Spear Phishing

Real Cases, Real Solutions

phishme.com

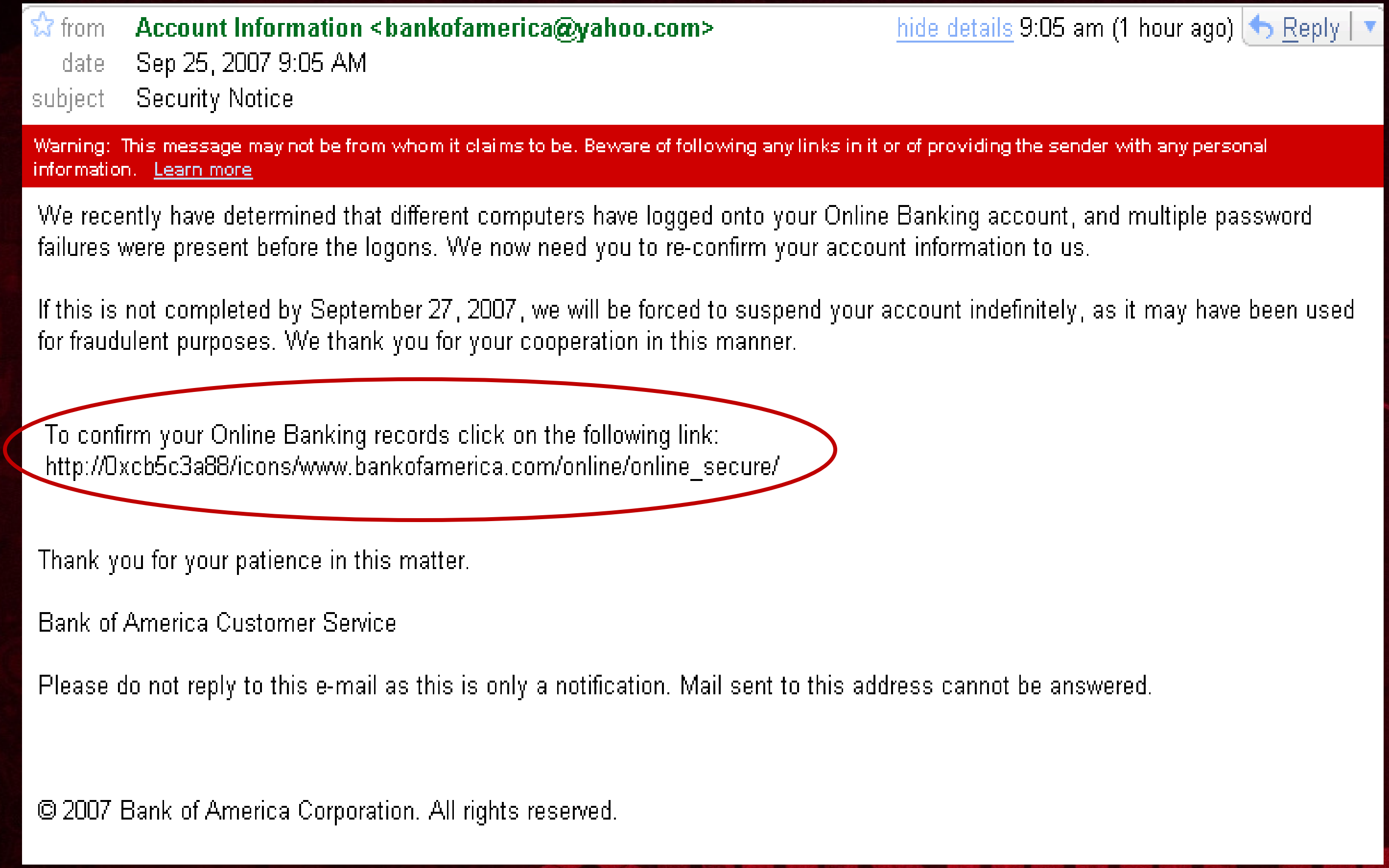
Who Am I?

- CEO of Intrepidus Group
- Adjunct Professor at Carnegie Mellon University
- Frequent Speaker at Black Hat, OWASP, MISTI, Hack In The Box

Phishing – Passé Definition

(fish´ing) (n.) The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Example banking “phish”



from Account Information <bankofamerica@yahoo.com> 9:05 am (1 hour ago)
date Sep 25, 2007 9:05 AM
subject Security Notice

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by September 27, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
http://0xcb5c3a88/icons/www.bankofamerica.com/online/online_secure/

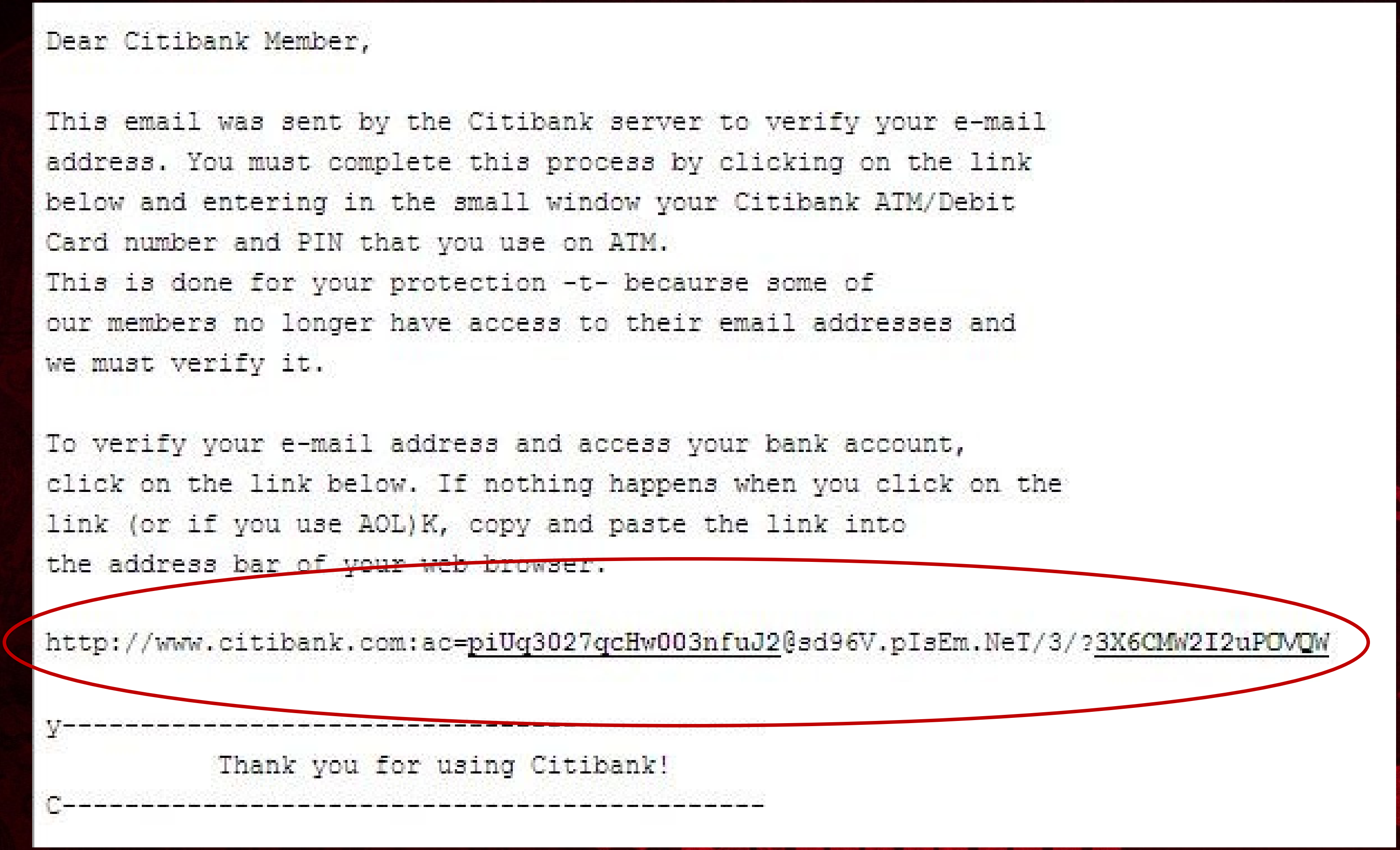
Thank you for your patience in this matter.

Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

© 2007 Bank of America Corporation. All rights reserved.

Another example



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---

Phishing – New Definition

(fish´ing) (n.) The act of electronically luring a user into surrendering private information that will be used for identity theft **or conducting an act that will compromise the victim’s computer system.**

A Report From The Trenches

Symptoms

- "I see a trade executed from my account … 10000 shares of a company I haven't even heard about, were purchased on January 17 (2006) @ 2 pm from my account!" – a client of a well-established brokerage firm in NYC.
- 7 other clients of the same brokerage firm report the same issue – in January 2006.

Investigation

- Was the brokerage firm hacked?
- Was it the end user who was hacked?
- We had dates and times of the trade executions as a clue.

Investigation

- Our team began reviewing the brokerage firm's online trading application for clues
  - Network logs
  - Web server logs
  - Security mechanisms of the application
- We asked to duplicate the victim's hard drive and review it for indicators of compromise.

Web Server Logs

- Requested IIS logs for January 17, 2006 from all the (load balanced) servers.
- Combined the log files into one common repository = 1 GB
- Microsoft’s Log Parser to the rescue

Microsoft LogParser

Parsed out all requests to execute.asp using Microsoft Log Parser:

```
LogParser -o:csv "select * INTO
  execute.csv from *.log where
          cs-uri-stem like
   '/execute.asp%'"
```

Can You Find The Smoking Gun?

```
#Fields:time c-ip              cs-      cs-uri-stem    cs-uri-query                                 Status
                               method
     1:03:15172.16.22.33       POST     /execute.asp   sessionid=90198e1525e4b03797f833ff4320af39      200
     1:04:35172.16.54.33       POST     /execute.asp   sessionid=3840943093874b3484c3839de9340494      200
     1:08:15172.16.22.33       POST     /execute.asp   sessionid=90198e1525e4b03797f833ff4320af39      200
     1:10:19172.16.87.231      POST     /execute.asp   sessionid=298230e0393bc09849d839209883993       200
     1:13:15172.16.22.33       POST     /execute.asp   sessionid=90198e1525e4b03797f833ff4320af39      200
     1:18:15172.16.22.33       POST     /execute.asp   sessionid=90198e1525e4b03797f833ff4320af39      200
     1:19:20172.16.121.3       POST     /execute.asp   sessionid=676db87873ab0393898de0398348c89       200
     1:21:43172.16.41.53       POST     /execute.asp   sessionid=3840943093874b3484c3839de9340494      200
     1:23:16172.16.22.33       POST     /execute.asp   sessionid=90198e1525e4b03797f833ff4320af39      200
```

Next Step

Parsed out all requests with the suspicious sessionid

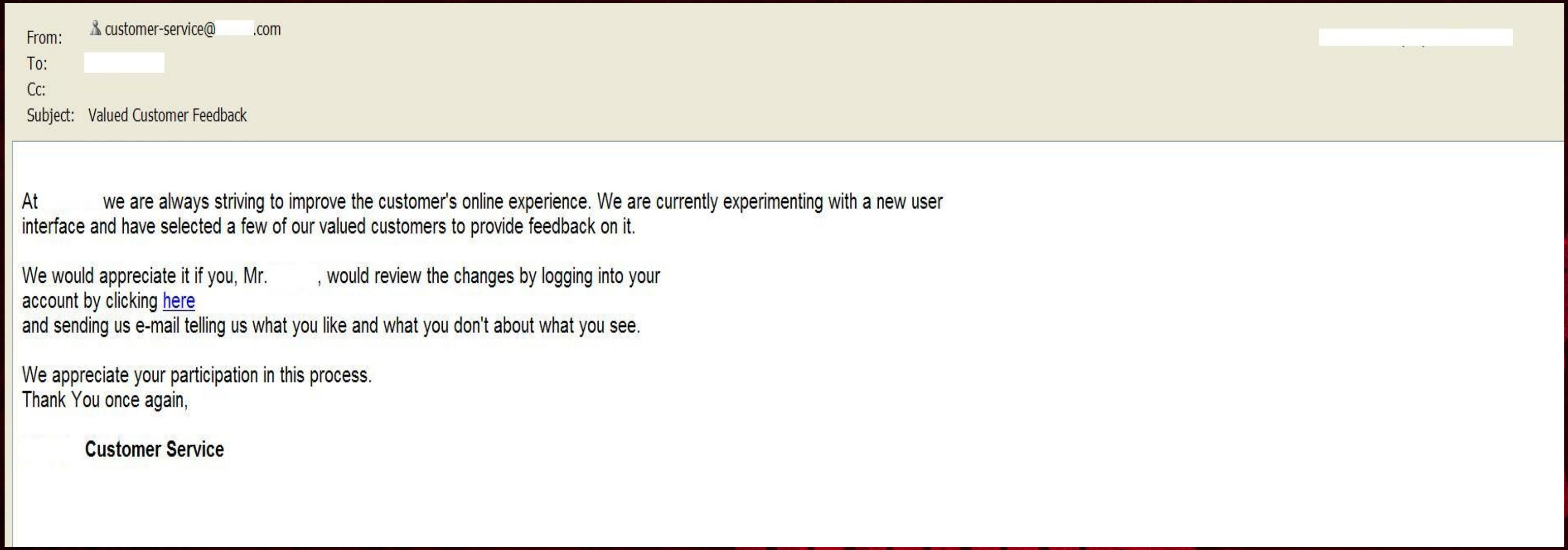
```
LogParser -o:csv "select * INTO
  sessionid.csv from *.log where
     cs-uri-query like
  '%90198e1525e4b03797f833ff4320af39'
  "
```

Can You Find The Smoking Gun?

```
#Fields:time   c-ip             cs-      cs-uri-stem     cs-uri-query                                       Status
                                method
     1:18:15172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200

     1:23:16172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200

     1:28:15172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200

            .      .            .           .                          .                                    .

            .      .            .           .                          .                                    .


    13:53:15172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200

    13:58:15172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200

    14:03:15172.16.22.33        POST     /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39            200
```

Phishing?

- No indications of key logging trojans, malware, viruses, etc. were found on the victim’s computer.
- Look what we found in the archived .pst file:



From: customer-service@[redacted].com [redacted]

To: [redacted]

Cc:

Subject: Valued Customer Feedback

At [redacted] we are always striving to improve the customer's online experience. We are currently experimenting with a new user interface and have selected a few of our valued customers to provide feedback on it.

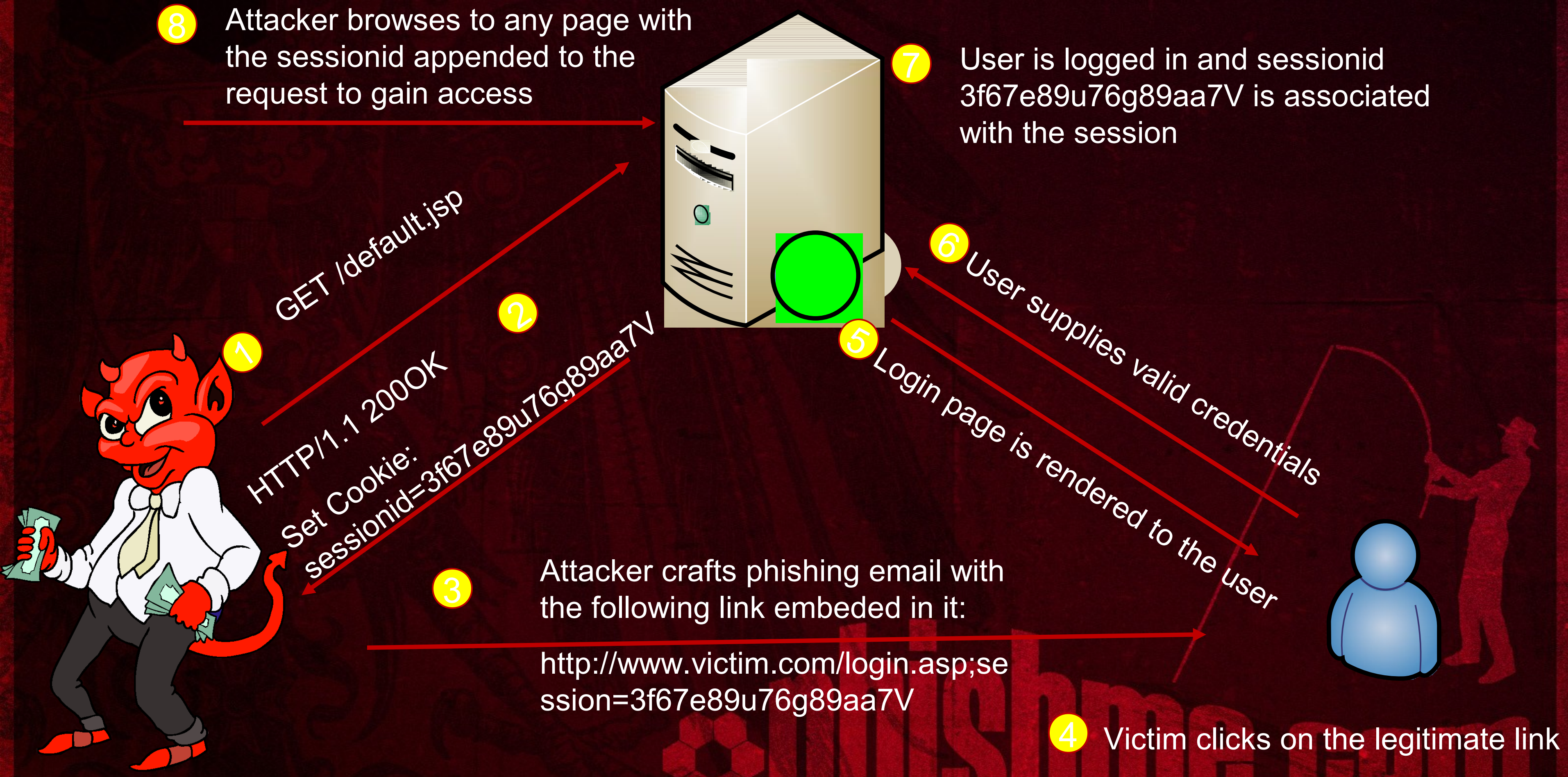
We would appreciate it if you, Mr. [redacted], would review the changes by logging into your account by clicking here
and sending us e-mail telling us what you like and what you don't about what you see.

We appreciate your participation in this process.
Thank You once again,

[redacted] **Customer Service**

URL: https://www.xyzbrokerage.com/login.asp?sessionid=90198e1525e4b03797f833ff4320af39

Session Fixation



1 GET /default.jsp

2 HTTP/1.1 200OK
Set Cookie:
sessionid=3f67e89u76g89aa7V

3 Attacker crafts phishing email with the following link embeded in it:

http://www.victim.com/login.asp;se
ssion=3f67e89u76g89aa7V

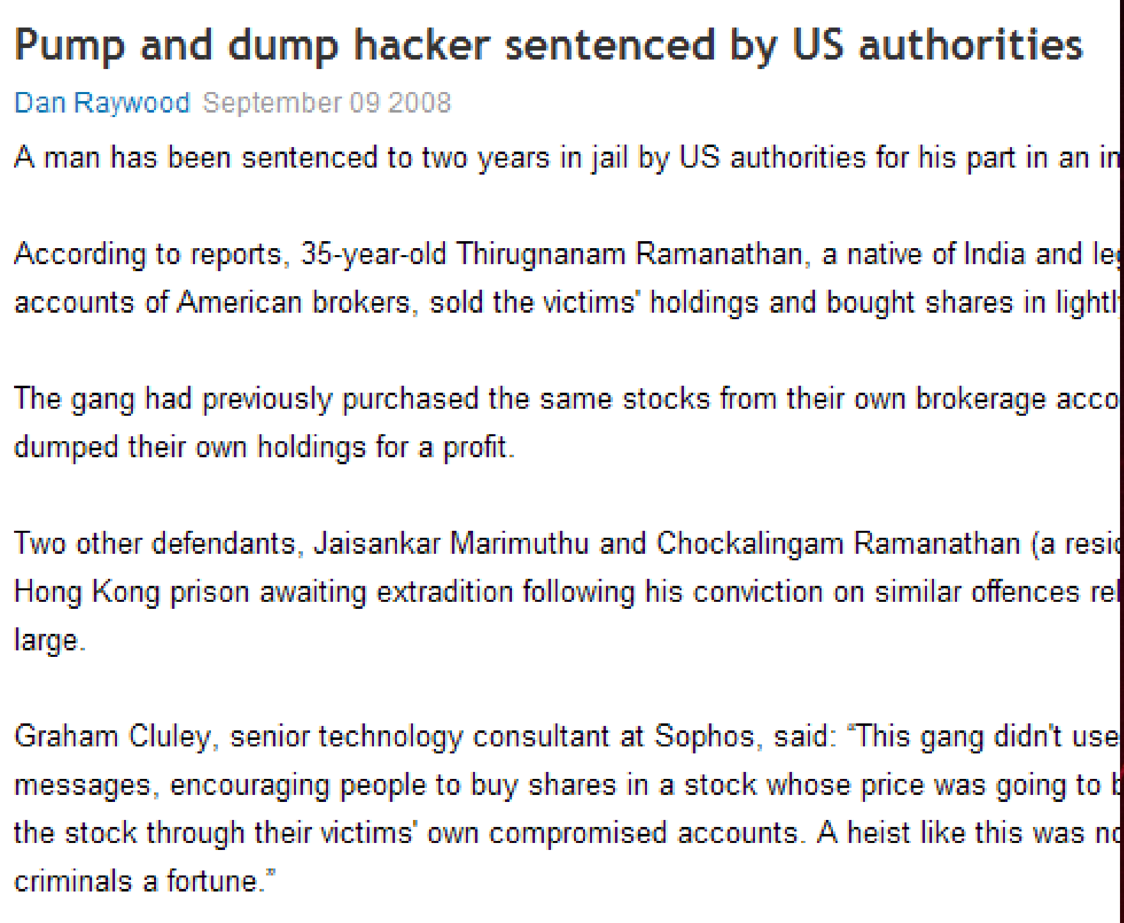
4 Victim clicks on the legitimate link

5 Login page is rendered to the user

6 User supplies valid credentials

7 User is logged in and sessionid 3f67e89u76g89aa7V is associated with the session

8 Attacker browses to any page with the sessionid appended to the request to gain access



Pump and dump hacker sentenced by US authorities

Dan Raywood September 09 2008

A man has been sentenced to two years in jail by US authorities for his part in an in

According to reports, 35-year-old Thirugnanam Ramanathan, a native of India and le
accounts of American brokers, sold the victims' holdings and bought shares in lightl

The gang had previously purchased the same stocks from their own brokerage acco
dumped their own holdings for a profit.

Two other defendants, Jaisankar Marimuthu and Chockalingam Ramanathan (a resi
Hong Kong prison awaiting extradition following his conviction on similar offences rel
large.

Graham Cluley, senior technology consultant at Sophos, said: "This gang didn't use
messages, encouraging people to buy shares in a stock whose price was going to b
the stock through their victims' own compromised accounts. A heist like this was no
criminals a fortune."

A Report From The Trenches

Symptoms

- On April 3, 2007
- Windows Security Event ID: 624 on Domain Controller

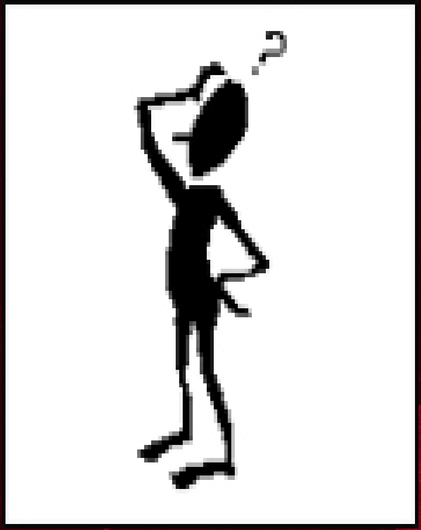
```
New Account Name: aelitasrvss
Caller User Name: SYSTEM
Privileges: administrator
```

Preliminary Investigation

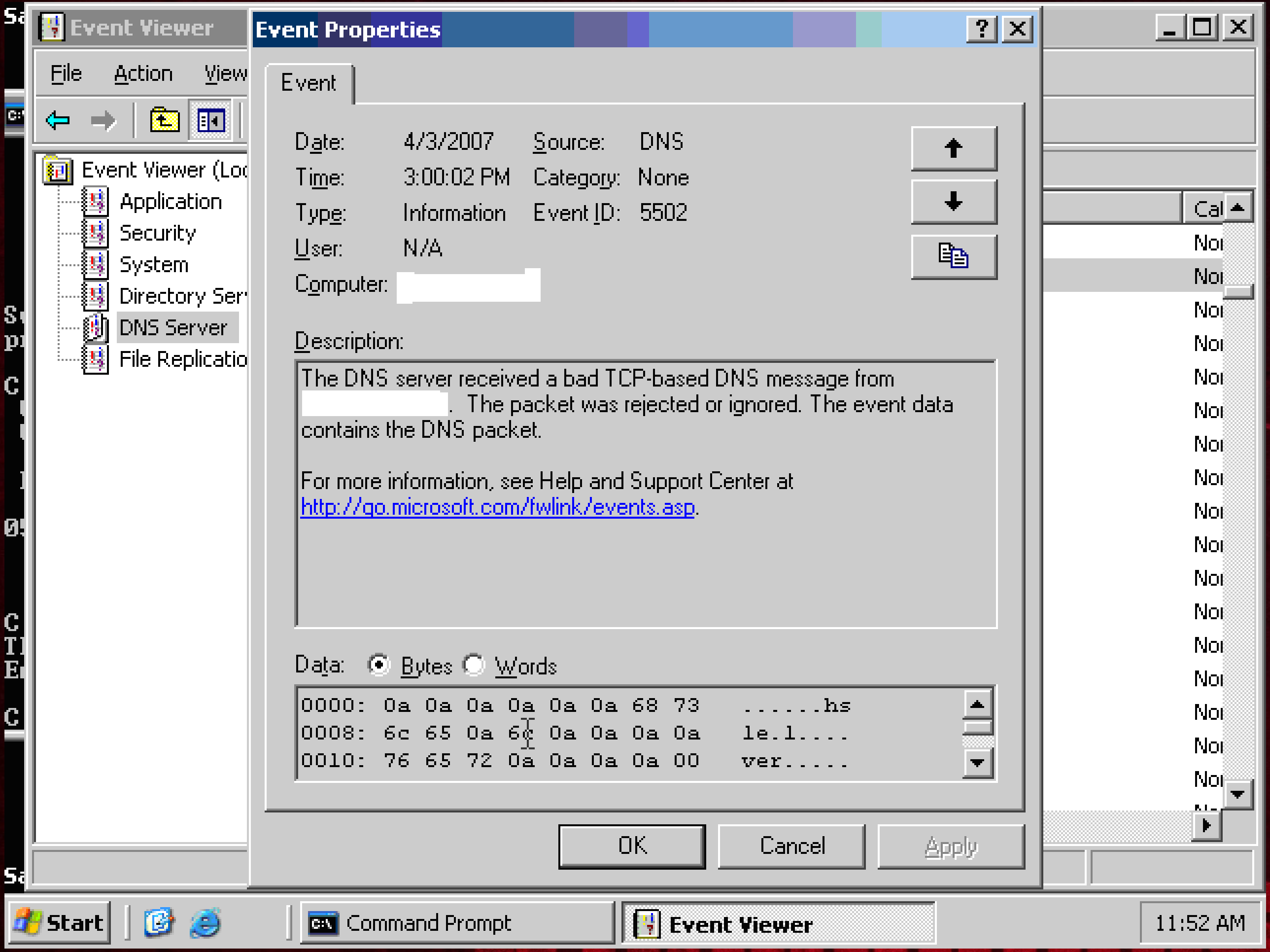
- Windows Security Event Log ID: 540 with a time stamp of (T+3) hours
- Username: `ABCDOMAIN \ ABCADMIN`
- Logon Type: 3 indicated Network Logon
- Source Network Address indicated that the logon originated from a workstation (`\\RIVER`) in the most guarded part of the network

Investigating the DC

- How did the attacker break in to the DC?
- How did the attacker run commands as SYSTEM?
- How did the attacker use an existing domain administrator account – ABCADMIN?



That's How the DC fell…



Event Properties

Date: 4/3/2007
Time: 3:00:02 PM
Type: Information
User: N/A
Computer: [redacted]
Source: DNS
Category: None
Event ID: 5502

Description:

The DNS server received a bad TCP-based DNS message from [redacted]. The packet was rejected or ignored. The event data contains the DNS packet.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 0a 0a 0a 0a 0a 0a 68 73   ......hs
0008: 6c 65 0a 6c 0a 0a 0a 0a   le.l....
0010: 76 65 72 0a 0a 0a 0a 00   ver.....
```

And what about ABCADMIN?

- This administrative account had a “strong” password
- The issue was it was hard to guess, but easy to crack

http://blog.phishme.com/2007/06/windows-pass

abili

- Using a combination of rainbow tables (ophcrack) and a password cracker (john) the password cracked in under 5 minutes!

Honing In On RIVER

- Live Response
  - `Smart Card Manager` service associated with `ipripsvc.dll`
  - An analysis of the DLL indicated that it was similar to Backdoor.Ripgof.B
  - No spurious processes

How did the attacker Own the Workstation

- The workstation wasn't Internet routable
- Did the user do something to facilitate the attack?
- Time to focus on user activity
    - Web browser history and cache
    - User's email inbox

Reviewing User Activity

- Browser History
  - Request to `/images/singup.exe` from a site in Taiwan on 3/27/2007

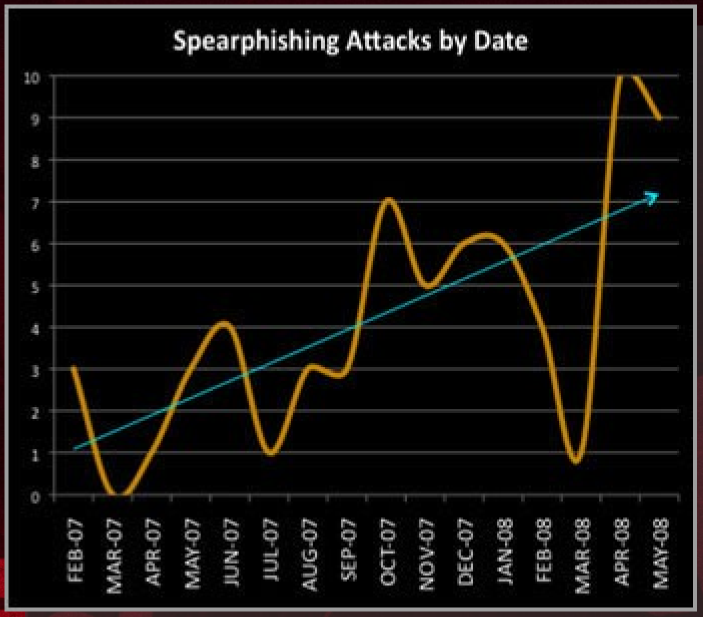
- Email Archives
  - Email from the organization’s HR department on 3/27/2007 with an attachment called Healthcare_Update.chm

Healthcare_Update.chm

- Compiled HTML
- Contained a link to /images/singup.exe
- Eureka!

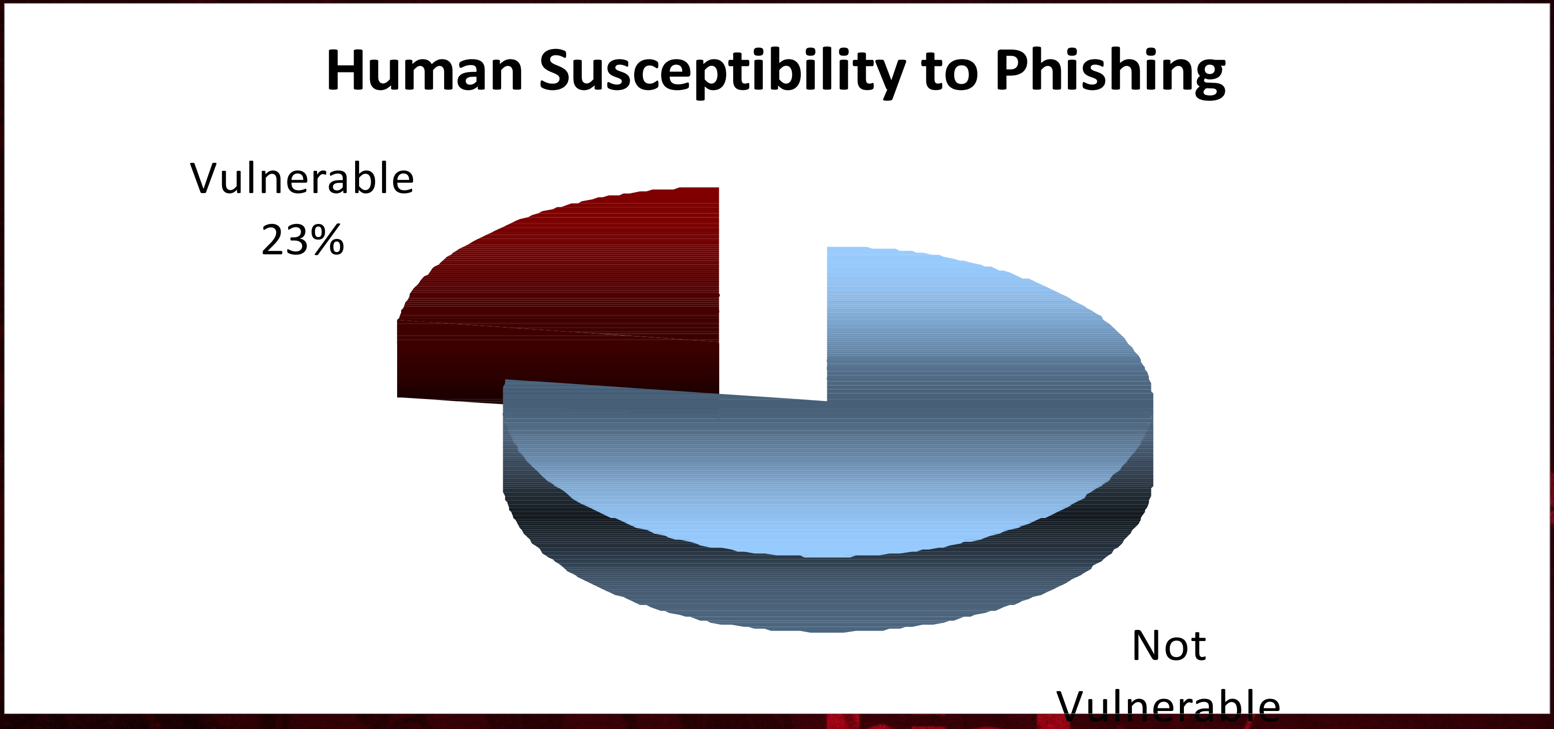
Spear Phishing Is A Problem

- > 15,000 corporate victims in 15 months
- Victim Losses have exceeded $100,000
- Recent Victims
  - Salesforce.com
  - Critical infrastructure at large energy company



Sources: iDefense Labs, Washington Post

How Vulnerable Are We?



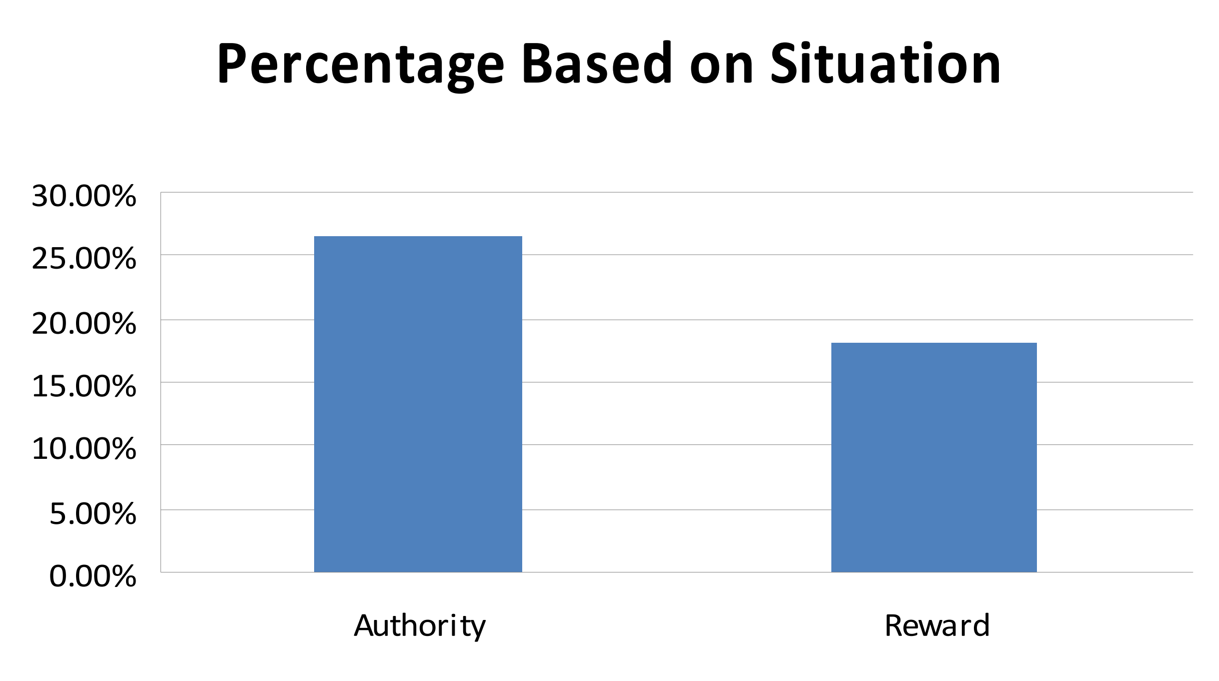
* ± 3% Margin of Error

How Does It Work?

Authority

Reward

Authority V/S Reward



Conclusion

Thank You

phishme.com

Rohyt Belani CISSP, CISM

rohyt.belani@intrepidusgroup.com