NuData Security

mastercard

NUDATA CASE STUDY

Case Study: Hybrid account takeover attack at login

Automation and humans join forces against companies.

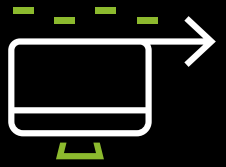
Case study: Bots and humans, a hybrid attack

Bot attacks are a long-known threat. They cycle long sets of data through a placement, such as login, to find the ones that are correct. Sophisticated attacks are the natural evolution of those common volume-focused bot attacks. This improved attack has scripts that try to mimic human behavior to avoid mitigation. They do this by triggering the use of the keyboard or by loading the JavaScript on the page, just like a normal user would.

To make things more complicated, today we also have hybrid attacks that are ushering cybercrime to a whole new level: they combine the convenience of automation tools with easy-to-access human workforce to bypass those pesky bot challenges.

In the next pages, we dissect a four-step attack mitigated by NuData's NuDetect solution that targeted login and wallet functionalities at the same company. This example shows how a sophisticated attack mimics human behavior and leverages human workers in real time to bypass bot-detection challenges.

Testing the scripts



Outsourcing CAPTCHAS

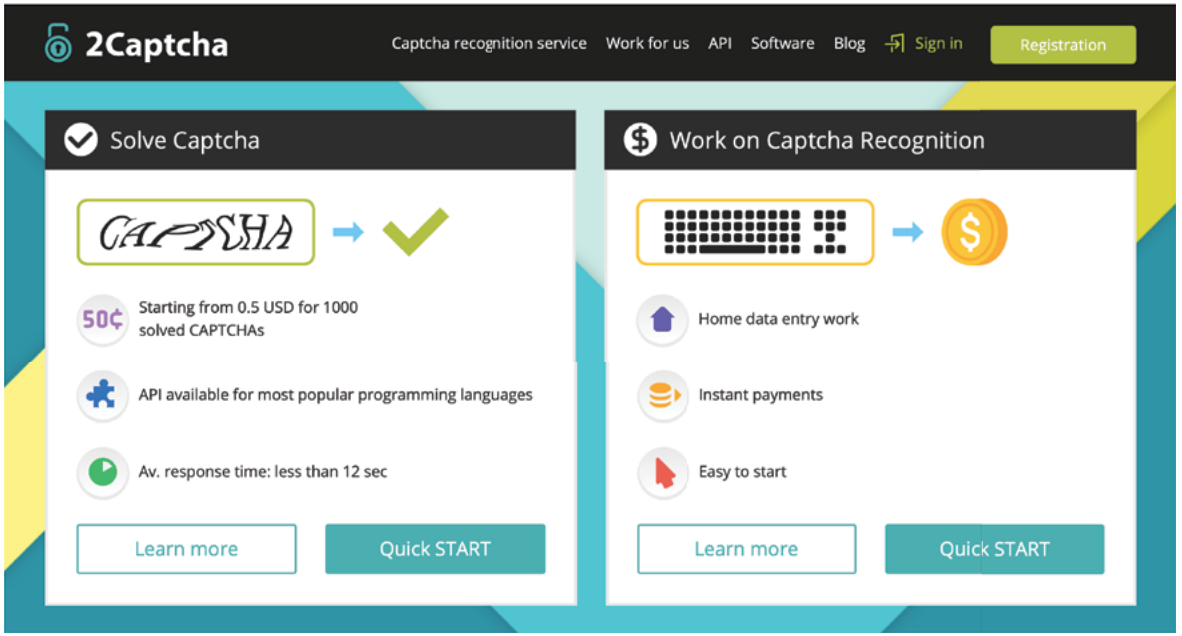
Harvesting payment information

Learn, rinse, and repeat

A hybrid attack in four steps

1. **Testing the scripts:** The attack script attempts to log into the targeted platform with a long list of credentials bought off the dark web. If a login attempt fails, the script records whether the failure was due to incorrect credentials or to a technical problem that may have triggered basic bot-detection tools, such as the login attempt taking place before the page has fully loaded. When the login fails due to a technical problem, the script knows to retry the same credentials again. This is a simple way for the attacker to optimize the list of credentials and get accurate results.

2. **Outsourcing CAPTCHAS:** When the NuData solution detects a script at work within a client's environment, the solution can push a bot challenge. In this case, the attack was intercepted with a CAPTCHA request. To solve the request, the script submitted it to a service called 2Captcha[3] whose human users solve CAPTCHAs in seconds for a small fee. This kind of service is useful for attackers as they can avoid recruiting and hiring workers themselves.

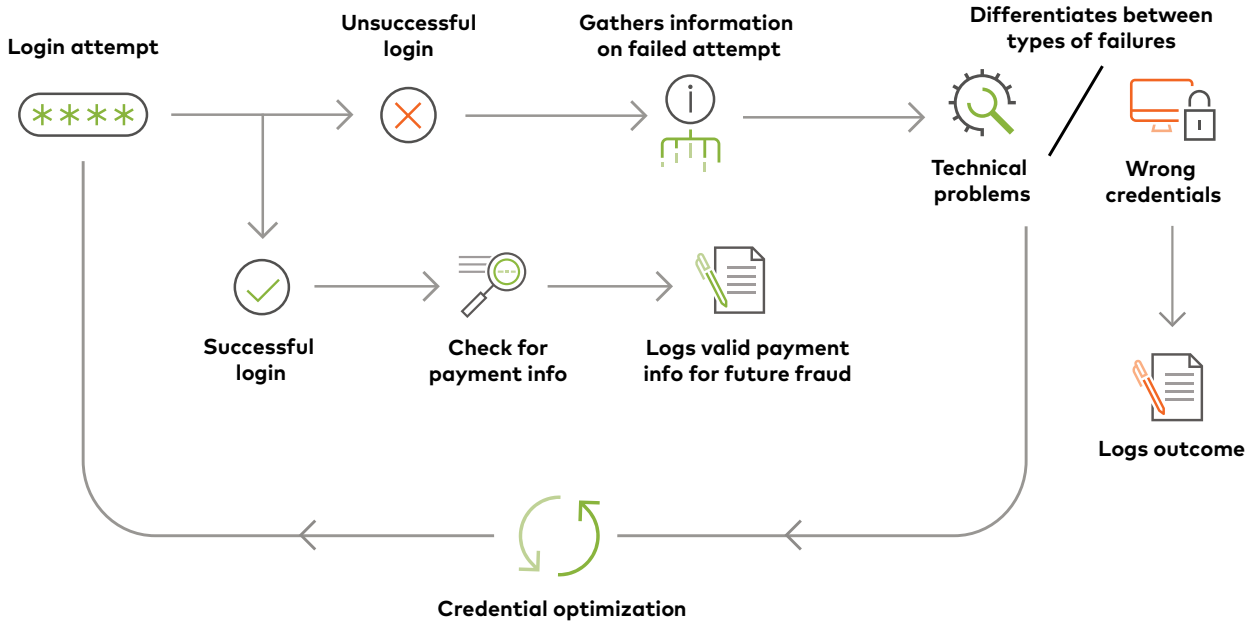


[3] *https://2captcha.com*

3. **Harvesting payment information:** The script made hundreds of thousands of login attempts, over 99.9% of which were mitigated by our NuDetect solution in real time. On the few occasions that a login bypassed our automation challenge and successfully opened the account (less than 0.01% of the time), our model detected that the script went on to access the account data and harvest the active payment information. The script didn't attempt to make any purchases: It simply logged the payment information in a text file, probably to leverage at a later time.

4. **Learn, rinse, and repeat:** The script logged the result of every attempt, even of those that were successfully blocked. With the few successful logins, the script logged whether there was payment information in the account or not. Logging this data into a text file gives the attacker useful information they can leverage to improve their tactics in the future, as well as enables them to use successful credentials and payment data for future fraud. Luckily, the majority of the attempts were mitigated from the start. The NuDetect model learned from this behavior to mitigate following attacks at an even higher rate.

How the sophisticated attack works



How companies can detect human-driven attacks: Signs to watch out for

Besides bypassing bot detection tools, human farms help bad actors open large quantities of new accounts and avoid other manual actions normally caught by tools. As leveraging workers grows in popularity, companies must apply stronger protections that can evolve along with the threat.

Human farm workers get paid for each completed action. Because of this, their behavior is subtly different from the behavior of a legitimate user, who doesn't have the time pressure of completing as many tasks as possible to earn a paycheck. Below are some of the patterns to identify human-driven attacks.

Familiarity with the form: A human worker might fill out the same form or request hundreds of times in a given day. Their familiarity with a platform can give them away: For example, the total distance their mouse travels during a session will probably be shorter than that of the average user.

Velocity: Workers filling out forms or requests also tend to submit or solve them faster than the average user who doesn't have the time pressure of completing as many tasks as possible to earn a paycheck; another key indicator.

Lack of familiarity with the data: In the case of creating new accounts or applications, human workers are typing out information they've never seen before. Because of this, their typing cadence is different from that of someone typing their own name, street address, or other data they are familiar with.

Gaining visibility into this suspicious behavior is crucial to prevent the growing threat of human-driven and hybrid attacks. Behavioral tools like NuData's NuDetect platform can automatically identify many of these patterns, allowing companies to weed out this harmful traffic relatively easily. Solutions like these are companies' first line of defense against the growing wave of human-driven attacks.

About NuData Security, a Mastercard company

Read our success stories to learn how we've helped other companies

If you have questions, email us at verifygoodusers@nudatasecurity.com

NuData Security, a Mastercard company, is an award-winning provider of behavioral biometrics and device intelligence solutions and is trusted by some of the world's largest brands across eCommerce, digital banking, and beyond. NuData helps companies stop account takeover, prevent new account fraud, and reduce unnecessary friction in real time.

With over 20 billion risk assessments and 4.5 billion devices processed yearly, businesses across the globe benefit from the power of NuData's Trust Consortium to validate good users without disruption and stop bad actors before they can cause damage.

+20B

risk assessments annually

+284M

accounts protected monthly

NuData Security

mastercard