Carbon Black.

CARBON BLACK HOLIDAY THREAT REPORT

Holiday Season Cyberattacks on Pace to Increase by Nearly 60%

NOVEMBER 2018

'Tis the season for cyberattacks.

According to the Carbon Black Threat Analysis Unit (TAU), organizations should expect to see a spike in potential cyberattacks starting with Black Friday/Cyber Monday and continuing through the holiday shopping season.

TAU's analysis across Carbon Black's global endpoint footprint - totaling more than 16 million endpoints - reveals that global organizations encountered a **57.5% increase in attempted cyberattacks during the 2017 holiday shopping season**. During a similar time period in 2016, attempted cyberattacks increased above normal levels by 20.5%.

"Based on existing precedent, we expect the same trend to continue, if not increase, during the 2018 holiday shopping season," said Tom Kellermann, Carbon Black's Chief Cybersecurity Officer. "During the holiday season, there is often a ton of noise in the online world and attackers do everything they can to take advantage of that. This applies not only to consumers who shop online, but also to businesses as well, many of which are understaffed and, in the case of retailers, approaching the busiest time of the year."

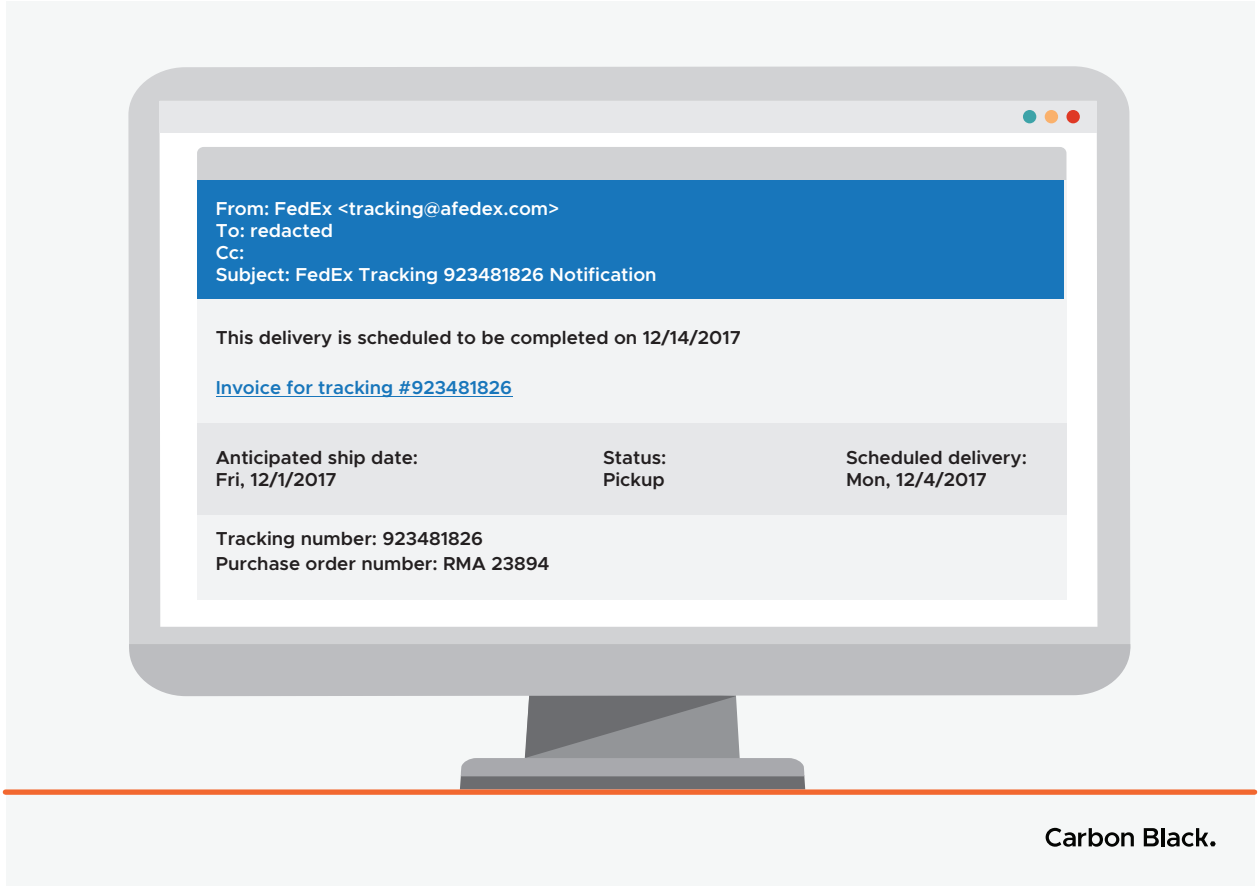
Following the Thanksgiving holiday, notable cybersecurity alerts spiked on Black Friday/Cyber Monday in 2017 and remained at elevated levels through the new year. Interestingly, the highest spike during the 2017 holiday shopping season occurred in the days following Christmas Day, when consumers are looking to take advantage of post-holiday shopping deals.

According to TAU, the majority of these attempted holiday-related cyberattacks were the result of commodity malware, commonly delivered through spear-phishing campaigns. In recent years, attacks targeting major retailers (often through supply chain partners) have resulted in the loss of millions of customer records and credit card numbers as well as major breach costs for the targeted organizations.

With cybersecurity, there are several nuances that come into play during the holidays. Most companies are going to be scrambling to find security team members who are willing to work or stay on call during the holiday hours, particularly with an expected upswing in business. This is compounded by the temptation to disable/reduce security tools to avoid slowing down business.

Employees, who frequently take work with them on the road during the holiday season, are often the targets of spear-phishing campaigns that promise low airfare and deals on gift cards.

Such attacks will often use fake package tracking emails to deliver malware:



Notice how the email domain in the image above has been changed from fedex.com to afedex.com. That's a simple change but it's one that has big consequences if an unsuspecting user is all too excited to receive a holiday package.

Unless you're a company the size of Amazon, Google, or Microsoft, your team is likely understaffed, and it's harder to manage your attack surface. So how do companies manage risk during the holiday season, especially when they're short staffed?

It comes down to something entirely nontechnical – creating a culture revolving around cybersecurity and internet safety.

3 Ways to Spot a Spear-Phishing Email

1. **Evaluate the Email's Basic Hygiene** - Even a cursory look at some spear-phishing emails reveals that something is just, well…"phishy." Often with these emails, you'll see poor grammar, misspelled words and unorthodox URLs. Also, regardless of who is sending an email, be sure to do a brief check to ensure the sender's domain and email address are accurate and known to you. Attackers will sometimes attempt to mask themselves as someone you know by changing a single character in a domain or username. For example, jane.doe@gmail.com might be changed to jane.doe@1gmail.com.

2. **Determine the Email's Content & Motivation** - Any requests for personal or financial information should be viewed with extreme caution, especially in business settings where attackers are keen to use spoofed emails from executives to target lower-level employees. One popular technique involves a fake email from a CEO to the finance team asking for the latest financial numbers or a request to move money into a certain account. Without proper awareness of such attacks, unsuspecting employees might be too quick to reply to the "CEO" request and potentially reveal sensitive information about the company. Bottom line? Be wary of any extraordinary requests in emails. A simple phone call or pop-in to the supposed requestor's office can go a long way in mitigating risk.

3. **Attachments & Link Landmines** - Downloading an attachment from anyone other than a verified, trusted source is perhaps the quickest way to get yourself in trouble when it comes to a phishing email. Attackers are aware of this and, as a result, will often use links inside of attachments to target victims. If you get an unexpected email from your bank, a shipping provider, or even a friend, some additional insight and verification is required.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.