State of Phishing
A Monthly Report

Confidence in a connected world.

symantec.

October 2009 Report #24

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.

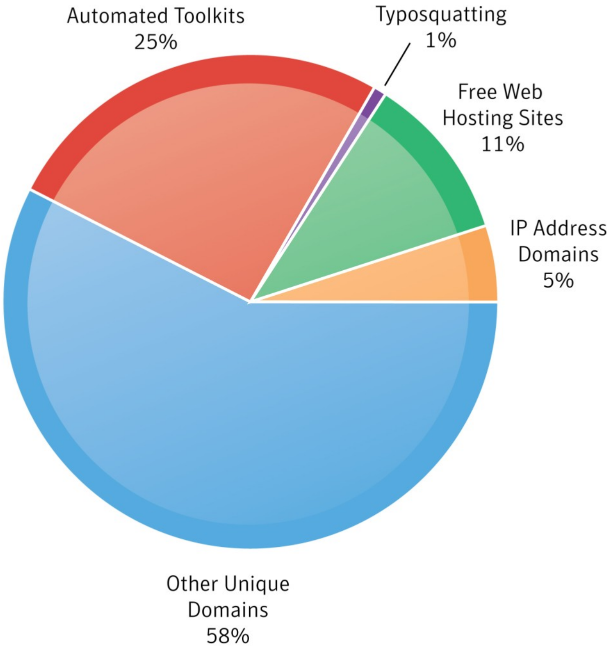
This report discusses the metrics and trends observed in phishing activity during the month of September 2009.

Highlighted in the October 2009 report:

- **Symantec observed a 5% decrease from the previous month in all phishing attacks**
- **25 percent of phishing URLs were generated using phishing toolkits; a decrease of 21 percent from the previous month**
- **Non-English phishing sites decreased by 33 percent from the previous month**
- **More than 110 Web hosting services were used, which accounted for 11 percent of all phishing attacks. Although the proportion remained the same as in August; there was a 3 % decrease in total Web host URLs in September**
- **Symantec identified an increase in a phishing tactic used in an attack targeting the U.S. tax payers**

Overall Statistics

Phishing Tactic Distribution: Phishing sites were categorized based upon the domains they leveraged. In September, an overall decrease was observed in almost all of the phishing metrics considered in the report. As seen in recent months, there was a considerable decrease observed in the number of phishing sites being generated using phishing toolkits. The continued downtrend of toolkit attacks was observed across all sectors in September. However, as cited earlier, these attacks are expected to gradually reappear as we approach 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

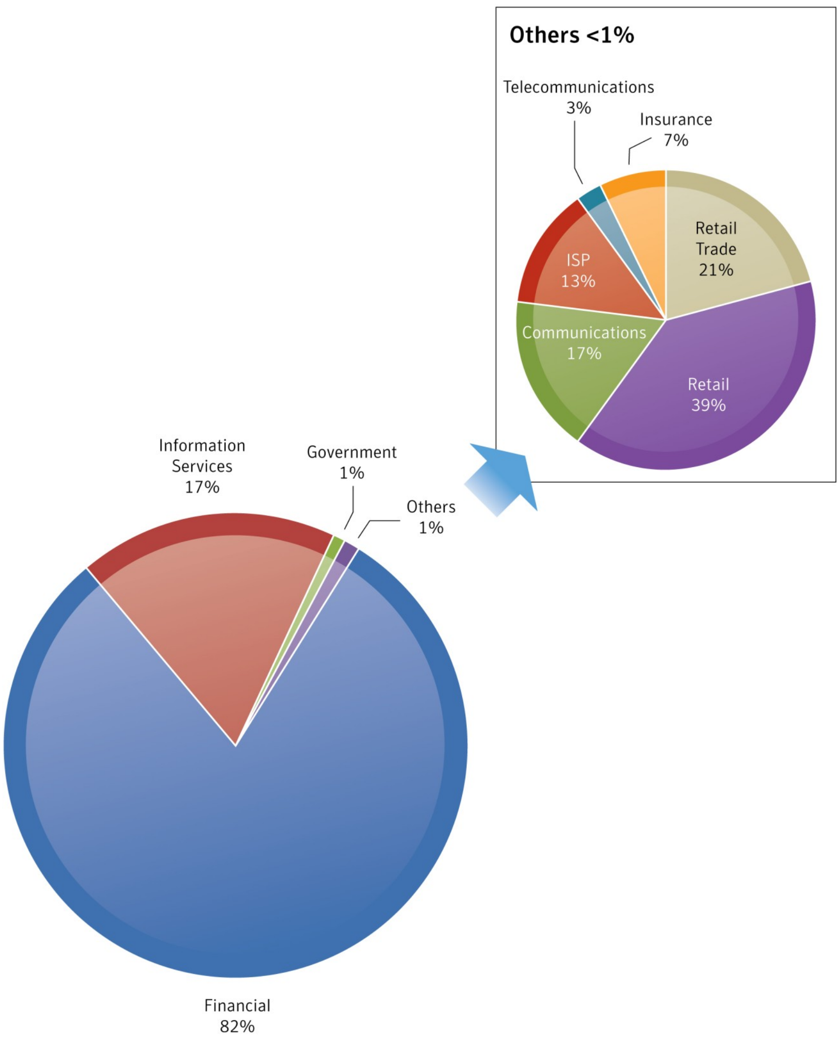
The following categories were analyzed:

- 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

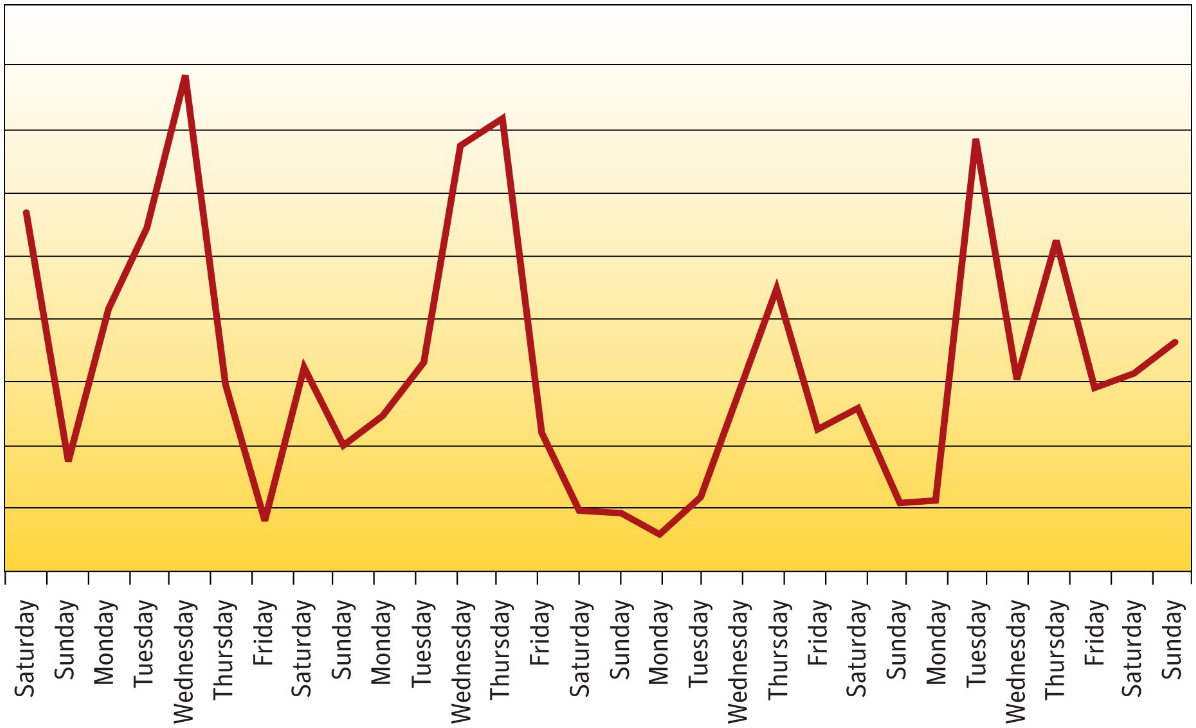
Sectors: Phishing target sectors are seen in the graphic below.

Number of Brands:
Symantec observed that 75 percent of all attacks were from unique phishing websites, which included more than 222 targeted brands. Although, the unique phishing activity remained nearly the same, the proportion of unique phishing URLs increased from 70 percent (in August) to 75 percent (in September). This was the result of a further decrease 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, in September, 25 percent of phishing URLs were generated using phishing toolkits. The number of toolkit attacks decreased considerably by 21 percent. Symantec observed that there was a continuous fluctuation in the toolkit attacks throughout the month. There was a sharp increase observed in the toolkit attack (primarily targeting a payment processing company) in the first week of the month. Symantec found this particular attack as the only exception wherein the number of phishing websites actually increased over the previous month.

The decrease in toolkit attacks was observed across all sectors. As explained in the previous month, this possibly could be a short term variation in the strategies of the fraudsters, before we see resurgence in the forthcoming holiday season. Symantec observed that the cutback in toolkit attacks has in recent months resulted in a slight increase in attacks employing other tactics such as Typo squatting.

Phishing Trojan Targets U.S. Taxpayers:

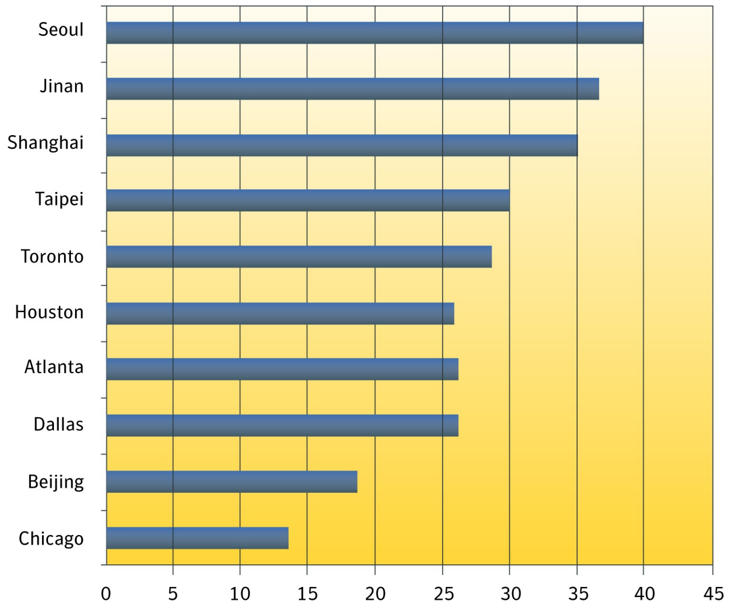
In September, Symantec observed a phishing attack facilitated by spam email messages, targeting the Internal Revenue Service tax settlement program for the U.S. tax payers. The phishing scam requested the intended victims to review their tax statement online by clicking on the link provided. The fraudsters reported the issue as “Unreported/ Underreported Income” to instill a sense of panic amongst the tax payers. The link directed the potential victim to a phishing Web page that requested to download and execute the tax statement file - “tax-statement.exe”, which in fact was a password stealing Trojan. The URLs in the phishing attack comprised of several recently created randomized domain names.

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 944 phishing sites were hosted in 60 countries. This amounted to a decrease of approximately 15 percent of IP attacks in comparison to the previous month. The United States continued to be the top ranked country hosting phishing sites. Although the proportion of IP attacks shows some increase for most of the regions, the numbers of IP attacks, with an exception of the Greater China region, have actually decreased. The Greater China region accounted for approximately 18 percent of IP attacks in the month. The total number of IP attacks originating from this region, increased by 11 percent over the previous month.

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



The top cities hosting phish sites were Seoul, Jinan and Shanghai. Symantec observed that phish sites with IP domains continued to originate from newer cities every month. In September, Jinan - the capital city of Shandong province of Republic of China, was one such debutant in the list of top cities hosting phish sites.

September 2009 Rank	August 2009 Rank	Country	September 2009 Percentage	August 2009 Percentage	Change
1	1	United States	37%	33%	4%
2	2	Greater China	18%	7%	11%
3	7	Canada	5%	4%	1%
4	3	United Kingdom	5%	6%	-1%
5	5	South Korea	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.

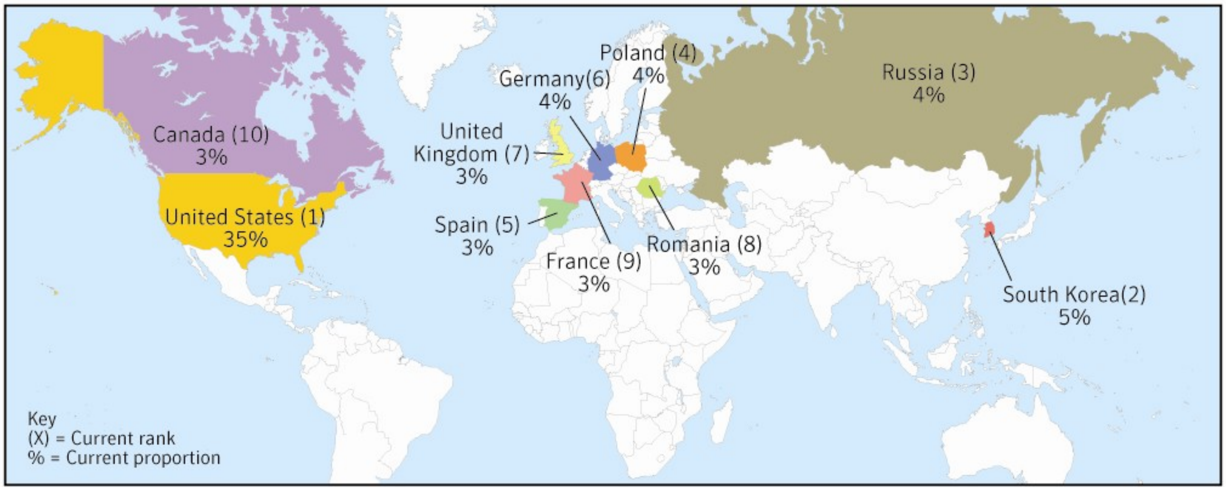
A total of 110 different Web hosting services served as the home for 2,237 phishing sites in the month of September. Symantec observed that there was a three percent decrease in the number of free Web hosting services utilized for developing phishing sites. More than 79 brands were attacked using this 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

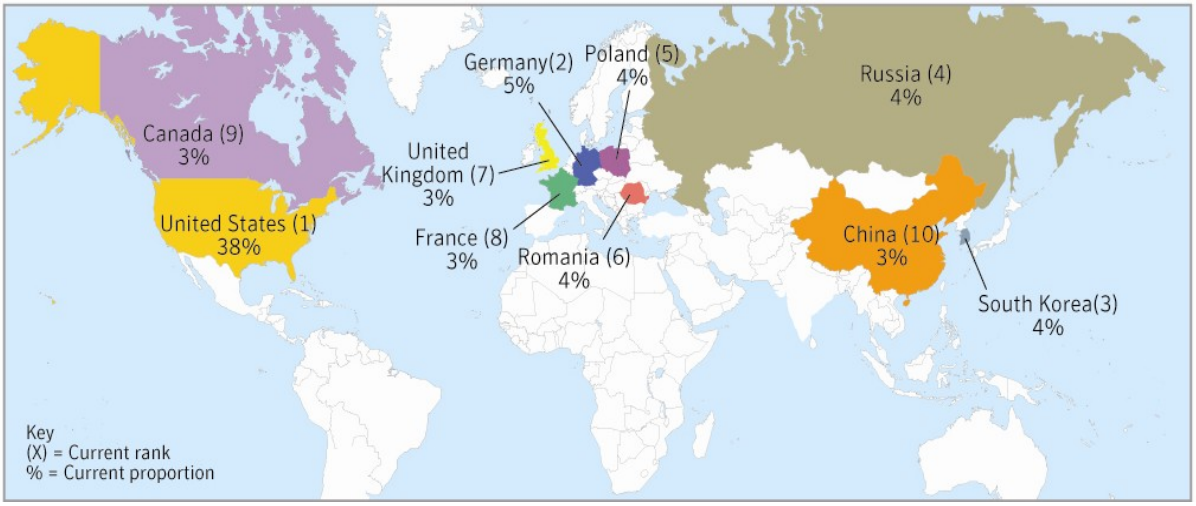


Leading this area are the USA (35 percent), South Korea (5 %) and Russia (4 %). In September, there was a considerable increase observed in the proportion of phishing lures for South Korea making an introduction at the second position. The proportion of active phishing lures remained evenly distributed for the rest of the locations.

2. Geo-Location of Phishing Web Hosts

The top countries are USA (38 percent), Germany (5 %) and South Korea (4 %). As seen in the phishing lures, there was a considerable increase observed in the proportion of phishing hosts for South Korea. In September, the distribution of Web hosts was evenly distributed for all other locations.

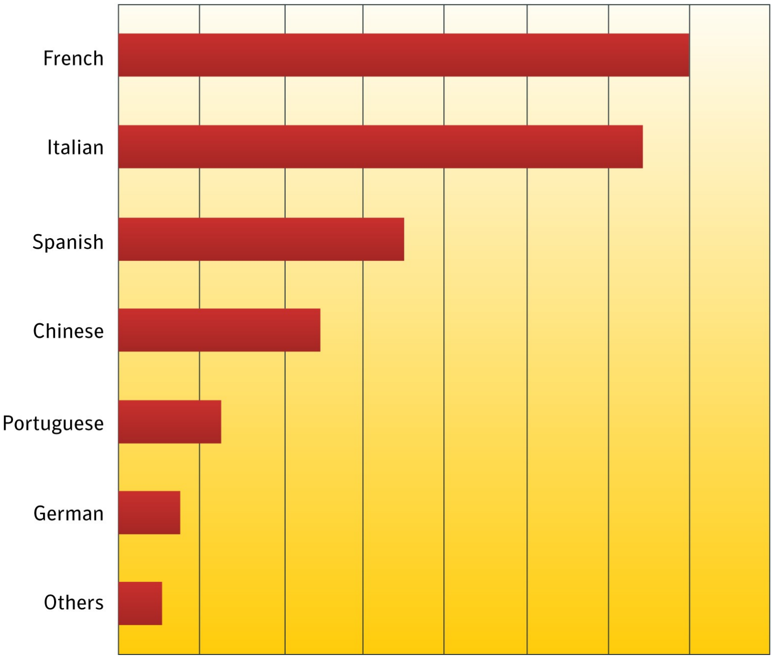
Geo-Location of Phishing Web Hosts



Non-English Phishing Trends

Phishing attacks in French, Italian and Spanish languages were found to be higher in September. French language attacks continued to be in the top position. Symantec observed that phishing websites in French, Italian and Spanish remained higher for the financial sector. 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

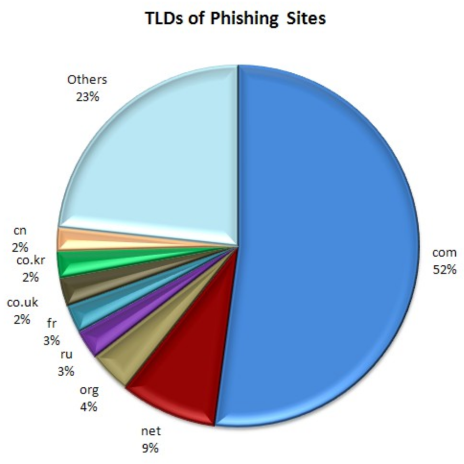
Overall TLDs

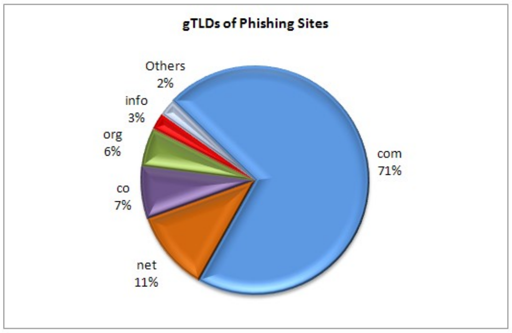
The most used TLDs in phishing sites in the month of September were, .com, .net and .org comprising of (52 percent), (9 %) and (4 %) respectively.

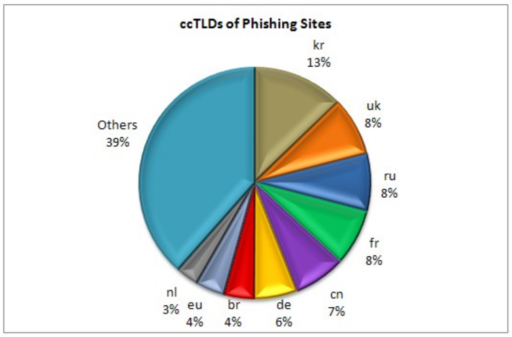
The Top-Level Domains in phishing were then further categorized:

1. Generic Top-Level Domains (gTLDs)

The generic TLDs .com, .net and .co were the most utilized with (71 percent), (11 percent) and (7 %) of the total phish attacks respectively.







2. Country Code Top-Level Domains (ccTLDs)

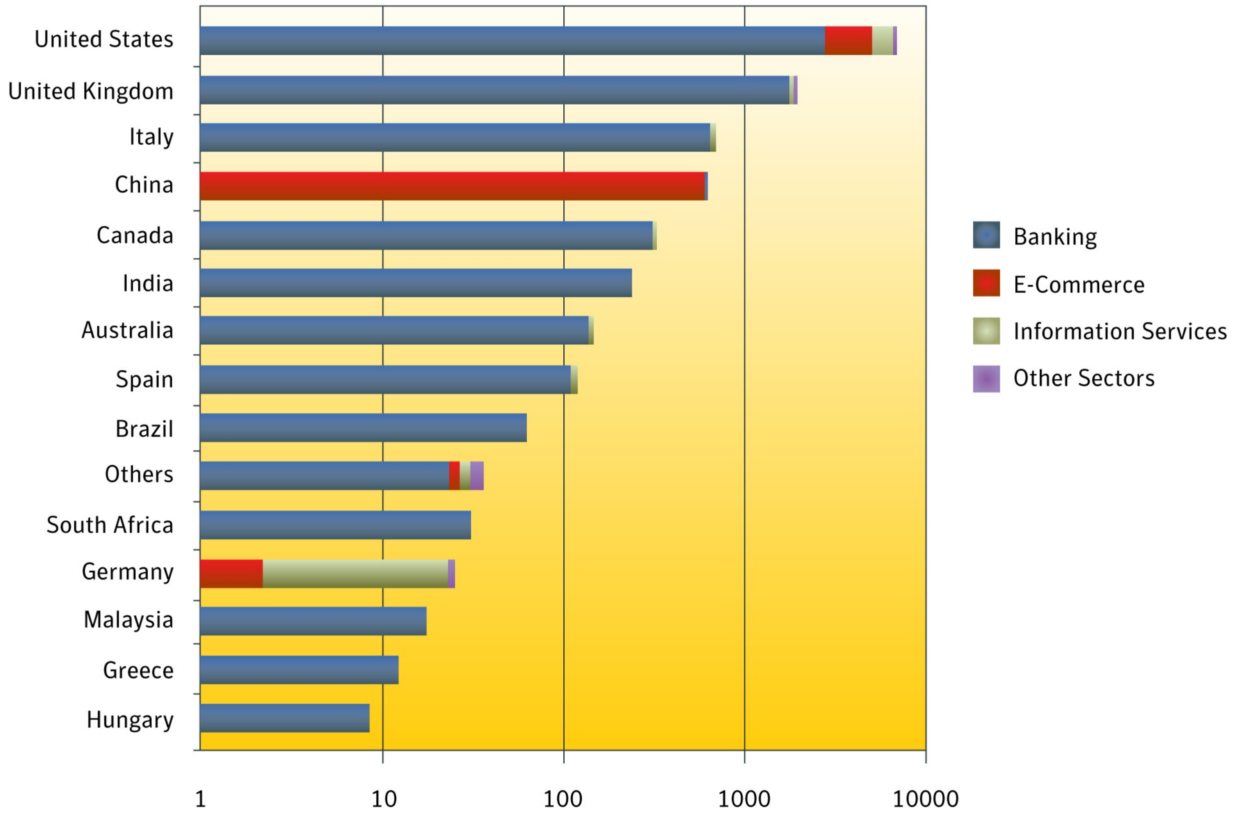
The Korean, United Kingdom and Russian ccTLDs were evaluated to be the highest in phishing attacks with (13 percent), (8 %) and (8 %) respectively.

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 September were the USA, UK and Italy. There were 27 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 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.

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.