

RSA Online Fraud Report

July, 2010

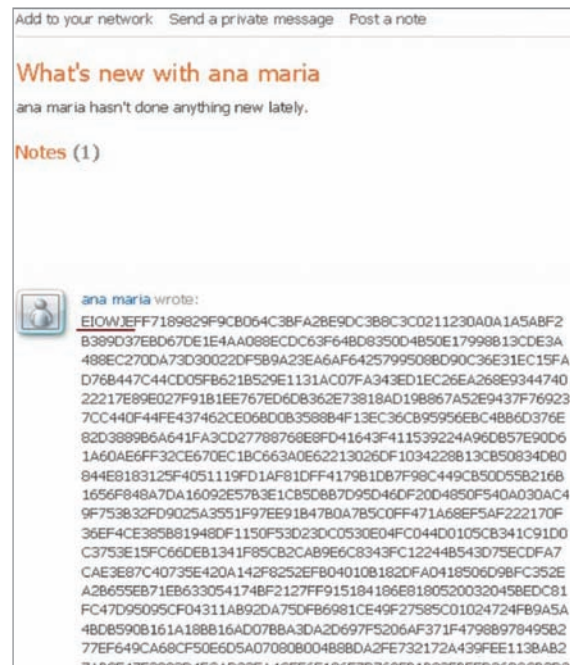
Cybercriminals Widely Using Public Social Networks to Give Command and Control Orders to Banking Trojans

While malware updating via public resources is nothing new in itself, the RSA FraudAction Research Lab recently witnessed this hosting method being used to operate a banking Trojan; specifically a variant of the “Brazilian Banker” family of Trojans. In effect, any website that allows users to upload virtually any type of content, and then publishes it in sequential form—without line breaks such as those denoted by the HTML tag
 for a single-line break—can be exploited to store Trojans’ encrypted configurations. This includes almost any social networking or Web 2.0 platform that enables the almost unrestricted posting of comments, creation of public profiles and the setup of newsgroups.

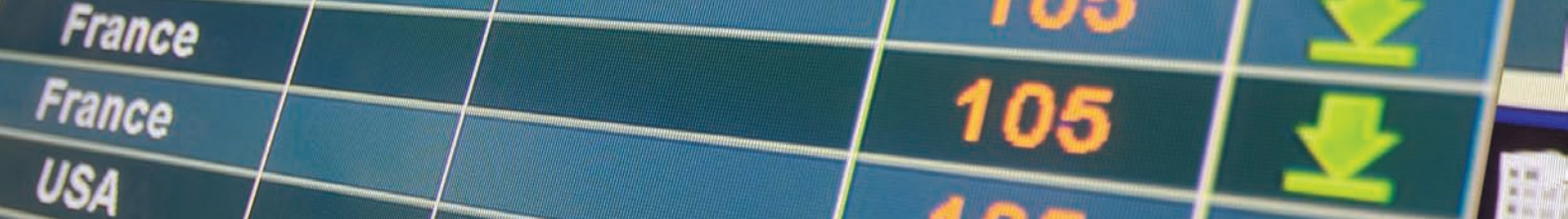
A Brazilian Banker gets Social

Brazilian Banker is a financial Trojan that targets consumers of Brazilian-based banks and other banks in Latin America. The Lab recently traced a social network profile that contained encrypted instructions for a variant of the Brazilian banker Trojan (see Figure 1). Shortly after our discovery of the Trojan’s configuration point, the offending content was handled and removed by the social network’s support team. It is important to note that the social network was in no way at fault for being exploited in the manner described above. Any site that enables the posting of user-entered content is vulnerable to this type of misuse, and is exploited precisely because of the freedom it affords its users.

Figure 1: Social Profile Serving Trojan’s Encrypted Configuration



The Security Division of EMC



This is how it worked:

1. The hacker behind the malware set up a bogus profile under the name of “Ana Maria” and entered the malware’s encrypted configuration settings as text uploaded to the profile.
2. After installing itself on a user’s machine, the malware searched the profile for the string **EIOWJE** (underlined in the above screenshot). The string signified the starting point of the malware’s configuration instructions.
3. All the encrypted commands following the **EIOWJE** string were decrypted by the malware and executed on the infected computer.

The above method allows the hacker to issue encrypted commands without renting a dedicated, bulletproof server or registering a domain for the malware’s communication points. Another example of a public resource being exploited as a command and control point belonging to a Trojan’s operation reportedly involves Twitter’s RSS feed option. The bot herder’s method of operation in this case is as follows:

1. A bogus Twitter account is set up by the fraudster.
2. By logging into a designated email account, the Trojan periodically checks for new instructions specified in status updates sent via Twitter’s RSS feed. Each new command appears as a status update and contains new instructions for the Trojan to execute.

One criminal even took this a step further and created a Twitter-based botnet builder. Another case in point involves the exploitation of Google Groups: After installing itself on a victim’s computer, the Trojan logs into a Google Gmail account and requests a page from a specific, bogus newsgroup set up in advance by the criminal for Trojan operations. The Trojan executes the commands specified in the newsgroup’s latest page and uploads its replies as posts to the same newsgroup.

Why ‘Go Public’ ?

Internet security companies have previously reported high profile Web 2.0 platforms, such as social networking sites and webmail providers, being exploited by Trojan operators to store malware configuration file. Some advantages that can make this storage technique attractive are:

- Criminals do not need to buy and maintain a domain name for their command & control point (aka update point).
- Criminals do not need to pay for or maintain a dedicated, bulletproof server for their activities.
- As soon as one public profile or account is removed by these services, a new profile or account can be easily set up, free of charge.
- From the criminal’s point of view, the exploitation of a public resource may seem more difficult to detect. Detecting Trojan-related communication resources hosted on public websites becomes virtually impossible by scanning suspicious URLs alone. These kinds of resources require other detection methods to be deployed by security companies.

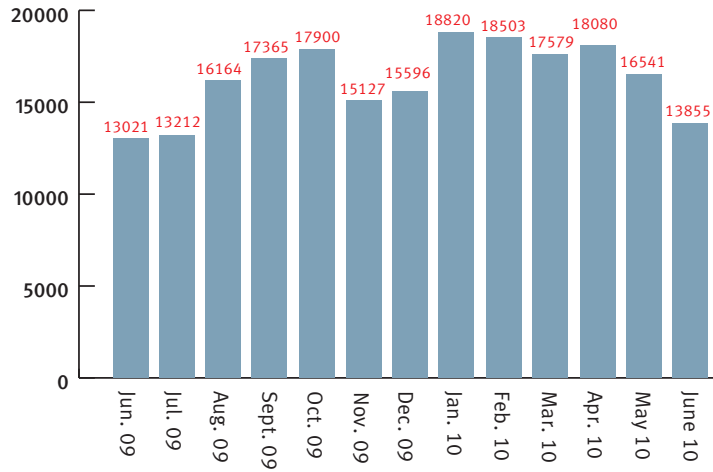
It is worth noting that despite these advantages, banking Trojan attacks that host communication resources on public resources are still quite rare; currently, this method remains the exception rather than the rule. Generally, after a threat is detected and the appropriate support team is informed, the removal of these command and control points is simple and quick.



Phishing Attacks per Month

June 2010 marked the second consecutive month where RSA witnessed a decrease in the volume of phishing attacks; total volume dropped 16 percent in June. Whereas attacks hosted using standard methods dropped last month by seven percent, attacks hosted on fast-flux networks fell an entire 70 percent.

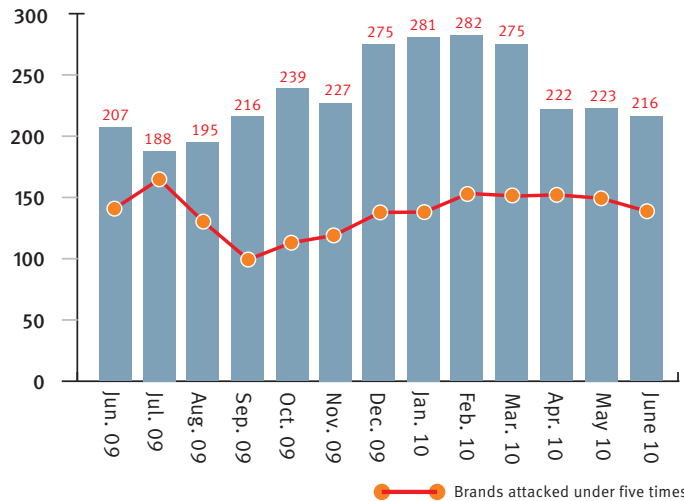
As reported in recent months by RSA, the Rock Phish gang (aka the Avalanche gang) has almost ceased its phishing activity and is currently most active in launching attacks to proliferate malware. As a result, very few attacks were launched from the MS-Redirect network (aka the Avalanche botnet) in June.



Source: RSA Anti-Fraud Command Center

Number of Brands Attacked

In June, phishing attacks were launched against 216 brands worldwide, a three percent decrease from May. One hundred and twenty (120) brands were targeted less than five times last month, accounting for 56 percent of all the targeted brands, and nineteen brands were targeted for the first time.



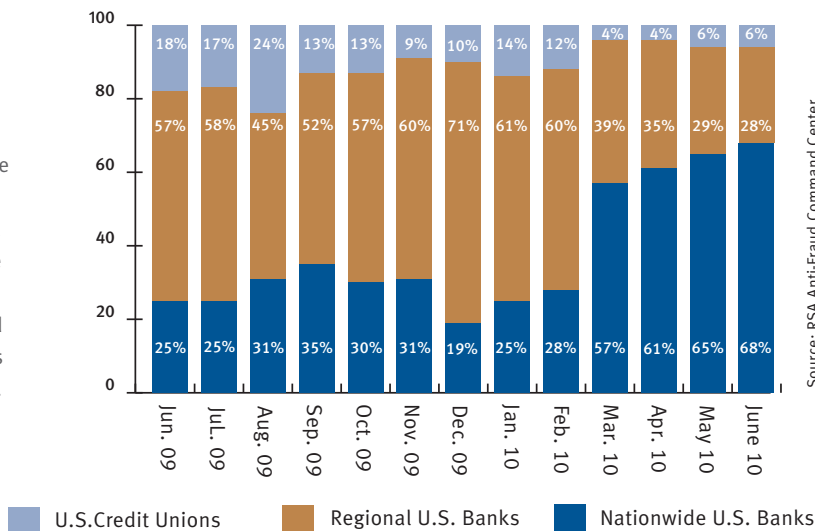
Source: RSA Anti-Fraud Command Center

Brands attacked under five times



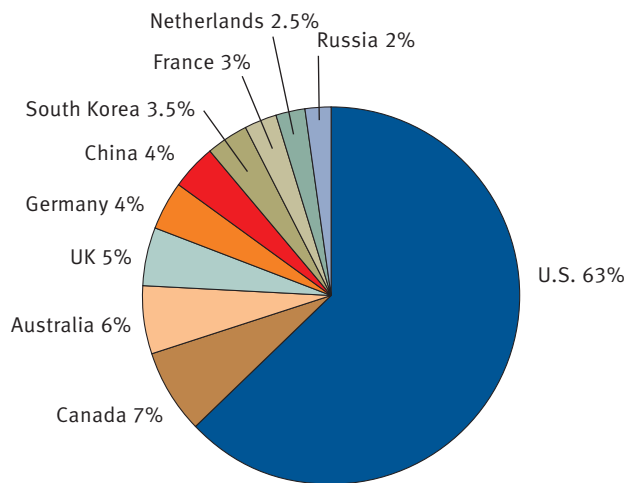
Segmentation of Financial Institutions Attacked Within the U.S.

Nationwide banks remained the most targeted brands in the U.S. financial sector (in terms of the number of brands attacked), climbing another three percent in June. The percentage of regional brands attacked dropped three percent while the portion of brands classified as credit unions that were attacked remained unchanged as compared to May. Since March 2010, U.S. nationwide banks have been the hardest hit by phishing compared.



Top Ten Countries Hosting Phishing Attacks

The U.S. continues to be the top hosting country for phishing attacks by a considerable margin for the eighth consecutive month; in June, the U.S. hosted 63% of the phishing attacks identified by RSA. Australia and Canada remained as top hosting countries while South Korea, which has been one of the top three hosts for several months, dropped to the seventh position, hosting just 3.5 percent of attacks in June.

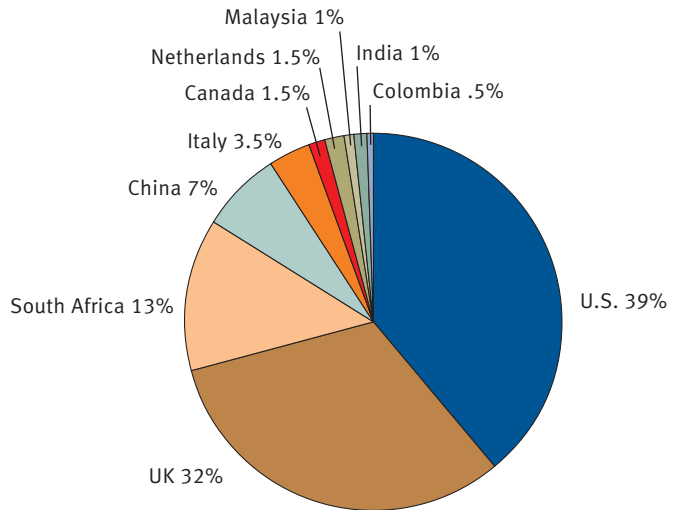


Source: RSA Anti-Fraud Command Center

Top Ten Countries by Attack Volume

In June, the volume of phishing attacks endured in the U.S. increased, replacing the UK as the country suffering the highest volume of attacks. In addition, after three consecutive months on the list, Brazil was replaced by Colombia as one of the top countries by attack volume.

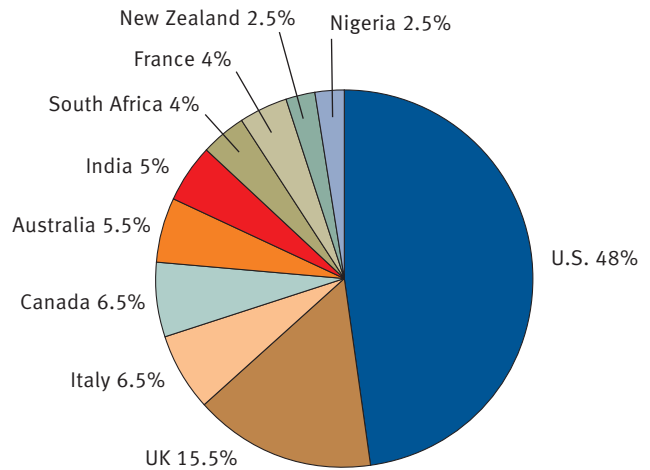
Source: RSA Anti-Fraud Command Center

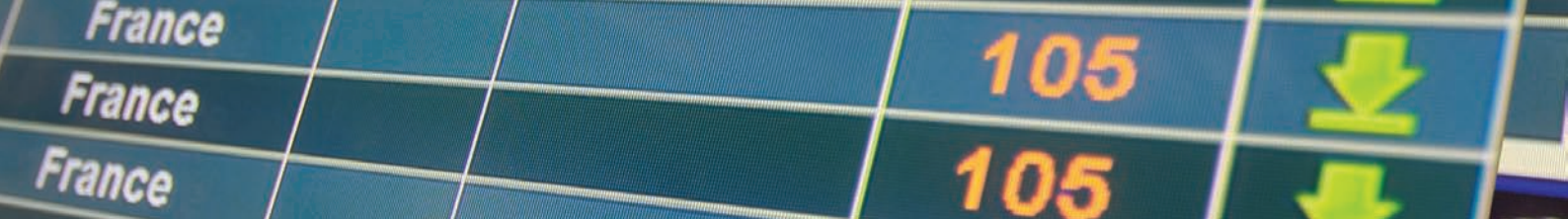


Top Ten Countries by Attacked Brands

In June, the U.S. brands were attacked at a nearly 2:1 ratio compared to all other countries. Brazil fell off the chart completely, while New Zealand reappeared on the list for the first time since September 2009. Since March 2010, phishers have continued to repeatedly attack brands in the same countries, namely the U.S., UK, Italy, Canada, Australia, India, South Africa and France.

Source: RSA Anti-Fraud Command Center





The Security Division of EMC

www.rsa.com

The information set forth in this RSA Online Fraud Report is based on sources and analysis that RSA Security Inc. ("RSA") believes are reliable. Statements concerning financial, regulatory or legal matters should be understood to be general observations of the RSA professionals and may not be relied upon as financial, regulatory or legal advice, which RSA is not authorized to provide. All such matters should be reviewed with appropriate qualified advisors in these areas. RSA reserves the right to notify law enforcement authorities and/or other relevant agencies regarding the information RSA uncovers in the course of doing business.

Usage Guidelines

Individuals and organizations may reference content from any RSA Online Fraud Report by following these guidelines:

- (1) Reprinting and/or distributing an entire RSA Online Fraud Report requires prior approval from RSA in all cases. This includes an entire Monthly Highlight and/or the full set of Statistics and Analysis from RSA's phishing repositories. Any requests to reprint and/or distribute an RSA Online Fraud Report must be directed to Heidi Bleau at heidi.bleau@rsa.com.
- (2) It is permissible to reference up to three sentences from the Monthly Highlight. They must be cited in their entirety and within quotation marks. Any requests to cite more than three sentences must be directed to RSA.
- (3) It is permissible to reference up to three sets of Statistics and Analysis from RSA's phishing repositories. Any requests to cite more than three sets may be directed to RSA. Charts may not be redrawn. All citations from related data analysis must appear in full sentences and within quotation marks.
- (4) It is required that all references to the RSA Online Fraud Report are credited in the following manner: "Source: RSA Anti-Fraud Command Center, RSA Online Fraud Report, [month], [year]" .

EMC, RSA, RSA Security, FraudAction™ and the RSA logo are registered trademarks or trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the properties of their respective owners.