

RSA Online Fraud Report

March, 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 ever faced by 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. To date, the AFCC has shut down over 80,000 phishing attacks in more than 185 different countries. In 2007 alone, the AFCC shut down more than 39,000 attacks for more than 260 customers 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: The Rock Phish Spam e-Mails

The notorious Rock Phish gang is a group of cyber criminals responsible for extremely large volumes of phishing scams. It is estimated that Rock Phish is accountable for over 50% of all phishing attacks worldwide, and the group is believed to have skimmed tens of millions of dollars from the bank accounts of unsuspecting victims. A large number of financial institutions are targeted by Rock Phish, including some of the world's leading banks.

Each time the Rock Phish gang advertises a new phishing website, the website receives a massive amount of hits, and usually many more than we would expect to see in a standard phishing attack. So how can we explain the high volume of activity on Rock Phish sites? One of the reasons may be the techniques they use to send their phishing e-mails.

The Rock Phish gang creates and sends spam e-mails using some interesting features that enable them to avoid detection. The gang uses "hash busters" to send phishing e-mails and – in addition – it deploys a Botnet to relay phishing e-mails.



The Security Division of EMC



What exactly is a Hash Buster?

Hash busting is a technique used to add random text to each e-mail message in order to create unique messages, and as a result, a unique hash for each message sent. This random text is added as hidden content to the phishing e-mail, making it difficult for anti-spam filters to qualify the e-mail as spam.

Most anti-spam tools work as follows: when a spam e-mail is detected, the message hash is calculated. When a similar e-mail is analyzed by the anti-spam filter, it will be blocked. It happens because both e-mails have the same hash value. The random text, which is hidden in these Rock Phish spam e-mails, makes them unique and thus enables these e-mails to bypass most anti-spam filters. For example, the following boxed text was extracted from one of the e-mails:

```
cvs: 0x7457, 0x5, 0x8758, 0x9019, 0x7, 0x697,  
0x17916501, 0x949, 0x80,0x030, 0x598, 0x97266747  
NCE TP6 X81P RH2E exe SGo include V8PW root api:  
0x17, 0x2879 JN9: 0x50270054, 0x28850104, 0x316,  
0x935, 0x01339377, 0x64, 0x0, 0x1658, 0x26765770,  
0x091, 0x162 BB4B: 0x9, 0x04, 0x1745, 0x0, 0x9597,  
0x33, 0x25692116, 0x58826863, 0x536, 0x9200,  
0x8236, 0x1759 EXJ: 0x1, 0x343, 0x88, 0x4917, 0x33,  
0x84363121, 0x2 0x502, 0x6163, 0x460, 0x783, 0x6,  
0x7, 0x805, 0x94, 0x343, 0x2, 0x2, 0x85653112  
0x671, 0x5, 0x67064212, 0x3, 0x01452899, 0x9, 0x6,  
0x4, 0x6, 0x9835, 0x94660375, 0x9 0x3181, 0x97,  
0x7700
```

In addition to adding random text in the e-mail content, the Rock Phish gang uses random sub-domain names within the phishing URLs. The random sub-domains have the same affect on many anti-spam filters, making them unable to qualify these Rock Phish messages as spam.

The Rock Spam Botnet

Additional research performed by the RSA FraudAction Anti-Trojan team showed that the Rock Phish gang infiltrates personal computers and installs a spam bot. These computers are then used as a relay to send e-mails. The spam bots contain built-in functionality that sends fake phishing e-mails to a victim's contact list. This way, the Rock Phish gang can send e-mails to an active list of users.

This spam bot was found in some YouTube phishing scams in 2007. You can find some public information here: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=818>.

Note that the Rock spam bot is not the same bot which is used to deliver Rock phishing content to the user via a proxy.

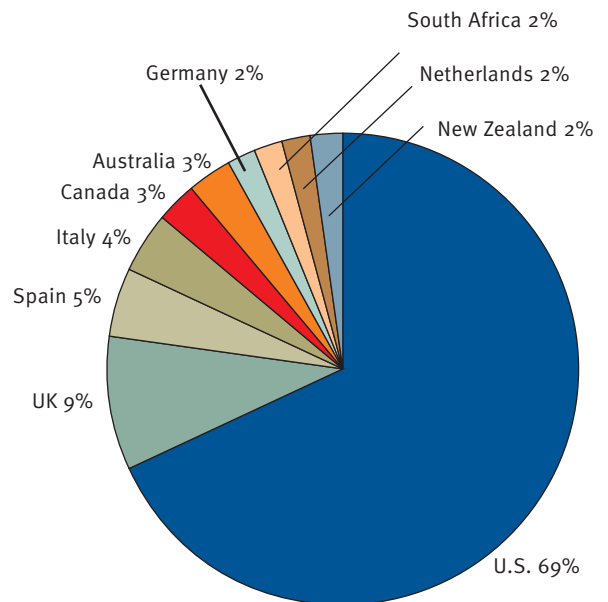
In summary, while these techniques are not at all new, by working in combination they can succeed in infiltrating thousands of mail servers and ultimately find a way to a user's inbox. This is why the Rock Phish gang receives such a massive number of hits to their phishing sites.



1. Breakdown of Global Banking Brands Attacked by Phishing

Trend Analysis

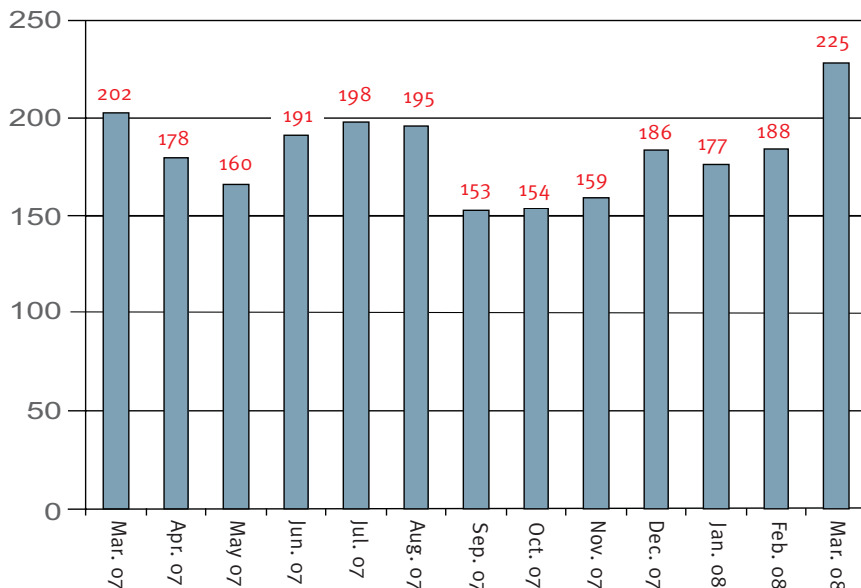
The distribution of attacked entities remained relatively similar to that of previous months. U.S. brands continue to be the most attacked, followed by UK brands for the 14th consecutive month. Most notable this month is that, as phishing increases in the Asia-Pacific region, both Australia and New Zealand make the list.



2. Number of Brands Attacked Per Month

Trend Analysis

The number of attacked brands grew quite dramatically in March. Similarly to the total phishing attacks indicator, March saw an all-time record in terms of the number of targeted institutions – an increase of 23 on March 2007. This record high was influenced by the spread of phishing to additional geographic regions and new verticals. In March 2008, the RSA Anti-Fraud Command Center detected attacks against 16 financial institutions that it had not seen attacked before.

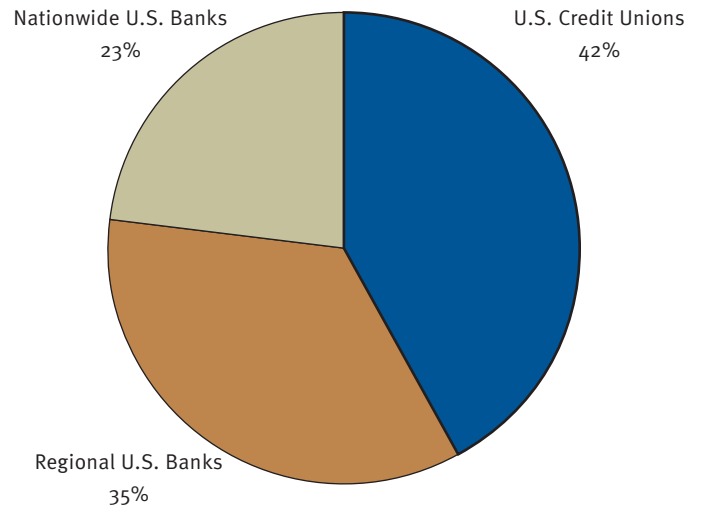




3. Segmentation of U.S. Banking Brands Attacked by Phishing

Trend Analysis

The distribution of attacked U.S. banking entities changed this month. The share belonging to nationwide banks, which has held steady since December 2007 at approximately 30%, fell to 23% in March. Regional banks and Credit Unions accounted for around one third of the attacked entities in February, and this also evolved in our latest numbers. It is fair to say that the share and distribution of these numbers have been very unstable over the past year.



4. Top Hosting Countries

Trend Analysis

Similarly to the last three months, the U.S. is top of the list and has maintained a consistent percentage of hosted attacks. Germany, South Korea and the UK occupy the following three positions, as we also observed in February. Germany's second place position is largely a result of Rock Phish and Fast-Flux domains which were registered in Germany during the month. Other notables: Canada and Hong Kong – typically regulars on the list – were absent in March, while the Netherlands and Italy took their places.

