Battling the Bots

What's behind a new threat to online commerce

by LIZ PARKS

In the retail world, customer convenience and speedy service are high priorities, contributing to growing sales and profits.

In the criminal world, however, those attributes are vulnerabilities that can easily be exploited by sophisticated fraudsters, particularly when it comes to swindling loyal customers by using automated attacks to troll through trusted retail sites to find and steal gift cards with unused balances.

Retailers of all types from luxury merchants to supermarkets are increasingly under gift card fraud attacks these days, two recent research reports found, and the situation is getting worse as fraudsters grow more creative through automation.

In February, an advanced persistent bot known as GiftGhostBot surfaced, according to bot detection firm Distil Networks, and in less than a month had attacked almost 1,000 websites.

GiftGhostBot is a card cracking, or token cracking, attack, which means the fraudsters use automation to test a rolling list of potential account numbers and request the balance. If the balance is provided, the bot operator knows that the account number exists and contains funds. Armed with that information, the account number can be used to purchase goods, or the cards can be sold on the dark web.

IMPACTING DATA

Bad bots account for roughly 20 percent of all internet traffic, says Distil Networks CEO Rami Essaid. They are capable of dozens of unique automated threats, and depending on the individual business, can impact factors such as conversion rates, traffic scores and customer satisfaction rates.

Distil analysts recently recorded 4 million bad bot requests per hour on one website, nearly 10 times its normal traffic, Essaid says.

Any website with gift card processing capability, including checking a gift card balance or replenishing funds, is a potential target.

"Like most sophisticated bot attacks, GiftGhostBot operators are moving quickly to evade detection, and any retailer that offers gift cards could be under attack at this very moment," Essaid says.

"While it is important to understand that retailers are not exposing consumers' personal information, consumers should remain vigilant."

Although retailers are not themselves being defrauded, they still must invest time, labor and money to successfully handle dissatisfied customers asking for refunds. Their retail businesses are also suffering on the front end of the attack, Essaid says.

"Requests into the website could reach millions each day and potentially inundate the servers leading to slowdowns or downtime. It amounts to an application denial of service."

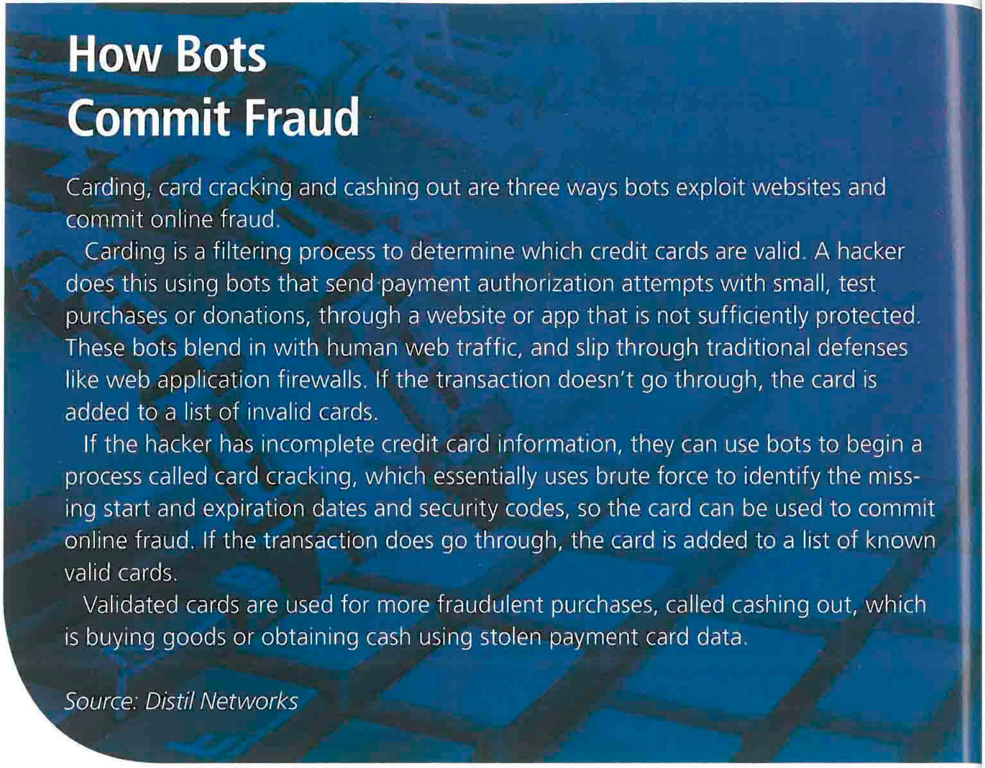
The information about visitors to that company's website is also heavily weighted toward fake bad bot traffic, he says. "Any data about where visitors to the website come from is seriously flawed."

'CRIMINAL PROFITEERING'

According to recent tracking research from Flashpoint, cybercriminals are increasingly using the deep web and the dark web to buy and sell fraudulent gift cards. Flashpoint analyst Olivia Rowley says this is a type of crime that has "grown substantially over the last several years because it can yield significant financial rewards at a relatively low risk for criminals."

Cybercriminals' continued interest in gift card fraud "aligns with a common practice among many gift card issuers — the prioritization of user experience and profits over security," she says.

Unlike bank-issued credit and debit cards, gift cards are not held to strict anti-fraud standards, which means that many gift cards may lack common yet effective security features aimed to help combat fraud. "This is just one example of criminal profiteering using the deep and dark web," Rowley says.



How Bots Commit Fraud

Carding, card cracking and cashing out are three ways bots exploit websites and commit online fraud.

Carding is a filtering process to determine which credit cards are valid. A hacker does this using bots that send payment authorization attempts with small, test purchases or donations, through a website or app that is not sufficiently protected. These bots blend in with human web traffic, and slip through traditional defenses like web application firewalls. If the transaction doesn't go through, the card is added to a list of invalid cards.

If the hacker has incomplete credit card information, they can use bots to begin a process called card cracking, which essentially uses brute force to identify the missing start and expiration dates and security codes, so the card can be used to commit online fraud. If the transaction does go through, the card is added to a list of known valid cards.

Validated cards are used for more fraudulent purchases, called cashing out, which is buying goods or obtaining cash using stolen payment card data.

Source: Distil Networks

In addition to being a very "low-risk" type of fraud because a perpetrator can pretend they didn't know anything about the history of the card, gift cards can be used at a multitude of businesses. To incentivize sales, "Many vendors of fraudulent gift cards sell their wares at a fraction of their actual value on the card," she says.

Gift cards were being treated by fraudsters as a way to cash out stolen

> "Bad bots account for roughly 20 percent of all internet traffic. Many gift cards may lack common yet effective security features aimed to help combat fraud."

"Flashpoint recommends that retailers require correct personal identification numbers to check balances or restrict gift cards to in-store purchases."

credit cards, the Flashpoint report notes, an activity known as "carded" gift cards. Retailers caught on to that approach, though, and increased security measures around the purchase and use of gift cards.

That led to inventive cybercriminals developing a way to obtain non-carded gift cards by identifying legitimately issued and purchased gift cards that were unused and maintained a balance. Some have developed bots to automate the process, which led to GiftGhostBot's emergence.

Most of the stolen cards are marked down to about 30 percent of their face value, Rowley says, but some cybercriminals, "attempting to undercut the competition," offer cards for as little as 5 percent of their face value.

AUTOMATED THREATS

Flashpoint recommends that retailers require correct personal identification numbers to check balances or restrict gift cards to in-store purchases. Merchants should also use a CAPTCHA system for all online purchases made with gift cards, which protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot.

Rowley notes that because many gift cards are numbered sequentially, it makes it "relatively easy for cybercriminals to ascertain the numbering convention used for many gift cards." Armed with the numbering convention, cybercriminals can test possible gift card number combinations on a targeted business's gift card balance checker.

Flashpoint suggests that retailers implement a more complex numbering system for gift cards and, overall, subject transactions that use certain gift card management applications to greater security. STORES