



# The Last Refuge of Scoundrels

**Linda Punch**

**The good news is that the once shadowy world of criminal sites that buy and sell stolen card and bank-account data isn't so shadowy any more. The bad news is that these bad-guy bazaars are devilishly hard to shut down.**

**L**ike many other Web merchants, GoldenDump.com has a home page promoting special discounts on featured products, a short list of prices, and a brief history of the company written by site owner "Pit Braidy." But GoldenDump.com is far from being the typical Web retailer. Instead of clothing, electronics, books, or other goods or services, GoldenDump.com specializes in selling stolen credit card data.

GoldenDump is just one of hundreds or more Web sites and chat rooms where stolen credit card data are sold for prices ranging from as little as 50 cents per account to \$30 or more. These underworld marketplaces constitute a cyber black market that thrives by selling credit card account numbers, bank-account numbers, and other confidential information stolen worldwide through data breaches, phishing attacks, and similar fraudulent actions. They also peddle malware technology and so-called "kits" that enable others to steal confidential data.

Just how many sites exist in this underground economy is difficult to determine. Web sites and servers operated by these so-called carders have

according to Symantec Enterprise Security, Cupertino, Calif. By the time law-enforcement officials discover sites, carders often have shut down and moved to other locations on the Web.

"I don't think anybody knows how many are out there," says Johannes Ullrich, chief technology officer, SANS Technology Institute, Bethesda, Md. "There appear to be hundreds. Sometimes it's hard to tell which ones are actually legit. There's actually fraud against fraudsters going on—people selling fake credit card numbers."

Equally hard to determine is how much money changes hands on these sites.

"We believe it's an approximately \$1 billion market," says Joram Borenstein, senior product marketing manager of the identity and assurance group at Bedford, Mass.-based RSA, known as The Security Division of EMC. "The industry vibe is that there are approximately two dozen very active and reliable sites that are used by the criminals in a variety of languages."

## **No 'Rookies'**

The breadth of the cyber black market is startling. In a study of underground

2007 and June 30, 2008, Symantec observed 69,130 distinct active advertisers and over 44 million total messages. The top 10 most active advertisers accounted for 11% of the total messages posted, with six of the top 10 listing credit card information as their top category for sale.

The potential value of advertised goods observed for the 10 most active advertisers totaled more than \$575,000 for the period, Symantec says. The potential worth of credit card information and bank-account credentials held on the servers of the 10 most active advertisers was \$18.3 million.

The size of some of the networks also is staggering. One of the largest Internet relay chat, or IRC, networks observed by Symantec had about 28,000 channels and 90,000 users at one point. One of the smallest underground economy servers had five channels and 40 users.

With the exception of a few high-profile carders, the identities of the site operators are largely unknown. Some sites appear to be operated by individuals while others are run by groups. In some cases, the operators of the sites committed the data breaches or phishing attacks that are the source of the numbers. In others, they're simply serving as the online middleman.

The type of operator behind a site seems to vary by region, the Symantec study found. America and India

groups operating out of North America tend to be loosely organized, often made up of acquaintances who met in online forums or IRC channels.

Nevertheless, the Web operators are highly skilled at acquiring and selling confidential information.

Bestuzhev, senior virus analyst at Kaspersky Lab, Woburn, Mass. "It is usually not just one individual behind the markets, [but] rather a group of people. And each member of the group is specialized in their area of the business."

by Symantec, credit card information topped the list at 31% of the total. It was also the most requested category, accounting for 24% of all goods requested.

The second most common category was financial accounts, with 20% of the total. This category included bank-account credentials, magnetic-stripe skimming devices, online payment services, online currency accounts, and online stock-trading accounts. Bank-account credentials were the most popular item for sale, accounting for 18% of the items advertised, according to Symantec.

The third-ranked category of goods and services was spam and phishing information, representing 19% of the total.

"There are different kinds of credit card shops depending on what you're looking for in terms of conditions, services, size, and even additional services, like offering stolen PayPal accounts, eBay accounts, Rapidshare [file hosting] accounts, ICQ accounts and so on," Kaspersky Lab's Bestuzhev says. "It is quite a well-organized group of people who focus on all the needs of their customers."

### 'Not Scared'

Stolen data sold on sites include names, addresses, driver's license numbers, Social Security numbers, credit card numbers, and many other types of personal information. "Some of them have a little bit of everything, some specialize," says Marc Fossi, manager of research and development, Symantec Security Response.

The sites also often sell kits that other criminals can use to steal information, Fossi says.

Prices typically range from \$1 for a credit card number and address to up to \$10 or more for complete identification information, such as

Free to attendees who register before Jan. 15  
with a room reservation

# Northeast Acquirers Association



## 2010 WINTER SEMINAR

January 26-28, 2010 at Mount Snow, Vermont.

The only conference this year in the Northeast

The original MLS event

Hot topics that impact your business

Snow Barn event sponsored by



Join The NEAA in picturesque Mount Snow, Vermont for our 2010 Winter Seminar and Outing. The NEAA is the foremost educational forum for financial institutions and every ISO/MSP/MLS in the acquiring industry. Our events are widely recognized for their educational value, top vendors exhibiting and exciting recreational activities. This seminar will prove to be the best yet!

### NEAA: A Tradition of Excellence

The Northeast Acquirers Association (NEAA), founded by dedicated experts over 20 years ago, has established itself as a foremost educational institution for ISO/MSPs in the acquiring industry. The NEAA is a non-member not-for-profit association that is best known for the informative and stimulating seminars it hosts on a biannual basis.

**DON'T MISS THIS ONE-OF-A-KIND EVENT!**

For information and registration material, please

security features are present on the card. "Let's say the Euro classic card or gold card doesn't have as much security as the USA classic or USA gold," says Sean-Paul Correll, threat researcher at Bilbao, Spain-based Panda Labs. "The value of that card would be higher because it's more

U.S. credit cards—which are the most common—are priced lower than cards from other countries. "I saw one card for the United Arab Emirates selling for more than \$30 because of the rarity," he says. "Cards from the European Union sell for more than cards from the U.S."

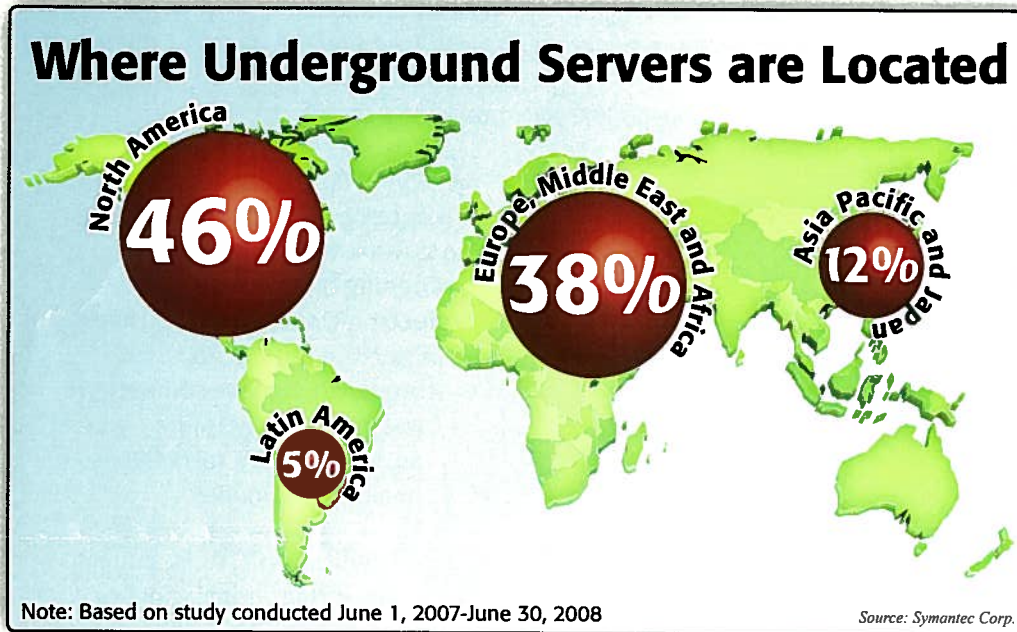
pages of results with a Google News Group heading the list.

"This is a news group discussion from cybercriminals somewhere in Russia offering their services of selling credit card data," Correll of Panda Labs says. "Obviously, they're not scared. They're not trying to hide

their communications as well as they could."

Indeed, at the Golden Dump site, Pit Braddy makes no effort to hide his illegal products:

"I am the credit card dumps seller. Our team skim (sic) dumps all over the world and sell (sic) them to you. Every few days we have a lot of fresh credit card dumps AA and AAA quality. We have usa/eu/Canada/asia/latin, etc. dumps. We occupy leading positions in this business. I hope you have pleasure (sic) working with us!"



likely that you'll be able to extract more money from it."

Card-account numbers accompanied by information such as the card-verification value, the cardholder's birth date, and Social Security number fetch a higher price than an account number alone, RSA's Borenstein says. "Those latter two pieces of information are very helpful if a criminal wants to call into a call center to authenticate himself to try to increase a credit line or something of that sort," he says.

And as with many other products, credit card account numbers sold in bulk bring lower prices. "The more you buy, obviously, the cheaper it gets," Correll says.

On the sites observed by Symantec, credit card account numbers sold for between 50 cents and \$12 per card

Sellers of card information also often will trade account numbers for malware tools, such as a new phishing kit for credit card account numbers, Fossi says.

Symantec estimates the value of goods advertised on the sites it observed totaled more than

## 'I am the credit card dumps seller. Our team skim dumps all over the world and sell them to you.'

\$276 million for the reporting period, with credit card information accounting for 59% of the total.

Finding the Web sites that sell credit card account data can be as simple as typing "credit card dump," "CVD" or the full name of a

### **Evasive Tactics**

But because law enforcement has closed down several carder Web sites, crooks increasingly are turning to Internet relay chat, or IRC, to exchange information and sell goods, Symantec's Fossi says.

"They set up a new channel on a large IRC site and might escape notice for awhile," he says, adding that once the new channel becomes too busy or it becomes clear too many people know about it, the carders shut down

# Revolutionary Magazine

We go to the players who are making revolutionary change happen. Subscribe to Digital Transactions today.

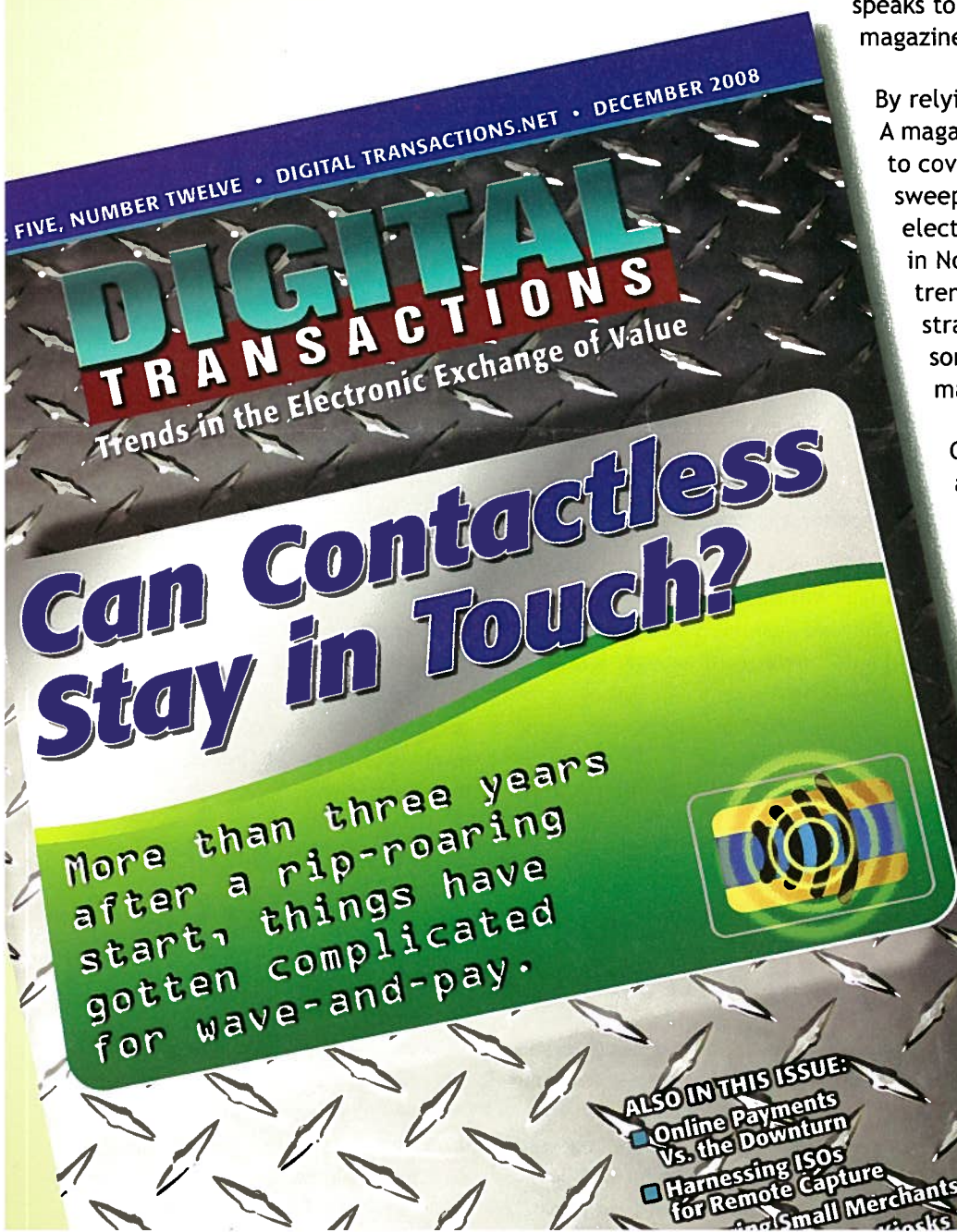
Go to [www.digitaltransactions.net](http://www.digitaltransactions.net) and hit "Subscribe."

That's why we created Digital Transactions. The consumer payments market isn't what it was five years ago. It's not even what it was five weeks ago. You know that. But how can you be sure you're really staying on top of this fast-changing market? Getting the latest and best insights on competitive strategies, the most informed analysis of market moves and trends. From a single publication that understands this market and speaks to its key players as no other magazine does?

By relying on Digital Transactions. A magazine created specifically to cover the dizzying change sweeping over the consumer electronic transaction business in North America. To cover trends. To explain competitive strategies. To help busy executives sort out reality from hype, and make more money.

Credit. Debit. ACH. Issuing, acquiring, originating, or receiving. Name the channel. Name the network. Name the platform. If it's a consumer-based electronic transaction, we cover it. We talk to the players who are making the revolutionary change happen. Every month. Rely on Digital Transactions to help you profit from a fast-changing, increasingly interconnected transactions market.

Make the transaction revolution work for you.



**ALSO IN THIS ISSUE:**  
■ Online Payments Vs. the Downturn  
■ Harnessing ISOs for Remote Capture  
■ ...ing Small Merchants ... risks

**DIGITAL**

ing them hard to detect in time for law enforcement to take action, Fossi says.

The Web masters of the black-market sites also use techniques that make it difficult for the typical search engine to index the sites, Bestuzhev says. Instead, they are promoted through banners on malicious sites.

## 'It's kind of a whack-the-mole effort. As you shut one down, others come up.'

But even carder sites operating in harder-to-track chat forums can be tracked, Bestuzhev says.

"These sites can be detected by monitoring other malicious sites and forums that cybercriminals use," he says. "Sites for coders, phishers, hackers, and even simple developers should be monitored, since some of the initial malicious activity may be born right here."

For example, someone pretending to be a developer may ask questions about code optimization on a non-malicious Web site, Bestuzhev says. That same developer's profile will be found on other sites showing that the person is in reality a cybercriminal.

"Sometimes we can find these sites by following banners and links mentioned in comments from suspected cyber criminals," he says. "They often lead you right to these types of sites."

Locating the sites is only half the battle. "Most of the markets are installed on Web servers located in countries with poor cybercrime legislation or countries that have a lot of bureaucracy," Bestuzhev says. "The criminals use bullet-proof server hosting services that make it very difficult and sometimes almost impossible to take the server down."

Complicating the problem is that

States," Correll says. "When you're dealing with several countries, the red tape becomes a problem. Sometimes the laws aren't put into place to be able to prosecute or extradite them. So it's difficult."

The Symantec study found that the United States hosted 41% of the

total observed servers worldwide, while Romania ranked second at 13%. Regionally, the North America hosted 46% of the servers, with Europe, the Middle East, and Asia hosting 38%, Fossi says.

"There's no one single country—it's widespread," Borenstein says. "There are forums that deal with criminals intent on committing fraud in Latin America. There are others focused on Asia, on North America, and on Europe. It really runs the gamut."

The criminals also evade law enforcement by shifting from server to server.

"Not only are they located in a variety of countries around the world, they actually move around on a fairly regular basis so that they're harder to detect and track and understand from a law-enforcement basis," Borenstein says.

### **Thriving Crooks**

Even when a site is detected, it can be difficult for law enforcement to break into an operation. Most of the sites require would-be participants to prove they have access to stolen goods or hacked a database, he says.

"Like in the real crime world, you essentially have to prove that you're a reliable criminal in order for them



**Tired of giving 1 – 2% of your sales to credit card companies?**

**Maybe it's time to check out our flat-fee i-Check\*!**

**Our services include:**

- Payment Via ACH
- Payment Via Paper Check
- Check, Phone & Address Verification
- NSF Recovery Services

***We can simplify your business' ability to get paid quickly while reducing fraud.***

**ITI Internet Services  
(800)436-1710**

**[www.itinternet.net](http://www.itinternet.net)**

\*NACHA rules prohibit some types



That's not to say that law enforcement hasn't succeeded in bringing some operators of these Web sites to justice, most notably the Shadowcrew criminal organization in 2004 and the Cardplanet Criminal organization in 2005.

"Law enforcement, generally speaking, is aware of these forums," Borenstein says. "There are many people in the industry who assume law enforcement themselves participate undercover in some of these forums as well."

But the nature of the underground economy makes it difficult to shut down the majority of the card-selling operations. "It's kind of a whack-the-mole effort," Ullrich says. "As you shut one down, others come up."

Adds Bestuzhev: "It's difficult to get a credit card shop Web site down.

<b>Bank account credentials</b>	\$10-\$1,000
<b>Credit cards with CVV2 numbers</b>	\$0.50-\$12
<b>Credit cards</b>	\$0.10-\$25
<b>E-mail addresses</b>	\$0.30/MB-\$40/MB
<b>E-mail passwords</b>	\$4-\$30
<b>Full identities</b>	\$0.90-\$25
<b>Cash-out services</b>	8%-50% of total value
<b>Scams</b>	\$2.50-\$100/week for hosting; \$5-\$20 for design

Note: Based on study conducted June 1, 2007-June 30, 2008; MB=megabytes Source: Symantec Corp.

The best thing we can do as an industry is to continue collaborating with ISP providers, domain registrars, and law-enforcement agencies."

As long as data breaches, phishing attacks, and other fraudulent activities enable criminals to steal large numbers of confidential card account and banking data, the eBays

of the underworld will continue to thrive.

"The crooks used to make a lot of money robbing banks," Borenstein says. "Now they've figured out they can earn just as much or more money and run a lower chance of being caught by simply hacking into a credit card database." **DT**

## ADVERTISER INDEX

Aegenis Group	888-615-3334	www.aegenis.com	Page 11
Allied Wallet	888-255-1137	www.alliedwallet.com	Page 5
CarpéCharge, a Splyce Inc. Company	253-857-6411	www.carpecharge.com	Page 29
Digital Transactions	877-658-0418	www.digitaltransactions.net	Pages 31, 35
Discover	800-347-2000	www.discovernetwork.com	Inside Back Cover
Epson	562-290-5306	www.pos.epson.com/financial	Page 1
First Data	866-752-8449	www.firstdata.com/about/partner_with_us	Page 15
FIS	888-323-0310	www.fisglobal.com	Inside Front Cover
Fiserv	800-872-7882	www.fiserv.com/mobile	Page 7
Humboldt Merchant Services	877-635-3570	www.hbms.com	Page 19
Ingenico	800-252-1140	www.ingenico-us.com	Page 3
ITI Internet Services	800-436-1710	www.itinternet.net	Page 37
Merchant Services Inc. (MSI)	800-226-5227	www.1800bankcard.com	Pages 20-21
North American Bancard	888-229-5229	www.gonab.com	Back Cover
Northeast Acquirers Association		www.northeastacquirers.com	Page 34
Payvision	917-237-0900	www.payvision.com	Page 12
United Bank Card	800-201-0461	www.isoprogram.com	Pages 16-17
USAePay	866-490-0042	www.usaepay.com	Page 32