Ethical Phishing Case Study

Maven Security Consulting Inc
www.MavenSecurity.com
1-877-MAVEN-HQ (+1-877-628-3647)
Agenda – Phishing Intro

- **phishing (v.)**
  - pronounced “fishing”
  - fake web site that impersonates a legitimate site
  - site captures personal data entered by victim (e.g. password)
  - (optional) spoofed email directs user to fake site
  - Full definition: http://www.wordspy.com/words/phishing.asp
“Ethical Phishing” – where you throw the fish back.

- Maven Security

Ethical Phishing – Maven Security Case Study

**Situation**
- Insurance company
- 1300 small remote offices for agents
- remote locations using DSL, dial-up, satellite, ISDN, for Internet
- agents access Insurance mainframe through HTTPS via Internet

**Objective**
- Get access to policy holder data on mainframe

**Defenses**
- Dynamic IP (i.e. moving targets)
- ISP IP Ranges (not identifiable as Insurance company employees)
- NAT router/firewall (no way to initiate connection from outside)

**Results**
- It took 15 minutes to get access to the mainframe

Case Study – A Closer Look (3-in-1)

• **Actually three separate attacks**
  – *Web bug in HTML email*
    • Result: revealed dynamic IP addresses in real time
  – *Classic phishing attack*
    • Result: User credentials stolen for web portal and main frame access
  – *Phishing + IE holes*
    • Result: Remote access gained to user’s desktop computer behind firewall
Case Study – Attack 1: Web Bug

• Send agents an HTML email with web bug
  – `<img src="http://www.mavensecurity.com/webbug.php" width=1 height=1>`

• Web bug pointed to script

• Script returned 1 pixel GIF image

• Script emailed the source IP address of the request to me (i.e. agent’s router/firewall address)

• Result: 2 of the 5 routers were compromised
  – one had trivial password on Cisco
  – one was Linksys with firmware vulnerability

• Created NAT pass-thru for my source IP address
  – Scanned the “non”-routable internal addresses behind the router/firewall

Case Study – Attack 2: Classic Phishing

- **Sent “spoofed” email**
  - Outlook & Outlook Express makes this easy (pseudo email spoof, or spoofing email for dummies)
    - Outlook: “Have replies sent to...bill@microsoft.com”
    - Outlook Express: “Display name: bill@microsoft.com”

- **Email contained misleading HTML link which pointed to spoofed web site that collected login data**

Case Study – Misleading HTML Links

- **HTML hypertext links can say one thing but mean another**

  \<A href="http://evil.site">http://friendly.site</A>\n
- **Above HTML gets rendered as:**
  - http://friendly.site

- **This is a fundamental feature of HTML and will not go away.**
Case Study – Attack 2: Classic Phishing

- **Email had misleading URL pointing to spoofed site**

A recent security test by a third-party vendor has caused your Agent Resources Login account to become locked. The link below contains a security token required to reactivate access to your account. Click the link below and login as normal to re-enabled your account.

https://biginsurance.dom/server1/AgentLogin?TOKEN=83jkwk8Ne5AQ28l93kdDud98gK49

We're sorry for any inconvenience.

John Doe
Supervisor, Information Services
Big Insurance Company
555-KL5-1234
jdoe@biginsurance.dom

Misleading hyperlink pointing to a web site different from the one displayed to user.
The Final Word on HTML Email

• **Impact**
  – More spam: web bugs validate your email address
  – Hacker GPS: They will get your IP address from the web bug
  – Worms & exploits: Potential for browser bugs being exploited via email

• **HTML + Email = wrong!**
  – “Two great tastes that taste bad together”
  – “A combination mother nature never intended”
  – “Friends don’t let friends use HTML email”

  – Just say no!
Case Study – Attack 3: Phishing + IE Hole

• **Spoofed HTML email with misleading URL**
• **Spoofed web site initiated software install**
• **But software was not digitally signed by a trusted party**
  
  – Browser generates warning
Case Study – Chromeless Windows

• **Microsoft’s Internet Explorer (IE) web browser has a “feature” called “chromeless windows”**.

• **This allows a borderless window to open in front of other windows.**

• **Result**

  – Security warning boxes now look safe!

Chromeless Windows – You won’t know who to trust!

- **Before chromeless windows**

![Security Warning](slide12.png)

Warning: The authenticity of this content cannot be verified, therefore it cannot be trusted.

Problem listed below:

The root certificate has not been enabled for the requested use.

Do you want to install and run signed on an unknown date/time and distributed by:

Thawte Freemail Member

![Security Warning](slide12.png)

- **After chromeless windows**

Warning: The authenticity of this content cannot be verified, therefore it cannot be trusted.

Problem listed below:

The root certificate has not been enabled for the requested use.

Do you want to install "Agent Patch v2" signed on 08/20/2003 6:47 PM and distributed by:

Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Click YES to continue.

Yes | No | More Info | Yes
Case Study – Attack 3: Spoofed HTML Email

It has come to our attention that the recent Blaster worm patch we deployed may not have been completely effective on a few agent desktops. Your PC may be one of the system's not fully patched.

…

Please use the link below to begin the new patch installation process.

http://biginsurance.dom/server1/agent-patch2/K9s7jUjw7eud26cIjWu73mS/

We're sorry for any inconvenience.

John Doe
Supervisor, Information Services
Big Insurance Company
555-KL5-1234
jdoe@biginsurance.dom

Misleading hyperlink pointing to a web site different from the one displayed to user.
Case Study – Attack 3: The Result

• Software was remote desktop control software – VNC
  http://www.tightvnc.com/
• Wrapped in a custom install script which caused VNC to connect outward to us – defeating non-routable IPs behind a NAT firewall

Result: Instant remote access to user’s desktop. We can see everything they are doing in real time.
Phishing Defenses

- **Keep your browser up-to-date**
  - Microsoft Security Bulletin MS04-004

- **IE is now fixed...sort of.**
  - Chromeless windows still work!

- **Use a non-IE browser**
  - Free: Mozilla, Firefox, Camino (Mac), [http://mozilla.org](http://mozilla.org)
  - Google for more

- **Disable HTML email**

- **FTC Consumer Alert Tips**

- **When in doubt, type the URL**