

# RSA Online Fraud Report

February, 2008

## A Monthly Report from the RSA Anti-Fraud Command Center Phishing Repository

Online fraud is evolving. Phishing and pharming represent one of the most sophisticated, organized and innovative technological crime waves faced by online businesses.

Fraudsters have new tools at their disposal; and are able to adapt more rapidly than ever.

The RSA Anti-Fraud Command Center (AFCC) is a 24x7 war-room that detects, monitors, tracks and shuts down phishing, pharming and Trojan attacks against more than 200 institutions worldwide. The AFCC has shut down over 42,000 phishing attacks and is a key industry source for information on phishing and emerging online threats.

The following statistics have been gathered from the AFCC's phishing repository. Each statistic includes a short analysis of the trends shown in the graphs based on the expertise of the fraud analysts in the command center.

---

### This Month: Insight into recent phishing trends

---

In this month's edition, RSA reports on several developments with phishing sites and networks. These new reported developments are small innovations and adaptations that have recently grown in numbers, as fraudsters try to avoid phishing site detection and make their sites harder to analyze and shut down.

#### New developments in Botnet and Fast-Flux phishing

In the December edition of the Phishing News we reported on an increase in "Rock-like", or Botnet-based, phishing attacks. This was a trend that we expected to see during 2008. Since then, our prediction has become a reality, as we continue to see a growing number of phishing groups or networks that utilize Botnets of proxies and Fast-Flux techniques.

Over the past four months the RSA Anti-Fraud Command Center identified five new phishing networks that rely on hijacked proxies, some of which were Fast-Flux networks. These new networks, or phishing groups attack financial institutions worldwide. The most infamous was the Storm Botnet, which fraudsters are now using to host phishing attacks, but other networks were detected as well. We expect this trend to continue and the number of Fast-Flux attacks to increase during 2008.



The Security Division of EMC



### Obfuscated/encoded phishing kits

Obfuscated phishing kits, where PHP scripts are decoded, are not a new phenomenon. However, during January and February we noticed an increase in the usage of such kits. Like most phishing kits, these kits contain mostly PHP scripts. When the kits are examined, the PHP source code is unreadable and obfuscated because it has been encoded. The kit cannot be analyzed without decoding the PHP source code. Decoding these kits is possible, but it requires a certain effort by security experts. Unless decoded, these kits cause some difficulties for researchers such as:

- Drop email accounts cannot be detected
- Drop file names where credentials are stored cannot be detected
- Web sites which the kit communicates with, such as real bank web sites in Man-in-the-Middle attacks, are also obfuscated in the kit

### The use of “multiple versions” of the same URL

During the past few months we have detected an increasing number of attacks that use multiple variations of the same spammed URL. Fraudsters do not send an exact copy of the phishing URL in each phishing email, but instead use several variations of this URL. In fact, the spammed URLs for a single attack can look almost the same, but contain a minor variation, which is demonstrated by a single digit or “serial number”, within the URL.

Note that in the example below, the URLs refer to the same attack which is hosted on the main domain, and therefore the exact URL itself doesn't matter. In this case all the victims connect to the same domain and therefore and the same attack regardless of the spammed URL.

The fact that fraudsters use multiple URLs to direct to the same attack is not new, and this technique is widely used in order to avoid spam filters and create “personalized” phishing messages. However, we are now seeing an increased use of this specific URL “multiplication” format. We estimate that the number within the URL makes it just slightly different than the previously spammed URLs in an effort to avoid anti-spam filters. Spam filters can identify patterns of phishing URLs, among other spam messages, and would block all email messages carrying a familiar pattern. The slight change in the URL makes it “unfamiliar” to these filters, and it takes time until anti-spam systems learn the new format.

The slight difference in the URL's allow the attacker to create “personalized” messages and work around spam filters while still leading the victim to the same attack.

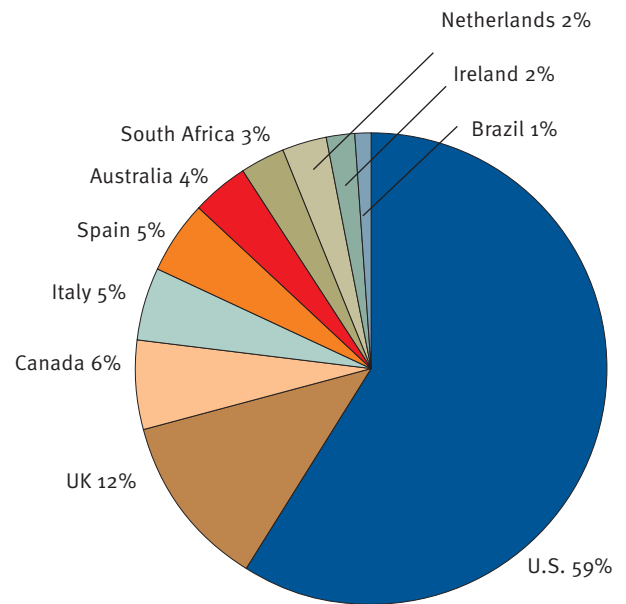
```
http://www.phish-domain.com/2004/en/abc/update/1/Bank/ibc.php?logon=logon  
http://www.phish-domain.com/2004/en/abc/update/2/Bank/ibc.php?logon=logon  
http://www.phish-domain.com/2004/en/abc/update/3/Bank/ibc.php?logon=logon  
http://www.phish-domain.com/2004/en/abc/update/4/Bank/ibc.php?logon=logon  
http://www.phish-domain.com/2004/en/abc/update/5/Bank/ibc.php?logon=logon  
http://www.phish-domain.com/2004/en/abc/update/6/Bank/ibc.php?logon=logon
```



## 1. Breakdown of Global Banking Brands Attacked by Phishing

### Trend Analysis

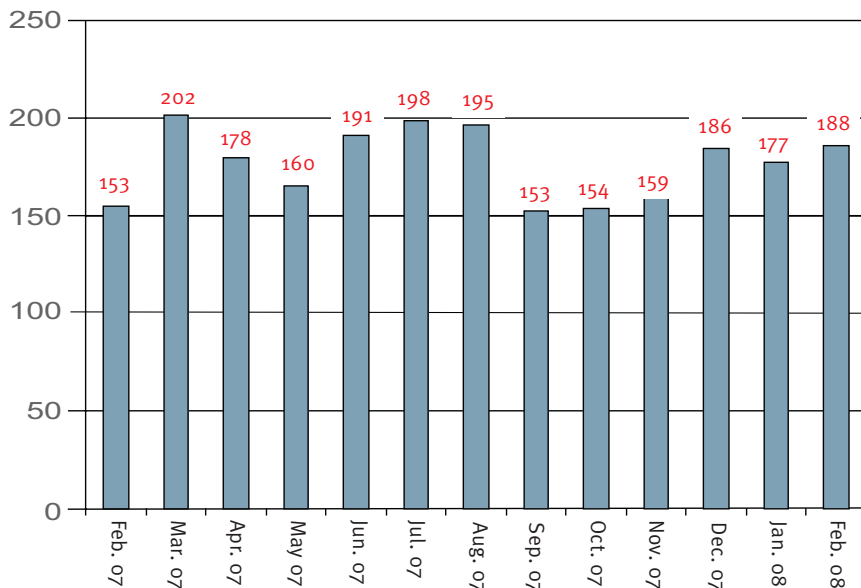
The distribution of attacked entities has remained relatively constant since June 2007. The U.S. brands are the most dominant, and it is now thirteen consecutive months during which UK institutions occupy the second spot, with 12% of the phished entities. New to the list are institutions from Ireland and Brazil. This is consistent with the recent trend in the past few months of South American countries making the list.



## 2. Number of Brands Attacked Per Month

### Trend Analysis

The number of attacked brands grew during February. This number is still lower when compared to certain record months of 2007 including: March, June, July and August. In February 2008, the RSA Anti-Fraud Command Center detected attacks against almost 20 financial institutions that it had not previously seen attacked. This is a consistent trend over the past four months.

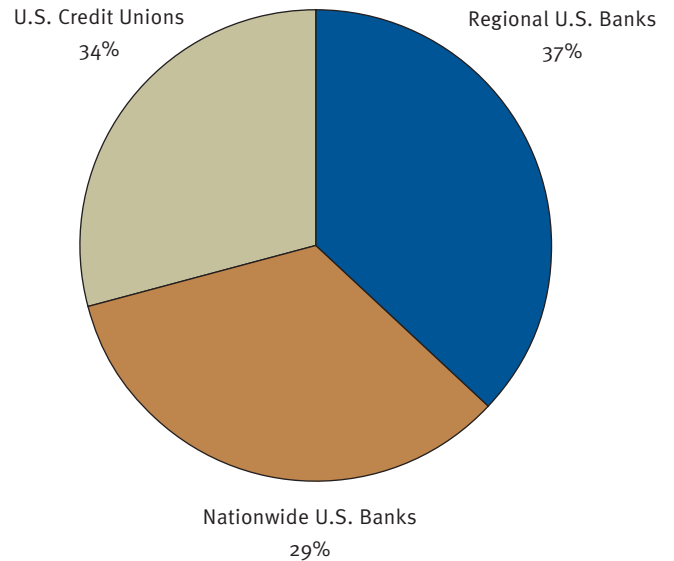




### 3. Segmentation of U.S. Banking Brands Attacked by Phishing

#### Trend Analysis

The distribution of attacked U.S. financial institutions by type was almost even in February. Each sector constitutes about one third of the attacked U.S. entities, with the regional banks sector being slightly more dominant. This is a unique situation, as in previous months RSA noted more differences in the percentage of attacks distributed between the three sectors. The share of nationwide banks has been quite steady over the last three months, at about 30% since December 2007.



### 4. Top Hosting Countries

The U.S. leads the list of Top Hosted Countries by a significant margin. Hong Kong, which ranked second in January with 9% of the attacks dropped to 6th place; while the rates for Germany and South Korea slightly increased. Rock Phish domains usually affect Hong Kong records; however fewer Rock Phish domains were registered in Hong Kong during February. The Philippines, which hosted a large amount of Rock Phish domains back in December, has not made the list in the last two months.

