

RSA Online Fraud Report

November, 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 almost 300 institutions worldwide. The AFCC has shut down over 117,000 phishing attacks to date and is a key industry source for information on phishing and emerging online threats.

The following statistics have been gathered from the RSA Anti-Fraud Command Center phishing repository. Each statistic includes a short trend analysis based on the expertise of the fraud analysts within the RSA Anti-Fraud Command Center.

New Phishing Kits Hit the Market: Trojan HTML Injections Now for Sale

The economic lifecycle of the underground fraud community functions very similarly to the world of legitimate business. Online fraudsters have supply chains, third-party outsourcers, vendors, and online forums where people with skills and people with opportunities to commit fraud can find each other. The underground fraud supply chain is becoming more technically and operationally sophisticated, and RSA has coined this "Fraud-as-a-Service" or "FaaS". FaaS consists of services for advanced hosting, Trojan infection kits and cashout services – all for sale within the fraudster underground.

Some fraudsters have developed websites to sell ready-made products to other fraudsters, such as phishing kits. Recently, the RSA Anti-Fraud Command Center traced a new type of service on a particular website to sell HTML injections, which can be combined with Trojan attacks. We will refer to this website as a Web Injection Shop.

HTML injections are not a new approach to stealing credentials and other personal information. However, the production-scale central repository for HTML injections in the Web Injection Shop is a new discovery, and is easily accessible by fraudsters. The Web Injection Shop that was traced is very similar to other websites that sell phishing kits and offers a long list of HTML injection codes designed to steal information from customers of dozens of financial institutions worldwide. Similar to phishing kits, each HTML injection is specifically tailored to match each bank's specific website design.



The Security Division of EMC

The Web Injection Shop offers HTML snippets, as well as entire web pages, designed to fool online banking users into divulging their credentials and other personal information. Prices vary by target and HTML injection type – ranging between USD\$10-30 – and fraudsters can browse through screenshots of various HTML injections that are for sale.

About HTML Injections

Many well-known types of Trojans – such as Zeus, Sinowal, and Limbo – feature HTML injection capabilities. They effectively inject new web pages through the browser and add new fields seeking credentials and other personal information that the bank would never request from its customers through its own legitimate web pages. However, the injected web pages look like legitimate web pages to the average online banking user. It is an effective way for fraudsters to receive more details from a victim of online crime than employing key logging or intercepting web traffic.

The Sinowal Trojan, for example, has a very large pool of HTML web pages to inject into numerous different domains within its list of triggers, allowing it to collect vast amounts of information regarding its infected users. Examples of fields that can be requested are “SSN”, “TAN”, “ATM PIN”, and other credentials and personal information. The elements which Trojans inject into the page are customized for the specific financial institution under attack, to match the design and context and to appear as seamless as possible.

The Web Injection Shop (see graphic below) offers two types of HTML injections. The first is “in-page HTML modifications”, designed to seamlessly merge within a bank’s web pages,

requesting that the user provide additional information such as their social security number, mother’s maiden name or ATM PIN code. The second type of HTML injection is a complete web page that is inserted locally into the user’s browser on the infected PC, once again requesting extra information from the user.

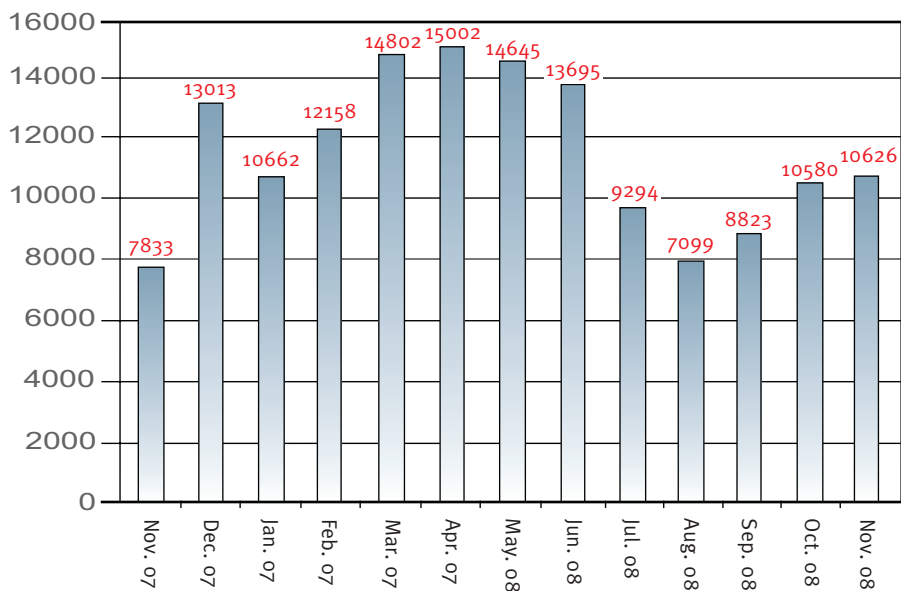
The “Balance Grabber”

The Web Injection Shop also sells a product called a “Balance Grabber”. Once users successfully log into their bank account, this particular piece of code runs locally on their PCs and seeks out the bank account’s balance field. When this “grabber” locates the balance field, it copies it and sends it to the fraudster’s drop server. In this way, fraudsters can get an account balance without actually entering the account itself. In this way, fraudsters can see the account balance without actually entering the account itself. Or, if they plan to sell the login credentials to another fraudster who specializes in cashing out funds, they can charge a fee for an account according to its balance.

The Web Injection Shop is perhaps the newest addition to a long list of fraudster commodities, such as payment card and bank account data sold by the batch. Phishing kits are now sold at low prices or sometimes given away for free. HTML injections could follow the path of phishing kits, at first selling at relatively high costs due to market demand and lack of availability. And when the fraudster market is saturated by HTML injection offerings, their price may drop since HTML pages are fairly simple to design.

Source: RSA Anti-Fraud Command Center

Фильтр		Маска		Описание	Скриншот	Цена	Купить
ID	Страна/Ресурс	Ресурс	Маска				
111	-	albergold.com	albergold.com	Запрашивает email и второй пароль от Alter Gold	Collects Email and 2nd password from Alter Gold	Примерно 12.00\$	<input type="checkbox"/>
5	-	albergold.com	albergold.com	Собирает email и второй пароль от e-Gold	Collects email and second password from E-Gold	Примерно 6.00\$	<input type="checkbox"/>
3	-	albergold.com	albergold.com	Собирает email и второй пароль от e-gold	Collects Email and 2nd password from E-Gold	Примерно 6.00\$	<input type="checkbox"/>
4	-	albergold.com	albergold.com	Собирает DOB (дата рождения) и номер банковской карты	Collects DOB from MoneyBooks	Примерно 20.00\$	<input type="checkbox"/>
117	-	albergold.com	albergold.com	Запрашивает номер баланса и статистику (Verified, Unverified) аккаунта PayPal	Logs PayPal balance and status	Грайфер 0.00\$	<input type="checkbox"/>
119	-	albergold.com	albergold.com	Собирает данные об активности аккаунта: логин, пароль за последние 30 дней	Collects account activity info	Грайфер 0.00\$	<input type="checkbox"/>
20	-	albergold.com	albergold.com	Собирает данные об адресе аккаунта: ТО ПИН/КО При входе копирует на сервер стравилку	Collects account activity info	Грайфер 0.00\$	<input type="checkbox"/>
76	AU	albergold.com	albergold.com	Грайфер баланса	Balance grabber	Грайфер 0.00\$	<input type="checkbox"/>
76	AU	albergold.com	albergold.com	Грайфер баланса	Balance grabber	Грайфер 0.00\$	<input type="checkbox"/>
77	AU	albergold.com	albergold.com	Грайфер баланса	Balance grabber	Грайфер 0.00\$	<input type="checkbox"/>
74	AU	albergold.com	albergold.com	Грайфер баланса	Balance grabber	Грайфер 0.00\$	<input type="checkbox"/>
70	BO	albergold.com	albergold.com	Запрашивает поле TAN и проверяет его на валидность	Creates "TAN" field and validates inserted info	Примерно 15.00\$	<input type="checkbox"/>
110	BY	albergold.com	albergold.com	Выдает поле email и проверяет его на валидность	Asks for email and validates inserted info	Примерно 20.00\$	<input type="checkbox"/>
117	BY	albergold.com	albergold.com	Запрашивает поле "Идентификационный Код" и проверяет его на валидность	Asks for "Firm" and validates inserted info	Примерно 20.00\$	<input type="checkbox"/>
144	BY	albergold.com	albergold.com	Запрашивает email и проверяет его на валидность	Asks for "Firm" and validates inserted info	Примерно 20.00\$	<input type="checkbox"/>
142	BY	albergold.com	albergold.com	Грайфер	Grabber	15.00\$	<input type="checkbox"/>
117	CA	albergold.com	albergold.com	Запрашивает поле Access Code	Creates "Access Code" field	Примерно 10.00\$	<input type="checkbox"/>
100	CA	albergold.com	albergold.com	Грайфер статистики аккаунта	Account statistics grabber	Грайфер 0.00\$	<input type="checkbox"/>
71	DE	albergold.com	albergold.com	Запрашивает TAN для ctaibank.de и проверяет поле на валидность	Asks for TAN for Ctaibank.de and validates info	Примерно 15.00\$	<input type="checkbox"/>
72	DE	albergold.com	albergold.com	Запрашивает поле Trader Password и делает проверку ввода ввода	Asks for "Trader Password" and validates user authentication (Login, pass, identifier, Login (little Trader Password examples))	Примерно 20.00\$	<input type="checkbox"/>
73	DE	albergold.com	albergold.com	Запрашивает TAN и проверяет его на валидность	Asks for TAN and validates info	Примерно 20.00\$	<input type="checkbox"/>
65	DE	albergold.com	albergold.com	Запрашивает поле Firma и делает проверку ввода	Asks for "Firma" and validates info	Примерно 15.00\$	<input type="checkbox"/>
128	ES	albergold.com	albergold.com	Запрашивает поле Firma и делает проверку ввода	Asks for "Firma" and validates info	Примерно 20.00\$	<input type="checkbox"/>
91	ES	albergold.com	albergold.com	Запрашивает поле Firma и делает проверку ввода	Asks for "Firma" and validates info	Примерно 15.00\$	<input type="checkbox"/>

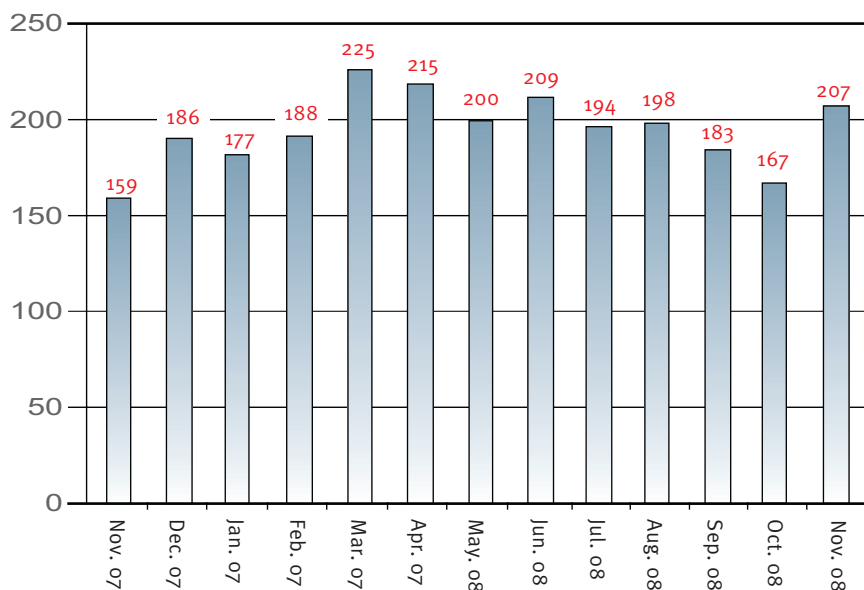


1. Total Number of Phishing Attacks

Trend Analysis

After a steady and remarkable increase in phishing attacks from August through October 2008 (an increase of 3481 attacks in total), the rate of increased phishing attacks between October 2008 and November 2008 slowed down dramatically – increasing only by 46 attacks.

In addition, the number of fast-flux attacks by the Rock Phish Gang and others dropped slightly during November 2008. Attacks initiated by groups outside of the Rock Phish Gang are still on the rise, mapping to trends from previous months, with November reaching the highest numbers to date.



2. Number of Financial Institution Brands Attacked

Trend Analysis

November 2008 marked a significant increase in the number of banking brands attacked - nearly 20%. The increase of brands attacked (40 in total) signifies the most substantial short term change in the number of brands attacked over the 12 months.

Also, the number of brands attacked during November 2008 was the fourth highest during the last 12 months. During November 2008, the RSA Anti-Fraud Command Center detected attacks against 23 bank brands that had not been previously attacked.



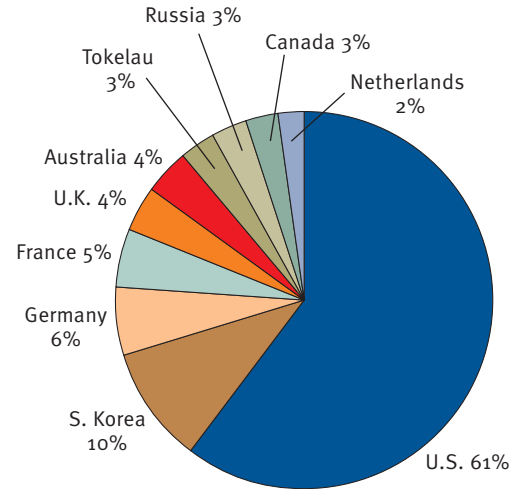
3. Top Ten Countries Hosting Phishing Attacks

Trend Analysis

During November 2008, the U.S. was once again the world's top hosting country for phishing domains - remaining steady with October 2008 with 61% of the total amount. By contrast, there is more than a 50% drop between the U.S. and the next country on the list, South Korea.

Comparing November 2008 to October 2008, South Korea and Germany retained their exact same positions on the chart. The top three countries have maintained their respective positions over the past 4 months. France, United Kingdom, Russia, the Netherlands and Canada retained steady positions compared against October 2008 – shifting by no more than +/- 1% of the total amount of hosted phishing domains. November's newcomer was Tokelau, a territory of New Zealand, landing at 7th place with 3% of the total amount of hosted phishing domains.

In November 2008 Australia is back on the list – tied for 5th place with the United Kingdom (both receiving 4% of total phishing attacks) – while China fell off of the list in November, after placing 7th in October 2008.

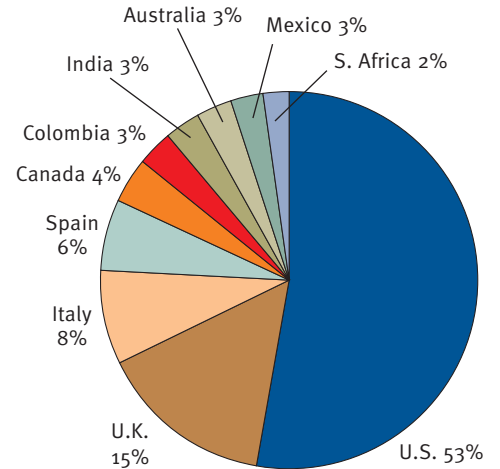


4. Top Ten Countries Most Targeted by Phishing Attacks

Trend Analysis

The U.S. continued to be the most widely targeted country in November, absorbing 53% of the world's phishing attacks. The U.K. was the second highest targeted country at 15%, and Italy was the third highest attacked country by phishing attacks at 8% - a significant increase of 3% over October 2008.

Other countries retained similar positions on the list with a change in rate of attack by +/- 1-2%. Colombia is back on the list in November 2008, while Poland fell off of the list completely. With the addition of Colombia, there are now two countries in Latin America on the top ten list of attacked countries, with Mexico being the second.



5. Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis

The rate of attacks within the three key segments of U.S. financial institutions during November 2008 remained quite steady when compared against October 2008. During November 2008 Regional U.S. Banks remained the most targeted, accounting for nearly half of the U.S. financial institutions attacked during the month, and down only 2% from October 2008.

The percentage of U.S. Credit Unions under attack rose by 4% in November, while the rate of attacks against Nationwide U.S. Banks decreased by only 1%.

