

RSA Online Fraud Report

May, 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 275 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 280 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: New Malware Attacks by the Rock Phish Gang

The notorious Rock Phish gang is a group of cyber criminals that is responsible for extremely large volumes of phishing scams. It is estimated that the gang's activities account 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 have been targeted by the Rock Phish gang, including some of the world's leading banks.

RSA recently reported that the Rock Phish gang had introduced a new type of attack, which combined a standard phishing attack with a Trojan attack. Victims of these attacks were subsequently infected with the Zeus Trojan. In April, the RSA Anti-Fraud Command Center detected yet another Rock Phish attack variant that also aims to infect victims with a Trojan - although this time with a new and unfamiliar Trojan.

The Rock Phish attacks containing the new Trojan were aimed at business account holders at several financial institutions. Victims of these phishing attacks were duped into downloading a Trojan which infected their computers when they visited the last page of the Rock Phish scam. Some social engineering text on this final page was designed to convince the victim, who had already fallen for the phishing attack, to download a "certificate" file which would update their computer. The subterfuge was that the



The Security Division of EMC

certificate would supposedly enable the user to successfully access his/her online banking account in the future. Upon clicking the certificate installation button within the phishing site, the following message appeared:



The crimeware delivered by these attacks

As stated, the targets of these attacks were mostly business account holders. The crimeware deployed in the attacks is likely to have had relatively limited, but well-targeted exposure due to this specific "manual" infection vector.

In other Trojan attacks, such as the massive Zeus attacks, we see that fraudsters go to many lengths to achieve the maximal exposure and infection rate. This is achieved using sophisticated infection and drive-by-download kits such as the IcePack, FirePack and MPack. Such massive Trojan attacks will often result in a large pool of infected computers, but the value of these victims for the fraudster varies, and it is hard to find the "high quality" data within this large pool of infected machines.

Information we collected on the new Trojan attack detailed above indicates that the Trojan also targets customers of additional financial institutions, other than the ones which were targeted by the phishing attacks. It is unclear whether the fraudsters who operate this Trojan use infection vectors other than the phishing attacks, and what these vectors may be (e.g. drive-by-download).

The "certificate crimeware", which currently remains nameless, has just a few hard-coded triggers which are visible upon infection. However, at the back-end the fraudsters are capable of further extracting information and filtering it as it arrives at the drop point. This can be achieved because the crimeware records all SSL-encrypted traffic which is generated by the infected victim. It is also interesting to note that the fraudsters capture ICQ usernames & passwords, and FTP credentials. Like most crimeware, it can also perform HTML injection and screen capturing.

The crimeware's communication with the mother ship is encrypted in order to protect itself from security researchers and reverse-engineering.

The Trojan's association to known groups

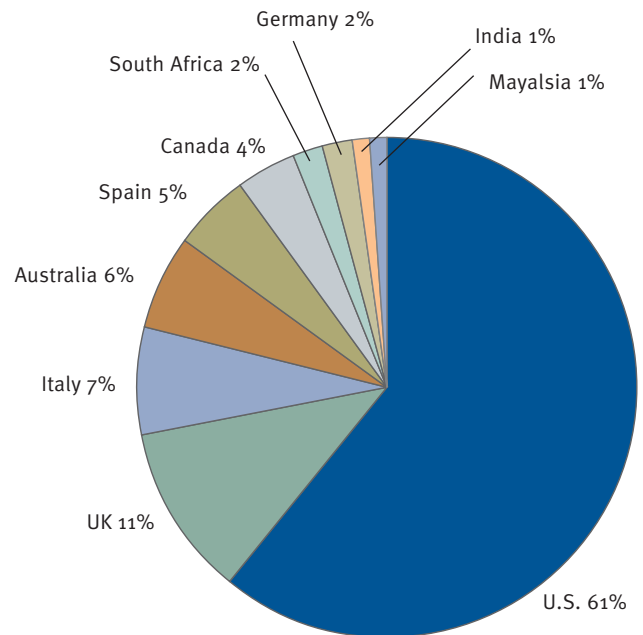
RSA had not seen this crimeware before, and has not seen it used by any other group. We believe it is the custom work of the Rock Phish gang, or that it is crimeware developed especially for the gang. Our data indicates that the Trojan's origin is Russian. It is NOT the Zeus Trojan or any other familiar Trojan, but a new Trojan which was recently introduced by the Rock Phish gang alone. In addition, the social engineering infection vector is one that had not previously been used by the Rock group.



1. Breakdown of Global Banking Brands Attacked by Phishing

Trend Analysis

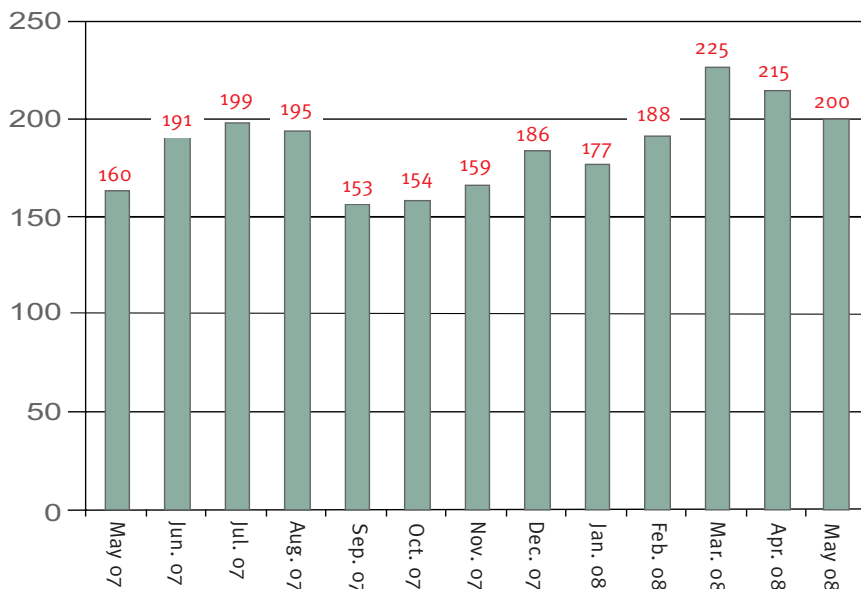
The distribution of attacked entities remained relatively similar to that of previous months. As usual, U.S. brands are dominant, followed by U.K. brands for the 16th consecutive month. The U.S. and U.K. attacked brands are followed as usual by brands from Spain, Italy, Canada and Australia - and also South Africa, which is becoming a regular member of this list. Malaysia and India represented the Asia-Pacific region in May, and we are seeing more institutions in these regions being attacked.



2. Number of Brands Attacked Per Month

Trend Analysis

The number of attacked brands decreased slightly for the second consecutive month, although the overall total remains high. In May 2008, the RSA Anti-Fraud Command Center detected attacks against 23 entities that it had not seen attacked before, a relatively low number when compared to last month when 30 new entities were detected.

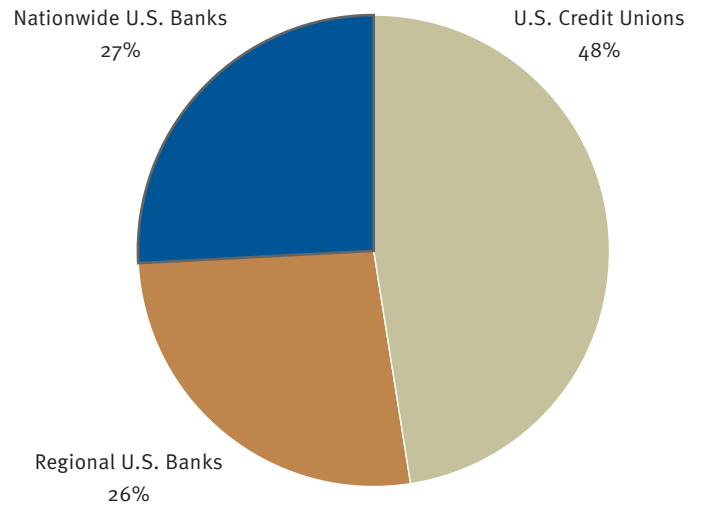




3. Segmentation of U.S. Banking Brands Attacked by Phishing

Trend Analysis

In May, almost half of the attacked U.S. financial entities were Federal Credit Unions. This is an extraordinary figure, and much higher than the typical percentage accounted for by this type of institution. The share of nationwide U.S. banks hardly changed in May, and the share of regional banks dropped from 36% in April to 26% in May. These figures do not indicate an obvious trend as they tend to change from one month to another.



4. Top Hosting Countries

Trend Analysis

The U.S. remains in first position for hosting the largest number of phishing attacks. China, despite its percentage dropping month-on-month from 19% to 11%, maintains the runner-up spot that it claimed in April. The UK, Germany, France, South Korea and Russia continue to host a similar monthly percentage of phishing attacks, and some interesting newcomers to this list in May were Afghanistan and Luxembourg, a result of the many Rock Phish and Fast-Flux domains that were registered in these countries during the month.

