What You Need to Know about Black Friday Threat Activity

For many consumers, it has become a Thanksgiving tradition, after stuffing themselves with turkey, to loosen their belts, fire up their devices, and start their holiday shopping online. According to Adobe Digital Index, in 2016, online shoppers filled e-commerce cash registers with more than $5.27 billion in sales through Black Friday.

Ever the opportunists, threat actors set up their operations where the money is; and in the case of the Black Friday phenomenon, it’s e-commerce. With more people than ever poised to partake in the November shopping frenzy in 2017, 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. In this report, we’ll show how many fake mobile apps and landing pages—many of which use fraudulent branding to fool consumers into downloading malware or giving up their login credentials and credit card information—RiskIQ has detected in the wild and added to our global blacklist.

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.

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—brands you’re extremely likely to leverage this holiday shopping season. 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 (pages that send users to a page hosting something malicious).
The findings confirmed that threat actors are using these well-known brands specifically to exploit the popularity of Black Friday shopping via both web and mobile.

*The source of RiskIQ’s Blacklists is our comprehensive collection of internet data, gathered by our exclusive virtual users by scanning, crawling, and passively sensing the internet—including web pages, mobile apps and stores, and the most popular social networks. RiskIQ’s crawling technology covers more than 2 billion daily HTTP requests, 783 global locations across more than 100 countries, 20 million mobile apps, and 300 million domain records.

**Mobile Findings**

In 2016, almost **40% of sales** on what used to be a brick-and-mortar shopping weekend occurred on a mobile device over Black Friday and Cyber Monday, making shoppers increasingly at risk of encountering phishing pages, malicious apps, and viruses that infect their phones and tablets to mine sensitive 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:

- Nearly **40% fewer blacklisted apps** in Q2 2017 over Q1, which may be a result of increased awareness of mobile threats by consumers and app store owners.
- Black Friday-specific apps: 4% (1 in 25) of mobile apps out of the 4,356 that can be found by searching “Black Friday” in global app stores are blacklisted (unsafe to use) as malicious.
- At least 15 blacklisted apps for each of the top-five e-tailer brands containing both the branded terms and “Black Friday,” in the title or description, showing clear intent by threat actors to leverage the shopping holiday.
- All apps for leading five retail brands: Threat actors have focused on the top five leading brands in e-commerce. These brands have a combined total of more than 32,000 blacklisted apps that contain their branded terms in the title or description.

<table>
<thead>
<tr>
<th>BRAND 1</th>
<th>BRAND 2</th>
<th>BRAND 3</th>
<th>BRAND 4</th>
<th>BRAND 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>922</strong> TOTAL</td>
<td><strong>180,763</strong> TOTAL</td>
<td><strong>1,004</strong> TOTAL</td>
<td><strong>10,204</strong> TOTAL</td>
<td><strong>94,118</strong> TOTAL</td>
</tr>
<tr>
<td><strong>364</strong> (39.5%) BLACKLISTED</td>
<td><strong>8,090</strong> (4.5%) BLACKLISTED</td>
<td><strong>542</strong> (53.9%) BLACKLISTED</td>
<td><strong>3,245</strong> (31.8%) BLACKLISTED</td>
<td><strong>20,242</strong> (21.5%) BLACKLISTED</td>
</tr>
<tr>
<td>15 with “Black Friday” in the title or description</td>
<td>18 with “Black Friday” in the title or description</td>
<td>20 with “Black Friday” in the title or description</td>
<td>27 with “Black Friday” in the title or description</td>
<td>22 with “Black Friday” in the title or description</td>
</tr>
</tbody>
</table>

**Protect Yourself**

While RiskIQ sees the majority of malicious applications hosted on third-party app stores, official stores run by Apple and Google have also been observed hosting malicious apps. The Google Play store led the way in hosting blacklisted apps found by RiskIQ in Q2, and it was recently discovered that despite Apple’s rigorous testing and validation of apps, the App Store hosted 85 legitimate applications that infected iPhone users with malware. 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 data shows $5.27 billion was spent online by the end of Black Friday in 2016, a 17.7 percent increase YOY, and forecasts online sales will pass the $100 billion benchmark in 2017, landing at $107.4 billion—marking nearly 14 percent growth YOY. 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:

- 19,218 cause-page URLs contain “Black Friday”
- 10,175 Blacklist URLs contain “Black Friday”
- The top five retail brands leading in e-commerce have had a combined total of more than 1,451 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:

<table>
<thead>
<tr>
<th>BRAND 1</th>
<th>BRAND 2</th>
<th>BRAND 3</th>
<th>BRAND 4</th>
<th>BRAND 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>143</td>
<td>226</td>
<td>117</td>
<td>208</td>
<td>757</td>
</tr>
</tbody>
</table>
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 by following 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.

⚠️ 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.

⚠️ 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.