Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 4

Cyberthreats that operators' customers will be facing during the holidays

By: Itay Yanovski

As consumers forsake the mall in favor of Internet shopping, retailers are becoming increasingly reliant on their telecom providers to maintain their growing online footprint. But as the shopping season approaches, online retailing's growth is threatened by a seasonal tsunami of cybercrime.

With cyberattacks on online retailers—including those who also maintain a brick and mortar presence—roughly doubling every year, retailers should be doing all they can to protect their customers as never before. As retailers expect to make roughly 40 percent of their annual sales during this period and consumers are doing an increasing proportion of their shopping online, this year offers cybercriminals a richer harvest than ever before.

While the retailers have been stocking their shelves with Christmas goods, the cybercriminals have been improving and sharing their already expert online hacking techniques—going through the operators' infrastructure, of course.

These attacks include directly inserting malicious code into retailers' websites using a form of malware known as "scrapers" or "skimmers" to exploit weakness in the code behind the payment processing pages. This was the form of attack used in the recent cyberattacks on British Airways (BA), which compromised the payment card details of 380,000 online customers. During this type of attack, the consumer is unable to detect anything unusual when finalizing a compromised transaction.

Other new techniques that have been perfected by the cybercriminals since last year include "domain jacking." One in four Fortune 500 companies—including IT giants such as Microsoft and Apple—currently hold sub-domains that are sufficiently insecure as to be open to attacks from threat actors orchestrating a new cyber scam known as "domain jacking." A staggering 236 million users visit the abandoned sub-domains of 96 percent of Fortune 500 companies on a daily basis, which means these consumers are vulnerable to orchestrated phishing attempts by threat actors. These consumers can also be directed to spoof ads or other promotional campaigns, exposing major retailers to brand damage and potential lost customer confidence in addition to financial loss.

In the run-up to what they hope will be a Christmas cybercrime bonanza, even relatively inexperienced and unskilled cybercriminals are currently filling their stockings with the kind of off-the-shelf malware designed to bypass most retailers' existing cyber defenses. Just as online retailing has evolved into a global industry worth almost three trillion dollars a year, so cybercrime has also evolved into a highly modern industry.

Under cover of the Dark Web, cybercriminals can use cybercrime-as-a-service software, which offers thoroughly tested off-the-shelf products. Sometimes the cybercriminals also receive customer support in the form of help desks and call centers. This effectively means that even relatively unskilled and novice hackers can now arm themselves with the latest cybercrime tools.

This forms a growing challenge for retailers and their service providers if they are to protect consumers from fraud and identity theft over the shopping season.

To stop the cybercriminals from scotching the continued growth of e-commerce and online shopping, there needs to be a cross-industry awareness of the growing threat of crime in the digital age. This should encompass not only cybersecurity advisers and online retailers but also the telecoms operators who supply the online infrastructure that powers the continued growth in Internet shopping.

For example, a joint investigative venture conducted earlier this year by CyberInt and Check Point uncovered a recent form of off-the-shelf malware: the [A]pache Next Generation Advanced Phishing Kit on the Dark Web, described as a fifth-generation level kit. The kit is relatively expensive, retailing for between $100 and $300, compared to the $20 or $50 most kits sell for, but for the price, [A]pache delivers what the researchers called one of the most advanced phishing kits yet spotted.

The [A]pache next-generation phishing kit provides threat actors of all kinds with a full suite of tools to carry out their attacks. These include an entire back-office interface with which they can create convincing fake retail product pages and manage their campaigns. This includes having their own versions of sites including Walmart, Americanas, Ponto Frio, Casas Bahia, Submarino, Shoptime, and Extra. With this year’s seasonal shopping spree expected to be well over a trillion dollars, the [A]pache kit is likely pay for itself many times over in the hands of criminal users.

As the cybercriminals become increasingly sophisticated in their methods of attack, retailers and the telecoms operators who provide their online infrastructure must prepare themselves to protect themselves and their customers.

In last year’s cybercrime spree, some Dark Web developers were even advertising off-the-shelf malware in the run-up to the seasonal shopping bonanza. CyberInt found a stockpile of tools on the Dark Web used to target customers. These included fake smartphone apps masquerading as the official Victoria's Secret app and a list of vulnerabilities on its website. One Dark Web ad claimed Victoria’s Secret’s official website was vulnerable and showcased malware that could be inserted undetected. Three versions of fake apps with Victoria’s Secret branding were also available, complete with Trojan-style software. The fake app was designed to grant total access—including pictures, documents, browsing habits and banking details—to fraudsters.

But since the 2017 shopping season, the planned threats for this year’s online retailers have become far more sophisticated. If retailers do not protect their customers against all the new and old threats now being deployed, the fallout will not only adversely impact individual retailers and their customers, it may also have a negative effect on the entire online retail industry. If sufficient numbers of customers who have done their seasonal shopping online discover their personal and financial details have been used to make them cybercrime victims as a result of shopping online, many may make a New Year’s Resolution to avoid Internet shopping entirely in 2019.

In the run-up to Black Friday (November 23) and Cyber Monday (November 26), retailers and criminals are now engaged in a cyber-race where time is of the essence. The stakes are this year’s consumers’ Christmas cash.

Cybercriminals are already trading stolen lists of customer credentials, frequently without the owner knowing the credentials have been compromised. When cybercriminals do acquire stolen credentials, they generally try to maximize their usefulness by a process known as “credential stuffing,” where a single user password is used to log into multiple sites. Credential stuffing is a serious threat to both consumers and businesses, which both stand to lose money, either directly or indirectly. It is therefore recommended that consumers create different and sufficiently strong passwords for each site.

For the site or service provider, the best solution comprises targeted threat intelligence, real-time technology, automation, cyber expertise, and holistic digital risk protection.

Threat intelligence is also crucial to operators and retailers’ online defenses. This means monitoring traffic on areas such as the Dark Web that are generally outside organizations’ traditional security boundaries to be aware of stolen customer credentials that are on sale or new attacks that are being orchestrated in time for the shopping season.

The use of state-of-the-art threat intelligence is crucial at all levels in order to enable operators’ and their customers’ full defenses against the latest generation of cyber threats.

Online retailers should also protect against image scrapping from their websites to create “look-alike" sites to steal traffic from genuine retail sites. Online retailers and operators should prepare and perform incident response playbooks for gift card, vouchers and discount code abuse during and before peak sales periods.

To combat the increasingly sophisticated techniques used by the cybercriminals, operators must lose no time in using effective threat intelligence to ascertain the nature of incoming cyber threats while helping their clients secure their websites against hackers of all kinds between now and Black Friday.

Given the increasing ingenuity of the cybercriminals and the growing challenge now facing retailers and consumers, telecom operators must now work closely with the cybersecurity industry to ensure they are doing their best to protect all users.