Netacea Bot Management Use Cases

NETACEA

Credential stuffing (Retail, telecoms, gaming)

Credential stuffing exploits people's tendency to reuse passwords across multiple web services to gain unauthorised access to users' accounts.

Adversaries can easily and cheaply obtain username and password pairs from the millions of credentials that have been leaked in data breaches, before testing these against their target's login page on a mass scale using automation. With every successful login request, the adversary can steal funds or personal data, lock the legitimate user out, or resell access to another party.

Scalper bots (Retail)

Scalping is the process of purchasing limited availability or high-demand goods (such as event tickets, limited edition fashion items, and high demand electronics) and reselling them for a profit on second-hand marketplaces.

Scalper bots monitor websites for new stock or releases, then automatically complete the checkout process faster than any human could, much to the frustration of legitimate customers.

Web scraping (Retail, media, gaming)

Web scraping is the use of bots to gather content or data from websites. Some scraper bots, such as Googlebot, are beneficial and help to bring more traffic to a website.

However, some scraper bots have malicious intentions. Content scraper bots may repost articles on their own website, drawing traffic away from the original website. Pricing scraper bots are used to undercut competitors. A scraper bot could also clone an entire website for use in a phishing campaign.

This activity can be very resource-intensive for the website targeted resulting in increased infrastructure costs for the website administrator.

Arb betting (Gaming and gambling)

Arbitrage (arb) betting exploits the differences in bookmakers' opinions on certain odds. By betting on all possible outcomes of the same event simultaneously with different bookmakers whose odds vary, it's possible to guarantee that a return will be made. The recent rise of automation and comparison sites has made arb betting a more serious problem than ever.

Arb betting tools scrape odds from gambling sites, identify arb opportunities, and then automatically exploit these by placing the relevant bets.

Netacea Bot Management Use Cases

NETACEA

Carding (Retail, financial services)

Carding, also called card stuffing or card cracking, is the process of illegally validating stolen payment card details without permission. Carding has a severe impact on both consumers, who get charged for purchases they didn't make, and eCommerce businesses, who deal with chargebacks and loss of customer trust.

The adversary tests payment card details stolen from underground forums against their target eCommerce webservice by making mass automated payment attempts. This includes trying multiple combinations to guess missing data. Where successful, adversaries can either make purchases with these payment card details or sell them on for other adversaries to use.

Fake account creation (Retail, telecoms, gaming)

Fake account creation bots abuse the signup process of a webservice to automate the creation of user accounts in bulk, often with stolen or fake identities. This can be spread out over long periods of time or using IP addresses from different geolocations to hide the fact that they are controlled by one person. Many advanced fake account creation bots can also bypass email, phone, and CAPTCHA verifications.

These accounts may be used to take advantage of a new customer promotion, bypass "one purchase per customer" policies, or as a launchpad for other attacks. They can also be sold on by the adversary for use by others.

Gift card and voucher abuse (Retail, telecoms, gaming)

Gift card and voucher abuse is used by attackers to try and complete purchases for free. Once adversaries have identified where and how gift card or voucher codes can be used on a website or mobile app, some will rapidly brute force random codes using automation. Others may find an API endpoint that generates gift card codes to exploit.

Once they have these codes, attackers then use them to complete purchases, or sell the codes to other attackers. This can cause substantial losses for an organization. Attackers will also sometimes generate or guess a one-time use code that belongs to a legitimate customer, causing frustration for the genuine user.