Newsweek

The Rise of Black Market Data

Criminals who steal personal data often don't use it themselves. Instead, they put it up for sale on one of the many vibrant online markets.

Benjamin Sutherland
NEWSWEEK
From the magazine issue dated Dec 15, 2008

Los Angeles discount retailer Forever 21 announced earlier this fall that the account details for 98,930 credit and debit cards had been stolen. Spyware-infected PCs that feed personal financial details to hackers are legion, security experts say. And e-mail "phishing" schemes that trick people into revealing financial information on bogus Web sites continue to flourish. Tales of theft abound, but where does all this stolen information go?

It goes to market. More often than not, criminals who steal data don't try to break into bank accounts or tap credit lines. Instead, they put the information up for sale on any of a constellation of vibrant online black markets, forums and chat rooms. François Paget, a security specialist for McAfee in Paris who works closely with law enforcement, estimates that several hundred online marketplaces are flush with newly stolen financial data. So many are popping up, Paget says, that there's a glut on the market. "It's a price war," he says.

The complete details of a bank account, including a password for online access, can be purchased often for 5 or 10 percent of the account's value. Credit-card data, by far the most heavily traded commodity, currently run about $450 per batch of 10 from the United States or Western Europe, Paget says. Premium cards of high rollers with big credit lines cost more, but accounts lacking key information, such as mothers' maiden names and billing addresses, go for as little as a dollar apiece for bulk orders, down from four dollars a year ago. Jason Franklin, a Carnegie Mellon University expert in ID-theft markets, says online offers are updated continually, so buyers "sit there and watch this market feed."

One factor driving down prices is efficiency. The marketplaces boost criminal productivity through division of labor. Instead of attempting to master a wide set of skills, crooks can perfect specialties—say, retrieving money from hijacked bank accounts—and pay others with complementary expertise. This dynamism fuels markets with surprisingly diverse offerings, from counterfeit Dutch credit cards to software that can record keystrokes on remotely hacked PCs. Visitors can get data to make fraudulent online purchases, manufacture counterfeit credit cards, transfer money out of a bank account or pull off more elaborate ID-theft scams.

Lack of trust among the criminals themselves is also depressing prices. In one forum, thought to be run by Vietnamese fraudsters, a seller of card details known as changetheworld1989 recently wrote, in broken English, the following phrase to a hesitant client: "I'm not scammer." The claim shows how uncertain it can be to do business with stolen data. Buyers struggle to determine if information is fresh, firsthand, authentic or if it will even be delivered or paid for as promised. Sellers often worry that a payment from a hijacked PayPal or bank account could be traced by cops.

Law-enforcement officials are doing their best to drive down the supply of stolen data, but they face big obstacles. Cracking into servers used by criminals to hold ID information is extremely difficult, says David Pérez, a Valencia, Spain-based security consultant to three Spanish banks. Of the last hundred or so illicit servers Pérez has identified, he has managed to break into only three. Because the servers are located, more often than not, in Russia, Spanish authorities must ask their Russian counterparts to open investigations and subpoena the servers. Server administrators are often in yet another country, adding to the diplomacy and paperwork. "You can see how this can go on forever," he says.

Some fraudsters are further complicating the cops' job by moving their activity offline. For instance, more than 300 Parisian cashiers regularly steal payment-card details from unobservant shoppers and diners, estimates Patrick Yvars, head of the fraudulent-payments brigade of the Paris Judiciary Police. Most of that pilfered data is sold face-to-face, he says, often between fraudsters who met online. This hybrid market "works really well" by partially skirting the territory of cyber law-enforcement agencies. International groups are also increasingly shunning the use of English—many opting instead for Russian—in an effort to evade U.S. cops. This is a big reason why the Secret Service and other Western law-enforcement agencies have been demonstrably less effective this year, says Kim Taipale, director of the Center for Advanced Studies in Science and Technology Policy in New York and cybercrime consultant to U.S. government agencies.

Financial institutions are trying to step up their role in fighting data theft. Specialists from some financial institutions pose as buyers and sellers to gather information to aid law enforcement, or to disrupt markets. Bill Dunn, VP of fraud management at Visa Europe in London, says his team tries to intercept stolen credit-card details so the card company can cancel accounts before a theft occurs, "making the data useless to criminals." Franklin, the Carnegie Mellon University researcher, explains another disruption technique: his team infiltrates markets and, posing as ripped-off buyers and sellers, slanders participants to foment confusion and mistrust. In the world of illicit data markets, such dishonesty fits right in.

Editor's note (published Dec. 9, 2008): A previous version of this story erroneously mentioned a report that payment details had been stolen from Best Western, which the company has refuted.

URL: http://www.newsweek.com/id/173398