Dissecting the Recent Cyber Security Breaches

Yu Cai
School of Technology
Michigan Technological University
Disclaimers

• Most information in this presentation was collected from various sources on the Internet.

• Although care has been taken to ensure accuracy of the information provided, the presenter assumes no responsibility therefore.

• The presenter also assumes no responsibility for the consequences of use of such information.
Thanks

• Thanks to Stephen Coty, Director of Threat Research at Alert Logic, for his talk on the Target breach.

• Thanks to Nick Bilogorskiy of Cyphort, for his talk on the Target breach.

• Thanks to John Gomez, CEO of Sensato, for his talk on the Anthem breach.

• The presenter has obtained permissions to use information from the above sources for education and research purpose.
2013 – 2015: the hack went viral

- Retailers like Target, Staples, Neiman Marcus, Michaels, and Home Depot announced breaches.
- Firms in health care (Community Health Systems, Anthem), finance (JPMorgan) and entertainment (Sony Pictures, Ashley Madison) also fell victim to cyberattacks.
- Major software vulnerabilities like the OpenSSL Heartbleed and the Shellshock vulnerability.
Target Breach: The largest hack in history - 2014

• **40 million** – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

• **70 million** – The number of records stolen that included the name, address, email address and phone number of Target shoppers.
Anthem Breach: The largest hack in history - 2015

- As many as **80 million records** were exposed
- Data breach: personal information such as their names, birthdays, medical IDs, **social security numbers**, street addresses, email addresses and employment information, including income data
- Thousands of IRS **fraudulent tax returns**...
Details of the Target breach
The Target Breach 2013

Hackers
- Email Phishing
- Get HVAC contractor credential
  - Oct, 2013

Target Corporate Network
- Login Target online billing system
- Previleged escalation
- Nov, 2013

Target Corporate Network
- Hack into Target POS central update server
  - Nov, 2013
- Install POS Malware on central server

Target POS network across the country
- 6 days: thanksgiving period
- Credit card info were collected and transferred to an internal fileshare
- Target fileshare
  - 11/27/2013

Upload credit card data files to external locations
- External servers
- 12/2/2013

Download data

Sell credit card data in black market
- 12/11/2013
- Russian / Ukraine?

Target announced the breach.
- 12/19/2013

2 weeks, 11GB data

Download data
Target Breach Timeline

- **Nov. 27th, 2013**: Malware installed
  - Malware stole credit card data for 6 days
- **Dec. 2nd**: Malware uploads stolen data
  - Hackers downloaded data for 2 weeks
- **Dec. 11th**: Forged cards selling on black market
  - Security firms noticed 10-20 fold increase in stolen cards
- **Dec. 12th**: Federal investigators warned Target
  - Target was investigating the breach internally
- **Dec. 19th**: Target announces 40M cards stolen
- **Jan. 8th, 2014**: Target announces 70M more data
- **Jan. 13th**: Target offers free credit monitoring
- **Mar. 5th**: Target CIO resign
- **May 5th**: Target CEO resign
About the Malware

• The malware is a modified version of BlackPOS or Kaptoxa (Russian for Potato).
• It runs on Point of Sale (POS) terminals and scrape memory for credit card data.
• Various POS malwares are available on cybercrime forums.
About the hacker

- The suspect in the breach is a person called “Rescator” aka “Hel”.
- The suspect is likely from Ukraine.

- The author of BlackPOS malware is called “ree4” aka “Antikiller” from Russia. However, he is not directly involved in the Target breach.
Details of the Anthem breach
Anthem Breach Timeline

- **Dec. 10, 2014**: hackers compromised a major Anthem database
  - Hackers stole data for 48 days
- **Jan. 27, 2015**: a Anthem database administrator discovered his credentials being used to run a questionable query.
- **Jan. 29, 2015**: Anthem alerted federal authorities of the data breach.
- **Feb. 4, 2015**: Anthem disclosed the breach to the public, and offer free credit monitoring services.
  - Quick & proper responses save CEO’s job (?)
About the attack

• Fraudulent domain
  – The hacker registered a domain on April 2014:
    • www.we11point.com
    • mimic the legitimate domain www.wellpoint.com
    • WellPoint is the parent company of Anthem

• Malicious VPN software
  – extcitrix.we11point.com
  – Hackers provided a fake VPN software in the fake site.
  – Citrix is a legitimate VPN software for Anthem employees and supply chain partners

• Scanbox: Javascript based attack framework
About the hacker

• Some evidence suggests the suspect is known as Axiom, Shell Crew or Group 72. Also being named as “Deep Panda”

• Commonly believed to be part of a broader Chinese Intelligence Group.
Lessons Learned
Email phishing is the starting point

*Only amateurs attack machines; professionals target people.*

- Social Engineering
- Hackers can easily make a forged email which *look almost the same as legitimate one*
  - It is dangerous to judge phishing emails based on sender’s address, subject, content, and grammar mistakes.
  - All these can be easily forged!
New Phishing Schemes

• New trend: **contextual spear phishing**
  
  – Spear: Specifically target at a small group of people!
    • For example, contractors with less IT training, or managers with high privileges...
    • Why? Bypass email filters; Avoid raising security alerts; High success rate
  
  – Contextual: Email content are well-in-context, nothing suspicious!
    • For example, a fake canvas email
    • Hackers can collect some related information from public websites and social medias.
Demo of Email Phishing

• Demo site:
  – http://www.tech.mtu.edu/~cai/temp/
  – Example 1: you can be Obama
  – Example 2: html enabled email

• In-context spear phishing
  – Example 3: fake facebook email
  – Example 4: fake canvas email
  – Example 5: fake senate election email
Practical suggestions for email phishing

• Be careful with opening email attachments
• Be careful with clicking links in emails
  • Ironically, IT security people keep telling you: “Don’t click links in emails”. But the entire IT industry keeps sending out legitimate emails with links to click.
    – If you have to click links
      • Be careful with the URL, don’t be fooled by malicious URLs
      • Never type in sensitive information in the web page redirected from email
      • Alternatively, you can open the browser, type in the URL manually or use bookmarks.
Answers to Email Phishing

• Current solutions 1 for email phishing: email filter + phishing check
  – Email filter can stop many phishing emails, but not all.
  – How to bypass or fool email filters?

• Current solutions 2 for email phishing: SPF+DKIM+DMARC
  – Really email sender identity technologies
  – End users don’t see those technologies
  – Can they stop email phishing? Arguably not
## Top 10 Phishing TLDs (Top Level Domain) s, 2014

<table>
<thead>
<tr>
<th></th>
<th>TLD</th>
<th>TLD Location</th>
<th># Unique Phishing attacks 1H2014</th>
<th>Unique Domain Names used for phishing 1H2014</th>
<th>Domains in registry, April 2014</th>
<th>Score: Phishing domains per 10,000 domains 1H2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.cf</td>
<td>Central African Republic</td>
<td>1,327</td>
<td>1,283</td>
<td>40,000</td>
<td>320.8</td>
</tr>
<tr>
<td>2</td>
<td>.ml</td>
<td>Mali</td>
<td>556</td>
<td>523</td>
<td>44,000</td>
<td>118.9</td>
</tr>
<tr>
<td>3</td>
<td>.pw</td>
<td>Palau</td>
<td>2,484</td>
<td>2,318</td>
<td>190,000</td>
<td>122.0</td>
</tr>
<tr>
<td>4</td>
<td>.ga</td>
<td>Gabon</td>
<td>285</td>
<td>270</td>
<td>63,000</td>
<td>42.9</td>
</tr>
<tr>
<td>5</td>
<td>.th</td>
<td>Thailand</td>
<td>262</td>
<td>176</td>
<td>64,099</td>
<td>27.5</td>
</tr>
<tr>
<td>6</td>
<td>.np</td>
<td>Nepal</td>
<td>105</td>
<td>93</td>
<td>39,000</td>
<td>23.8</td>
</tr>
<tr>
<td>7</td>
<td>.ma</td>
<td>Morocco</td>
<td>106</td>
<td>92</td>
<td>43,350</td>
<td>21.2</td>
</tr>
<tr>
<td>8</td>
<td>.pk</td>
<td>Pakistan (est.)</td>
<td>115</td>
<td>86</td>
<td>42,000</td>
<td>20.5</td>
</tr>
<tr>
<td>9</td>
<td>.cl</td>
<td>Chile</td>
<td>1,188</td>
<td>921</td>
<td>455,886</td>
<td>20.2</td>
</tr>
<tr>
<td>10</td>
<td>.ke</td>
<td>Kenya</td>
<td>63</td>
<td>53</td>
<td>34,790</td>
<td>15.2</td>
</tr>
</tbody>
</table>

### Malicious domains: How about

- [http://www.mtu.np](http://www.mtu.np)
- [http://www.mtuedu.th](http://www.mtuedu.th)
What we should do now?

• Better phishing education with live demo
  – A lot of misleading, out-of-dated and conflicting phishing information online and in people’s mind!

• Review possible security vulnerabilities in our current systems
  – For example: electronic ballot systems or survey systems.
Contact me for additional information

• Dr. Yu Cai,
  – Associate Professor, School of Technology
  – Email: cai@mtu.edu

• I offered a new cyber security course named “Dissecting the recent cyber security breaches”: SAT3812
  – Dissect the real-life cyber security breaches including the Target breach and the Anthem breach.
  – Guide students to follow the footprint of hackers and look into the details of those cyber security breaches.