

RSA Online Fraud Report

July 2009

A Monthly Intelligence Report from the RSA® Anti-Fraud Command Center

Online crime is constantly evolving, and fraudsters do not discriminate against any organization or person. Online attacks involving phishing, pharming and Trojans represent one of the most organized and sophisticated technological crime waves worldwide. Online criminals work day and night to steal identities, online credentials, credit card information, or any other information that they can efficiently monetize. They target organizations in all sectors, as well as any person who uses the Internet at work or at home.

These online criminals also have new tools at their disposal and are able to adapt more quickly than ever with advanced crimeware; rapidly deployed using stealth mechanisms. Their supply chains have evolved to match that of the legitimate business world, including the ability to provide what RSA coined "Fraud-as-a-Service".

This monthly intelligence report has been created by the experienced team of fraud analysts from the RSA Anti-Fraud Command Center. It includes a monthly highlight based on keen insight into the world of online fraud as well as statistics and related analysis from RSA's phishing repositories.

About the RSA Anti-Fraud Command Center

The RSA® Anti-Fraud Command Center is a 24x7 war room that helps organizations detect, block, monitor, track and shut down phishing, pharming and Trojan attacks across more than 140 countries. Protecting more than 300 organizations against online attacks, the RSA Anti-Fraud Command Center has shut down more than 165,000 phishing attacks to date and is a key industry source for intelligence on new and emerging online threats.

The RSA Anti-Fraud Command Center is staffed by over 100 experienced fraud analysts and has established direct, open channels with dozens of Internet Service Providers around the world, as well as numerous CERTs and law enforcement agencies. Multi-lingual translation support is available in nearly 200 languages to further enhance its ability to detect, block and shut down fraudulent websites and significantly reduce the average uptime of online attacks around the globe.



The Security Division of EMC



Fraudsters Infiltrate the Call Center

The RSA Anti-Fraud Command Center recently published a report that summarized its predictions and trends in online fraud over the next 12 – 18 months. Among the predictions was an increase in the variety of services offered for hire in the underground, including professional ‘call center’ services. Online criminals use these services in order to commit fraud within the phone channel.

Fraudulent call center services have existed for some time and were historically used as a way to confirm transactions processed through money transfer providers. A fraudster who wanted to complete a transaction could work around language barriers by posting a message online to seek out another fraudster who spoke the language of the legitimate sender of the money. That service was referred to as a “confirmer service.” The “confirmer” would then receive the necessary details from the fraudster in order to complete the transaction over the phone.

The incentive to target the phone channel for the purposes of committing fraud has increased due to the extensive efforts on improving authentication in the online channel. In response, many organizations began to implement additional layers of security in the phone channel, including identification of the caller through the use of the originating phone number, or ‘Caller ID.’

This compounded the challenge to fraudsters to successfully commit phone fraud: First, they would need to enlist confirmer services to overcome the language barrier.

Second, they would need to ensure the confirmer could solicit Automatic Number Identification (ANI) services that could spoof the number of the genuine account holder.

Fraudsters Work to Commit Phone Fraud More Effectively

Fraudsters have been using publicly available services offered over the Internet that spoof the Caller ID on outgoing calls. However, by using public spoofing services, fraudsters are opening themselves up to the risk of exposure. In order to avoid getting caught, some fraudsters are looking to advance the service even further by building their own infrastructure for ANI spoofing through the use of a Public Branch Exchange (PBX). A PBX performs Voice over IP (VOIP) in many protocols and can interoperate with most standards-based telephony equipment using relatively inexpensive hardware. Using this infrastructure, fraudsters can set the ANI to any number when making an outgoing call and create a fake caller ID.

Recognizing an opportunity to illegally make money with lower risk of getting caught, service providers in the underground have evolved phone fraud services into a singular location to provide other fraudsters with the ability to conduct phone channel fraud to any destination and in any language. RSA has uncovered a criminal professional call service available to other fraudsters that can spoof any number in the United States and also offers cash out in multiple languages (see graphic). The service costs USD\$12.00 and enables phone numbers to be customized depending on the state where the account holder resides and enables fraudsters to accept incoming calls, posing as the genuine account holder.

Professional Call Service
Calling: Shops, Drops, Casinos, Banks, Hosting Companies, UPS, FedEx
9 english speaking males, 3 females
Italian: Male (15 WMZ. Calling time etc. may be discussed)
German: Only Female
Spoofing numbers to any number (USA)
Can accept incoming calls on mine or your number.
Can fix up a custom number by state.
Working hours - Mon-Fri , Sat. 18:00 -02:00 Moscow Time.
(99% of days I am online until 04:00)
Prices:
Any call 12\$
Incoming call 12\$
Creating a number:
10\$. Time To Live: 1 Week min, probably longer. Almost all area codes.
We accept money only for "full" calls: called the right location, talked with the person we needed to.
We don't charge you for answering machines. No additional charge to leave a message.
If an operation fails (example: failure in a balance transfer) because of insufficient data provided by customer
we hold no responsibility (example: question about cardholder's neighbors, an we didn't have this info) and other reasons.
Its possible to arrange a drop-project phone support.
Returning customers are allowed to delay payment, discounts, etc.
Contact ICQ

A chat room featuring fraudster call center services was discovered by RSA Fraud Center analysts.



Challenges to Securing the Phone Channel

There are several issues that organizations encounter when attempting to secure the phone channel. First, the online and phone channels are often disconnected operational units within the structure of most organizations. Therefore, identifying attempts to commit fraud across different channels remains a challenge. For example, if a fraudster attempts to cash out a bank account using the online channel but is unable to circumvent the security measures in place or correctly pass a secondary authentication challenge, the phone channel is often the next possible option. However, a representative within the call center may have no insight into any previous failed attempts. The lack of a multi-channel view makes it more viable to commit fraud over the phone.

Also, the outsourcing of call center services to countries outside of the U.S. makes management of the process even more difficult for the fraudsters. Cultural and language barriers can create hurdles as foreign representatives may not be fully trained to distinguish between even the most basic information such as the difference between male and female names. This can make it more viable for fraudsters to use the phone channel for cashing out accounts.

Mitigation Techniques

There are a number of measures that can be considered to secure the phone channel and assure the identities of customers beyond utilizing their phone number as an identifier (which is easy to circumvent with ANI spoofing). Not every call that comes into the call center needs to go through a verification process, but certain activities – such as activating a debit card or conducting high-value transactions – should require an additional security measure to be passed.

Knowledge-based authentication tools are being used more frequently with banks and other organizations as a means to prevent fraud occurring in the call center. Knowledge-based authentication utilizes a question and answer format. Leveraging information available in public records and commercially available databases, a series of questions and answers are developed that are unique to each individual. The question and answer choices are presented to the customer and based on their responses, a simple “pass/fail” result is delivered. The answers to the question types used are not easily found by an Internet search, thus making it very difficult for anyone other than the genuine customer to guess correct responses.

The RSA Anti-Fraud Command Center is staffed by over 100 experienced fraud analysts.

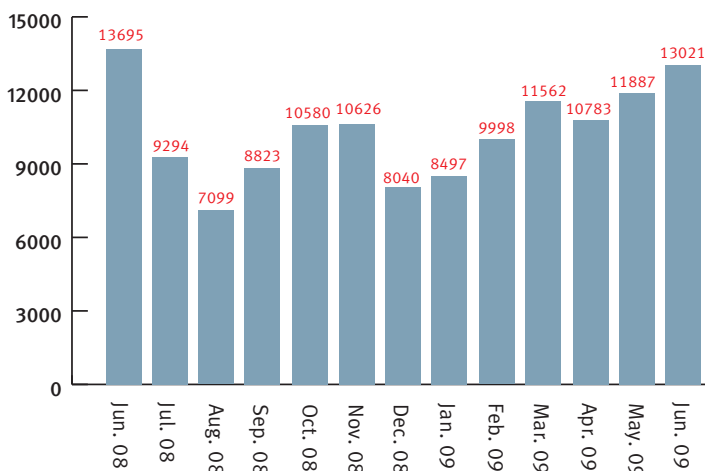




Phishing Attacks per Month

Trend Analysis

As in May, the number of attacks launched in June rose by 10 percent, setting a new 11-month peak. Both fast-flux and standard attacks increased last month; standard attacks by 13 percent and fast-flux attacks by 5 percent. As in the previous month, the number of fast-flux attacks launched in June was greater than the number of standard phishing attacks.

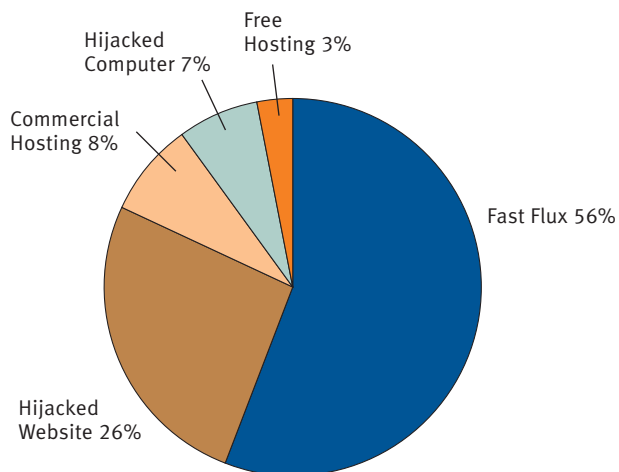


Source: RSA Anti-Fraud Command Center

Distribution of Attacks by Hosting Method

Trend Analysis

As demonstrated in June's distribution of Hosting Methods, fast-flux attacks continue to comprise the largest portion of attacks (56 percent). Throughout June, hijacked websites were used to a slightly lesser extent than in May (26 percent), while the portion of attacks hosted via commercial web hosting doubled (to 8 percent). The portion of attacks hosted on hijacked computers also increased, while the portion of attacks using free hosting dropped slightly.



Source: RSA Anti-Fraud Command Center

Hosting Methods

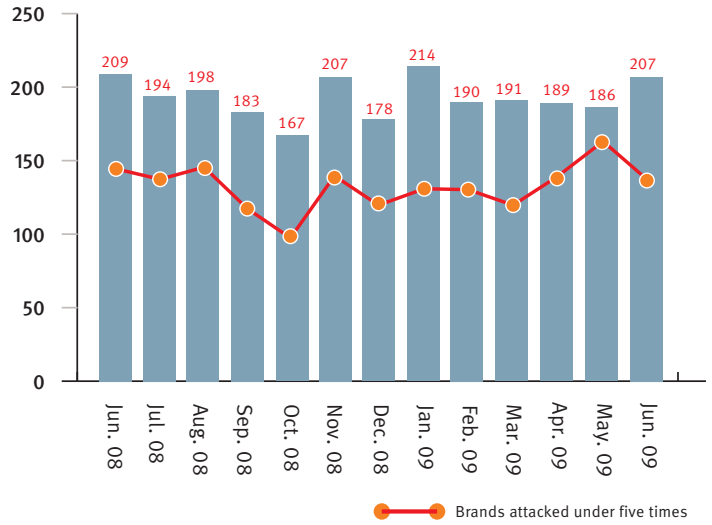
- Fast-flux networks produce an advanced Denial of Service (DNS) technique that utilizes a network of compromised computers, known as a botnet, to host and deliver phishing and malware websites. The compromised computers act as a proxy, or middleman, between the victim and the website. It is difficult to expose and shut down fast-flux networks as content servers that deliver phishing and malware websites are hidden behind a cloud of compromised machines whose addresses change very quickly in order to avoid detection.
- Hijacked websites are those where fraudsters host their illegal content on legitimate websites' sub-domains, avoiding the registration of their own domains used for phishing attacks.
- Commercial hosting involves fraudsters who host their malicious websites for other fraudsters in exchange for a fee.
- Hijacked computers consist of compromised computers whose IP addresses were assigned to a specific phishing domain.
- Free Hosting refers to attacks that leverage free hosting services.



Total Number of Brands Attacked

Trend Analysis

The number of brands attacked in June rose 11 percent as compared to May, with 15 new targets enduring their first attack last month. There were 130 brands that suffered less than 5 attacks throughout the month of June, a portion equivalent to 63 percent. As compared to the figure of 85 percent reported in May, this demonstrates that not only were more brands attacked, but that a larger portion of brands were attacked repeatedly.

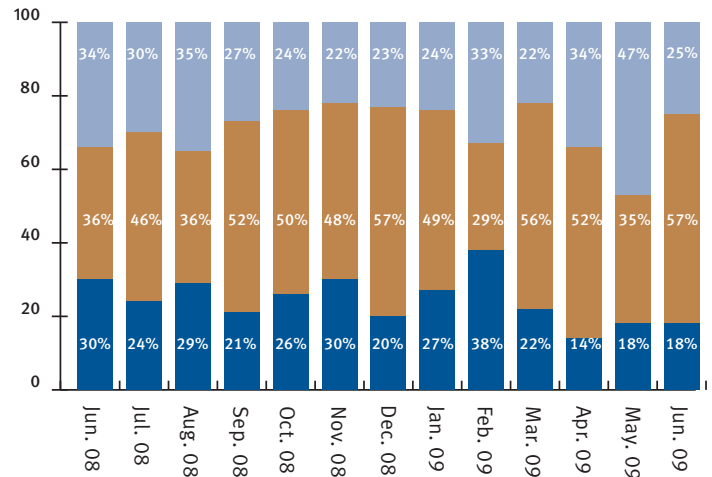


Source: RSA Anti-Fraud Command Center

Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis

In June, the regional bank sector reclaimed its lead after six months, with an increase of over 60 percent in the number of brands targeted in June 2009. The portion of US credit union brands targeted remained constant from the figures reported for May, while nationwide brands experienced a drop of over 50 percent in the number of targeted brands.



Source: RSA Anti-Fraud Command Center

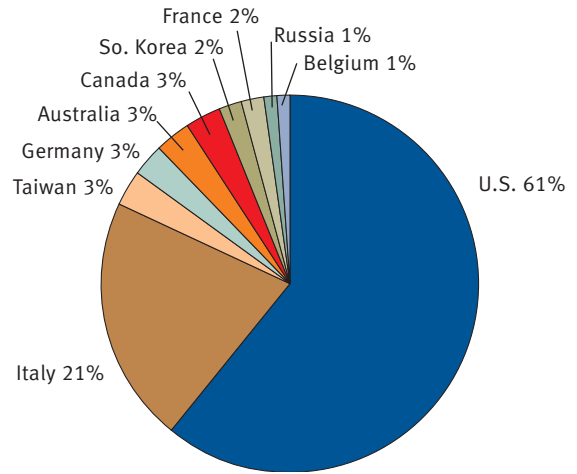
Nationwide U.S. Banks
 Regional U.S. Banks
 U.S. Credit Unions



Top Ten Countries Hosting Phishing Attacks

Trend Analysis

While the U.S. suffered the most attacks, in terms of the portion of attacks it hosted, Italy hosted a massive 21 percent of June's phishing attacks. Not surprisingly, this surge in hosting is due to the many domains registered there by the Rock Phish gang for its fast-flux attacks. After Italy, the remaining top ten hosting countries hosted a relatively small portion of attacks. In addition to Italy, Taiwan, Australia and Russia made it to the roster this month while most of May's newcomers, including Singapore, Israel and Hong Kong, fell off the list completely.



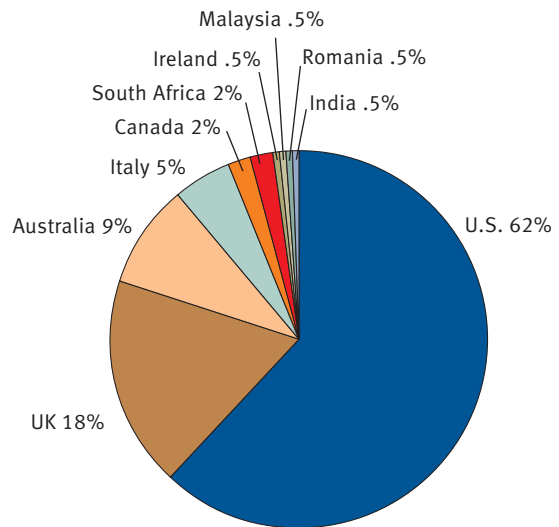
Source: RSA Anti-Fraud Command Center

Top Ten Countries by Attack Volume

Trend Analysis

Among the ten countries that endured the largest portion of attacks, the U.S. and the UK retained portions similar to those reported in May. Australia and Italy traded places in June, with Australia suffering the third largest portion of attacks, and Italy dropping to fourth. Except for this month's newcomer, Malaysia who ranked eighth in the portion of attacks endured, the remaining countries retained positions similar to those of May.

Over the past year, the five countries that have consistently suffered the largest portion of attacks have been the US, the UK, Italy, Canada and South Africa.



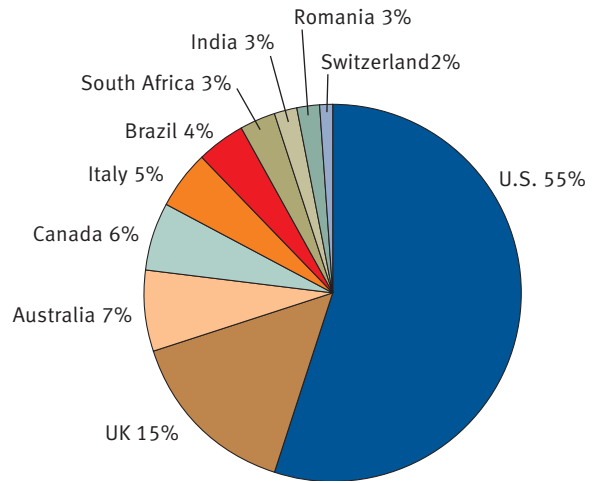
Source: RSA Anti-Fraud Command Center



Top Ten Countries by Attacked Brands

Trend Analysis

In June, U.S. and UK brands remained the most targeted brands, with Australia climbing to third while keeping the same rate of attacks as in May. Canadian brands were targeted twice as much in June as they were in May, followed by Italy, whose brands retained steady rates as compared to the month prior. Brands from Brazil, Romania and Switzerland entered the list last month, while brands from the Dominican Republic and Ireland fell off the list completely.



Source: RSA Anti-Fraud Command Center



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

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.

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]".

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

ONLINE FRAUD REPORT JULY 09