Geo-Phisher: The Design of a Global Phishing Trend Visualization Tool

[Poster Abstract]

Leah Zhang-Kennedy
Carleton University
leahzhang@carleton.ca

Elias Fares
Carleton University
eliasfares@cmail.carleton.ca

Sonia Chiasson
Carleton University
chiasson@scs.carleton.ca

Robert Biddle
Carleton University
robert.biddle@carleton.ca

1. INTRODUCTION

Phishing is a significant type of internet crime that tricks users into giving up their personal and financial information. To combat phishing, browser manufacturers, software vendors, and organizations have compiled repositories of phishing URLs (blacklists). These lists enable the analysis of reported phishing attacks to be shared among anti-phishing communities to gain awareness of evolving phishing trends. For example, during the third quarter of 2014, the Anti-Phishing Working Group (APWG) received approximately 50,000 unique phishing e-mail reports from consumers monthly, targeting more than 500 unique brands [1]. This data is analyzed and released as a quarterly report.

To assist in the analysis of phishing blacklist data, we propose an information visualization tool called Geo-Phisher (available online at [4]). The application features a scatterplot map interface that plots the temporal and geographical information of phishing URLs. Applied to blacklist data from the APWG [3], the prototype reveals several interesting patterns in hosting locations of phishing URLs and distributions of the top phished brands across the globe.

2. BACKGROUND AND RELATED WORK

Phishing Blacklist: A phishing blacklist collects information about reported phishing websites. The largest blacklists are operated by major browser vendors like Google and Microsoft, and by organizations like Phishtank and APWG, all containing manually verified phishing URLs. Blacklists are integrated with popular web browsers to automatically block phishing sites. Phishtank and APWG each maintains a database of phishing URLs reported by users.

Phishing Visualization: Visualizations about phishing are primarily created to educate users about phishing attacks. For example, PhishGuru [6] uses illustrated comics to teach users after they have responded to a fake phishing message. The APWG/CMU-Cylab's phishing education landing page program [2] also uses a graphics approach to communicate phishing material to users.

Government and various organizations created anti-phishing campaigns that use diagrams and infographic posters to spread awareness. An infographic by GetCyberSafe [5] depicts cyber pirates on a "phishing" trip to tell the story of email phishing scams. PhishMe [8], a threat management company, offers a range of infographics on phishing. The APWG [1] uses a variety of phishing trend diagrams in their quarterly reports. Lavasoft [7], an anti-malware company, provides a map of phishing URL geographic distribution.

3. DESIGN OF GEO-PHISHER

The main purpose of the Geo-Phisher application is to assist in trend analysis of phishing attacks from blacklist records, and to enable any member of the anti-phishing community, affected enterprises, and consumers to learn about the data. Users can explore the relationship between IP addresses, geolocations, and targeted brands from more than 40,000 records from the APWG database [3] collected during the month of January, 2015. In comparison to other blacklist sources, the APWG database contained the most complete information that we seek to visualize, such as a timestamp, an URL, the targeted brand, and an IP address that enabled us to obtain geoIP information. Geo-Phisher is developed as a web application using p5.js, a javascript interpretation of the Processing language.

The Geo-Phisher interface (Figure 1) shows a scatterplot display over a world map. Tiny points are applied an alpha value to show high versus low concentrations of light to represent the frequency of phishing URLs. Any point on the map can be moused over to reveal the location. A zoom feature enables the user to enlarge any area of the map (Figure 1(b)). Time is controlled by an interactive filter-map-by-date feature (Figure 1(g)). Dragging the mouse over the line graph produces an animated effect of the map display. The filter-map-by-brand feature (Figure 1(h)) filters points on the map based on user selected brands. For example, if the user selects Paypal, the map will display locations where Paypal is targeted. Users can select several brands at once represented by a different colour. A "show all" button (Figure 1(d)) resets all the points on the map (i.e., no filter).

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

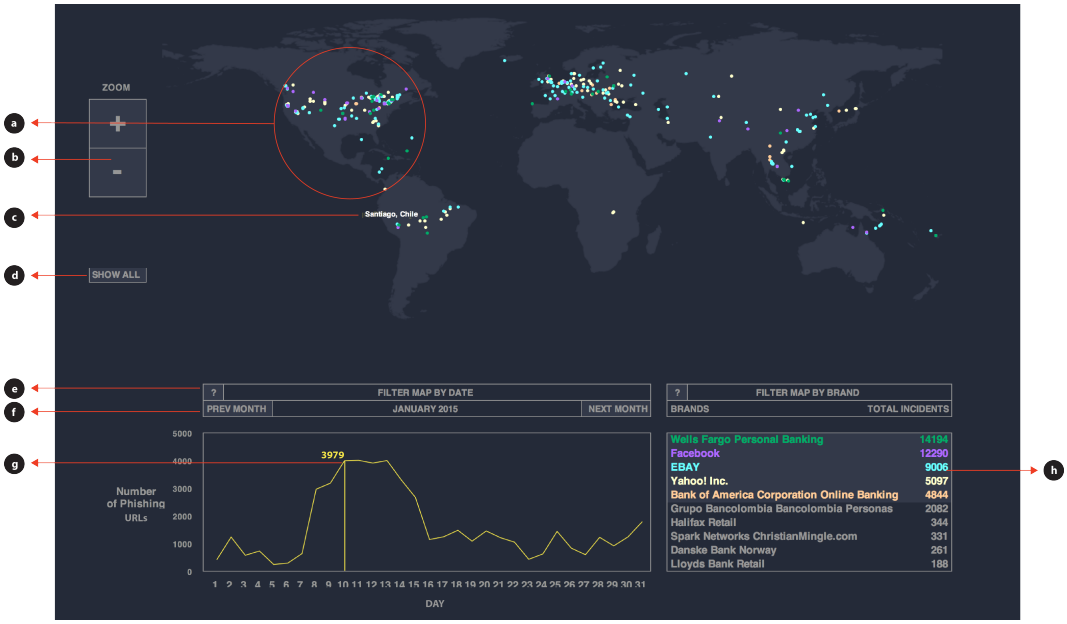

Figure 1: Screen of the Geo-Phisher application: (a) Map display, (b) Zoom, (c) Rollover points, (d) Reset map, (e) Tool tip, (f) Next/previous month, (g) Filter-map-by-date feature, (h) Filter-map-by-brand feature.

4. DISCUSSION AND FUTURE WORK

The Geo-Phisher application supports the following tasks:

1. *Track the number of reported phishing websites:* The line graph shows that phishing attacks occurred between 250 times and 4000+ times a day during the month of January, 2015. The highest number of attacks occurred near the middle of the month. We suspect that phishers are exploiting peaks in gift exchanges/returns and consumers getting back "online" after the Christmas holidays.

2. *Discover where phishing URLs are located in the world:* The Geo-Phisher application maps phishing URLs by latitude and longitude. Phishing URLs are concentrated mostly in the United States, western Europe, and southern Asia. Concentrations of light appear mostly over major cities, showing a possible correlation between where phishers are located and the population density of the city.

3. *Identify brands targeted by phishing campaigns in relation to geography:* Our system shows the top 6 phished brands in January were: Wells Fargo, Facebook, Ebay, Yahoo, and Bank of America, and Grupo Bancolombia. Financial institutions were targeted most frequently, followed by E-commerce and social media sites. Certain targeted brands were more distributed across the globe than others. For example, brands like Ebay or Yahoo showed up across the globe compared to Grupo Bancolombia, which was targeted more frequently from Spanish speaking countries, and Facebook, which was targeted mainly from North America.

The current version of Geo-Phisher displays one month of data. Future work includes extending to data to include other months and possibly years, and implementing additional features to facilitate smoother user interaction.

5. CONCLUDING REMARKS

As phishing blacklists continue to grow in size, it would be useful to visualize how phishing data changes over time. To the best of our knowledge, Geo-Phisher is the first publicly available phishing visualization tool. We demonstrated how the tool could assist in several data analysis tasks, and believe that it could help in the exploration, analysis, and dissemination of knowledge about phishing trends among anti-phishing communities, enterprises, and consumers.

6. REFERENCES

[1] APWG. Phishing activity trends report, March 2015. `http://docs.apwg.org/reports/apwg_trends_report_q3_2014.pdf/`.

[2] APWG. Phishing education landing page program, Accessed February 2015. `http://phish-education.apwg.org`.

[3] APWG. URL Block List (UBL), Accessed February 2015. `https://ecrimex.net`.

[4] Fares, E., and Zhang-Kennedy, L. Geo-Phisher, 2015. `http://bit.ly/geophisher`.

[5] Get Cyber Safe. Phishing: How Many Take the Bait?, accessed April 2015. `http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx`.

[6] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2):7, 2010.

[7] Lavasoft. Phishing URLs geographic distribution, April 2015. `http://www.lavasoft.com/mylavasoft/securitycenter/whitepapers/detecting-malicious-urls-part-2-"where"`.

[8] PhishMe. Infographics, April 2015. `http://phishme.com/resources/infographics/`.