RISKIQ

Research By Steven Pon and Jordan Herman

Crucial Threat Intel for This Year's Black Friday/Cyber Monday Shopping Weekend

This Thanksgiving weekend, you can be sure that threat actors will be getting their fill, too.

Ever the opportunists, threat actors set up their operations where the money is; and in the case of the Black Friday and Cyber Monday phenomena, it's e-commerce. According to Adobe Digital Index, in 2017, online shoppers stuffed e-commerce cash registers with more than $19.6 billion in sales through the Black Friday weekend—a more than 15 percent increase over 2016.

With more people than ever poised to partake in this year's November shopping frenzy, attackers will capitalize by using the brand names of leading e-tailers to exploit users looking for Black Friday deals and coupons by creating fake mobile apps and landing pages to fool consumers into downloading malware, using compromised sites, or giving up their login credentials and credit card information.

In this report, we'll show how these attackers target the brands of:

- The 10-most trafficked e-commerce sites over the Black Friday Weekend
- Five of the leading e-tailers in the UK

The threat facing e-commerce this holiday shopping season is even more grave given the rise of Magecart, a collection of digital credit card-skimming groups that have stolen the records from an untold number of consumers across thousands of sites including British Airways and Ticketmaster. One of the leading traffic-getters on Black Friday, Newegg, has already been affected by Magecart earlier this year.

For shoppers, what starts 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 of customers and prospects. Talk about indigestion.

Once Again, E-commerce will Get a Big Slice of the Black Friday Pie

$19.6 billion

Consumers spent $19.6 billion in online sales over last year's Black Friday weekend, up 15.2% from 2016.

+

Cyber Monday 2017 was the largest online shopping day in history.

$2 billion

Mobile had its first $2B day on Cyber Monday 2017. The conversion rate on smartphones was up 10.1% to a rate of 3.5%.

40%

40% of all 2017 Black Friday online transactions took place on smartphones, up 11% from Black Friday 2016.

14.8%

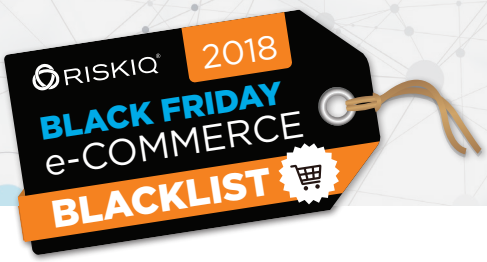
Consumer spending this holiday season is expected to increase by 14.8 percent from the same period in 2017.

$23.4 billion

Consumers will spend $23.4 billion online during this year's Thanksgiving holiday weekend,, up 19.4% from the same period in 2017.

$7.8 billion

Cyber Monday will be the biggest online shopping day in history, with $7.8 billion in e-commerce sales, up 17.6% year over year.



RISKIQ

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 above—brands you're extremely likely to leverage this holiday shopping season.

For our research into web properties, we looked for domain infringement and phishing events for each of the e-tailers, as well as instances of their branded terms appearing alongside the term "Black Friday" or "Cyber Monday" 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 and Cyber Monday 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, hundreds of locations across the world, 40 million mobile apps, and 600 million domain records.*

Mobile Findings

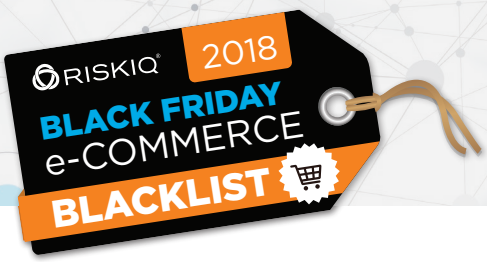
In 2017, 40 percent of all Black Friday online transactions took place on a mobile phone—$35.9 billion was spent via mobile devices, which accounts for a record-setting 33.1% of online holiday revenue. This makes shoppers increasingly at risk of encountering phishing pages, malicious apps, and viruses 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 adware and ad-clicks or 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.

RiskIQ also regularly blacklists apps that request excessive permissions including the ability to read sensitive log data, receive text messages (SMS), collect data from Internet, modify system settings, and steal other data.

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

- In total, RiskIQ observed 52,885 Blacklisted apps in Q2, which was 4% of all apps we saw and a 2% increase over Q1.
- Black Friday-specific apps: 5.5% of mobile apps out of the 4.324 that can be found by searching "Black Friday" in global app stores are blacklisted (unsafe to use) as malicious. 4.6% (44) of the 959 that can be found by searching "Cyber Monday" are blacklisted as malicious.
- The top-10 most trafficked brands averaged over 17 blacklisted apps containing both its branded terms and "Black Friday," in the title or description, showing clear intent by threat actors to leverage the shopping holiday.
- All apps for the 10 most trafficked retail brands: Threat actors have focused on these leading brands in e-commerce. They have a combined total of 6,615 blacklisted apps that contain their branded terms in the title or description.



RISKIQ

Top-10 most trafficked sites on Thanksgiving weekend 2017

BRAND 1	BRAND 2	BRAND 3	BRAND 4	BRAND 5
73,177 TOTAL	**27,460** TOTAL	**13,768** TOTAL	**7,115** TOTAL	**621** TOTAL
3,772 (5.15%) BLACKLISTED	**1,334** (4.86%) BLACKLISTED	**540** (3.92%) BLACKLISTED	**349** (3.28%) BLACKLISTED	**27** (4.35%) BLACKLISTED
45 with "Black Friday" in the title or description, **10** with "Cyber Monday"	**17** with "Black Friday" in the title or description, **5** with "Cyber Monday"	**30** with "Black Friday" in the title or description, **7** with "Cyber Monday"	**32** with "Black Friday" in the title or description, **509** with "Cyber Monday"	**3** with "Black Friday" in the title or description, **10** with "Cyber Monday"

BRAND 6	BRAND 7	BRAND 8	BRAND 9	BRAND 10
2,823 TOTAL	**4,012** TOTAL	**3,518** TOTAL	**4,254** TOTAL	**2,043** TOTAL
86 (3.05%) BLACKLISTED	**150** (3.74%) BLACKLISTED	**127** (3.61%) BLACKLISTED	**158** (3.71%) BLACKLISTED	**74** (3.62%) BLACKLISTED
4 with "Black Friday" in the title or description, **3** with "Cyber Monday"	**4** with "Black Friday" in the title or description, **1** with "Cyber Monday"	**17** with "Black Friday" in the title or description, **6** with "Cyber Monday"	**17** with "Black Friday" in the title or description, **6** with "Cyber Monday"	**4** with "Black Friday" in the title or description, **4** with "Cyber Monday"

Top-5 'Elite' Retailers (UK)

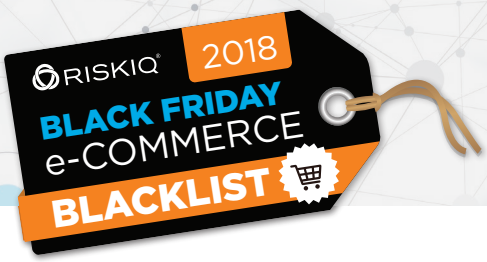
BRAND 1	BRAND 2	BRAND 3	BRAND 4	BRAND 5
1,262 TOTAL	**11** TOTAL	**600** TOTAL	**380** TOTAL	**4,753** TOTAL
58 (4.6%) BLACKLISTED	**0** (0%) BLACKLISTED	**23** (3.8%) BLACKLISTED	**11** (3.71%) BLACKLISTED	**179** (3.6%) BLACKLISTED
17 with "Black Friday" in the title or description, **6** with "Cyber Monday"	**17** with "Black Friday" in the title or description, **6** with "Cyber Monday"	**1** with "Black Friday" in the title or description, **1** with "Cyber Monday"	**0** with "Black Friday" in the title or description, **0** with "Cyber Monday"	**2** with "Black Friday" in the title or description, **1** with "Cyber Monday"

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. For instance, the Google Play store led the way in hosting blacklisted apps found by RiskIQ in Q2. 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 big 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.



RISKIQ

Web Findings

Adobe predicts Cyber Monday 2018 will be the biggest online shopping day in history with $7.8 billion in e-commerce sales, up 17.6% year over year. Black Friday will come in second with $5.9 billion in online sales, up 17.2% 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.

Domain Infringement

Domain infringement targeting brands, employees, and customers is a prolific, effective tool in the hands of attackers and has only grown worse in recent years due to the opening of thousands of new gTLDs, the growth of free and cheap domain registration services, and attack techniques like domain shadowing.

Because corporate attack surfaces are changing, threat actors are also changing their methods. Since business has moved many critical financial and data transactions beyond the firewall to the open internet, attackers are following suit, directly scamming end-users with high-volume phishing campaigns against consumers or targeted spear-phishing campaigns attempting to fool corporate employees.

These attacks are cheap to execute, and they are proving to be incredibly efficient in breaching sensitive data—a recent query of the branded terms of 20 Fortune 100 companies in RiskIQ's domain infringement detection revealed 37,000 probable instances of domain infringement over a two-week period or 1,850 incidents per brand.

RiskIQ detected:

145

145 incidents of domain infringement containing **"Black Friday"**

3,947

3,947 new hostnames containing **"Black Friday"**

365

365 new hostnames containing **"Cyber Monday"**

Magecart

Magecart is an umbrella term given to at least seven cybercrime groups that are placing digital credit card skimmers on compromised e-commerce sites at an unprecedented rate and with frightening success. In a few short months, Magecart has gone from relative obscurity to dominating national headlines and ascending to the top of the e-commerce industry's public enemy list and increasing in frequency.

Responsible for placing skimmers on scores of e-commerce sites and recent high-profile breaches of global brands Ticketmaster, British Airways, and Newegg, in which its operatives intercepted thousands of consumer credit card records, Magecart is only now becoming a household name.

RiskIQ, which detects internet-scale threats, is alerted to new Magecart breaches hourly, a clear indication that the group is extremely active and will continue to be a critical threat to all organizations offering online payment facilities, especially over the Black Friday weekend.

319,678

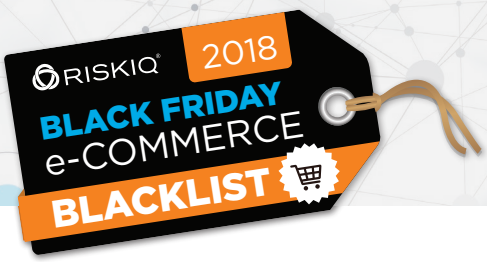
319,678 instances of **Magecart** in 2018

31,967

31,967 instances of **Magecart** in each month

89,837

89,837instances of **Magecart** between August and October



RISKIQ

Blacklisted URLs

Threat actors build out malicious infrastructure including URLs to leverage in their threat campaigns. We queried the RiskIQ Global Blacklist for URLs of malicious pages and pages that lead to malicious pages leveraging these brands as well as "Black Friday and "Cyber Monday."

We found:

727
727 Cause-page URLs contain **"Black Friday"**

732
732 Cause-page URLs contain **"Black Friday"**

776
776 Cause-page URLs contain **"Black Friday"**

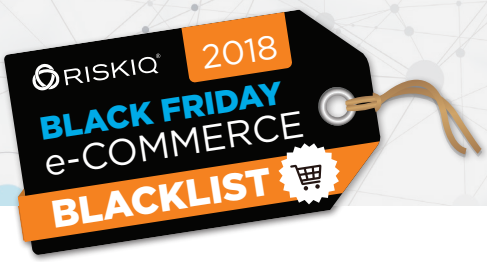
16
16 Cause-page URLs contain **"Cyber Monday"**

354
354 Blacklisted URLs contain **"Cyber Monday"**

363
363 sequence URLs contain **"Cyber Monday"**

Looking at a sample of five of the top 10 most trafficked sites on Thanksgiving weekend 2017, we found an average of 2,995 blacklisted URL containing their branded terms. Broken down by brand, you can see threat actors are purposely leveraging these brands for their campaigns:

BRAND 1	BRAND 2	BRAND 3	BRAND 4	BRAND 5
11,862	2,348	58	364	346



RISKIQ

Protect Yourself

When shopping this Black Friday weekend, 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.
- If possible, only use credit card information saved in your account as a payment method. This way, you can bypass typing in your credit card information to avoid it being intercepted by Magecart actors.
- If you do provide your credit card information, make sure 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.
- Keep a close eye on your bank and credit card statements so you can quickly dispute any suspicious charges.

RISKIQ

Learn how RiskIQ could help protect your digital presence by scheduling a demo today.

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by thousands of security analysts, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures. Visit RiskIQ.com or follow us on Twitter.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net
RiskIQ.com
1 888.415.4447
@RiskIQ