InformationWeek's Security Weblog

Topics: Security

Who's Fighting Identity Theft? You'd Be Surprised

Posted by Larry Greenemeier, Jul 12, 2007 05:43 PM

I love a good scrap, and one of the more interesting ones I've been following this year involves the U.S. Justice Department and E-Gold, an organization that provides a payment system for online transactions. The government says that E-Gold facilitates cybercrime by allowing the criminal element to pay online for stolen goods. Yet E-Gold portrays itself as a fellow cybercrime fighter and asserts the government ignores its offers for assistance and is taking credit for E-Gold's investigative work.

» E-Mail
» Print
» Write To Editor
» Digg
» Slashdot

A federal grand jury in late April indicted E Gold Ltd, Gold & Silver Reserve Inc., and the owners of these related digital currency businesses on charges of money laundering, conspiracy, and operating an unlicensed money transmitting business.

However, E-Gold chairman Douglas Jackson disputes these charges and asserts that the U.S. Secret Service's recent announcement that it has arrested and indicted four members of an organized fraud ring in south Florida was helped by E-Gold's own investigative efforts. "The recent USSS press release is the second instance in three weeks where the USSS is claiming credit for work that was actually initiated and performed last year by e-gold's own in-house investigators," Jackson told me in an e-mail exchange today.

Why is all of this squabbling important to you? As you'll see in *InformationWeek's* upcoming 10th Annual Global Security Survey, which hits InformationWeek.com this weekend, often companies don't know when their IT systems have been breached and their customer data stolen and sold on the black cyber market. In the 2006 Annual Global Security Survey, only 8% of U.S. respondents said that identity theft had occurred within their organization. You'll be surprised to see where that percentage is in this year's survey results. Anecdotal evidence (including the TJX and Polo cases), suggests that companies should be more worried.

It also suggests that law enforcement should be using every tool at its disposal to crack down on crooks looking to ruin your credit and, worse, the credit of your customers.

The Secret Service's south Florida bust resulted in the recovery of about 200,000 stolen credit-card account numbers responsible for fraud losses roughly calculated to be more than $75 million. One of the keys to the arrests was information that the Secret Service obtained after earlier this year arresting a 30-year-old Florida man--who used the online handle "Blinky"--and his girlfriend. Blinky is accused of trafficking counterfeit credit cards and identifications for years over the Internet. His arrest turned up evidence of an organized fraud ring involving Cuban nationals operating in south Florida and led to the four arrests and indictments announced this week.

The four fraudsters were sending large amounts of money via E-Gold accounts to known cyber criminals in Eastern Europe in return for tens of thousands of stolen credit card account numbers. The stolen credit card account numbers were then used to counterfeit credit cards in “plants” throughout southern Florida, the Secret Service said in a statement.

But Douglas says it was his company that first brought Blinky to the attention of law enforcement in March 2006. Jackson told *InformationWeek* that investigators working for E-Gold began monitoring Blinky pursuant to an undercover operation it was conducting with law-enforcement agents from the U.S., U.K., and Russia.

"In May 2006, working with records supplied by an exchange service that had sold [Blinky] some e-gold, we were able to supply general location (Miami), three confirmed phone numbers he used, and the usual IP/timestamp combos that even in this day and age are often useful," Jackson said. "In September 2006 we were able to set up a quasi-ambush where the guy was sent a Fed Ex package such that we were able to supply law enforcement with a specific physical location (a garage in Miami) and a time to nab him."

Jackson sent me a copy of an e-mail exchange he claims to have had with a Secret Service contact in January 2006. In an e-mail Jackson ostensibly sent to the agency, he requested the Secret Service use information gathered by E-Gold investigators to crack down on a card-counterfeiting ring. An enthusiastic-sounding response from the agency informed Jackson his Secret Service liaison had made contact with "our guys at HQ and they will be in contact with you or your staff concerning this matter." Jackson told me that E-Gold was later "rebuffed" by the Secret Service and doesn't know if they followed up on the information he says he sent them.

If you're curious about the Justice Department's side of this story, so am I. While I've reached out to them several times as the TJX case has unfolded, I rarely hear back from them.

The TJX data breach has cost that company more than $20 million, and counting. For that company, law enforcement's successes are probably bittersweet. On the one hand, crooks are being put away. On the other hand, the evidence is mounting that their customers have become victims of identity theft. Still wondering whether law enforcement should be working with, rather than against, E-Gold?

« Network Operators' Worst Fears Realized: They Will Be Dumb Pipes | Main | Ubuntu Aftermath: Puncturing The Linux 'Urban Legend' »

Discuss This

1 message(s). Last at: Jul 12, 2007 10:10:08 PM

ePanama
commented on Jul 12, 2007 10:10:08 PM

Great post Larry, there's more than one side to every story. I think e-gold has a lot to say and we need to hear more.

Mark Herpel

Add Your Comment:

Post as user

Please login or register here for a free Techweb account to post

Post as guest

Name

Submit Comment