



RSA® Monthly Online Fraud Report: December 2007

Online fraud is evolving. Phishing and pharming continue to serve as a major part of the innovative and technological crime wave faced by online businesses. And with new, sophisticated tools at their disposal, fraudsters can 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 250 organizations worldwide. The AFCC has shut down over 60,000 phishing attacks and serves as a key industry source for information on phishing and other 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 RSA's fraud analysts.

Monthly Highlight

New "Rock-like" phishing attacks

December's dramatic increase in phishing attacks is mostly due to the increased activity of the Rock Phish group. In addition, RSA has recently noticed other interesting developments in phishing attacks against leading financial institutions worldwide. We detected (and shut down) many proxy-based attacks in all likelihood performed by several groups, using a new "Rock-like" phishing infrastructure.

These attacks show some similarities to Rock Phish attacks, but are hosted on completely different networks and do not demonstrate any known Rock signatures. Their magnitude and impact are far lower than Rock's, but they do exemplify some advanced phishing techniques and show that other groups are starting to adopt some of the Rock Phish methodologies.

Here are some Rock-like features of the recent attacks:

The use of proxy servers

The phishers behind the recent attacks use proxy servers, much like in Rock attacks. Victims of the attacks communicate with these proxy servers, which deliver the phishing content from "mother ships." There is no direct communication between the victims and the actual phishing site. These attacks are not based on a known fast-flux network. It seems that these groups do not use large botnets of proxies, and so far, we have not detected any other data that associates the attacks with known fast-flux networks.



The Security Division of EMC



Multiple attacks under a single domain

With some similarities to the Rock Phish attacks, a single domain sometimes hosts attacks against multiple financial institutions. In addition, a single proxy server, to which the domain points, is used to direct victims to attacks against multiple institutions. For example, we traced one proxy server which was used to instigate attacks against six different financial institutions in the U.S.

Mitigation of such attacks

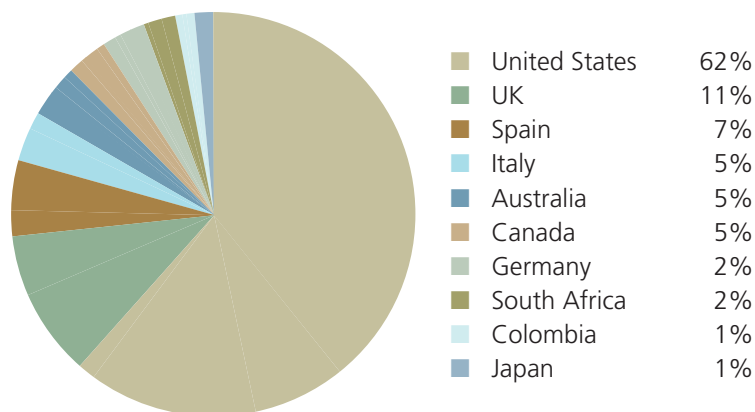
These new attacks demonstrate that more and more phishers are now starting to adopt techniques which had so far been associated with the Rock Phish group and some fast-flux phishing attacks.

Like in Rock attacks, the structure of these attacks make them harder to shut down at the ISP level since IP addresses are changing and the hosting server cannot be determined. The RSA Anti-Fraud Command Center usually chooses to focus on taking down domains listed for those attacks at the registrar level, which is the common course of action for Rock Phish attacks as well. De-listing the domains ensures that the attacks are taken down, regardless of the servers on which they are physically hosted. Through the RSA 24x7x365 Anti-Fraud Command Center and an extensive global partner network, RSA delivers a comprehensive service to detect, analyze, and shut down these phishing attacks.

Tracing the “Mother Ships”

Part of RSA’s mitigation work is to try to find the attacks’ “Mother Ships” through intensive forensics work. Recently, our forensics research team was able to trace a “Mother Ship” being used by one of the new phishing groups. Phishing content against several institutions was hosted on this server and was delivered to the victims via the proxy servers. Information regarding this server was shared with law enforcement.

Breakdown of Global Banking Brands Attacked by Phishing

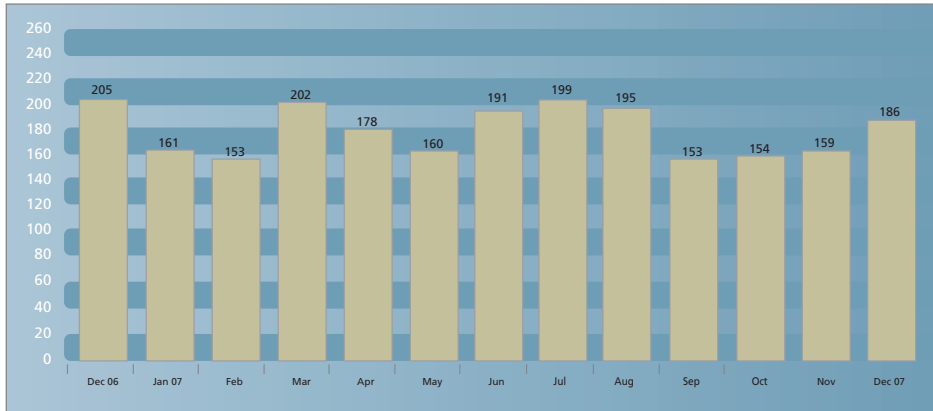


Trend Analysis

The distribution of attacked entities has remained relatively constant since June 2007. As usual, U.S. brands are very dominant, and December was the 11th consecutive month in which UK institutions occupied the second spot, with 11% of the phished entities. Australia and Colombia are in the same positions for the sixth consecutive month. Spain, a regular top-5 member, leaped again into 3rd position this month. Peru and Mexico fell off the list in December, making way for Japan.



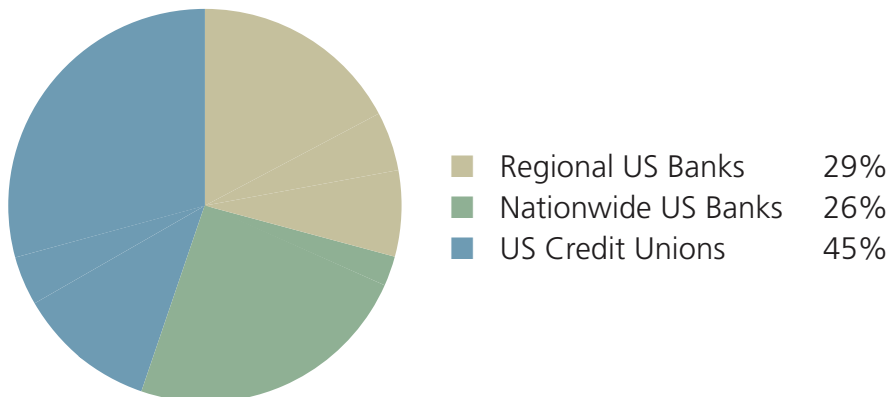
Number of Brands Attacked Per Month



Trend Analysis

The number of attacked brands increased dramatically during December. However the figure is still much lower than that seen in December 2006. In December 2007, the RSA Anti-Fraud Command Center detected attacks against 20 financial institutions that it had not seen attacked before.

Segmentation of US Banking Brands Attacked by Phishing

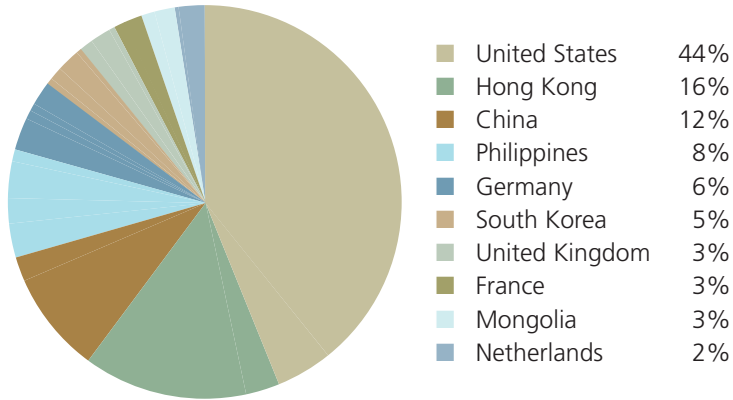


Trend Analysis

Nationwide banks formed only 26% of the targeted U.S. financial institutions during December. This is a major decrease from the rate of 44% seen in November. Most of the load shifted to the FCU sector, which climbed from 33% in November to 45% of the attacked U.S. institutions in December. The regional bank segment increased in turn by 7% month-over-month.



Top Hosting Countries



Trend Analysis

The percentage of attacks hosted in the U.S. has dropped once more to 44% (a similar rate to that seen in September and October 2007). As in many months in 2007, Hong Kong and China occupy the 2nd and 3rd positions. Hong Kong and China are typically featured more prominently in this chart when Rock Phish attacks are on the rise. An interesting newcomer to the list is the Philippines, which also hosted a large amount of Rock and Rock-like domains. The UK, France, Germany and South Korea are still present in the list, with their individual hosting rates remaining typically constant in December.