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.

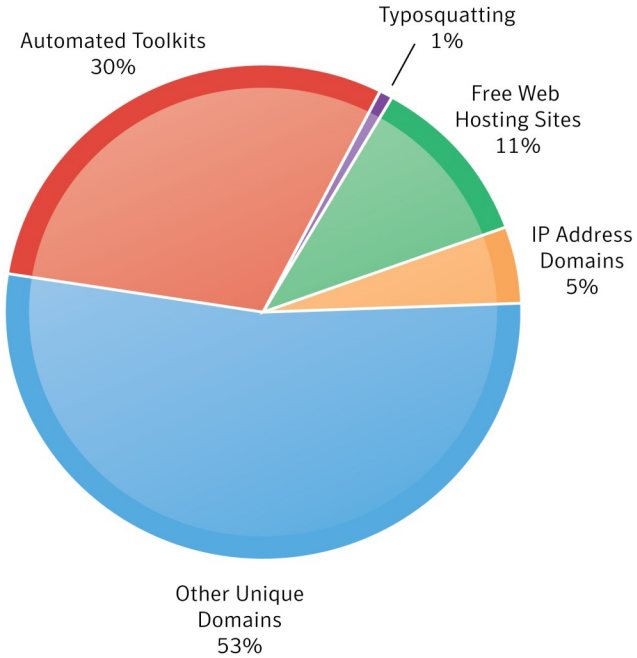
This report discusses the metrics and trends observed in phishing activity during the month of August 2009.

Highlighted in the September 2009 report:

- **Symantec observed a 45 percent decrease from the previous month in all phishing attacks**
- **30 percent of phishing URLs were generated using phishing toolkits; a decrease of 74 percent from the previous month**
- **There was a 11 percent increase from the previous month in non-English phishing sites**
- **More than 111 Web hosting services were used, which accounted for 11 percent of all phishing attacks; a decrease of 4 percent of total Web host URLs when compared to the previous month**
- **Symantec identified an increase in a phishing tactic used in an attack targeting a popular email client application**

Overall Statistics

Phishing Tactic Distribution: Phishing sites were categorized based upon the domains they leveraged. A considerable decrease was seen in the number of phishing sites being generated using phishing toolkits. This was largely due to the discontinuation of a large toolkit attack targeting a social networking site. Although, there is some decrease in phishing toolkit activity, it possibly could be a short term variation in strategies before we see resurgence in the upcoming holiday season. The decrease in phishing toolkit activity is also partially attributable to an overall decrease in the volume of phishing activity in the reporting period.



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

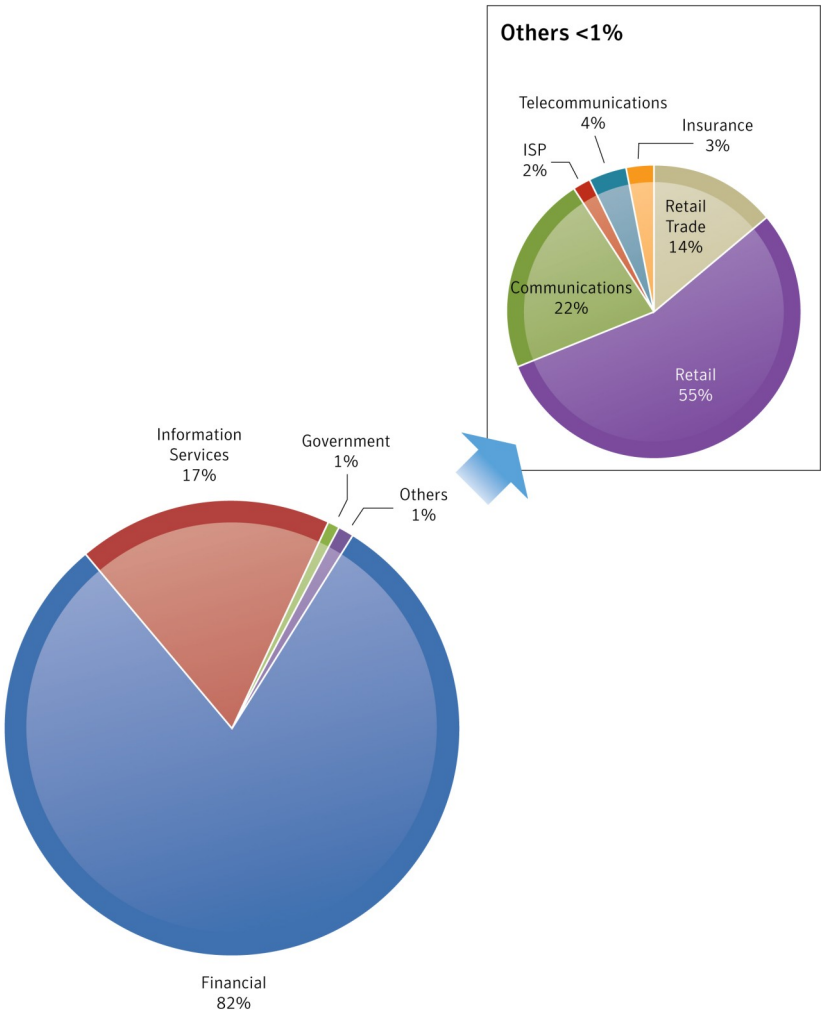
The following categories were analyzed:

- 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.

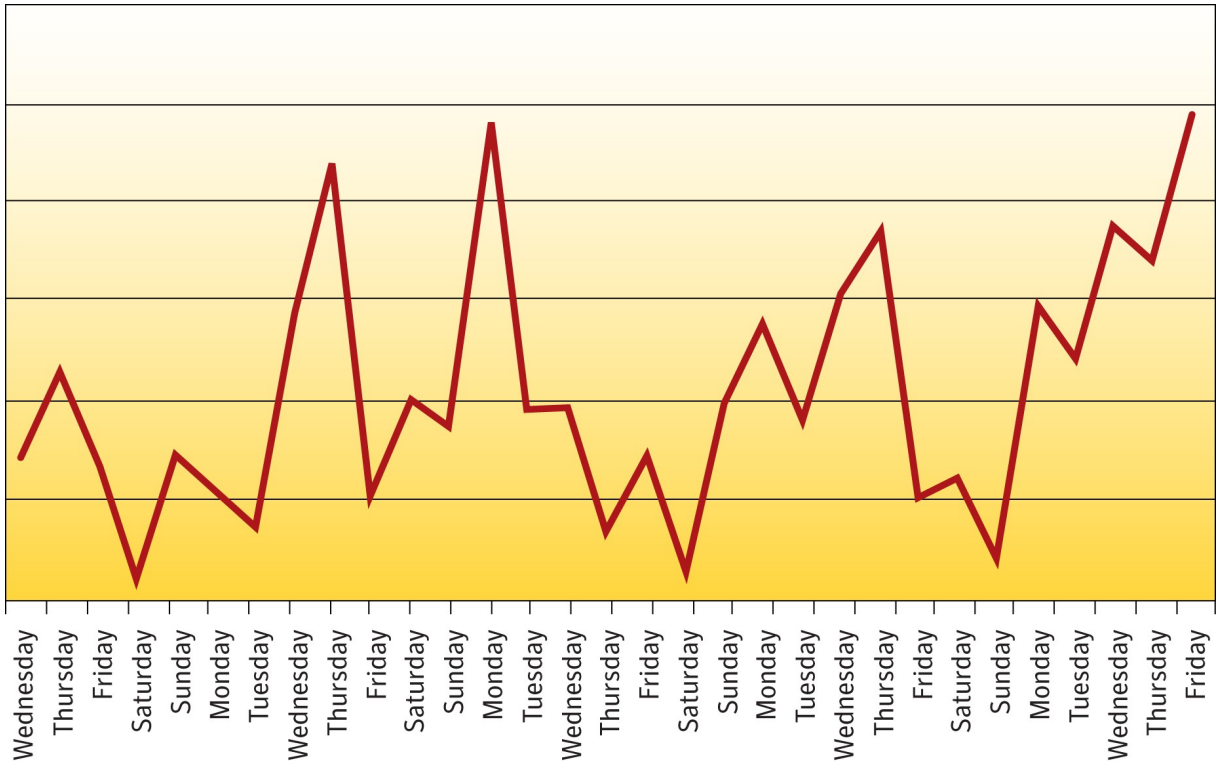
Sectors



Number of Brands:

Symantec observed that 70 percent of all attacks were from unique phishing websites, which included more than 222 targeted brands. Although, the unique phishing activity increased by only 3 percent in August, the proportion of unique phishing URLs increased considerably from 37 percent (in July) to 70 percent (in August). This was the result of a sharp decrease 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 August 30 percent of phishing URLs were generated using phishing toolkits. The number of toolkit attacks decreased dramatically by 74 percent. Symantec observed that there was a continuous fluctuation in the toolkit attacks throughout the month. There was a slight increase observed in the toolkit attack (primarily targeting the information services and financial sector) towards the end of the month.

The increase in toolkit attacks observed in the recent months primarily targeted a social networking site, and was discontinued in August. This in all likelihood is related to a specific Command & Control servers' activity being brought down. Symantec observed that this resulted in a slight increase in toolkit attacks targeting the financial sector, as the fraudsters possibly activated another botnet from their distributed infrastructure, to carry out the phishing attack.

Phishing Trojan Targets Email Client:

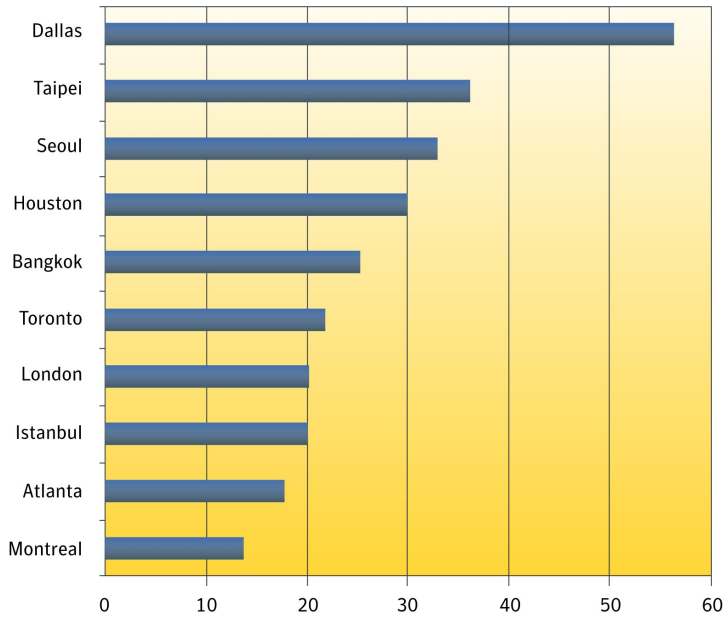
In August, Symantec observed an increase in phishing attacks facilitated by spam email messages targeting a popular email client application. The phishing scam messages lured the intended victims to re-configure their email client application by a link provided in the email. The link directed the potential victim to a phishing Web page that requested the download of a critical security update for the email application. The security update was in fact a malicious application file developed by the fraudsters that further attempted to acquire user credentials such as the email account name, password, and the mail server name. This would enable the fraudsters to gain control over the email application and steal critical information, or even use it for further spamming activities.

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 easily be noticed. Also, many banks use IP addresses in their website URLs.

A total of 1115 phishing sites were hosted in 71 countries. This amounted to an increase of approximately five percent of IP attacks in comparison to the previous month. The United States continued to be the top ranked country hosting phishing sites. The Greater China region accounted for approximately 7 percent of IP attacks in the month. The total number of IP attacks originating from this region, reduced by 2 percent over the previous month. South Korea is a new member in the top five countries, making its debut appearance at the fifth position. Panama, which has found a steady uptrend in Internet usage, for the second consecutive month featured in the list of top five countries hosting phishing sites. It is a possibility that attackers have identified vulnerabilities in the hosting environment of this region.

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



The top cities hosting Phish sites were Dallas, Taipei and Seoul. Symantec observed that Phish sites with IP domains continued to originate from newer cities every month. In August, Istanbul was one such debutant in the list of top cities hosting phish sites.

August 2009 Rank	July 2009 Rank	Country	August 2009 Percentage	July 2009 Percentage	Change
1	1	United States	33%	29%	4%
2	2	Greater China	7%	9%	-2%
3	7	United Kingdom	6%	Not listed in the top five regions of phish origin	N/A
4	3	Panama	5%	7%	-2%
5	10	South Korea	5%	Not listed in the top five regions of phish origin	N/A

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.

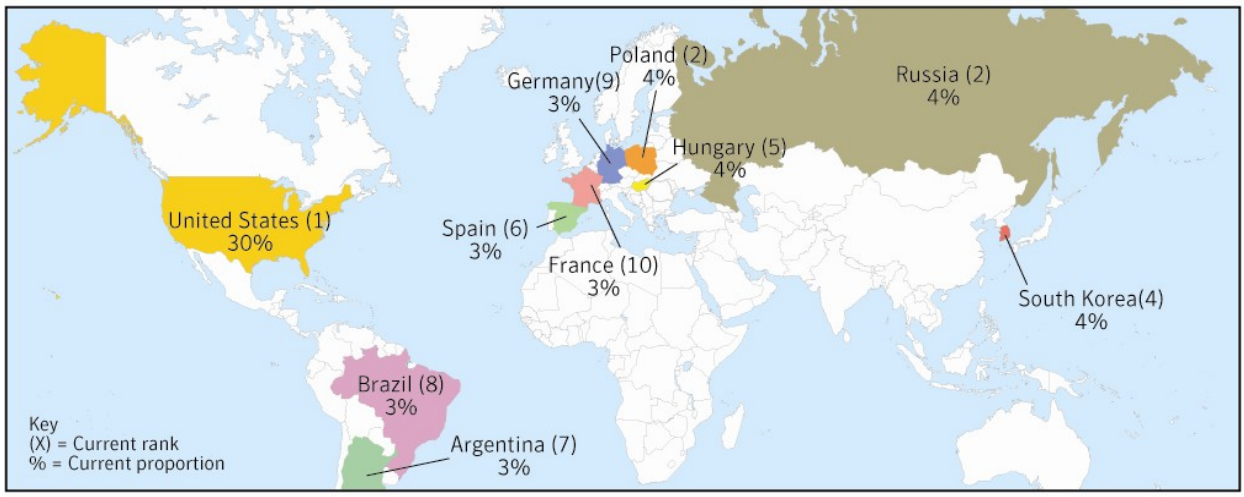
A total of 111 different Web hosting services served as the home for 2,314 phishing sites in the month of August. Symantec observed that there was a three percent decrease in the number of free Web hosting services utilized for developing phishing sites. More than 86 brands were attacked using this method 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 websites. 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

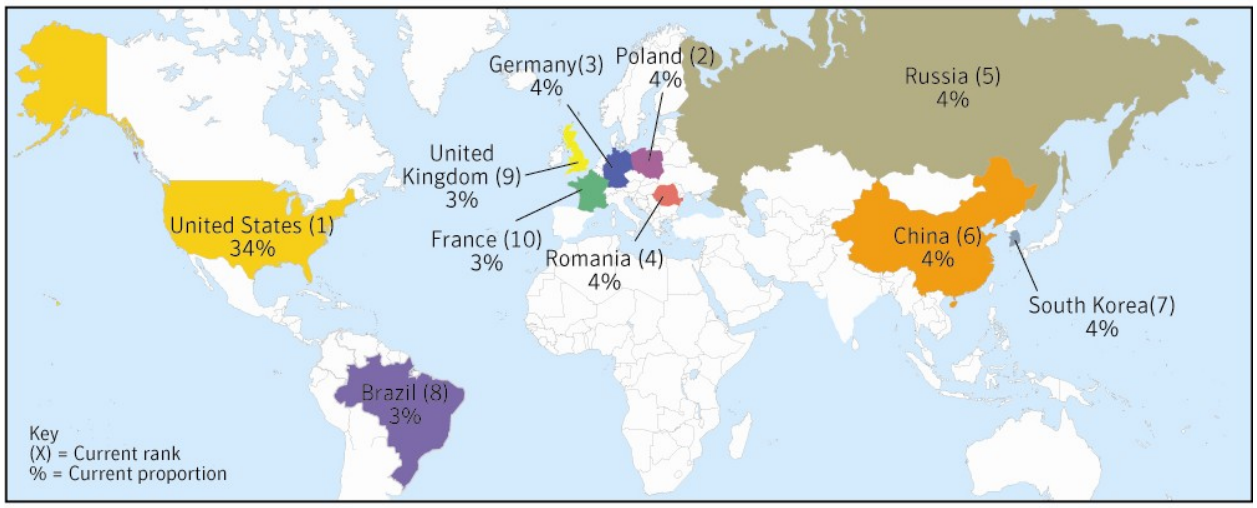


Leading this area are the USA (30 percent), Russia (4 percent) and Poland (4 percent). In August, there was a considerable increase observed in the proportion of phishing lures for Hungary and Brazil making an introduction at the fifth and the ninth positions respectively. The proportion of active phishing lures remained evenly distributed for the rest of the locations.

2. Geo-Location of Phishing Web Hosts

The top countries are USA (34 percent), Poland (4 percent) and Germany (4 percent). There was a considerable increase observed in the proportion of phishing hosts for Poland. In August, the distribution of web hosts was evenly distributed for all other locations.

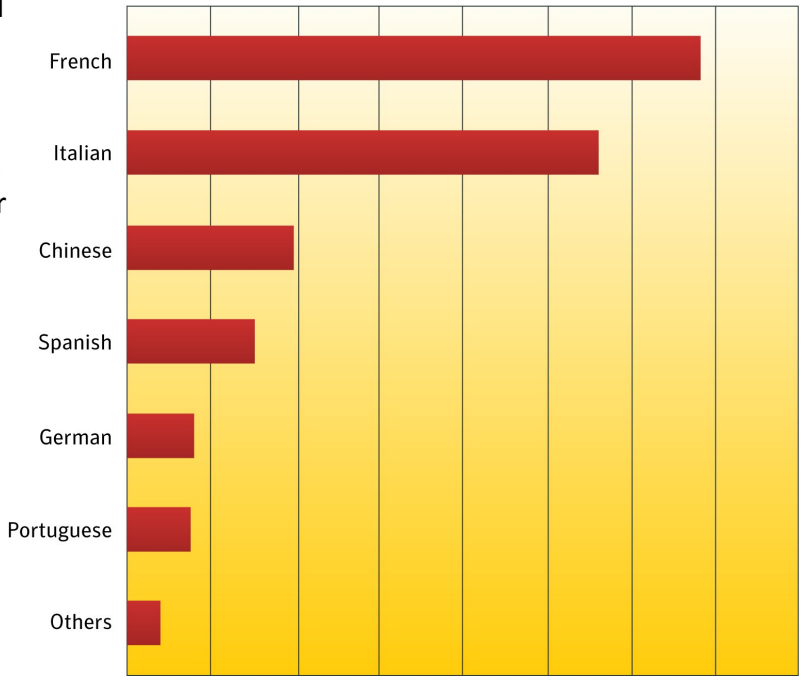
Geo-Location of Phishing Web Hosts



Non-English Phishing Trends

Phishing attacks in French, Italian and Chinese languages were found to be higher in August. French language attacks continued to be in the top position. Symantec observed that phishing websites in French and Italian remained higher for some popular financial brands. 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.

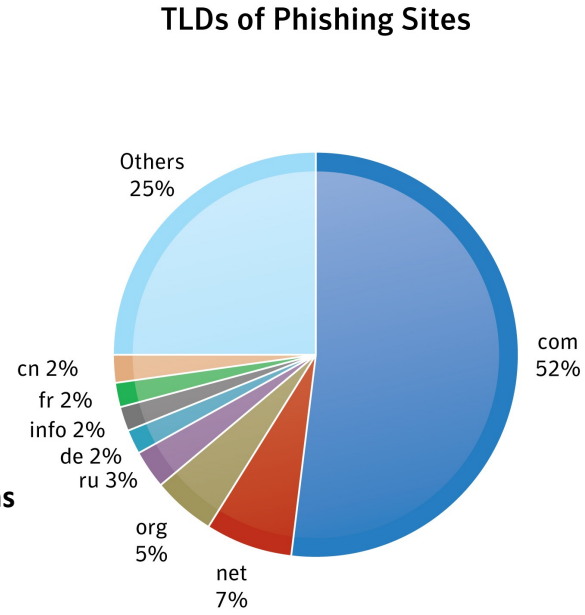
Comparisons of Top-Level Domains of Phishing Sites

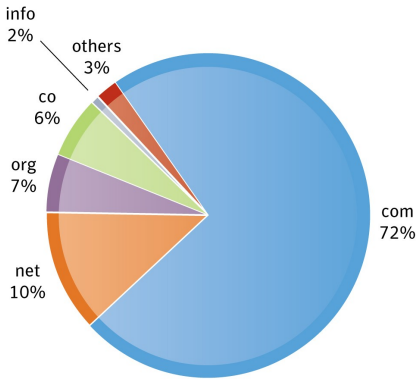
Overall TLDs

The most used TLDs in phishing sites in the month of August were, .com, .net and .org comprising of (52 percent), (7 percent) and (5 percent) respectively.

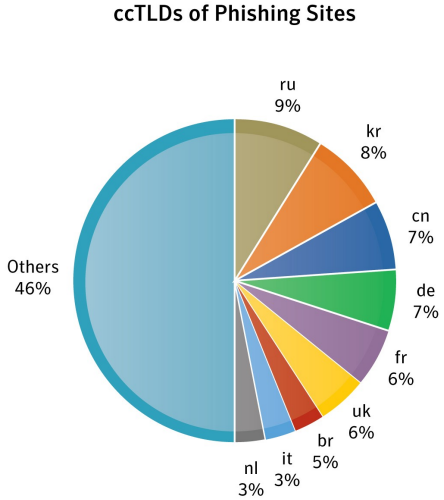
The Top-Level Domains in phishing were then further categorized:

1. Generic Top-Level Domains (gTLDs)
The generic TLDs .com, .net and .org were the most utilized with (72 percent), (10 percent) and (7 percent) of the total phish attacks respectively.





2. Country Code Top-Level Domains (ccTLDs)
The Russian, Korean and Chinese ccTLDs were evaluated to be the highest in phishing attacks with (9 percent), (8 percent) and (7 percent) respec-tively.

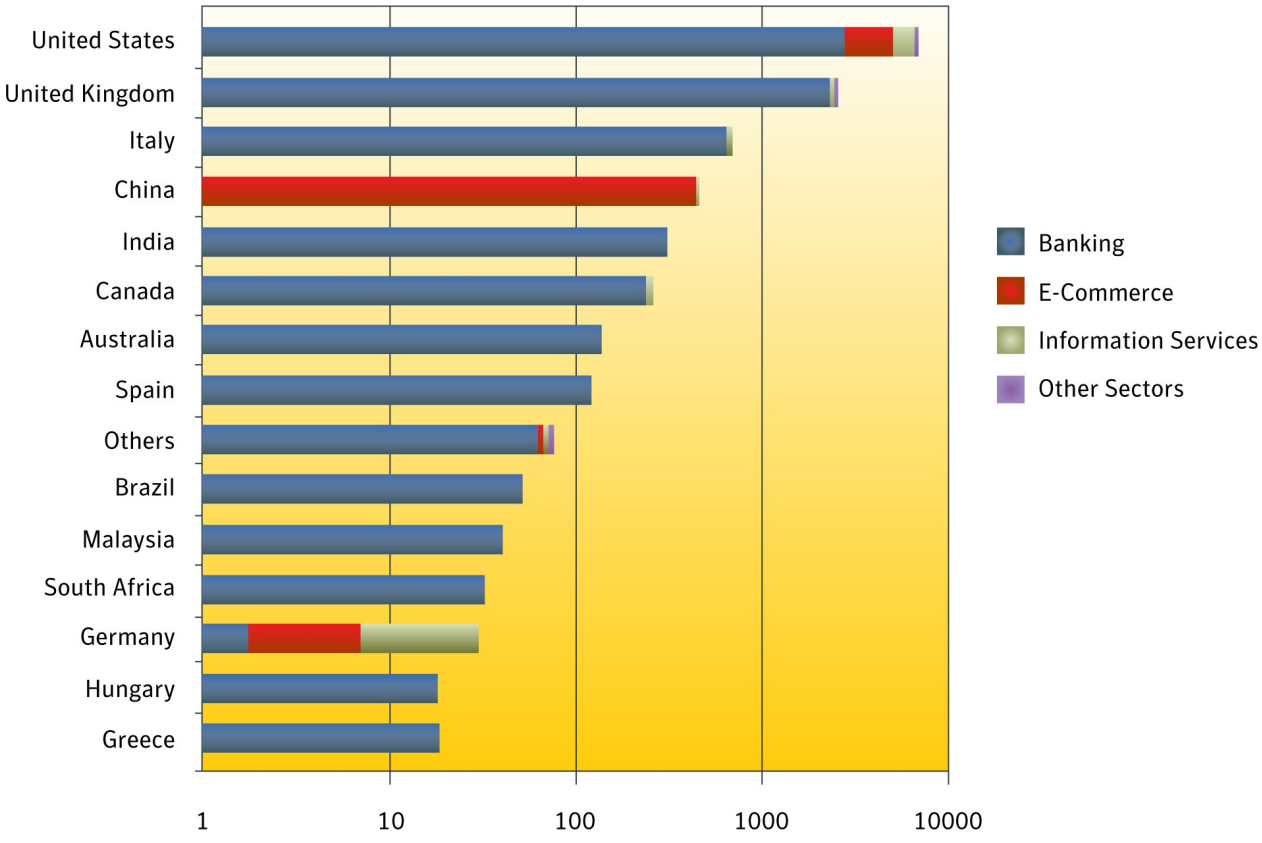


Country of Targeted Brands

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 August were the USA, UK and Italy. There were 30 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. A slight increase was observed in the phishing sites from the information services sector in the case of German brands. In China, the e-commerce sector remains a primary target. In August, there was a considerable increase observed in phishing sites targeted towards popular Indian banks.

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.