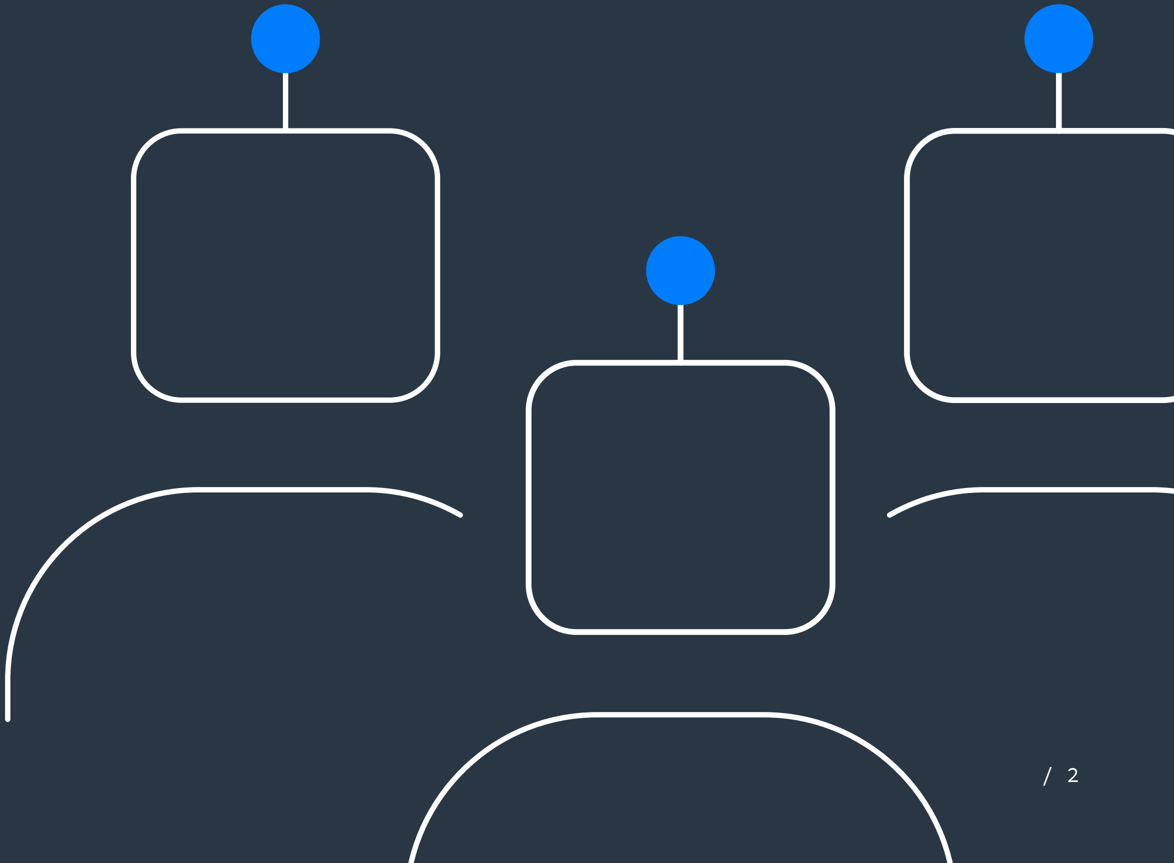
NETACEA / WHITEPAPER

The Top Threats of 2021: Trends in Bot-Based Attacks

NETACEA

A QUICK OVERVIEW OF BOTS

Bot traffic is any request that is made by an automated process rather than triggered by a direct human action. Good bots include search engines, SEO tools and price comparisons, and are used daily by individuals and businesses across the globe. Bad bots, however, are automated processes that carry out legitimate activity to exploit business logic weaknesses within your website, mobile apps and APIs. This activity exposes your business to malicious automated attacks such as credential stuffing, scalping and carding.



LOOKING BACK ON 2020

2020 saw an increasing number of bot-based attacks as everyone and everything moved online in an unprecedented movement during the Covid-19 pandemic. The global number of internet users grew by 7.3% to 316 million last year, as more people relied on digital services. Online shopping became crucial when stores closed in March, employees moved to working completely remotely for the first time, and even medical supplies and advice was consumed digitally. The pandemic affected consumer behaviour worldwide, with retail platforms undergoing a huge global traffic increase between January 2019 and June 2020, surpassing even holiday season traffic peaks. Overall, retail websites generated almost 22 billion visits in June 2020, up from 16 billion global visits in January of the same year.[1] Populations started purchasing essential and non-essential services online, with online traffic in the supermarket segment significantly increasing by 34.8% compared to the reference period in January 2020.[2]

Internet sales as a percentage of total retail sales increased from 19.1% in February to 32% in May after three months of national lockdown, climbing to 36.3% as restrictions tightened once again in January 2021.[3] As a result, we saw bot attacks grow in prominence across the globe. As internet activity increased, so too did the opportunity to exploit users. The interest in bots peaked partially out of curiosity, while others were interested in using bots to acquire products for personal profit, exacerbated by the economic uncertainty of Covid-19, the rise in unemployment, and the need for quick cash fixes. There were more account takeover attacks as consumers – now forced to stay indoors – were signing up for online accounts, particularly streaming services accounts. Criminals were able to exploit this uptake in activity, and there was a sizeable rise in credential stuffing attacks throughout 2020, compared with 2019.

Bots were also brought to the forefront in 2020 by scalper bots targeting high profile clothing and gaming ‘drops’, most notably the PS5 scalper bot attack. Ordinary consumers were left frustrated and out of pocket when automated bots bought the consoles faster than any human had the opportunity.

With the public deliberately purchasing more products and services online in 2020 – 24% said they did so with clothing – there has also been a rise in carding attacks, as attackers demonstrated an increased proliferation of stolen credit cards.[4] Research for Aite Group’s Fraud and Anti-Money Laundering practice estimated that by the end of 2020, the US was seeing around $11 billion worth of losses due to credit card fraud.[5]

Sources:
1.Statistica: Coronavirus impact on retail e-commerce website traffic worldwide as of June 2020, by average monthly visits
2.Statistica: Coronavirus impact on online traffic of selected industries worldwide as of October 2020
3.ONS: Internet sales as a percentage of total retail sales
4.Statistica: Have you deliberately purchased any of these products or services online instead of offline because of the COVID-19 / coronavirus pandemic?
5.CNBC: Credit card fraud will increase due to the Covid pandemic, experts warn

WHAT COMES NEXT: PROTECTING YOUR BRAND IN 2021

The increase in online activity over the course of Covid-19 lockdowns has made scalper, account takeover and carding attacks extremely appealing, as attackers seek to profit from shifting consumer behaviour. Even non-malicious actors are tempted by scalper bots to secure the products they want, and bot developers and users are teaming up to professionalise their service, making them much more capable and much harder to stop. Unfortunately for brands, this means there is significant potential for financial and reputational brand damage from such attacks in 2021. As lockdown begins to ease but restrictions are expected to remain in place for some months, we predict that the level of internet activity across the globe will remain high. The way we work, shop and interact has changed – resulting in more communication and purchases being made online.

This whitepaper explores why carding attacks, scalper bots and credential stuffing attacks were the most notorious attacks of the last 12 months, why we should be aware and prepared to face them head on in 2021, and how they could damage your brand reputation, customer loyalty and, ultimately, profit.

SCALPER BOTS: WHAT ARE THEY?

A scalper bot – often referred to as a sneaker bot – is used to automate part of, or the entirety of, the purchasing journey of goods or services through non-human means. Scalper bots allow the attacker to automatically monitor websites for the selected target and place objects into the shopping cart, ready to resell or proceed straight to purchase. Scalper bots affect brands, retailers and customers alike, as attackers seek high-demand items and buy the highly anticipated stock in seconds before genuine users have the opportunity. The merchandise is then sold on the thriving reseller market at a significantly higher price that puts it beyond the reach of ordinary consumers.

> Between 60% and 70% of all traffic to checkout pages is made up of malicious bots.[6]

Scalper bots use various techniques to bypass security defences and controls across websites, including:

/ **Account aggregation**
Also known as financial data aggregation, is a method that involves compiling information from different accounts, which may include bank accounts, credit card accounts, investment accounts, and other consumer or business accounts, into a single place.

/ **IP rotation**
Assigned IP addresses are distributed to a device at random or at scheduled intervals. For example, when a connection is active via an internet service provider (ISP), an IP address is automatically attached from a pool of IPs. Rotating IPs makes it harder to detect that the attacker is one person.

/ **CAPTCHA**
CAPTCHA challenges can be can be bypassed by sophisticated bots easily. There are multiple online services that claim to solve CAPTCHA challenges with high degrees of accuracy using automated methods such as APIs and plugins. Humans can intervene through CAPTCHA farms, where large groups of people solve CAPTCHA for vendors who provide these solutions at a low cost. There is also a widely available browser extension which will solve CAPTCHA challenges for a small fee, often as low as $1 for 500 reCAPTCHA solves. Online CAPTCHA-solving vendor services are not limited to traditional text or picture CAPTCHA; Google’s audio CAPTCHA can be solved using their own speech-to-text API.

/ **Invoice abuse**
This involves notably changing addresses and using fake credit cards and is a well-used technique for detracting attention from one attacker.

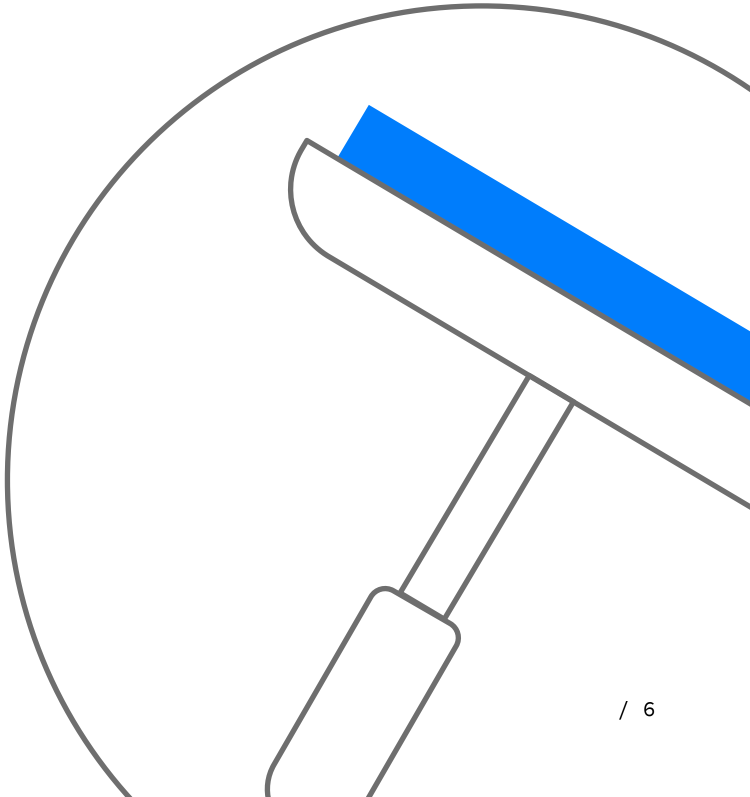
Sources:
[6] Merchant Fraud Journal: Javelin releases 2020 Identity Fraud Study

THE EXTENT OF THE SCALPER BOT THREAT

Scalper bots are becoming increasingly well known as attackers target high-end 'hot drops' like the PS5 launch and the latest designer trainers, consequently receiving extensive media coverage. The problem has been worsened and intensified by the economic uncertainty of Covid-19 as bot developers and groups run recruiting campaigns and people look for additional income during periods of high unemployment and the need for quick cash fixes. With more time spent inside and a proportion of the population in a better economic position with non-essential activity restricted, people are spending more time than ever online shopping – and more online commerce means more targets for attackers.

Furthermore, the scalper bot industry is also becoming increasingly professionalised and sub-industries are developing as the number of scalper bot actors grows, elite bot groups come to the forefront, and cook communities and hybrid groups form. Many groups are well funded and make significant profit off the back of attacks, suggesting some notable investment.

The recent PS5 launch has been perhaps the most well-publicised, large-scale scalper bot attack in recent times. In fact, Netacea data shows that a botnet which used 300 compromised machines to buy PS5s made one million purchase attempts over six hours. The PS5 scalper bots provide us with some useful insights into the scale of the scalper bot issue and how it can be expected to develop in the future. Fig. 1 shows a clear correlation between interest in PS5s and scalper bots over time. As the PS5s were bought up by bots, people who wanted a PS5 increasingly researched acquiring their own bot, resulting in the spikes we see here.



HOW THE INTEREST IN SCALPER BOTS HAS RISEN OVER TIME:

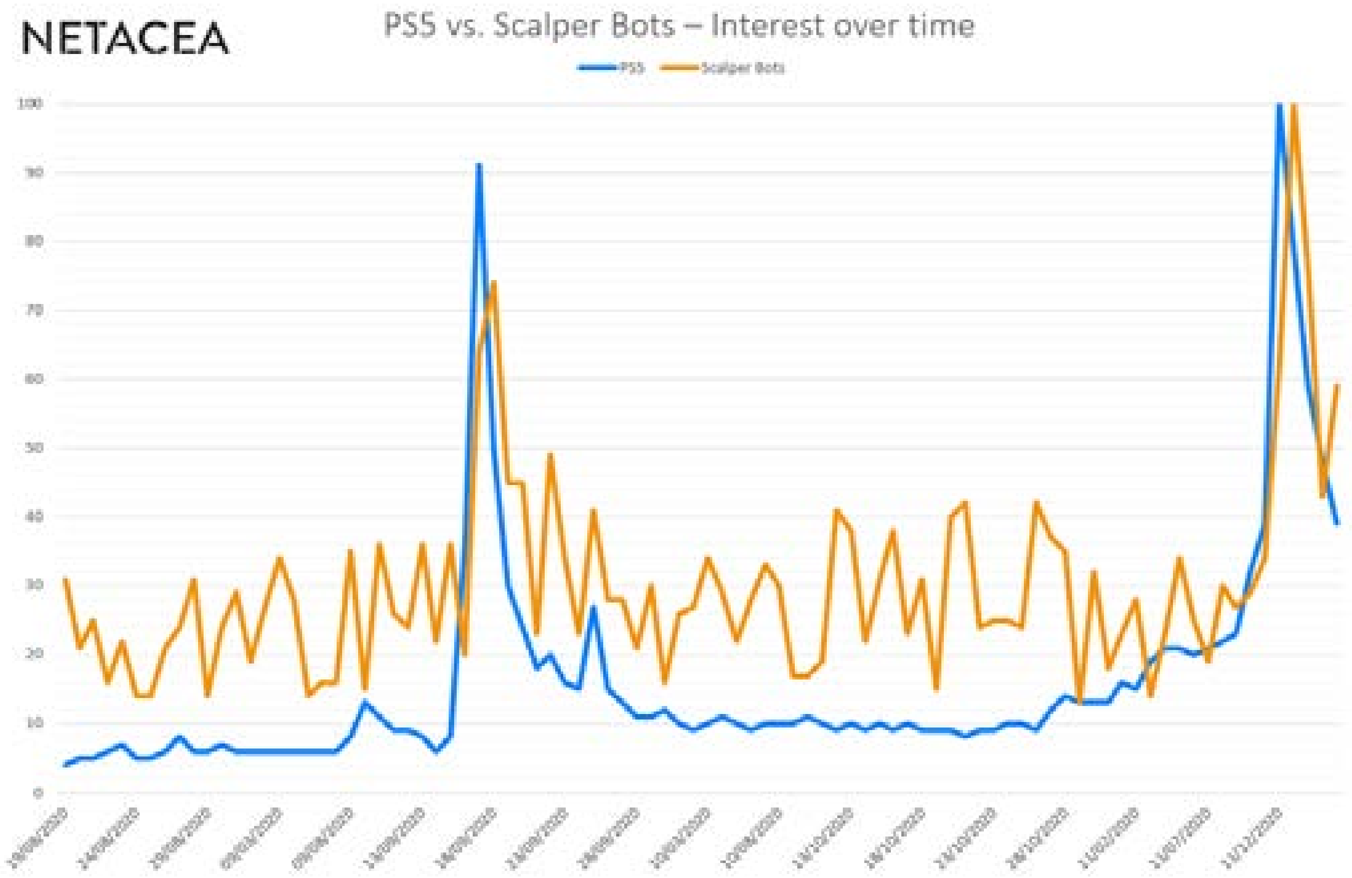


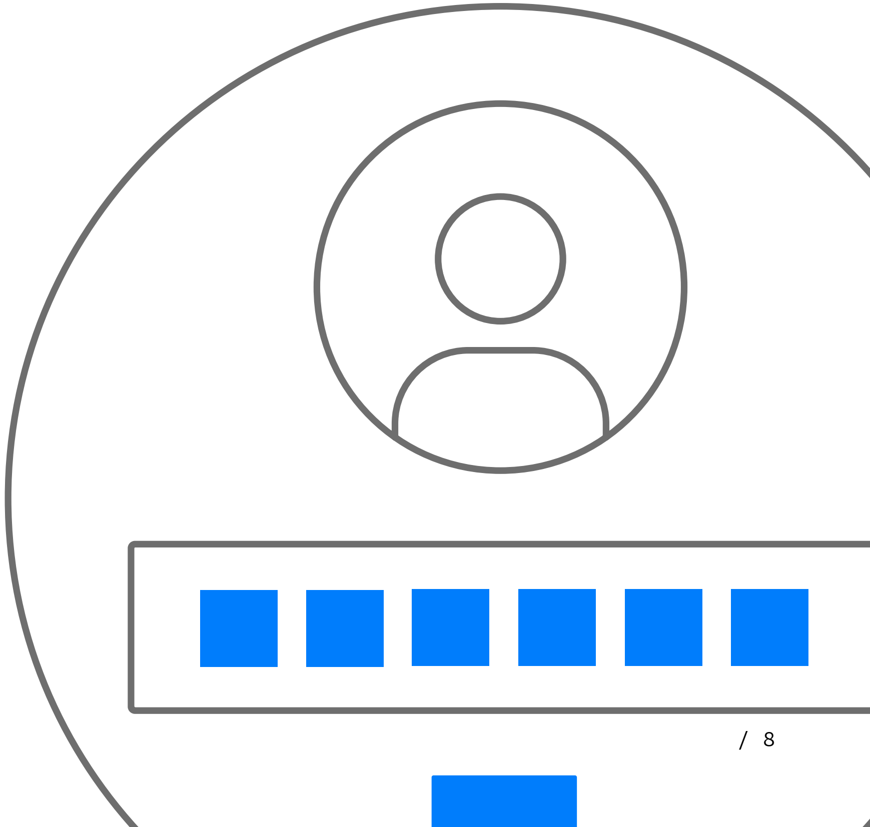
Fig. 1

CREDENTIAL STUFFING: WHAT IS IT?

Credential stuffing is a common account takeover technique used to gain brute force access to an account by continually and automatically injecting usernames and passwords into website login forms until they get a match. There are currently more than 15 billion attacks in circulation – up 300% from 2018.[7]

Account takeover has never been easier or cheaper for cybercriminals. During Covid-19 lockdowns, more people have been spending time at home looking for entertainment, and streaming services have become even more prolific as a result. Accounts for all of these services have resale value, and attacks are very low risk with potentially very high pay outs. Saved payment details mean attackers can impersonate users and gain access to streaming services with ease. Both consumers and businesses are exposed to risks in the instance, with the attacker able to carry out a range of illicit and often fraudulent activity once they have gained access.

> Account takeover attempts saw a spike of 282% between Q2 2019 and Q2 2020.[8]



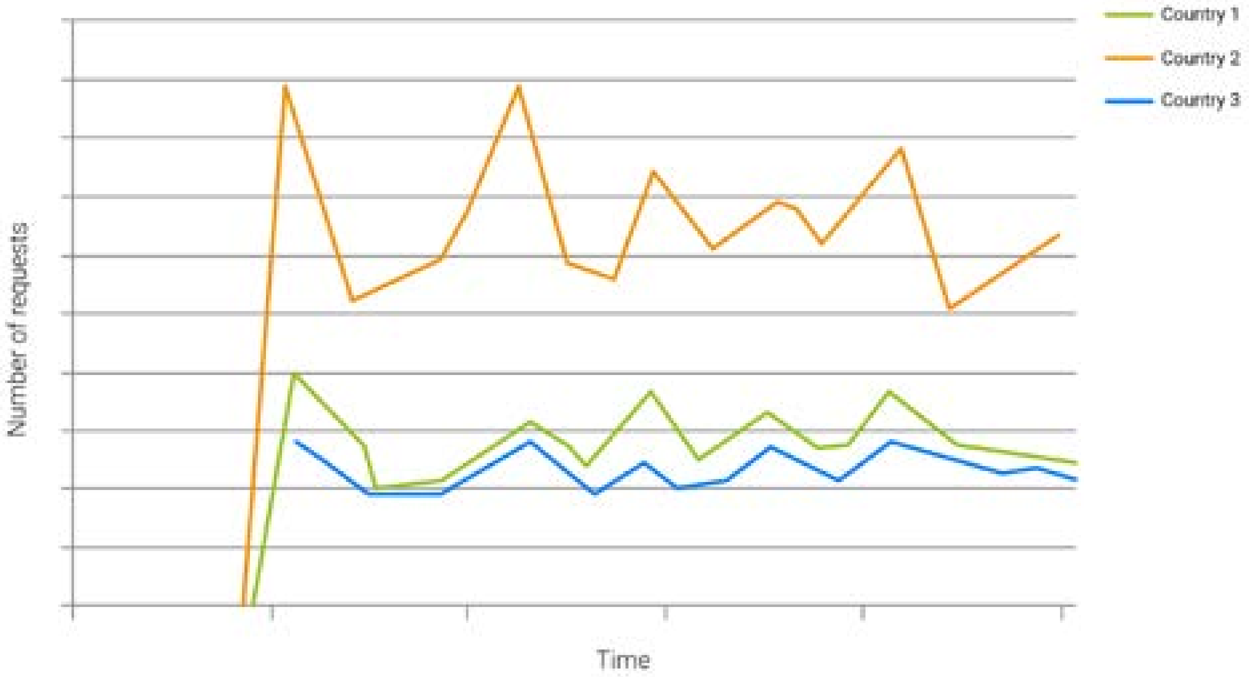
Sources:
7. Digital Shadows: From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover
8. Global Newswire: Report: Account Takeover Becomes Weapon of Choice for Fraudsters Leading Up to Holiday Shopping Season

HOW DOES A CREDENTIAL STUFFING BOT ATTACK WORK?

Credential stuffing attacks trawl lists of leaked usernames and passwords, using bots to continually test combinations on multiple sites until they are successful. Usernames and passwords are easily accessible in mass data dumps consisting of millions of credentials amassed from years of data breaches. Although a portion of the data in data dumps is likely to be stale and unusable, there will be plenty of users that have not updated their passwords in some time and whose accounts are open to attack. Once an attacker has successfully accessed one account, each of the consumer's accounts using the same password are vulnerable to exploitation of the personally identifiable information (PII) it contains. In many cases the PII will be sold on or the account itself will be sold. A 0.005% success rate can mean thousands of successes, and even just a few successful acquisitions can mean a profit.

Fig. 2 shows the spread of credential stuffing attacks on average, from common source countries:

Fig. 2

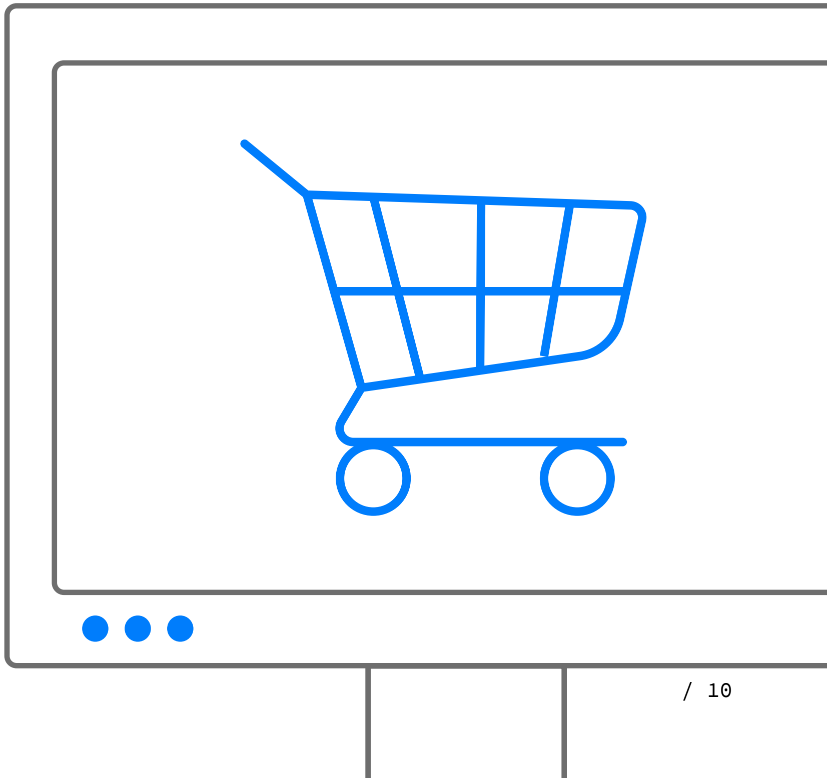


CARDING BOTS: WHAT’S THE THREAT TO RETAILERS?

Every year, more retailers are falling victim to the breadth of techniques used by attackers to steal payment card information and use it for their own gain. Payment card fraud losses reached over $28 billion worldwide in 2019, with the United States alone responsible for more than a third of the total global loss, making it the most card fraud-prone country in the world.[9]

Carding is the illegal use of credit or debit cards by unauthorised people – or ‘carders’ - to buy a product. It typically starts with an attacker gaining access to a store or website’s credit card processing system. The attacker then has a useful list of credit or debit cards that were recently used to make a purchase at their disposal. Attackers test lists of payment card data to check for valid details, and small purchases are often made to validate the correct payment details and avoid suspicion. Generally, those who acquire the stolen details are the ones looking to resell. For online retailers, carding is a huge problem that must be addressed to prevent loss of revenue.

> The recent Nilson Report predicts over $32 billion will be lost to card fraud in 2021, set to reach $38.5 billion by 2027.[10]



Sources:

[9] CNBC: Credit card fraud will increase due to the Covid pandemic, experts warn

[10] Nilson Report December 2020

HOW DO CARDING ATTACKS WORK?

As more people went online to buy groceries and other essentials during 2020, we saw more attacks targeting customer credentials. There are more, and smaller, stores online than ever before, and supporting online stores has become more popular than ever, providing a prime opportunity for carders.

To successfully carry out this fraudulent activity, multiple payment authorisation attempts are used to validate stolen payment card information in bulk and thousands of stolen credit card numbers. When limited cardholder data is available, and the expiry date and security code are unknown, the process is instead known as card cracking. Bots come in handy when carrying out any carding activity, enabling the attacker to try multiple values quickly, and identify the missing start and expiry dates and security codes for payment card data. To mitigate this malicious activity, it is vital that eCommerce sites apply security measures that protect consumers and sellers alike.

Fig. 3 shows the amount of requests from one user per path on an average eCommerce site, with the largest bar representing the payment path (or the number of times a user attempted to pay). Generally a legitimate user will visit the payment path far fewer times than other paths on a store. In this case it is significantly disproportionate, suggesting the user attempted to make lots of payments. This unusual behaviour is indicative of an attacker testing different sets of payment details.

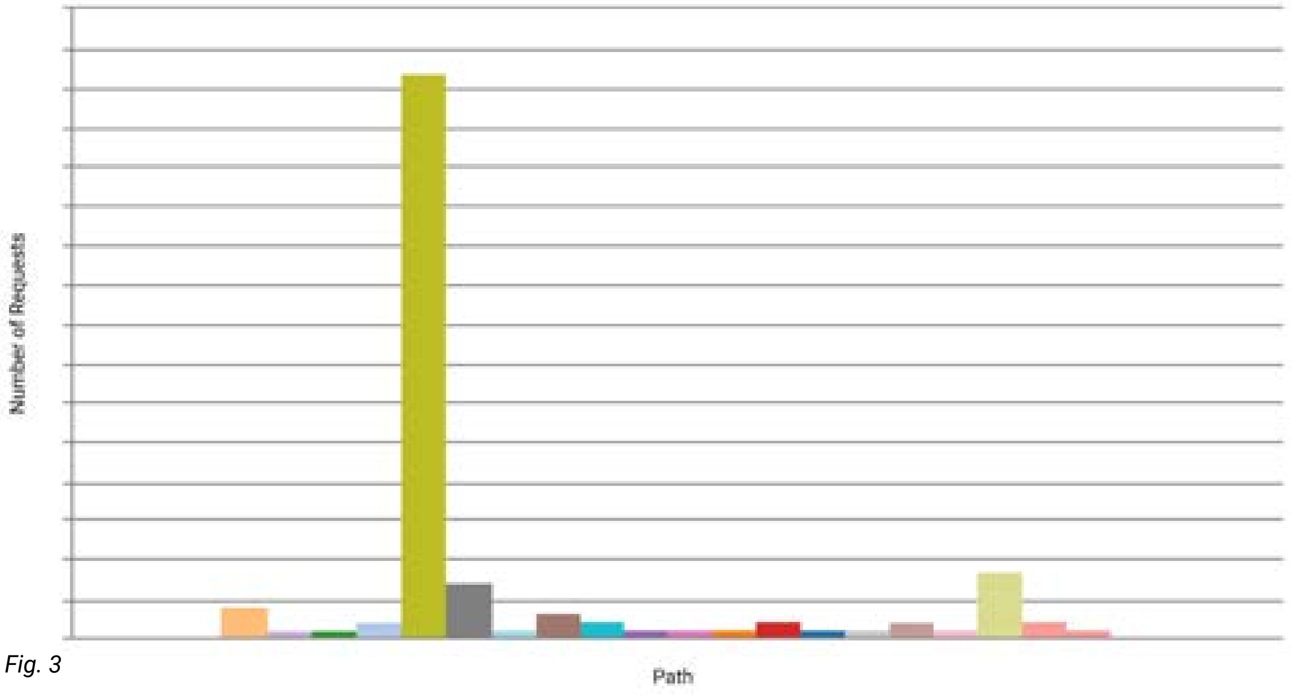


Fig. 3

SUMMARY: THE WIDER BOT THREAT

Credential stuffing, scalper and carding attacks are the three top threats Netacea has observed increasing in frequency and becoming more sophisticated throughout 2020, as online activity continues to grow. However, these are not the only bot threats to have on your radar. Although these are the three threats we expect to see the most of this year, other threats to be aware of and put mitigation solutions in place for include:

FAKE ACCOUNT BOTS

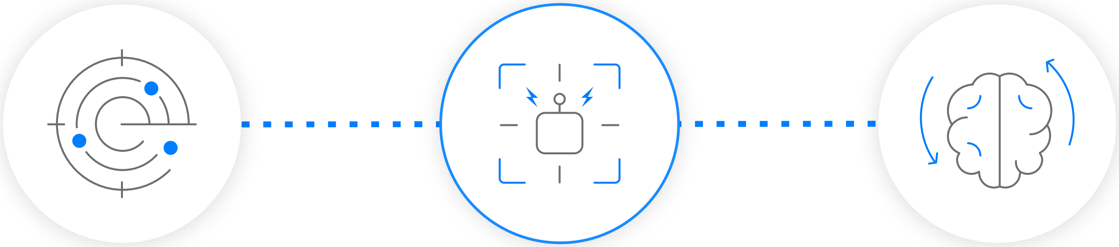
SKEWED MARKETING ANALYTICS

SCRAPER BOTS

CARD CRACKERS

CHOOSING THE RIGHT BOT MANAGEMENT SOLUTION

Choosing the right bot management solution is a major decision for any business. At Netacea we take a consultative approach, working closely with you to understand not only the threats bots pose to your business, but how our solution fits into your wider strategy and organisation. This partnership, paired with our server-side approach and innovative Intent Analytics™ technology, allows us to seamlessly integrate with your business and deliver accurate, intelligent and effective bot mitigation.



DETECT MALICIOUS BOTS

RESPOND TO ATTACKS

EVOLVE AND ADAPT

To find out more about Netacea's unique approach to stopping the top bot threats to your business in 2021 and beyond, visit www.netacea.com/why-netacea or talk to our team today at hello@netacea.com.

- Real-time analysis powered by Intent Analytics™
- Best-of-breed anomaly detection
- Threat intelligence feed
- Insightful, data-rich dashboards
- Total control over response options
- Seamless and flexible integrations
- Dedicated bot experts with 24/7 support