Phi.sh/$oCiaL: The Phishing landscape through Short URL's
1. Introduction

- With the advent of Web 2.0 technologies, social services like Twitter, Facebook, and MySpace have emerged as popular media for information sharing;
- While phishing detection through traditional channels such as email has been extensively researched; these solutions may not be directly applicable in online social media;
- Phishers are making use of the URL shorteners to obfuscate the phishing URLs to spread their phishing statuses (links).
Example

A tweet with a short phishing URL (using bit.ly). When a user clicks on the link, he is directed to http://wenbinginTwitter.appspot.com/, a phishing page.
Objectives

• Track the evolution of phishing through the landscape of URL shorteners on online social media
• Which are the brands (traditional vs. online social media) targeted by phishers?
• Where (on the web) do these shortened phishing URLs originate from?
• What is the spread (across the globe) of the victims clicking on these shortened phishing URLs?
2. Related Work

• An analysis of source of automated tweets reveals that automated tweets are sent using services like Twitterfeed and Twitter’s REST API which provide automation and scheduling;

• Phishing (one form of spam), is to fool gullible users out of their essentials for gaining monetary benefits, is a $2.8 billion “industry” in US;

• First lure the customer to click on the link and second fool him/her to divulge their credentials by spoofed webpage;
3. METHODOLOGY AND DATASETS

3.1 Data Collection

• The first step was to fetch the PhishTank database for the year 2010 and filter those which were voted ‘yes’;
  ▪ Phishtank: an openly available phish database
  ▪ Obtained 118,119 such URLs;

3.1 Data Collection

- There are cases when phishing pages are hosted inside famous and trustworthy domain names for example there were a few (in our dataset) on Google Spreadsheets;
  - To filter such false negatives (popular domains), was removed URLs with exceptionally high number of clicks. At the end of this process, they had 6,474 short URLs for “phishing” URLs with 3,692 exact matches;
- In the third step, for every short URL they query different API end-points namely clicks, clicks-by-day, countries and referrers from bit.ly.
Architecture

Dataset Collection

Filtering

Analysis

Brands analysis

Geographical analysis

Temporal analysis

Referral analysis

Twitter | API

Behavior analysis

Text analysis

Network analysis
Distribution of URLs
Distribution of number of primary domain names with number of URLs
4. RESULTS

4.1. Space Gain

• To ascertain if bit.ly has really helped phishers, we calculate the space gain for each URL. By space gain, we mean the fraction of space saved by using bit.ly URL instead of the actual long URL;
  o They find average space gain to be 39%;
• For 50% of the phishing URLs, they observe a 37% or less space gain; for generic URLs, researchers have shown 91% space gain;
The cumulative space gain
4.2. Target Brands

- In this section, they present the evolution of phishing targets from e-commerce services / financial institutions to on-line social media brands like Facebook, Orkut;
Frequencies for top 10 brands with number of clicks
4.2. Target Brands

- The figure shows the frequencies for top 10 brands with number of clicks they received during the period of their analysis. Four of the top 10 are online social media brands;
- We see that there are many brands where the number of URLs are low, but the median clicks are high and some where the number of URLs are high and the median clicks are low which negates the silent assumption that large number of phishing URLs trap large number of victims;
Average of clicks for top 5 brands
4.2. Target Brands

- We see that Habbo’s average number of clicks increased heavily after Sept 2010; there seems to be a large difference between average clicks for Habbo and the next hit brand PayPal after Sept 2010;
- We also observe that on average PayPal’s clicks are increasing with time and follows a cyclical pattern whereas Facebook achieved peak during July and August;
- This indicates about the change in focus of phishers, from financial institutions / e-commerce websites to online social media;
4.3. Referral Analysis

<table>
<thead>
<tr>
<th>Twitter Referral</th>
<th>Clicks</th>
<th>Countries</th>
<th>Lifetime</th>
<th>Referrals</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>70.2(0.0)</td>
<td>2.7(0.0)</td>
<td>12.8(0.0)</td>
<td>2.5(1.0)</td>
</tr>
<tr>
<td>Yes</td>
<td>95.1(14.0)</td>
<td>7.2(4.0)</td>
<td>84.0(8.0)</td>
<td>7.2(4.0)</td>
</tr>
</tbody>
</table>

- Summary statistics for URLs with / with-out Twitter referral. All values are mean with median in bracket. Shows that phishing URLs which were referred from Twitter has an edge over the others.
4.3.1 Behavior Analysis

- They classified user profiles into organic and inorganic. **An organic account is one of a legitimate Twitter user who posts her tweets manually;**
- An organic user usually has a uniform distribution of tweets with respect to time. Whereas, an inorganic account would exhibit detectable non-uniformity in timing pattern
- Inorganic accounts exhibit a robotic pattern of status updates as shown in figure
Temporal pattern for status updates of a user
A point on the plot is time-stamp for a tweet.

Past (black X) is the posting pattern for user in the past (2000 tweets back)

and Present (red circle) is the posting pattern in the present for 200 tweets

Shows change from organic (manual) to inorganic (automatic).
4.3.2 Network Analysis

- We found that the friend-follower network is sparse.
- Even though this is a small sample, they found 1/3rd of nodes were connected. The network density is 0.01 and reciprocity is 56%, which is significantly higher than the 22% that has been observed in general population of Twitter.
- Spammers increase their influence by following various strategies to increase the number of followers. One of the strategy is to follow others in hope of getting followees (return favor).
Network of the people tweeting the phishing URLs
4.3.3. Text Analysis

- They did text analysis of these tweets to infer the properties of phishing tweets;
- There were 120 tweets of which 67 were in English rest were in Brazilian, Dutch, Russian and others;
- The average length of English tweet was 95.7 characters (min. 33, max. 140, var. 32.5) which is close to the limit (140 characters).
- Use of third party Twitter applications to schedule their tweets is popular among phishers. Tweetdeck is the most popular app used in 48.5% tweets followed by Twitrobot at 21.6%. 
Tag Cloud for the words from tweets containing phishing URL
4.4. Locational analysis

- For each URL, they got a list with number of clicks and ISO code for the country (e.g. IN = India);
- In total, these URLs were clicked from as many as 140 different countries across the globe;
- For every country, they divided the number of clicks by respective Internet population;
Location information for the clicks
Top brands in different countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Brands</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>Habbo, PayPal, Facebook</td>
</tr>
<tr>
<td>India</td>
<td>Orkut, PayPal, Facebook</td>
</tr>
<tr>
<td>Brazil</td>
<td>Habbo, Bradesco, Orkut</td>
</tr>
<tr>
<td>Great Britan</td>
<td>Habbo, PayPal, Facebook</td>
</tr>
<tr>
<td>Russia</td>
<td>PayPal, HSBC, Habbo</td>
</tr>
<tr>
<td>Australia</td>
<td>Habbo, PayPal, Orkut</td>
</tr>
</tbody>
</table>
Top brands in different countries

- Except for Russia, all other countries have two of three brands as some online social media brand;
- This shows that online social media has become a favorite target for phishing attacks;
Scatter plot of phishing URLs for geographical and temporal spread

---

The scatter plot illustrates the geographical and temporal spread of phishing URLs. The x-axis represents the lifetime in days, while the y-axis shows the number of countries affected by these URLs. The plot includes different levels of clicks, indicated by varying shades and sizes of dots, with higher click counts shown by darker, larger dots.
• In the figure, we see that there are URLs which had short lifetime but spanned more than 80 countries with more than 1000 clicks;
• there are URLs which have lifetime of more than 400 days but few clicks and not spread in more than 20 countries;
• We observe large number of clicks for URLs which are evenly spread geographically and temporally.
5. DISCUSSION

- Phishers were using URL shorteners not only for reducing space but also to hide their identity;
- Online social media brands account for more than 70% clicks amongst the top 10 brands. Online social media brands like Facebook, Habbo, and Twitter are targeted by phishers more than traditional brands like eBay and HSBC;
- Phishing URLs which were referred from Twitter had an edge over the others with respect to attracting victims;
5. DISCUSSION

- Around 30% of the users turned organic (manual) to inorganic (automatic) in last 2000 tweets which is an indicator of spread of phishing (spam in general) campaigns.
- On analyzing the tweet text they found, usage of proper English, longer tweets and more hashtags
- A filter based on both semantic and syntactic text features and network properties can be effective for detection of such Twitter accounts.