

RSA Online Fraud Report

April, 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 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: "All-in-one" Zeus Trojan package for sale

Over the past few months RSA has witnessed an increased use of the Zeus Trojan (also known as "wsnpoem") in attacks against financial institutions worldwide. Zeus is extremely user-friendly and easy to operate. Fraudsters who execute Zeus attacks simply need to take control of a compromised server or have their own back-end servers; once they have a server in place, they merely need to install the Zeus administration panel, create a username and password – and start launching their attacks. The administration panel can easily be controlled by unsophisticated users.

Recently, we traced a new service which makes Zeus installation and the deployment of Zeus Trojan attacks even easier than before. Fraudsters in the underground are now offering access to an "all-in-one" solution – a bullet-proof hosting server with a built-in Zeus Trojan administration panel and infection tools.

Why is this interesting?

The usual process for deploying an attack involves several stages:

- Finding a reliable server that can support ongoing attacks and store credentials
- Purchasing the Zeus Trojan kit and installing the Zeus administration panel on the server
- Obtaining effective infection tools and spreading the Trojan



The Security Division of EMC



Fraudsters can now rent a service that provides them with a ready-made Zeus attack infrastructure. The service includes all of the required stages above in a single package, meaning that all the fraudster now has to do is pay for the service, access the newly-hired Zeus Trojan server, create infection points and start collecting data.

The Zeus administration panel which is installed on the servers is one of the latest versions. Moreover, such servers are also offered with advanced “exploit packages” that facilitate Zeus infections. The exploit package allows fraudsters to easily infect users and grow a Botnet of compromised machines. Thus, an entire Zeus attack comes alive, using a single service package that fraudsters can buy in the underground.

The “Zeus package” servers are also offered with a stable operating system and easy-to-use web hosting control panels which further facilitate the deployment of attacks. The simple hosting control panels can be used by virtually any fraudster. One of these hosting control panels is a commercial application which has recently gained some popularity among fraudsters. In addition, the servers have enough storage space to collect large amounts of stolen credentials. In this way, Trojan attacks launched by multiple groups, or a single attack which yields a large volume of results, can be supported.

The bottom line is that with such services, creating the infrastructure for Zeus attacks and actually implementing these attacks is now easier than ever before.

About the Zeus Trojan

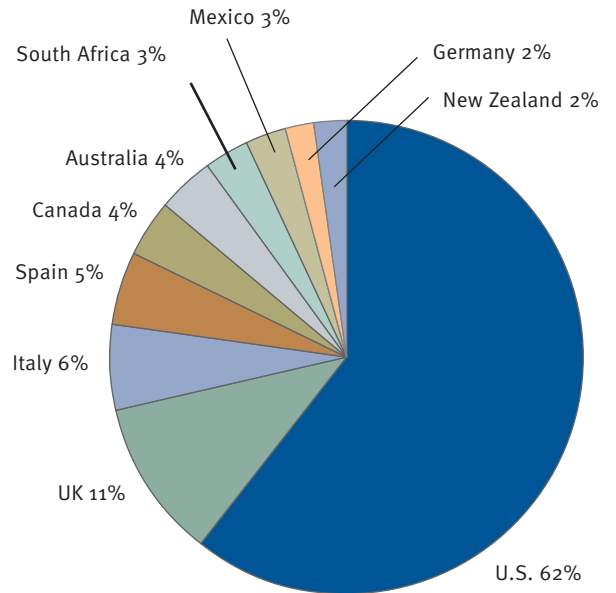
The Zeus Trojan is considered the latest step in the evolution of a family of financial crimeware that began with the notorious Limbo Trojan. Limbo, and its successor Zeus, are designed to perform advanced key logging when infected users access specific web pages, including pages which are protected by SSL protocols. Zeus is also equipped with impressive self-protection mechanisms and encryption: Zeus’ entire communication is encrypted, and the information it collects is encrypted when it is sent to the drop point. In comparison with other common Trojans, such as the Limbo and Snatch variants, Zeus utilizes a type of encryption which is much harder to deal with. One of the latest variants of the Zeus Trojan even communicates with its Internet resources over SSL encryption.



1. Breakdown of Global Banking Brands Attacked by Phishing

Trend Analysis

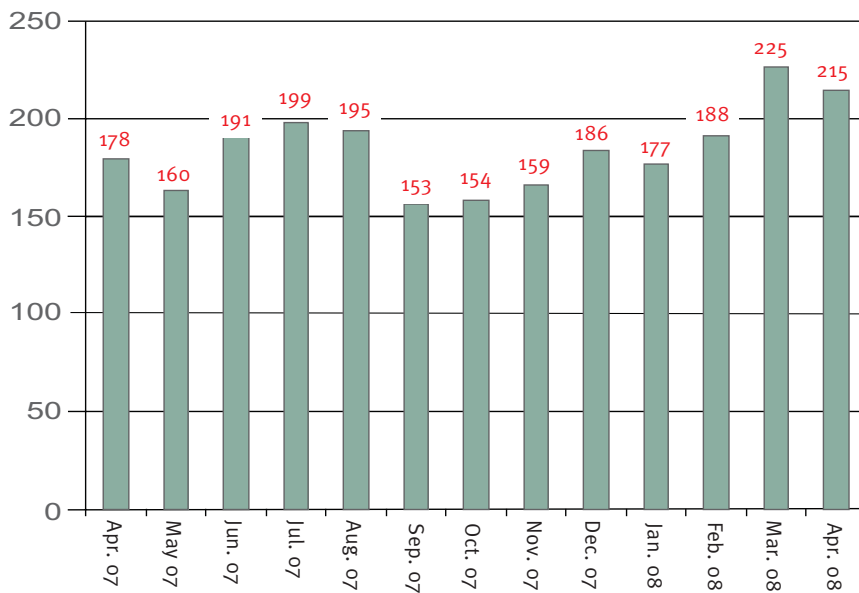
The distribution of attacked entities remained relatively similar to that of previous months. As usual, U.S. brands continue to dominate, followed by UK brands for the 15th consecutive month. These are followed, as usual, by Spain, Italy and Canada. Note that as phishing increasingly spreads into the Asia-Pacific region, both Australia and New Zealand made the list in both March and April.



2. Number of Brands Attacked Per Month

Trend Analysis

Despite a further rise in the number of phishing attacks, the number of attacked brands decreased slightly during April. However, even with this decrease, April still saw the second highest number of phished brands in the last year. In April 2008, the RSA Anti-Fraud Command Center detected attacks against more than 30 entities that it had not seen attacked before.

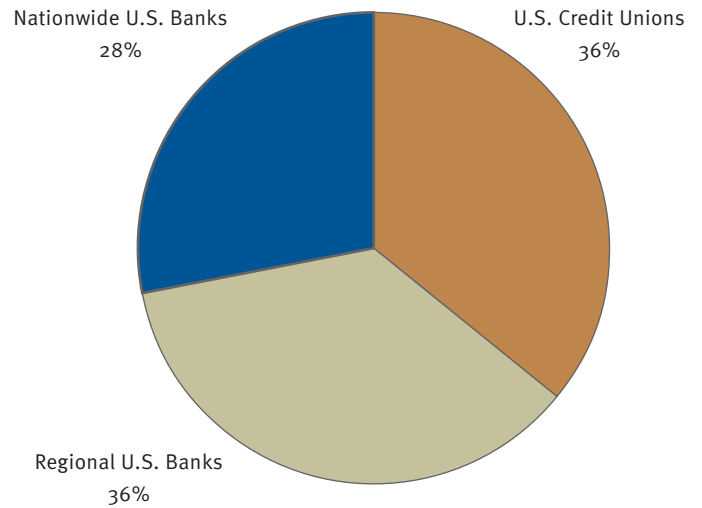




3. Segmentation of U.S. Banking Brands Attacked by Phishing

Trend Analysis

The distribution of attacked U.S. entities hardly changed in April. The share of nationwide banks, which has been holding steady at around 30% since December 2007, maintained a similar percentage this month (28%). The numbers for the regional banks and the Federal Credit Union sector changed slightly, month-over-month: the share of the regional banks rose by 1%, and that of the Federal Credit Unions fell by 6%. Together the two groups form a little more than two thirds of the attacked U.S. entities. These figures do not indicate on an obvious trend but should be followed over a longer period of time: the distribution of attacked brands has been very unstable over the past year.



4. Top Hosting Countries

Trend Analysis

The U.S. continues to lead the way in hosting the largest number of phishing attacks, but April saw the U.S. percentage decrease by 12%, month-over-month. China, which was not on the list in March, reappeared in second position in April with 19% of all attacks, something that we can attribute to the many Rock Phish and Fast-Flux domains that were registered in China during the month. As in March and February, Germany, South Korea and the UK occupy the following three spots. The rest of the list remained relatively unchanged, except for the appearance of Tokelau, a territory of New Zealand that also hosted many Fast-Flux domains last month. This is the second consecutive month in which Canada and Hong Kong – both traditionally regular “members” of this Top 10 – did not make the list.

