SECURITY
BOULEVARD

Home ▾ Security Bloggers Network ▾ Webinars ▾ Chat ▾ Library

We Phish You a Very Merry Christmas and a Fraudulent New Year

by Ericka Chickowski on December 2, 2019

The holiday season is kicking into full gear, and so is the annual holiday cybercrime surge. As gift givers scour the web to seek out the best deals, cybercrooks put in extra work to profit off of the holiday shopping frenzy.

Cybersecurity researchers report that this annual holiday fraud cycle has firmly established itself in recent years. The bad guys always follow the money and, at this point, once we round into Black Friday and Cyber Monday the money inevitably pours into online shopping channels.

“Cybercriminals thrive during peak holiday shopping,” security researcher Emily Wilson of Terbium Labs told Credit Union Times in a recent report. “The hustle and bustle of transactions and unusual shopping patterns create countless opportunities to capture payment data and attempt fraudulent transactions”

Cyber criminals are looking to take a bite of the profit through a number of different attack methods, including:

Phishing

Phishing activity experiences an annual spike right around the holidays and this year is shaping up to be an particularly bad one. The latest research shows that the use of ecommerce phishing URLs this year has more than doubled since its holiday peak in 2018. The holiday lures are plentiful from cyberattackers, who are trying everything from order confirmation scams in email and SMS to enticing promotional offers.

Promo Scams and Domain Impersonation

A lot of the phishing is paired with very convincing domain impersonation scams that masquerade as real ecommerce operations by running lookalike retail impersonation sites that ape both big and small brands alike. Many of them are also tied into social media impersonation and they usually promote ‘unbeatable’ deals and a sense of urgency with ‘limited time offers’ that convince consumers to part with their payment details.

Credential Stuffing

The criminals work overtime to direct automated bots to carry out credential stuffing attacks that try credentials stolen from one site on a bunch of other different sites in case the victim reuses passwords. According to researchers at Radware, these bad bots carrying out account takeover attempts reach their peak right before Black Friday in prep for the holiday season—the bots usually represent 96.6% of retailer traffic in that time. Normally the human-to-bad bot ratio on login pates is 2 to 1 on a normal day but just before the holidays that shoots up to 1 to 20.

Ad Fraud

After attackers have harvested plenty of accounts and start to monetize that with card fraud, they transition their bot activity to another lucrative venue: ad fraud. According to Radware, the onslaught of advertising fraud usually happens right after Cyber Monday. Last year, programmatic advertising vendor Pixalate found that ad fraud increased 24% during the holidays.

Magecart Attacks

Online skimming Magecart attacks have grown very popular among criminals today, as they take advantage of vulnerabilities in payment platforms like Magneto to collect consumer payment card information as they enter it into legitimate transactions. Criminals are already getting the jump on the holiday rush to amp up their Magecart mojo. The recent Macy’s breach announced in mid-November came at the hands of Magecart attackers.

Charity Scams

The government pundits at the US Cybersecurity and Infrastructure Security Agency (CISA) just recently released a blanket warning against holiday scams and malicious cyber campaigns. One of the sometimes forgotten scams they called attention to were charity scams, warning consumers to “verify a charity’s authenticity before making donations.”

Gift Card and Loyalty Point Scams

A report from CNBC shows that the Dark Web is awash in stolen gift card account information, and the bad guys are seeking every way they can to siphon off the monetary value stored not only in gift card but also retail loyalty accounts. This includes everything from brute forcing account number and PIN combos on retail sites using bots to demanding payment in gift cards for ransomware extortion.

Current economic estimates state that holiday shopping sales in the US alone will top the $1 trillion mark for the first time ever in 2019. An increasing amount of that will come on the back of ecommerce sales, which are expected to grow 3x more quickly than overall retail holiday sales according to the experts with Deloitte.

They predict US ecommerce sales for November 2019 through January 2020 will jump by 14%-18%, compared to a max 5% gain in overall retail sales during the same time period. What's more, a study just released by TransUnion, the 2019 Holiday Retail Fraud Survey, found that some 75% of consumers say they'll do at least half of their shopping online this year. In spite of that, Deloitte figures show that ecommerce sales will still only make up 14% of all retail receipts this holiday season.

However, as retail organizations invest in digital transformation efforts that focus on omnichannel customer experiences—including online ordering for curbside pickup, in-store kiosk orders shipped to the home, and a plethora of mobile loyalty apps—the lines between ecommerce and 'traditional' retail are blurrier than ever. Deloitte experts say the focus on convenience through this expansion of the digital footprint is retail's number one driver today:

"We've seen retailers continue to improve customer experience, invest in the fundamentals and leverage relationships with innovative startups to boost engagement and efficiency. But, convenience is the new retail currency; retailers who offer seamless experiences, have products available and can deliver items more quickly than ever are most likely to win this holiday season."

However, anyone who has been in the security world long enough understands that increased omnichannel customer interactions will inevitably yield increased omnichannel fraud. And the TransUnion study shows that while convenience is huge, consumers are growing more security conscious about their online holiday shopping. The study found 46% of consumers are worried about becoming a victim of fraud this holiday season. Over half of shoppers surveyed said they'd be more likely to make an online purchase from a retailer that provides two-factor authentication.

Nevertheless, retailers must walk a fine line between security and convenience.

"More and more consumers are turning to online shopping, yet consumers demand that retailers not only provide them with a secure checkout process, but also make it as convenient as possible," said Geoff Miller, head of global fraud and identity for TransUnion. "Retailers need to do all they can to ensure transactions are secure and seamless for all consumers."

*** This is a Security Bloggers Network syndicated blog from Business Insights In Virtualization and Cloud Security authored by Ericka Chickowski. Read the original post at: http://feedproxy.google.com/~r/BusinessInsightsInVirtualizationAndCloudSecurity/~3/ylmlcpbMeIA/phish-christmas-fraudulent-new-year