For Authorized Use Only
TLP White

CYBER THREAT INTELLIGENCE

Threat Awareness – 2018 Holiday Season

Date: October 31, 2018

Moderate Risk	
Relevance	High
Impact	Moderate
Likelihood	Moderate
Confidence	High

[Scale is: High, Moderate, Low]

Summary:

Scams and Malware Campaigns are projected to increase this holiday season.

Holiday spending in the U.S. is projected to exceed $1.1 trillion, up more than 5% from 2017, according to an annual consumer survey from Deloitte.

- Fifty-seven percent of spending is expected to be online, compared to 36% in stores, according to Deloitte.

Threat actors are attracted to the opportunities to intercept transactions from the $1.1 trillion projected spending this year, and Threat assesses with high confidence, attacks will increase using the following tactics:

Card skimming:

- Roughly 107.3 million Americans will journey 50 miles or more from home during Dec. 23 through Jan. 1st according to AAA. Threat actors see this as a major payday – adding credit card skimmers in retail locations. In an attempt to combat these thieves, the Secret Service is ramping up their efforts this holiday season. Secret Service agents are inspecting fuel pumps around the US for illegal skimming devices that steal your credit card information.

  Guidance:

  - To reduce your chances of being a victim of a credit card skimmer, the Secret Service is advising customers to use cash, or pay using your credit card inside the store.

Point of Sale (POS) malware:

- Cybercriminals are becoming more adept, innovative, and stealthy by adopting more clandestine techniques to manipulate retail operations, and their attacks include the use of new variants of malware that relies on a unique technique to steal payment card information from point-of-sale (PoS) systems which is undetectable by antivirus software.
  - The new POS malware relies upon User Datagram Protocol (UDP) DNS traffic for the exfiltration of credit card information, security researchers at Forcepoint Labs, who have uncovered the malware, dubbed it UDPoS. Besides using 'unusual' DNS requests to exfiltrate data, the UDPoS malware disguises itself as an update from LogMeIn—a legitimate remote desktop control service used to manage computers and other systems remotely—in an attempt to avoid detection while transferring stolen payment card data pass firewalls and other security controls.

Targeting:

- Some of the common ways users get scammed is through malware disguised as something safe. For example, an e-card you receive from a gift may seem like a sweet gesture, but be careful, there may be malicious code disguised inside it. Criminals try

to lure unsuspecting individuals with free gifts and discount coupons during the holiday season. Victims of this ruse click on malicious links and fill out forms providing personally identifiable information which cybercriminals use to sell to other criminals who charge purchases with the victim's banking information and open lines of credit as the victim.

Guidance:

- Don't shop on Public Wifi, change passwords often, don't use the same credentials on multiple sites, check the URL of the site you are expecting to visit, ensure it matches your expectations, don't click on links to "great deals" in email (Go to the site directly), use credit card vs debit card.

Phishing campaigns:

There has been an increase in spam and phishing emails offering hard to beat bargains. Throughout the holiday season, advertising will increase with online and in-store discount offers. Cybercriminals will pose as retailers, sending phishing emails and enticing offers that unsuspecting shoppers may click.

Fake coupons tend to pop up on social media during major shopping holidays. Coupon scams generally start with a legitimate-looking image of a coupon with the retailer's logo in your feed and instructions to click the post to claim it. In reality, these coupons are cleverly designed phishing scams.

- **Targeting:**
  - Shoppers looking for deals, Shoppers waiting for their package,
    A security company is warning that cybercriminals are targeting Black Friday and Cyber Monday sales in massive phishing campaigns that attempt to steal personal and financial details from unsuspecting consumers. The goal is to convince consumers to register or log into what they think is their account in order to receive a gift card or discount. "Sadly, no gift card or bonus bucks will be received, but instead consumers end up surrendering their account credentials

Guidance:

- Consumers are advised to play it safe by not clicking through on any promotional Black Friday and Cyber Monday emails they receive but instead visit the intended site directly. In addition, consumers should check hyperlinks to make sure they look legitimate.

CYBER THREAT INTELLIGENCE

Threat Awareness – 2018 Holiday Season

Date: October 31, 2018

Credential Stuffing:
Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts.

- **Targeting:**
  - Users who reuse the same credentials across multiple platforms. Criminals use a password re-use attack.

- **Guidance:**
  - A password manager could help to deter this type of attack

Analyst Note:

Consumers should consider using a mobile payment app like Apple Pay, Google Pay or Samsung Pay rather than a physical card. Mobile wallets use a single-use token system that encrypts your card information. So, even if the retailer gets hacked, the information the data thieves steal won't be your real card number.

Do not reuse credentials across multiple platforms and consider using a password manager. Password managers keep all your passwords secure and helps you create different, strong passwords for each one of your accounts.

Be cognizant of things looking out of place, e.g. an ATM with the door partly opened, a fuel pump with wires hanging out or the card insert is harder than normal to insert. Pay inside whenever possible. Be aware of people shoulder surfing for your PIN.

Security Risks and Concerns:

Vulnerability perspective:

- Previous years have proven to be very lucrative for cyber criminals, thus there is no indication there will be decrease in cybercrime this coming holiday season

Threat perspective:

- Consumers should expect the unexpected. Cyber criminals' tactics have become extremely savvy. Some tactics are extremely challenging to distinguish from being nonfraudulent.
- It would benefit us all if we practice heightened awareness and caution when making online transactions this holiday season; verify then trust.

Next Steps:

- The Threat Intelligence team will continue to monitor for imminent cyber-attacks targeting customers and employees through online scams, phishing attacks, etc.

CYBER THREAT INTELLIGENCE

Threat Awareness – 2018 Holiday Season

Date: October 31, 2018

Sources:

https://www.experian.com/blogs/ask-experian/ecommerce-fraud-what-it-is-and-how-to-protect-yourself/

https://blogs.quickheal.com/beware-cyber-attacks-holiday-season/

https://www.makeuseof.com/tag/6-scams-watch-black-friday-cyber-monday/

https://siliconangle.com/2017/11/21/cybercriminals-targeting-black-friday-cyber-monday-massive-phishing-camgpaigns/

https://blackfriday.com/news/cyber-monday-security-tips

https://www.zdnet.com/article/phishing-attacks-why-is-email-still-such-an-easy-target-for-hackers/

Appendix 1 – Other common instances of ecommerce fraud include:

Chargeback fraud	**Chargeback fraud**, also referred to as *friendly-fraud*, occurs when a consumer purchases an item online with their own credit card but challenges the charges—telling their credit card provider they never received the items when they actually did receive the purchased items.
Billing fraud	**Billing fraud** occurs when the suspected victim's address is tied to the payment account used to purchase the stolen goods. Typically items are bought using the victim's billing address but then shipped to an address where the fraudster can pick up the items. Billing fraud is not location specific and can happen all across the country, whereas as shipping fraud tends to happen in certain areas near the coast or port cities.
Shipping fraud	**Shipping fraud** occurs when the delivery address used for the purchased good is actually for the fraudsters. Sometimes a business address is used as the shipping address and the business may or may not know they are part of a fraud ring. Shipping fraud activity is concentrated in coastal states with major port cities and airports.
Reshipping fraud	**Reshipping fraud** is a relatively new scheme targeting businesses and credit card owners. The scam begins when criminals buy high-dollar merchandise—such as computers, cameras, and other electronics—via the Internet using stolen credit cards. They then have the merchandise shipped to U.S.-based addresses of paid "reshippers" (who may be unaware they are handling stolen goods). These reshippers repackage the merchandise and mail it to locations internationally where the items can be sold.
Freight forwarder fraud	**Freight forwarder fraud** is a person or company that organizes shipments for individuals or corporations to get goods from the manufacturer or producer to a market, customer or final point of distribution.

Appendix 2: