Radware Cybersecurity Alert

E-Retailers' Shopping Season Threats
A Virtual Door-Busting Survival Guide

Nov 18, 2020

E-Retailers' Shopping Season Threats

A VIRTUAL DOOR-BUSTING SURVIVAL GUIDE FOR ONLINE RETAILERS

This Shopping Season Will Be Crucial

2020 retail sales were down significantly because the pandemic forced many brick and mortar stores to find new ways of generating revenue. Cloud computing became strategic for survival as retailers transitioned to ecommerce business models. New players are joining established, mature and experienced ecommerce businesses. The competition for consumers will be fierce as survival will depend on online performance. This holiday season will be crucial for retailers and it will be spent mostly online.

In its recently published **Analytics Holiday Forecast report**, Adobe forecasted this year's holiday spend to represent two years of growth in a single season.

> *"U.S. online holiday sales will total $189 billion, shattering all previous records with a 33% YoY increase. Online sales will surpass $2 billion every day between Nov 1-21 and increase to $3 billion a day Nov 22-Dec 3. Black Friday is projected to generate $10 billion in online sales, a 39% YoY increase, and Cyber Monday will remain the biggest online shopping day of the year with $12.7 billion, a 35% jump YoY."*
>
> **ADOBE ANALYTICS**

Knowing and understanding the most important cyberthreats your ecommerce business will face is crucial this holiday season.

User Experience and Digital Trust

Availability and user experience are crucial to online success. When online shopping is sluggish, not accessible, or critical components such as checkout and payment processing fail repeatedly, shopping cart abandonment rates increase and visitors will bounce.

An online brand and reputation will be undermined if your website falls victim to fraudulent bots that take over customers' accounts and use their credit cards, gift cards or premium discounts. The very measures you implemented to generate customer loyalty and stickiness increase the risk from fraudsters.

If you have the misfortune to fall victim to a data breach and your customers' sensitive data leaks, digital trust and reputation can be damaged for years.

Major Threats

ACCOUNT TAKEOVER

Account takeover (ATO) attacks are amongst the most harmful types of bot attacks in terms of financial and reputational damage for ecommerce business. They result is user accounts being compromised to execute theft of account balances, including money, store credits, gift cards and loyalty points. ATO attacks rely on lists of breached or stolen account credentials to take over user accounts on websites and applications.

The two main types of attacks employed in ATO are **credential stuffing** (multiple log-in attempts to verify the validity of stolen username and password combinations) and **credential cracking** (trying out different usernames and password combinations to identify valid login credentials).

During the shopping season, many ecommerce shops have special sales or deals reserved for premium customers. The holiday season is also the season of gifts, so not surprisingly many personal accounts will have new credit via recently redeemed gift cards. For this reason, Radware witnesses increased ATO activity in ecommerce customers during the holiday season.

Impacted by massive changes in consumer behavior that began due to the pandemic, the growth of digital gift cards is expected to accelerate this holiday season. Further impacting ecommerce are malicious actors that leverage breached accounts and bots for tokens or gift card cracking.

During an ATO attack, the objective of the attacker is testing credentials, either generated or based on a purchased list of recently leaked accounts, as fast and efficiently as possible. ATO campaigns typically concentrate around the login page and can easily reach levels of activity similar to DDoS attacks.

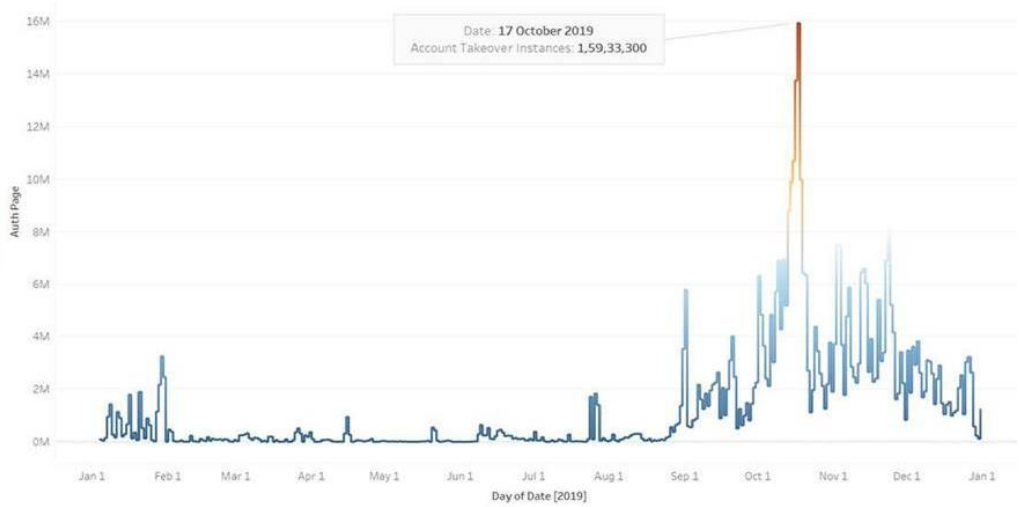

Figure 1: Number of account takeover attacks from bots on login page of Radware ecommerce customer

In some cases, ATO might not even be distinguishable from a DDoS attack. It is in the attacker's best interest to keep the server going and not disrupt it so the attacker can continue their malicious activity.

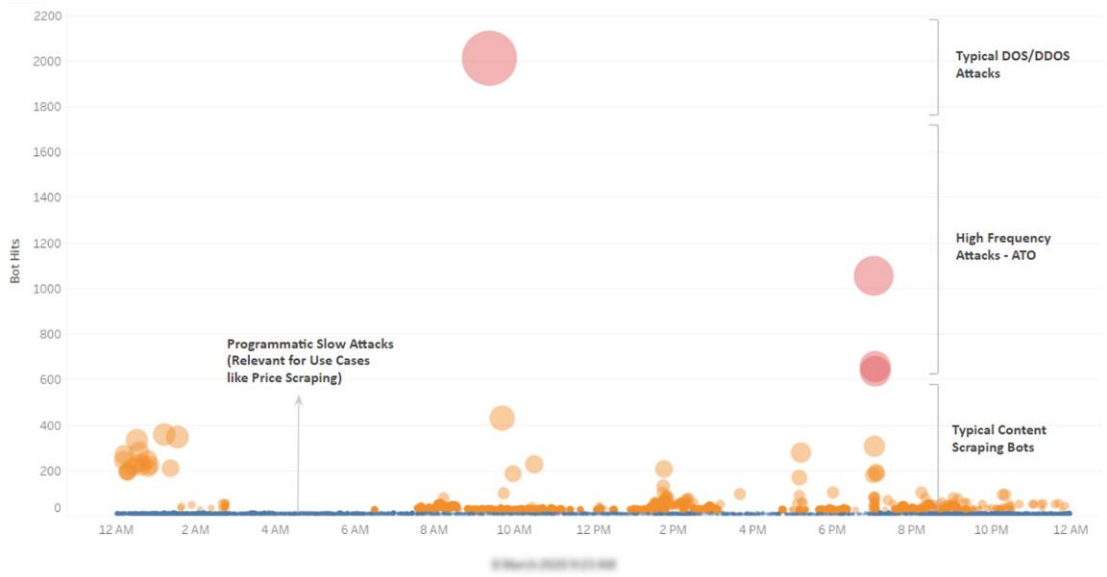

Figure 2: All traffic to a customer website over the course of one day

Even if ATO does not impact infrastructure performance, it severely impacts customers who will experience long login times, failed logins caused by timeouts, etc. Even if ATO, low and slow DDoS attacks, and content scraping activity from bad bots do not immediately disrupt services and customer experience, they tax resources and result in inflated charges from the cloud hosting provider to the ecommerce company.

DATA BREACH

Ecommerce operations require personal and sensitive data to operate, including mailing addresses, email addresses, phone numbers, payment details stored for convenient checkout, etc. These operations are a ludicrous target for malicious actors that like to leverage sensitive data for extortion or sell account lists on underground forums. The latter in turn will be used to perform credential stuffing and ATO attacks.

Data breaches in ecommerce can take many forms:

- Data can leak from a vulnerable API or web service
- Accounts can be compromised via ATO
- The organization or cloud infrastructure could have been compromised, either through its remote access infrastructure using known vulnerabilities in remote access solutions, from a successful phishing attempt, or through ATO in enterprise remote access or cloud infrastructure management

- A ransomware could be at the origin, when the attackers were not successful extorting you for a decryption key they might fall back to blackmailing and threatening to publish sensitive customer information acquired during the encryption phase of their attack
- The application stack can fall victim to supply chain attacks that exfiltrate sensitive information through compromised application modules running on the server or in the client's browser

The attack surface for a data breach is considerable and securing against it impacts the whole of the organization and third parties. Regular patching, web application and API protection, third-party audits, penetration testing, and employee education and awareness campaigns are all critical.

SUPPLY CHAIN ATTACKS

Protecting online applications requires an increasing amount of attention to the supply chains that makes up a modern web application. Following a string of fraudsters, such as **Magecart**, pilfering payment details in payment skimming attacks, the Payment Card Industry (PCI) **highlighted** this emerging threat that requires urgent awareness and attention.

Threat actors use various methods from exploiting vulnerable plugins, credential stuffing, phishing and other social engineering techniques to gain access to ecommerce sites and inject malicious code. These attacks can target the ecommerce site directly or can target a third-party application and service such as advertising scripts, live chat functions, customer review and rating features, etc. Once compromised, the third-party services are used to inject malicious JavaScript code into the target websites. Because these third-party functions are typically used by many ecommerce sites, the compromise of one of these functions can allow an attacker to compromise many websites at the same time through mass distribution of the malicious JavaScript.

The malicious code is often triggered when a victim submits their payment in the target website. Data entered by users through their browser are directly exfiltrated from the client and can include billing address, name, email, phone number, credit card details, username and even clear-text password.

PRICE SCRAPING & SKEWED ANALYTICS

Price scraping is the process of using bots for illegal competitive price monitoring and tracking other valuable information related to pricing intelligence from ecommerce and travel sites. Competitors employ this strategy to copy dynamic pricing information (which is one of the most important strategies used by ecommerce portals to influence consumer-buying decisions and optimize revenue) in real-time, so that they can attract price-sensitive buyers by setting their prices lower than baseline prices in the marketplace. While pricing information is generally available to consumers, price scrapers try to undercut competitors' pricing and growth strategies. Price scraping also results in skewed analytics, cart abandonment and degraded website performance.

Bots are not only used to scrape content and pricing, but also contribute to skewed site analytics. Both good and bad bots contribute to skewed analytics. If there are unexpected spikes in your analytics reports,

chances are that these are from bot activities or it be a legitimate spike in website performance. How can you be sure?

CART ABANDONEMENT

Cart abandonment happens when bots are used by competitors and fraudsters to add items to shopping carts on ecommerce sites, but instead of buying them, are left unpurchased. Cart abandonment is also called 'Denial of Inventory' (OAT-021 — 'Deplete goods or services stock without ever completing the purchase or committing to the transaction') by the OWASP Automated Threats to Web Applications Project, and ranks among the most serious bot threats to ecommerce websites and applications.

CARDING

Carding is an automated form of payment fraud in which fraudsters test a bulk list of credit/debit card data against a merchant's payment processing system to verify the stolen card details. Such card details are stolen from different payment channels, another application, or purchased from darkweb marketplaces. Hackers also apply card cracking practices to obtain credit card details.

The primary reason behind carding attacks is to illegally purchase goods or cash out the cards. Hackers deploy bots on payment processing pages to verify the validity of stolen card details. The authenticity of stolen card details are often unknown to the carders, and therefore, bots are deployed on payment processing pages to compose the correct set of card details. After identifying the right set of card details, hackers can sell them on darkweb marketplaces or simply cash out the cards.

SERVICE DEGRADATION AND DISRUPTION

An inaccessible website cannot generate revenue. When a service is unavailable, sluggish and has failing components such as checkout and payment processing, even loyal customers will leave. During times of heightened promotions and privileges, the result is increased customer churn and lasting reputation/credibility loss.

Service degradation and disruption can be the result from aggressive ATO campaigns but can also come from targeted DDoS attacks, illegally leveraged by a competitor to gain an edge and take a share of your revenue.

The **DDoS-for-hire threat landscape has been growing** despite global efforts by researchers and law enforcement. People with bad intentions will not find it hard to get access to a DDoS-as-a-Service portal or an attacker for rent. Booter and stresser services provide the convenience of a cloud application with prices starting as low as $10 per month to perform an unlimited number of attacks with an attack power of 15Gbps.

Competitors leverage DDoS attacks as well. For example, **court papers** revealed in January of 2019 an employee from Cellcom Liberia approached a self-taught hacker, Daniel Kaye, who offered individuals his skills to target and destroy their business rivals. Outside of the knowledge of Cellcom, he offered Kaye $10,000 per month to use his skills to destroy the reputation of its competitor, Lonestar. Kaye's Mirai botnet was so aggressive it knocked the whole of **Liberia offline** in November of 2016.

Protecting your Online Business

To secure your revenue this holiday, you should ensure the availability, efficiency, and security of your online applications with solutions that enable you to manage automated threats, defend against disruptive DDoS attacks and protect your web applications and APIs against vulnerabilities and intrusions.

MANAGE AUTOMATED THREATS

The major automated threats for ecommerce are ATO, price scraping, skewed analytics, cart abandonment and carding attacks. These threats can be detected and managed or mitigated using a bot management solution.

Besides the traditional browser clients, an increasing number of ecommerce sites use mobile applications to provide a better user experience and more customization and personalization features that will impact the buying behavior. The backend of these mobile applications are provided by Web Application Programming Interfaces (APIs).

"Americans will spend $28.1 billion more on their smartphones vs. 2019, accounting for 42% of all online sales, a 55% increase YoY."

ADOBE ANALYTICS

A bot management solution should provide protection for both websites and APIs, support traditional browsers but also native mobile applications. Mobile applications use the same protocol (HTTPS) but with different content and in different behavioral patterns compared to websites. Traditional device identification, client behavior and CAPTCHA are mostly useless and will reduce the accuracy of bot detection solutions. Mobile applications require a native SDK solution that integrates with the app.

DEFEND AGAINST DDOS ATTACKS

An adequate DDoS protection will ensure the availability of your online business. DDoS protection comes in different forms and factors. It is important to remember that you will need to protect against all potential threats, including those that are not all revealing and completely disrupting but are insidious and impacting enough to cause failures and annoy visitors or significantly increase your cloud hosting expenses.

PROTECT WEB APPLICATIONS AND APIS

Protect yourself against known vulnerabilities, web application attacks, and API manipulations in online applications. Ensure not to fall victim to massive exploit campaigns run by malicious actors seeking to steal sensitive information or leverage your trusted site to deliver malware or skim for credit card information. And do not forget: protect web APIs.

PROTECT AGAINST ONLINE SKIMMING

Web-based or online skimming attacks infect ecommerce websites with malicious JavaScript code and are very difficult to detect as they do not generate server-side events. Once a website is infected, the sensitive information is "skimmed" from a JavaScript function that runs from the context of the client browser, triggered by a transaction in that webpage. The backend (web server or API) does not take part in the extraction or exfiltration or even executes the code.

Regular reviews and audits of third-party services and products should be performed, ensuring they adhere to industry best practices, standards or regulatory compliance. The ability to detect these threats before they cause damage is significant.

The controls provided by the Payment Card Industry Standards PCI DSS Requirements enable you to detect and minimize the attacker surface for code injection and online skimming attacks:

- Reviewing code in order to identify potential coding vulnerabilities (Req. 6)
- Use of vulnerability security assessment tools to test web applications for vulnerabilities (Req. 6)
- Audit logging and reviewing logs and security events for all system components to identify anomalies or suspicious activity (Req. 10)
- Use of file-integrity monitoring or change-detection software (Req. 11)
- Performing internal and external network vulnerability scans (Req. 11)
- Performing period penetration testing to identify security weaknesses (Req. 11)

Conclusion

This document only covered the major threats online businesses face. It is critical that both consumers and providers stay vigilant so not to fall victim to malicious actors and scammers. Online business will be the only way this year to recover a fraction of the losses incurred because of the pandemic.

It is important to be aware of the risks and understand that security is a shared responsibility that includes retailers, cloud hosting providers and consumers. Malicious actors have ways to automate their exploits and are able to maximize their reach, such that there is very little probability to escape the consequence of an oversight or negligence.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks

- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.