BLACK FRIDAY eCOMMERCE BLACKLIST

What You Need to Know about Black Friday Threat Activity

For many consumers, it has become a Thanksgiving tradition, after stuffing themselves with turkey and cranberry sauce, to loosen their belts, fire up their laptops, and start their online shopping. According to Adobe Digital Index, in 2015, online shoppers filled eCommerce cash registers with more than $5.8 billion in sales over Black Friday weekend.

But ever the opportunists, threat actors set up their operations where the money is; and in the case of the Black Friday phenomenon, it's eCommerce. With more people than ever poised to partake in the November shopping frenzy in 2016, many threat actors will try to capitalize by using the brand names of popular e-tailers to exploit user traffic looking for Black Friday deals and coupons. They'll set up fake mobile apps and landing pages, often using fraudulent branding to fool consumers into downloading malware or giving up their login credentials and credit card information.

For shoppers, what starts out as an attempt to fulfill their holiday shopping checklist for pennies on the dollar can turn into a financial nightmare. For brands, what begins as an event that significantly boosts sales can turn into a security fiasco that erodes the trust between them and their customers and prospects—talk about indigestion.

eCommerce is Poised to Get a Big Slice of the Black Friday Pie

- In 2015, online spend exceeded $5.8 billion on Black Friday and Cyber Monday
- Adobe Digital Index calculated that shoppers spent $2.74 billion online on Black Friday alone in 2015, an increase of 14.3 percent over 2014
- Custora reported online revenue up 16 percent over 2014 Black Friday, with orders increasing 15.6 percent year-over-year
- Nearly 30 percent of spend on Black Friday and Cyber Monday will take place on mobile devices
- In 2015, it was discovered that 85 applications infected iPhone users with malware —something once considered unthinkable

The Proof is in the Stuffing

To analyze the methods threat actors will employ this shopping season and where they're targeting their malicious efforts, RiskIQ ran a keyword query of the RiskIQ Global Blacklist and mobile app database* looking

for instances of the brand names of five leading e-tailers in the United States. For our research into web properties, we looked for instances of each of the five e-tailer's branded terms appearing alongside the term "Black Friday" in blacklisted URLs or cause page URLs.

The findings confirmed that threat actors are using these well-known brands specifically to exploit the popularity of Black Friday shopping in both web and mobile.

**The source of RiskIQ's Blacklists is our collection of internet data, which our collection architecture of virtual users gathers by scanning, crawling, and passive-sensing the internet—including web pages, mobile apps and stores, and a variety of social websites and apps. RiskIQ's crawling technology covers more than 300 million mobile devices, 1.8 billion HTTP sessions, 783 global locations across more than 100 countries, 16 million mobile apps, and 300 million domain records.*

Mobile Findings

Nearly 30 percent of the massive influx of spend caused by Black Friday and Cyber Monday will take place on mobile devices, making shoppers increasingly at risk of encountering phishing pages, malicious apps, and viruses that infect their phones and tablets to steal money and data. Much of this potential damage comes from mobile apps built to fool users into entering credit card information, which opens them up to potential financial fraud. Some fake apps contain malware that can steal personal information or lock the device until the user pays a ransom. Others encourage users to log in using their Facebook or Gmail credentials, potentially exposing sensitive personal information.

Using RiskIQ data sets centered around malicious applications, we found:

- **Black Friday-specific apps:** 1 in 10 mobile apps out of the 5,315 that can be found by searching "Black Friday" in global app stores is blacklisted (unsafe to use) as malicious
- **All apps for leading five e-tailers:** Threat actors have focused on the top five leading brands in eCommerce. These brands have a combined total of more than one million blacklisted apps that contain their branded terms in the title or description
  - Brand 1: 12,971 Total, 1,093 blacklisted
  - Brand 2: 2,911,141 Total, 410,094 blacklisted
  - Brand 3: 39,443 Total, 6,367 blacklisted
  - Brand 4: 770,380 Total, 112,254 blacklisted
  - Brand 5: 3,121,706 total, 470, 522 blacklisted

Protect Yourself

While RiskIQ sees the majority of malicious applications hosted on third-party app stores that few American consumers know of, official stores run by Apple and Google have been observed hosting malicious apps. It's important to realize that protection by most mobile app stores is good, but not bulletproof, and even the official App Stores host apps that can be dangerous.

Fortunately, there are ways to help reduce digital risk during this holiday shopping season:

- Ensure that you are only downloading apps from official app stores such as Google or Apple
- Be wary of applications that ask for suspicious permissions, like access to contacts, text messages, administrative features, stored passwords, or credit card info.
- Just because an app appears to have a good reputation doesn't make it so. Rave reviews can be forged, and a high amount of downloads can simply indicate a threat actor was successful in fooling a lot of victims. Before downloading an app, be sure to take a look at the developer—if it's not a brand you recognize or has a strange appearance or spelling, think twice. You can even do a Google search on the developer for more clues about its reputation.
- Make sure to take a deep look at each app. New developers, or developers that leverage free email services (e.g., @gmail) for their developer contact, can be enormous red flags—threat actors often use these services to produce mass amounts of malicious apps in a short period. Also, poor grammar in the description highlights the haste of development and the lack of marketing professionalism that are hallmarks of mobile malware campaigns.

Web Findings

Adobe Digital Index calculated that shoppers spent $2.74 billion online on Black Friday 2015, an increase of 14.3 percent over Black Friday 2014. Custora reported online revenue up 16 percent over 2014, with orders increasing 15.6 percent year-over-year. With all the online activity around Black Friday, it's easy for threat actors' infrastructure to hide in plain sight—often using brand names in malicious URLs to fool people into visiting pages that phish for sensitive information, infect users with malware, or redirect traffic to other malicious or fraudulent pages.

In the RiskIQ Global Blacklist, we found:

- The top five retail brands leading in eCommerce have had a combined total

of more than 1,950* blacklisted URLs that contain their branded terms as well as "Black Friday" and are linked to spam, malware, or phishing

- Broken down by brand, you can see threat actors are purposely leveraging these brands' Black Friday presence for their campaigns:
  - **Brand 1**: 536 Total, 249 Spam, 218 Malware, 79 Phishing
  - **Brand 2**: 319 Total, 159 Spam, 142 Malware, 37 Phishing
  - **Brand 3**: 216 Total, 41 Spam, 140 Malware, 29 Phishing
  - **Brand 4**: 408 Total, 147 Spam, 218 Malware, 73 Phishing
  - **Brand 5**: 476 Total, 87 Spam, 194 Malware, 79 Phishing

**The blacklist events total may exceed the sum of the three because some are listed under multiple categories*

Protect yourself

When shopping this Black Friday, it's important to keep in mind that the internet may be more dangerous than you think—do your part to work with the security teams of major retailers. Follow these tips to avoid Black Friday scams:

- ⚠ Check website addresses after following links on Twitter, Facebook, or other social media channels to be sure you end up on the true website of the retailer you want.
- ⚠ Look for the "S" in HTTPS when you visit shopping sites. Beware of shopping sites that do not use HTTPS in their website addresses or do not display the symbol of a lock next to the web address. Secure sites use HTTPS, and without that, you're dealing with unsecured connections or weak encryption of personal data.
- ⚠ Never provide your credit card information unless you are in a secure online shopping portal. Sites that ask for it in return for "coupons" or to win "free" merchandise are almost always scams.