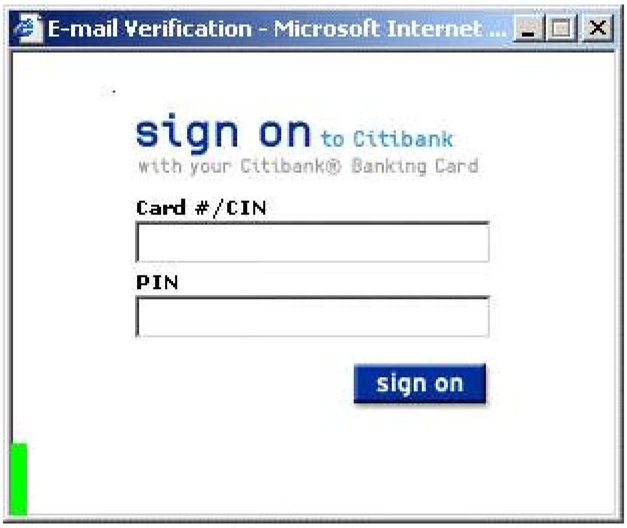
```
Received: from host70-72.pool80117.interbusiness.it ([80.117.72.70])
          by mailserver with SMTP
                    id <20030929021659s1200646q1e>; Mon, 29 Sep 2003 02:17:00 +0000
Received: from sharif.edu [83.104.131.38] by host70-72.pool80117.interbusiness.it (Postfi
ESMTP id EAC74E21484B for <e-response@securescience.net>; Mon, 29 Sep 2003 11:15:38 +0000
Date: Mon, 29 Sep 2003 11:15:38 +0000
From: Verify <verify@citibank.com>
Subject: Citibank E-mail Verification: e-response@securescience.net
To: E-Response <e-response@securescience.net>
References: <F5B12412EAC2131E@securescience.net>
In-Reply-To: <F5B12412EAC2131E@securescience.net>
Message-ID: <EC2B7431BE0A6F48@citibank.com>
Reply-To: Verify <verify@citibank.com>
Sender: Verify <verify@citibank.com>
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Dear Citibank Member,

This email was sent by the Citibank server to verify your e-mail
address. You must complete this process by clicking on the link
below and entering in the small window your Citibank ATM/Debit
Card number and PIN that you use on ATM.
This is done for your protection -t- becaurse some of
our members no longer have access to their email addresses and
we must verify it.

To verify your e-mail address and access your bank account,
click on the link below. If nothing happens when you click on the
link (or if you use AOL)K, copy and paste the link into
the address bar of your web browser.

http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.pIsEm.NeT/3/?3X6CMW2I2uPOVQW
```

```
y-------------------------------------------
           Thank you for using Citibank!
C-------------------------------------------

This automatic email sent to: e-response@securescience.net
Do not reply to this email.

R_CODE: ulG1115mkdC54cbJT469
```

At a quick glance, this email appears to be from Citibank, as it contains a Citibank URL. But a closer inspec

- The email contains multiple misspellings and grammatical errors, such as "becaurse" and "This autor
- The content contains hash-busters (unique characters in the contents that are used to bypass hash-l example, the "-t-" and "K" in the main paragraphs, and the "y" and "C" before the long lines of hyph the message with different hash-buster characters.
- Although the included URL begins with "www.citibank.com", it actually goes to "sd96v.pisem.net" [re Moscow, Russia and is not part of Citibank.
- The email header does not originate from Citibank. Instead, it originated from a DSL system in Italy. (Appendix A) indicate that the system was likely compromised.

People who clicked on the link saw the Citibank web page and a popup that prompts for login information (Citibank web page actually came from Citibank, the popup came from a non-Citibank server. Victims that e the popup essentially gave their accounts to an unknown scam artist.


E-mail Verification - Microsoft Internet ...

sign on to Citibank
with your Citibank® Banking Card

Card #/CIN

PIN

sign on

Your E-Mail Was Verified. -

Thank y

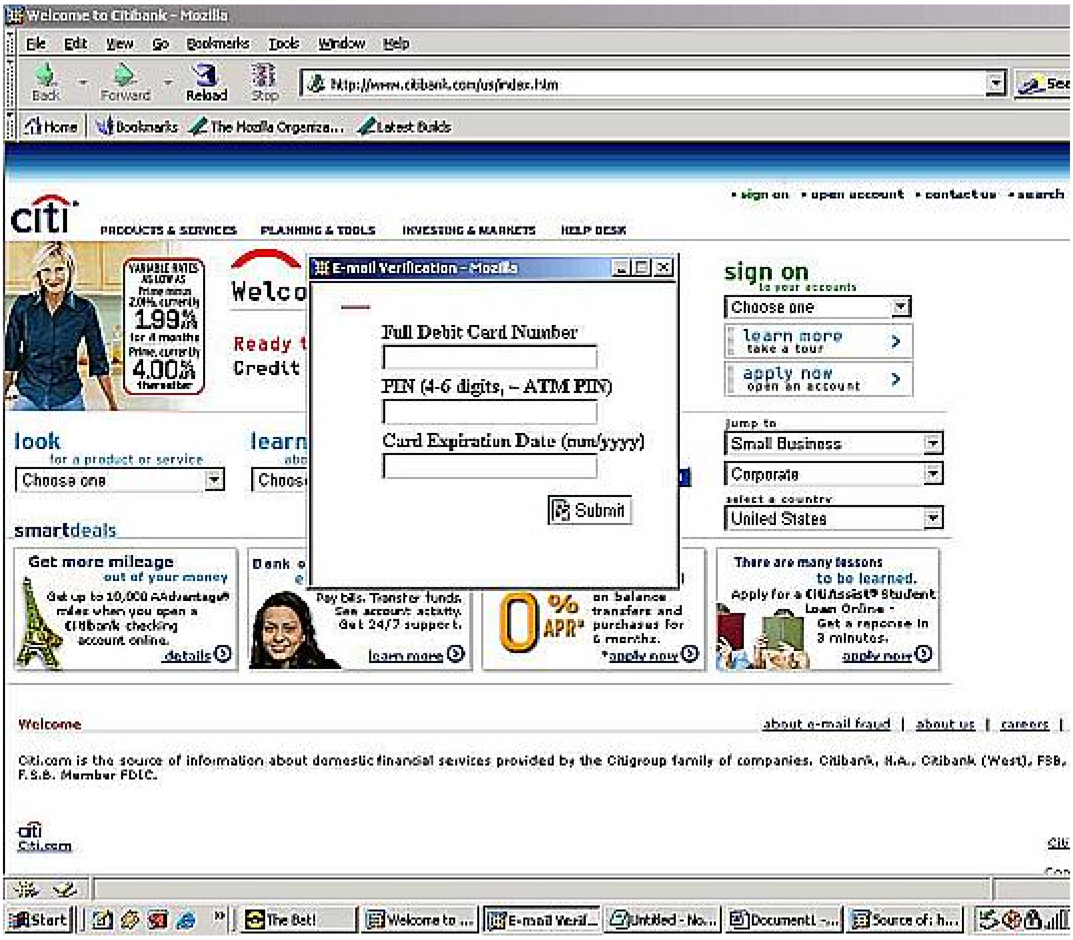
Your E-Mail Ac
Successful V

Figure 2: Trojan login popup from 29-Sep-2003.[ref 2] **Figure 3: Reply screen after e**

2.1 Mass Mailing Revisions

The 29-Sep-2003 mass mailing (Fig. 1, Fig. 2, and Fig. 3) is actually the second revision of the fraudulent l appeared on 16-Aug-2003 and asked the recipient to view new banking terms and conditions. Users who cl to a server in China. The first revision included the recipient's email address as a field in the URL. The seco field with a series of random characters. The popup for the second revision only asked for the user's Card a release on 25-Oct-2003 (Fig. 4) was revised to prompt for the user's Card number, PIN number, and expira

In nearly every case, a Russian server was used, either to host the requests, or to act as a web-bug and cc example, the web bug from the first revision can be found here. According to this web-log, there were 107, 91,573 hits on 17-Aug-2003 (Fig. 5). These were primarily due to responses to the first spam message. In mass mailing, there was only one web-log entry, from "68.82.62.191" - a cable modem in Tybouts Corner, was used 8 out of 10 times in the week prior to the mass mailing [ref 3] (Fig. 6) and was likely used for tes unclear whether this is the IP address of the actual perpetrator or a compromised host. Network scans of tl a firewall and no open proxy services, so it is unlikely that the host previously provided an open proxy [ref


Welcome to Citibank - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://www.citibank.com/us/index.htm
Home Bookmarks The Mozilla Organiza... Latest Builds
citi
• sign on • open account • contact us • search
PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK
VARIABLE RATES AS LOW AS Prime minus 2.01% currently 1.99% APR for 4 months Prime, currently 4.00% APR thereafter
Welco
Ready t
Credit
sign on to your accounts
Choose one
learn more take a tour
apply now open an account
look for a product or service
Choose one
learn
Choose
jump to
Small Business
Corporate
select a country
United States
smartdeals
Get more mileage out of your money
Get up to 10,000 AAdvantage® miles when you open a Citibank checking account online.
details
Bank o
Pay bills. Transfer funds. See account activity. Get 24/7 support.
learn more
0% APR* on balance transfers and purchases for 6 months.
*apply now
There are many lessons to be learned.
Apply for a CitiAssist® Student Loan Online - Get a reponse in 3 minutes.
apply now
Welcome
about e-mail fraud | about us | careers |
Citi.com
Start
The Bat!
Welcome to ...
E-mail Verif...
Untitled - No...
Document1 -...
Source of: h...

E-mail Verification - Mozilla

Full Debit Card Number

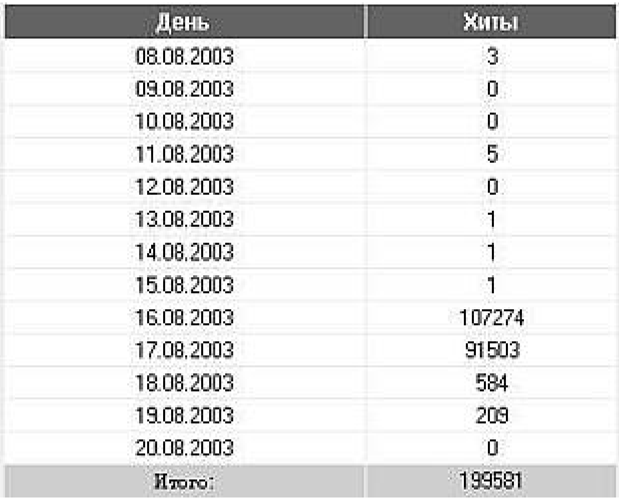
PIN (4-6 digits, – ATM PIN)

Card Expiration Date (mm/yyyy)

Submit

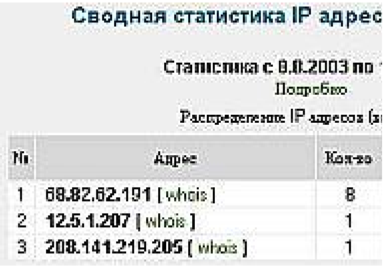
Citi.com is the source of information about domestic financial services provided by the Citigroup family of companies. Citibank, N.A., Citibank (West), FSB, F.S.B. Member FDIC.

Figure 4: The third revision of the Citibank trojan login, from 25-Oct-2003. A server ir the popup but the main window actually is the Citibank home pa



День	Хиты
08.08.2003	3
09.08.2003	0
10.08.2003	0
11.08.2003	5
12.08.2003	0
13.08.2003	1
14.08.2003	1
15.08.2003	1
16.08.2003	107274
17.08.2003	91503
18.08.2003	584
19.08.2003	209
20.08.2003	0
Итого:	199581

Figure 5: Number of daily web hits recorded by the Russian web bug from the 16-Aug-2003 Citibank mailing.



Сводная статистика IP адрес

Статистика с 8.8.2003 по

Подробно

Распределение IP адресов (

№	Адрес	Кол-во
1	68.82.62.191 [whois]	8
2	12.5.1.207 [whois]	1
3	208.141.219.205 [whois]	1

Figure 6: IP addresses from the we 2003 mailing. A Delaware address web bug prior to the mass mailir someone testing before th

3 Linking Scams

In order to operate a spam-based financial scam, three items are required: (1) a bulk mailing tool, (2) an i tool, and (3) a method to collect victim information. By identifying these items, we can identify related scai and distinguish these scams from scams initiated by other groups.

3.1 Bulk Mailing Tool

People that send spam operate with millions of email addresses. To generate the emails within a reasonabl
email tool is used. Different tools have different unique traits. In the case of this Citibank scam, the tool ha
in the email header: 16 to 17 characters consisting of "A-Z" and "0-9", followed by "@" and the forged sen
unique sequence to a large spam collection such as the Great Spam Archive [ref 5] (GSA) and the newsgro
abuse.sightings (NANAS), we can identify similar messages. For example, between 11-Nov-1997 and 21-A
17,867 spam messages. Of those, only 16 messages matched the unique signature of this specific bulk-ma
found clustered in the last five (5) months of the archive.

GSA Date	GSA Message-ID value	GSA Subject
24 Apr 2003 13:01:55	0JJ9H7JGA03EI8A7I@att.net	Rich, Hello! My
15 Jun 2003 12:41:00	D4CI74IDH3FKH13D@att.net	Dear Rich! I've
07 Jul 2003 07:43:51	2EF98ADD2HG3CJ54@att.net	Rich, Any softwa
17 Jul 2003 10:39:28	76E7A5HFIJIHK63C@e-loan.com	[Ftpserver] Re:
17 Jul 2003 10:46:08	6J76H1B289HCC313@e-loan.com	Re: Your E-Loan
22 Jul 2003 01:21:52	77EGJ4AGC1F3AIB5@wellsfargo.com	Re: Wells Fargo
26 Jul 2003 09:43:59	JFHAL1CJIB78IFA8@security.org	Newsletter
26 Jul 2003 23:00:46	H8HFB0BB06232180@e-gold.com	The Great E-Gold
29 Jul 2003 18:39:15	4K63GFHLE8FJ1GK7@utp.edu.co	Rich, software f
30 Jul 2003 19:03:38	3FHG03G0I213JJ92@yahoo.com	I want to introd
31 Jul 2003 05:26:44	BG5L3CAI6J586EK0@headgear.org	new mail
02 Aug 2003 10:21:12	J9D9GK1H1IJ47920@hotmail.com	Rich,Want sex <r
09 Aug 2003 11:59:24	50LJ6D9B4EK320HD@annexia.org	Ïëÿæíûé îòäûõ
17 Aug 2003 07:58:36	2J73600018ECI75J@virtualitas.net	Re: mail
17 Aug 2003 17:49:39	FBE6962ED2FJFK58@hotmail.com	Rich, Instant Pl
20 Aug 2003 19:37:45	A60I9A7D890FL51L@cbshost-68-111-42-31.sbcox.net	Re: mail

Although we expect the GSA to contain more entries by this bulk-mailing tool, the GSA is only updated per
ends on 21-Aug-2003, so more information will not be available until the GSA is updated.

The narrow timeframe and near weekly appearance of spam from this bulk-mailing tool by the GSA recipie
First, there is likely only one or two senders using the tool; this tool does not have a large distribution. Sec
days and a week to cycle through the entire address list. Because the same email recipient does not receiv
gang is likely using subsets from their mailing list. The subsets may be due to a slow network connection (
an intentional selection of recipients. Finally, the minor change from 17 to 16 characters in the Message-ID
observed messages, indicates that the sender is likely also the developer.

3.2 Scam Content Analysis

Most of the email messages sent by this group contain grammatical errors and spelling errors (Fig. 7). For
correct in Spanish, German, and other Slavic- and Latin-based languages, but proper English would be, "I a
similar to those made by Europeans who have English as a second language. In addition, the currency nota
("300$" instead of "$300").

Figure 7: GSA 24-Apr-2003 Contents

```
Hello. My name is John Turner....  I am the customer of AURUM INVESTMENT
There is nothing like this program. At first I spent 800$ and in 4 weeks I have
earned more than 300$ of profit    I am really impressed. You doesnt get any better than
```

```
Just follow the link http://am-it.biz//sign.php?ref_id=28934887

There is only one honest way to get money:

to invest them wisely

Money and you must keep a good company, right?
```

Although the spam topics used by this bulk-mailing tool rotate, there appears to be two distinct content typ indicates a spam sender that delivers content for bulk-message customers (spammer for hire). The content software to penis enhancements. Other bulk-mailing tools have been observed delivering similar messages notations and common American grammatical errors. The grammatical errors and currency notations assoc mailing tool suggests a European.

The second content type is more interesting: many messages show a desire for banking and credit card inf download software. These messages do not have the same style of grammatical errors nor the European cu different sender than the bulk-message individual. This different sender is likely in the United States or Car

Figure 8: GSA Dates for Financial Fraud	**Figure 9: GSA Dates for Bulk Me**
24 Apr 2003 15 Jun 2003 17 Jul 2003 22 Jul 2003 26 Jul 2003 (two different instances)	07 Jul 2003 29 Jul 2003 30 Jul 2003 31 Jul 2003 02 Aug 2003 17 Aug 2003 (two different instance 20 Aug 2003

Besides the GSA, other spam archives have been analyzed. Some archives only contain the "bulk-message other archives only contain the "financial fraud" messages, and many archives contain both types of messa differences in content, we can conclude that multiple groups use this specific bulk-mailing tool. However, th dates, independent mailing lists, and content text that is specific and unique to this tool indicates that (1) t fraud emails are different than the general bulk-message senders, and (2) the financial fraud emails are ge

3.3 Collecting Victim Information

The financial fraud spam group appears to use multiple methods for gathering information from fraud victir responses by email. These emails went to unverified accounts that likely acted as blind-drops where the inf forwarded or gathered later.

3.3.1 Use of Malware

For a brief period, email messages sent by this particular financial fraud spam gang contained hostile attac 2003 a series of email messages were observed being sent from this particular bulk-mailing tool. The first c customers and included the "Trojan.Download.Berbew" [ref 6] malware. This trojan code was written in C (backdoor program attempts to steal passwords and send them to a remote web server. When used in conju system monitors passwords and presents the user with the actual bank login screen. Thus, when the user l becomes compromised. On 22-Jul-2003, the same bulk-mailing tool generated a second wave of email. The Fargo and Citibank customers, and included a newer version of Trojan.Download.Berbew.

Trojan.Download.Berbew was not the only malware used by this group. On 26-Jul-2003, an email claiming "admin@security.org" was observed. The text contents contained poor grammar and appeared to have bee attachment contained the Exploit-Codebase [ref 7] malware. According to Network Associates:

> "[Exploit-Codebase] is a generic detection of malware which tries to exploit a Microsoft Internet Expl

> discovered February 25, 2002. This exploit could result in an executable file being run without the us
> when visiting a web page or viewing HTML email message. This affects Internet Explorer 4.x and hig
> Microsoft Outlook Express." [ref 8]

Exploit-Codebase malware appears to have been written in C, similar to Trojan.Download.Berbew. While it individual created the Trojan.Download.Berbew and Exploit-Codebase malwares, it is unlikely that the malv the Expoit-Codebase vulnerability nearly a year prior.

3.3.2 Web Impersonations

After using email blind-drops and malware, the group quickly progressed to impersonating web sites. The i web redirections. The hypertext transport protocol (HTTP) permits web servers to redirect requests to alter codes). In this case, the gang's web server returned an HTTP 303 return code redirecting browsers to the t the HTTP response may also contain valid HTML code. The valid code usually tells the user that the page ha This gang used the redirection response's HTML code to generate a popup requesting the victim's banking i page is the targeted financial institution, but the popup comes from a hostile server (Fig. 4). The hostile se victim information.

3.4 Related Financial Scams

The same bulk-mailing tool has been observed sending similar fraudulent content that targets many financ presents dates and targets that are verifiable based on the sending email tool's unique fingerprint and com But, this is unlikely to be a complete list. Prior to July 2003, this spam gang appears to send "regular" bulk imitate financial login screens, a practice known as "phishing". In addition, there is no record of this particu anyone prior to April 2003.

Although this spam gang has targeted other financial groups, there is a strong emphasis on eBay and Citib may indicate a grudge, familiarity, specific knowledge, or specific access. The recent increase in banking ta capture more victims before being blacklisted, caught, or ignored.

On 20-Oct-2003 the group attempted a 419 scam [ref 9]. Individuals rarely attempt the 419, or Nigerian s requires a noticeable amount of manpower and resources. The appearance of a 419 by this particular bulk- increase in scam operators. There are many different groups that operate 419 scams; the text from this pa the 419 scam - other 419 gangs have better contents and better methods to identify themselves as the pe volume of 419-style scams since April 2003, these approaches have become relatively common, easy to sp likelihood, this financial fraud gang's attempt on 20-Oct-2003 was likely a failure. This may also account fo impersonations in the following days (5 banks targeted in 3 days). The group may have applied their additi successful strategy and simply branched out. In addition, the sudden focus change from USA financial sour Halifax, Nationwide, and Lloyds) at the end of October likely indicates new spam gang members with famili

				Targeted Financial Groups				
Date	E-Loan	E-Gold	Yahoo	eBay	PayPal	Wells Fargo	Citibank	O
17-Jul-2003	Malware							
21-Jul-2003						Malware	Malware	
26-Jul-2003		X						
16-Aug-2003							X	
3-Sep-2003			X					
17-Sep-2003			X					
19-Sep-2003				X				
23-Sep-2003				X				
25-Sep-2003							X	
28-Sep-2003							X	
30-Sep-2003				X				
2-Oct-2003				X			X	

4-Oct-2003							X	
5-Oct-2003				X				
9-Oct-2003					X			
18-Oct-2003				X				
20-Oct-2003							X	
21-Oct-2003				X				
25-Oct-2003							X	
26-Oct-2003								Ha
27-Oct-2003								

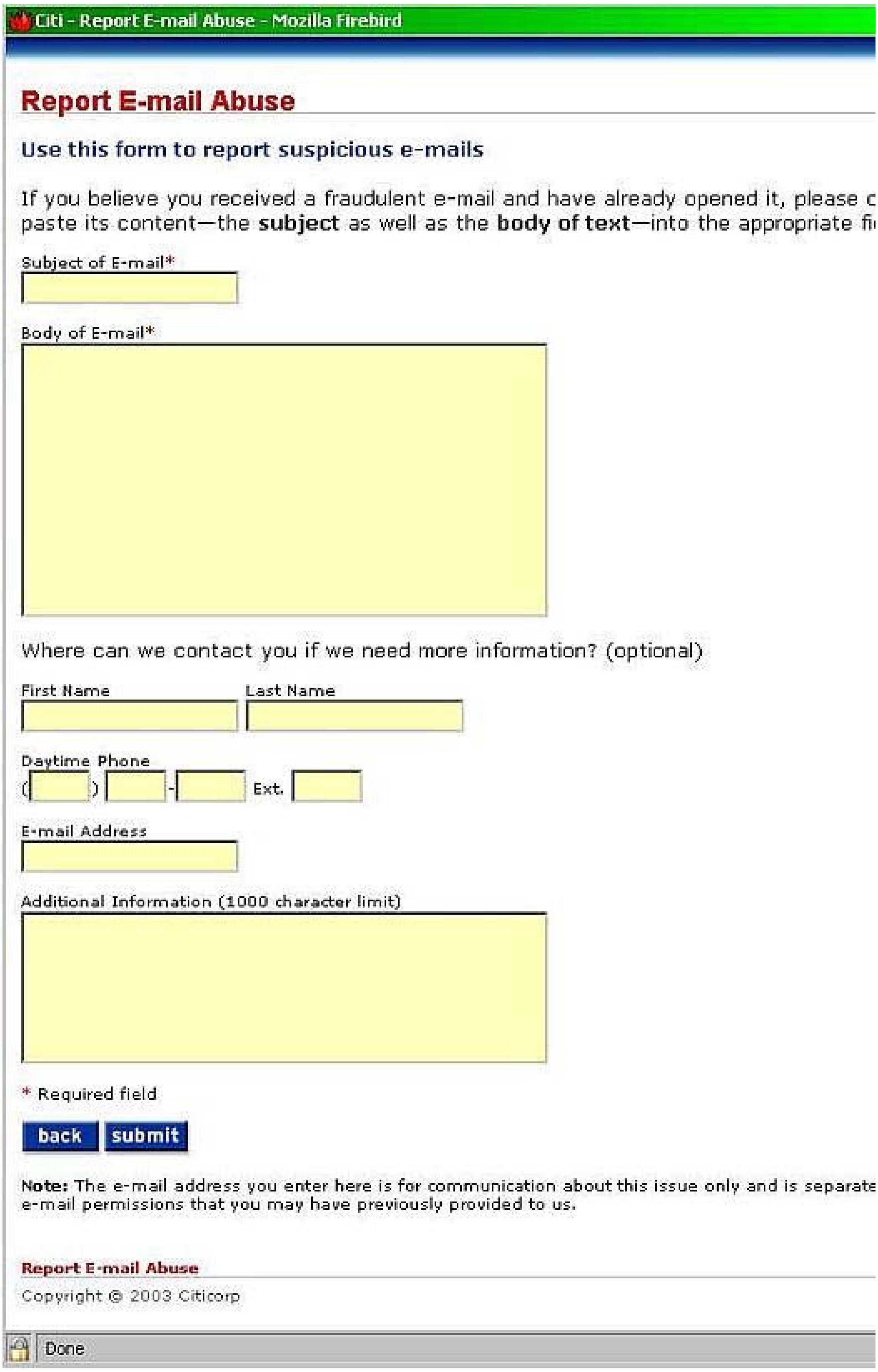
Malware: Use of email with a hostile attachment.
X: Use of email requesting information by email or hostile web site.

3.5 Unrelated Financial Scams

Not all financial fraud email messages can be attributed to this particular group. For example, this particula
with requesting users to update eBay account information on 15-Oct-2003 and 17-Oct-2003; a different sp
the fraudulent email messages. Additionally, the financial fraud messages from "verify@online-banking.net
such as Citibank, Wells Fargo, Bank of America, Affinity Bank, and the Union Bank of California, all appear
that focuses on banks located in California.

4 Reporting to Citibank

The first financial-fraud email that we received (Fig. 1) claimed to be from Citibank. As such, we proceeded
fraud reporting system (Fig. 10).



Report E-mail Abuse

Use this form to report suspicious e-mails

If you believe you received a fraudulent e-mail and have already opened it, please c
paste its content—the **subject** as well as the **body of text**—into the appropriate fi

Subject of E-mail*

Body of E-mail*

Where can we contact you if we need more information? (optional)

First Name Last Name

Daytime Phone
( ) - Ext.

E-mail Address

Additional Information (1000 character limit)

* Required field

Note: The e-mail address you enter here is for communication about this issue only and is separate
e-mail permissions that you may have previously provided to us.

Copyright © 2003 Citicorp

Figure 10: The Citibank online fraud reporting system.

A few hours later, a response from Citibank was received (Fig. 11). Unfortunately, this reply has a significa
aspects. In particular:

- The reply discusses fraudulent email content that differs from the submitted email. The submitted cc
transfers, include a virus, nor contain an attachment, as suggested by the response. This could be d
generic form letter.

- The reply concludes with a static string of odd characters. These appear to be a hash-buster (used b based spam filters) but never change. Strings such as this have not been observed with other officia
- The content directs further questions to a toll-free number: 1-877-4-MYCITI. Unfortunately, this toll- People who call this number receive the following short message: "The number you dialed is invalid. to the Citibank web site, is different than the invalid number provided in the automated reply.
- The content directs future fraud emails to be sent to a non-Citibank email address: hatsu1@aol.com is unknown. In no other Citibank web page or official Citibank email is a non-Citibank email address *Nov-03, this email address is still used in Citibank's response.*
- "Cleatis Hawkins" signed the email. According to an operator at Citibank?s correct toll-free number, not worked at Citibank for a few months. There is no evidence to suggest that "Cleatis Hawkins" is r email scam or possible system compromise. It is unclear how his name became attached to the reply

No aspect of the email headers appears forged. The reply from Citibank originated from the Citibank Devel California (CDCLA). It is now left to the reader to draw his own conclusions from this email.

Figure 11: The Citibank reply from 29-Sep-2003.

```
Received: from mango2-a.citicorp.com (HELO mango2.citicorp.com) ([192.193.196.141])
(envelope-sender )
by smtp-1-2a.secureserver.net (qmail-ldap-1.03) with SMTP
for <e-response@securescience.net>; 29 Sep 2003 19:03:14 -0000
Received: from myrtle1.citicorp.com (imta.citicorp.com [192.193.195.186])
by mango2.citicorp.com (8.12.10/8.12.9) with ESMTP id h8TIvn3v029897
for <e-response@securescience.net>; Mon, 29 Sep 2003 14:57:49 -0400 (EDT)
Received: from iewa.cdcla.citicorp.com (localhost [127.0.0.1])
by myrtle1.citicorp.com (8.12.10/8.12.10) with ESMTP id h8TJ3BA4014816
for ; Mon, 29 Sep 2003 15:03:11 -0400 (EDT)
Delivered-To: sqrl@mydomain
Subject: Citibank Email Verification
Reply-To: autoreply.iewa@citicorp.com
To: <e-response@securescience.net>
Date: Mon, 29 Sep 2003 11:00:00 -0800
X-MIMETrack: Serialize by Router on DOMINO13/ADG-LA(Release 6.0.1|February 07, 2003) at
09/29/2003 11:00:02 AM

Dear e-response@securescience.net,

Thank you for your message regarding an Email asking for our Citicard and PIN number and
wire $500.00. This is a fraud Email and it is not an official communication from Citibank
strongly recommend that you delete the Email and should not attempt to reply to the messa
open the attachment.

Citibank is aggressively investigating this fraudulent Email that has been sent to numero
addresses. Citibank is also working with law enforcement on the issue.

However, if you did open the attachment, we recommend that you run your virus protection
software. You may need to download an updated version of the Anti-Virus Software from you
vendor. We advise that you change all Passwords used online, after your Anti-Virus Softwa
certified that all malicious programs have been cleared from your system.

You can contact your local technical support for options on removing the malicious progra
did open the attachment and do not have an Anti-Virus Software.

However, we recommend that you not log on to any site that requires a User ID and Passwor
the system is cleaned. You should also change any Passwords which you have entered online
opening the attachment. These changes will need to be performed with the institution and
online.

You can forward the fraud Email to hatsu1@aol.com.

If you have further questions concerning Myciti.com, please send another email or call us
877-4-MYCITI and we will be happy to assist you.

Thank you for using MyCiti.com,
Cleatis Hawkins
```

```
&3925000440863888ZSU@L6<G<"@L6<G<ECT&
```

5 Conclusion

A single spam gang, using a unique bulk-mailing tool, appears responsible for the recent rash of financial fr targeted over a dozen financial sources, had dabbled in malware, and has struck over 20 times, showing w pattern.

Attempts to report these findings to Citibank were unsuccessful, and Citibank was unavailable for comment that they do not know who has been victimized by the Citibank scams, nor do they know how many victims logs very likely indicate exactly who fell victim to the 16-Aug-2003 fraudulent Citibank scheme. In addition identify "who" fell victim on 25-Sep-2003 and 25-Oct-2003 to the second and third revisions of the fraud s "how many" victims are likely. This is because the fraudulent web sites used HTML links that directly refere web site.

6 About the Author

Secure Science Corporation is a professional services and software company that develops advanced techn online assets. Clients of Secure Science Corp. are provided with in-depth security evaluations, as well as co seamless in both deployment and maintenance. Secure Science Corp. is pioneering innovative ways to tran environment for both online communications and transactions.

Comments on this article can be sent to e-resonse@securescience.net or to the SF editor.

7 Appendix A: Network Scans

The initial fraudulent Citibank email that we received, leading toward this investigation, originated from "80 *host is now down.]* Network scans of host were conducted within five (5) minutes of receipt of the email. T sending host was likely compromised. It is unclear whether the email sender was responsible for the compr with an open proxy server.

7.1 Italy DNS and Whois Scan

Based on the IP address, we can identify the hosting company, country, and often the city. In addition, ma type of network connection. In this case, the host is located in Italy and provided by Telecom Italia. The ho

```
ping: 80.117.72.70 IS ALIVE!
70.72.117.80.in-addr.arpa domain name pointer host70-72.pool80117.interbusiness.it.
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum:      80.117.0.0 - 80.117.255.255
netname:      TINIT-ADSL-LITE
descr:        Telecom Italia
descr:        Accesso ADSL BBB
country:      IT
admin-c:      BS104-RIPE
tech-c:       BS104-RIPE
status:       ASSIGNED PA
remarks:      Please send abuse notification to abuse@telecomitalia.it
notify:       ripe-staff@telecomitalia.it
mnt-by:       TIWS-MNT
```

```
changed:      net_ti@telecomitalia.it 20020927
source:       RIPE
```

7.2 Italy Nmap Results

Nmap is a system utility for determining open services and operating system on a remote host. Nmap is av
http://www.insecure.org/nmap/.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (2), OS detection may be less accurate
Interesting ports on host70-72.pool80117.interbusiness.it (80.117.72.70):
(The 1617 ports scanned but not shown below are in state: closed)
Port       State       Service
1025/tcp   open        NFS-or-IIS
1026/tcp   open        LSA-or-nterm
1027/tcp   open        IIS
5555/tcp   open        freeciv
6666/tcp   open        irc-serv
6699/tcp   open        napster
8888/tcp   open        sun-answerbook
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXPN

map run completed -- 1 IP address (1 host up) scanned in 88 seconds
```

7.3 Italy Nessus Results

Nessus is a vulnerability scanner and can be used to determine if a host as unspecified services, or known :
available from http://www.nessus.org/.

```
+ 80.117.72.70 :
 . List of open ports :
    o NFS-or-IIS (1025/tcp) (Security notes found)
         o LSA-or-nterm (1026/tcp)
         o IIS (1027/tcp)
         o unknown (4455/tcp) (Security hole found)
         o freeciv (5555/tcp) (Security hole found)
         o unknown (6186/tcp)
         o irc-serv (6666/tcp)  (Security hole found)
         o unknown (6699/tcp)
         o loc-srv (135/udp)
         o profile (136/udp)
         o netbios-ns (137/udp)
         o netbios-dgm (138/udp)
         o netbios-ssn (139/udp)
         o microsoft-ds (445/udp)
         o isakmp (500/udp)
         o route (520/udp)
         o general/tcp (Security notes found)
         o general/udp (Security notes found)
. Information found on port NFS-or-IIS (1025/tcp)
    An unknown service runs on this port.
             It is sometimes opened by this/these Trojan horse(s):
                       Fraggle Rock
                            md5 Backdoor
                            NetSpy
                            Remote Storm

                 Unless you know for sure what is behind it, you'd better
                      check your system

                 Solution: if a trojan horse is running, run a good antivirus scanner
                      Risk factor : Low

. Vulnerability found on port unknown (4455/tcp) :
     The 'Count.cgi' cgi is installed. This CGI has
          a well known security flaw that lets anyone execute arbitrary
          commands with the privileges of the http daemon (root or nobody).

          Solution : remove it from /cgi-bin.
          Risk factor : Serious
          CVE : CVE-1999-0021
          BID : 128

. Vulnerability found on port unknown (4455/tcp) :
     The 'upload.cgi' cgi is installed. This CGI has
          a well known security flaw that lets anyone upload arbitrary
          files on the remote web server.

          Solution : remove it from /cgi-bin.
          Risk factor : Serious

. Vulnerability found on port unknown (4455/tcp) :
     The Cobalt 'siteUserMod' CGI is installed.
          Older versions of this CGI allow any user to change the
          administrator password.

          Make sure you are running the latest version.
          Solution :

          RaQ 1 Users, download :
          ftp://ftp.cobaltnet.com/
           pub/experimental/security/siteUserMod/RaQ1-Security-3.6.pkg

          RaQ 2 Users, download  :
          ftp://ftp.cobaltnet.com/
           pub/experimental/security/siteUserMod/RaQ2-Security-2.94.pkg

          RaQ 3 Users, download :
          ftp://ftp.cobaltnet.com/
           pub/experimental/security/siteUserMod/RaQ3-Security-2.2.pkg

          Risk factor : High
          CVE : CVE-2000-0117
          BID : 951

. Vulnerability found on port unknown (4455/tcp) :
     /cgi-bin/.cobalt/overflow/overflow.cgi was detected.
          Some versions of this CGI allow remote users to execute arbitrary commands
          with the privileges of the web server.

          *** Nessus just checked the presence of this file
          *** but did not try to exploit the flaw, so this might
          *** be a false positive

          See: http://www.cert.org/advisories/CA-2002-35.html
          Solution : get a newer software from Cobalt
          Risk factor : High

. Information found on port unknown (4455/tcp)
    A web server is running on this port

. Information found on port unknown (4455/tcp)
    The remote  web servers is [mis]configured in that it
         does not return '404 Not Found' error codes when
         a non-existent file is requested, perhaps returning
         a site map or search page instead.

         Nessus enabled some counter measures for that, however
         they might be insufficient. If a great number of security
         holes are produced for this port, they might not all be accurate

. Information found on port unknown (4455/tcp)
    The remote web server type is :
         Apache/1.3.22
         Solution : You can set the directive 'ServerTokens Prod' to limit
         the information emanating from the server in its response headers.

. Vulnerability found on port freeciv (5555/tcp) :
   The 'guestbook.cgi' is installed. This CGI has
    a well known security flaw that lets anyone execute arbitrary
         commands with the privileges of the http daemon (root or nobody).

         Solution :  remove it from /cgi-bin.
         Risk factor : Serious
         CVE : CVE-1999-0237
         BID : 776

. Vulnerability found on port freeciv (5555/tcp) :
     The 'webdist.cgi' cgi is installed. This CGI has
          a well known security flaw that lets anyone execute arbitrary
          commands with the privileges of the http daemon (root or nobody).

          *** Nessus reports this vulnerability using only
          *** information that was gathered. Use caution
          *** when testing without safe checks enabled.

          Solution : remove it from /cgi-bin.
          Risk factor : Serious
          CVE : CVE-1999-0039
          BID : 374

. Warning found on port freeciv (5555/tcp)
    The 'printenv' CGI is installed.
         printenv normally returns all environment variables.
         This gives an attacker valuable information about the
         configuration of your web server.

         Solution : Remove it from /cgi-bin.
         Risk factor : Medium

. Information found on port freeciv (5555/tcp)
   A web server is running on this port

. Information found on port freeciv (5555/tcp)
    The remote  web servers is [mis]configured in that it
         does not return '404 Not Found' error codes when
         a non-existent file is requested, perhaps returning
         a site map or search page instead.

         Nessus enabled some counter measures for that, however
         they might be insufficient. If a great number of security
         holes are produced for this port, they might not all be accurate

. Information found on port freeciv (5555/tcp)
    The remote web server type is :    Apache/1.3.22

         Solution : You can set the directive 'ServerTokens Prod' to limit
         the information emanating from the server in its response headers.

. Vulnerability found on port irc-serv (6666/tcp) :
   The file /wwwboard/passwd.txt exists.
    This file is installed by default with Matt's Script wwwboard
         software.  This can be a high risk vulnerability if the
         password used is the same for other services.  An attacker
         can easily take over the board by cracking the passwd.

         Solution : Configure the wwwadmin.pl script to put
                    the passwd.txt file somewhere else.
    Risk factor : High
         CVE : CVE-1999-0953
         BID : 649

. Vulnerability found on port irc-serv (6666/tcp) :
     The CGI /scripts/tools/newdsn.exe is present.
          This CGI allows any attacker to create files
          anywhere on your system if your NTFS permissions
          are not tight enough, and can be used to overwrite
          DSNs of existing databases.

          Solution : Remove newdsn.exe
          Risk factor : High
          CVE : CVE-1999-0191
          BID : 1818

. Warning found on port irc-serv (6666/tcp)
   The 'mailnews' cgi is installed. This CGI has
   a well known security flaw that lets an attacker execute arbitrary
   commands with the privileges of the http daemon (usually root or nobody).

   Solution : remove it from /cgi-bin.
   Risk factor : Serious
   CVE : CAN-2001-0271
   BID : 2391

. Warning found on port irc-serv (6666/tcp)
   The 'nph-test-cgi' CGI is installed. This CGI has
   a well known security flaw that lets an attacker get a listing
   of the /cgi-bin directory, thus discovering which CGIs are installed
   on the remote host.

   Solution : remove it from /cgi-bin.
   Risk factor : Serious
   CVE : CVE-1999-0045
   BID : 686

. Information found on port irc-serv (6666/tcp)
   A web server is running on this port

. Information found on port irc-serv (6666/tcp)
   The remote  web servers is [mis]configured in that it
   does not return '404 Not Found' error codes when
   a non-existent file is requested, perhaps returning
   a site map or search page instead.

   Nessus enabled some counter measures for that, however
   they might be insufficient. If a great number of security
   holes are produced for this port, they might not all be accurate

. Information found on port irc-serv (6666/tcp)
    The remote web server type is :    Apache/1.3.22

         Solution : You can set the directive 'ServerTokens Prod' to limit
         the information emanating from the server in its response headers.

. Information found on port general/tcp
   Nmap found that this host is running Windows Millennium Edition (Me), Win
    2000, or WinXP

. Information found on port general/tcp
   Remote OS guess : Windows Millennium Edition (Me), Win 2000, or WinXP
   CVE : CAN-1999-0454
```

8 Appendix B: GSA Email Message Summary

The following table summarizes the email message from the Great Spam Archive that were sent by this grc

GSA Date	GSA Content Summary
24 Apr 2003 13:01:55	A financial fraud asking people to invest in "AURUM INVESTMENT". The contains grammatical and spelling errors, and indicates a European aut
	A financial fraud asking people to invest in a program called "Daily Earr

15 Jun 2003 12:41:00	The text contains grammatical and spelling errors, and indicates a Euro
07 Jul 2003 07:43:51	An offer for discount software from "CheapWarez.com". The content is have been observed using the same text. But, the text has been modifi ("15$") rather than the American notation ("$15"). In addition, the orig the URL. This likely indicates that the spam sender has negotiated an a for this site.
17 Jul 2003 10:39:28	Financial fraud requesting E-Loan account information. The attachment "Trojan.Download.Berbew" [ref 11]. It was written in C (not C++). The steal passwords and send them to a remote web server. When used in system monitors passwords and presents the user with the actual bank user logs in, their login information is compromised.
17 Jul 2003 10:46:08	A second E-Loan fraud message. This indicates that the address list cor with the GSA. 22 Jul 2003 01:21:52 Financial fraud requesting Wells Fa Trojan.Download.Berbew. A similar mailing was observed on NANAS tar the executable appears to be modified; the reporting server address ch differences indicating a work-in-progress.
26 Jul 2003 09:43:59	A scam claiming to come from "admin@security.org". The content conta to have been written in haste. The attachment contains Exploit-Codeba Network Associates, "This is a generic detection of malware which tries Explorer vulnerability, which was discovered February 25, 2002. This ex executable file being run without the user's permission or knowledge, w viewing HTML email message. This affects Internet Explorer 4.x and hig Microsoft Outlook Express." It is unlikely that the author of this bulk-ma vulnerability.
26 Jul 2003 23:00:46	Financial scam for E-Gold. The URL redirects the user to a false login sc for www.e-gold.com, but is actually running on a different server. Users information compromise their account.
29 Jul 2003 18:39:15	Offer for free software. This same content appears in NANAS periodicall 12-Sep-2003. This could be related to the GSA 7-Jul-2003 software rela
30 Jul 2003 19:03:38	Similar to the 15-Jun-2003 "Daily Earnings" software, this content offer Similar text content was seen in NANAS between 15-Jun-2003 and 23-I amounts in the new message matches the European notation.
31 Jul 2003 05:26:44	An offer for free email. Text is present in both English, and the Window Russian, and other Slavic languages). The hosting site is located in Mos
02 Aug 2003 10:21:12	An offer for pornography.
17 Aug 2003 07:58:36	A free email offer similar to the GSA 31-Jul-2003 record. But the text is
17 Aug 2003 17:49:39	An offer to increase your sexual organ size. Although NANAS reports sig back to 16-Jan-2003, this particular bulk-mailing tool has only recently addition, while this tool has been observed sending this particular conte have also been observed delivering the content. This indicates an agree companies.
20 Aug 2003 19:37:45	A free email offer identical to the 17-Aug-2003 email and similar to the

References

[1] The generic URL format is "http://[username[:password]@]server[:port]/path[?options]". Items in bra this email's URL, the string "www.citibank.com" is part of the username. The actual server is found after th

[2] Screen captures included without consent from SYNACK (no contact method available), <http://www.dslreports.com/forum/remark,8089564~root=scambusters~mode=flat>.

[3] The Russian web-log can display the most used IP addresses. <http://www.hotlog.ru/cgi-bin/hotlog/sit id=126298&b_day=8&b_month=8&b_year=2003&e_day=15&e_month=8&e_ year=2003&var=HOSTS_RAW&max_items=50> shows all 11 IP addresses that accessed the site prior to t 11 came from the same host, and likely indicates the machine used for testing.

[4] Network scans of the Delaware host were performed periodically, between 26-Sep-2003 and 27-Oct-20 have been reassigned to a new host in the preceding month, DSL IP addresses are rarely rotated. The peri provided the similar replies: no open ports, and many ports "filtered" or "closed". This suggests the same h reassignment of the IP address.

[5] The Great Spam Archive can be found at www.annexia.org.

[6] Trojan.Download.Berbew is described at http://www.symantec.com/avcenter/venc/data/trojan.downloa http://www.upenn.edu/computing/virus/03/trojan.download.berbew.html.

[7] Exploit-Codebase is described at http://vil.nai.com/vil/content/v_99383.htm.

[8] Source: http://vil.nai.com/vil/content/v_99383.htm. This quote has not been modified from the initial c

[9] The "419 scam" is commonly known as the Nigerian scam and is a type of Ponzi scam. The name "419" Nigerian criminal code.

[10] Source: "Citibank warns customers of e-mail scam." Reuters. Aug. 18, 2003. http://news.com.com/21 tag=mainstry.

[11] ibid, 6.

[12] ibid, 7.