NuData Security

mastercard

JULY 1 - DECEMBER 31, 2020

2020 H2: Fraud Risk at a Glance

NuData analysts report on cybersecurity trends

Contents

Foreword

Attacks continue to grow in sophistication

The digital shift during the early pandemic ushered in many online habits that are here to stay. During the second half of 2020, businesses adapted to the "new normal" of online services and purchases. Customers grew increasingly wary of COVID-19-related credential-stealing scams. Online companies encountered new challenges, such as progressively sophisticated automated attacks and unexpected shifts in holiday traffic patterns.

In this follow-up to our H1 fraud risk report, which studied the first half of 2020, we leverage NuData intelligence to understand the evolving nature of online activity and digital threats over the second half of the year. NuData analysts report on monitored activity across the global NuData network. This report summarizes our findings about the changing digital landscape to dissect what happened in H2 2020 and what organizations should expect and prepare to address in 2021 and beyond.

The pandemic changed user behavior in some noticeable ways, like a longer and earlier holiday shopping season. Attack patterns continued to grow with sophisticated scripts targeted at more industries. These attacks bypass security protections by displaying more human-like behavior. More cybercriminals learned to better hide telltale signs of bot behavior, like reusing IP addresses, and gained access to higher quality credentials that increased the success rates of their attacks.

As these trends accelerate, creating a safe and secure environment that users trust is essential. Security solutions that monitor users' inherent behavior, such as NuData's NuDetect, are key to separating sophisticated bots from human users. As part of Mastercard, NuData benefits from a broader global network of online transactions and is integrated into Mastercard's innovative solutions to protect the online ecosystem. This wide-reaching network helps NuData look at the entire user journey — enabling security solutions to work together and progressively learn from each other at every point of interaction.

If you're curious to know more about fraud and risk trends — and our efforts to prevent them — please feel free to reach out. Together, we can build a safer, more trusted online world.

Sincerely,

NuData Analyst Team
verifygoodusers@nudatasecurity.com

The second half of 2020 in numbers

76%

Of attacks on retail companies were sophisticated

45%

Of IP addresses used in attacks were new instead of reused

2.6%

Of stolen credentials used in attacks were successful

A shifted holiday shopping season affected attack patterns

As 2020 holiday shoppers made purchases earlier, fearing shipping delays, attack traffic rose earlier than usual too, showing that companies can't always depend on seasonal trends to predict security needs.

Sophisticated attacks spread across more industries

Attackers using sophisticated scripts that imitate human behavior reduced their H1 focus on financial institutions to target other industries — notably retail, where 76% of attacks in the second half of 2020 followed this pattern.

Human-driven attacks are on the rise

Thwarted by CAPTCHAs and bot-detection tools, attackers increasingly turn to human farms of paid cyber workers to help them fill out forms and bypass security protections at scale.

Attackers evolved their tactics to combat improved security

As security tools get better at identifying suspect IP addresses, attackers are reusing IPs less. Only 55% of attacks involved reused IP addresses in the second half of 2020, compared to 77% in the first half of the year.

Attackers gained access to higher quality credentials

The average percentage of successful credentials per attack nearly doubled from 1.4% in the first half of 2020 to 2.6% in the last half of the year. This may be a sign of the success of popular COVID-related phishing scams designed to steal users' personal information for account takeover attempts.

Traffic trends by industry

In terms of online traffic, the second half of 2020 was in many ways a continuation of patterns from earlier in the pandemic. For example, across multiple verticals, new account creation remained elevated as even more users were forced to move their activities online.

However, new trends revealed themselves in late 2020, the most notable one being an earlier start to the holiday shopping season. Worried that high demand would slow shipping times, shoppers made their purchases an average of three weeks earlier than in 2019, according to Mastercard SpendingPulse™. This affected attack patterns, particularly in retail and eCommerce.

The following pages examine the ongoing impact of the pandemic on both trusted and attack traffic across the largest industries in the NuData network: retail or eCommerce, digital goods, financial institutions, events, and subscription services.

Retail and eCommerce

Financial Institutions

Events

Subscription services

Digital Goods

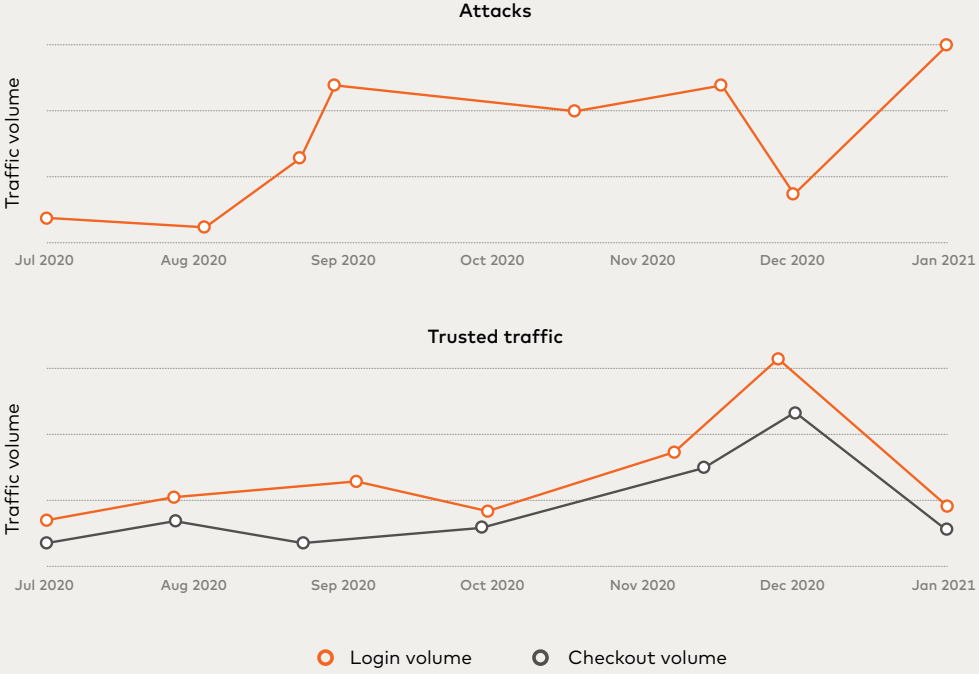
Retail and eCommerce traffic

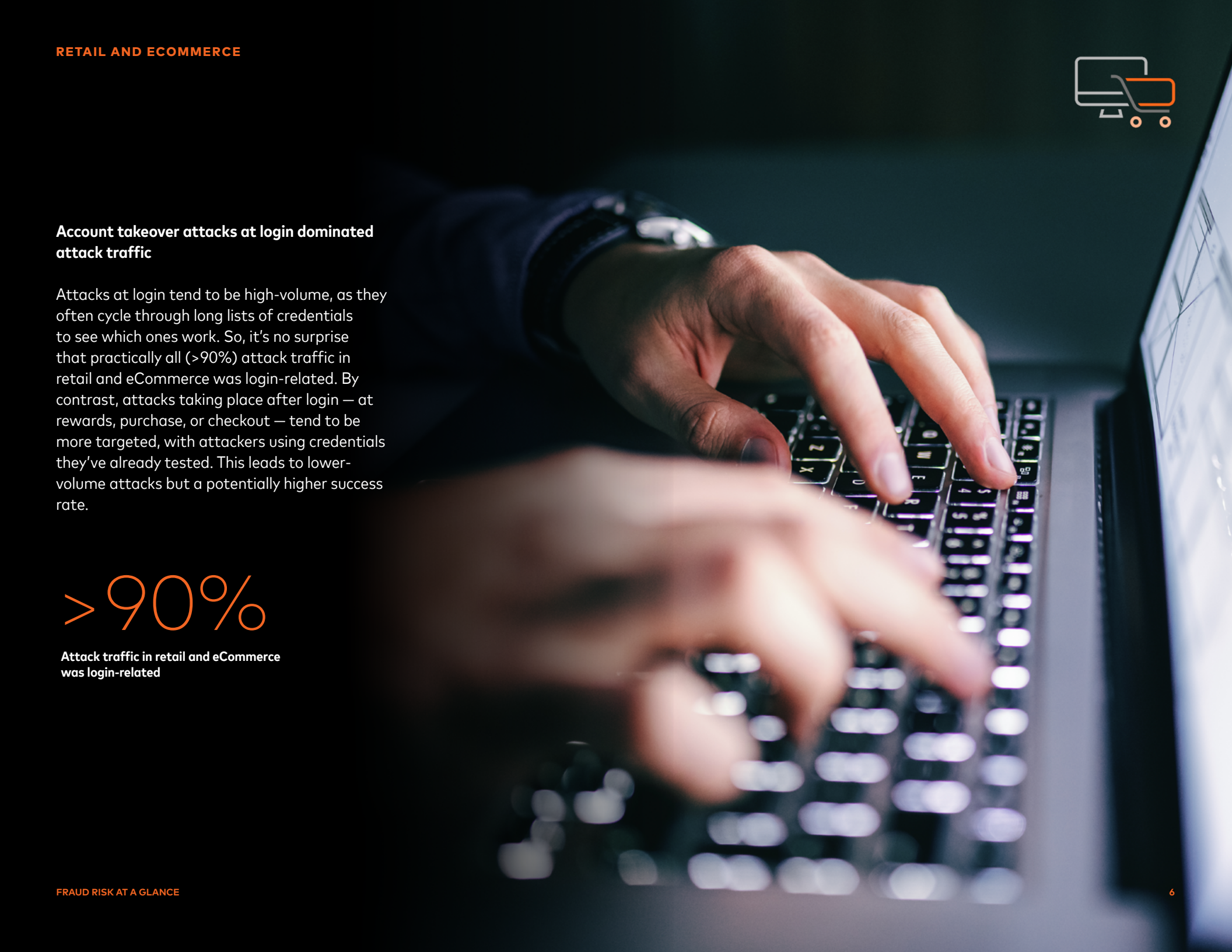
A high-stakes holiday season made retail and eCommerce companies a top target for attacks in the second half of 2020. Here are a few traffic trends that defined the industry.

The holiday shopping season started earlier — and so did attacks

According to Mastercard SpendingPulse™, 2020's expanded holiday season started around three weeks earlier than the previous year, beginning on October 11 rather than November 1. On NuData's network, attack traffic also rose earlier, rising in early fall and maintaining its intensity through the following months.

Usually, NuData analysts see a lull in attack traffic in September and October as bad actors prepare their ploys for the holidays — for example, by opening new accounts in preparation to use them for fraud downstream. This year, it seems that attackers didn't slow down to prepare their scripts and other tools until November. This longer period of holiday attacks is an important reminder that cybercriminals don't always follow expected seasonal trends, making it vital to have security that is scalable across the year.





Account takeover attacks at login dominated attack traffic

Attacks at login tend to be high-volume, as they often cycle through long lists of credentials to see which ones work. So, it's no surprise that practically all (>90%) attack traffic in retail and eCommerce was login-related. By contrast, attacks taking place after login — at rewards, purchase, or checkout — tend to be more targeted, with attackers using credentials they've already tested. This leads to lower-volume attacks but a potentially higher success rate.

>90%

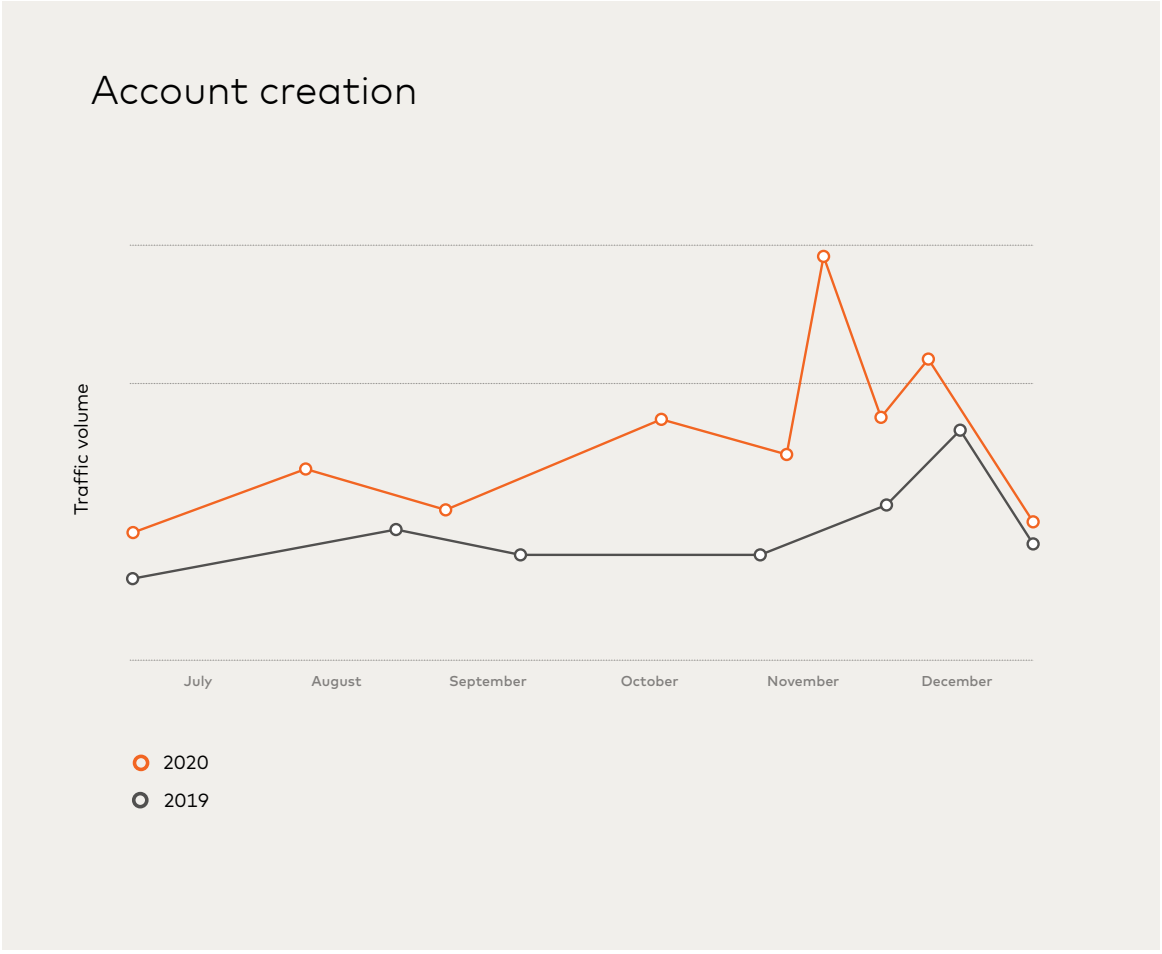
Attack traffic in retail and eCommerce was login-related

Account creation traffic remained high

Consumers' desire to shop from the safety of their homes during the pandemic continued to elevate account creation traffic in retail and eCommerce above 2019 levels in the second half of 2020. Overall, valid account creation traffic volume was 30% higher in 2020 than it was the year before. As new users build relationships with online providers and begin reusing their accounts, this metric is expected to stabilize over time.

30%

Higher valid account creation traffic in 2020 than it was the year before

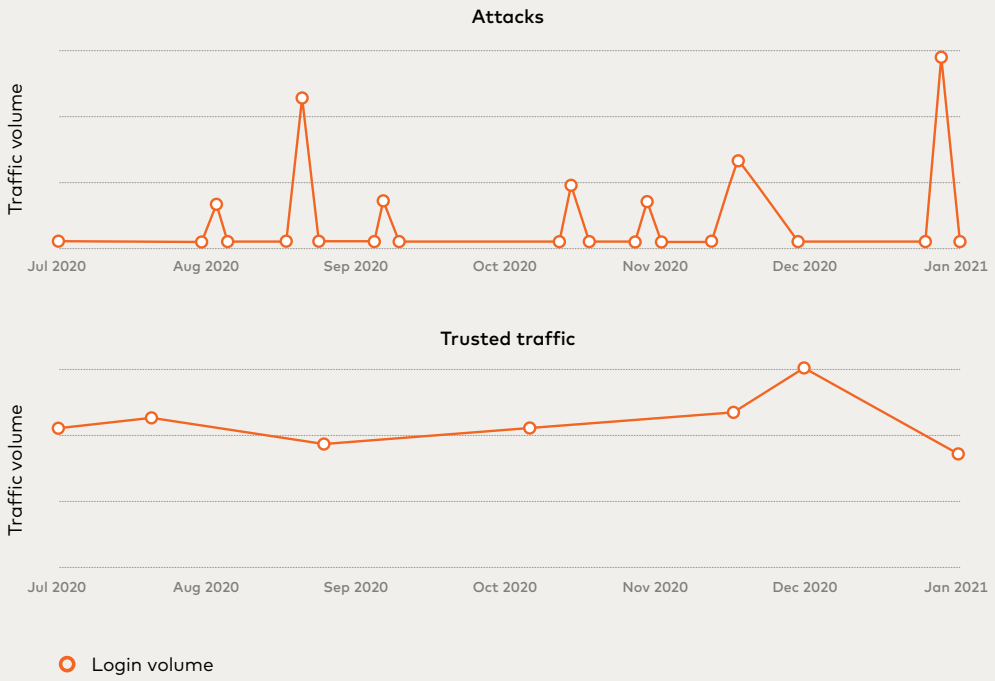


Traffic trends in other industries

Digital goods

While trusted digital goods traffic remained fairly consistent throughout the second half of the year, attack traffic showed spikes traceable to key product launches for retailers. Attackers are quick to identify goods they can easily resell or monetize, leading to sudden large attacks that can overwhelm companies without the right security tools.

Digital goods traffic globally



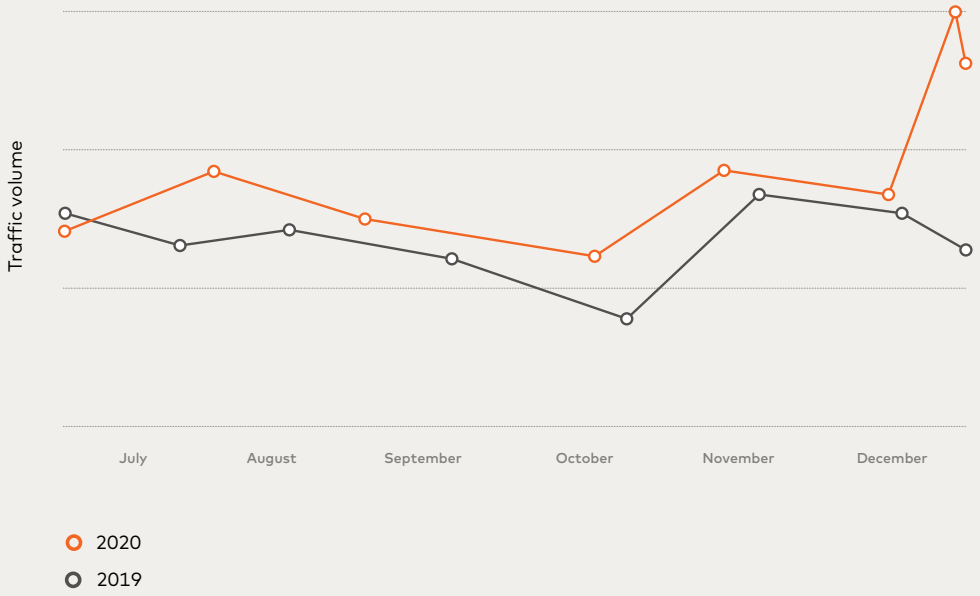
Financial institutions

Online login traffic in the financial industry increased 10% year over year in 2020. This reflects temporary branch closures and health recommendations that ushered more users to online apps. As noted by Aite Group, one FI reported a 250% increase in digital channel usage in a single week in late March in the wake of the COVID-19 shelter-in-place orders, and a number of others report incremental usage of digital channels as well as services such as remote deposit capture and P2P.[1] At the same time, account creation attacks at application placements are also on the rise. Application fraud is expected to cost financial institutions $4.1 billion by 2023.[2]

10%

Increase in online traffic in the financial industry year over year in 2020

Financial institution traffic at login globally, 2019 vs. 2020



[1] *Adapting Fraud and AML Operations to COVID-19. An Aite Group research, Julie Conroy, 2020*

[2] *Application Fraud: Strategies for a Head Start in the Identity Fraud Arms Race, Trace Fooshée, 2020*

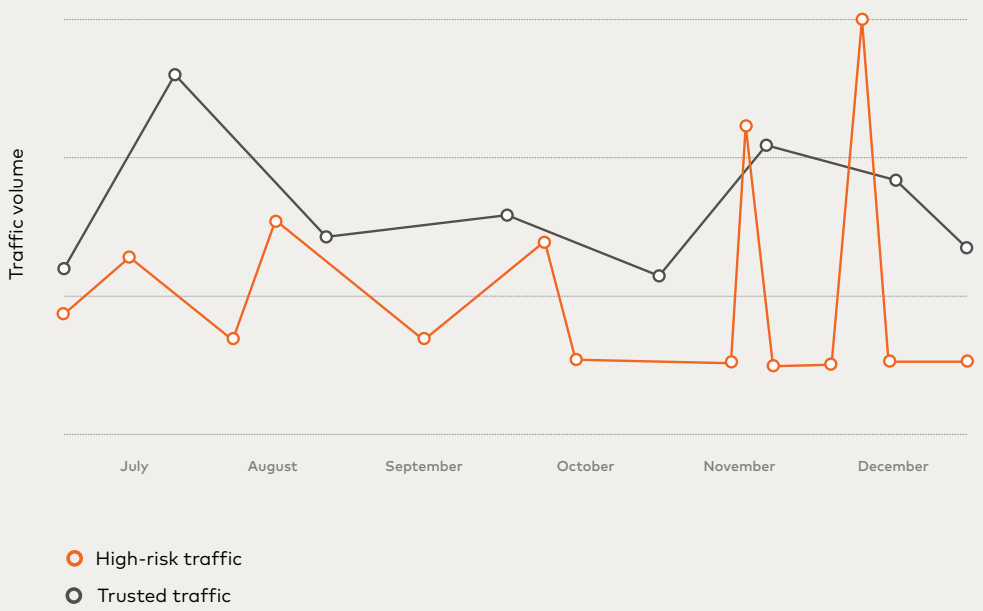
Events

Even though legitimate traffic among event-related companies was at an all-time low due to the pandemic, attacks didn't go down proportionally. Attacks made up 22% of total traffic in the events industry. This is a stark reminder that, even if legitimate traffic is low, it is paramount for companies to never drop their guards.

22%

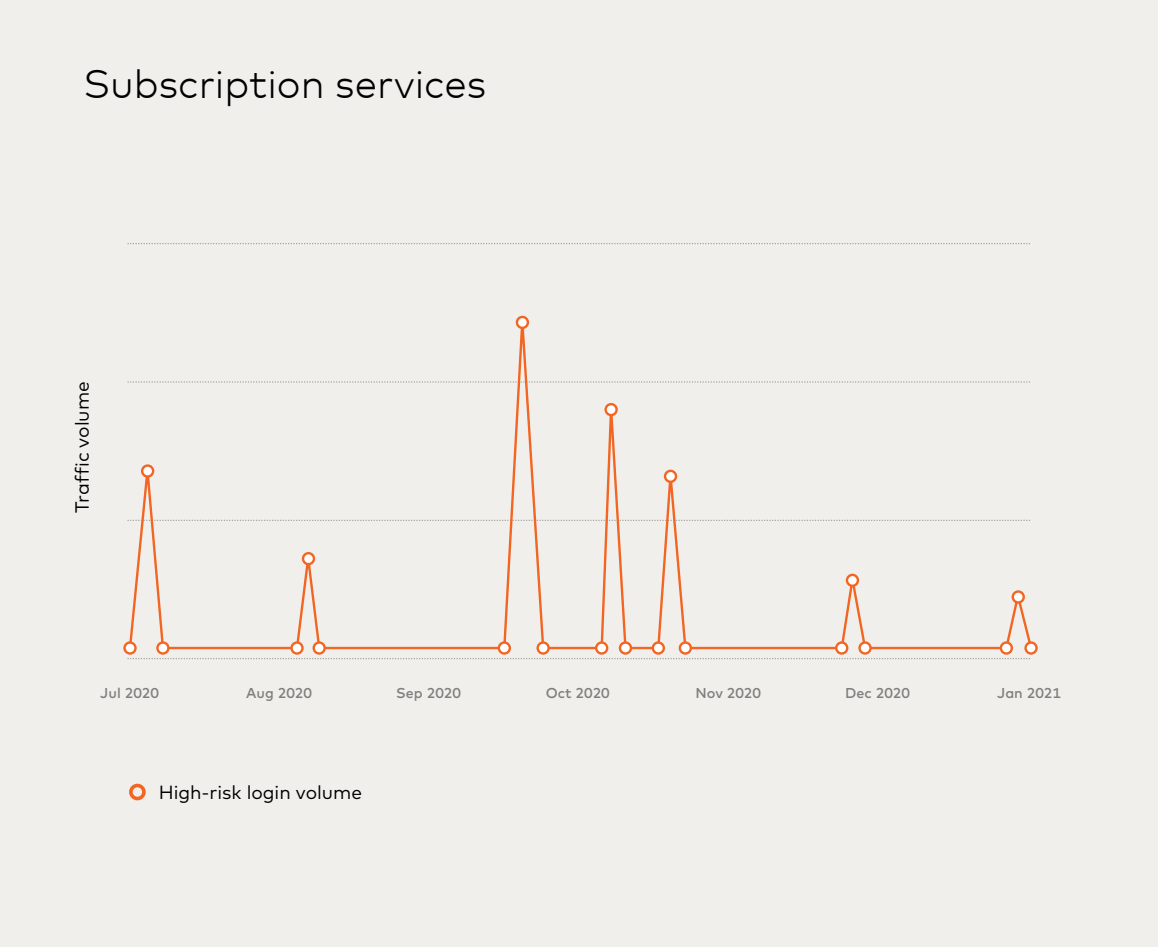
Of total traffic in the events industry were attacks

Events traffic globally



Subscription services

Subscription services in the NuData network were targeted with specific one-off attacks rather than ongoing efforts. These attack spikes show attackers were selective and had short-term goals, unlike attackers carrying out ongoing campaigns in other industries.



Sophisticated attacks: Not just for financial services anymore

Modern security tools are relatively good at identifying automated attacks that exhibit stereotypical bot behaviors. For example, if a user connects directly to a server without executing any JavaScript, that's a telltale sign that they aren't a human interacting with a browser but a potentially malicious bot.

Our H1 report warned of a new type of attack on the rise — sophisticated scripts that emulate human behavior to evade detection. The new trend was most pronounced in financial services, where 96% of all attacks in the first half of 2020 were of this nature.

Sophisticated vs. Basic Attacks

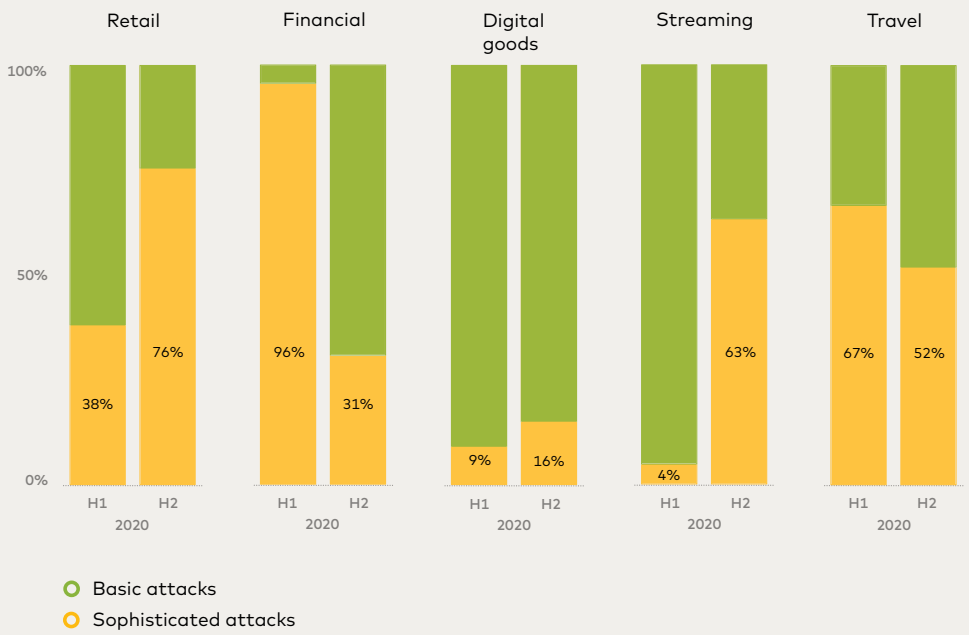
A **basic automated attack** lets a bad actor test a large number of credentials very quickly but often shows telltale bot behavior such as repeated use of the same IP address or a lack of JavaScript execution. As a result, it's easier for security tools to detect.

A **sophisticated automated attack** imitates real human interaction by running scripts that display common browser or application behavior. While sophisticated attacks are usually lower volume than basic attacks, they're much harder for common security tools to detect.

Our H1 report predicted this focus was likely to shift as attackers tested their new techniques against industries that are perceived to have weaker security protections. The percentage of attacks on financial institutions that were sophisticated dropped to 31% as attack volumes in the sector declined overall.

At the same time, sophisticated attacks expanded rapidly to other verticals — notably retail, where 76% of attacks were categorized as sophisticated in the second half of 2020, compared to only 38% in the first half of 2020. In this section, we dive deeper into how such attacks are continuing to evolve to evade common security tools even more effectively.

Sophisticated vs. basic attacks by industry



The rise of human-driven attacks

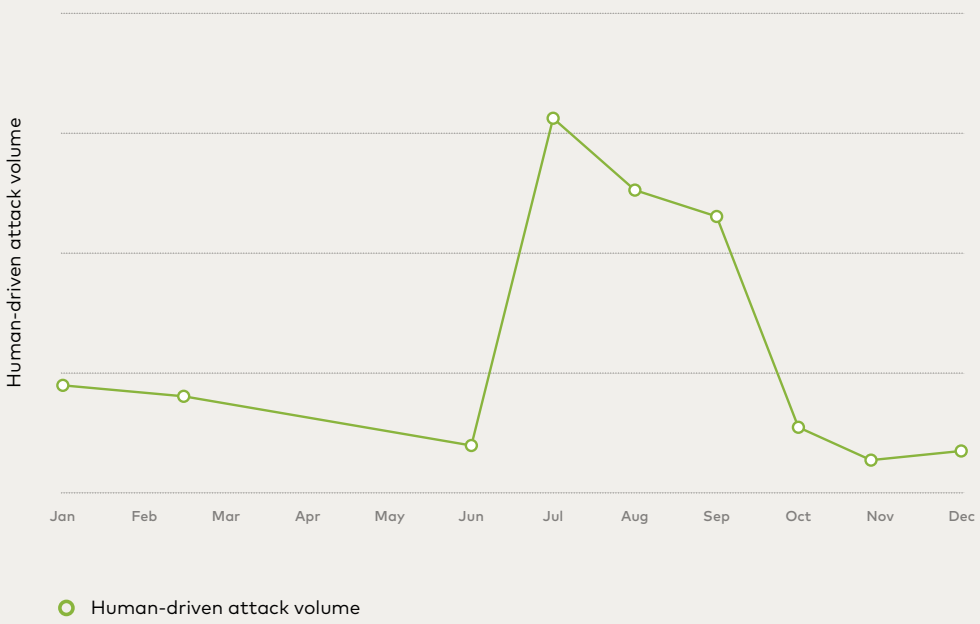
Besides writing more advanced or complex software scripts, cybercriminals are also increasingly turning to a new tool to thwart security protections: other humans.

Bot-detection tools, improved CAPTCHAs and other technologies that mitigate basic automation are starting to affect bad actors and reduce the ROI of their attacks. As a result, they're increasingly looking for alternatives to bypass these bot defenses, especially when targeting high-value accounts, such as financial accounts and accounts holding payment information or loyalty points.

One option is to pay small sums to human farms to complete online tasks, such as solving CAPTCHAs, posting reviews, or creating new accounts.

As the use of bot detection tools becomes more widespread, this tactic is growing in popularity. Within the NuData network in the summer of 2020, we saw a four-month spike of attacks using this type of human labor to attack high-value accounts within the financial industry — a 350% increase in human-driven attack traffic compared to the 2020 average.

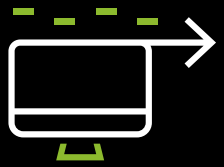
Human-driven account takeover attack volume by month



Case study: Bots and humans – A hybrid attack

What do these sophisticated and human-driven attacks actually look like? We dissect a four-step attack from our network that targeted account login and wallet functionalities at the same company. This example shows how a sophisticated attack mimics human behavior and can even leverage human workers in real time to bypass bot-detection challenges.

Testing the scripts



Outsourcing CAPTCHAS

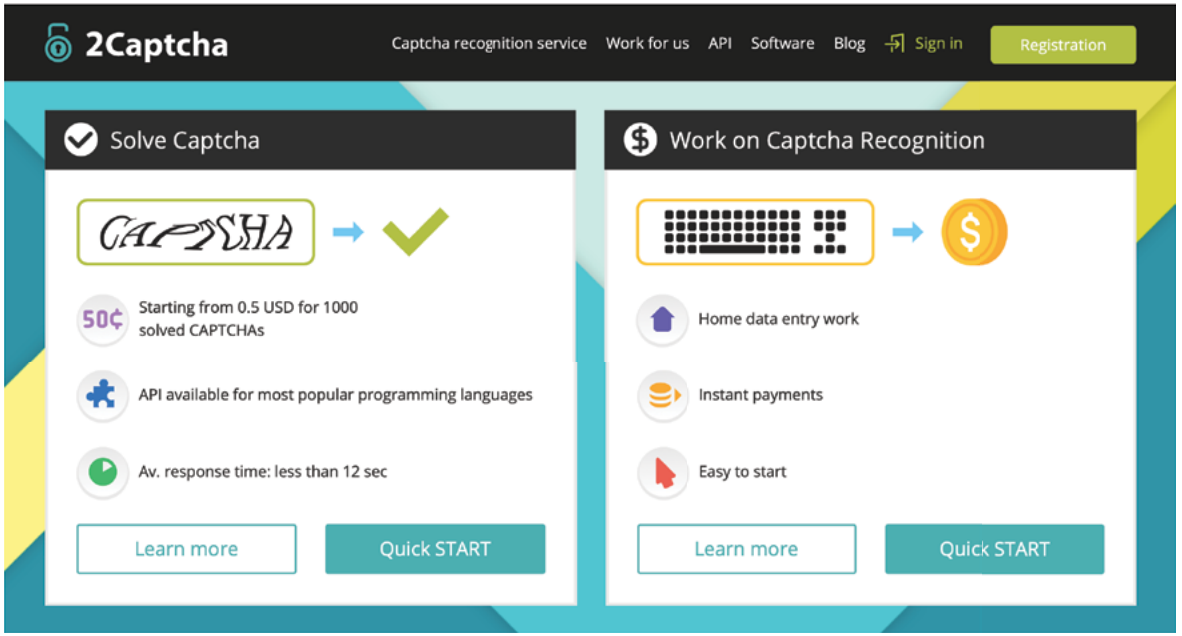
Harvesting payment information

Learn, rinse, and repeat

An 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.

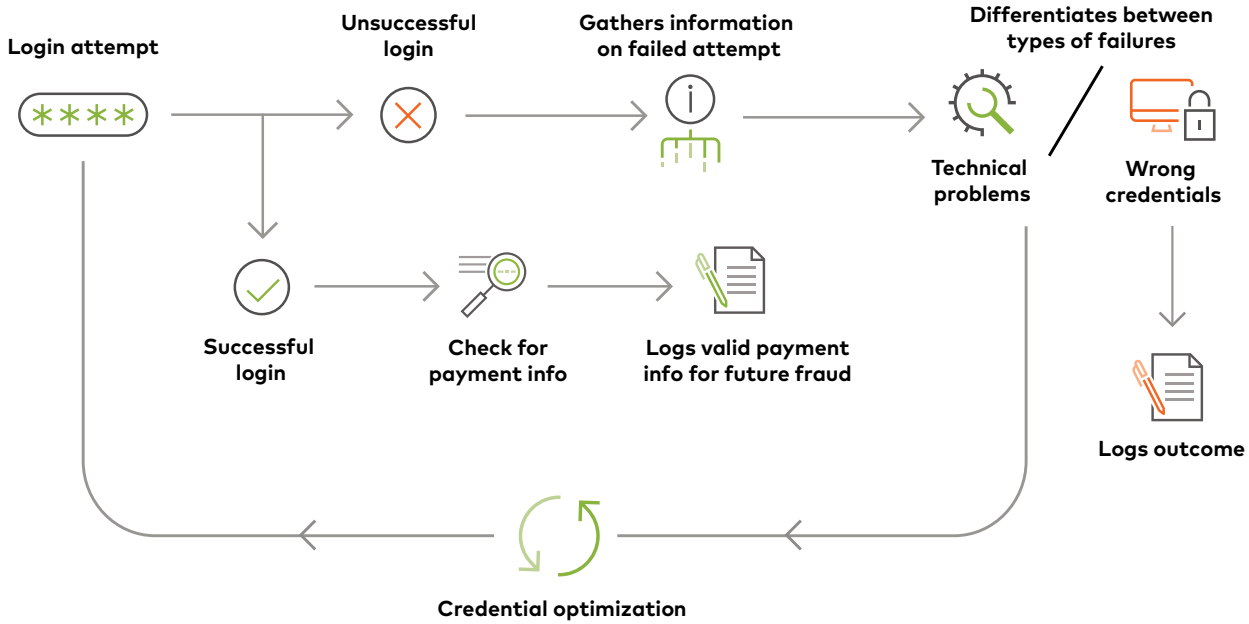


[3] *https://2captcha.com*

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 was successful in opening 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, whether the login attempt was mitigated by our solution or it worked, and — for the few successful logins — 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 enabling 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 activity: Signs to watch out for

Besides bypassing bot detection tools, human farms help bad actors open large quantities of new accounts for fraud use. As these and other human-driven tactics grow 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 hundreds of times in a given day. Their familiarity with a form 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 also tend to submit a new account or application faster than the average user, another key indicator.

Lack of familiarity with the data: 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.

Use of copy-paste: Often, the workers copy personal data like names and birth dates from an Excel spreadsheet or other document, rather than typing it in manually as a legitimate user likely would.

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 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.

New IP addresses

As mentioned in the section about sophisticated attacks, the reuse of IP addresses is a telltale sign of a basic automated attack.

87%

Of attacks showed some login anomoly that allowed NuData to flag them in real time

55%

Of IP addresses used in attacks in H2 2020 were reused, compared to 77% in H1

Companies once had limited means to detect and block reused or otherwise suspect IPs, but detection capabilities have improved as companies have strengthened and formalized their approaches. As Aite Group Senior Analyst Trace Fooshée explains:

> " In the early days, [companies'] countermeasures were largely home-grown and were heavily biased towards internally developed lists of suspect ranges of IP addresses associated with TOR nodes and/or suspect geolocations. As time wore on, more FIs and merchants began deploying more sophisticated and formally-structured solutions that required less maintenance, less cost, and that were able to scale more effectively than their home-grown countermeasures. "

These "more sophisticated and formally structured solutions" have put increasing pressure on fraudsters to refine their tactics and attempt to stay ahead of security tools.

One resulting tactic has been an uptick in the usage of new IP addresses used by attackers. In the second half of 2020, only 55% of IP addresses used in attacks were reused, compared to 77% in the first half of the year. This signifies that attackers are increasingly using services that cycle through clean IP addresses to bypass device-based security tools that look at IP reputation.

Still, the vast majority (87%) of attacks showed some login anomaly that has allowed NuData to flag them in real time, proving the robustness of some existing security solutions to deal with the new threat.

2020	Login anomalies	Reused IP addresses
H1	90.3%	76.7%
H2	87.0%	54.8%

Quality of stolen credentials

When an automated attack involves millions of attempts, any success rate above zero can have devastating consequences.

Unfortunately, the second half of 2020 has seen a nearly twofold increase in the average percentage of successful credentials per attack, up to 2.6% from 1.4% in the first half of the year.

Where did these high-quality stolen credentials come from? It's possible they fell into fraudsters' hands during the wave of COVID-related phishing attacks that hit users earlier in 2020 — or they could be the result of the ever-recurring breaches that exposed 22 billion user records in 2020.[4]

Fortunately, we don't expect these high success rates to sustain themselves in 2021. Still, these statistics serve as a reminder of the importance of closely monitoring login behavior to protect customer account data.

Percentage of successful credentials used in attacks by industry, first vs. second half of 2020

	Digital Goods	Retail	Financial	Travel	Streaming	Events
First half of 2020, successful credentials	0.02%	1.18%	0.40%	1.37%	0.19%	3.95%
Second half of 2020, successful credentials	0.11%	11%	0.09%	0.001%	0.9%	3.5%

Average H1 2020: **1.4%** Average H2 2020: **2.6%**

[4] *https://www.itp.net/security/95637-over-22-billion-records-were-exposed-in-data-breaches-in-2020-report*

Conclusion: What the data tells us about 2020 — and what to expect in 2021

1

Just because legitimate traffic drops doesn't mean that attacks will. For example, while trusted traffic in the events industry slowed to a trickle in the second half of 2020, attacks continued — to the point where attacks made up almost a quarter (22%) of total traffic across the events industry. It's important never to drop your guard, even when you see low overall traffic.

2

As attackers gain access to higher-quality credentials, success rates can go up, multiplying the potential for damage. Even if the majority of the attempts in a mass-scale attack fail due to wrong credentials, cybercriminals still gather valuable information about which credentials work and which ones don't. Companies need the means to stop these attacks from the start.

3

The sophistication of automated cyberattacks keeps reaching new heights. NuData analysts are seeing scripts that include actions beyond login, as we saw in the hybrid attack NuData mitigated. These attacks leverage humans to circumvent bot-mitigation tools without much overhead. Companies must be ready to detect these attacks from the start and block them effectively — and do so without impacting legitimate users who are trying to access a company's goods and/or services.

4

Human-driven attacks are still a minority, but they're highly dangerous as they are hard to differentiate from legitimate humans. Tools that include passive biometrics and behavioral analytics are crucial to identifying telltale patterns in human farm behavior, such as how they type personal information into a form or how far they move a mouse.

Glossary of terms

Account creation or online account origination fraud: The opening of a new account with fake or stolen information with the intent of committing fraud.

Account takeover: A fraudster illegally accessing a victim's account for fraudulent purposes.

Basic attacks: Attacks focused on quantity rather than quality. They don't attempt to emulate human behavior or browser interaction and they typically don't execute JavaScript. They characterize for displaying high velocity and cloud-hosted IPs.

Bot-detection challenge: A challenge such as a CAPTCHA that could help confirm if the user is a machine or a human, applied when an event is suspected to be fraud.

Bot-detection tool: Tools detecting bot behavior by looking at data such as IP, location, connection, or input.

Digital goods: Includes companies selling any goods that are stored, delivered and used in their electronic format, including SaaS.

eCommerce: Includes companies buying and selling goods or services online.

Events: Includes companies that sell tickets for online or in-person events such as concerts or conferences.

Financial institutions: Includes institutions that provide financial services such as banking and credit unions, including FinTech (Financial Technology).

High risk: Session or sessions (client interaction) with a high-risk score that exceeds a a baseline of a safe interaction, based on the NuData platform's assessment.

Placement: User interaction points, such as account creation, login, and checkout.

Sophisticated attacks: Attacks deploying lower volume but attempting to emulate user behavior. They display expected browser or application. They are highly organized and have significant resources at their disposal behavior and run scripts in the environment to simulate human interaction.

Subscription companies: Includes companies that offer digital services, often related to multimedia, for a monthly fee.

Success rate: The number of login attempts (mitigated) with correct credentials for every 100 attempts. In the context of an attack, the success rate is not how successful the attack was but how many credentials were correct, despite the attack being blocked.

Travel: Includes companies with travel portals.

Trust Consortium: Historical data of events and accounts aggregated from the NuData network to improve the accuracy of each assessment. NuData hosts the largest behavioral network, with 650 billion behavioral events monitored only in 2019, this data is hashed and doesn't include personally identifiable information.

About NuData, 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 is a Mastercard company. It helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing over 650 billion behavioral events annually, NuData harnesses the power of behavioral analytics and passive biometrics, enabling its clients to distinguish legitimate users from high-risk ones. This allows clients to verify users before a critical decision, block account takeover, stop automated attacks, and reduce customer insult. NuData's solutions are used by some of the biggest brands in the world to prevent fraud while offering a great customer experience.

+100M

accounts protected monthly

+650B

behavioral events monitored annually

About Mastercard SpendingPulse™

Mastercard SpendingPulse™ reports on national retail sales across all payment types in select markets around the world. The findings are based on aggregate sales activity in the Mastercard payments network, coupled with survey-based estimates for certain other payment forms, such as cash and check. As such, SpendingPulse™ insights do not in any way contain, reflect or relate to actual Mastercard operational or financial performance, or specific payment-card-issuer data.

Mastercard SpendingPulse™ defines "U.S. retail sales" as sales at retailers and food services merchants of all sizes. Sales activity within the services sector (for example, travel services such as airlines and lodging) are not included.

NuData Security

mastercard