perimeterx | Whitepaper

Protecting E-commerce Sites from the Growing Threat of Carding Attacks

Table of Contents

Executive Summary

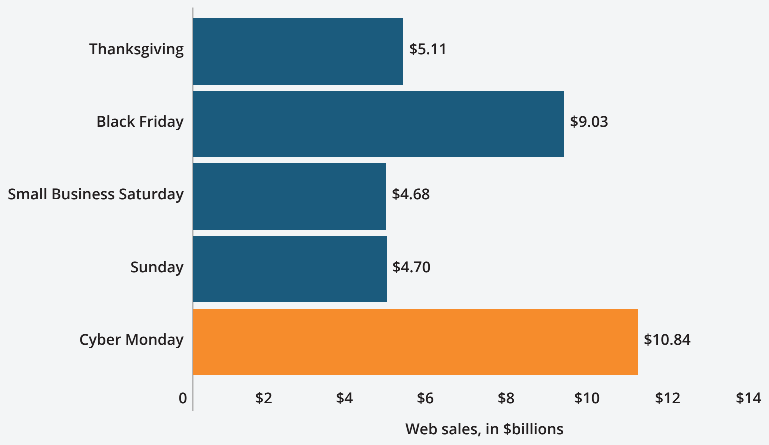
U.S. shoppers spent a record $34.36 billion on retail websites over the five-day period from Thanksgiving to Cyber Monday in 2020. This is a 21% increase from $28.49 billion for the same period last year. Shopping trends defied predictions this year as COVID drove buying patterns from in-store to online.

All this online activity did not escape the attention of scammers, and fraudsters increased their level of attacks while turning to automation to increase their efficiency and to find ways to bypass web application security measures.

Digital fraud negatively impacts a number of processes within the e-commerce buyer's journey, from the login page to the checkout page and everywhere in between.

US consumers spent more than $34 billion online during Cyber 5

2020 ecommerce sales by day, in $billions



Source: Adobe Analytics, December 2020

U.S. shoppers spent a record $34.36 billion

on retail websites over from Thanksgiving to Cyber Monday in 2020.

The PerimeterX research team investigates carding attacks as part of a wide range of bot attacks across many e-commerce, travel and hospitality, and consumer services, looking specifically at web and mobile applications that accept online payment transactions. This research led to the discovery of interesting trends in malicious carding attacks leading into the online holiday shopping season.

While investigating these increasing attacks against checkout pages during the months leading up to the holiday shopping season, the team warned of previously unknown carding bots. This paper covers two key carding bots that were identified by our researchers. The first, dubbed the canary bot, exploits top e-commerce platforms, which could have a significant impact on thousands of websites if they are not blocked. The second, dubbed the shortcut bot, exploits the card payment vendor APIs used by a website or mobile app and bypasses the e-commerce website entirely.

Fraud Goes Digital, Business Impact Deepens

The increase in digital fraud mirrors the growth in online transactions. The impact from digital fraud influences many facets of the business including unrealized revenue, damage to the brand due to erosion of customer confidence and the impact from higher operational costs related to payment processing fees and penalties.

Login Page	**Checkout Page**	**Product and Pricing Page**	**Web Analytics**
ACCOUNT ABUSE	**CHECKOUT ABUSE**	**SCRAPING**	**SKEWED ANALYTICS**
Account Takeover (ATO) Fake Account Creation	Carding Hoarding Scalping	Pricing Scraping Content Scraping	Skewed Dashboards Skewed AB Testing
Damage Brand and Consumer Confidence	Lost and Unrealized Revenue	Increased Cost of Payment Processing	Faulty Business Decisions from Bad Data

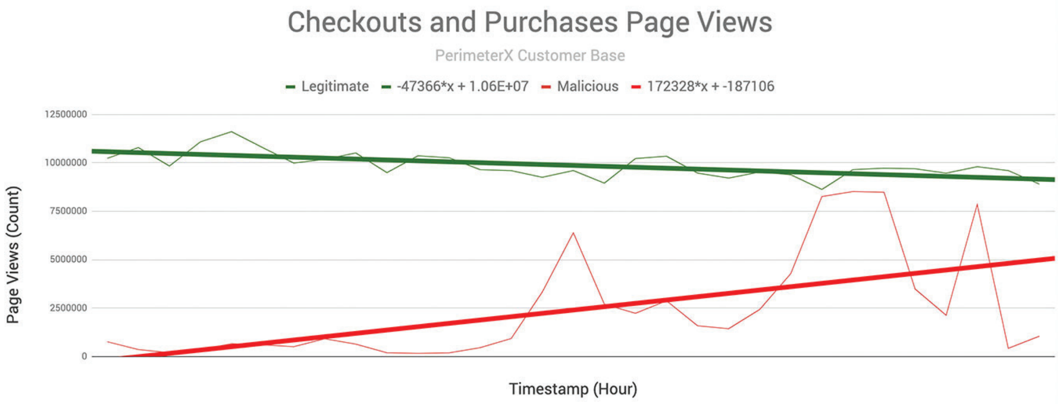
PerimeterX Uncovers Carding Bots

PerimeterX security experts observed that the regular checkout pattern of human traffic increased during business hours, versus the pattern of the bot traffic, which had no correlation with the time of day. In analyzing this pattern, two malicious types of carding bots were identified:

- Canary carding bots
- Shortcut carding bots

In both types, the attackers tested their carding attack methods with increasing sophistication on every iteration.

The graph below shows the checkout page traffic across PerimeterX customers just prior to the holiday shopping season. Real shoppers, as opposed to bad actors, tend to buy less before the holiday season. They save for the holiday season and wait for Black Friday and Cyber Monday discounts on big ticket items. It is clear that just before the holiday season started, there was a 15% drop in legitimate traffic and a significant uptick in malicious traffic—an increase of over 700%. This trend confirms that carding attackers are preparing for the holiday season.



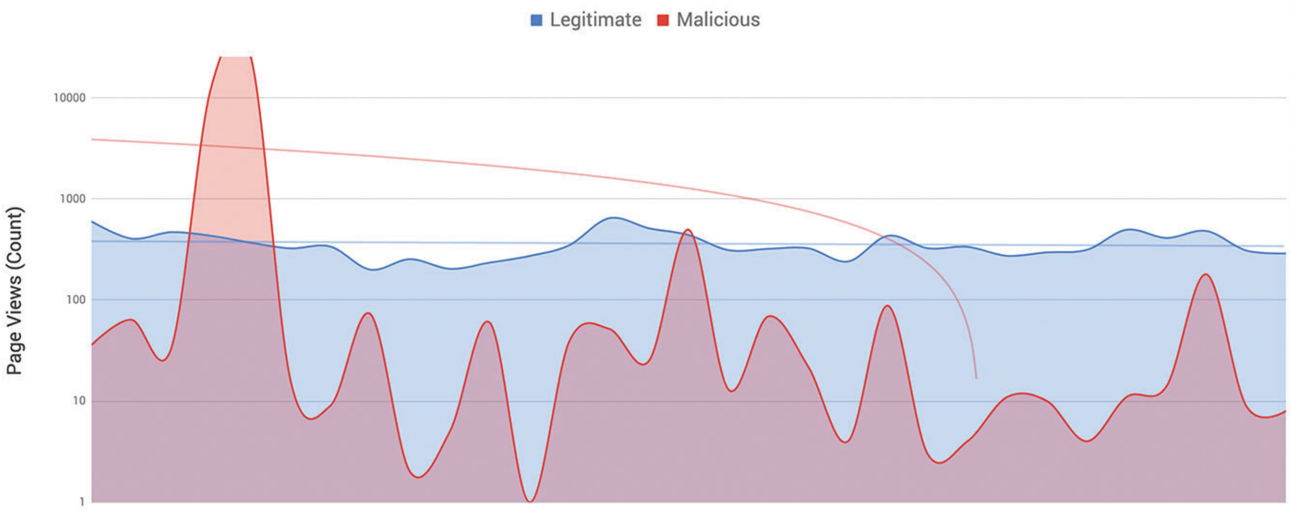
Canary Carding Bots

True to its name, the canary carding bot uses an attack method that reduces the risk of new attack discovery by slow rolling changes to a small subset of users to test checkout page defenses. Once the attackers find a successful final version of the bot, they execute a mass deployment to a larger set of e-commerce sites at a later point in time. The canary carding bot can exploit thousands of e-commerce sites since the attackers are specifically targeting the top e-commerce platforms used by thousands of businesses.

Malicious bots, like the canary carding bot, increase stolen card validation activity with small-value transactions leading up to the holidays. Canary carding bots explore well-known platforms and test their vulnerabilities to carding attacks to exploit a potentially large number of e-commerce website users.

Canary Carding Bot Attack #1

Here is one example of a canary carding bot attack targeting the checkout pages of e-commerce websites built on one of the leading e-commerce platforms.



The initial attack started as a primitive one and was conducted using an old Safari browser dating back to 2011 that would switch IPs every day and originate from cloud and colocation services. Real users rarely use cloud services for shopping. Additionally, these IPs coming from cloud and colocation services typically do not bring real paying customers. The bots did other atypical actions such as not configuring the request language and the content type.

The sophistication of this attack comes from its mimicking human user behavior. In this attack, the bots create a shopping cart, add products to the cart, set shipping information, and finally execute the carding attack. All of the steps except for the carding attack exhibit normal user behavior through a website.

Canary Carding Bot Attack #2

The second attack happened closely on the heels of a failed first attempt. This time, it targeted a sporting goods e-commerce website that was using the same e-commerce platform as the previous attack.

In this case as well, the automated bot attempted to mimic human traffic. It was altering IP addresses, user agents, browsers and devices quite frequently. They were successful in creating the impression of traffic originating from widely distributed sources, making this attack less notable. Another interesting characteristic of the attack was the high enumeration on mobile devices and versions that were quite old. Typically paying customers use recent mobile devices with old versions being a rarity.

We see a common theme from the canary carding bot with the usage of cloud and colocation services. Bots are starting to change the velocity of the flow and the rate with which attacks are originated in the hopes of appearing more human-like when monitored.

The second attack targeted only two paths, simply adding the product to the cart, skipping the product page and going to checkout. In general, the attackers used as few paths as possible to reduce resource usage by the bot infrastructure. While using fewer paths may seem like a good idea to avoid detection, the ultimate use of checkouts with small purchase amounts does trigger thresholds for suspicious bot activity.

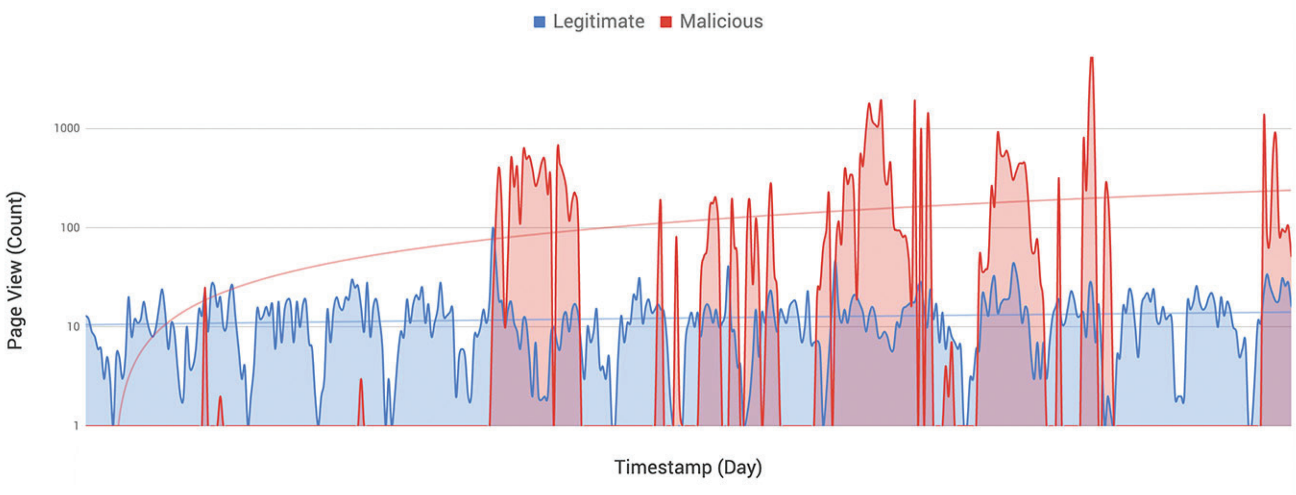
Shortcut Carding Bots

There are typically no shortcuts to success, but this shortcut carding bot may have found one. Like every malicious bot, carding bots try to shorten their user flow and time on the target website or mobile app to avoid detection and mitigation. Shortcut carding bots exploit the card payment vendor APIs used by a website or mobile app and bypass the target e-commerce website completely. Very neat trick indeed!

In some cases, the attackers are discovering paths with API calls that are unknown to even the website operators. In general, there has been an increasing trend in API endpoint abuse to validate credit cards on websites and on mobile applications.

E-commerce websites often use external services to handle the payment process. Some payment services prefer direct access through an API endpoint that verifies the credit card and returns an answer. This direct API call is attractive to the shortcut carding bots since they can validate cards without the need to put any product in the shopping cart or complete the billing process.

Shortcut Carding Bot Attack #1



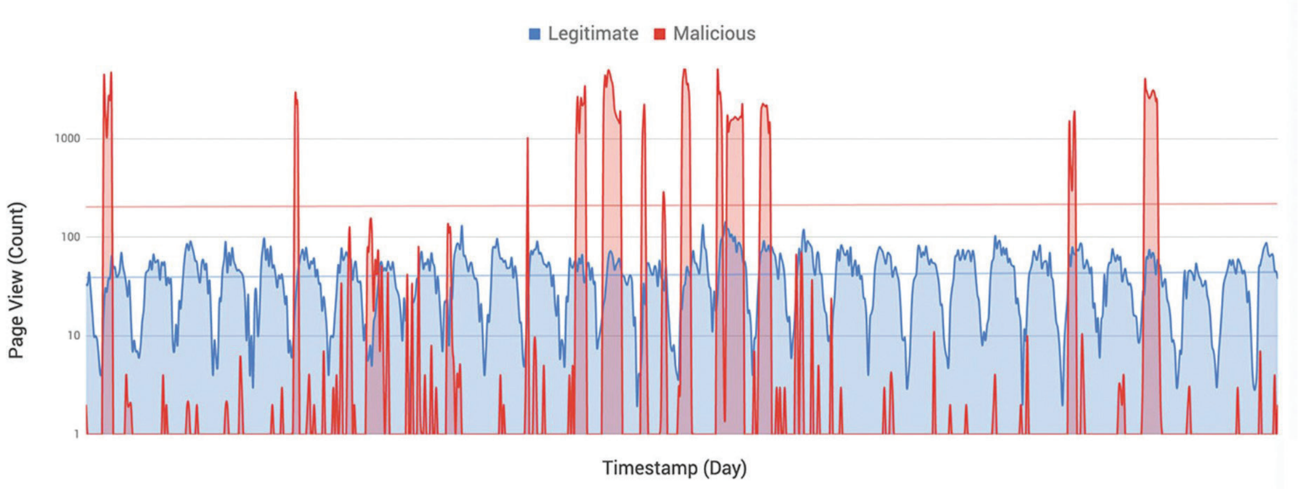
This carding attack occurred on a large apparel e-commerce website targeting APIs using a diverse list of user agents centered around Internet Explorer including a mix of old and new versions. The attack originated from multiple networks utilizing several cloud and hosting providers, and the request did not define any accepted content which is typically anomalous. What is interesting about this attack is that it targeted only one path that used a third-party payment service with a very simple url path: ***/creditcard/tokenize.

By using this path, all the attackers needed to do was send credit card information and the service returned an answer if the card was valid or not. The existence of this kind of shortcut path, which uses the payment vendor's API, makes it easy on the carding bots but harder on the website owners. Typically, the payment vendor's API integration with e-commerce sites will have transaction volume limits as well as low chargeback thresholds.

If the fraudulent transactions exceed a specified threshold, the provider may stop working with the e-commerce site causing business disruptions and forcing the site to adopt higher cost providers. These costs are often incurred in addition to fines and chargebacks already resulting from carding.

Shortcut Carding Bot Attack #2

Another similar attack happened on a large grocery e-commerce website at about the same time as the previous attack.



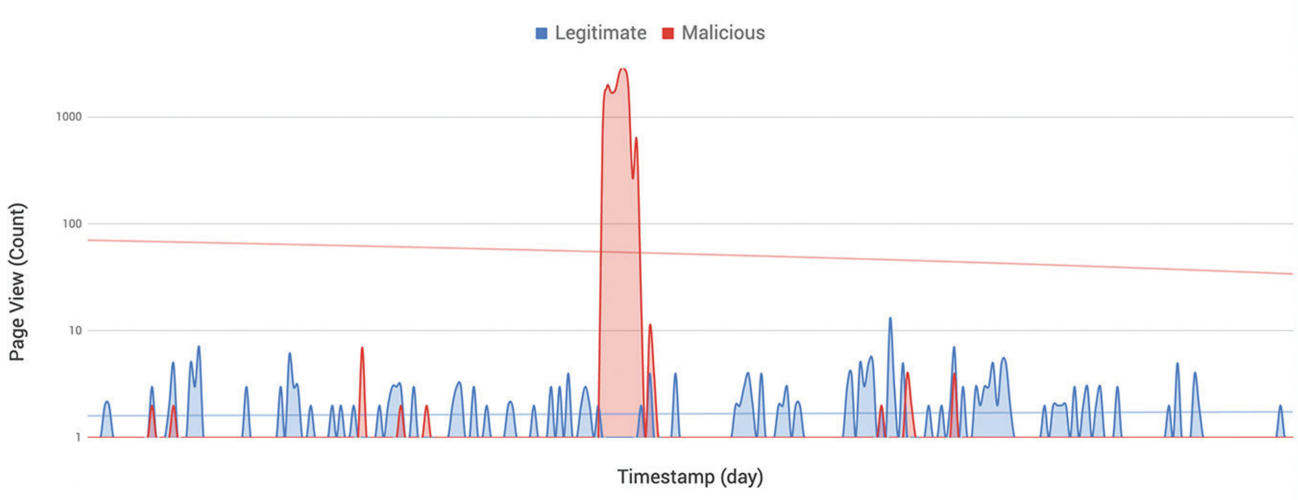
This one also deployed a primitive bot, using a residential IP address and a single modern and popular user agent. This attack, however, did have some anomalous HTTP headers on its requests, a sign it was malicious. Like in the previous case, this attack was targeting a single url: **/api/billing.

By having a single path that enabled the bots to get quick and direct verification of the credit card, the website made it easier on the carding bots to quickly validate stolen credit cards using simple methods. Although this shortcut often employs an API endpoint, it could also be a path within the website structure that only bots can find.

Shortcut Carding Bot Attack #3

This example highlights a recent carding attack on another sporting goods e-commerce website.

This bot enumerated multiple user agents—mainly old ones—and used diverse ASN networks, including overseas



telecom operators as well as cloud and co-located infrastructure. The URL that was used was also suspiciously simple: /OrderShippingBillingView.

Shortcut carding bot attacks have been on the rise lately due to two main reasons:

1. Increase in the number of e-commerce websites that use third-party payment services. There are also many more payment services now and the smaller payment processors often lack adequate API controls.

2. Increase in the complexity of e-commerce websites and the burden on programmers, resulting in unplanned and undocumented paths that become easy targets for malicious automated activity.

Preparing Your Fraud Strategy to Include Carding

Assessing your Risk from Carding Attacks

E-commerce, finance and security managers should first work to understand the extent of risk to the organization from carding bot attacks. Unfortunately, uncovering attacks like those from the shortcut carding bots are very difficult using legacy security tools. PerimeterX provides a simple web-based self-service calculator, free of charge, that delivers a preliminary estimate of the ongoing financial impact from carding attacks based on your inputs. This can provide initial justification for making automated bot management a part of your strategy to combat bot attacks.

Uncover the Impact of Carding Attacks

Access the PerimeterX Carding Calculator Here

Adopting an Automated Bot Management Solution

Adopting a successful fraud management strategy entails understanding what types of threats the organization is dealing with and putting in place solutions to address them.

Automated bot attacks can specifically target applications from login to checkout. Having a sophisticated solution that can deal with these variations of commerce-related attacks such as ATO, carding, scraping and skewed analytics is important.

It is equally important to understand that relying only on traditional web application security tools such as a WAF, or hoping that CDNs or PCI DSS solutions will protect organizations from evolving threats is not a good strategy. PerimeterX provides cloud-native solutions backed by continuous cybersecurity research that can deliver the following:

1. Accuracy of detection and protection that is AI and ML-based

2. Ease of integration with existing web architecture and across various infrastructure platforms

3. Scalability with protection across web, mobile and APIs

Conclusion

As the usage of credit cards for online purchases increases, so do carding attacks and the diversity of methods used by attackers. Recent increases in these new types of attacks across multiple unrelated segments, indicate the quick evolution of these attack tools. Cybercrime is a business that has evolved much like the software and cloud world has evolved, using readily-available tools and sophisticated infrastructure. Attackers look to gain efficiencies by targeting sites built on common platforms. They often use similar attack tools using identical mechanisms. This dynamic is similar to competing companies that may be running their services on the same cloud vendor and using the same open-source libraries.

To be prepared, e-commerce website owners can take a number of actions. First, since legitimate consumers would probably never attempt payment with an empty cart, website owners can prevent users from getting to the payment page without an item in the cart. This basic practice increases the effort required by bots, and stops simple carding attacks. Second, with bots improving constantly and mimicking user behavior, e-commerce website owners should pay more attention to advanced automated threats and investigate solutions to stop them.

PerimeterX continuously investigates automated bot attacks, including carding, to understand how they work and stay ahead of them. This research is incorporated into the PerimeterX product portfolio, including PerimeterX Bot Defender, to protect against known and unknown attacks that target the largest and most reputable websites, mobile applications and APIs.

About PerimeterX

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender, and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

perimeterx
www.perimeterx.com