BioCatch

Case Study

BioCatch puts the brakes on a sustained cyber attack and produces demonstrable results for Top 5 UK bank

Account takeover fraud from advanced malware drastically reduced with behavioral biometrics

Problem

The corporate banking division of a Top 5 UK bank was experiencing a prolonged cyber attack involving the Dridex malware which was capable of taking over customer accounts and circumventing its traditional controls such as malware detection, transaction monitoring and device fingerprinting.

Solution

The bank required a solution that could generate a deeper level of behavioral analysis. The bank adopted BioCatch to gain visibility into anomalies in user behavior and interactions. BioCatch quickly identified several high-risk activities based on user behavior, even when it appeared the session came from a trusted device and location.

Results

81%

FRAUD DETECTION RATES WITH ONLY A 0.05% FALSE POSITIVE RATE

23x

RETURN ON INVESTMENT

£1.6M

STOPPED A £1.6M ATTEMPTED FRAUDULENT TRANSACTION

Most authentication and fraud prevention solutions rely on known device and IP location parameters to measure fraud risk. While these controls can be effective, advanced malware can easily bypass them. This is especially true in the case of Remote Access Trojan (RAT) attacks as they entirely take over a device and makes it appear that the transaction is coming from the legitimate user. When a RAT is present, a bank's systems detect a genuine device fingerprint, with no traces of proxy, code injections, or malware, and the proper IP and geo-location.

The banking environment itself has also become more complex. In the case of corporate banking, financial institutions inherit much risk with high value transaction amounts that are often sent to international or unknown destinations. Digital transformation has also put pressure on the financial services industry to move money faster and with minimal disruption to businesses.

Traditional Fraud Detection Controls Leave Blind Spots

A Top 5 UK bank was experiencing a sustained cyber attack which was capable of bypassing its fraud prevention controls, such as malware detection, transaction monitoring and device fingerprinting. BioCatch behavioral biometrics was deployed within their online banking application and very quickly spotted several high-risk behaviors indicative of criminal activity.

During the initial pilot period, the bank realized a 23x return on investment in fraud detection, and with BioCatch alone, was able to detect 81% of fraudulent transactions with less than a 0.05% alert rate. In one of the most notable cases, BioCatch was able to prevent an attempted £1.6M fraud transaction that involved a remote access attack with highly sophisticated malware. The transaction, although high in value, was not unusual for this corporate customer. The transaction also seemed normal, appearing to come from the regular corporate proxy and trusted device.

Unknown to the user and the bank, that device had been infected with Dridex malware which is invisible to most anti-malware defenses. Using a clever set-up, the malware redirected the user to a fake website resembling the real bank's website, which allowed them to harvest the user's credentials. The attackers then leveraged a VNC back-connect Remote Access function and attempted the £1.6M transaction. BioCatch was the only fraud prevention control that generated an alert. Other fraud prevention tools used by the bank, including transaction monitoring, anti-malware, device recognition, and location analysis solutions, did not recognize the threat.

Behavioral Biometrics Gets Inside an Advanced Malware Attack

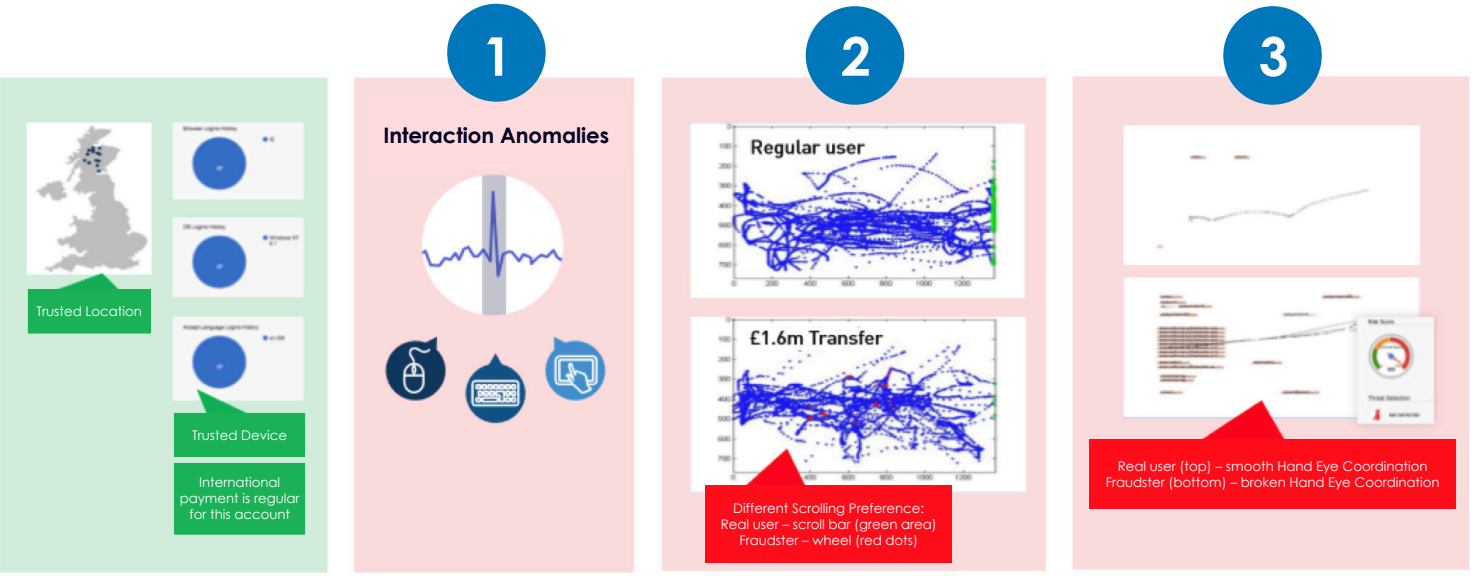
Analyzing the user's cognitive preferences, BioCatch noticed several anomalies in the session as follows:

1. There were several anomalies in the interaction patterns with specific fields. For example, the attacker used the keyboard to select the destination country, whereas the regular user always used the drop-down. There were also changes in the way the user interacted with the reference text.

2. The user always used the scroll bar (green area in the upper middle screenshot) to navigate, while the attacker scrolled up and down with the mouse wheel (red dots on the lower middle screenshot).

3. There was a disruption in hand-eye-coordination, determining the session was being done via remote access, a never-seen-before occurrence for this user.

As a result, BioCatch generated a real-time alert allowing the bank to stop the transaction and prevent a catastrophic loss.



Despite coming from a trusted location and device, BioCatch behavioral biometrics spotted several interaction anomalies typical of advanced malware, and not of the user.

Today, BioCatch helps the bank with additional capabilities including detecting RATs, protecting OpenAPI flows, investigating disputes, and fighting social engineering attacks such as Help Desk scams and authorized push payment fraud. The bank also extended BioCatch across multiple business units to protect the financial assets of 19 million corporate, retail and wealth management customers.

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch