BANK INFO SECURITY®

http://www.bankinfosecurity.com/

Stolen Cards Tested on Charity Sites

Cybercriminals Exploit Sites, Automate Card Verification

Tracy Kitten (FraudBlogger) • November 25, 2014 2 Comments

Cybercriminals are perfecting the automated systems they use to verify stolen card data by exploiting charitable websites that accept debit and credit card donations.

See Also: Simplifying Microsoft Azure Deployments with Cloud-Friendly Security

On Nov. 21, **PhishLabs'** research team reported the discovery of a new interactive bot script that enables cybercriminals to automate their card verification processes in a virtually undetectable way.

The bot, which is programmed to automatically log on to online chat channels in search of instant messages containing **payment** card data, is being used by cybercriminals to share and test stolen card numbers.

Through a selective invitation process, hackers are invited to join the chatroom, where they freely exchange information, PhishLabs reports. The bot basically sits in this chatroom, which is unrelated to the not-for-profit or charitable websites used to test the stolen card data.

Once card data is submitted through chat, the bot parses the data and uses it to attempt a donation to a charity website that also has been infected by the bot. The bot then reports back to the hackers to let them know if the transaction was successful.

"When cybercriminals join the online channel and chats, the bot uses the data provided [cardholder name and information] to input and run transactions against the websites of charities and other non-profits in order to verify that the card data is correct and the account is active," notes Don Jackson, director of threat intelligence at PhishLabs, in a blog he posted about this new verification method. "The bot then reports the results and any transaction details back the crook."

Charities: A Soft Target

The cybercriminals are intentionally targeting websites run by charities and not-for-profit organizations, Jackson tells Information Security Media Group, because these organizations rarely challenge the donations they receive online. That makes their websites ripe for hackers who want to test their stolen card data.

"These types of websites seem to have fraud detection profiles that result in a relatively low number of declined transactions for valid card data," Jackson writes in his blog post. "The ability to verify small amounts from many different types of cards issued in many different countries seems to work more reliably for the criminals than, for example, retailer websites."

PhishLabs has been monitoring this bot since February, Jackson tells ISMG. In May, his research team recovered card numbers that were processed through the bot in early 2014.

In June, PhishLabs started alerting card issuers, law enforcement, the card brands and the affected not-for-profits and charities about the compromised data and the verification scheme, he says.

"We've seen wholesale card verification services long before, often with Web interfaces," Jackson tells ISMG. "However, this is the first one I've seen operating on this scale. This service has many more users and a much higher volume of card data than those we've investigated previously."

What's more, this newly discovered bot script has advanced features that overshadow other card-verification services, he adds.

"This is a full-service cybercrime shop," Jackson says. "The bot has modules for ordering retail goods and services, package tracking, credit management and message relays to money mule managers, and supports many more essential cybercrime monetization functions. It's also the first time we've run across the purposeful abuse of charity and non-profit organizations' websites based on their lack of anti-bot functionality and the differences in their **fraud**-detection profiles."

Minimizing Risk

To prevent these functions from compromising chat features and charitable sites, Web forms that accept card information must be protected against automated submission, Jackson says. Randomized URLs, hidden card data input fields and CAPTCHAs can help reduce risk, he says.

Although those strategies could require additional steps for the donation process, they're relatively minor compared to the steps consumers go through when buying from online retailers, Jackson says.

"Operators of this criminal service maintain a list of unprotected payment submission Web pages and configure the bot for how to run transactions against each one," he writes in his blog. "Those targets that have implemented one or more of these countermeasures have been pruned from the bot configuration."

Julie Conroy, a financial fraud expert who's an analyst at the consultancy Aite, says fraudsters' card testing activity is up across the board, hitting e-commerce retailers at an unprecedented rate. But most retailers have implemented strategies to detect and stop these testing schemes, she says.

"So it makes perfect sense that criminals would target soft targets like non-profits, which not only have fewer resources to fight fraud, but which also want to keep the barriers to genuine donations as low as possible," Conroy adds.

Most of the mitigation strategies, such as hidden card-data entry fields and randomized URLs, that Jackson suggests have proven successful for retailers, Conroy says. But she also says online charities and not-for-profits that accept donations would be wise to invest in systems that can detect anomalous navigation patterns.

John Buzzard, who heads up FICO's Card Alert Service, says all e-commerce sites should have systems in place that raise flags when waves of low-dollar donations or transactions are submitted. "They may hit in spurts from similar IP addresses, regardless of the personal information entered by the criminal's automated tool," he says. "The thieves aren't going to donate much to the charity - they want the mother lode for themselves."

But investment in most automated tools is cost-prohibitive for not-for-profits and charities, says **Al Pascual**, direct of fraud and security for Javelin Strategy & Research. "That places the onus on issuers to automatically monitor for these transactions and consider them as a potential precursor to fraud," he says.

Fraud expert **Avivah Litan**, who is an analyst at the consultancy Gartner, contends that the card brands should do more to detect and prevent these types of testing schemes.

"The criminals know that the charities normally don't have fraud controls, so they are easy prey for this type of activity," she says. "The charities typically find out about it when MasterCard or Visa contacts them to tell them they have too many chargebacks ... or because

some processor notices strange transaction patterns emanating from their website, i.e., a high velocity of transactions from the same IP address requesting authorizations for tiny donation amounts."

Ultimately, the charities are the ones that lose, Litan says. "They are non-profits and there is no reason for them to suspect their donors use stolen cards to make donations," she says. "It's incumbent upon Visa and MasterCard and the other card brands to provide them free fraud detection services, which would basically cost the card brands next to nothing. Surely, the card brands can afford to offer a few 'charitable' and pro-bono services themselves."

About the Author

Tracy Kitten

Executive Editor, BankInfoSecurity & CUInfoSecurity

A veteran journalist with more than 18 years' experience, Kitten has covered the financial sector for the last 11 years. Before joining Information Security Media Group in 2010, where she now serves as the Executive Editor of BankInfoSecurity and CUInfoSecurity, she covered the financial self-service industry as the senior editor of ATMmarketplace, part of Networld Media. Kitten has been a regular speaker at domestic and international conferences, and was the keynote at ATMIA's U.S. and Canadian conferences in 2009. She has been quoted by CNN.com, ABC News, Bankrate.com and MSN Money.