A Crypto Nerd’s Imagination:
His laptop’s encrypted.
Let’s build a million-dollar cluster to crack it.

No good! It’s 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:
His laptop’s encrypted.
Drug him and hit him with this $5 wrench until he tells us the password.

GOT IT.
Security & Trust

Trends on security and trust within the Internet – A focus on Phishing trends and some solutions
Background

• In the past several months a series of highly sophisticated and targeted cyber attacks has revealed a shift in the threat arena and their persistence on networks (APT buzz)

• Attackers are moving beyond schemes to acquire financial data (such as credit cards and identity theft) and are pursuing high-value digital assets such as intellectual property, access to critical operations, and other proprietary data systems

• We are involved with businesses in attempt to review possible strategies and validation of business models that aim to offer mitigation against a portion of this space.
Social Engineering

• Most recent compromises that are reported use a technique called social engineering

• Defined - social engineering is using deception, manipulation, and influence to convince a human who has access to a computer system to do something, such as click on an attachment or a link in an email

• Social-engineering schemes historically use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords.

• Recent attacks now bundle this method via spear phishing, which leads to a much more targeted attack; in order to access to a key person’s workstation, data, etc.
Spear Phishing

• Phishing is a mechanism that employs both social engineering and malicious means to steal identity & financial account credentials

• Defined – Phishing is the act of tricking someone into surrendering private information over the Internet, follows the idea of actual fishing — you throw out bait with the hopes that while some ignore it, others will bite.
  • Traditional attacks mimic financial sites to collect credentials or online shopping sites to collect credit card data
  • Attacks most commonly come in the form of emails or messages that contain viral links.

• Recent trends show an increase of compromises that use techniques to allow an attacker access to a key person
Increased Effectiveness - Social Networking

• Social Networks make it easy.....one can go into Twitter, Facebook, LinkedIn, etc. to search for someone or use current events to lure recipients to react to a communication
• Online communities are powerful, trusted and perfect for cyber crime to leverage such relationships
  • Social networking attacks leverage a trusted link between friends, either to deliver malware or to phish for confidential and financial information.
  • Easier for attackers to spread malicious software through links, photos and applications because those users are typically more trusting
Increased Effectiveness - Social Networking

• At the end of 2010, nearly 85 percent of recorded phishing attempts used social networks as a lure, up from 8.3 percent at the start of the year.

• Tiny URLs have also enabled better hiding of phishing domains from users. Phishing detection software generally looks for HTML-based content, hence some attacks are using Flash, JavaScript and MIME type content that autocorrects to HTML in browsers for success.
Phishing Trends – Reports 2H2010

- Phishing reports submitted to APWG during the second half 2010

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
Phishing Trends – Sites Detected 2H2010

- Sites reported to APWG reached the highest point in September 2010

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
### Trends - 2H2010

#### Phishing Trends per APWG (member report):

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique phishing email reports received by APWG from consumers</td>
<td>26,353</td>
<td>25,273</td>
<td>22,188</td>
<td>23,619</td>
<td>23,017</td>
<td>21,020</td>
</tr>
<tr>
<td>Number of unique phishing web sites detected</td>
<td>30,582</td>
<td>29,713</td>
<td>31,705</td>
<td>28,985</td>
<td>29,226</td>
<td>26,124</td>
</tr>
<tr>
<td>Number of brands hijacked by phishing campaigns</td>
<td>274</td>
<td>301</td>
<td>335</td>
<td>317</td>
<td>305</td>
<td>279</td>
</tr>
<tr>
<td>Country hosting the most phishing websites</td>
<td>Sweden</td>
<td>Sweden</td>
<td>Sweden</td>
<td>USA</td>
<td>USA</td>
<td>USA</td>
</tr>
<tr>
<td>Contain some form of target name in URL</td>
<td>82.82%</td>
<td>95.13%</td>
<td>92.94%</td>
<td>79.93%</td>
<td>76.44%</td>
<td>75.86%</td>
</tr>
<tr>
<td>No hostname; just IP address</td>
<td>1.45%</td>
<td>0.84%</td>
<td>1.93%</td>
<td>3.89%</td>
<td>15.11%</td>
<td>3.05%</td>
</tr>
<tr>
<td>Percentage of sites not using port 80</td>
<td>0.12%</td>
<td>0.10%</td>
<td>0.23%</td>
<td>0.60%</td>
<td>0.43%</td>
<td>0.48%</td>
</tr>
</tbody>
</table>

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
Phishing Trends - Global

- Phishing trends saw a global increase (vs APWG member rpt)
  - Average site uptime – 73 hours (longest measurement)
  - Age of site ? (turnaround - currently reviewing)

<table>
<thead>
<tr>
<th></th>
<th>2H2010</th>
<th>1H2010</th>
<th>2H2009</th>
<th>1H2009</th>
<th>2H2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing domain names</td>
<td>42,624</td>
<td>28,646</td>
<td>28,775</td>
<td>30,131</td>
<td>30,454</td>
</tr>
<tr>
<td>Attacks</td>
<td>67,677</td>
<td>48,244</td>
<td>126,697</td>
<td>55,698</td>
<td>56,959</td>
</tr>
<tr>
<td>TLDs used</td>
<td>183</td>
<td>177</td>
<td>173</td>
<td>171</td>
<td>170</td>
</tr>
<tr>
<td>IP-based phish (unique IPs)</td>
<td>2,318</td>
<td>2,018</td>
<td>2,031</td>
<td>3,563</td>
<td>2,809</td>
</tr>
<tr>
<td>Maliciously registered domains</td>
<td>11,769</td>
<td>4,755</td>
<td>6,372</td>
<td>4,382</td>
<td>5,591</td>
</tr>
<tr>
<td>IDN domains</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>13</td>
<td>10</td>
</tr>
</tbody>
</table>

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
Trends 2H-2010

• Phishing Attacks by TLD:

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
Trends Q2-2011

- Phishing Attacks by TLD:

Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.
AV Solutions – Impact or Lack Thereof

• Methodology generally ineffective against antivirus clients given lag in detection rates (cat & mouse)
• Malware Detection Rates by AV Vender (2010):

<table>
<thead>
<tr>
<th></th>
<th>Trend Micro</th>
<th>Sophos</th>
<th>McAfee</th>
<th>Kaspersky</th>
<th>F-Secure</th>
<th>Dr Web</th>
<th>AVG</th>
<th>Nod32</th>
<th>F-Prot</th>
<th>Virus Buster</th>
<th>Norman</th>
<th>eTrust-Vet</th>
<th>Symantec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>17%</td>
<td>20%</td>
<td>22%</td>
<td>22%</td>
<td>27%</td>
<td>7%</td>
<td>13%</td>
<td>37%</td>
<td>17%</td>
<td>10%</td>
<td>17%</td>
<td>16%</td>
<td>21%</td>
</tr>
<tr>
<td>Day 8</td>
<td>29%</td>
<td>36%</td>
<td>53%</td>
<td>87%</td>
<td>50%</td>
<td>29%</td>
<td>85%</td>
<td>86%</td>
<td>23%</td>
<td>30%</td>
<td>29%</td>
<td>21%</td>
<td>36%</td>
</tr>
<tr>
<td>Day 15</td>
<td>32%</td>
<td>75%</td>
<td>85%</td>
<td>91%</td>
<td>59%</td>
<td>33%</td>
<td>92%</td>
<td>88%</td>
<td>34%</td>
<td>46%</td>
<td>31%</td>
<td>27%</td>
<td>43%</td>
</tr>
<tr>
<td>Day 22</td>
<td>32%</td>
<td>81%</td>
<td>86%</td>
<td>92%</td>
<td>62%</td>
<td>33%</td>
<td>92%</td>
<td>88%</td>
<td>37%</td>
<td>74%</td>
<td>32%</td>
<td>29%</td>
<td>46%</td>
</tr>
<tr>
<td>Day 30</td>
<td>38%</td>
<td>85%</td>
<td>86%</td>
<td>92%</td>
<td>64%</td>
<td>33%</td>
<td>93%</td>
<td>89%</td>
<td>39%</td>
<td>74%</td>
<td>32%</td>
<td>30%</td>
<td>47%</td>
</tr>
</tbody>
</table>

AV detection rates sourced from Cyveillance, Inc. analysis (August 2010) and are provided for examples and informative use only.
Methods of the Attack

- Reconnaissance to build knowledge of organization/-target
- Social engineering and/or spear phishing to target end users
- Exploitation of vulnerabilities at end point
- Expand to peer relationships to roam the network
- Escalation of privileges / rights
- Additional spear phishing or decrypting
- Administrators’ passwords
- Compromise of internal systems
- Exfiltration of data or other
- Cleanup
Examples of the Typical Attack

- Earthquake (Haiti / Chile)
- Japan Earthquake & Tsunami
- Chilean miners
- Poland President
- Gulf oil spill
- Michael Jackson
Examples of the Attack

• “Is this a video of you? <link>” sent from a trusted friend to a circle of friends quickly infects new systems to propagate to the next layer of friends

![Twitter Direct Message Example]

Hi, David Snyder.
You have a new direct message:

elizabethgeorge: rofl this you on here? [video link]

Reply on the web at [video link]
Send me a direct message from your phone: D ELIZABETHGEORGE
Another Possible Example

• Security Question – Password Update:

- EMAIL ACCOUNT SETUP – TO VERIFY YOUR IDENTITY, WE NEED TO ASK YOU A QUESTION NOBODY ELSE COULD ANSWER.

Q: WHERE ARE THE BODIES BURIED?
A: BEHIND THE

BEHIND THE

... NICE TRY.

DAMN.

Stick-figure strip humor sourced and courtesy of http://xkcd.com and is provided for informative use only.
Recent Sophisticated Examples

• Most recent sophisticated compromises reportedly used spear phishing which allowed the attacker access to a key person’s workstation:
• IMF: International Monetary Fund (IMF): 2011 attack gained access via spear phishing employee
• Google: Early 2010 – Attackers were able to install spyware on the resilient networks by manipulating key employees who had access to sensitive data to click on malicious links that exploited an Internet Explorer zero-day vulnerability. The attacks were timed for the holidays when IT administration is thinly staffed to cover operations.
• Q1 RSA SecurID data compromise occurred when an RSA employee clicked on a malware link in an apparent communication from a Human Resources department.

All names, logos and company data where referenced are trademarks or property of their respective owners.
Q: How many of our users would fall prey to a spear-phishing attack?

Q: Would attackers be able to hijack admin accounts?

Recent examples raise questions about important web defense strategies such as protecting remote users and office-based workers through 24/7 security…
Do Current Efforts Make Sense?

- **Troubadour & 3**
  - Uncommon (non-gibberish) base word
  - Order unknown
  - Caps? Common substitutions
  - Numerical punctuation

  Difficulty to guess: EASY
  Difficulty to remember: HARD

- **Correct horse battery staple**
  - Four random common words

  Difficulty to guess: HARD
  Difficulty to remember: You’ve already memorized it

- **~28 Bits of Entropy**

  $2^{28} = 3$ days at 1000 guesses/sec
  Plausible attack on a weak remote web service yes, cracking a stolen hash is faster, but it’s not what the average user should worry about.

  Difficulty to guess: EASY
  Difficulty to remember: HARD

- **Was it trombone? No, troubador. And one of the Os was a zero?**

  And there was some symbol...

Stick-figure strip humor sourced and courtesy of http://xkcd.com and is provided for informative use only.
What Do We Do?

• Everything - There is no one solution
• Need to use a mix of user education and layered security solutions to defend the networks
• Employees should treat emails with suspicion and IT teams should leverage multiple resources (AV, IDS, User Restrictions)
• Some other ideas:
  • Products that send phishing emails to your employees safely and easily trains your employees - immediately - when they fall for an attack
  • Gathers actionable data to finely target future employee training and how to avoid the ever evolving threat on the Internet.
  • Complete formal spear phishing awareness training
  • Separate corporate and open systems – create an “air gap”
  • If data exfiltration is discovered, collect intelligence such as: What did they take, Where was the vector, How Long, Did they Leave, Where was it sent
Mitigation Examples

• User Training Examples:
Thoughts

- The real issue isn't the type of mechanism being used to target victims. It's that users are simply not learning how to avoid being tricked on the Internet.
Our Pending Solution – “Guidon”

• Understanding that when information is shared by a user the victim knows, attackers assume (generally correctly) that the attempt will be more successful
  
  - Example 1: You see a message from a friend or a link on your Facebook news feed. You click on it only to find...... common scams
  
  - Example 2: You continue to get messages from your father/friends

• Edgemount Solutions Pending Tool Development:
  
  - Leverage historical metadata analysis for trend
  - Global IP – Country location
  - Mail Client – Proxy service (known or unknown)
  - Time of message
  - Age of IP Domain
  - Trend based on historical dates
  - Various modes: Grandparent, Parent, Technical User, Kids

“Guidon” and related intellectual property are property and trademark of Edgemount Solutions, LLC. Patent pending technology/software.
References & Various Resources

• APWG (www.antiphishing.org/index.html)
• MAAWG (www.maawg.org/)
• McAfee Security Trends & Reports (www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx)
• Verizon / Verizon Business Security (securityblog.verizonbusiness.com)
• Microsoft Security Center (www.microsoft.com/security)
• Wombat Security Technologies (www.wombatsecurity.com/contact)
• Carnegie Mellon University (cups.cs.cmu.edu/anti)
Other Fun

```
robm@homebox ~$ sudo su
Password: 
robm is not in the sudoers file. This incident will be reported.
robm@homebox ~$ 
```

```
HEY — WHO DOES SUDO REPORT THESE "INCIDENTS" TO?

YOU KNOW, I'VE NEVER CHECKED.
```

```
NICE NAUGHTY
```

Stick-figure strip humor sourced and courtesy of http://xkcd.com and is provided for informative use only.