

# Phishing 2.0

Breaking Into Wall Street & Critical Infrastructure

FSP Toronto

May 2008



## Intrepidus Group

- Information security consultancy
- Former Foundstone, McAfee, Symantec, Air Force, Lucent and EDS engineers
- Offices in NYC and Chantilly, VA
- Regular speakers at Black Hat, DefCon, OWASP, HITB, ISSA, and MISTI events
- Faculty at Carnegie Mellon University



## Phishing – Passé Definition

(fish'ing) (n.) The act of sending an e-mail 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.

phishme.com

Intrepidus Group, Inc. © 2007

## Example banking “phish”

☆ from: **Account Information <bankofamerica@yahoo.com>** [hide details](#) 9:05 am (1 hour ago) [Reply](#)

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://0xctb5c3a88/cons/www.bankofamerica.com/online/online\\_secure/](http://0xctb5c3a88/cons/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.

phishme.com

Intrepidus Group, Inc. © 2007

## 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- because 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=piUq3027gcHw003nfaJ2@sd96V.pIsEm.NeT/3/?3X6CMW2I2uPOVQW>

Y-----

Thank you for using Citibank!

C-----

Intrepidus Group, Inc. © 2007

## 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.

The logo for phishme.com features a stylized gear icon to the left of the text "phishme.com". The text is in a bold, lowercase, sans-serif font. A red silhouette of a fisherman with a bow is positioned to the right of the text.

Intrepidus Group, Inc. © 2007

## A Report From The Trenches



 phishme.com

Intrepidus Group, Inc. © 2007

## 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.

 phishme.com

Intrepidus Group, Inc. © 2007

## 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.



Intrepidus Group, Inc. © 2007

## 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.



Intrepidus Group, Inc. © 2007

## 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

phishme.com

Intrepidus Group, Inc. © 2007

## 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%'"
```

phishme.com

Intrepidus Group, Inc. © 2007

## Can You Find The Smoking Gun?

#Fields:time	c-ip	cs-method	cs-uri-stem	cs-uri-query	Status
1:03:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:04:35	172.16.54.33	POST	/execute.asp	sessionId=3840943093874b3484c3839de9340494	200
1:08:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:10:19	172.16.87.231	POST	/execute.asp	sessionId=298230e0393bc09849d839209883993	200
1:13:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:18:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:19:20	172.16.121.3	POST	/execute.asp	sessionId=676db87873ab0393898de0398348c89	200
1:21:43	172.16.41.53	POST	/execute.asp	sessionId=3840943093874b3484c3839de9340494	200
1:23:16	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:28:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200

phishme.com

Intrepidus Group, Inc. © 2007

## 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'  
"
```

phishme.com

Intrepidus Group, Inc. © 2007

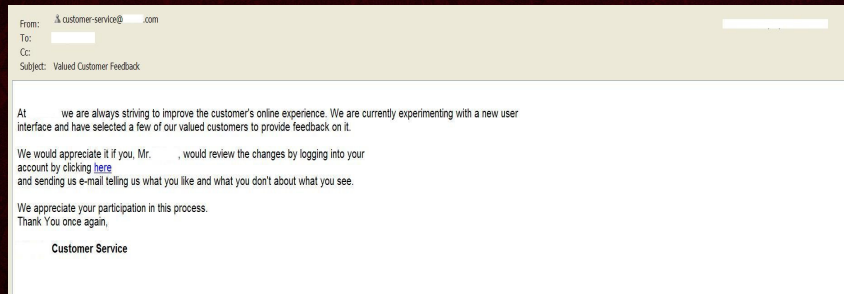
# Can You Find The Smoking Gun?

#Fields:time	c-ip	cs-method	cs-uri-stem	cs-uri-query	Status
1:18:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:23:16	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
1:28:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
.	.	.	.	.	.
13:53:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
13:58:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
14:03:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
14:07:23	172.16.14.166	POST	/login.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
14:07:54	172.16.14.166	POST	/account.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
14:08:15	172.16.22.33	POST	/execute.asp	sessionId=90198e1525e4b03797f833ff4320af39	200
14:10:09	172.16.22.33	POST	/confirm.asp	sessionId=90198e1525e4b03797f833ff4320af39	200

Intrepidus Group, Inc. © 2007

# 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:



URL: <https://www.xyzbrokerage.com/login.asp?sessionId=90198e1525e4b03797f833ff4320af39>

Intrepidus Group, Inc. © 2007

## Session Fixation

The application was confirmed to be vulnerable to session fixation:

- A session id was issued before login
- The same session id was used by the application after login for the purposes of user authorization
- This allowed an attacker to hijack legitimate user sessions using a bit of social engineering

  
pinishme.com

Intrepidus Group, Inc. © 2007

## A Report From The Trenches



  
pinishme.com

Intrepidus Group, Inc. © 2007

## Symptoms

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

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

The logo for phishme.com, featuring a stylized gear icon to the left of the text "phishme.com".

Intrepidus Group, Inc. © 2007

## 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

The logo for phishme.com, featuring a stylized gear icon to the left of the text "phishme.com".

Intrepidus Group, Inc. © 2007

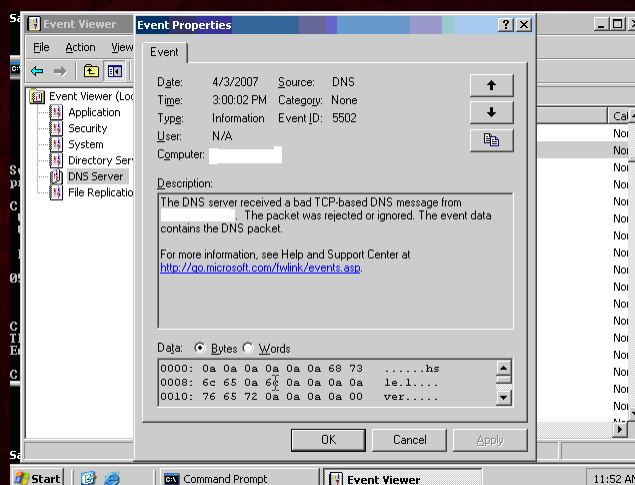
# Investigating the DC

- How did the attacker break in to the DC?
  - No traces of password guessing
  - DC was up to date on patches...or at least MBSA so reported
- How did the attacker run commands as SYSTEM?
- How did the attacker use an existing domain administrator account – ABCADMIN?



Intrepidus Group, Inc. © 2007

# That's How the DC fell...



Intrepidus Group, Inc. © 2007

## And what about ABCADMIN?

- This administrative account had a “strong” password
- The issue was it was hard to guess, but easy to crack
- Using a combination of rainbow tables (ophcrack) and a password cracker (john) the password cracked in under 5 minutes!

<http://blog.phishme.com/2007/06/windows-passwords-guess-ability-vs-crack-ability/>



Intrepidus Group, Inc. © 2007

## 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

  
phishme.com

Intrepidus Group, Inc. © 2007

## 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



Intrepidus Group, Inc. © 2007

## 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`



Intrepidus Group, Inc. © 2007

## Healthcare\_Update.chm

- **C**ompiled **H**TML
- Contained a link to /images/singup.exe
- Eureka!



Intrepidus Group, Inc. © 2007

## Conventional Countermeasures

### User Awareness Campaigns

- Poster Campaigns
- Brown Bag Sessions



### Reactive Technologies

- Email Filtering Software
- Cousin Domain Monitors
- Site Takedown Services

Intrepidus Group, Inc. © 2007

## Mock Phishing Exercises

- **Recommended by SANS Top 20 (2007)**

“The most promising method of stopping spear phishing is continuous periodic awareness training for all users; this may even involve **mock phishing attempts** to test awareness ”

- **CMU study finds them to be the most effective user training mechanism (Oct 2007)**

“..users learned more effectively when the **training materials were presented after they fell for the phishing** attack (embedded) than when the training materials were sent by email (non-embedded)...”

Intrepidus Group, Inc. © 2007



- 10,000 employees “phished”
- First run...
  - 75% of employees opened the email
  - 17% followed the link
  - 15% entered data
- Second Run ...
  - Only 8% even opened the email

Source: Wall Street Journal





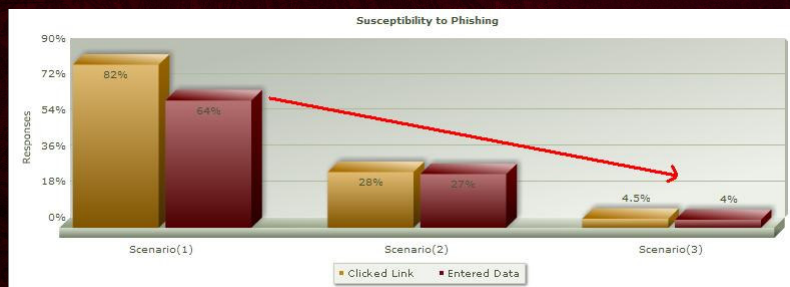
- 500 Cadets “phished”
- 80% fell prey
- Mock Phishing Exercises run Quarterly

Source: Wall Street Journal



## Intrepidus Group Client

- 24,000 employees
- 3 times in a 12 month period
- Significant Improvement



Thank You

The logo for phishme.com, featuring a stylized gear icon with red and grey segments to the left of the text "phishme.com" in a white, bold, sans-serif font.

A larger, semi-transparent version of the phishme.com logo, including the gear icon and the text "phishme.com", positioned in the lower right area of the slide.

Intrepidus Group, Inc. © 2008

