Phishing Trends
ISITPHISHING.AI

JPAAWG, Tokyo, November 8th 2018

Olivier LEMARIE
CTO
Phishing Trends Overview

• Rise of credential phishing attacks
  • Gaining access to a treasure trove of confidential files, financial data, contacts,..

• Compromised accounts to fuel additional attacks
  • Sending Emails but also to conduct spear phishing, or other insider attacks

• High level of sophistication
  • Defeating traditional layers of protection

• Industrialization of Phishing
  • With significant financial capacity
Trend: Phishing Targeting Businesses

New Phishing URLs, Q3 2018

Microsoft Phishing YTD

Source: Vade Secure Phisher's Favorites Report Q3 2018

Source: IsItPhishing.AI
Can you “still” spot the real Office 365 login page?
Can you “still” spot the real Office 365 login page?

Trend: Higher Content Quality to Drive Phishing Effectiveness
## Trend: Combining Technics to Defeat Traditional Layers of Protection

<table>
<thead>
<tr>
<th>Email Source</th>
<th>From Domain</th>
<th>Email Content</th>
<th>URL Link</th>
<th>Landing Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IPs</td>
<td>Specific Domain</td>
<td>Static</td>
<td>Static</td>
<td>Static</td>
</tr>
<tr>
<td>Botnets</td>
<td>Hacked Domains</td>
<td>Body Random Obfuscation</td>
<td>Parameters Randomization &amp; Encoding</td>
<td>Frequent Randomization / Rotations</td>
</tr>
<tr>
<td>Public Cloud / Snow Shoe</td>
<td>Well known Brand Domains</td>
<td>Templating Legit Brand Content</td>
<td>URL Shorteners &amp; Redirections</td>
<td>Very close to Legit Brand Content</td>
</tr>
<tr>
<td>Legit Sources (compromised accounts)</td>
<td>Homographic / Confusable Domains</td>
<td>Small Payload (URL) or just an image</td>
<td>Via Legit Sites and Smart URL Redirection</td>
<td>Dynamic &amp; Distributed Content</td>
</tr>
<tr>
<td>IP Reputation based systems</td>
<td>Domain reputation, DKIM / DMARC,…</td>
<td>Content filtering, Signatures, Fingerprints…</td>
<td>URL blacklists &amp; Centralized crawling</td>
<td>HTML signature based analysis &amp; humans…</td>
</tr>
</tbody>
</table>

---

**Phishing Trends**

©2018 – Vade Secure
Example: Targeted credential phishing attack (Oct 2018)

- Targeting one large ISP
- More than 150,000 compromised accounts
- 10 minutes cycles
- Below threshold volumes
- Every email different in structure and payload
- Several legit urls
- 1 phishing URL (never the same)
- Variety of redirection technics (shorteners, tracking..)
- Rotation out of 25,000 domains specifically registered for the attack (2 months before)
- Serving content only for few minutes
- And not at time of email delivery
- Thousands of canary accounts
- Instant detection of blocking and rotation
AI To Address New Challenges

- Not replacing but complementing existing filtering layers
- Allowing the detection to happen from the first email
- Processing massive amount of data in realtime
- Expertise driven approach
- Prediction Models build out of features extracted from source, content & context of the emails.
- Moving towards predictive models
Machine Learning Predictive Models for Phishing

- Models for Phishing detection integrated in our IsItPhishing.AI platform
- Analysis of urls and documents in real time at time of click
- Selected 47 features to drive for effectiveness

Support Vector Machine

Random Forest

Recursive Feature Elimination Algorithm

# features / Accuracy

- Accuracy

• 2 others areas of focus in roadmap:
  - Computer Vision / Phishing Brand detection
  - Targeted Attacks Detection
Machine Learning Models for Spear Phishing

Example: CEO Fraud / Business Email Compromise (BEC)

I need you to arrange a transfer of $140,000 to a supplier today. It is for an acquisition that we have been trading privately for a few weeks and the supplier has accepted our payment terms of 10% down payment. Let me know if you can do it immediately, I can send you the bank details.

- Highly damaging
- Using Employee impersonation
- Extremely rare
- Often text based only

- Anomaly detection FP rate can be high
- Natural Language Processing (NLP) requires a lot of tuning
- Classification / Machine Learning requires quantitative and qualitative data
Data Augmentation Technics

• Presented at MAAWG NYC last month

• Enrich a dataset used to construct models
  • Synonyms Replacement, Mispelling, Name Replacement, Amount transformation, Language Translation, ...

• Ensure quality of augmented data
  • Semantic similarity, Syntactic similarity

Example on CEO Fraud: English -> French -> Spanish -> English

Hi,
I need you to arrange a transfer of $140,000 to a supplier today. It is for an acquisition that we have been trading privately for a few weeks and the supplier has accepted our payment terms of 10% down payment. Let me know if you can do it immediately, I can send you the bank details. Thank you.
Sincerely
Sandy

Hello, I'll need you to arrange a transfer of 136,700 € to a vendor today. This is for an acquisition that we have been negotiating privately for some weeks and the vendor agreed to our payment terms of 10% down payment. Let me know if you can get this done immediately, I can forward you the bank details.
Thanks.
Best regards
Irene
Thank You