

RSA Online Fraud Report

January 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 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 is designed to detect, monitor, track and shut down phishing, pharming and Trojan attacks targeted against more than 300 institutions worldwide. It has shut down over 125,000 phishing attacks to date and is a key industry source for information on phishing, Trojans and emerging online threats.

The RSA Anti-Fraud Command Center is staffed by an experienced team of fraud analysts who work to 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 from approximately 115 hours to 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.



Uri Rivner, Head of New Technologies,
at the RSA Anti-Fraud Command Center



The Security Division of EMC

Fraudsters Launch Social Engineering Scams and Manipulate Media Websites: The “Cease-Fire Trojan Attack”

On January 7, 2009, the RSA Anti-Fraud Command Center first discovered a social engineering scam designed to lure people via an email spam attack to a fake news website designed to look like CNN.com. RSA named this the “Cease-Fire Trojan Attack” and it attempted to bait readers leveraging recent news and “graphic and striking” images regarding the Israel-Hamas conflict in Gaza. RSA located the domain hosted in China, and shutdown the attack.

On January 9, the RSA Anti-Fraud Command Center detected that the same gang of fraudsters responsible for the Cease-Fire Trojan Attack had registered five new domains and designed five new URLs – and were launching new waves of attacks targeted to their fake CNN.com news webpage. RSA shut down this second Cease-Fire Trojan Attack within a period of four hours.

The likely result of this attack upon its victims was the infection of their computers with a Trojan. The attack began shortly after RSA’s discovery and the fake website was designed to look like CNN.com, *but was not a legitimate CNN.com webpage nor was it directly associated with CNN, its parent company, or its affiliates in any manner.*

The fake webpage (see next page), designed and hosted by the online criminals, was embedded as a link within the spam attack email (see next page). This fake webpage included another link to what appeared to be a legitimate video but was actually a form of crimeware. When visitors clicked on the video, they received a pop-up window containing a message informing them that they needed to install Adobe Flash Player version 10 in order to play the video, and a link was provided. *The fake download was created by the fraudsters and was not associated with Adobe Systems Inc. or its affiliates in any way.* The gang behind this Trojan is known by some who have blogged about its previous attacks.

The Cease-Fire Trojan Attack scam is yet another example of how adept fraudsters have become in engineering attacks with near real-time response to breaking news. It also underscores the opportunistic nature of fraud purveyors who increasingly prey upon public interest and/or concern regarding national or global events of broad importance such as the current worldwide economic crisis.

How a Trojan “SSL stealer” Works

The Trojan that is launched when a link to a fraudster’s fake Adobe Flash Player software update is accessed is called a Trojan “SSL stealer” and it captures financial and personal information of the infected user found on their computer. This particular Trojan is not new or a newly advanced piece of crimeware. What *was* new about the Cease-Fire Trojan Attack was the socially engineered application of this Trojan that exploits users concerned about the events in the Middle East.

By opening an executable file designed by the fraudsters and disguised as a legitimate Adobe Flash Player update, the user’s computer becomes infected with the Trojan. The SSL stealer is generic. Instead of being activated by a trigger-list containing specific URLs; it is activated by any URL that uses the HTTPS protocol.

As soon as users access a website over an HTTPS connection, the Trojan is called into action. When users start entering data into SSL-protected websites, the Trojan collects the data via the users’ web browsers. And this can happen on any website in both the public and private sectors. The Trojan invisibly intercepts the data and sends it to the criminal’s drop zone – *before* the data becomes SSL-encrypted. The criminals therefore receive unencrypted data, including usernames and passwords. The data is then encrypted using SSL or TSL, and sent to the legitimate website. Most unfortunately, this type of hidden interception of data via users’ web browsers is not readily discernible by victims of this Trojan horse.

Late January 2009 Attack Launched by Same Gang behind Cease-Fire Trojan

On January 26, 2009, the same gang behind the Cease-Fire Trojan launched a very similar Trojan attack. This time, the fraudsters lured users via another spammed email to visit yet another fake news website (see next page) again of their own design and meant to look like the Swiss website 20 Minuten. *The fraudster’s website was not associated with the legitimate website 20 Minuten or any of their affiliates in any way.* This time, the social engineering “lure” was an article concerning a recent increase of prostitution in Switzerland.

The gang copied the article from the authentic news webpage. And also just like their Cease-Fire Trojan, the fraudsters embedded a pop-up window to a fraudulent and fake Adobe Flash Player update. The associated and completely fake download was not a product of Adobe Systems Inc. or its affiliates in any way. Just like the Cease-Fire Trojan, the pop-up did not exist in the legitimate news article.



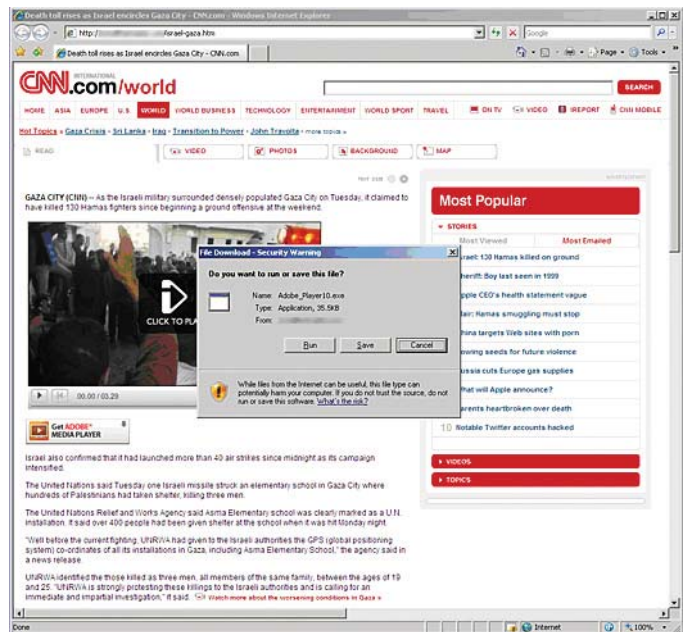
Israel offers short respite from strikes

Israel will halt its bombardment of Gaza for three hours every day to allow residents of the Hamas-ruled Palestinian territory to obtain much-needed supplies, a military spokesman says. The images broadcast here were graphic and striking. The Al Jazeera English report below captures the extent of the devastation caused by the initial strikes.

<http://edition.cnn.com/2009/WORLD/meast/01-07.bigvideo.2009.israel.and.gaza/index.html>

2009 Cable News Network. A Time Warner Company. All Rights Reserved.

The Cease-Fire Trojan Attack: The link within the spammed email was fake and fraudulent – and after clicking the link within the email, the browser opened the fake and fraudulent web page that could have led to an unknown download of the Trojan.



Contrary to this online gang's previous attacks, which up until recently only targeted the U.S. with attacks disguised by fraudsters as email communications from media websites like CNN.com or social networking websites like Classmates.com, the gang is now casting its net over other regions of the globe. The RSA Anti-Fraud Command Center informed the Swiss CERT of the offending domains that hosted this attack.

RSA's Call to Action

These social engineering scams launched by fraudsters are a call to action for Internet users to remain vigilant and educated regarding the latest online threats – as infection by these Trojans are accomplished via a silent “drive-by-download” infection kits such as Neosplit, or via social engineering scams like the ones RSA detected, shutdown and/or reported in January 2009.

As such, RSA cautions Internet users both at home and in the office to be cautious when tempted to click on links within emails from unknown individuals or organizations. Clicking on these links may result in directing the user to a fake website that can inject an infection into their computer and a compromise of their personal or their company's data.

It is a best practice for Internet users to be wary of all unsolicited emails that request personal or business information, or entice them to look at something online considered interesting. This is especially important if an email seems normal or routine, such as those that arrive from a friend, financial institution, or a social networking website.

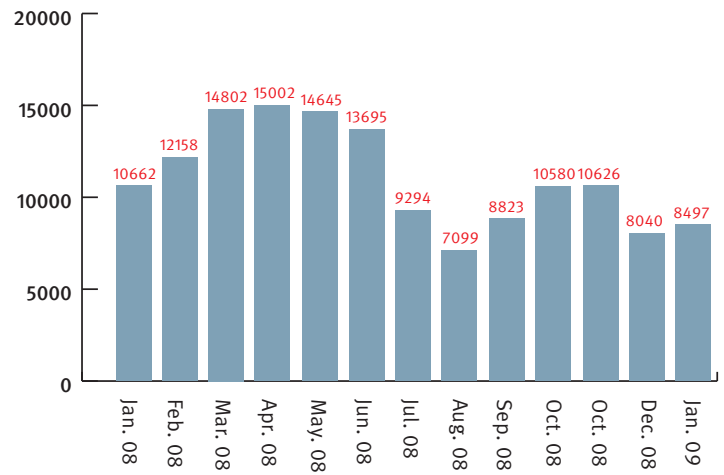


Total Number of Phishing Attacks Detected by the RSA Anti-Fraud Command Center

Trend Analysis

The year 2009 began with a slight increase in the total number of phishing attacks detected by the RSA Anti-Fraud Command Center. The number of attacks that were directly instigated by the Rock Phish gang, combined with other fast-flux attacks, rose by 20%. This constituted most of the increase in phishing attacks over the course of January.

Similar to December 2008, Rock Phish and fast-flux attacks continued to make up approximately 30% of the total number of attacks. The RSA Anti-Fraud Command Center has now shut down over 125,000 phishing attacks to date.



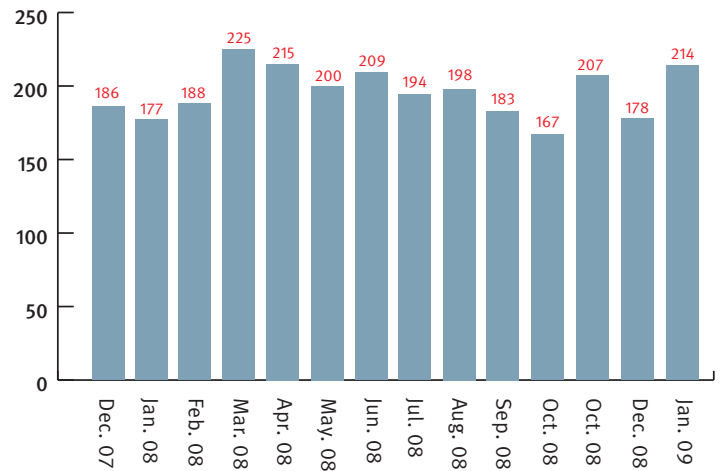
Source: RSA Anti-Fraud Command Center

Total Number of Brands Attacked

Trend Analysis

During January 2009, there were 214 attacks against financial institutions and other brands – the highest number since April 2008. In addition, the total number of attacked brands increased a significant 17% when compared to December 2008. Over the course of January 2009, twenty-one new brands were attacked that had never been attacked before.

Since the Rock Phish Gang and other fast-flux networks only accounted for two different attacks, the high number of new attacks may indicate that fraudsters who launched “standard” attacks are now attempting to cast a wider net over new targets. Based on the peaks of the total number of attacked brands in March and April 2008, it remains to be seen whether or not online fraudsters will attempt to attack a higher number of brands over the course of 2009.



Source: RSA Anti-Fraud Command Center



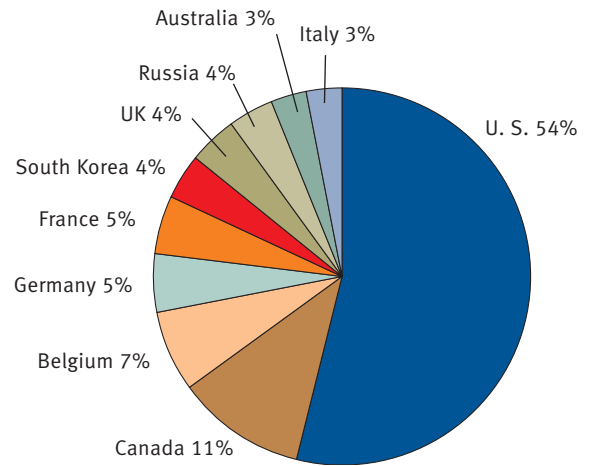
Top Ten Countries Hosting Phishing Attacks

Trend Analysis

Fraudsters within the United States continue to host the most phishing attacks (as enumerated by the location of the ISP or the hosting company). However, the U.S. share within the global figure dropped below the 60% mark in January 2009, after three consecutive months above that figure.

Canada passed a milestone usually held by countries in second place on this list - hosting more than 10% of attacks. Canada hosted 11% of online attacks during January 2009. France had previously placed second on the list in December 2008 and hosted 8% of that month's attacks, but decreased to 5% of the total attacks and landed in fifth place on the list in January 2009.

By registering numerous phishing domains in Belgium, the Rock Phish Gang enabled that country's strong entrance into the top ten, landing at third place by hosting 7% of the total number of attacks. New to the list in January 2009 were Belgium and Italy at third and tenth place respectively. Pakistan and China fell off the list completely in January.



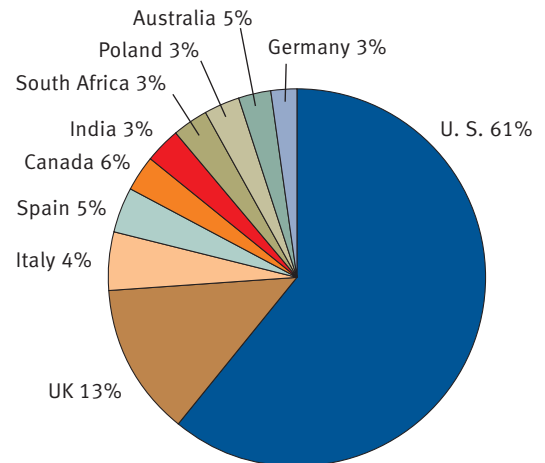
Source: RSA Anti-Fraud Command Center

Top Ten Countries by Attacked Brands

Trend Analysis

The United States and the United Kingdom still endured the largest portion of financial institution and other brands attacked worldwide during January 2009, with a combined total of 74%.

Italy placed third on the list, while Canada moved from that spot in December 2008 down to fifth place in January 2009. Colombian and Mexican brands were able to evade the top ten list altogether in January 2009. Poland (sixth place) and Germany (tenth place) were both back on the list in January 2009 after a two month and five month absence, respectively.



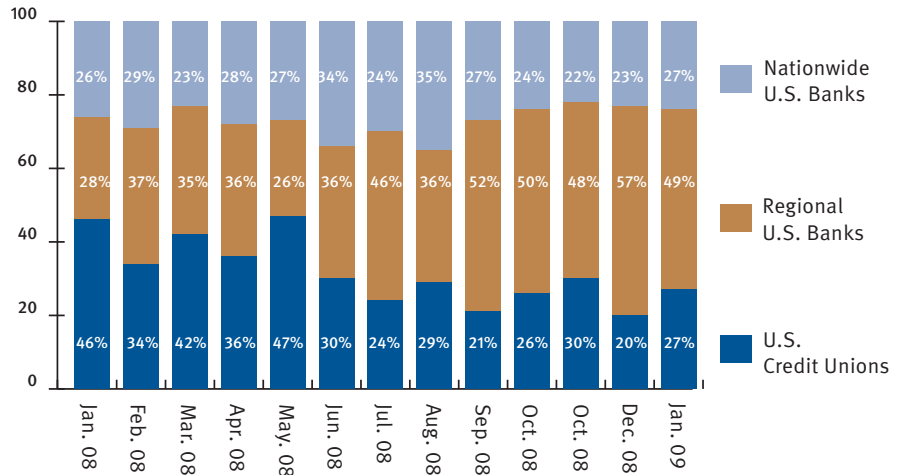
Source: RSA Anti-Fraud Command Center

Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis

The rate of attacks against regional U.S. bank brands maintained an eight month lead heading into 2009 as the most targeted type of U.S. financial institution. However, the rate of attack against regional U.S. banks declined by 6% in January 2009 when compared to December 2008, and now accounts for 49% of the total.

The share of nationwide US bank brands attacked during January 2009 increased by only 1% over December 2008 – maintaining a rate of the share of the total attacks that has changed no more or less than 3% since September 2008. During January 2009 the rate of attacks upon U.S. credit unions increased by 7% when compared to December 2008.



Source: RSA Anti-Fraud Command Center



The Security Division of EMC

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

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 0109