

RSA Online Fraud Report

August, 2010

Prices of Goods and Services offered in the Cybercriminal Underground

Online forums serve as platforms for cybercriminals to exchange their criminal tools, services, and know how; but even more so, forums are flourishing markets used by those who profit from the sale of compromised bank accounts and payment card data. In order to keep feeding the cybercrime economy, vendors of compromised data mainly¹ obtain their “merchandise” by launching phishing and Trojan attacks or hacking into merchants’ databases; they then offer the harvested data for sale in a varying number of underground forums.

¹ Other sources of compromised data may also include hacked payment processing systems and skimmers placed by fraudsters on POS devices and ATM machines.

If you were to take a glimpse into the fraud black market, you would see that not only do cybercriminals trade stolen data, but they also offer a multitude of tools and services for sale that enable others to harvest this information and/or monetize it. Examples of some criminal ‘product’ offerings would include fraudster call center services that “outsource” fraudulent phone calls made to banks or merchants; information services that provide a rich set of personal and financial data on potential victims; phishing kits that target different banks; Trojan infection kits; and credit card checking services, just to name a few.

For the purposes of our research, the RSA FraudAction Intelligence Team has gone out “shopping” in the larger underground forums where a variety of goods and services are offered for sale. Today, we bring you an up-to-date shopping list straight from the underground cybercriminal market, along with the corresponding price tags as advertised in the major online fraudster forums. We’ve also outlined several hypothetical scenarios we’ve developed in order to help illustrate the potential impact of this fraud marketplace.

Example Scenario #1

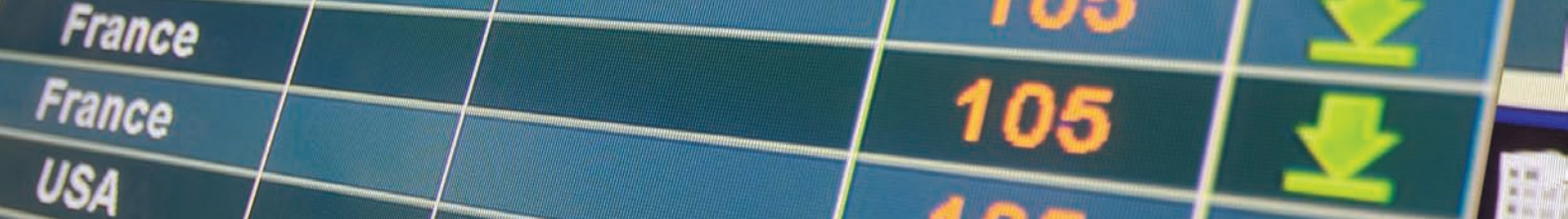
A would-be cybercriminal browses the Internet and reads how lucrative the botnet business can be for individuals with minimal technical computer savvy. After deciding to proceed with the ‘fraud business plan’ – he goes shopping in the underground. Here’s a look at his shopping list:

- One powerful banking Trojan (Zeus) with a full builder and extra plugin options: \$4,000 to start
- One month of bulletproof hosting – up to \$400 per month
- One infection campaign via e-mail (spam blasting) – Approximately \$70 per campaign with CAPTCHA circumvention option included

Total estimated startup cost: \$4,470

Credential harvesting potential: Limitless





How does this would-be cybercriminal set his wares in motion? He promptly launches a Trojan infection campaign, and potential victims begin accessing the infected URL, inadvertently getting the cybercriminal's Trojan variant installed on their computer.

The cybercriminal now begins building his new botnet as more and more victims fall for his tricky e-mail messages and continue browsing to the compromised site (often referred to as the "infection point").

In just a matter of time, victims will access their online banking services and all their login credentials will get captured and transmitted from their PCs directly into the cybercriminal's drop server. Whether he decides to sell these credentials to other cybercriminals or uses them to commit fraud himself is all up to the level of involvement he wants to partake in, the risks of getting caught – and how much profit he has his sights set on.

Example Scenario #2

A seasoned fraudster, well-versed in cybercrime techniques, begins planning his Christmas shopping for the year. He quickly opts for purchasing compromised "Fulls" or credentials, specifically those belonging to customers of large American financial institutions. This cybercriminal visits his trusted vendor to fulfill the following shopping list:

- 50 sets of freshly compromised "Fulls" credentials – \$ 500 on average
 - 30 fraudulent phone calls to online merchants, banks and money transfer services: \$300
 - Item drop mules as needed: Mule-herder is commission based
- Potential for big ticket item purchase and cash resale: Unlimited

How does this seasoned cybercriminal make a buck off of the "Fulls" credential sets he has obtained? He is able to use the genuine cardholder's information including online banking account (via username and password combination), billing address, credit card number, CVV2 code, expiration date, mother's maiden name (MMN), date of birth (DOB), and Social Security Number (SSN). Using the data, the cybercriminal can modify the card's billing address with the

help of a fraudulent call to the call center, buying credibility to a random item-drop address. He can then purchase big ticket items online, having them shipped to that same item-drop mule, then directly into his hands for cash resale in his own local grey market.

Shopping the Underground Market²

A stroll through some leading underground forums provided us with a complete cybercriminal shopping list. Overall, the list below reflects an accurate view of the prices of goods and services as they are currently sold in this black market. While prices vary, the list below offers a price range rather than one absolute market price and truly represents what cybercriminals illicitly buy and sell in order to carry-out their fraud operations both in the online realm and in the real world.

Looking at this non-exhaustive list one can review basic pricing of credit card data, customer credentials, crimeware, Phishing, hosting, private consumer information, etc. It is evident the fraud supply chain proves to work through a vast and vibrant underground market where a fraudster's key purpose is targeting the best avenue to maximizing his ROI.

A cybercriminal can procure credit card data for as little as the price of a latté. What may seem marginal enough at first sight may carry the potential for heavy losses to consumers, the banks and credit card associations involved.

Various fraud products and services are sold in the underground for not more than \$50, but can be associated with the loss of thousands of dollars in the end. Worse yet, in the case of consumers, one can never put a price tag on the loss of privacy.

Even when looking at the relatively high price of Trojans, which may cost up to thousands of dollars per kit, the initial cost is not very telling of the massive damage and monetary losses it is capable of perpetrating in a rather short time span.

Today, there are myriad underground forums operating throughout the world. Law enforcement and the security industry invest efforts in thwarting cybercriminal enterprises and turning this black market economy into an unprofitable business. A good example to demonstrate was the shutdown of the Dark Market forum in October 2008 by the Federal Bureau of Investigation, which ultimately resulted in 56 arrests and the prevention of \$70 million in potential losses.

² All prices quoted in US Dollars

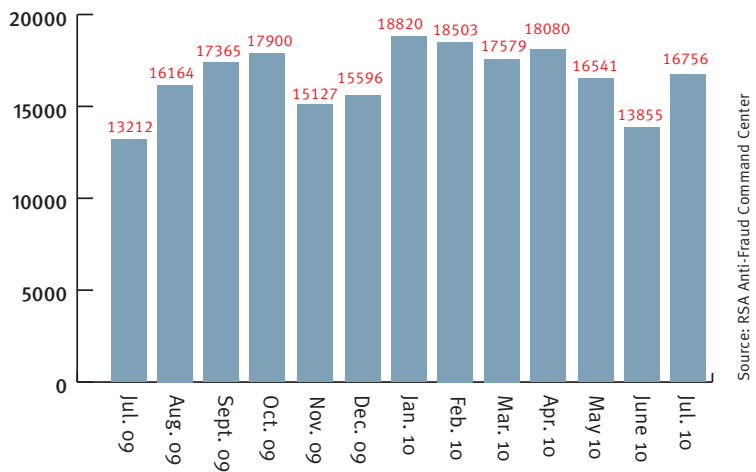


Sale Item	Underground Price
CVV2 Data Sets The CVV2 data set consists of a credit card's 16-digit PAN, CVV2 code, expiration date, billing address and embossed name. Fraudsters buy this data set in order to commit e-commerce (card-not-present) fraud, specifically buying merchandise online and then reselling it for cash.	\$1.50 - \$3.00
SSN / DOB / MMN These personal details are very often used by banks to authenticate an individual's identity in both the online banking and phone banking channels; also used by some money transfer services.	\$1.50 - \$3 per query MMN \$5 - \$6 SSN \$1 - \$3 DOB \$1 - \$3
Track 2 Data (aka "Dumps") 'Track-2' information is found on a payment card's magnetic stripe. By purchasing 'dumps', fraudsters can produce counterfeit payment cards that can be used in stores (aka 'carding'). This is done by encoding the data onto blank plastic cards or onto an old payment card.	Classic/ Standard cards: \$15 - \$20 <small>*Prices for these may be as low as US\$ 9 per card when buying dumps in bulk, with minimum bulk orders normally starting at purchases of \$200</small> Gold/ Platinum cards: \$20 - \$80 <small>**Prices may vary widely</small> Worldwide/ Business/ Corporate/ Signature: \$30 - \$40
Online Banking Logins Logins consist of a consumer's username, password, and in some cases additional information. After obtaining these credentials, fraudsters would normally attempt to cash the account out by completing wire transfers into mule accounts they control.	\$50 - \$1,000 per account, depending on the account type and balance.
'Fulls' Data Sets 'Fulls' information includes the full details of an account holder, such as a consumer's online banking credentials (e.g., username and password), mailing address, card number, CVV2 code, card's expiration date, MMN, DOB, SSN.	\$5 - \$20 per set
Fraudulent Phone Calls Completed by Fraudster Call Centers, fraudulent phone services are offered to cybercriminals as a means to overcome language and gender barriers encountered by those who need to impersonate the account holder	\$10 - \$15 per call Prices vary according to the destination of the call, for example: a call made to a mule, a bank's customer service center, or other destinations.
CC Checking/ Verification CC (credit card) checkers are used by cybercriminals to verify the validity of the compromised payment cards they obtain/ purchase in advance.	\$0.40 per check Prices may vary widely. \$20 for 50 checks
SMS or Phone-Flooding Services (aka Telephony DoS/ TDoS) Phone-flooding is usually performed in order to render a consumer's mobile phone unavailable for incoming authentication calls or SMS text messages sent from the bank.	\$25 - \$40 per 24 hours of phone-flooding
DDoS Attack Service A 'Distributed Denial of Service' attack is an attempt to make a computer resource unavailable to its intended users by overloading, or "flooding" its bandwidth with an overwhelming volume of web traffic.	\$50.00* per 24 hours of DDoS. <small>*Average price for DDoS'ing a site for 24 hours. The exact price depends on the DDoS'ed site</small>
Bulletproof Hosting Bulletproof hosting is a hired service used by cybercriminals to host malicious content. The main idea is suggested by its name: "Bulletproof" – much harder for law enforcement to take down than any other hosting method out there. BP infrastructures will host any and all criminal content.	\$87 - \$179 per month depending on the service level and up to \$400 per month for certain infrastructures.
Zeus Trojan Kit One of today's most pervasive banking Trojans. With an infection rate of thousands of computers per day, highly advanced features, evolving code, new variants and communication resources being detected and analyzed by RSA on an ongoing basis, it is the Trojan family most frequently encountered in the wild.	– Zeus Kit: \$3K - \$4K – Backconnect \$1500 – Firefox form grabber \$2000 – Jabber (IM) chat plugin \$500 – VNC (Virtual Network Computing) private module \$10K – Windows 7/ Vista Support \$2000 <small>*Note: Unauthorized Zeus variant copies sold in the underground would go for ~\$800</small>
SpyEye Trojan Kit One of the most advanced current-day Trojans, boasting its own IE and Firefox HTML injections, pre-defined bank triggers and a growing list of unique features. Thus far, SpyEye has been 2010's biggest Trojan innovation, being the only commercially available banking Trojan able to challenge Zeus' market-share.	– Basic kit – \$1,000 – Firefox Injection tool – \$1,000 - \$2000 – SOCKS plugin – \$750 - \$1750



Phishing Attacks per Month

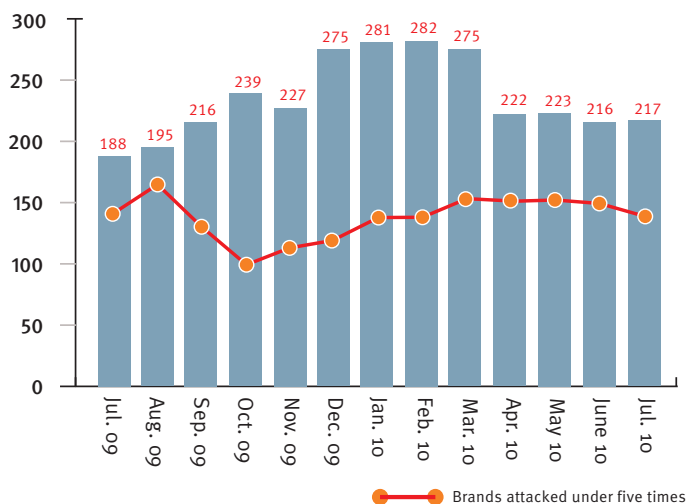
RSA witnessed a 21 percent increase in the number of phishing attacks launched worldwide during July 2010. While there was a sharp spike in phishing attacks, our analysis shows this growth can be directly attributed to an increase in the number of attacks launched against a handful of large entities. Attacks launched against US and UK-based financial institutions accounted for the majority of the increase witnessed in July.



Source: RSA Anti-Fraud Command Center

Number of Brands Attacked

Last month, phishing attacks were launched against 217 brands worldwide, an almost identical number compared to June. The number of brands targeted less than five times last month was also similar to the figures reported in June.

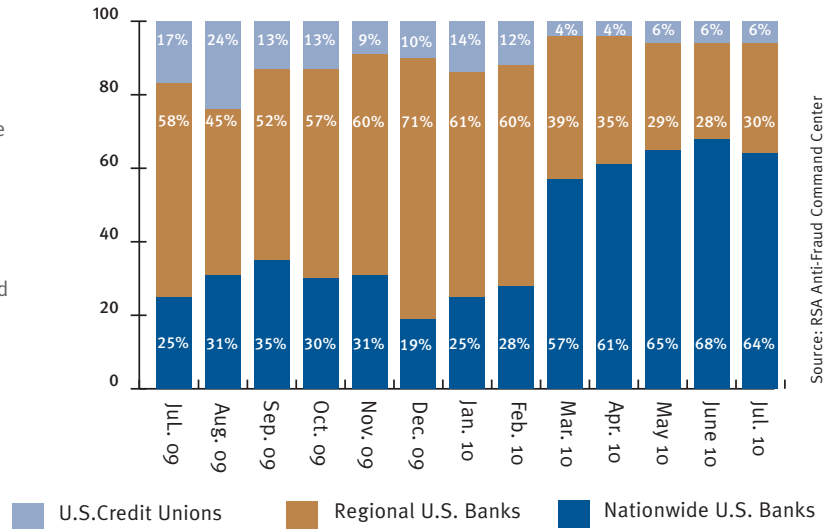


Source: RSA Anti-Fraud Command Center

Online Attacks

Segmentation of Financial Institutions Attacked Within the U.S.

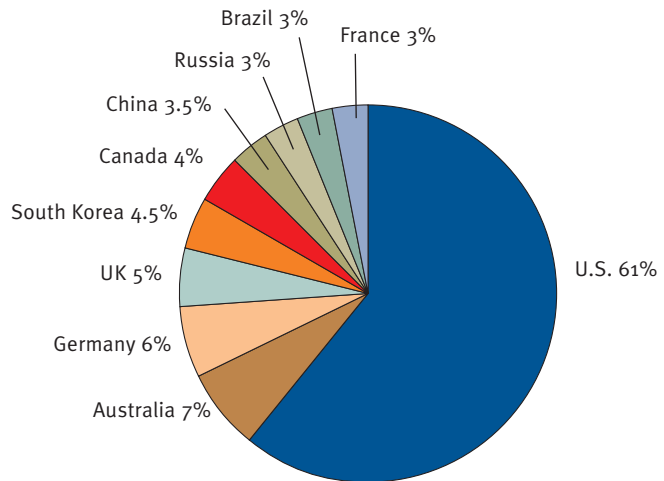
Despite a four percent decrease in July, nationwide banks remained the most targeted financial segment in the U.S. (in terms of the number of brands attacked). The portion of regional banks attacked increased four percent while the portion of targeted U.S. credit unions remained unchanged for the third consecutive month.

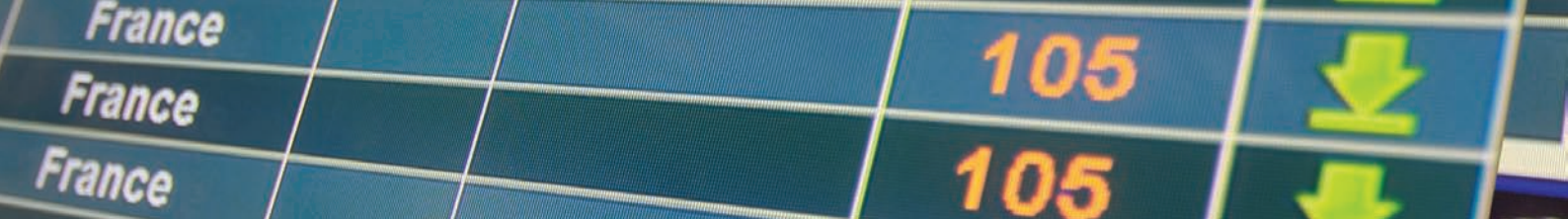


Top Ten Countries Hosting Phishing Attacks

The U.S. remains the country hosting the largest portion of phishing attacks; in July, the U.S. hosted 61 percent of phishing attacks. All other hosting countries reported have remained much the same with the exception of Brazil, who became a top country, hosting three percent of phishing attacks in July.

Source: RSA Anti-Fraud Command Center

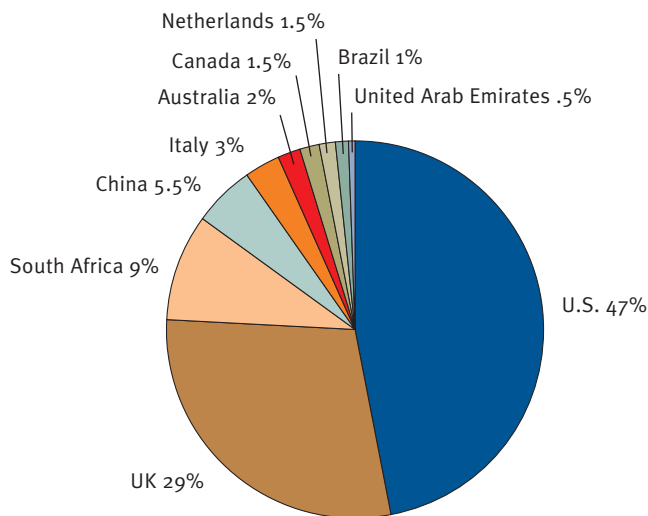




Top Ten Countries by Attack Volume

The volume of phishing attacks endured by the U.S. increased by eight percent from last month, representing 47 percent of all phishing attacks in July. The UK and South Africa endured a smaller portion of attacks, both dropping four percent from June. The United Arab Emirates appeared on the chart this month as one of the countries suffering a high volume of phishing attacks; it is the first time it has appeared on the chart since November 2009.

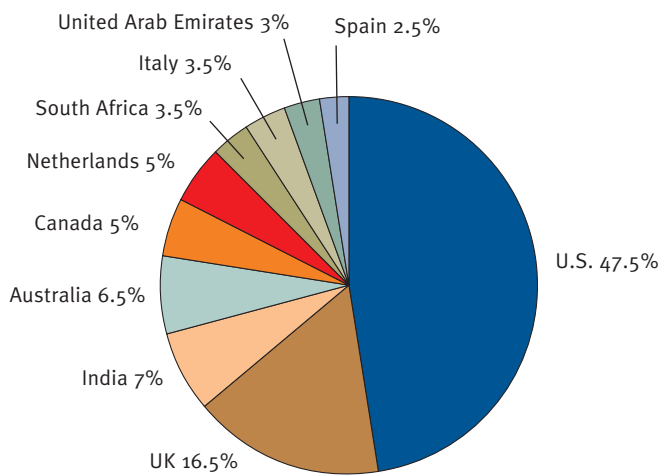
Source: RSA Anti-Fraud Command Center



Top Ten Countries by Attacked Brands

Phishers continue to heavily favor targeting U.S. brands; nearly half of all brands targeted in July were in the U.S. Together, the U.S. and UK continue to represent about two-thirds of all targeted brands. The United Arab Emirates is a newcomer to the list, with their brands suffering about three percent of identified phishing attacks in July.

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.