WIRE ME THROUGH MACHINE LEARNING

Ankit Singh
Threat Analyst Engineer, Symantec
@ankit5934
Ankit_singh@Symantec.com

Vijay Thaware
Security Response Lead, Symantec
@021vj
Vijay_Thaware@Symantec.com
AGENDA

• BEC scam walkthrough
• Social engineering, Social network hygiene and human psyche
• Recon and profiling
• Machine Learning – The attacker’s way
• Design and Execution
• SOS : Defender’s way
• Mitigation
What's Not to Expect...

- This talk is about human hardware so NO exploits or codes are involved.
- Machine will not perform any magic here and start sending BEC attacks.
- You are welcome to disagree at our points, We are ok with it.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>BEC scam walkthrough</strong></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Social network hygiene and Defects in human psyche</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Recon and profiling</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Machine Learning – The attacker’s way</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Design and Execution</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SOS: Defender’s way</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mitigation</td>
<td></td>
</tr>
</tbody>
</table>
BEC?

Umm..Never heard of it!

Features:

• Don’t showcase strong technical exploit
• Use of high influential skills.
• Sent with short content sensing a need for urgency.

Top 5 BEC Subject keyword

transfer payment request

Over 400 businesses are hit by BEC scams daily

Sent Monday to Friday, standard working week

Organizations have lost over $3 billion to BEC Scams

Wire Me Through Machine Learning
1. BEC scam walkthrough
2. Social engineering, social network hygiene and human psyche
3. Recon and profiling
4. Machine Learning – The attacker’s way
5. Design and Execution
6. SOS: Defender’s way
7. Mitigation
Social engineering, Social network hygiene and Human psyche

“An art of exploiting human behavior in order to steal confidential or valuable information from people.”

It is all about how we present ourselves on social network ...

Defects in Human Psyche

“BEC attacks are highly targeted attacks and involve high level of research through social engineering.”
AGENDA

1. BEC scam walkthrough
2. Social engineering, social network hygiene and human psyche
3. Recon and profiling
4. Machine Learning – The attacker’s way
5. Design and Execution
6. SOS: Defender’s way
7. Mitigation

Wire Me Through Machine Learning
Reconnaissance: Preliminary surveying or research

Publicly available Data:

- Social Media Profile
- Company website
- Current affairs
- Hierarchy of an Organization

Source: https://www.pinterest.com/pin/414683078160855915/
Google Dork: “Chief Financial Officer” + “Email”

1. jeanbednarz@berkeley.edu
2. William.Moeller@communityisd.org
3. LoRossouw@justice.gov.za
4. jhagen@iu.edu
Twitter Search

Twitter users with ""Chief finance officer"" in their bios only

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Tweets</th>
<th>Following</th>
<th>Followers</th>
<th>Account Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nickson</td>
<td>Nakuru, Kenya</td>
<td>1,415</td>
<td>6,193</td>
<td>6,293</td>
<td>6.65 years</td>
</tr>
<tr>
<td>Loreto</td>
<td>Abuja, Nigeria</td>
<td>7,654</td>
<td>1,932</td>
<td>1,300</td>
<td>4.03 years</td>
</tr>
<tr>
<td>Christia</td>
<td>London</td>
<td>721</td>
<td>7400</td>
<td>921</td>
<td>4.17 years</td>
</tr>
<tr>
<td>Aly</td>
<td>istanbul</td>
<td>29,163</td>
<td>479</td>
<td>792</td>
<td>6.02 years</td>
</tr>
</tbody>
</table>

LinkedIn Search

Showing 21,961 results

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Location</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sara Maurice</td>
<td>2nd Senior Finance Officer at Washf.</td>
<td>Greater Seattle</td>
<td>Connect</td>
</tr>
<tr>
<td>Sandhya Goel, CPA</td>
<td>2nd Senior Finance Manager at SPM Corporate Services</td>
<td>Greater Philadelphia Area</td>
<td>Connect 1 shared connection</td>
</tr>
<tr>
<td>Ying Chen</td>
<td>2nd Senior ERP Finance Manager - ERP Tax Design Leader at GE Power</td>
<td>Greater Boston Area</td>
<td>Connect 1 shared connection</td>
</tr>
</tbody>
</table>
EMAIL VALIDATOR

https://hunter.io
- To identify valid Email address
- Bulk Email Verifier
- API
PROFILE FINGERPRINTING

- Maltego
- Recon-ng
<table>
<thead>
<tr>
<th></th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BEC scam walkthrough</td>
</tr>
<tr>
<td>2</td>
<td>Social network hygiene and Defects in human psyche</td>
</tr>
<tr>
<td>3</td>
<td>Recon and profiling</td>
</tr>
<tr>
<td>4</td>
<td>Machine Learning – The attacker’s way</td>
</tr>
<tr>
<td>5</td>
<td>Design and Execution</td>
</tr>
<tr>
<td>6</td>
<td>SOS: Defender’s way</td>
</tr>
<tr>
<td>6</td>
<td>Mitigation</td>
</tr>
</tbody>
</table>
Why Attackers Might Need ML

- To increase *success* rate
- Defeat other *machines* out there
- Acquire *target* list
Objective

• To find the target for attack
• Obtain the model and test with real victim profile

Machine Learning

• Supervised Machine learning
• Support Vector Machine
  ✓ For possible Target profile prediction

Ground Truth

• Anti Spam telemetry
• Profile of people who were attacked
### FEATURE SELECTION

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Sex</th>
<th>No of LinkedIn Connection</th>
<th>Twitter Followers</th>
<th>No of Tweets</th>
<th>Spear Phished on Twitter</th>
<th>Spear Phished on LinkedIn</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lisa</td>
<td>45</td>
<td>F</td>
<td>2640</td>
<td>25</td>
<td>10871</td>
<td>1</td>
<td>1</td>
<td>True</td>
</tr>
<tr>
<td>John</td>
<td>40</td>
<td>M</td>
<td>241</td>
<td>4781</td>
<td>1472</td>
<td>0</td>
<td>0</td>
<td>False</td>
</tr>
<tr>
<td>Dave</td>
<td>50</td>
<td>M</td>
<td>357</td>
<td>5871</td>
<td>1571</td>
<td>1</td>
<td>0</td>
<td>False</td>
</tr>
</tbody>
</table>

**Assumptions:**
- The attacker has collected stats and data of all attacks that were conducted earlier.
- The attacker is also labeling the profile for successful and failed attempts.
TRAINING MODEL

Years of data from scammer → Train Model → Model → Prediction → Attack → Record result (Success/Fail)

New data → Model → Attack

Blacklist → YES → Record result (Success/Fail)

Feed Data
Machine Learning Model:

- Data contains both Success and failed attempts of BEC
- SVM (Support Vector Machine)
- Model performance testing is done with Cross-validation
### TEST RESULTS

#### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>93.64% +/- 4.21%</td>
</tr>
<tr>
<td>Recall</td>
<td>81.08% +/- 5.59%</td>
</tr>
<tr>
<td>AUC</td>
<td>0.925 +/- 0.041</td>
</tr>
<tr>
<td>Accuracy</td>
<td>83.30% +/- 4.99%</td>
</tr>
</tbody>
</table>

**Precision**

<table>
<thead>
<tr>
<th></th>
<th>true false</th>
<th>true true</th>
<th>class precision</th>
</tr>
</thead>
<tbody>
<tr>
<td>pred. false</td>
<td>139</td>
<td>64</td>
<td>88.47%</td>
</tr>
<tr>
<td>pred. true</td>
<td>19</td>
<td>274</td>
<td>93.52%</td>
</tr>
<tr>
<td>class recall</td>
<td>67.97%</td>
<td>81.07%</td>
<td></td>
</tr>
</tbody>
</table>
YOU GOT 80% RECOGNITION RATE

WHY NOT 100%
AGENDA

1. BEC scam walkthrough
2. Social network hygiene and Defects in human psyche
3. Recon and profiling
4. Machine Learning – The attacker’s way
5. Design and Execution
6. Mitigation
Design and Execution

• Target Identified
• Email crafting
• Similar domain name registered
<table>
<thead>
<tr>
<th>Service</th>
<th>Term</th>
<th>Price</th>
<th>Subtotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>symanteç.com</td>
<td>1 Year</td>
<td>$45.00/yr*</td>
<td>$3.99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$3.99</td>
<td></td>
</tr>
<tr>
<td>.COM Domain</td>
<td></td>
<td>$0.18</td>
<td>$0.18</td>
</tr>
</tbody>
</table>

*Plus ICANN fee total charged at .18 per year per applicable TLD

- Keep my identity safe with Directnic Privacy

[CLEAR CART] [REMOVE PRIVACY]
TIMING

• Timing plays an important role in BEC attacks

• Attacks are launched mostly from Monday to Friday

• Attacker may plan the attack as per travel plan of CEO

Source: https://tweetchup.com/

Norwich High @NorwichHigh · Jun 19
We’re thrilled that @cherylGDST, CEO @GDST will be joining us as AM Keynote speaker and panel leader at our @InspFemales Summit on Monday

TwelveDotSecurity @ TwelveDotSec · Jun 19
Our CEO will be giving a keynote presentation entitled "IOT Security – Preventing a Global Disaster" tomorrow

Hilton Careers EMEA @ Hilton_Careers · Apr 26
Chris Nassetta, President & CEO traveling to Saudi Arabia and meeting with our incredible Team Members
**TIMING**

Tweets by days of the week

- Mon
- Tue
- Wed
- Thu
- Fri
- Sat
- Sun

Tweets by hours of the day

- 12am
- 1am
- 2am
- 3am
- 4am
- 5am
- 6am
- 7am
- 8am
- 9am
- 10am
- 11am
- 12pm
- 1pm
- 2pm
- 3pm
- 4pm
- 5pm
- 6pm
- 7pm
- 8pm
- 9pm
- 10pm
- 11pm

**Our Assumption**

- Bed Time
- Ready for office/Walk
- Travel to office
- Lunch time
- Bed Time
Send Email and wait
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>AGENDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BEC scam walkthrough</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Social network hygiene and Defects in human psyche</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Recon and profiling</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Machine Learning – The attacker’s way</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Design and Execution</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>SOS: Defender’s way</strong></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mitigation</td>
<td></td>
</tr>
</tbody>
</table>
SOS: Defender’s way

- Check Social media hygiene
- Human pentesting inside organization
- Finding out potential targets inside the organization
- Educate and help hardening social media profile
MITIGATIONS

• Protect your social network account, **Keep it clean**
• Do not click on emails and links which are **not** meant for you.
• Start reading emails from the “**FROM:**” field itself.
• **Cross check** before making any wire transfer and take time even if CEO says
• Training for EVERYONE...including top management.
  Most importantly... **TOP MANAGEMENT**
More than enough personal data is available publically and can be used for social engineering.

Machine learning can be used offensively for target profiling or finding high value targets.

As the attackers may start labeling the profile with proper success and unsuccessful attack, the machine leaning model may become more and more accurate.
Thanks!!

Ankit Singh
@ankit5934

Vijay
@021vj