The State of Phishing
A Monthly Report – May 2009

Compiled by Symantec Security Response
Anti-Fraud Team

Sainarayan Nambiar
Principal Author
Security Response

Suyog Sainkar
Principal Author
Security Response

David Cowings
Editor & Author

Sagar Desai
Editor
Public Relations
Sagar_Desai@symantec.com

Contributors

Zahid Raza
Researcher
Security Response

Rohan Shah
Researcher
Security Response

Ashutosh Raut
Researcher
Security Response

Ravish Bagul
Researcher
Security Response

Phishing Trends

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 May 2009.

Phishing Highlights

- The Phisher King: Phishing toolkits continued to professionalize fraud attacks. Symantec observed 25% of phishing URLs to be generated using phishing toolkits. Although there was a 19% increase in the toolkit attacks over the previous month, the proportion of toolkit attacks remained constant of the total phishing attacks observed in the month.

- Good Hosts Fry Phish: More than 113 Web hosting services were used, which accounted for 9% of all phishing attacks. Although Web hosting companies continued to improve their phishing mitigation tactics, phishing attacks using Web hosting services increased by 5% from the previous month. However when looking at the total number of phishing attacks observed in the month, the proportion of phishing attacks using Web hosting services actually decreased compared to the previous month.

- Phishing in International Waters: Among the non-English phishing sites, French language phishing sites were most frequently recorded followed by sites in Italian and Chinese language. A total of 3,650 non-English phishing sites were recorded in the month of May. This is an increase of 5% from the previous month. A rise in the non-English phishing sites in May can be the result of a slight increase in the total volume of phishing sites observed by Symantec, over the previous month.

symantec.

Overall Statistics

Overall Statistics
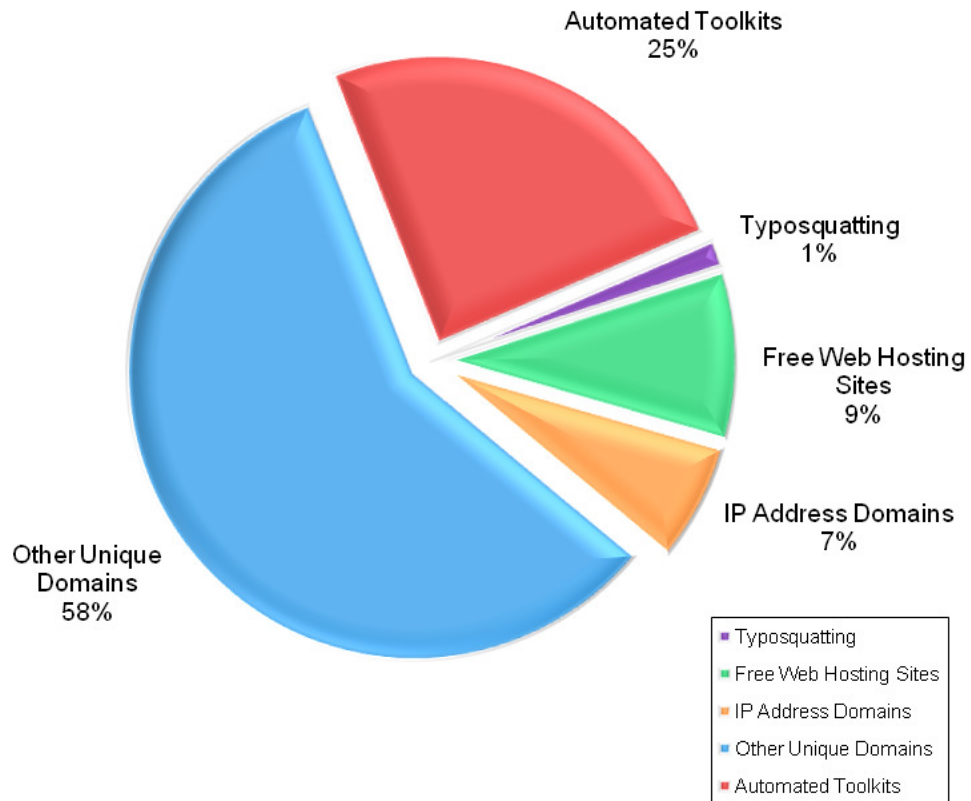
Based on their domains, all phishing sites were categorized as Automated Toolkits (25%), Typosquatting (1%), Free Web-hosting sites (9%), IP address domains (7%), and other unique domains (58%). As compared to the previous month, an increase was seen in the proportion of phishing sites using IP address domains. For the second consecutive month in a row, Symantec observed that the number of automated toolkit attacks remained at lower levels.

Confidence in a connected world

symantec.

Phishing Sectors

Phishing sites in May were categorized and analyzed to understand the attack methods and to determine the sectors and brands impacted by the attacks.

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

Confidence in a connected world

symantec.

Sectors

Phishing URLs were categorized based on the sector by evaluating the brands attacked by the phishing Web sites.
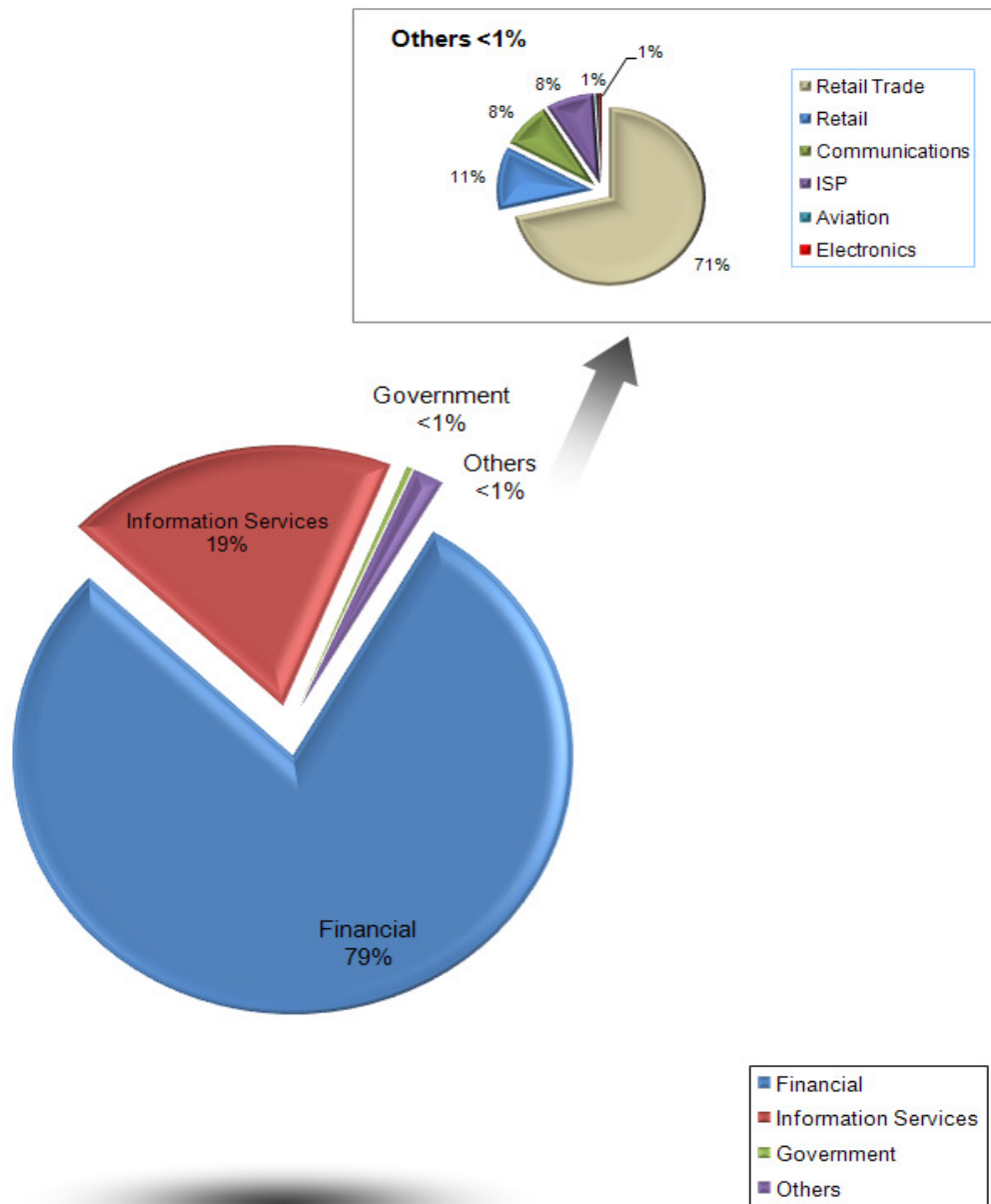
Number of Brands

> ➢ Symantec observed that 75% of the total attacks were from unique phishing Web sites, which included more than 227 known brands being targeted by phishers.

> ➢ The unique attacks increased by 25% from the previous month. However, of the total phishing attacks, there was no increase observed in unique phishing websites from the previous month as a result of the proportionate increase observed in the toolkit activity in the month.

Automated Phishing Toolkits

During the month, Symantec observed that 25% phishing URLs were generated using phishing toolkits. Although this was a 19% increase from the previous month, there was no rise in the proportion of toolkit attacks of the total phishing attacks.

Symantec observed that there was a drop in the toolkit attacks in-between the month, primarily in the Information Services sector. Besides, the toolkit attacks in this period towards the Financial sector were also observed to be at a lower level of activity than the rest of the month. Symantec observed that a previously widely used toolkit attack targeting a particular financial brand was discontinued in the month contributing to the decline in financial toolkit attacks. As toolkit activity often fluctuates with Command & Control servers and botnets going up and down, this is likely related to a specific Command & Control server being taken down.

Confidence in a connected world

symantec.

Weekly behavior of attacks from phish kits:
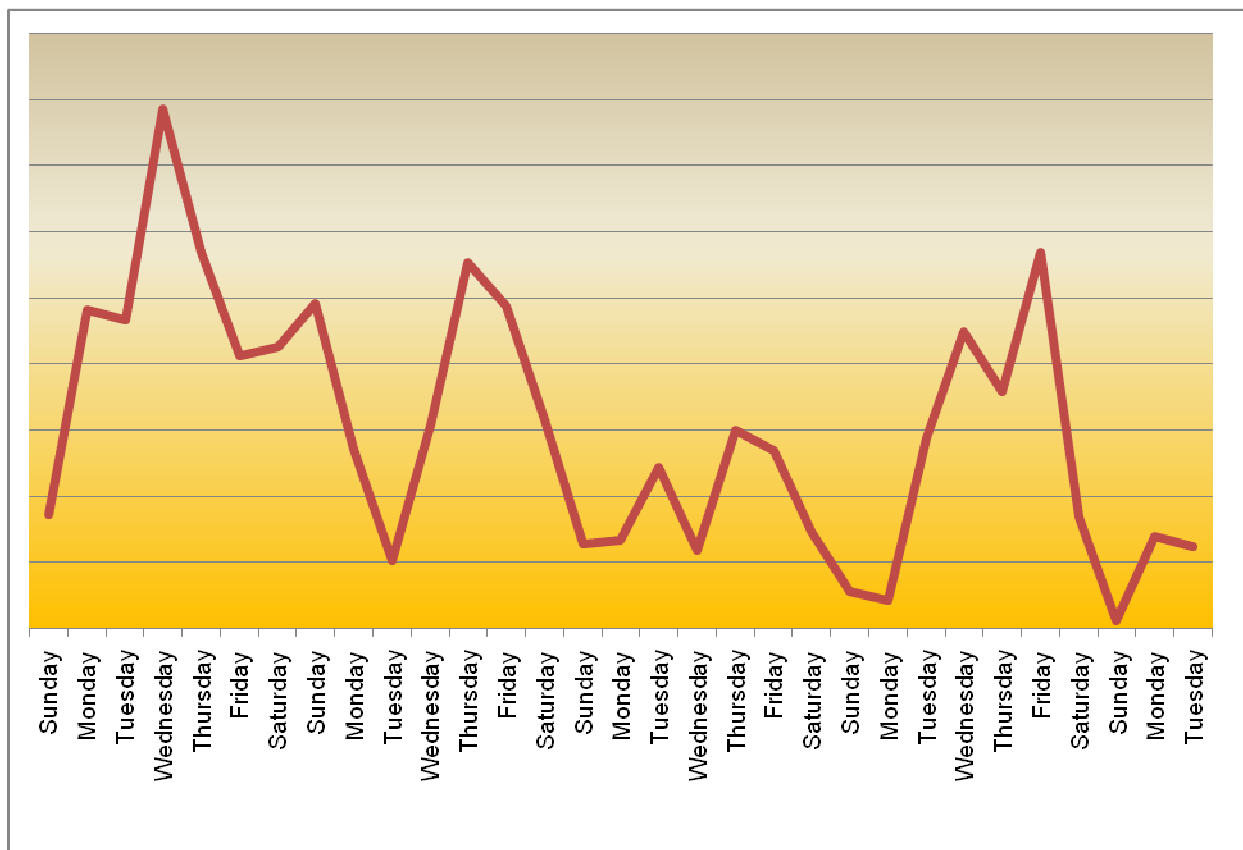
Fraud Attacks Using IP Addresses

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. This makes it confusing for customers from distinguishing a legitimate brand IP from a fake IP address.

Confidence in a connected world

symantec.
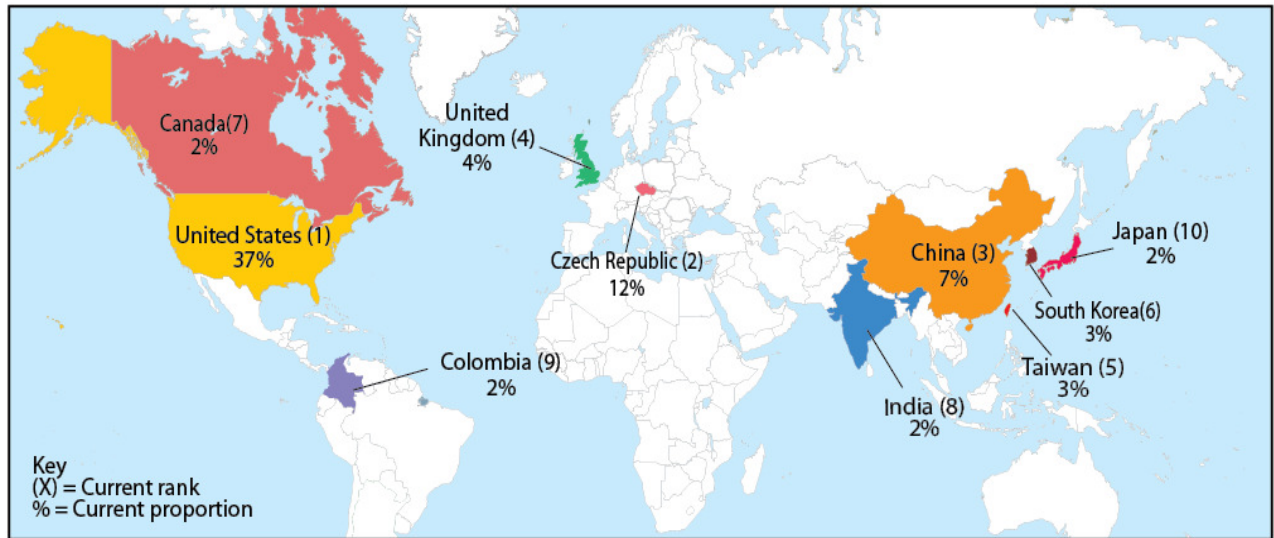
A total of 1260 phish sites were hosted in 74 countries. This accounted for an increase of approximately 53% of IP attacks in comparison to the previous month. The Greater China region accounted for approximately 10% of IP attacks in the month. Czech Republic which is usually not in the list of top ten countries where phishing sites are hosted surprisingly featured in the second position this month after United States.

May 2009 Rank	March 2009 Rank	Country	May 2009 Percentage	March 2009 Percentage	Change
1	1	United States	32%	37%	-5%
2	32	Czech Republic	12%	Not listed in the top five regions of phish origin	N/A
3	2	China	7%	11%	-4%
4	4	United Kingdom	3%	3%	No Change
5	9	Taiwan	3%	Not listed in the top five regions of phish origin	N/A

A study of two sources "Global Web-hosting Companies" [1]and "Internet World Users"[2] provide some insight into the behavior of phishing for the countries mentioned in the chart. Two sets of statistics "leading Web hosting companies having maximum users" and "the countries with most Internet users" were examined. By correlating these we find that the USA, China, Japan, India, Germany, France, UK, South Korea are amongst the leading countries with most internet users.

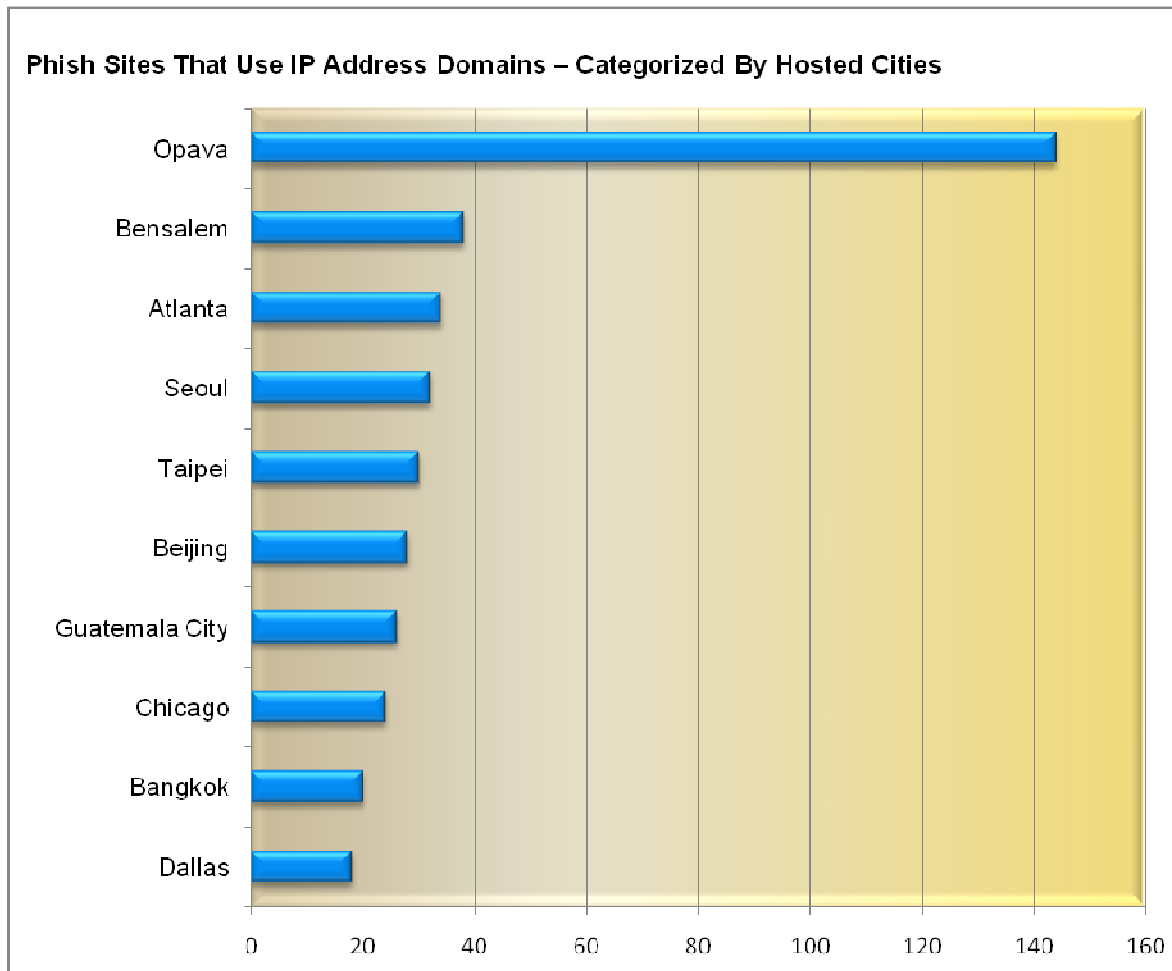Phish Sites That Use IP Address Domains – Categorized By Hosted Cities

Among the fraud attacks using IP addresses, the countries hosting phishing sites were further narrowed down to locate their city of origin. For the month of May a couple of new cities featured in this category. The top cities hosting the phish sites were Opava, Bensalem and Atlanta. The Czech Republican city of Opava which never appeared as a city hosting phish sites using IP addresses was the topmost city in the month, with a large number of phish sites originating from this region. Likewise, the city of Bensalem in the Pennsylvanian state of United States had previously never featured in this section. Guatemala City, the capital city of Republic of Guatemala was another new entrant in the top cities hosting phish sites with IP addresses.

Confidence in a connected world

symantec.

Phish Sites That Use IP Address Domains – Categorized By Hosted Cities

City	Value
Opava	~143
Bensalem	~38
Atlanta	~35
Seoul	~32
Taipei	~30
Beijing	~28
Guatemala City	~26
Chicago	~24
Bangkok	~20
Dallas	~18

Use of Web-Hosting Sites

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

> 113 Web hosting services were used with 1,794 Web sites for hosting phish pages.
> More than 67 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. These types of attacks are also suspended without much delay once they have been reported by end users as fraud. This makes it a less preferred method for professional attackers.

Confidence in a connected world

symantec.

Geo-Location 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 utilized to lure victims to the phishing Web hosts.

1. *Global Distribution of Active Phishing Lures*

Geo-locations were evaluated based upon unique URLs of active phishing sites. The top countries were found to be the USA (34%), United Kingdom (5%) and South Korea (5%). The proportion of active phishing lures was more evenly distributed for the rest of the locations. It is interesting to observe this newly evolving trend as was seen in the previous month as well.
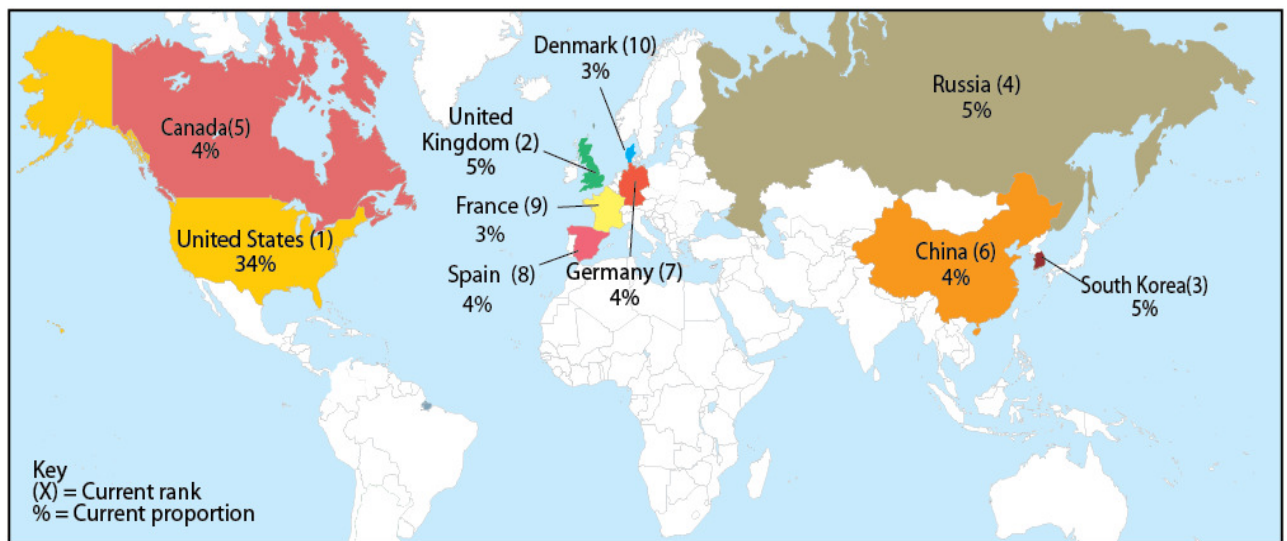
2. Global Distribution of Phishing Web Hosts

The Web hosts IPs for active phishing sites were analyzed to determine their geo-locations. The top countries are the USA (42%), Romania (5%) and Russia (5%). Similar to the distribution of active phishing lures, the proportion of the phishing Web hosts to some degree was evenly distributed over the rest of the locations.
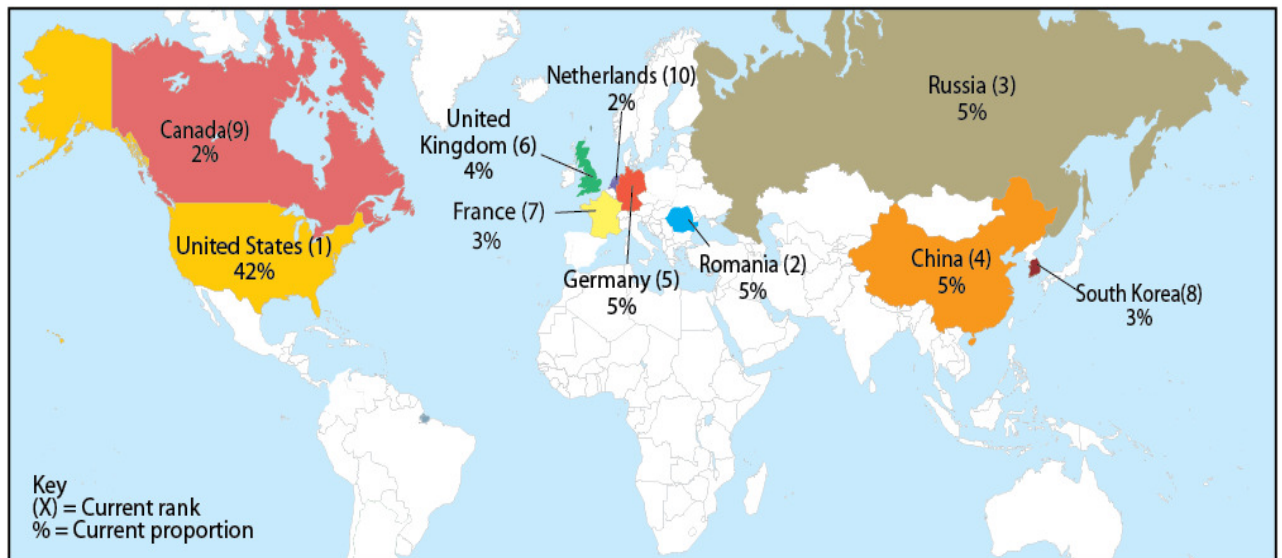
✸ symantec.

Non-English Phishing Sites
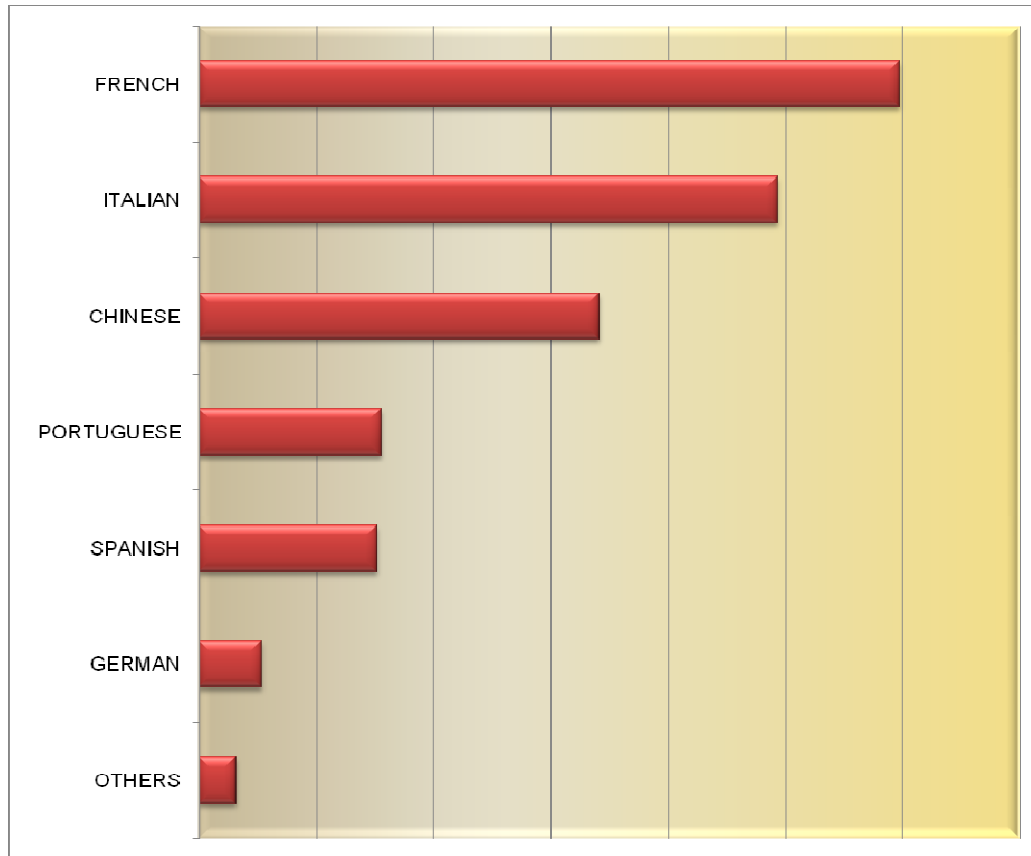
Phishing attacks in French, Italian and Chinese language were evaluated to be higher in May. French language attacks overtook attacks in Italian language to reach the top position. Symantec observed that phishing Web sites in French language were more than the usual level for a popular brand that resulted in the variation this month. French and Italian language phishing sites were mainly from the Financial sector, while Chinese language phishing sites were from the E-Commerce sector. By correlating statistics on Internet users worldwide[3] and the top global financial brands[4] and limiting them to non-English phishing sites, we obtained some significant figures. The Internet usage in France is nearly 35 million, Italy approximately 33 million, China approximately 253 million and 50 million in Brazil. These countries represent a fairly large population of non-English Internet users who are customers to large financial companies. This provides significant evidence to find more phishing attacks in these languages.

---

[3] http://www.internetworldstats.com/stats.htm
[4] http://www.forbes.com/lists/2008/18/biz_2000global08_The-Global-2000_Rank.html

symantec.

Top-Level Domains of Phishing Sites

Overall TLDs
Phishing URLs were categorized based on the Top-Level Domains (TLD). The most used TLDs in phishing sites this month are .com, .net and .org comprising of (50%), (9%) and (5%) respectively.
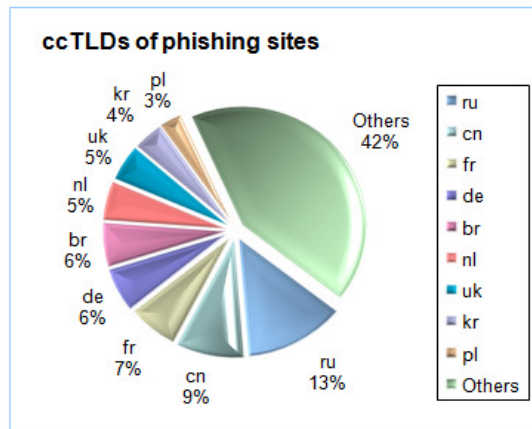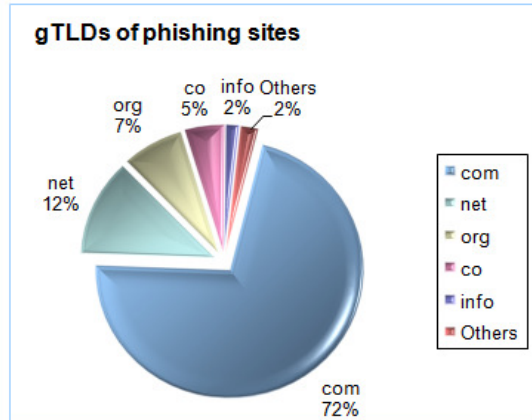
The Top-Level Domains in phishing were *further* categorized:

1. Generic Top-Level Domains (gTLDs)
The generic TLDs .com, .net and .org were the most utilized with (72%), (12%) and (7%) of the total phish attacks respectively.
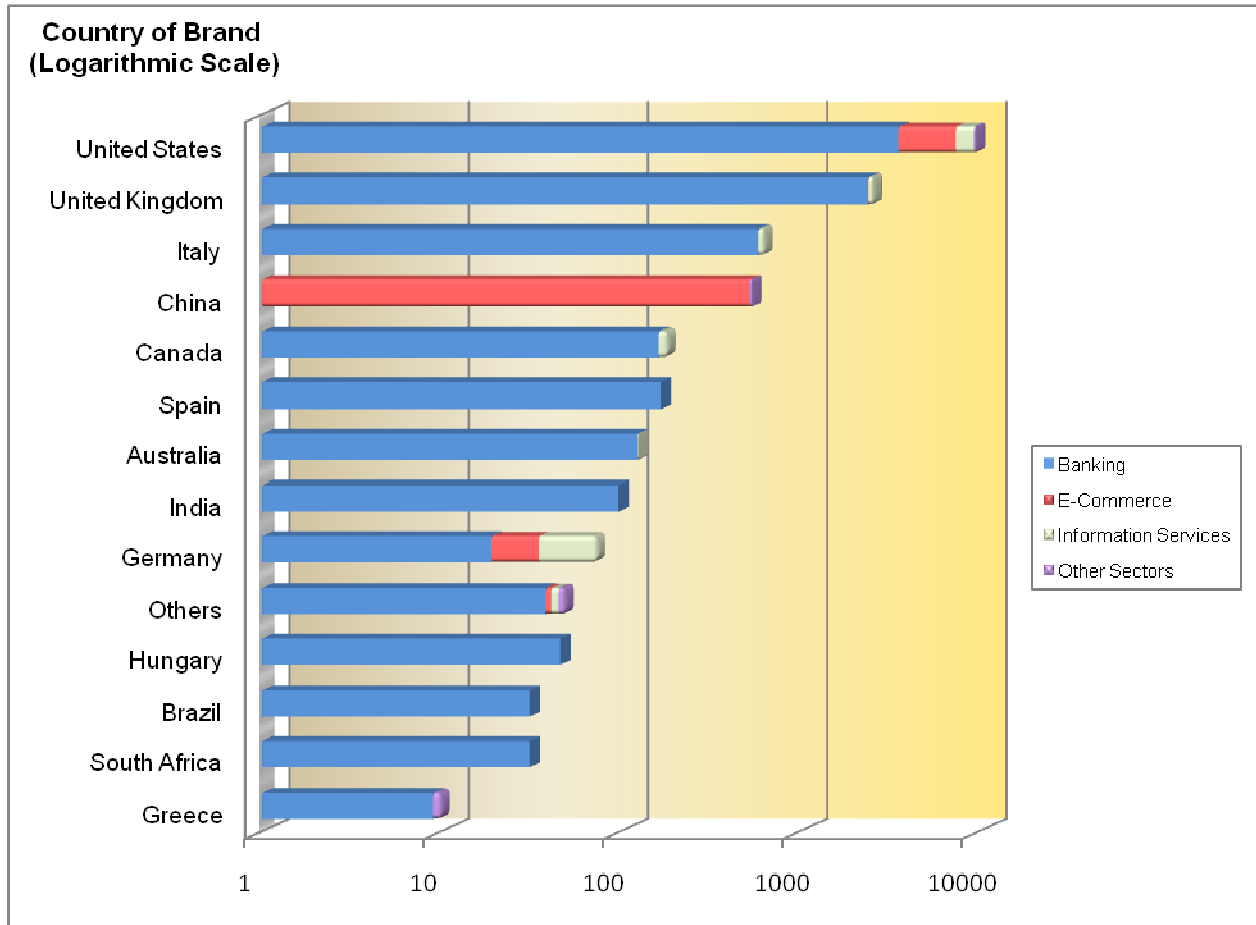
2. Country Code Top-Level Domains (ccTLDs)
The Russian, Chinese and French ccTLDs were evaluated to be the highest in phishing attacks with (13%), (9%) and (7%) respectively.

Confidence in a connected world

symantec.

TLDs of phishing sites

Legend:
- com
- net
- org
- ru
- cn
- fr
- de
- Others

Others 25%

de 2%
fr 2%
cn 3%
ru 5%
org 5%
net 9%
com 50%

gTLDs of phishing sites

org 7%
co 5%
info 2%
Others 2%
net 12%
com 72%

Legend:
- com
- net
- org
- co
- info
- Others

ccTLDs of phishing sites

kr 4%
pl 3%
uk 5%
nl 5%
br 6%
de 6%
fr 7%
cn 9%
ru 13%
Others 42%

Legend:
- ru
- cn
- fr
- de
- br
- nl
- uk
- kr
- pl
- Others

Confidence in a connected world

symantec.

Country of Brand

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 are the USA, UK and Italy. There were 27 countries whose brands were attacked. Sectors being targeted are similar throughout the countries of brands except for those belonging to Germany and China. There was a combination of Banking, E-Commerce and Information Services sectors in Germany. In the case of China, the E-Commerce sector has been a primary target. There was an increase observed in the Banking sector brands belonging to India.

Confidence in a connected world

symantec.

Glossary

- 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.

- A 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 un-sponsored Top-Level Domains (uTLD), e.g. .biz, .info, .name and .pro.

Confidence in a connected world

symantec.