INSIGHTS

Cyber made simple.

CYBERTHREATS IN RETAIL

BY JAY BORDEN

The upcoming holiday season is critically important for the retail industry. For many vendors it is the make-or-break time. The day after Thanksgiving is called Black Friday because for many retailers it was the day their business went from being in the red to being in the black.

Regardless of the size of the business, the number of on-line and in-store transactions skyrocket during this period. Online transactions represent a significant portion of the transactions and are of course done with a debit or credit card. In-store transactions may be cash but many are done by card.

This makes it a prime time for cybercriminals. They recognize the rush of the season will distract store employees and impact systems.

Online traffic will spike during this period and may overload servers. Last year there was a 12% increase in traffic over the October and November period. But individual days may be much higher. Monday of Black Friday week saw an increase of 54%. Traffic on Cyber Monday was 42% higher than on Black Friday.

The meaning of all this is that card transaction traffic will increase dramatically during the season even if traffic for specific days varies and will be difficult to predict. Even the days that have historically been the highest may no longer be.

Bots are automated systems that have legitimate purposes but are also tools of attackers. Bot traffic will also rise during this period with hopes of convincing employees to click on bad links or download malicious attachments or simply to overload servers and interfere with your business. The bots can attempt to purchase high demand products using fake or stolen credit cards or to take advantage of new customer discounts.

onebrightlycyber.com
(888) 773-1920
A global leader in cyber service, technology, insurance and innovation.

CYBERTHREATS IN RETAIL

CONTINUED

Don't make the mistake of thinking bot attacks are rare or that they are easy to spot. Bot attacks in retail average almost 102,000 attacks every day! It wouldn't be that high if they didn't work!

The bots are growing in sophistication and look to exploit business logic by using promotional codes, new customer discounts or take advantage of return policies. This is all in order to get what they want at lower prices. In the case of stolen credit cards, their price is effectively zero as someone else will get the bill.

Nor is business logic exploitation rare. It accounted for about 30% of all attacks and 50% of retailers experienced attacks attempting to exploit business logic.

Equally pervasive are Distributed Denial of Service, DDoS, attacks; also at about 30% of all attacks. The point of DDoS attacks is to interfere with server ability to process real purchases. This has the obvious impact of reducing or stopping sales but also harms your reputation. If customers can't reach your site because of DDoS attacks they will go elsewhere. Adding to the DDoS direct impacts are costs associated with bringing the servers back online after a successful attack.

Artificial Intelligence, AI, is being used by cybercriminals to drive business logic based and DDoS type attacks. Using AI makes the attacks more prevalent, more successful, and more costly to retailers. AI powered bots are better at imitating a person making them more believable to your systems and business logic. It also means they are more difficult for protective systems to filter out.

Another area that attackers exploit for cybercrime is Application Programming Interfaces, APIs. These are the ways systems "talk" to each other, that is, share information. APIs need accounts like any other user and often have enhanced privileges making them very desirable targets for attackers. APIs may be used between the public facing web sites, purchase systems, credit card authorization systems, inventory updating, reorder systems, and the systems of trading partners. Compromised APIs are an effective way for attackers to spread malware onto multiple systems often at multiple companies.

CYBERTHREATS IN RETAIL

CONTINUED

What to do
Are your servers prepared to handle this level of traffic? If not, then they will slow down substantially or possibly even crash. Be sure your servers are ready to handle the rapid growth of traffic.

Review your cyber protections to see if they are effective in screening out bots including the types discussed above. If not, upgrade the protections quickly.

Look at your business logic. Are there vulnerabilities that can be exploited? What is in place to review transactions for possible violations? Anomalies in anything are a red flag.

How do you defend against DDoS attacks? Can they be screened out to not interfere with real traffic to your sites? Are protective systems sized to handle the holiday surge?

What about your APIs? Are protections in place to prevent or limit exploitation? Do you use least-privilege accounts for everyone including API users? Are the APIs monitored to see who is using them and what is being requested?

Are all your protections up-to-date to discover and block the latest attack types? If not, don't delay any longer. If you believe they are, check again. You may not get a second chance.

Don't forget your trading partners. A weakness on their systems may provide access to your systems for cybercriminals, human or bot.

The holidays are almost here. It is time to act now.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.