RSA FraudAction™ Intelligence

Black Friday and Cyber Monday Among Cybercriminals

Overview

Black Friday and Cyber Monday are just around the corner and are arguably the biggest shopping events of the year.

Transaction traffic is always exceedingly high, but every recent year has set a new spending record for consumers; according to predictions, 2020 will be no different with an estimation that sales will surpass $23 billion, about $6 billion more than last year.

The safety and health concerns caused by COVID-19 are the best reason to stay at home and shop online. Online shopping has increased drastically because of the pandemic, and this trend is not expected to change. A recent survey found that 84% of U.S. shoppers plan to shop online for Black Friday and Cyber Monday 2020, and this is not unique for U.S. shoppers but is common among western countries.

This presents cybercriminals with a fertile ground to set up successful cyber-attacks, including phishing, trojan, and rogue apps. Amidst the mayhem and shoppers' fear of missing the best deals, consumers are more likely to give away their credit card details to cybercriminals unwittingly.

RSA FraudAction's analysts and researchers analyze a wide range of cyber-attacks and monitor fraud forums and hacking forums on the darknet, underground marketplaces, open-web sources, and fraud groups in social media.

In this report we will share a glimpse into the different fraud scenarios surrounding the upcoming Black Friday and Cyber Monday events.

Many Forms of Fraud

FraudAction researchers have found that in addition to stealing payment data and credentials from unsuspecting shoppers, another common scam is selling bogus products and taking away consumers' hard-earned money without ever sending the goods.

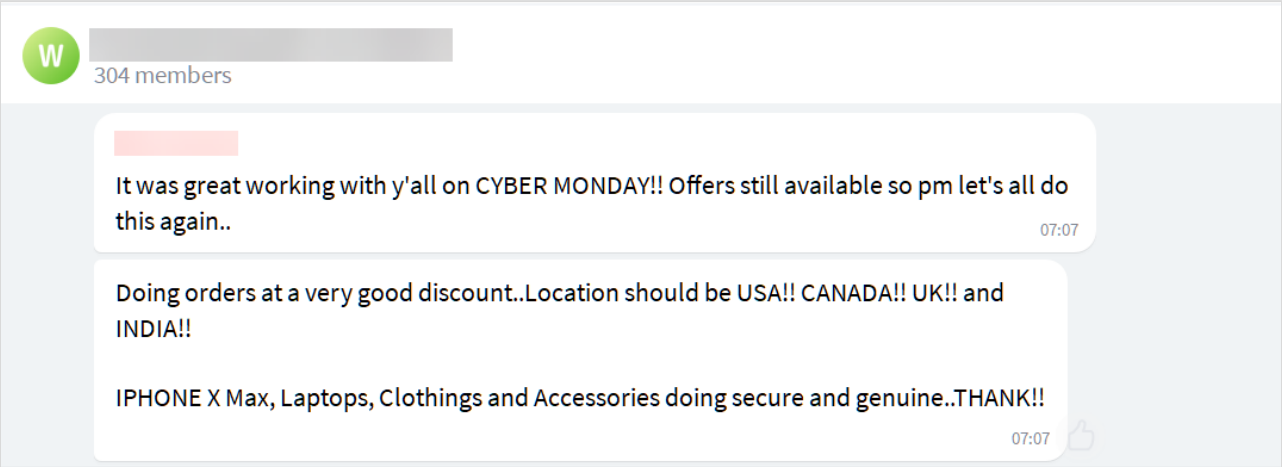

Figure 1: Fraudster thanking his peers for their successful carding on Cyber Monday

Figure 2: Fraudster would like to order a new phone with the stolen credit card information of a victim

Wide Range of Cyber-Attacks

FraudAction analysts have identified a wide range of cyber-attacks, including phishing, trojan, and rogue apps. Over the past month, the Anti-Fraud Command Center has detected over 800 newly registered domains containing keywords that are variations of Black Friday or Cyber Monday. This number is expected to increase as we get closer to these events. These domains might be used to spread or host phishing attacks.

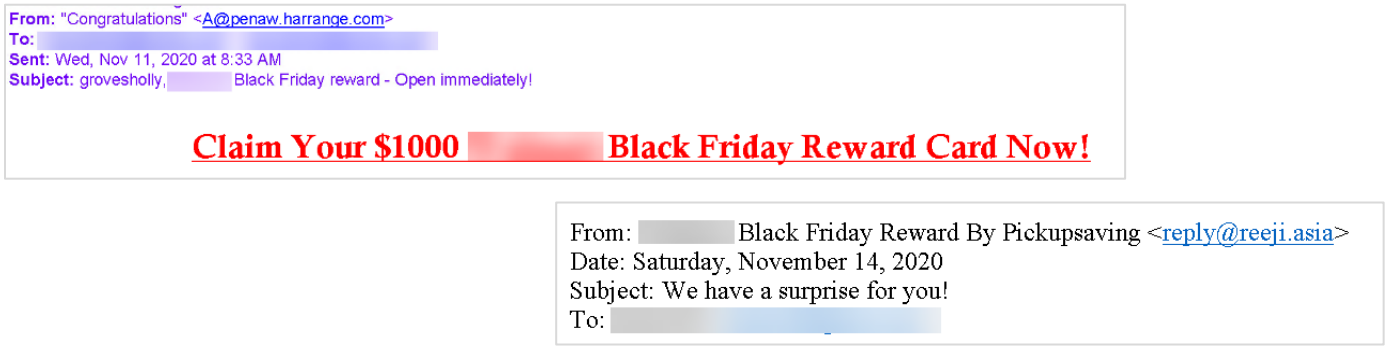

Figure 3,4: Examples of phishing fraud emails sent to consumers

Figure 5: Example of phishing attack hosted on a "Black Friday" domain

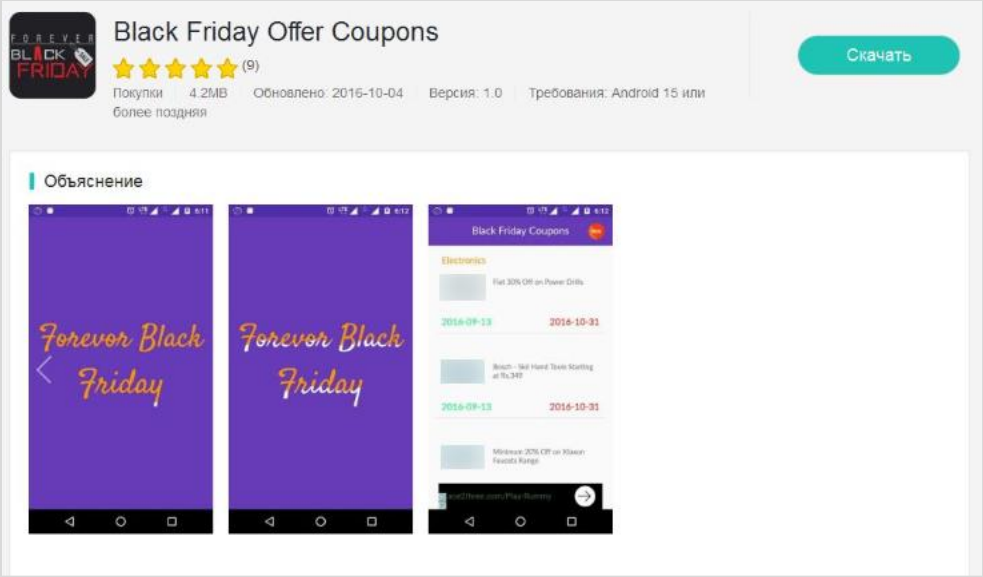

***Figure 5**: Rouge App offering coupons for Black Friday*

About RSA FraudAction

FraudAction offers its customers a holistic, all-encompassing solution for external threat management and brand protection. In addition to proactive detection and mitigation of a wide array of online threats such as phishing, trojans and brand abuse, customers also gain deep insight into emerging internal and external threats via a broad range of intelligence reports and data feeds that provide deep visibility into the cybercrime landscape.

With an all-encompassing 24/7 service, organizations can deploy fewer in-house resources to manage external cyber threats without leaving any vector uncovered.

FraudAction caters to hundreds of global customers, diverse in size and sector, including many of the top Fortune 500 companies. To support the different needs of each organization, FraudAction offers flexible subscriptions that can be customized based on attack volumes and areas of interest.

For additional information about RSA FraudAction please refer to FAS.Customer.Ops@rsa.com and a FraudAction representative will reach out to you.