RESEARCH REPORT

The Rising Tide of E-commerce Fraud: Methods, Patterns, and Defensive Measures

November 20, 2019

Key Takeaways

- On average, retailers experience 206,000 web attacks a month.
- Attacks happen constantly, every day of the week, using increasingly sophisticated and innovative tactics.
- Criminal behavior often mirrors that of legitimate shoppers in order to hide attack activity amid increased transaction volume. As consumer activity rises during the holiday shopping season, so do attacks against e-commerce sites. While it's important for retail businesses to safeguard their mission-critical web apps and mobile apps at all times, this is especially crucial during peak shopping periods.
- Attacks tend to spike on day 15 and day 30 of the month, as well as on weekends, following the tendency of consumers to shop on paydays and on their days off.
- The most common types of attacks used by e-commerce threat actors include account takeovers, bot impostors, attempting known backdoors, cross-site scripting, and SQL injection attacks.

E-commerce is booming — and so is online retail fraud. While retailers celebrate sales projected to reach over **$630 billion*** by 2020, they also face persistent and sophisticated attacks by cybercriminals. In the U.S. alone, threat actors will cause more than **$12 billion*** in losses by next year. And direct financial losses are only part of the picture, as bad customer experiences further damage the company's brand and reputation.

Signal Sciences inspects over **70 billion** web requests and blocks over **2 billion** web attacks monthly for customers operating e-commerce sites. For this report, Signal Sciences analyzed a sample of 4.9 million retail web attacks to identify key trends in e-commerce fraud. By better understanding the nature of the threat, and common methods and patterns in their usage, online retailers can take more effective, proactive countermeasures to prevent fraud and protect their business.

Retail Average Monthly Web Attacks

A typical medium to large scale retailer serving web traffic of roughly 3 billion requests per month experiences approximately 206,000 web attacks monthly.

Signal Sciences

Top Five Attacks Against E-commerce Sites

Attackers use a variety of sophisticated methods to attack e-commerce sites or abuse APIs that connect payment processors to online shopping carts. The goal of the attack is generally to steal credit card information, guess shopping cart tokens to take over the shopping session, or exfiltrate consumer account PII (personally identifiable information) that can be used to perpetrate other fraud.

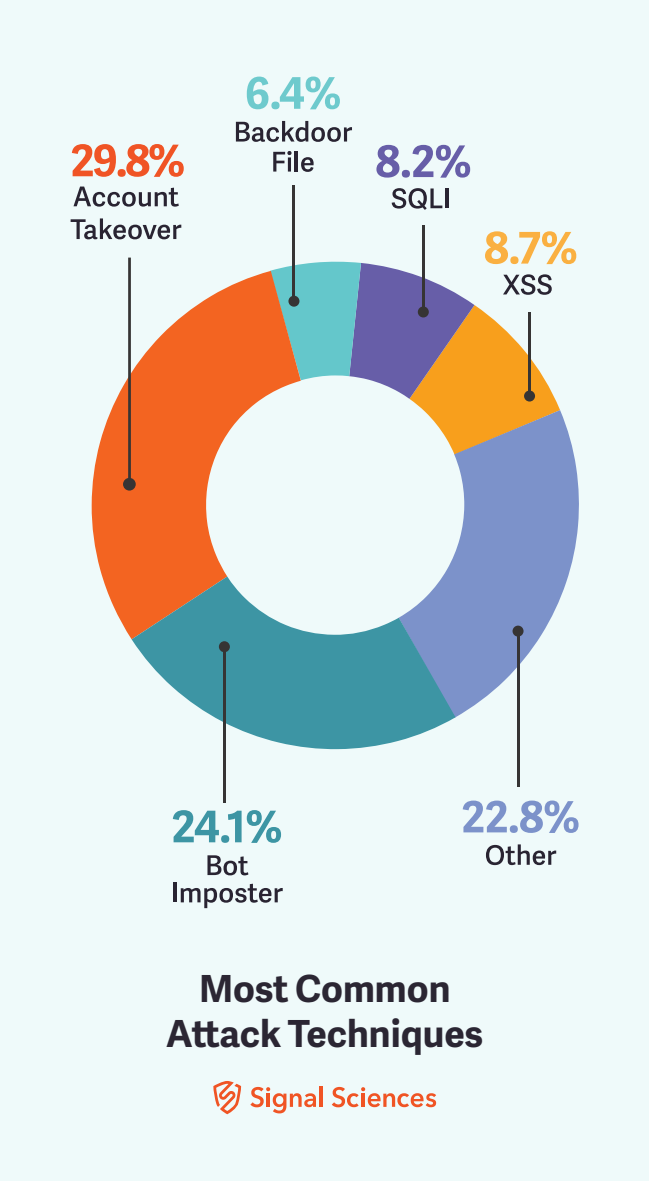
Signal Sciences' telemetry found that the most common techniques for attacks impacting retail e-commerce organizations were:

1. **Account Takeover**
   The automated process of testing stolen user credentials against the authentication flow of a website. When an attacker finds valid user credentials, they enter the victim's account; change account recovery settings (such as email, phone number, and answers to account verification questions); and lock the victim out. At that point, the attacker can fraudulently order goods and services on the initial website, as well as run automated tests of the same valid user credentials against other major finance and e-commerce sites to conduct further fraudulent activity.

2. **Bot Impostor**
   A malicious web request intended to masquerade as a Google or Bing search bot. Within an e-commerce context, such bot impostors seek to gather pricing and inventory data.

3. **SQL Injection (SQLI)**
   An attempt to gain access to an application or obtain privileged information by executing arbitrary database queries.

4. **Cross-site Scripting (XSS)**
   An attempt to hijack a user's account or web-browsing session through malicious JavaScript code. Attackers use this method against e-commerce sites to take over a consumer's shopping cart and have the goods shipped elsewhere for resale.



5. **Backdoor File**
   An attempt to access backdoor tools installed on applications or APIs, allowing hackers to gain remote access and introduce additional attack activity into the retailer's environment.

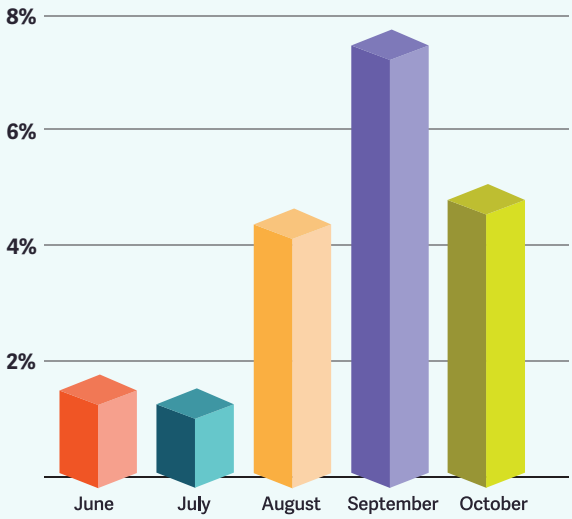
Additional types of attacks in the "other" category include private file, attack tooling, command execution, malicious IPs from a known list, directory traversal, datacenter traffic, CVE (known vulnerability), forceful browsing, PHP code injection, and Tor traffic.

Backdoor Files: The Fastest Growing Malicious Behavior

As retailers with e-commerce sites intensify their defensive measures during the critical holiday shopping season, they should monitor their server instances carefully for backdoor file attempts, which are rising quickly in prevalence. A backdoor file is often delivered via malware that identifies and exploits vulnerable components in a web application; in other cases, the hacker may simply use an unchanged default password to log into the user's account. In either case, the installation of the backdoor file makes it possible for the hacker to negate normal authentication procedures and access the system freely. At that point, the threat actor can execute a wide range of malicious activities including:

- Data Theft
- Website Defacing
- Server Hijacking
- Distributed Denial of Service (DDoS) attacks

Serving as the "keys to the kingdom" for attackers, a backdoor file can be a highly lucrative type of attack — accounting for its strong and growing popularity.



Backdoor File Attempts by Month

(% of total web attacks)

Signal Sciences

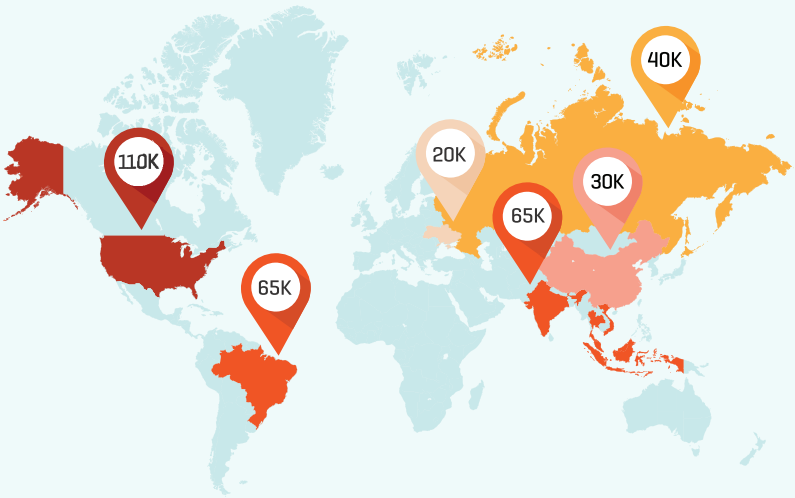
The Origins of Online Retail Web Attacks

While e-commerce attacks originate from locations around the world, the largest number of malicious web requests come from the United States, followed by countries in Southeast Asia.

Top Attack Sources by Country

Average Monthly Volume

Signal Sciences

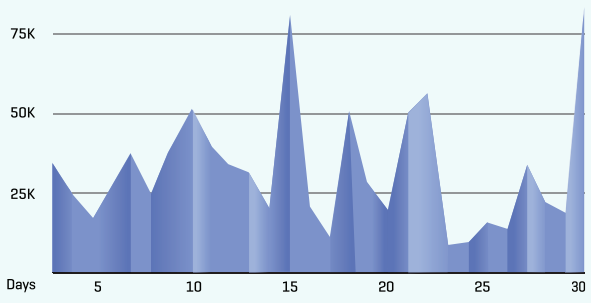


Analysis of web request data across e-commerce organizations reveals that attacker web requests originating from the United States utilized advanced attack tooling and were more widely distributed. Threat actors from the United States typically used multiple IP addresses to perform attacks in an attempt to learn an organization's security system behaviors — making them harder to detect and track.

By comparison, threat actors based in other nations (Indonesia, Malaysia, India and Brazil) tend to utilize the same IP address to perform high volumes of malicious web requests, making them easier to catch and have their attack attempts thwarted.

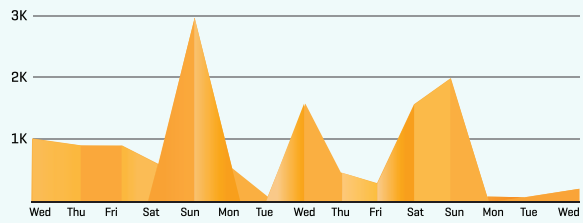
When Do Attackers Strike?

E-commerce sites are under constant attack as threat actors send malicious web requests or otherwise seek to exploit the retailer's payment flow or login process. Web attacks tend to spike on weekends. Criminals may hope that as consumers log into their accounts to shop on their days off, automated testing of stolen user credentials will blend in with the increase in overall web traffic. Similarly, an examination of daily attack volumes over a 30-day period from the start to the end of the month shows major attack spikes on day 15 and day 30. An obvious correlation is that many organizations issue paychecks on those days, leading to increased online shopping volume. Again, this provides better cover for illicit activity — and greater opportunities for attackers to get "paid," too.



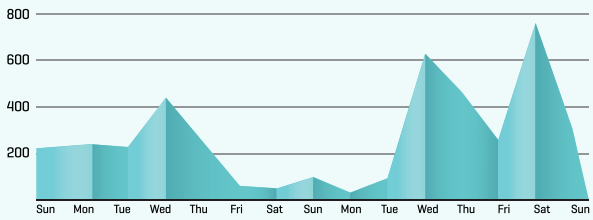
30 Days Attack Trend
(Daily Attacks)
Signal Sciences

While attackers use the full range of methods throughout the week, including cross-site scripting, backdoor file, SQL injection and others, they show a preference for account takeovers during weekends.



Account Takeover Attacks
2 Weeks View
(Daily Attacks)
Signal Sciences

When it comes to growing backdoor file activity, there does not appear to be a pattern in terms of common days of the week or month for such attempts. In any given time period, attackers use a variety of methods, trying one tactic and then another until they succeed in penetrating web apps that allow access to valuable customer data and fraudulent transactions.



Backdoor File Attempts
2 Weeks View
(Daily Attacks)
Signal Sciences

Take Action

To prevent fraudulent transactions, companies with an e-commerce presence must protect the retail sites and mobile apps that power their shopping experience. Proactive web defense requires identifying and blocking malicious traffic from those seeking to perpetrate web attacks that result in e-commerce fraud losses.

An effective online retail web defense strategy must incorporate:

Visibility: Gain insight into granular web request volumes, the types of attacks threat actors attempt, when and where attacks occur and originate, and how attackers seek to exploit a web app.

Flexibility: Accommodate different users — from security, to development, to operations — by providing feedback loops with actionable attack data and integrating security tools into common DevOps tools.

Threat Detection and Mitigation: Execute automated rapid response to block attacks while allowing legitimate traffic through to web apps, which is critical for high volume retail sites. Make sure your solution inspects and makes decisions based on the abusive nature of requests instead of just blocking a list of static IP addresses.

Scalability: Utilize security technology with coverage across every platform and infrastructure in use by the organization.

Methodology

The findings in this paper are drawn from analysis of anonymized web traffic directed at actual retail e-commerce apps, APIs, and microservices in the e-commerce vertical. This report summarizes a sample of 4.9 million web attacks over a five-month period from June 1 to October 31, 2019. These web attacks are identified from events where the source IP address of a web request crossed a defined attack threshold volume.

About Signal Sciences

Signal Sciences is the fastest growing web application security company in the world. With its award-winning next-gen WAF and RASP solution, Signal Sciences protects over 28,000 applications and over a trillion production requests per month. Signal Sciences patented architecture provides organizations working in a modern development environment with comprehensive and scalable threat protection and security visibility. The company works with some of the world's most recognizable companies, like Under Armour and WeWork, across industries, including five of the top e-commerce companies, five of the largest software companies, in addition to many others in the financial services, retail, healthcare, media and entertainment, and government sectors. Signal Sciences is the recipient of InfoWorld's Technology of the Year and Computing's DevOps Excellence Award for Best DevOps Security Tool. For more information, visit Signal Sciences or follow @SignalSciences.

Source:

* The Nilson Report - Issue 1142, Nov. 2018