NuData Security
mastercard

Attacks are more sophisticated during COVID times - How to detect them with behavioral technologies.

FINANCIAL INSTITUTION EBOOK

Attacks getting sophisticated... and then COVID.

Last year closed with 7,098 data breaches[1] that exposed over 15 billion user credentials. The stolen credentials and personally identifiable information (PII) are available on the dark web for schemes such as account takeover and credential stuffing attacks.

Most risk and fraud departments are familiar with these login threats, such as an automated script that tests a set of username and password combinations against a login page to see which ones gain access to an account. The login attempts occur rapidly and often have obvious giveaways: they reuse the same IP address repeatedly or don't even load the JavaScript on your browser or app, for example.

This is a common scheme that all financial institutions experience. However, a new breed of refined attacks is growing into a dangerous threat to all banks operating online. This wave of attacks tricks most bot-detection tools into thinking they are human users instead of scripts by mimicking human behaviors, such as typing speed or cadence, or other sophisticated techniques.

In a time when users increasingly rely on online services – and attacks are evolving – financial institutions have greater pressure to differentiate their good users from threats. Many FIs are benefiting from behavioral and passive biometrics tools that help businesses detect sophisticated attacks and protect customers.

> **"Financial institutions are starting to increasingly leverage behavioral biometric technologies in their user verification platforms in order to prevent sophisticated attacks and protect customers, while minimizing impact on the customer experience."**
>
> **Julie Conroy, Research Director, Aite Group**

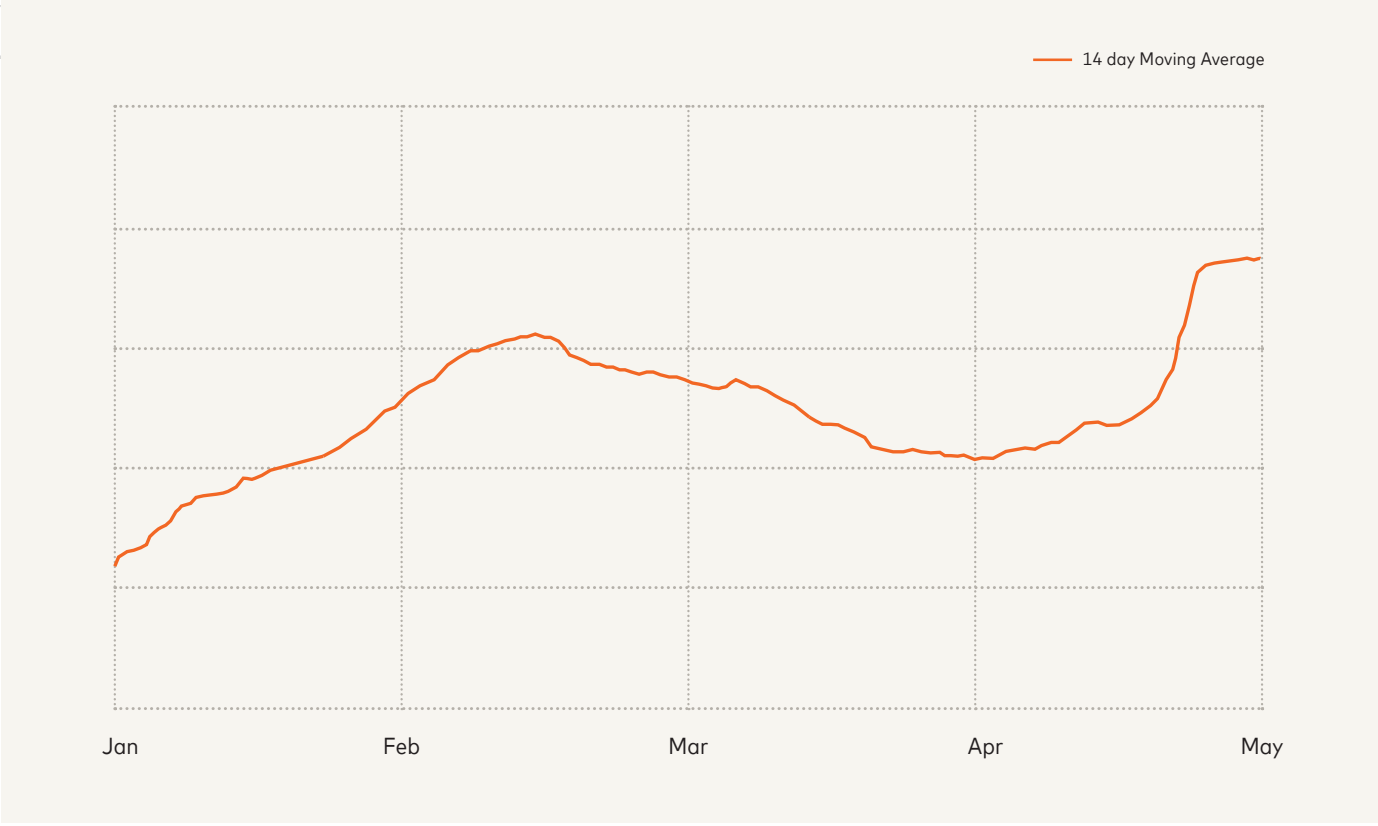
[1] RiskBased Security, 2019 Year-end Report - Data breach QuickView

Traffic changes during lockdowns

With movement restrictions and the temporary closure of branches, customers are going online for their banking services. According the Aite Group, "one FI reports 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[2]."

This change is also reflected in the NuData Trust Consortium (a pool of aggregated and anonymized data). Below, we can see that aggregated financial-related traffic is steadily rising compared to January of 2020.

A portion of this customer base prefers banking in the branch but are now forced to access services online. Some are less computer-savvy and more susceptible to online scams that steal banking credentials – perpetuating the problem of account takeover attacks.



Financial institution traffic volume globally. Source: NuData

[2] Workplace Distancing: Adapting Fraud and AML Operations to COVID-19, Aite Group, 2020

The blurry line between attackers and customers

According to NuData analysts, customers interact with an average of three devices: a work computer, a home computer, and a smartphone. However, due to movement restrictions, there are behavioral changes that analysts have detected in good users, including a higher number of logins per account and unusual amounts in money transfers.

It is important to incorporate these variations into a machine learning model to maintain user verification accuracy. This pandemic has impacted users' daily activities and behaviors, also changing the way they interact with technology. A good user verification tool needs to adapt to this new normal as well, verifying users in real time.

Static security tools that don't look at the user changes or lack machine learning capabilities can mistakenly flag behavioral deviations as fraud and block legitimate login or money transfer attempts.

Organizations need tools that help them discern changing customer behavior to avoid false declines – when a user is mistakenly marked as fraudulent – and, more importantly, mitigate fraudulent traffic.

"There are behavioral changes that analysts have detected in good users, including a higher number of logins per account and unusual amounts in money transfers."

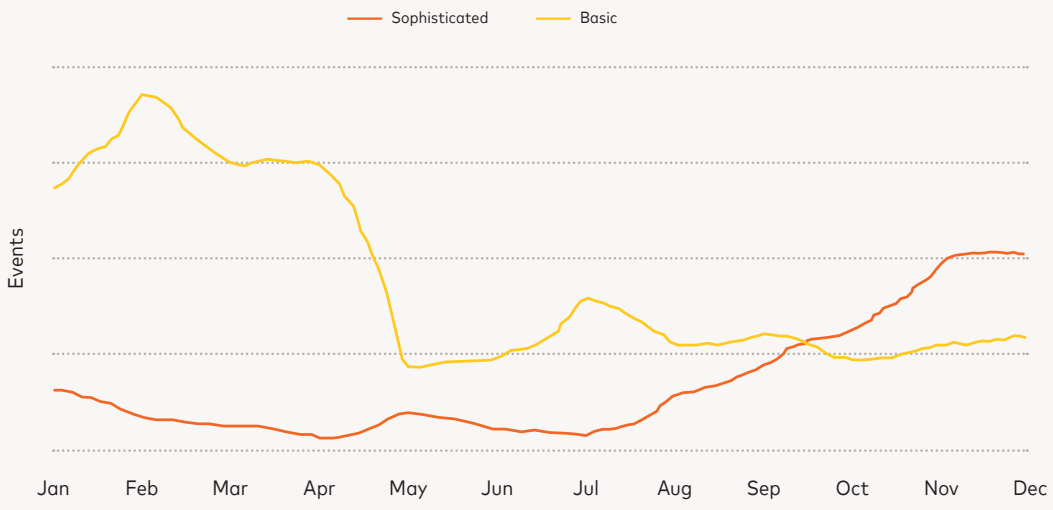
Protecting against a new breed of attacks

As we said at the beginning, attacks are becoming cleverer and more sophisticated. Bad actors are improving their techniques to seem human and bypass most bot-detection tools.

Bot-detection tools are good at identifying basic automation signs such as velocity, unrealistic travel, or whether the JavaScript on a page or app was loaded. But sophisticated attacks go beyond and make an additional effort to emulate human behavior with their scripts.

During 2019, NuData saw a threefold increase in attacks categorized as sophisticated, for the first time ending the year with a higher number of sophisticated attacks than basic attacks (see graph below). This means bad actors are focusing on quality, investing more time in developing their scripts than deploying volume-driven basic attacks.

Sophisticated attacks vs. basic attacks



Aggregated high-risk traffic divided into sophisticated and basic attacks. Source: NuData

A basic attack focuses on high volume rather than quality. It doesn't attempt to emulate human behavior or browser interaction, and it typically doesn't execute JavaScript.

A sophisticated attack attempts to emulate user behavior, increasing its effectiveness. It displays expected browser or application behavior and runs scripts in the environment to create a human-like interaction.

A closer look at what sophisticated attacks look like

Sophisticated cyber-attacks automate the behavior that would normally come from a human.

Common patterns of attacks that emulate a real user include:

- **Trigger of the keyboard to type user information (e.g., username and password):** An attack doesn't need to use a keyboard to provide credentials, but the script can trigger the keyboard to seem human, showing additional effort from the perpetrator.
- **Use of irregular keystrokes and pauses to mimic human behavior:** When a script uses a keyboard to seem human, it can be enhanced by programming a series of random pauses between keystrokes to resemble a user's uneven typing.
- **Use of fake IP and location combinations that match (e.g., the IP belongs to an area in Boston, and the geolocation is Boston):** Most attacks use randomized IPs and locations to keep attack costs down. Pairing up geolocation with an IP from that same location requires additional effort from the hacker, showing further sophistication.
- **Lowering the velocity of the attack:** A script can test thousands of credentials within a few seconds. However, because no human can be that fast, it can expose the attack. Sophisticated attacks lower their velocity to simulate human speed.

Within the NuData Trust Consortium, we constantly see sophisticated attacks attempting to access our clients' environments. Some of these attack vectors go on for months before the attacker realizes they can't permeate the security barrier and suddenly stop. Once they disappear from one platform, they often move on to another one for better luck. As attack vectors move from platform to platform, financial institutions need to make sure their security will block the threat until it moves on – and the next one comes in.

How to mitigate these attacks

To mitigate these sophisticated attacks, companies need technologies that can look at traffic beyond static parameters such as location, IP, or attack velocity. While many business approaches focus on building more security barriers, these can block good users too. A security approach with an invisible barrier can protect the good user's experience and only make itself perceptible for risky traffic.

Behavioral and passive biometrics tools enhance the collection of data for every event assessment and build a holistic view to discern if it is made by a human or bot without blocking legitimate customers. These technologies help financial institutions mitigate sophisticated threats targeting their environments, including credential stuffing, account takeover, and money-transfer fraud.

WHAT ARE BEHAVIORAL ANALYTICS AND PASSIVE BIOMETRICS?

Behavioral analytics is a technology that evaluates signals across the user interaction. Looking at the device, type of browser, type of information input, and other parameters help determine if the user is behaving like a good user or like a bad actor.

Passive biometrics builds an online user profile based on a user's inherent behavior when they interact with a device. The typing cadence, how one holds the device, and other parameters build a unique profile. This technology determines if the behavior from a user matches the behavior of that same user in the past. This effectively determines not only if the behavior is that of a good user, but if it is indeed the expected behavior of this user.

Behavioral tools help financial institutions detect the most sophisticated threats, even if these attacks:

- use a keyboard to type a password;
- mimic a human typing cadence;
- show an expected IP and location;
- use new devices that are not linked to past fraud.
- allow the JavaScript to load, slowing the attack;
- combine automation with human interaction, such as human farms, to solve bot challenges, such as CAPTCHA.

HOW BEHAVIORAL TECHNOLOGIES HELPED A LARGE BANK PREVENT A SOPHISTICATED ATTACK

In March of 2020, a financial institution was targeted by a sophisticated attack vector that lasted weeks, with nearly 750K account takeover attempts. This sophisticated attack was hybrid, combining automation and human-driven work. When NuData flagged each event as a bot and triggered a challenge, the script rerouted the request to a human worker.

Some of the sophisticated traits:

- Valid JavaScript loaded.
- Human-style input (e.g., keystrokes, longer time on page).
- IPs located within the United States, where this bank's regular customers are.
- Fast cycling of IP addresses, 9 attempts per IP.
- Combine automation with human interaction, such as human farms.

Summary of attack results

Nearly

750K

account takeover attempts.

99.6%

account protection accuracy.

In conclusion

As bad actors gather more user data from COVID-related online scams, attacks are expected to become increasingly targeted with more user credentials and personally identifiable information. At the same time, the changes in good user behavior can make some legitimate customers seem risky, increasing false positives.

Behavioral and passive biometrics technologies are allowing many financial institutions to gather additional intelligence for better account protection against sophisticated attacks.

To learn more about how to implement NuData's behavioral solutions to prevent sophisticated attacks while protecting your customers, contact verifygoodusers@nudatasecurity.com

Read another case study about how NuData helped a top U.S. bank prevent a mass-scale attack.

ABOUT NUDATA

NuData Security is a Mastercard company that helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing over 650 billion events only in 2019, NuData harnesses the power of behavioral and biometric analysis, enabling its clients to identify the human behind the device accurately without additional friction. This allows clients to verify users before a critical decision, reduce customer insult, block account takeover, and stop automated attacks. NuData's solutions are used by some of the biggest brands in the world to offer a great customer experience while preventing fraud.

NuData Security
mastercard