Retail Advisory

‘Tis the Season: Preparing for the 2020 Shopping Holidays

NOVEMBER 2020

Cyberint

INTRODUCTION

Cyberint's threat intelligence analyst team leverages the Argos™ TI platform to follow threat actor activity, TTPs and threat trends affecting retail organizations on the dark, deep and open webs. Among these trends, in recent years the team has observed a marked increase in activity around several retail organization attack vectors in the days and weeks before the November & December holiday season. This season includes classic "shopping holidays", both official and unofficial, such as Singles Day (11/11), Black Friday (day after Thanksgiving), Cyber Monday (Monday after Black Friday), Super Saturday (Saturday before Xmas) and New Year's Eve (12/31). The correlation is clear and indicates threat actors are preparing for the season with increased fraud and cyberthreat activity, taking advantage of retailer discounts, higher sales volume, and often fraud controls that are relaxed to improve buyer experience.

This year the Cyberint team has observed an even larger rise in threat actor activity targeting retailers, as compared to the average for holiday seasons in past years. The assumption is that this phenomenon is related to increased online purchasing in 2020 due to the effects of the COVID-19 pandemic. A recent Qubit[1] study on U.S. and U.K. consumers found a sharp shift towards online spending in 2020, with 66% of respondents having increased online shopping since the start of COVID-19 and 44% planning to shop online this holiday season more than in 2019.

Based on the intelligence items and chatter detected, retail organizations should expect an increase in threat actor operations and fraud targeting their customers during the 2020 shopping holidays, and would benefit from preparing accordingly.

This advisory details the attack vectors where Cyberint tracked an increase in activity, showing examples detected by the Argos™ platform. It also lists the recommendations and best practices advised by the Cyberint team for mitigation of the different threats described.

[1] https://www.qubit.com/blog/christmas-in-july-consumer-behavior-infographic/

ATTACK VECTORS

RANSOMWARE

RANSOMWARE

- In 2020 ransomware continued to consolidate its place as one of the major threats to organizations worldwide. Throughout the year, almost every known ransomware group began adhering to the relatively recent "business model" combining data encryption and data exfiltration; exfiltrated data is published on the ransomware group's news site in order to pressure the victim into paying the ransom.

- The infamous Maze Group has ceased operating since early November, but several other ransomware variants are vying for the top spot in the market (Egregor, Ragnar Locker, etc.).

- With the upcoming holiday season, Cyberint is seeing the retail sector being increasingly targeted. Many ransomware operators are moving to Egregor, which was responsible for recent attacks on retailers such as Barnes & Noble[2] and Cencosud (largest retailer in Chile)[3].

- Cyberint has also observed a rise in Ransom DDoS (RDDoS) threats in recent months by actors claiming to be known APT groups (Fancy Bear, Lazarus Group, etc.). Retailers should be prepared for increased targeting in their sector, with DDoS attacks having the potential to affect consumer experience and impact holiday sales negatively.

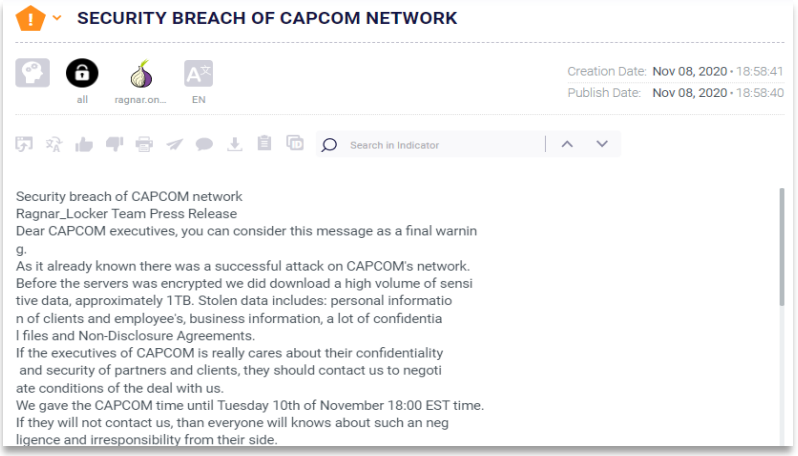

Figure 1: Dark web news site for Ragnar Locker ransomware announcing breach of game maker Capcom, as seen on Argos™

RECOMMENDATIONS

1. The entry point of ransomware for victim organizations is commonly spear-phishing emails; email gateway protection is crucial as well as adding proper Endpoint Protection controls (EDR, updated antivirus). Avoid spoofing through correct configuration of DMARC and SPF.

[2] https://www.bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/
[3] https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/

2. System backup strategy and best practices should be followed in order to be able to recover data and renew operations as soon as possible after ransomware attacks.
3. Implement a business continuity plan in case of a real attack, including well sharpened IR procedures.
4. Focus on employee awareness to spear-phishing attacks and other entry points.

PHISHING TARGETING CUSTOMERS

PHISHING SITES

- **Argos™ indicates an 117% rise in phishing sites targeting retail organization customers in November, as compared to the 2020 average.**
- A large amount of these attacks employ "site cloning" whereby threat actors duplicate customer interfaces by fully copying their source code, and leverage them to harvest victim credentials. To obfuscate their activity, clone sites may employ geo-blocking or redirect users when accessing from outside of a targeted region.

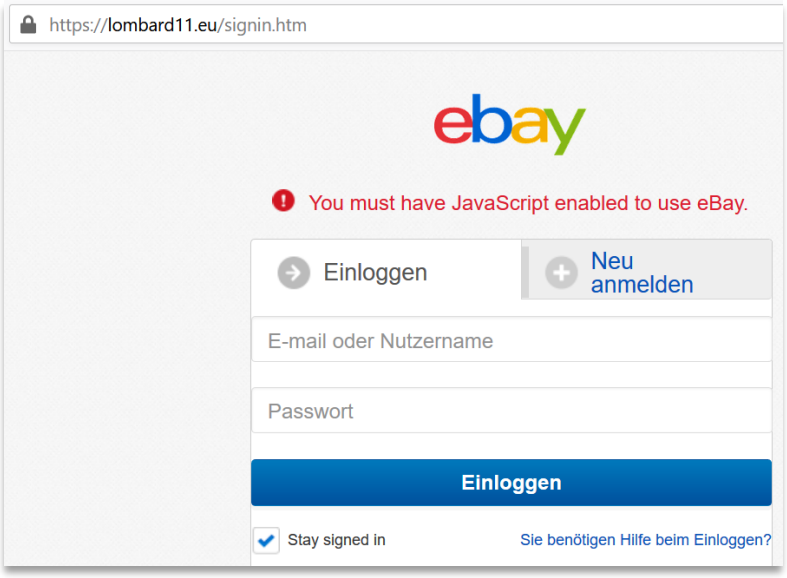

Figure 2: "Site Cloning" for the eBay site

LOOKALIKE DOMAINS

- **Argos™ indicates an 125% rise in newly registered lookalike domains (domain squatting) targeting retail organization customers in November, as compared to the 2020 average.**
- Several of these are clearly registered for the purpose of holiday season attacks, as they reference "Black Friday", "discounts" and "coupons".
- These lookalike domains can be weaponized in a short span of time through hosting phishing content or adding an MX record and sending phishing emails.

SOCIAL MEDIA BRAND IMPERSONATION

- Cyberint observed a recent increase in threat actor activity originating in China focusing on impersonation of retail organization customer service agents or social media profiles.
- The threat actors primarily target customers who are seeking assistance on issues such as product returns or changes to orders. To gain trust from victims the scammers may "offer" refunds or other benefits, in an attempt to phish their credentials.

RECOMMENDATIONS

1. Raise customer awareness of phishing in preparation for the shopping holidays.
2. Implement a "site cloning" solution such as Cyberint's phishing beacon, alerting on site code being pasted on non-company pages.
3. If phishing sites are detected, a DMCA takedown request should be filed with the host. For lookalike domains, legal steps such as domain dispute (UDRP) should be considered.
4. Although this might create friction during sales season and is therefore less relevant, consider implementing MFA or One Time Password on customer retail login interfaces in order to reduce possibility of account takeover with stolen credentials.

FRAUD ACTIVITY

CARDING

- **Argos™ indicates a 290% rise in stolen payment cards for sale on major dark web payment card marketplaces in November, as compared to the 2020 average.**
- Stolen payment cards are commonly "cashed out" through carding, where threat actors purchase goods from online retailers with the payment card details. The goods are usually resold for a profit. Many threat actors prefer to purchase digital goods (videogames, gift cards, etc.) as no physical residential address needs to be given for product delivery, making the carding process more anonymous.
- **Argos™ indicates an 110% rise in threat actors searching for or offering carding "tutorials" and services in November, as compared to the 2020 average.** Many of these tutorials leverage failures in payment card checks on the online retailer website, such as CVV checks.
- Cyberint has observed an increase in mule reshipping fraud since the start of the COVID-19 pandemic, due to rising unemployment. Mules are hired by threat actors (usually under the guise of legitimate work) to receive goods ordered through carding and reship them to the threat actor. This allows the threat actor to remain anonymous and will prevent raising any red flags when the item is being ordered (as the residential address seems legitimate).

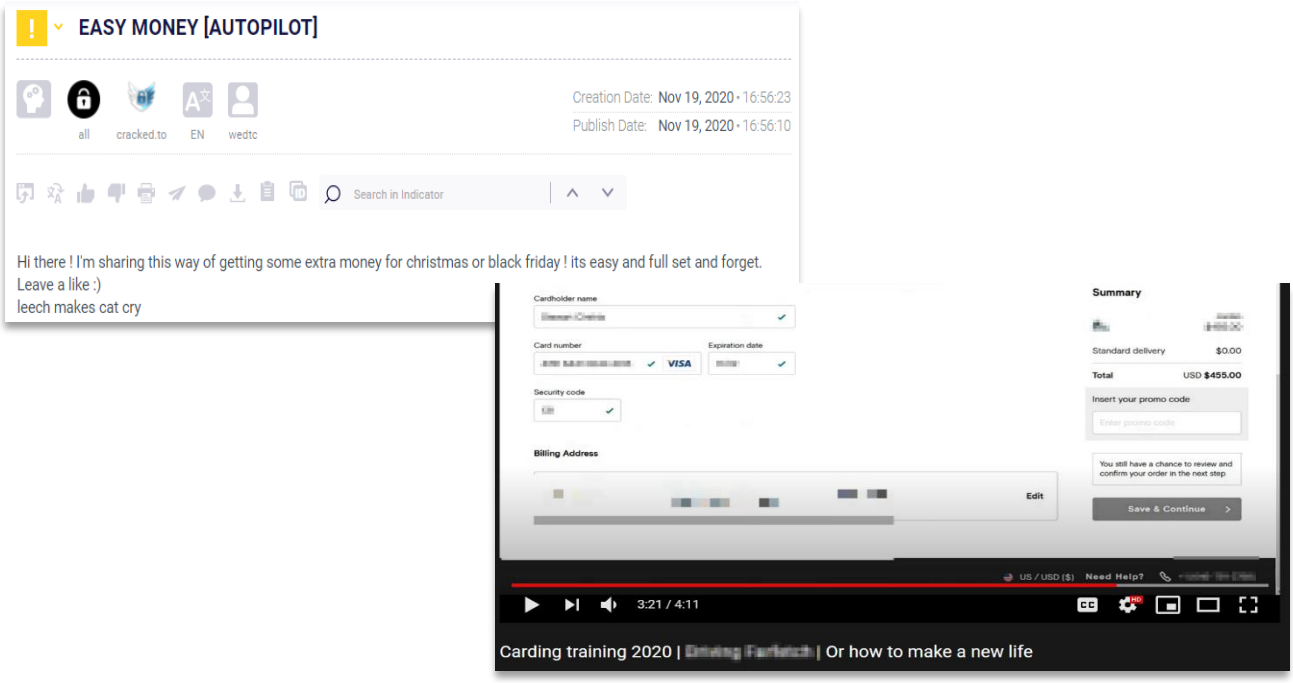

Figure 3: Carding tutorials offered free on a deep web forum and on YouTube

GIFT CARDS & COUPONS

- **Argos™ indicates an 175% rise in gift card and coupon fraud activity in November, as compared to the 2020 average.**
- Gift cards are popular presents for friends and family during the holiday season; last year 54% of shoppers opted to buy these as gifts during this time period according to the 2019 U.S. National Retail Federation (NRF) survey[4]. Gift cards are often targeted by criminal actors as they are easy to monetize anonymously.
- One popular method used by threat actors to obtain gift cards is through generators, software capable of generating potential gift card numbers in large quantities based on the retail organization's algorithm. Once generated, these numbers are automatically checked for a funds balance against the retailer site (through bots or "checkers"). Where balance is found, the threat actor will either utilize the number for online purchases or resell for a profit.
- Coupon codes are also often generated by threat actors, and checked against the retailer website on product checkout. Shopping holidays tend to see larger numbers of coupons distributed by retailers, raising the possibilities of generators coming across valid ones.

[4] https://nrf.com/media-center/press-releases/half-holiday-shoppers-have-already-started

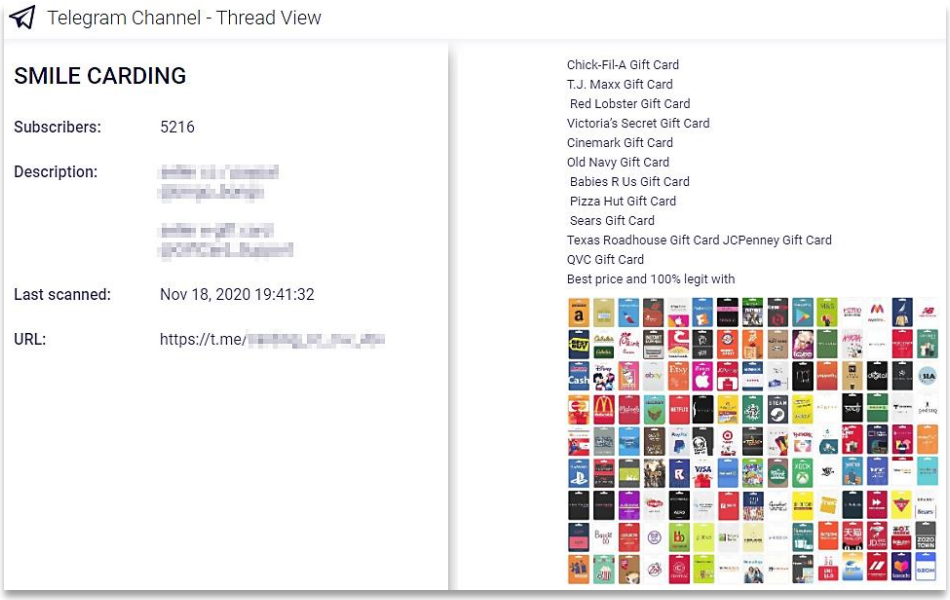

Figure 4: Telegram channel selling stolen gift card details, as seen on Argos™

RETURN FRAUD

- Fraudulent refund services and tutorials continue to be offered on dark web forums. Threat actors file fraudulent chargebacks exploiting retailer good faith policies, claiming products have not arrived or were not the products purchased. The business impact for retailers is direct revenue loss as well as inventory management process manipulation.

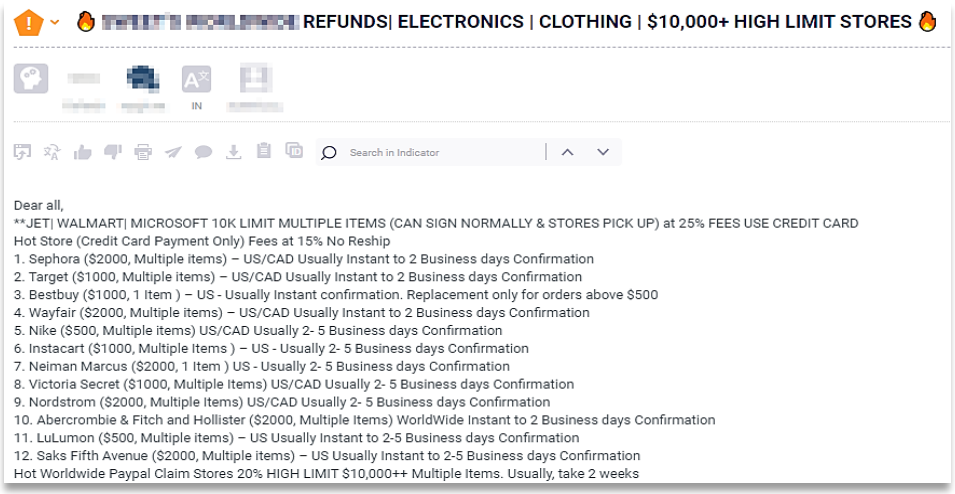

Figure 5: A threat actor offering refund services on a crime forum, as seen on Argos™

RECOMMENDATIONS

1. Many retailers tend to relax internal fraud monitors during the holiday season in order to improve buyer experience. However, the shopping holiday period sees increased fraud activity, meaning retailers stand to take a heavy hit in terms of revenue loss and reputation damage from both legitimate and non-legitimate chargebacks, as well as higher operational costs. Fraud checks on buyer payment card should be tweaked and heightened in preparation.

2. Verification methods for returns and chargebacks should be enforced in order to prevent fraudulent refund requests being successful.

3. For gift card generators, the ultimate way to avoid these types of fraud would be replacing online balance checks with phone value-checks. On the other hand, companies who wish to keep the online interface should increase gift-card structure complexity, and implement strong and secure CAPTCHA tests to prevent automatized checking.

4. Work closely with Cyberint in order to map out fraudulent methods and tactics, including internal threats, thereby covering the entire fraud map.

CUSTOMER CREDENTIALS EXPOSED & FOR SALE

CREDENTIAL-HARVESTING MALWARE

- **Argos™ indicates an 186% rise in retail organization customer credentials harvested by malware in November, as compared to the 2020 average.**

- Botnets and malware operators are attempting to expand their operations in preparation for large-scale account takeovers during the shopping holiday season. Retail customer credentials are often harvested by keyloggers, sending user inputs to the botnet C&C server. Credentials are then used by threat actors to carry out fraudulent transactions, or monetized on dark web marketplaces.

ACCOUNT MARKETPLACES

- **Argos™ indicates an 110% rise in retail organization customer accounts (credentials) for sale in major dark web marketplaces in November, as compared to the 2020 average.**

- Dark web marketplaces and seller platforms are used to monetize stolen retail customer credentials. These credentials are stolen in various forms, including phishing and malware. In cases where malware was used, each record can contain additional information on the victim's digital fingerprint (OS, browser, IP address, cookies, etc.), which are leveraged by threat actors to impersonate the victim and avoid raising red flags on fraudulent transactions.

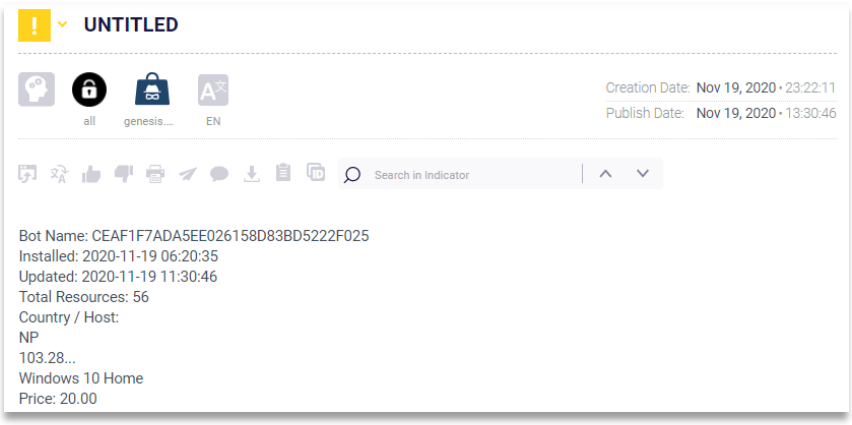

Figure 6: Retail customer credentials for sale on Genesis marketplace, as seen on Argos™

RECOMMENDATIONS

1. Encourage good credential hygiene on customers such as not reusing passwords, enabling MFA and prompting for verification whenever significant changes are made to an account. This will avoid account takeover and fraudulent transactions resulting in victim chargebacks.

2. Fraud internal monitoring and checks on buyer residential address, IP address, etc. should be tweaked and heightened in preparation for the holiday season.

3. If exposed customer credentials are detected, aside from password reset it is recommended to clean the victim's machine (in cases of malware infection, the new reset password would be harvested as well).

ATTACK TOOLS

CREDENTIAL STUFFING

- **Argos™ indicates an 130% rise in credential stuffing tools shared or offered for sale, and an 110% increase in "combo list" sharing activity in November, as compared to the 2020 average.**

- Credential stuffing tools (or "account checkers") automatically bulk test lists of breached credentials for different services ("combo lists") against online retailers to identify credential reuse and accounts for takeover. Many checkers extract pertinent account information from any valid account, such as details of any payment card, and the subscription status. The information is then either directly abused or traded on underground forums and marketplaces.

- Based on ongoing monitoring and techniques found by Cyberint, attacks of this type are originating from massive botnets globally, to perform low-and-slow attacks that will go under the thresholds of controls in place (e.g. number of sign in attempts per IP per minute).

- In a recent example, outdoor retail giant The North Face suffered a successful credential stuffing attack in early October and had to reset the passwords for some of its customers.[5]

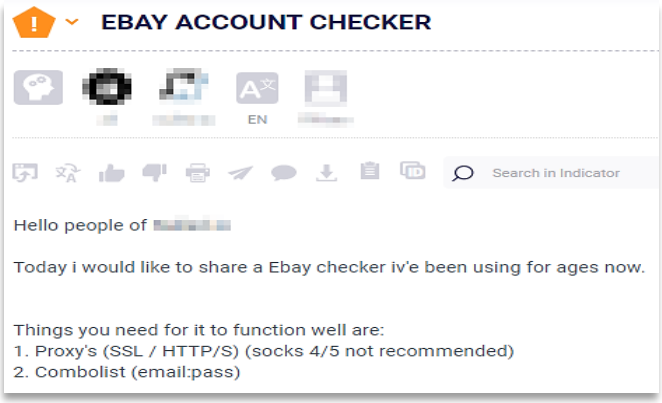

Figure 7: An account checker for eBay, as seen on Argos™

[5] https://securityaffairs.co/wordpress/110952/data-breach/the-north-face-credential-stuffing.html?utm_source=feedly&utm_medium=rss&utm_campaign=the-north-face-credential-stuffing

CARDING BOTS

- The time period preceding the shopping holidays is high season for carding, but before using stolen payment card details for fraudulent purchases threat actors often validate the details on retailer websites using automated tools called carding bots. These perform brute-force or "card stuffing" attacks on retailer websites, testing thousands of stolen cards with low-value purchases which, when successful, "validate" the relevant cards have a balance and have not been blocked.

- In 2019, Cyberint observed bot traffic increasing on retailer sites in this time period, in comparison to legitimate traffic which tends to drop due to buyers saving purchases for the discounts on the holidays themselves. This is expected to occur again in 2020.

PURCHASING BOTS & CART ABANDONMENT

- Purchasing bots are automated tools which are utilized to reserve and purchase goods on retailer sites, often to take advantage of a certain promotion or discount faster than human users. Sometimes they even register new accounts, in order to take advantage of welcome discounts. The products are commonly resold to members of the bot operator's instant messaging group (hosted on Discord, Slack, Telegram, etc.).

- Cart abandonment occurs when these bots add items to the cart but leave them unpurchased, rendering them unavailable for other buyers. This not only impacts customer experience leading to revenue loss and churn, but also retailer pricing algorithms and stock purchasing decisions.

- Cyberint has also observed logic-based DoS attacks on retailers, where attackers attempt to reserve as much stock as possible forcing backend teams to scale up their operations in order to allow this traffic. This resulted in higher operational costs for the retailers involved.

RECOMMENDATIONS

1. Monitor for systematic attempts to query the database from the same HTTP client (based on IP, User Agent, device, fingerprint, patterns in HTTP headers, etc.).

2. Limit the number of payments attempts that can be made from one IP address within a certain period of time.

3. Consider blocking user access to the checkout or payment page if the cart is empty.

4. Consider turning off reservations specifically for the holiday season in order to minimize potential "Destruction of Inventory" attacks, that may impact other customers and computing resources.

5. Restrict automated process by one of the following:

    - Fingerprinting

    - Reputable methods such as geo-location and/or IP address block lists.

6. Beware other signs of malicious bot activity during this time period, including:

- Increased checkouts on carts with one low-value item
- Increased chargeback filing
- Increased payment authorizations from one common IP address or device.

7. Deny access or enforce enhanced CAPTCHA tests against suspicious IP addresses such as those associated with known public proxies, VPN endpoints and Tor exit nodes. Consideration can also be given to IP addresses associated with cloud infrastructure providers although legitimate customers using corporate networks may also be proxied.
8. Flag transactions where IP address and billing country do not match for further monitoring.
9. Monitor for, and alert on, high volumes of account activity, especially failed login attempts that may be indicative of credential stuffing attacks.
10. Ensure websites and ecommerce platforms are adequately secured to prevent the exposure of sensitive data including application programming interfaces (API).
11. Ensure that mobile applications are adequately protected to thwart or complicate attempts to mimic their behavior.
12. Network traffic monitoring can lead to the identification of anomalous traffic, such as that originating from unusual geolocations or at unusual times, as well as allowing the investigation of unexpected peak activity.

SKIMMING

PAYMENT SKIMMING ATTACKS

- In recent years, payment skimming attacks have become a major threat on e-commerce platforms. Threat actors commonly exploit vulnerable plugins to gain access to the target site and inject malicious JavaScript code. Once injected, payment data and credentials entered by users through their browser will be exfiltrated.
- One of the main skimming groups is Magecart, primarily targeting online shops using the Magenta platform, but also WordPress and Shopify.[6] In September 2020, one of the largest Magecart attacks was exposed, affecting 2,800 online stores using Magenta 1, which ceased being supported in June 2019. It is believed that the attackers used a 0day Magenta exploit sold for $5,000 just several weeks prior, allowing remote code execution without the need of an admin account[7].

RECOMMENDATIONS

1. Ensure e-commerce platforms are updated to their latest versions.

[6] https://geminiadvisory.io/wp-content/uploads/2020/07/Appendix-C-1.pdf
[7] https://sansec.io/research/cardbleed

2. Continuously monitor 3rd party JS scripts embedded on sites, and closely check for any signature changes using the industry's best practices, in order to prevent the hijack of a 3rd party.

3. Follow PCI DSS Requirements in order to minimize attacker surface for code injection and skimming attacks.

CONCLUSION

All evidence found by Cyberint and detailed in this advisory points to a high probability of the 2020 holiday season being one of the most eventful in recent years in terms of fraudulent activity and cyberattacks. This is in direct correlation to increased online sales volume due to the effects of the COVID-19 pandemic, including retail physical store closures with lockdowns and lower consumer appetite for physical purchases.

Cyberint advises retailer organizations use the upcoming days to prepare for the shopping holidays and peak sales periods in the next two months, following the recommendations set out in this advisory. During the holiday season Cyberint will provide its clients with enhanced detection and support in order to mitigate threat actor activity as widely as possible. Clients are encouraged to share any attack IOCs (IPs, domains, email addresses, etc.) or suspicious account activity for Cyberint to conduct further investigation and threat intelligence enrichment on.

Happy holidays!

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City