

RSA Online Fraud Report

June, 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: Phishing kits store stolen data in SQL database.

Launching a phishing attack, or a Trojan attack, is only the first task on the fraudster's list of things to do in order to be successful. Collecting stolen credentials from people who were successfully phished is a good start if you are a fraudster, but there are other tasks to complete. After an attack, fraudsters often have collected large amounts of data that should be stored, manipulated and cleansed in order to make it usable. False data needs to be discarded, and accurate account data needs to be extracted from the total amount collected so that it can be subsequently used by the fraudster or sold in the underground.

Those who create Trojans sell their products in the form software kits and, as a result, have made life a little easier for other fraudsters. These individuals provide Trojan kits that include a user-friendly management console application and users of such "productized" Trojans can easily view collected data and manipulate it. In addition, the infection status of a Trojan and other important statistics are presented within management consoles.

When looking at most phishing kits, this is clearly not the same case. Phishing kits usually involve much less intricate technology and have simple data management capabilities. In most cases, information stolen during phishing attacks can be managed in two different ways:

- (a) it is sent as text to the fraudster's email address which is coded within the PHP files of the phishing kit
- (b) It is simply stored on the phishing server (or another server) as a text file, containing all the information collected in the attack.



The Security Division of EMC

Naturally, the data that fraudsters collect is not entirely usable. The text files they create are not structured and do not allow fraudsters to conveniently view the stolen data and use it. They contain a large amount of information in a single file but much of it is actually worthless since many phishing victims deliberately provide false information.

Recently, RSA discovered some phishing kits that correct this flaw: instead of sending credentials via email or storing them in a simple text file, these newer phishing kits directly store

```
# connection to db
$server = "localhost";
$username = "XXXXX";
$password = "XXXXX";
$database = "XXXXX";

$conn = mysql_connect($server,$username,$password) or die ("Error");

mysql_select_db($database,$conn) or die ("Error");

# Insert record:
if($_POST){
    $fecha = '10/10/10';
    $user = $_POST['USERID'];
    $pass = $_POST['PASSWORD'];
    $XXXXX = $_POST['PASSWORDo'];
    $ip = getenv("REMOTE_ADDR");
    $estado = "";

    $result=mysql_query("select * from datos where user='$user'", $conn);

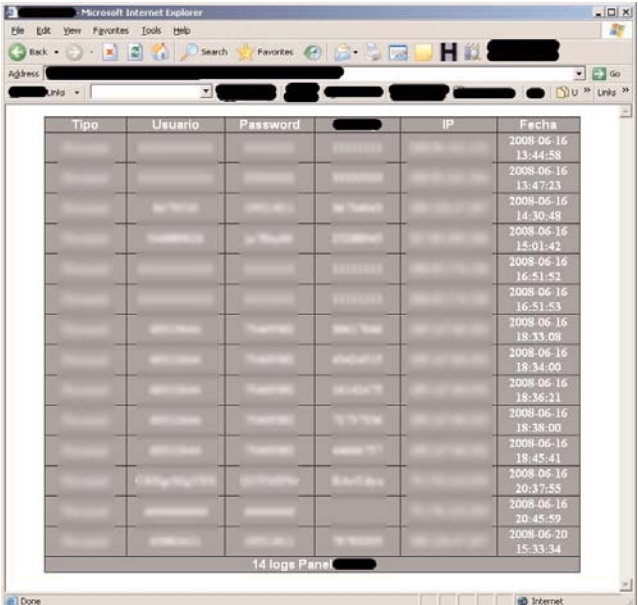
    while($row=mysql_fetch_array($result))
    {
        @$estado = $row[estado];
    }

    if($estado != 'Erectado'){
        if($estado != 'Otro'){
            if($estado != 'Pobre'){

                mysql_query("INSERT INTO datos (user, pass, XXXXXX, ip, fecha,tipo) VALUES ('$user', '$pass', '$XXXXX', '$ip',now(), 'Empre' ) ") or die(mysql_error());
            }
        }
    }
}
```

the credentials in a MySQL database on the phishing server. These databases are user-friendly and allow fraudsters to quickly and easily view the results of a phishing attack and manipulate the data. This is much more efficient than the tedious task of reviewing a text file which is full of false and partial data entered by users. In some cases, RSA saw that fraudsters can even filter the list of victims and delete false or partial data. The database can be accessed and viewed by the fraudster via PHP pages.

These innovations in phishing kits were designed to make them much more user-friendly. Fraudsters who use them can easily manage the stolen data, in a similar manner to the management of Trojan logs. Trojan herders do. Like some other fraudster innovations, these kits are not a new threat to banks or their users, but simply an improvement that makes the fraudsters' lives much easier. As a result, these kits can grow in popularity within the underground and eventually become a commodity.



Tipo	Usuario	Password	IP	Fecha
				2008-06-16 13:44:58
				2008-06-16 13:47:23
				2008-06-16 14:30:38
				2008-06-16 15:01:42
				2008-06-16 16:41:42
				2008-06-16 16:51:53
				2008-06-16 18:33:08
				2008-06-16 18:34:00
				2008-06-16 18:36:21
				2008-06-16 18:38:00
				2008-06-16 18:45:41
				2008-06-16 20:37:54
				2008-06-16 20:45:39
				2008-06-20 15:33:34

A screen shot of the fraudster's interface, where the database can be viewed on the server and displayed through a PHP page.

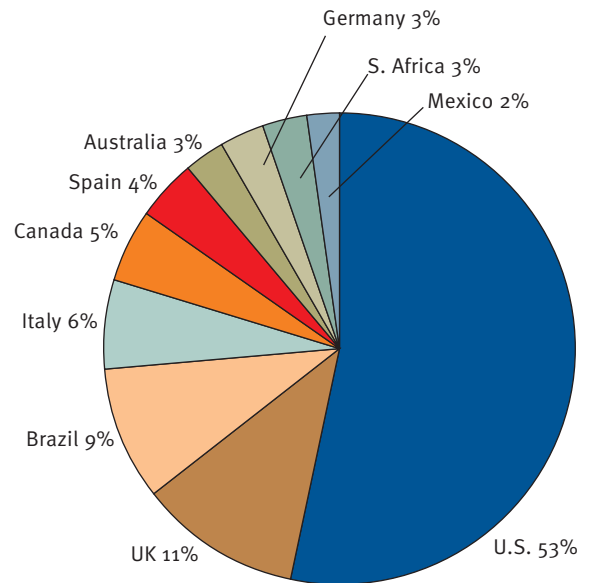
Part of the new phishing kit's code discovered by RSA. This particular piece of code inserts the stolen credentials in the MySQL database on the phishing server.



1. Breakdown of Global Banking Brands Attacked by Phishing

Trend Analysis

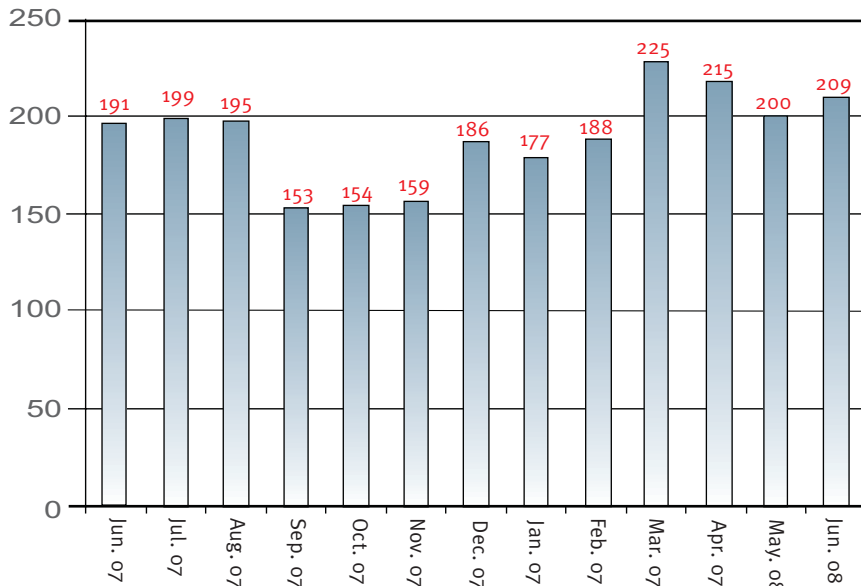
The U.S. brands remain in first position for the 17th consecutive month. The most interesting development in June was Brazil making the list and being in the 3rd position. Brazil had a large impact this month and follows the trend we have seen of more South American brands under attack. The remainder of the list reflects the distribution of attacked entities relatively similar to that of previous months. As usual, U.S. brands are the most dominant, followed by the UK brands. These two are usually followed by Spain, Italy, Canada, Australia and South Africa, who are also becoming a regular member in this list.



2. Number of Brands Attacked Per Month

Trend Analysis

The number of attacked brands rose slightly during June, despite the decrease in the total number of phishing attacks. In June, the RSA Anti-Fraud Command Center detected attacks against 36 entities that it had not seen attacked before. This is a relatively high number compared to our findings over the past few months, where attacks on 20-25 new entities were typically detected.

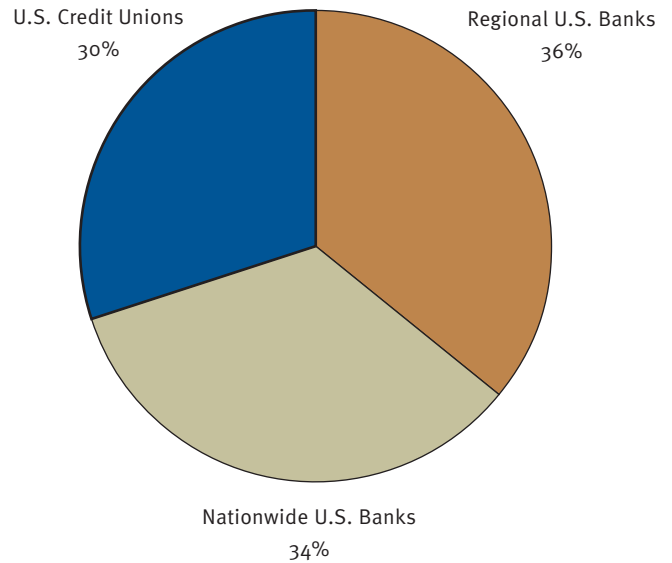




3. Segmentation of US Banking Brands Attacked by Phishing

Trend Analysis

In May, almost half of the attacked U.S. banking entities were Federal Credit Unions. This was an extraordinary figure, and in June RSA saw a return to 'normal' levels in this regard. As in May, the proportions of regional and nationwide U.S. banks that were attacked were very similar – only differing by two percentage points.



4. Top Hosting Countries

In June the UK moved back into 2nd position in this list, a place that China had occupied for two consecutive months. Interestingly, however, China did not make the Top 10 Hosting Countries chart at all in June. This change is due to a shift in the hosting of Rock Phish and other Fast-Flux domains. France, South Korea and Russia continue to host similar percentages of attacks on a monthly basis. Luxembourg, which first appeared on the list after hosting Fast-Flux attacks in May, is still in the Top 10 but hosted a smaller proportion of attacks when compared to last month.

