NuData Security

mastercard

CASE STUDY

Client spots login attacks despite correct credentials thanks to NuData technology

Overview

Credential stuffing attacks make up the majority of threats our clients mitigate with the NuData technology. Interestingly, in the last while, NuData and its clients have seen an increase in the quality of attackers' credentials used at login. Bad actors use more accurate information for their ploys and pose a bigger threat to companies that can't mitigate these sophisticated attacks.

This case study analyzes what is actually happening in the background: whether attacks are indeed using better credentials or if bad actors are just better at pretending – as well as how to mitigate them.

Credential stuffing: A numbers game

Much of the stolen personal information used by fraudsters is outdated or inaccurate, forcing bad actors to cycle through large numbers of credentials just to get a single hit. Historically, between 0.5% and 2% of login attack attempts across industries have used correct credentials. That might sound low, but when a single automated attack can input one million credentials, that 0.5%–2% of attack attempts turn into thousands of compromised accounts and can do a lot of damage if other mitigations aren't in place to stop the attack.

In the first half of 2021, the average login credential success rate we observed on our network jumped dramatically to 9.9%, up from an average of 1.9% in 2020. The jump was particularly noticeable in the retail, streaming and event-ticketing industries, while finance remained the most stable.

	Digital goods	Retail	Financial	Travel	Streaming	Event ticketing
Successful credentials H2 2020	0.02%	1.18%	0.40%	1.37%	0.19%	4%
Successful credentials H1 2021	0.03%	12%	0.40%	1.7%	29%	16%

2M

Fishing websites registered by Google.

20%

Increase in phishing websites since 2019.

While it's impossible to know exactly why credential quality has increased — particularly, why it increased so significantly in a handful of industries — four factors may play into the change.

1. As-yet-undiscovered data breaches

It takes an average of 287 days before a data breach is discovered and contained, according to IBM.[1] A high credential success rate in a given industry could be a sign that a company in that industry has suffered a breach that simply hasn't been identified yet, resulting in the compromise of a large amount of personal information.

2. Attackers prioritizing rapidly-evolving industries

The transition to digital during the pandemic was incredibly fast and left many merchants handling large amounts of online customer data without much experience in how to secure it. Fraudsters aware of this may be targeting industries that began evolving digitally in the past 18 months, since they may be perceived as less experienced with fraud and security controls.

3. An increase in phishing

Fraudsters are acquiring valid credentials through phishing scams, which exploded in popularity during the pandemic. In 2020, Google registered a record 2 million phishing websites, an almost 20% increase over 2019.

4. Fake accounts created as part of sophisticated attacks

Many rules-based security tools automatically flag users with low credential success rates as potential bots. To evade detection, some attackers artificially improve their credential success rates by creating fake accounts (more in the case study in the next page).

[1] *2021 Cost of a Data Breach Report, IBM*

Artificially increasing credential success rate

2%

Average rate of success, until recently, for a credential stuffing attack.

70–90%

Success rate of legitimate users logging into their accounts.

40%

Rate of success recently discovered in a credential stuffing attack on our network.

As we mentioned earlier, until recently, it was rare for a fraudster carrying out a credential stuffing attack to see more than a 2% credential success rate. So, if even 5% of the credentials they used turned out to be valid, they'd likely be celebrating a resounding success.

At NuData, we know that when an attack appears to contain a high percentage of correct credentials, it doesn't necessarily mean the attacker had a good quality dataset. So, when we encountered an attack with an unheard-of 40% credential success rate on our network, even if we mitigated it, we decided to look at ways they might have gotten so many credentials right.

This attack included tens of thousands of login attempts. However, we quickly realized it didn't originate at login, but at account creation — a placement that the client was protecting with a non-behavioral solution. The attacker was able to achieve a high credential success rate in part because many of the accounts they were logging into, they created themselves.

If this sounds pointless, it isn't — because the rate of correct credentials in an attack can impact the deployment of the attack itself.

Remember, the average credential success rate of an automated attack at login is usually low — less than 2%. By contrast, legitimate users only mistype their passwords occasionally, giving them success rates in the 70% to 90% range. That's why some companies protect their login pages with simple rules that identify any user with a high number of failed logins as a potential bad actor. By artificially raising the credential success rate, an attacker can get around these rules and improve their chances of succeeding in the attack.

4 ways fraudsters artificially raise the credential success rate

1

Purge data

Before attempting to log in, the attacker runs their list of stolen usernames at the new account or password reset placement to check if these usernames exist. When they try to open an account with an existing username, the platform will return an error saying the account already exists. Now the attacker can rule out any nonexistent usernames on their list before starting the attack at login, lowering the failed-login rate.

2

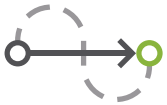
Create new accounts

To increase the credential success rate further, the attacker creates new accounts en masse with usernames and passwords they know.

3

Test at login

Attackers now finally deploy the attack at login, combining login attempts on their own accounts with login attempts on those stolen accounts they are targeting. They don't know the passwords for the targeted accounts, but know the usernames exist and have a set of username and password combinations to test.



4

Reap the benefits

By removing credential sets from usernames that don't exist in that platform and by including their own accounts in the attack, they can reach a high enough credential success rate to fool many rules-based security tools. In this case, they reached a 40% correct-credential rate.

Results

Fortunately, the login placement was protected by more than just a few simple security rules. NuData's solution detected and mitigated these tens of thousands of login attempts at a +99% rate, protecting the accounts and the subsequent direct fraud losses, brand damage, and customer churn.

NuData's NuDetect solution did this by leveraging behavioral biometrics and analytics to flag anomalous activity. In particular, a few behavioral red flags showed us that the person making these login attempts with stolen credentials was unlikely to be the true owner of any of the accounts:

- Anomalous typing behavior at login compared to expected user behavior
- Unusual device information compared to expected user
- Anomalous bot behavior solving a challenge compared to the general population

+99%

Rate of detecting and mitigating these attcks using NuData's solution.

CASE STUDY

About NuData, a Mastercard company

With its award-winning intelligence, NuData clients can continue to protect accounts confidently despite the threat of correct stolen credentials during login – or other – attacks.

Look at our dashboard to see the intelligence or contact us for a quick demo.

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