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.

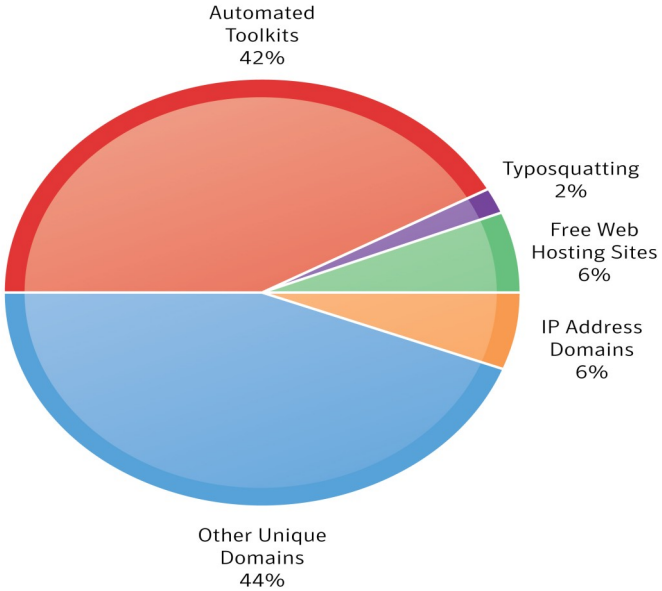
This report discusses the metrics and trends observed in phishing activity during the month of June 2009.

Highlighted in the June 2009 report:

- **Symantec observed that 42% of phishing URLs were generated using phishing toolkits; an increase of 100% from the previous month**
- **There was a 14% decrease from the previous month in non-English phishing sites**
- **More than 98 Web hosting services were used, which accounted for 6 percent of all phishing attacks; a decrease of 5 percent from the previous month**
- **Symantec observed a new trend of phishing attack towards the popular social-networking site Facebook**

Phishing Tactic Distribution: Phishing sites were categorized based upon the domains they leveraged. A considerable increase was seen in the number of phishing sites using automated toolkits. This increase was a result of a large toolkit attack targeting an information services brand.

Overall Statistics



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

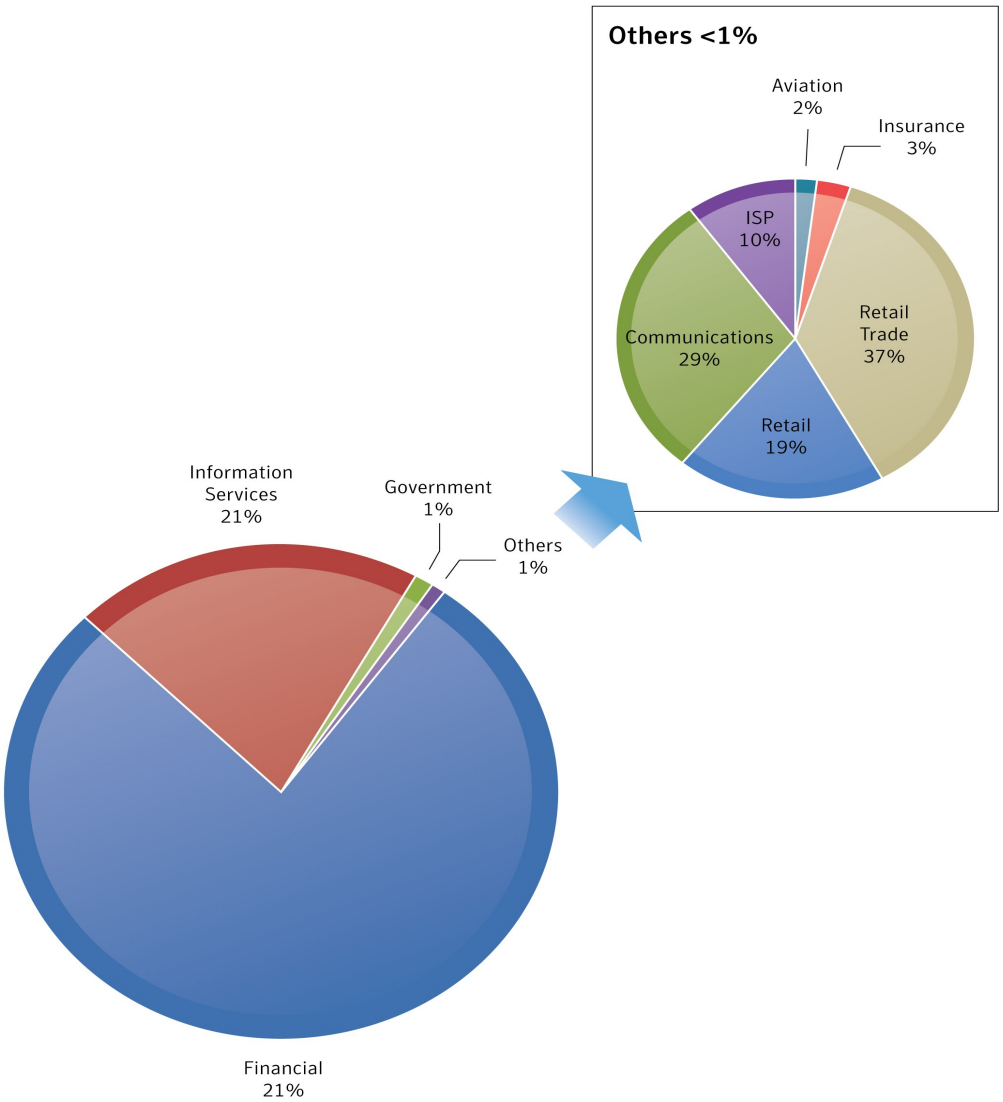
The following categories were analyzed:

- Sectors
- Number of brands
- Phishing toolkits
- Fraud URLs with IP addresses
- Phish sites 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

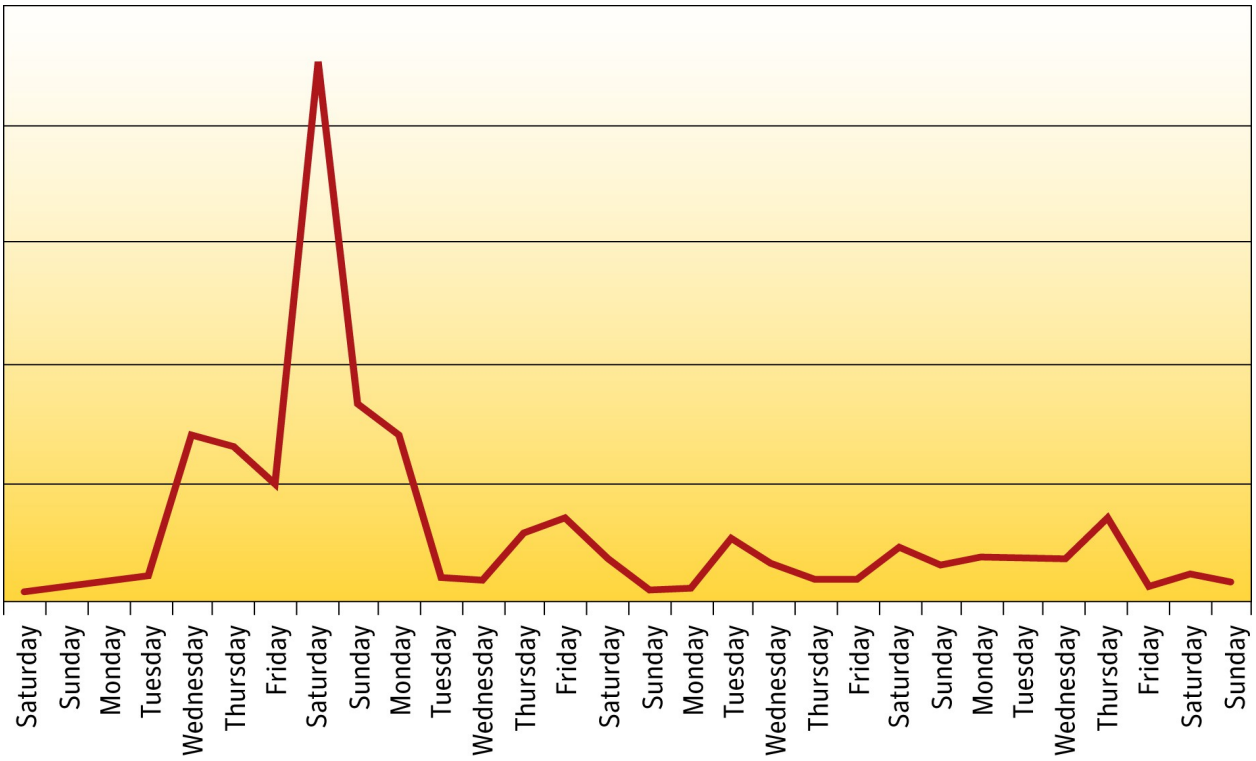
Sectors: Phishing target sectors are seen in the graphic below.

Number of Brands: Symantec observed that 58 percent of all attacks were from unique phishing Web sites, which included more than 206 targeted known brands. The unique attacks decreased by 9 percent from the previous month. This was the result of a sharp increase in toolkit activity as the trending of the two is usually inversely correlated.

Sectors



Weekly Behavior of Phishing Toolkit Activity



Automated Phishing Toolkits: Symantec observed that 42 percent of phishing URLs were generated using phishing toolkits in the last month. The number of toolkit attacks increased by 100 percent. Symantec observed that there was a sudden increase in toolkit attacks during the first week of the month (primarily targeting the information services and Financial sectors).

The rise in toolkit attacks was primarily the resurgence in phishers targeting a popular information services brand. This is in all likelihood related to a specific Command & Control server being reactivated, as toolkit activity often fluctuates with the activities of Command & Control servers and botnets.

In May, Symantec observed a new trend of phishing attacks towards the popular social-networking site Facebook. The domains hosting the phishing sites were mainly a jumble of haphazardly generated names all of which included a country code (many of which were ".im", ".at" or ".be"). Most of these phishing sites were based out of Latvia and China.

Symantec suspects that the initial Facebook phishing attack vector was through forged spam email. However, once user accounts had been compromised, the attacks were most likely launched through Facebook itself. The purpose of phishing attacks towards popular information services sites are primarily to obtain a large number of credentials and leverage email services for spamming activities. Fortunately the team at Facebook regarded the phishing attacks very seriously and worked diligently to remove messages with those links, and helping secure any compromised accounts.

Phishing Attacks Using IP Address Domains

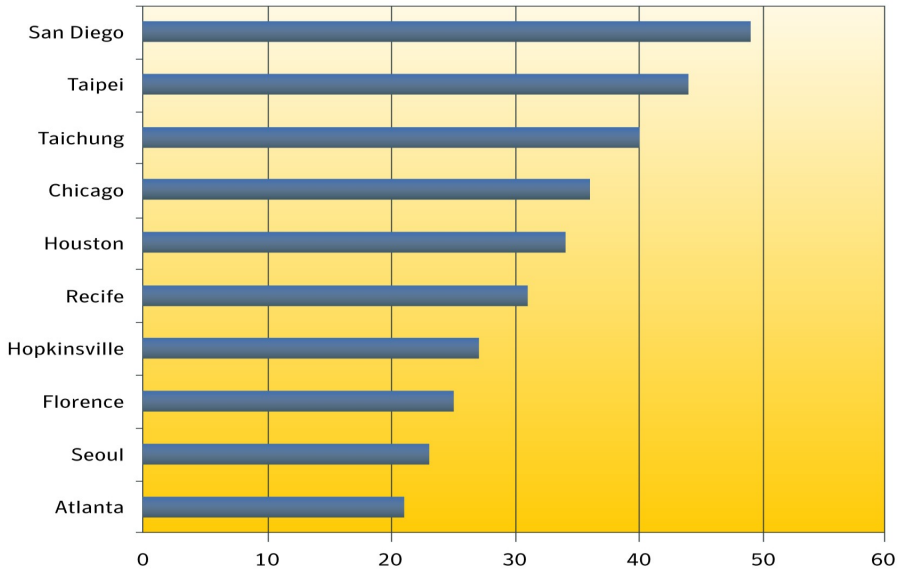
Phishers today use IP addresses as part of the hostname instead of a domain name. This is a tactic used to hide the actual fake domain name that otherwise can be easily noticed. Also, many banks use IP addresses in their Web site URLs.

A total of 1237 phishing sites were hosted in 77 countries. This amounted to an increase of approximately 2 percent of IP attacks in comparison to the previous month. The Greater China region accounted for approximately 15 percent of IP attacks in the month. Brazil and Russia are new members in the top ten list making their debut appearance at the third and fourth positions respectively.

The top cities hosting Phish sites were San Diego, Taipei and Taichung. Symantec observed that Phish sites with IP domains continue to originate from more and more new cities every month.

May 2009 Rank	April 2009 Rank	Country	May 2009 Percentage	April 2009 Percentage	Change
1	1	United States	37%	32%	5%
2	3	Greater China	15%	10%	5%
3	17	Brazil	5%	Not listed in the top five regions of phish origin	N/A
4	18	Russia	4%	Not listed in the top five regions of phish origin	N/A
5	4	United Kingdom	4%	3%	1%

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



Phishing Exploits of Free Web Hosting Services

Free Web-Hosting services has been the easiest form of phishing in terms of cost and technical skill required to develop fake sites.

A total of 98 different Web-Hosting services served as the home for 1,434 phishing sites. More than 52 brands were attacked using this method in the reporting period.

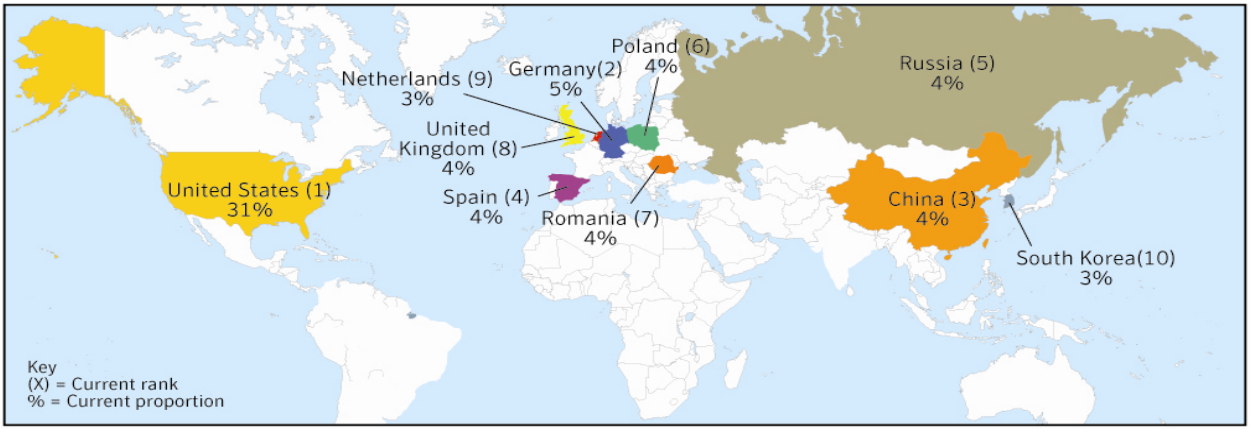
However, this form of attack is not as widely used as it frequently requires manual efforts to prepare the phishing Web page, unlike the automated kit generated Web sites. Many Free Web Hosts have also improved their preventative and corrective anti-phishing measures significantly decreasing the lifespan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

Leading this area are the USA (31 percent), Germany (5 percent) and China (4 percent). It is interesting to observe that the proportion of active phishing lures remains evenly distributed for the rest of the locations as in the recent months.

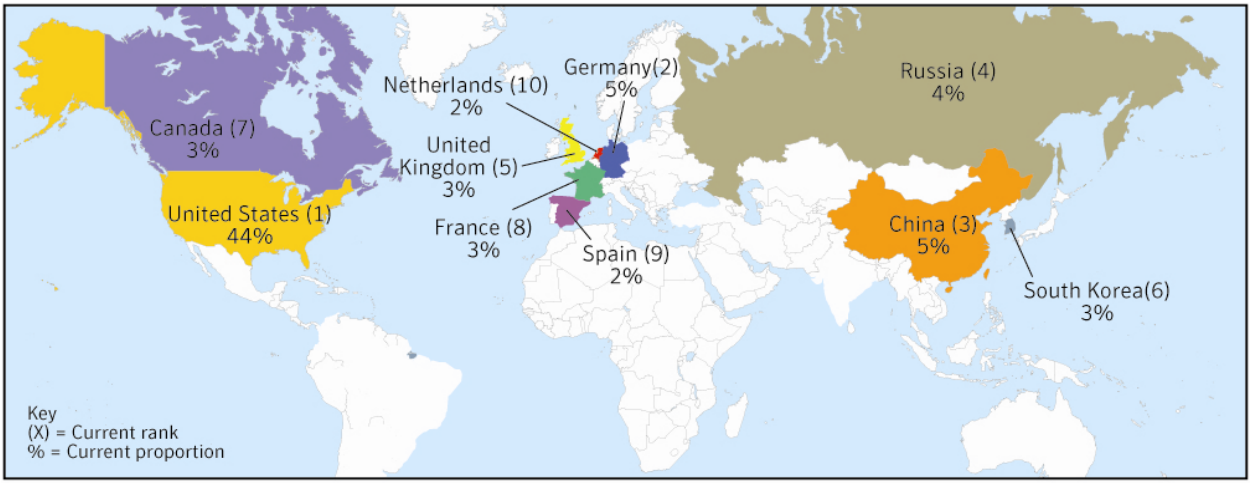
1. Geo-Location of Phishing Lures



2. Geo-Location of Phishing Web Hosts

The top countries are USA (44 percent), Germany (5 percent) and China (5 percent).

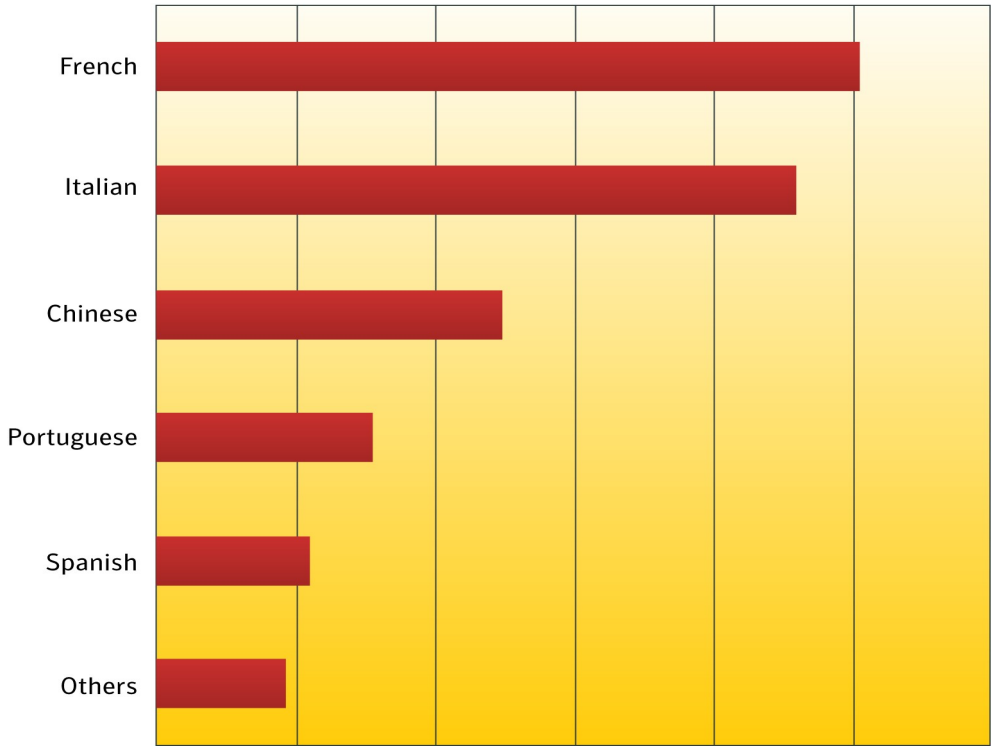
Unlike the active phishing lures, the distribution of web hosts was somewhat unevenly distributed.



Non-English Phishing Trends

Phishing attacks in French, Italian and Chinese languages were found to be higher in May. French language attacks topped the list for the second consecutive month. Symantec observed that phishing Web sites in French and Italian language remained to be higher for some popular financial brands. French and Italian language phishing sites were mainly from the financial sector, while Chinese language phishing sites were from 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 particular classes of organizations (.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 (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 May were, .com, .net and .org comprising of (54 percent), (8 percent) and (5 percent) respectively.

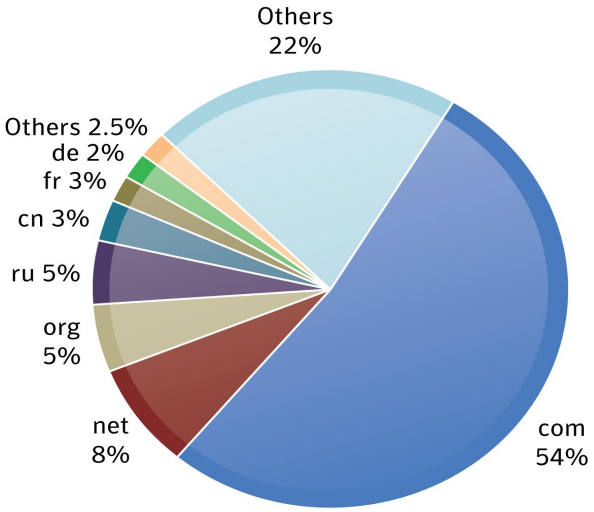
The Top-Level Domains in phishing were then further categorized:

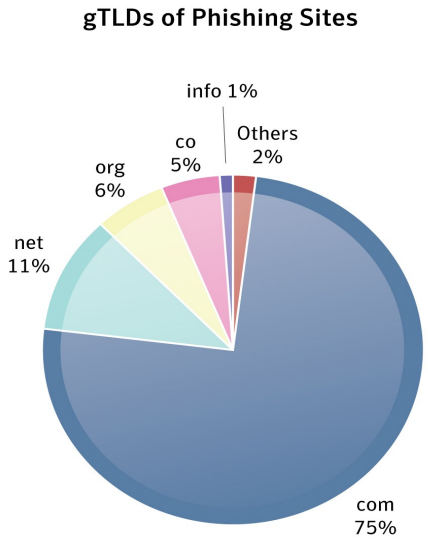
1. Generic Top-Level Domains (gTLDs)

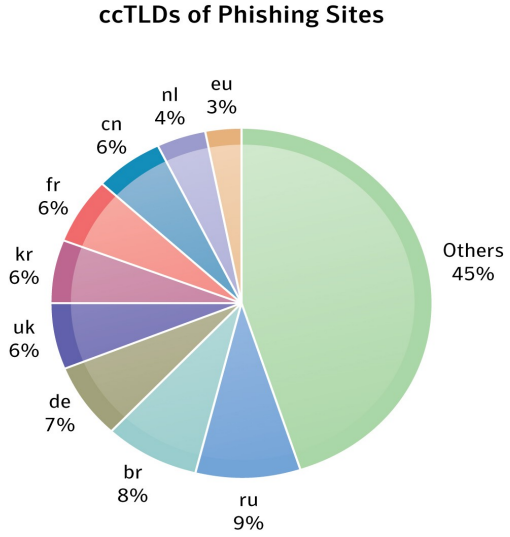
The generic TLDs .com, .net and .org were the most utilized with (75 percent), (11 percent) and (6 percent) of the total phish attacks respectively.

2. Country Code Top-Level Domains (ccTLDs)

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

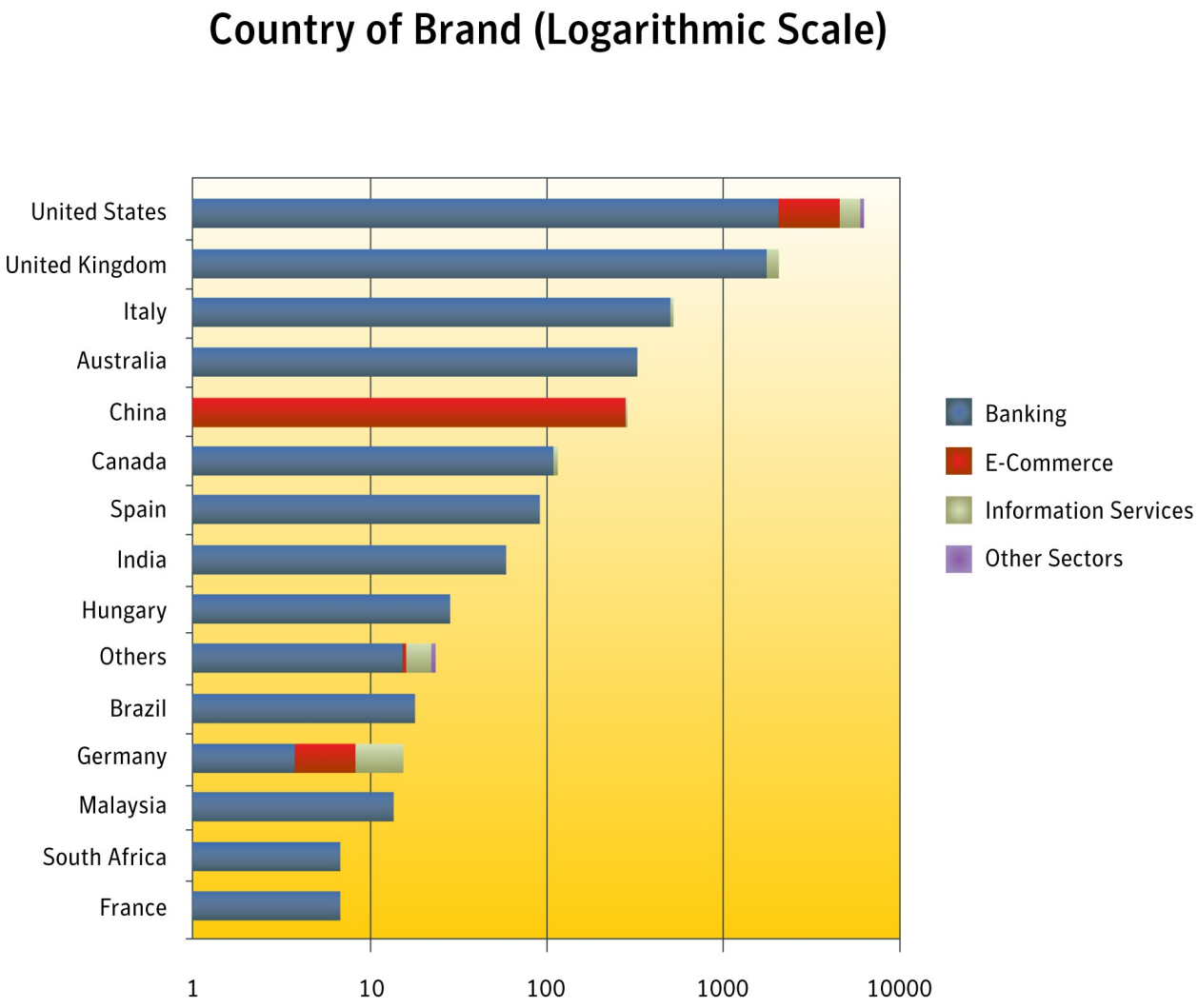






Country of Targeted Brands

The brands that the 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 May were the USA, UK and Italy. There were 24 countries whose brands were attacked. 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 has been a primary target. Also in the month of May, there was a considerable increase observed in the phishing sites targeted towards some Australian Financial brands.

Glossary of Terms

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

Unique Phishing Web site: The phishing Web sites that have a unique Web page are classified as "Unique Phishing Web sites". 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 Web sites 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 Web sites. These Web sites 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 Web sites.

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

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.