



The data in this report is aggregated from a combination of sources including Symantec’s Phish Report Network (PRN), strategic partners, customers and security solutions.

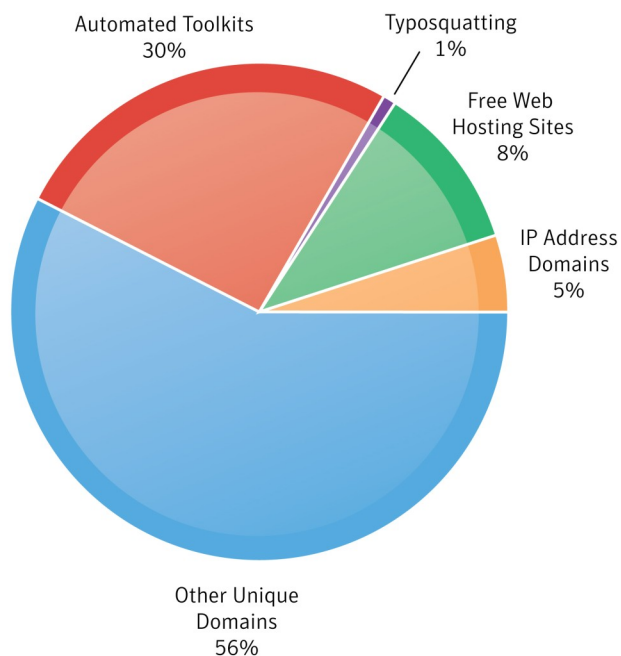
This report discusses the metrics and trends observed in phishing activity during the month of October 2009.

Highlighted in the November 2009 report:

- Symantec observed a 17 percent increase from the previous month in all phishing attacks
- 30 percent of phishing URLs were generated using phishing toolkits; an increase of 24 percent from the previous month
- Symantec observed a 45 percent increase from the previous month in non-English phishing sites
- More than 97 Web hosting services were used, which accounted for 8 percent of all phishing attacks; a decrease of 19 percent in total Web host URLs when compared to the previous month

Overall Statistics

Phishing Tactic Distribution: Phishing sites were categorized based upon the domains they leveraged. In October, there was an increase observed in the volume of phishing activity, as forecasted in the previous months. There was a considerable increase observed in the number of phishing sites being generated using phishing toolkits. The recent downtrend of phishing attacks, in all likelihood, is seen to have been discontinued with the resurgence in toolkit attacks in October, and signals the approach of the holiday season.



David Cowings
Executive Editor
Security Response

Suyog Sainkar
Editor
Security Response

Sagar Desai
PR Contact
Sagar_desai@symantec.com



Phishing site attack methods and target sectors

The following categories were analyzed:

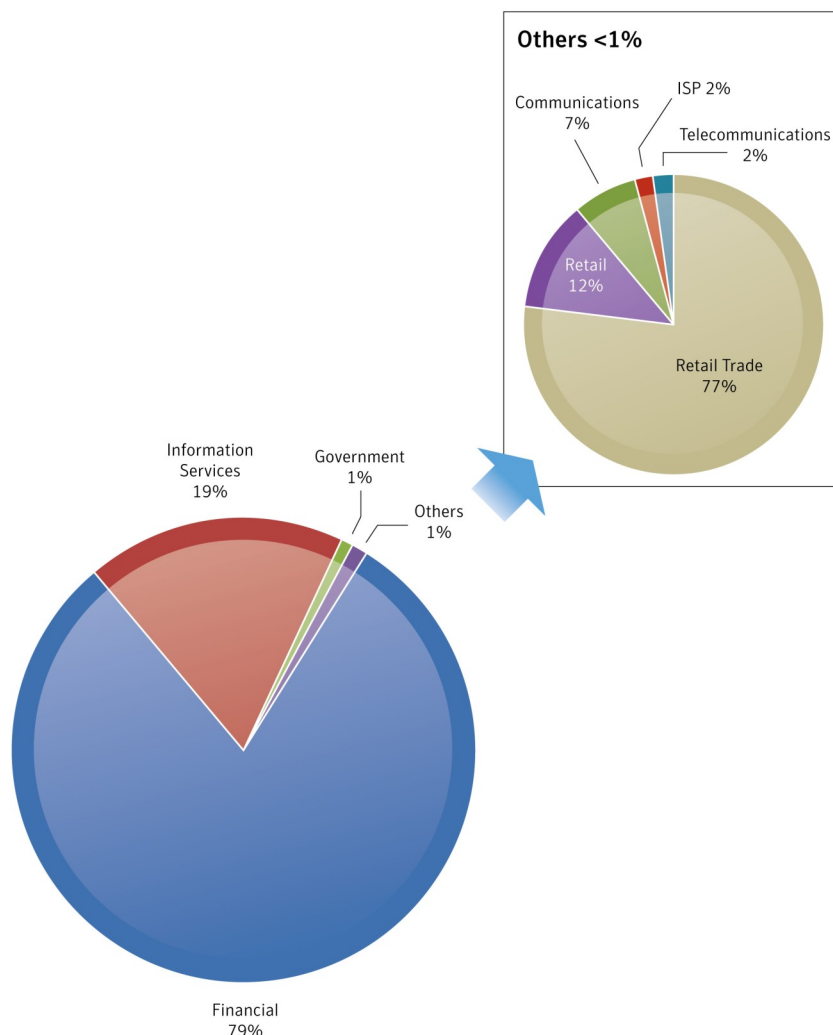
- Sectors
- Number of brands
- Phishing toolkits
- Fraud URLs with IP addresses
- Phish sites that use IP address domains – categorized by hosted cities
- Use of Web hosting sites
- Geo-locations of phishing sites
- Non-English phishing sites
- Top-Level domains of phishing sites
- Country of brand

Sectors: Phishing target sectors are seen in the graphic below.

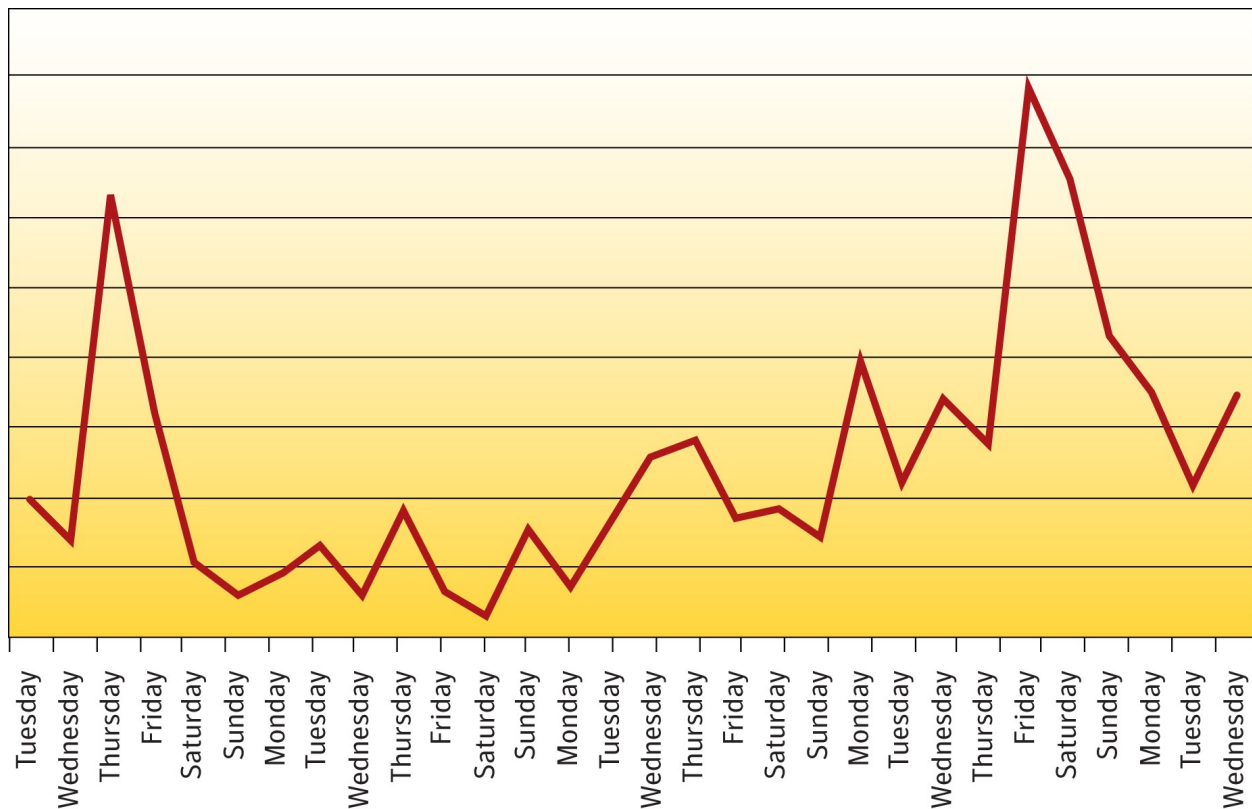
Sectors

Number of Brands:

Symantec observed that 70 percent of all attacks were from unique phishing Websites, which included more than 201 targeted brands. In October, the unique phishing activity decreased by 4% over the previous month. The proportion of unique phishing URLs decreased from 75 percent (in September) to 70 percent (in October). This was partially attributable to an increase in toolkit activity as the trending of the two is usually inversely correlated.



Weekly Behavior of Phishing Toolkit Activity



Automated Phishing Toolkits:

Symantec observed that in October, 30 percent of phishing URLs were generated using phishing toolkits. The number of toolkit attacks increased considerably by 24 percent. Symantec observed that the toolkit attacks were more in number at the beginning and towards the end of the month. The sharp increase observed in the toolkit attacks was primarily attributed to a phishing attack targeting a popular information services brand.

attacks targeted a wide range of brands from diverse sectors. It further turned out interesting to observe that most of these brands, for a while, had been disengaged by the fraudsters from the toolkit activities. This in all likelihood indicates that the fraudsters have reactivated many command-and-control servers, withdrawn recently, for a new season of phishing activity. Symantec observed that the resurgence in toolkit attacks has resulted in other tactics such as Typo squatting which had increased in the recent months, back to a normal level of activity.

Symantec observed that the increased toolkit

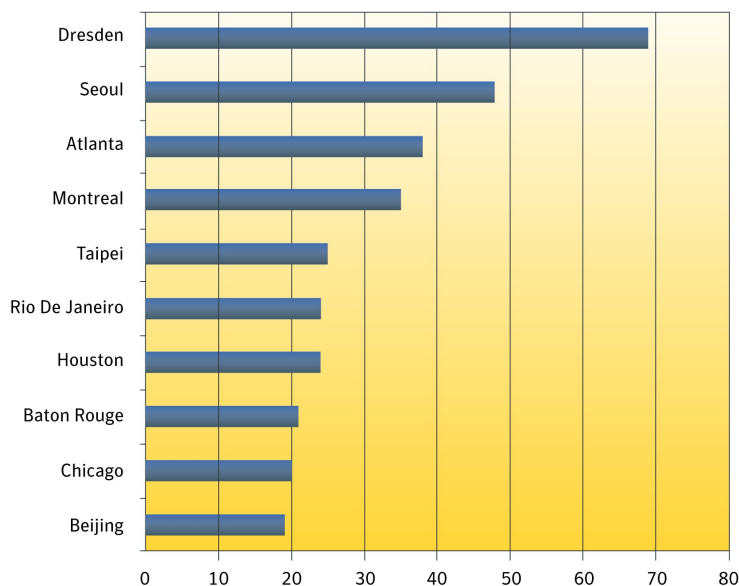
Phishing Attacks Using IP Address Domains

Phishers today use IP addresses as part of the hostname instead of a domain name. This is a tactic employed to hide the actual fake domain name that otherwise can easily be noticed. As many banks use IP addresses in their website URLs, this establishes a precedent that spammers can follow as it raises less suspicion.



A total of 977 phishing sites were hosted in 57 countries. This amounted to an increase of approximately 3 % of IP attacks in comparison to the previous month. The United States is still home to a majority of phishing activity and continues to be the top ranked country hosting phishing sites-primarily due to its significantly developed Internet infrastructure. In October, Germany accounted for approximately 9 % of IP attacks making its debut at the second position. The Greater China region accounted for approximately 8 percent of IP attacks in the month. The total number of IP attacks originating from this region reduced by 10 percent as compared to the previous month.

Phish Sites that Use IP Address Domains – Categorized by Hosted Cities



The top cities hosting phish sites were Dresden, Seoul and Atlanta. It was interesting to observe that phish sites with IP domains continued to originate from newer cities every month. In October, Dresden-a city in Germany and Baton Rouge-the capital city of Louisiana State, introduced themselves in the list of top cities hosting phish sites.

October 2009 Rank	September 2009 Rank	Country	October 2009 Percentage	September 2009 Percentage	Change
1	1	United States	36%	37%	-1%
2	14	Germany	9%	Not listed in the top five regions of phish origin	N/A
3	2	Greater China	8%	18%	-10%
4	5	South Korea	5%	4%	1%
5	3	Canada	5%	5%	No Change

Phishing Exploits of Free Web Hosting Services

For phishers, using free Web hosting services has been the easiest form of phishing in terms of cost and technical skills required to develop fake sites.

A total of 97 different Web hosting services served as the home for 1,813 phishing sites in the month of October. Symantec observed that there was an 18 percent decrease in the number of free Web hosting services utilized for developing phishing sites. More than 71

brands were attacked using this method in the reporting period.

However, this form of attack is not as widely used as it frequently requires manual efforts to prepare the phishing Web page, unlike the automated kit generated Web sites. Many free Web hosts have also improved their preventative and corrective anti-phishing measures significantly decreasing the lifespan of phishing sites on their systems.

Global Distribution of Phishing Sites

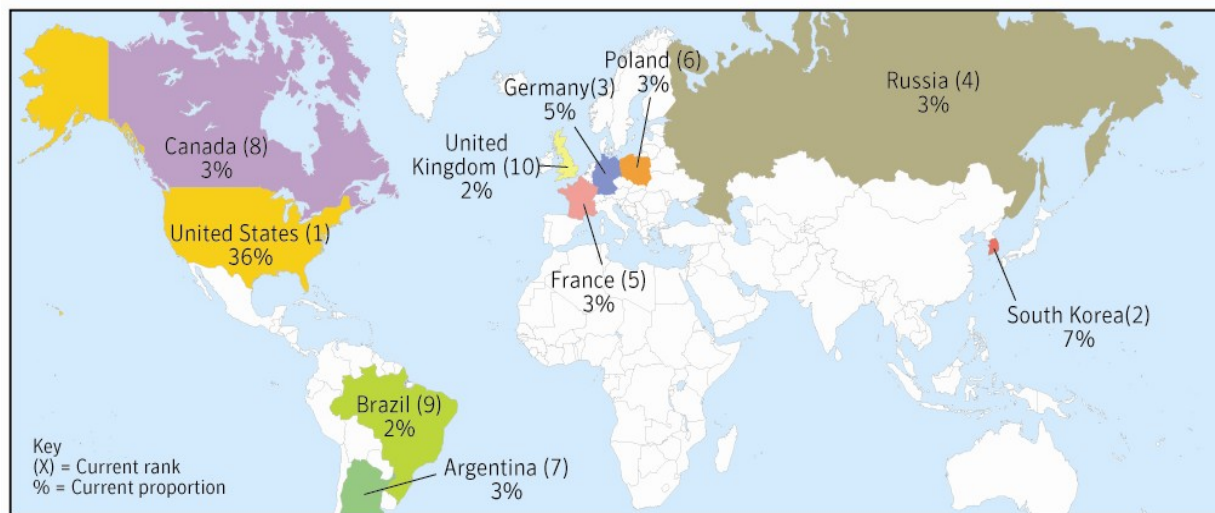
Phishing sites were analyzed based upon the geo-location of their Web hosts as well as the

number of unique URL's (referred to in this report as "lures") utilized to lure victims to the phishing Web hosts.

1. Geo-Location of Phishing Lures

Leading this area is the United States (36 percent), South Korea (7 %) and Germany (5 %). In October, there was a considerable increase observed in the number of phishing lures for

South Korea and Germany. The proportion of active phishing lures remained evenly distributed for the rest of the locations.

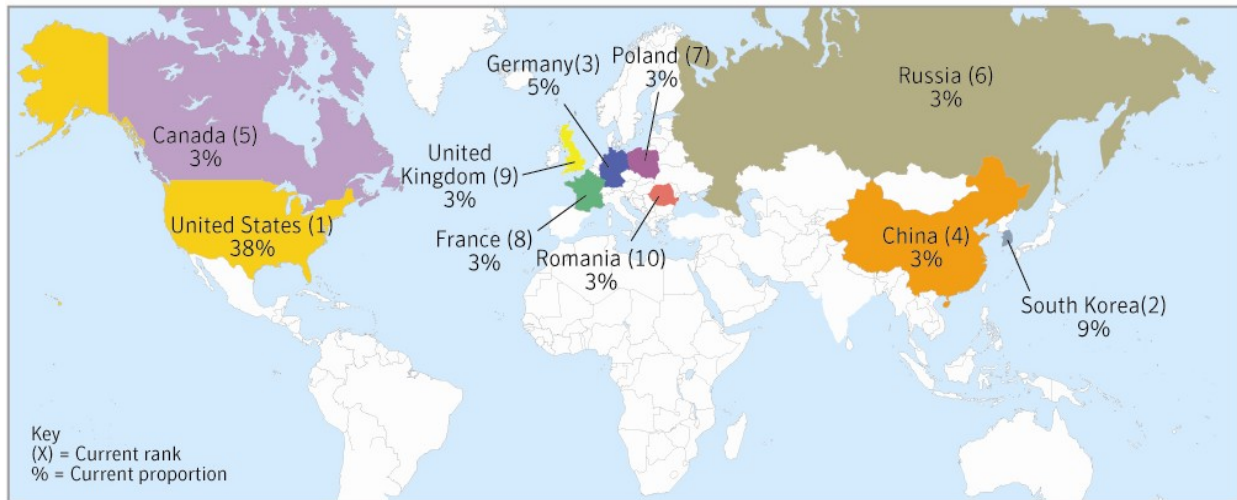


2. Geo-Location of Phishing Web Hosts

The top countries are USA (38 percent), South Korea (9 %) and Germany (5 %). There was a staggering 100 percent and more increase observed in the total number

of phishing hosts for South Korea. In October, the distribution of Web hosts was evenly distributed for all other locations.

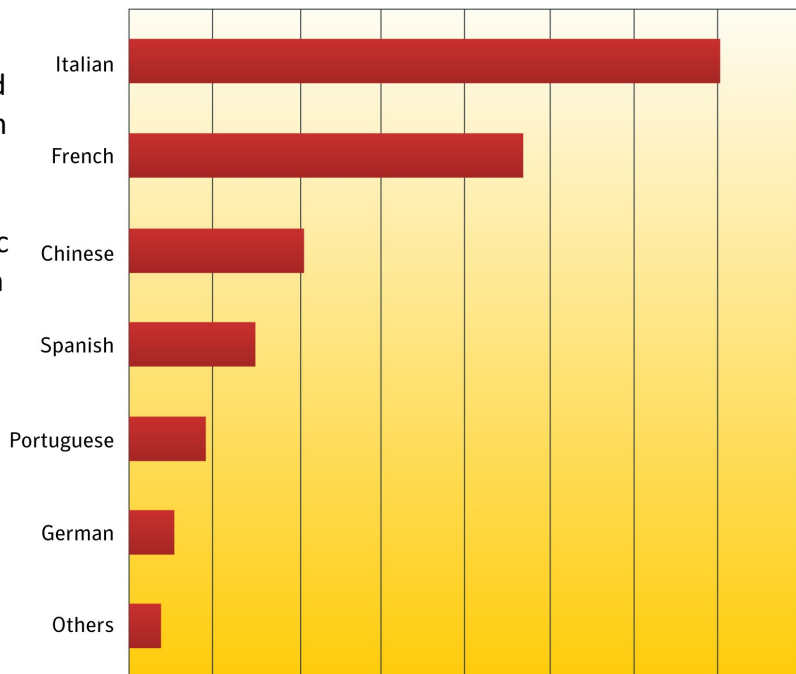
Geo-Location of Phishing Web Hosts



Non-English Phishing Trends

Phishing attacks in Italian, French and Chinese languages were found to be higher in October. The Italian language attacks, increased in number and superseded the French language attacks. Symantec observed that phishing websites in Italian, French and Spanish remained higher for the financial sector; while, the phishing attacks in Chinese language prevailed in the e-commerce sector.

Non-English Phishing Sites



Top-Level Domains of Phishing Sites

Phishing URLs were categorized based on the Top-Level Domains (TLD). TLDs are the last part of an Internet domain name; i.e., the letters that follow the final dot of any domain name.

E.g., in the domain name `www.example.com`, the Top-Level Domain is `.com` (or `COM`, as domain names are not case-sensitive). Country Code Top-Level Domains (ccTLD) are used by a country or a territory.



They are two letters long, for example .us is for the United States. Generic Top-Level Domains (gTLD) are used by a particular type of organization (.com for a commercial organization).

It is three or more letters long. Most gTLDs are available for use worldwide, but for historical reasons .mil (military) and .gov (government) are restricted to use by the respective U.S. authorities.

Comparisons of Top-Level Domains of Phishing Sites

Overall TLDs

The most used TLDs in phishing sites in the month of October were, .com, .net and .org comprising of (50 percent), (9 %) and (4 %) respectively.

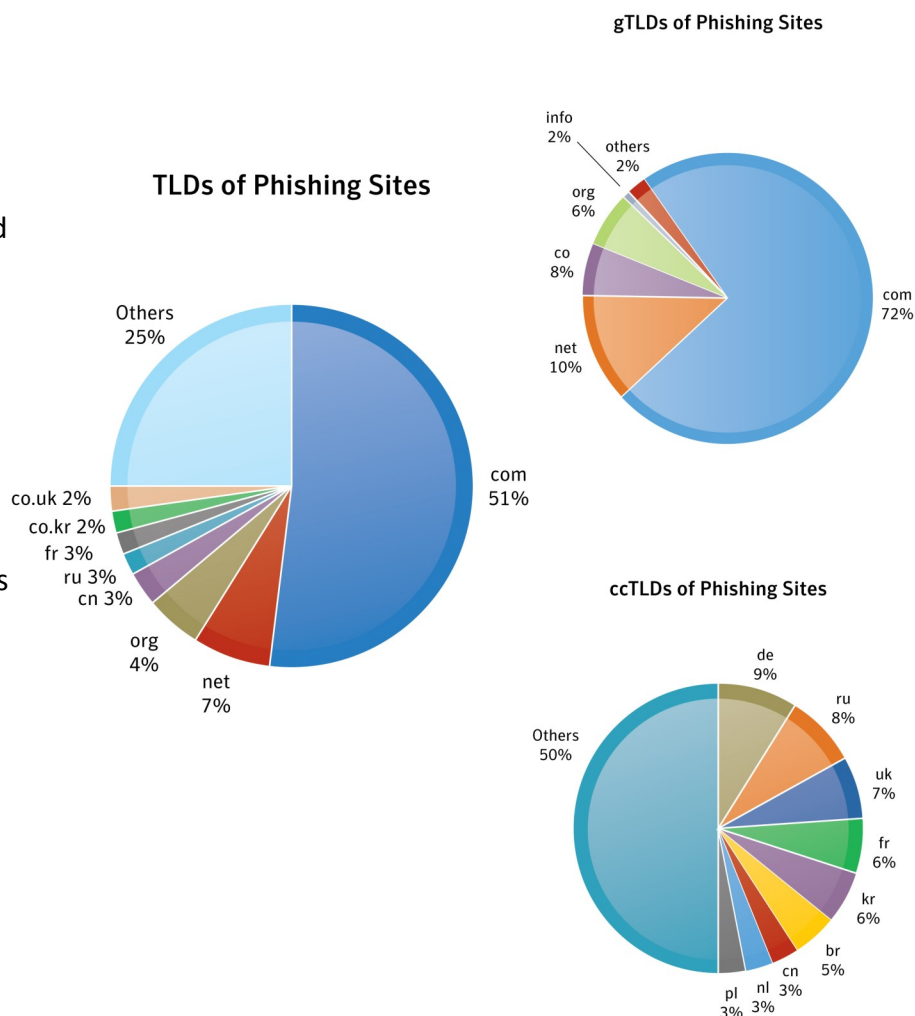
The Top-Level Domains in phishing were then further categorized:

1. Generic Top-Level Domains (gTLDs)

The generic TLDs .com, .net and .co were the most utilized with (73 percent), (12 percent) and (6 %) of the total phish attacks respectively.

2. Country Code Top-Level Domains (ccTLDs)

The German, Russian and United Kingdom ccTLDs were evaluated to be the highest in phishing attacks with (9 %), (8 %) and (7%) respectively.



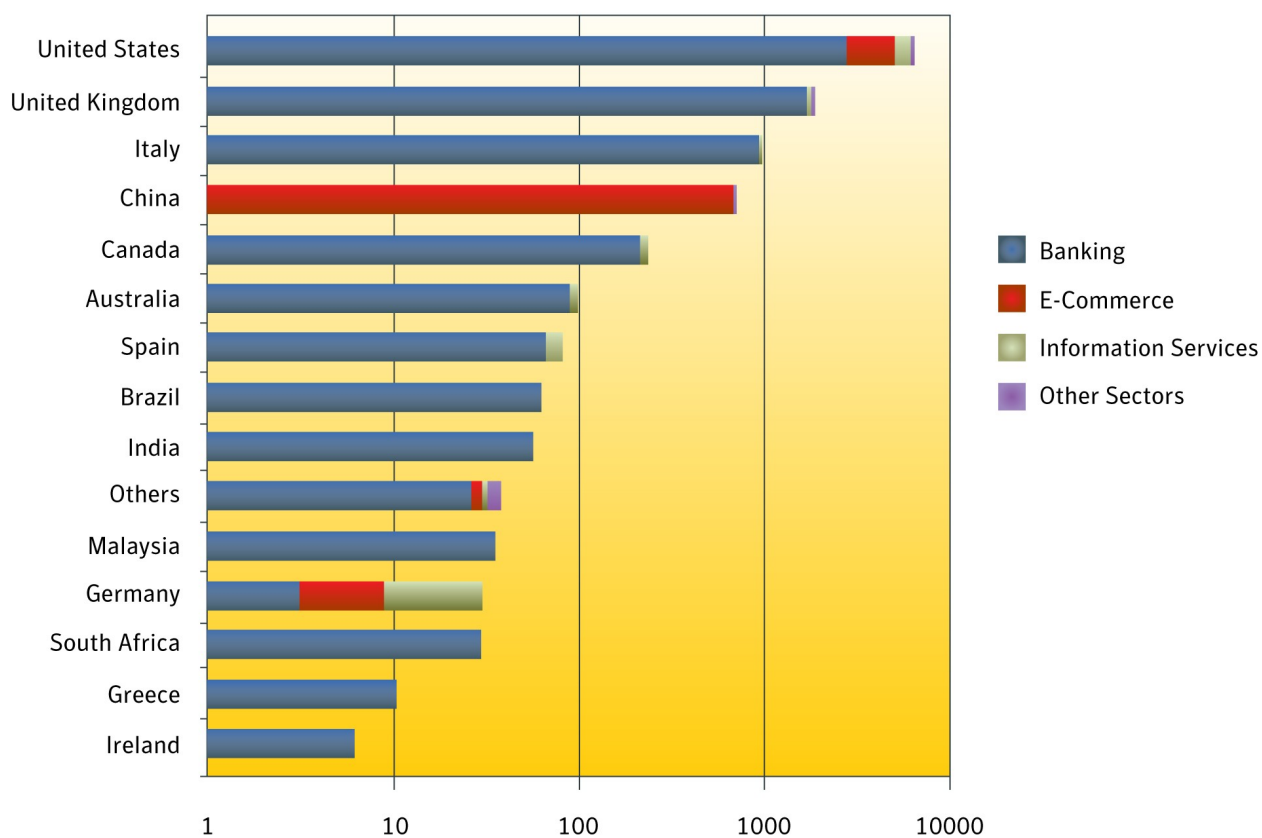


Country of Targeted Brands

The brands that phishing sites spoofed were categorized based on the country in which the brand's parent company is based.

The top countries of brands attacked in October were the USA, UK and Italy. There were 29 countries whose brands were attacked. As seen in the previous months, the trend of the sectors targeted is similar throughout the countries of brand origin except for those belonging to Germany and China. There was a combination of banking, e-commerce and information services sectors in German brands. In China, the e-commerce sector remains a primary target.

Country of Brand (Logarithmic Scale)





Glossary of Terms

Phishing Toolkits: Phishing toolkits are automated toolkits that facilitate the creation of phishing Websites. They allow individuals to create and carry out phishing attacks even without any technical knowledge.

Unique Phishing Website: The phishing Websites that have a unique Web page are classified as “Unique Phishing Websites”. URLs from phishing toolkits that randomize their URL string are observed to point to the same Web page and do not contain a unique Web page in each URL. Unique Phishing websites are the ones where each attack is categorized on distinct Web Pages.

Web-Hosting: Type of Internet hosting service which allows individuals and organizations to put up their own websites. These websites run on the space of Web host company servers accessible via the World Wide Web. There are different types of Web hosting services namely, free Web hosting, shared Web hosting, dedicated Web hosting, managed Web hosting, etc. of which the free Web hosting service is commonly used to create phishing websites.

Typo-Squatting: Typo-squatting refers to the practice of registering domain names that are typo variations of financial institution websites or other popular websites

Phishing Lure: Phishing lures are URLs distributed in spam/phishing email utilized to lure victims to fraudulent phishing websites.

Top-Level Domain (TLD): Sometimes referred to as a Top-Level Domain Name (TLDN): It is the last part of an Internet domain name; that is, the letters that follow the final dot of any domain name. For example, in the domain name www.example.com, the Top-Level Domain is com (or COM, as domain names are not case-sensitive).

Country Code Top-Level Domains (ccTLD): Used by a country or a dependent territory. It is two letters long, for example .us for the United States.

Generic Top-Level Domains (gTLD): Used by a particular class of organizations (for example, .com for commercial organizations). It is three or more letters long. Most gTLDs are available for use worldwide, but for historical reasons .mil (military) and .gov (governmental) are restricted to use by the respective U.S. Authorities. gTLDs are sub classified into sponsored Top-Level Domains (sTLD), e.g. .aero, .coop and .museum, and unsponsored Top-Level Domains (uTLD), e.g. .biz, .info, .name and .pro.