

RSA Online Fraud Report

June 2009

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

Online crime is constantly evolving, and fraudsters do not discriminate against any entity or person. Online attacks involving phishing, pharming and Trojan attacks represent one of the most sophisticated, organized and innovative technological crime waves worldwide. Fraudsters work day and night to steal identities, credentials or any other information that they can efficiently monetize. They target online businesses in all sectors, as well as any person who uses the Internet at work or at home for e-commerce, social networking, e-mail and more.

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 series of online fraud 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 is designed to detect, monitor, track and shut down phishing, pharming and Trojan attacks spread across more than 140 countries. Protecting more than 320 institutions against online attacks, the RSA Anti-Fraud Command Center has shut down over 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 an experienced team of fraud analysts who shut down fraudulent websites, deploy countermeasures, and conduct extensive forensic analysis to stop online criminals and prevent future attacks – reducing the average lifetime of an online attack to a median of just five hours.

The RSA Anti-Fraud Command Center has established direct, open channels with dozens of Internet Service Providers around the world, as well as several CERTs and law enforcement agencies. It also provides multi-lingual translation support in nearly 200 languages to further enhance its ability to detect, block and shut down fraudulent websites on a global scale.



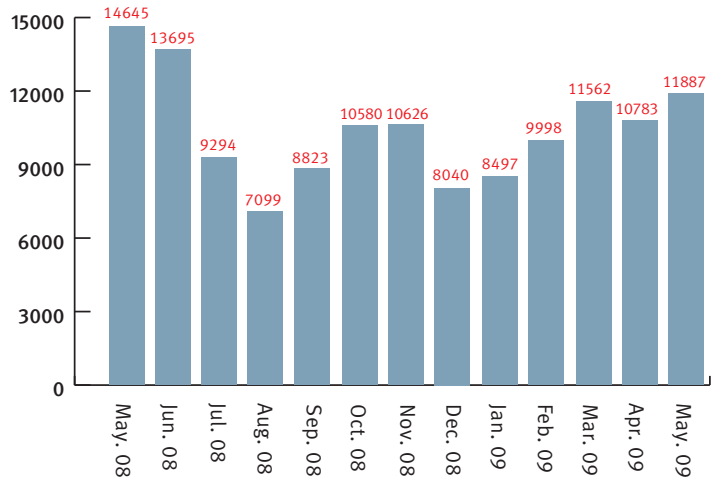
The Security Division of EMC

Total Number of Phishing Attacks Detected by the RSA Anti-Fraud Command Center

Trend Analysis

The total number of phishing attacks in May 2009 increased 10 percent when compared to April 2009 (11,887 attacks in total) – marking a 12 month high. This may indicate an annual trend of higher numbers of phishing attacks occurring during the summer months.

While the number of standard phishing attacks dropped last month by nearly seven percent, the number of fast-flux attacks (which are mostly comprised of Rock Phish attacks) increased by almost 30 percent.

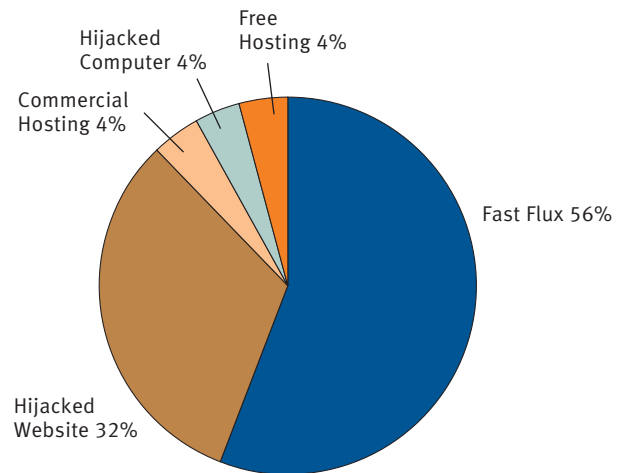


Source: RSA Anti-Fraud Command Center

Distribution of Attacks by Hosting Method

Trend Analysis

Considering the significant number of Rock Phish attacks in May 2009, it is not surprising that fast-flux networks continue to represent the most common method for hosting attacks. The portion of attacks hosted on fast-flux networks (56 percent) grew slightly in May 2009 as compared to April 2009. Attacks hosted using hijacked websites remained the same as April 2009 (32 percent). Commercial hosting and hijacked computers declined slightly to four percent of the total respectively, while free hosting increased very slightly to four percent of the total.



Source: RSA Anti-Fraud Command Center

Descriptions of 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 utilize free hosting services.

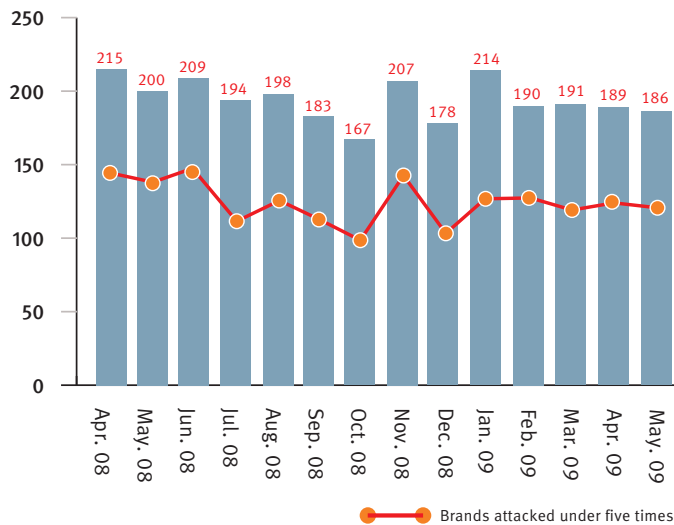


Total Number of Brands Attacked

Trend Analysis

The number of brands attacked during May 2009 slightly dropped when compared to April 2009, even though the total attack volume in May 2009 grew by ten percent. May 2009 is rather exceptional where the portion of brands that are attacked less than five times in a given month typically falls within the 60-65 percent range – whereas in May 2009 over 85 percent of the brands attacked suffered only five attacks or less.

These figures indicate that fraudsters concentrated their attack efforts on a smaller number of brands in May 2009. Similar to the number of new targets enumerated in April 2009, sixteen new brands were attacked for the first time in May 2009.



Source: RSA Anti-Fraud Command Center

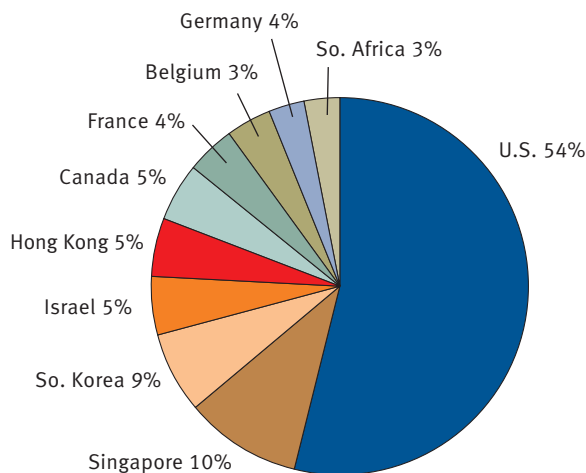
Top Ten Countries Hosting Phishing Attacks

Trend Analysis

After a one-month hiatus from its very steady lead as the country that hosts the most phishing attacks (as enumerated by the location of the ISP or the hosting company) the United States reclaimed its top spot on this top ten list. The U.S. hosted only 32 percent of all phishing attacks in April 2009 which sharply increased to 54 percent of the total in May 2009.

Spain was first on this list in April 2009 with 33 percent of the total, yet dramatically disappeared off of the list in May 2009. In fact, May 2009 demonstrated a significant shift in the countries that host the highest portions of phishing attacks. This shift is a result of the many domains registered by the Rock Phish gang in such countries as the U.S., Singapore, South Korea, Hong Kong, Canada, and Israel.

Singapore appeared very strongly in second place, hosting ten percent of all attacks. Norway fell off of the list in May 2009, as did South Africa and Australia. Israel made its first-ever debut within the top ten list – in a three-way tie for fourth place with Hong Kong and Canada – with each country claiming five percent of the total.



Source: RSA Anti-Fraud Command Center

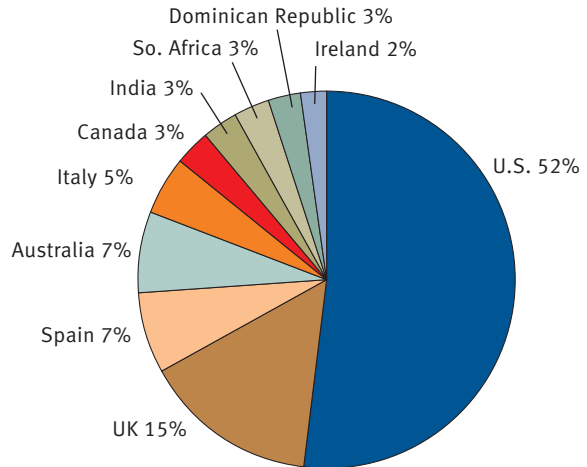


Top Ten Countries by Attacked Brands

Trend Analysis

Over the course of May 2009, the United States maintained its stronghold as the country with the most attacked brands, with fifty-two percent of the total. The U.K. appeared in its usual second position with fifteen percent of the total.

The Dominican Republic and Ireland made their debut within the top ten list in May 2009 while the Netherlands and Brazil fell off the list completely. Brands from Spain, Australia, Italy, Canada, India, and South Africa all maintained steady attack rates as compared to April 2009.



Source: RSA Anti-Fraud Command Center

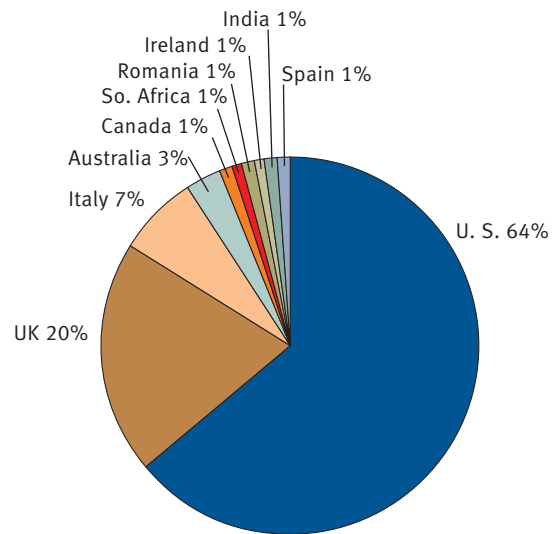
Top Ten Countries by Attack Volume

Trend Analysis

Attack volumes in May 2009 showed a typical result based on the order of the top three countries that appear on this list – with the U.S. in first place (64 percent), the U.K. in second place (20 percent) and Italy in third place (seven percent).

In May 2009, Ireland and Spain appeared on the list, while Malaysia and Greece fell off of the roster. Australia’s share of attacks grew slightly – from one percent in April 2009 to three percent in May 2009. There was a six-way tie for fifth place on the list with Canada, South Africa, Romania, Ireland, India and Spain all receiving one percent of the total number of attacks.

Over the past year, the six countries that have consistently suffered the largest portion of attacks are the U.S., the U.K., Italy, Canada, Spain and South Africa.



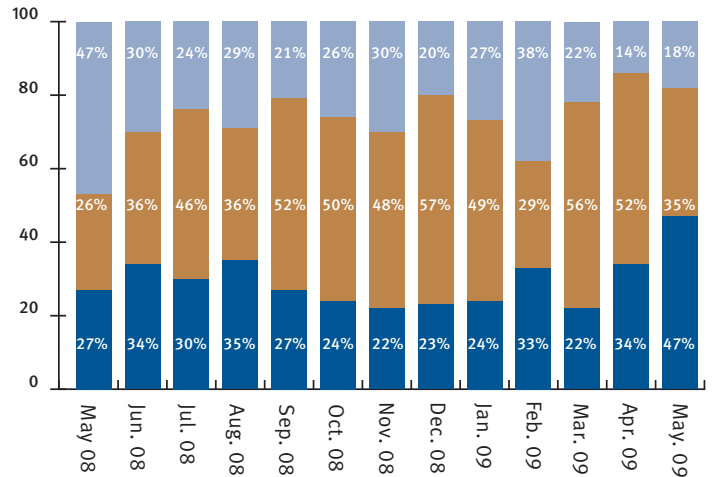
Source: RSA Anti-Fraud Command Center



Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis

In May 2009, the rate of attacks against nationwide US banks (35%) was higher than any other point in the past 12 months – with this segment taking first place, where RSA usually sees regional U.S. banks. In May 2009 the total share of attacks for nationwide banks among these three segments grew by almost 40 percent, while the total share among regional bank brands shrank by 33 percent. In addition, the portion of attacked credit union brands grew by almost 30 percent in May 2009.



Source: RSA Anti-Fraud Command Center

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