

Spear Phishing: A Report From The Trenches



Key Points

- Evolution of Phishing Attacks
- Case Study
- How Vulnerable Are We?
- If I Were A Phisher...



Intrepidus Group

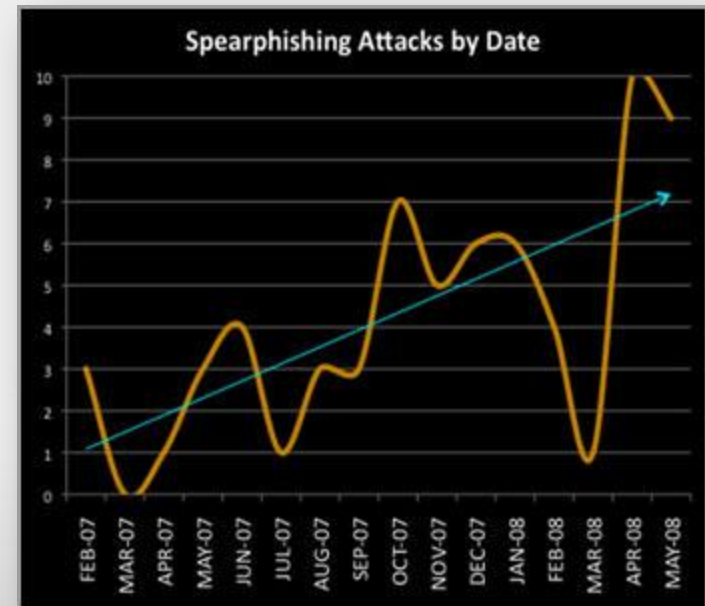
- Company
 - Information security boutique
 - Product: PhishMe.com
- Team
 - Former Foundstone, McAfee, Symantec, Lucent
 - Faculty at Carnegie Mellon University
 - Speakers at ISSA, MISTI, FISSEA, OWASP, Black Hat, DefCon, and ShmooCon

What Is Spear Phishing?



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



SANS – September 15 2009

SANS: Security Ignores the Two Biggest Cyber Risks

Client-side application vulnerabilities and insecure web apps deserve more attention than operating systems bugs, says new research from SANS Institute

» Comments

By Joan Goodchild, Senior Editor

September 15, 2009 — CSO —

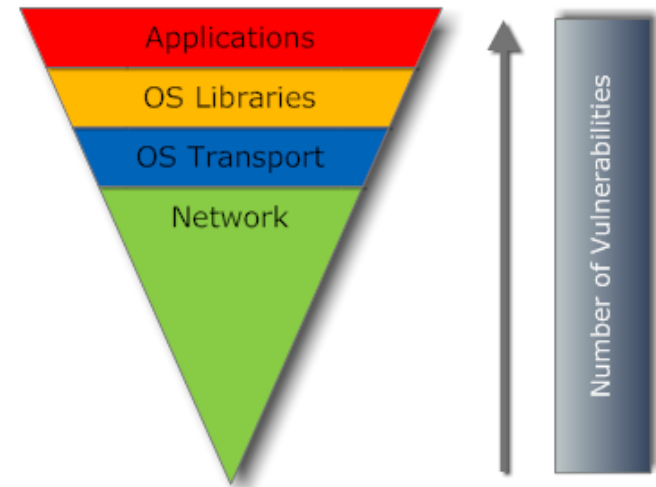
Two major cyber risks dwarf all others, but organizations are failing to invest in the proper tools to mitigate them, choosing instead to focus security attention on lower risk areas, according to a report released Tuesday by SANS Institute.

The research, which draws upon data collected from March to August 2009 from thousands of organizations, claims companies give insufficient attention to today's risks and put their systems in peril by continuing to maintain the status quo with an emphasis on operating system patches and other outdated protection methods. Attack data for this research was drawn from TippingPoint appliances deployed at customer sites, while vulnerability data was collected from Qualys scanning services.

Also see 7 Reasons Websites Are No Longer Safe

The most surprising conclusion may be that client-side application software vulnerabilities pose the largest threat to network security as opposed operating system vulnerabilities, which tend to get more attention when it comes to patching. SANS claims many spear-phishing attacks exploit vulnerabilities in commonly-used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office.

"This is currently the primary initial infection vector used to compromise computers that have Internet access," the report states.

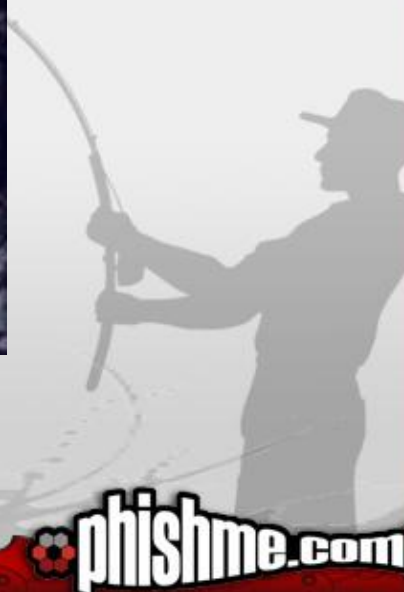


Source: SANS Top Cyber Security Risks – www.sans.org

Evolution of Phishing Attacks

- Spam-like mass phishing campaigns were easy to identify
- Targeted (Spear) phishing attacks -
 - Are low volume
 - Are difficult to differentiate from legitimate emails
 - Are technically advanced
- Anti-Phishing filters have a hard time!

A Report From The Trenches



Symptoms

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

New Account Name: xyzservice

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...

The screenshot shows the Windows Event Viewer application with the 'Event Properties' dialog box open. The event is from the 'DNS Server' log, dated 4/3/2007 at 3:00:02 PM. The event type is 'Information' with ID 5502. The description states: '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.' Below the description, the event data is displayed in hexadecimal and ASCII format.

Event Properties

Event

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

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	68	73hs
0008:	6c	65	0a	6c	0a	0a	0a	1e.1....
0010:	76	65	72	0a	0a	0a	0a	ver.....

Taskbar: Start | Command Prompt | Event Viewer | 11:52 AM

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-passwords-guess-ability-vs-crack-ability/>

- 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/temp.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`

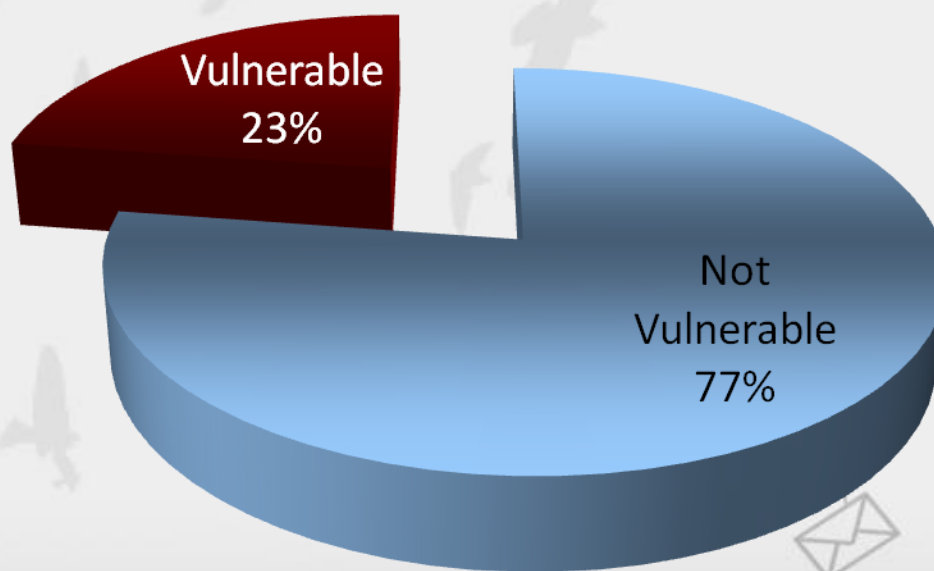
Healthcare_Update.chm

- **Compiled HTML**
- Contained a link to </images/temp.exe>
- Eureka!



How Vulnerable Are We?

Human Susceptibility to Phishing



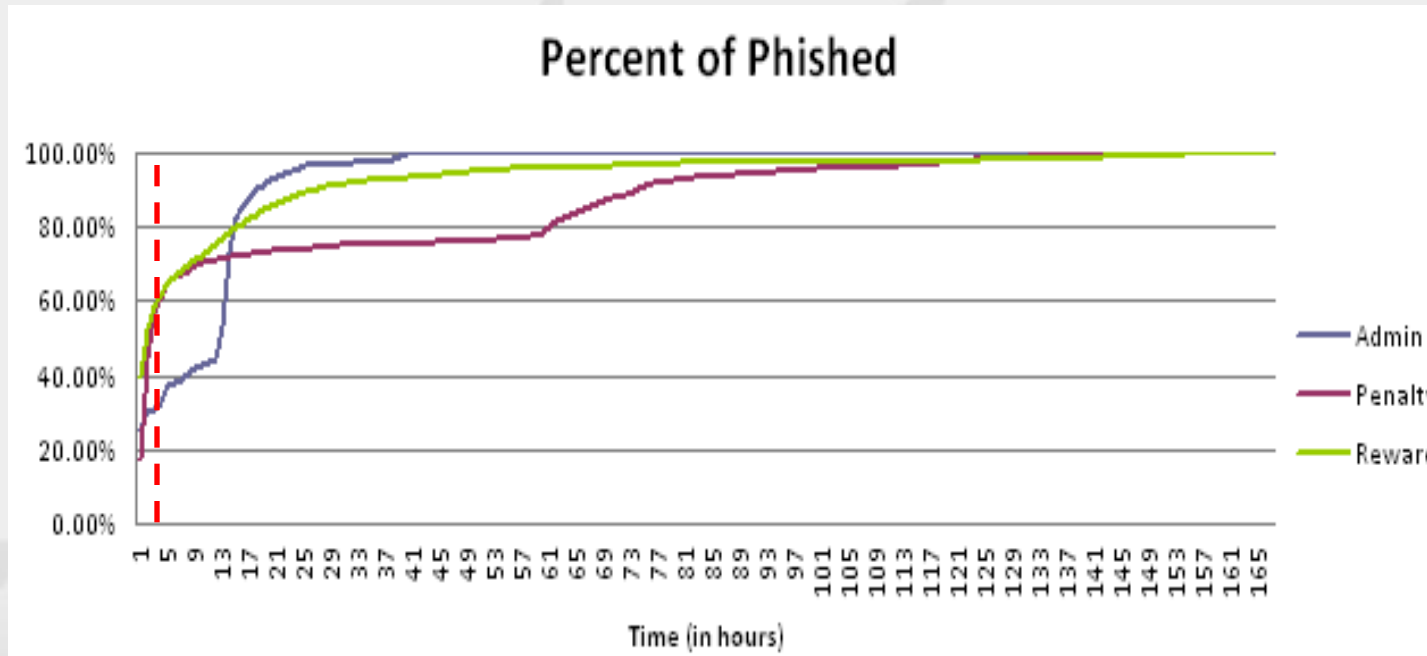
* 3% Margin of Error

Technical Controls

- Filters look for:
 - High volume which does not exist
 - Raw IP Address-based URLs
 - Lack of Personalized Salutation
 - Established Black Lists
- Site Takedown Services
 - Guarantee takedown within 4 hours



Is Four Hours Fast Enough?



How Does It Work?

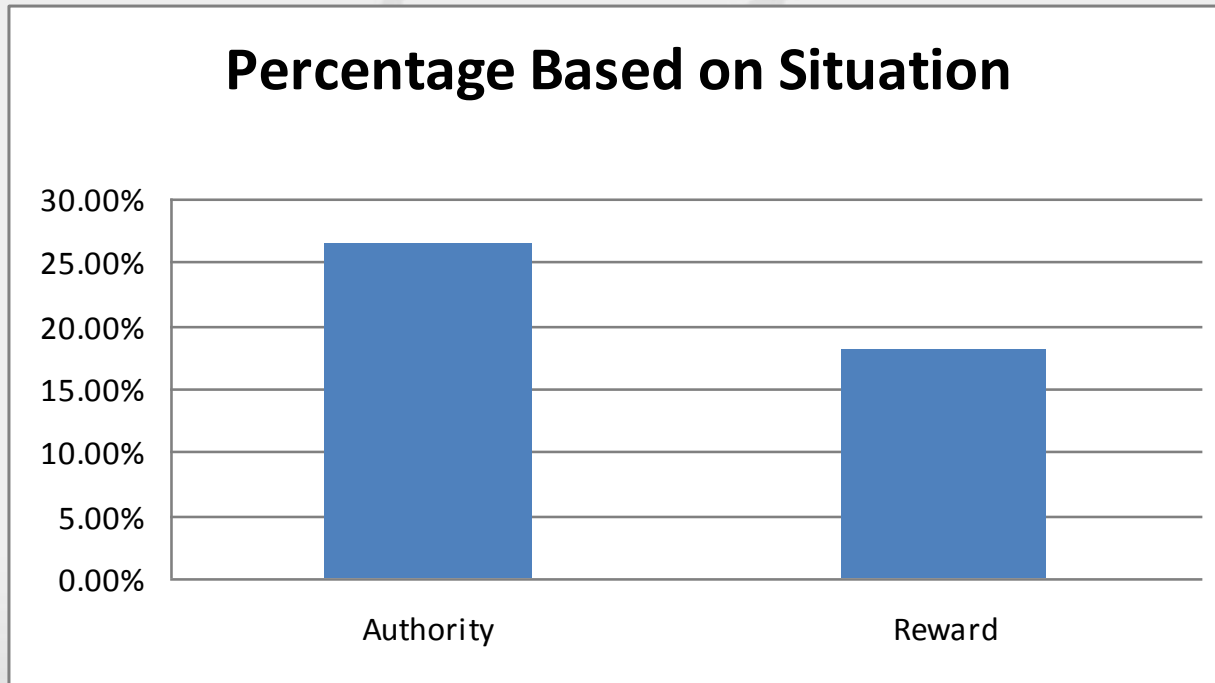
Authority



Reward



Authority V/S Reward



If I Were A PhisherMan I Would...

- Identify key targets using Google and the target company's website
- Use an authority-based scenario
- Procure a fake SSL certificate and make the phishing link https

<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202423911432>

If I Were A PhisherMan I Would...

- Employ click-based malware or send malware via file attachments
- Spend time on replicating the official look and feel in the phishing email and website

Conventional Countermeasures

- Brown Bag Sessions
- Security Posters
- Email Blasts



There Is A Better Way...

Mock Phishing Exercises

- Emulate real phishing attacks
- Train subjects by example
- Measure susceptibility



Expert Opinions

The SANS logo is displayed in a white rectangular box. The word "SANS" is written in a blue, serif font with horizontal lines through the letters.

“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 ”

The Carnegie Mellon logo is presented in white text on a dark red rectangular background.

“..users learned more effectively when the training materials were presented after they fell for the phishing attack than when the training materials were sent by email..”

Conclusion



Thank You

 phishme.com



 phishme.com