The State of Phishing

A Monthly Report – October 2007

Compiled by Symantec Security Response Anti-Fraud Team

Prabhat K Singh
Director, Development, Security Response

Shankar Jayaraman
Manager, Development, Security Response

Sainarayan Nambiar
Supervisor, Security Response

Mathew Maniyara
Sr. Antifraud Analyst, Security Response

David Cowings
Sr. Manager of Operations, Security Response

Pamela Reese
Manager, Public Relations
Pamela_Reese@symantec.com

Contributors

Zahid Raza
Antifraud Analyst, Security Response

Rohan Shah
Antifraud Analyst, Security Response

Ashish Diwakar
Antifraud Analyst, Security Response

Ashutosh Raut
Antifraud Analyst, Security Response

1.0 Phishing Trends

The data in this report is aggregated from a combination of sources including the Symantec phish report network (PRN), strategic Symantec partners, Symantec customers and Symantec security solutions.

This report discusses the metrics and trends observed in phishing activity during the month of October 2007.

2.0 Phishing Highlights

The main highlights for the reporting period:

- The financial sector accounted for majority of the phish attacks which was at 84% of the total fraud activity observed during this period.
- A total of 17,507 unique phishing web sites were recorded. The count of unique sites has seen a drop of 5% in comparison to the previous month.
- There was an increase of 7.1% in *rock phishing* attacks from the previous month.
- A total of 2424 attacks used IP addresses instead of domain names in the URL field. This was an increase of 3.8% from the previous month.
- The month of October witnessed a drop in the use of free web hosting sites which have been used for hosting phish sites. A total of 2000 such sites were recorded in this month. This was a drop of 5.7% in comparison to the previous month.
- Among the non-english phishing sites- Italian language phish sites were most frequently recorded followed by sites in Chinese and Spanish.
- 421 domains, spoofing 26 brands, were used for mounting *typosquatting* attacks.

3.0 Phishing Discussion

October’s phishing sites were categorized and studied for understanding the attack methods involved and to determine the sectors and brands impacted by the attacks.

Following are the categories that were analyzed

- Sectors
- Number of Brands
- Rock Phish
- Fraud URLs with IP addresses
- Use of Web-hosting Sites
- Non-English Phishing Sites
- Look-alike Fraud Domains

3.1 Sectors

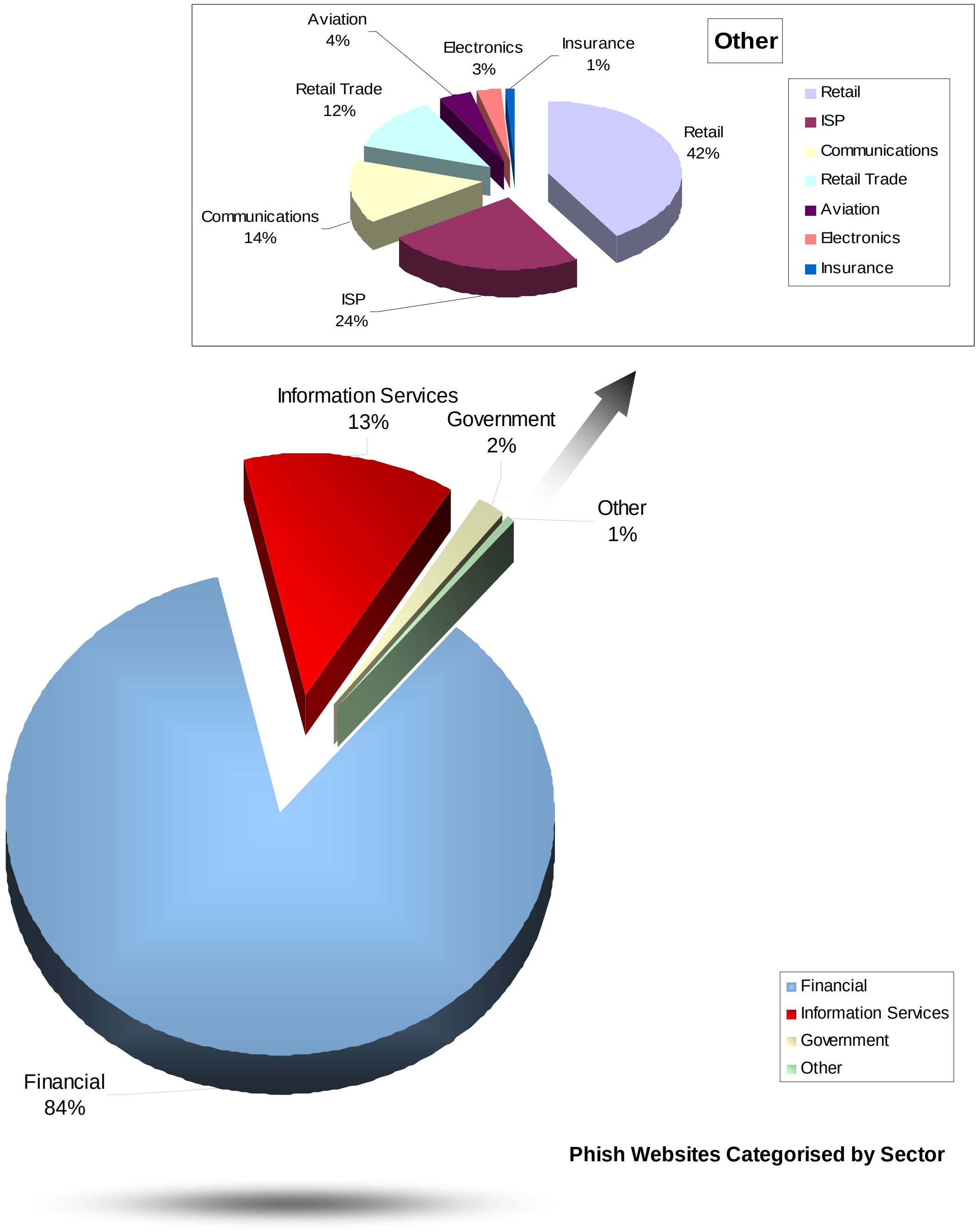
Phishing URLs were categorized based on the sector by evaluating the brands attacked by the phish websites.

The financial sector accounted for the majority of phish attacks which was at 84% of the total phishing URLs. Next in line was the information services sector at 13%.

Unlike the financial sector, most of the phishing attacks on the information services sector did not involve stealing user credentials for the purpose of money but probably for carrying out spam activity.

Phish web sites targeting the government sector was at 2% of the total fraud activity recorded. The primary purpose for attacking this sector was for stealing money through fraudulent tax refunds.

The remaining 1% includes a variety of sectors. They were- retail, ISP, communications, retail trade, aviation, electronics and insurance. Among these, retail and ISP formed the majority.



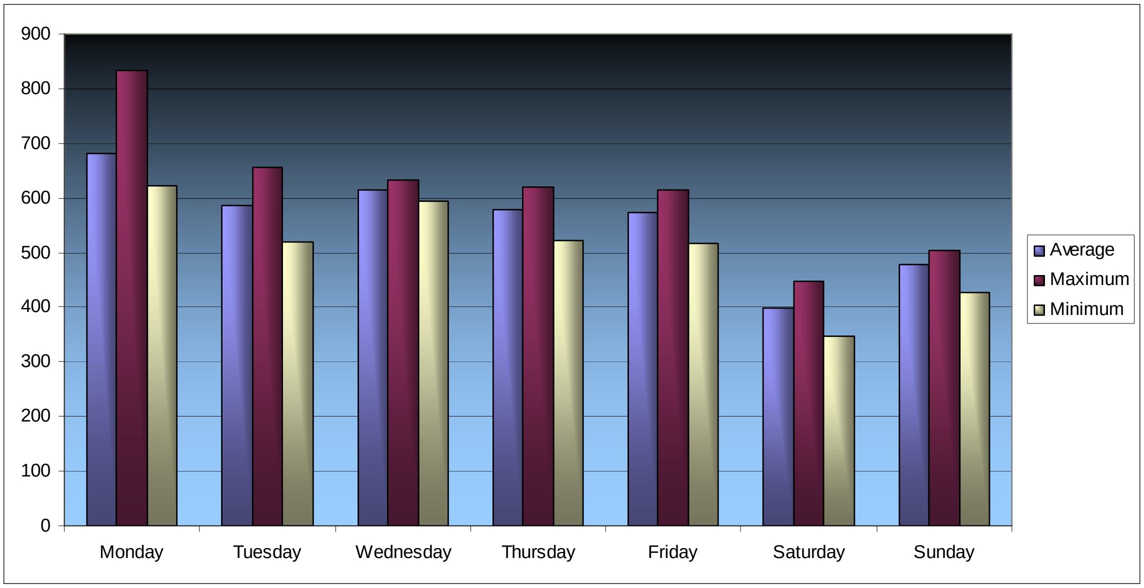
Phish Websites Categorised by Sector

3.2 Number of Brands

Symantec tracks the number of brands attacked by phishers. A total of 204 known brands were targeted by phishers in the reporting period of which,17507 unique phishing web sites were recorded.

The number of unique phish sites reduced by 5% (Approx.) in comparison to the previous month.

Phishing behavior was also monitored for weekly activity based on the days of the week. Mondays and Tuesdays had the most unique attacks; 17.42% and 15% respectively. On weekends, phishers are probably attacking lesser as fewer people access their mails. Statistics show that Saturdays and Sundays witnessed the minimum with 10.17% and 12.24% respectively.

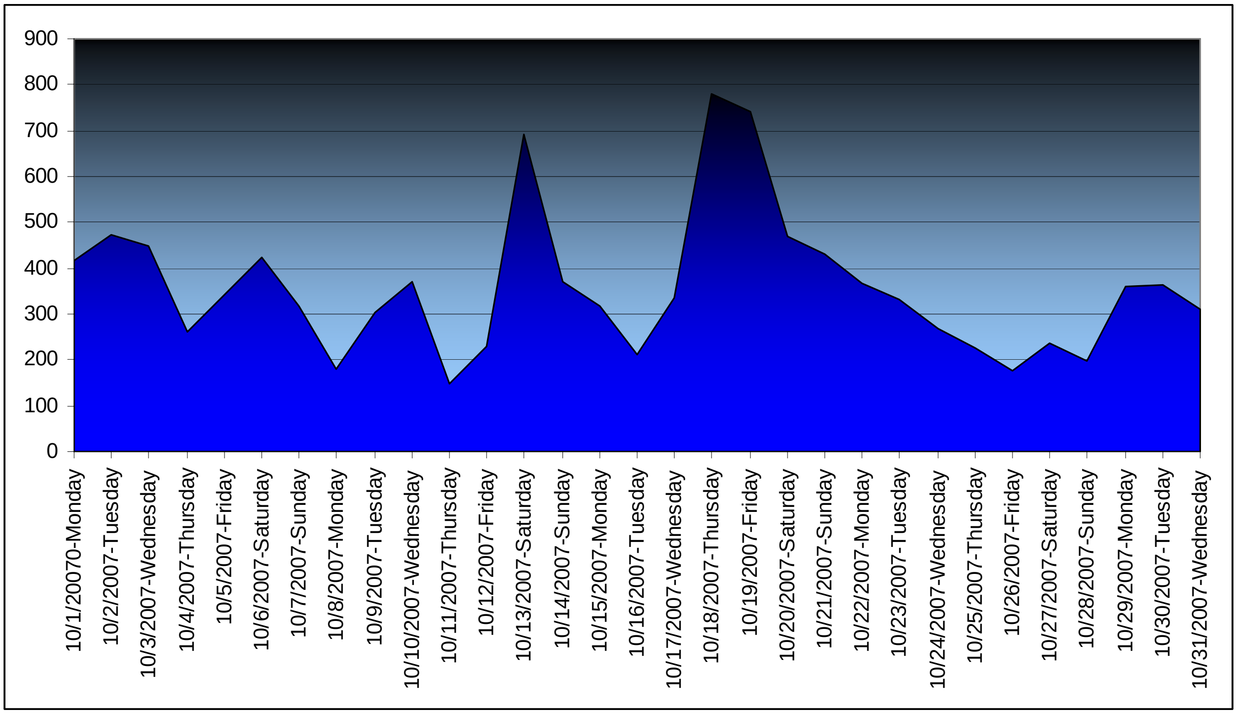


3.2 Rock Phish

Rock phish is a term used for websites that are created by a phishing toolkit which can be widely used for carrying out large attacks on brands and can be used by individuals who are not very technical. This attack goes on in the following way:
A large number of unique domains is created by randomizing a sub-domain within the URL in extensive numbers. Many of today's anti-phishing technologies employ a predefined black list which would contain known phishing URLs. If the site is found in the list then the anti-phish toolbar will give a warning. As rock phish attacks are delivered with such an extreme level of randomization, all URL variants may not be available in these toolbars thus allowing the phishers to evade detection.

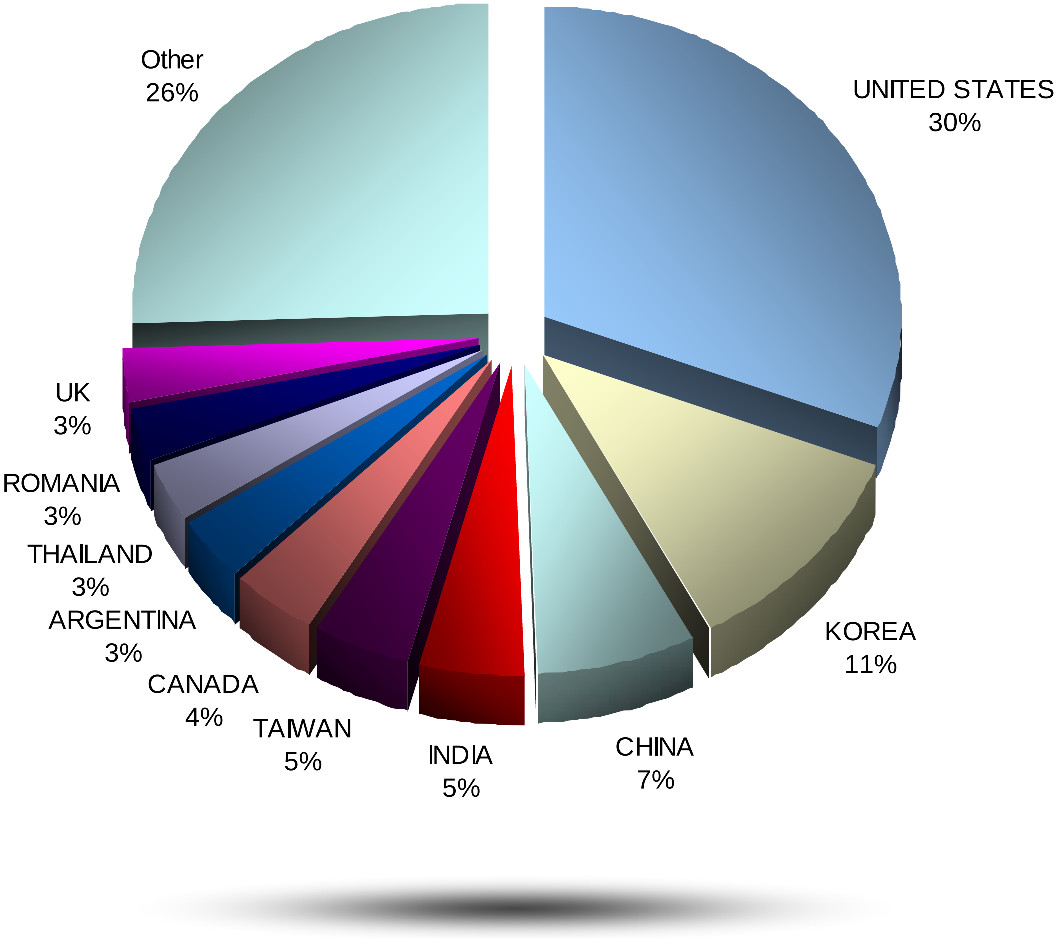
Over 11,000 rock phish URLs were found in the month. This is an increase of 7.1% of the stats from the previous month.

Weekly behavior of Rock Phish:



3.3 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 which, 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.



A total of 2424 phish sites were hosted in 75 countries which accounts for an increase of 3.8% of attacks in comparison to the previous month.

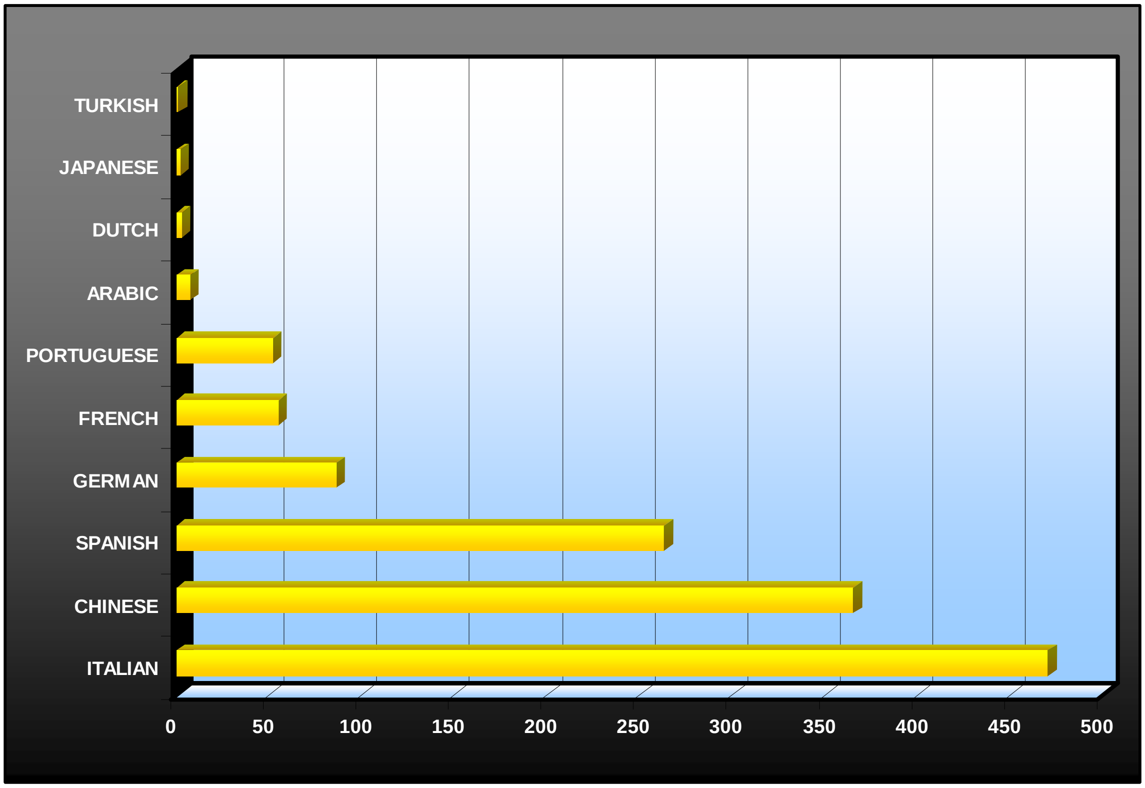
Current Rank	Previous mo	Country	Percentage of Attack	Previous month
1	1	UNITED STATES	31%	34%
2	2	KOREA, REPUBLIC OF	11%	8%
3	3	CHINA	7%	7%
4	7	INDIA	5%	4%
5	9	TAIWAN	5%	3%

3.5 Use of Web Hosting Sites

Usage of free web-hosting services for creating fake web sites has been the easiest form of phishing. More than 110 web hosting services were used for hosting phish pages for the purpose of attacking over 60 brands in the reporting period.

Over 2000 sites were detected but this is a drop than the previous month's record by 5.7%.

3.6 Non-English Phishing Sites



3.7 Look-alike Fraud Domain Names (Typosquatting)

A total 421 domains were recorded that spoofed 26 domains.

4.0 Conclusion

The majority of phishing attacks are targeting the financial sector. The attacks are not concentrated on the big brands alone but phishers are choosing smaller, less known brands as well. The reason for such a case may be due to declining success rates in phishing the big brands. Highly reputable brands are capable of devoting more resources towards educating their customers as well as taking down phish sites and so attackers are going for smaller brands to steal more identities.

The trend shows that attackers have consistently lower volumes of unique attacks on weekends. The recent stats show an increase in Chinese phishing sites in addition to the increase in Italian phishing sites.

There is an increase in typosquatting based attacks. At times this becomes a very confusing scenario for customers as a fake domain name looks very similar to the original one and may also be types in accidentally by users. Phishers today might be gaining more success in this area which possibly explains the increase in such domain names. The large increase in registrars allowing the purchase of domains without credential validation as well as some registrars allowing the trial use of domains are likely major contributors to this trend.