BIOCATCH™
Less Friction. Less Fraud.

Fraud Detection Case Study

A Top-5 U.S. Bank Detects *TrickBot* Malware Attacks with BioCatch's Behavioral Biometrics Solution

Problem

Malware infections and Remote Access Trojan (RAT) attacks are on the rise, enabling cyber criminals to take over accounts from afar and automate fraud. Despite traditional fraud detection measures and cybersecurity safeguards, malware and RAT attacks remain prevalent. Undetected malware attacks can result in direct losses to account holders and have a long-term detrimental effect on business and customer confidence.

Solution

BioCatch's next generation authentication tools leveraging behavioral biometrics were integrated into the bank's digital channels to provide real-time alerts on suspected fraud. BioCatch behavioral biometrics analyzes interactions between users and devices and applications to prevent identity theft and fraud inside authenticated sessions. The technology can distinguish between human and non-human imposters and alert the bank's fraud/security teams in real-time.

Results

BioCatch detected a series of TrickBot malware attacks that bypassed the traditional fraud detection measures, preventing fraud that could have resulted in astronomical losses to the bank.

This Top-5 U.S. bank has tens of millions of customers around the world. It serves clients across investment banking, private banking, corporate lending and securities services.

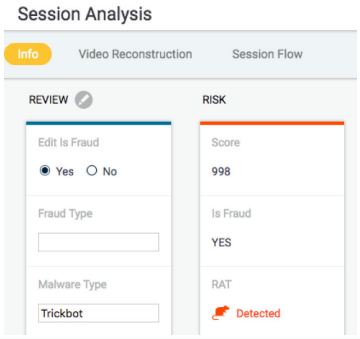
Background

The *TrickBot* banking Trojan emerged in 2016, menacing banks and financial institutions around the world. By 2017, TrickBot became a widespread malware family and global threat, accounting for 9.5% of attacked users. The *Trickbot* malware combines remote access (RAT) and redirection techniques to conduct sustained, multi-phased campaigns. It then slowly manipulates victim accounts until ready to deploy a standard remote access protocol, which is completely invisible to device recognition and geo-location tools. After switching off all active components of the malware, it opens a browser from within the genuine victim's machine, logs into online banking and proceeds uninterrupted to empty the victim's account.

In Q1 2018, a Top-5 U.S. bank with global corporate customers approached BioCatch to leverage its next generation authentication tools in combating these types of malware attacks against its wealth management customers. After a few weeks in operation, BioCatch was able to detect several attacks launched against online customers and provide real-time alerts to the bank.

Specifically, a legitimate user in Africa had been a victim of a *Trickbot* attack, which BioCatch immediately spotted in real-time. The user behavior was quite different than norm.

Detecting the Presence of TrickBot Malware with Behavioral Biometrics



[1] Source: Kaspersky

BioCatch detected a *TrickBot* session and gave a high score of 998 of 1000 after a real-time behavioral biometric analysis. This is how it happened:

Through a malicious spam campaign that contained an "expanded webinject configuration", TrickBot infected the machine of this global bank's customer. When the customer went to his online banking page, the Trickbot virus redirected him to a phony site, while at the same time maintaining the live connection with the genuine page and leveraging the login that the legitimate user did to enter his account. As the Trojan manipulated the user's activity, BioCatch detected the anomalous behavior and provided an alert to stop the fraud in real-time.

BioCatch runs in the background, providing a passive and continuous authentication layer that maintains the integrity of sessions without any friction or disruption. This capability provides ongoing security throughout the session and guides the customer to escalate only in which the anomaly rate is very high. Behavioral biometrics is based on the following pillars:

1. **Behavioral Biometric Profiling:** The BioCatch solution collects and analyzes over 2000 behavioral parameters including: mouse dynamics, keystroke rhythm, navigational patterns, cognitive traits, user preferences, and many more.

2. **Invisible Challenges™:** This patented approach, refers to tests that are invoked into an online session without the user's knowledge, but that elicit subconscious responses that can be used to distinguish a fraudster from a legitimate user.

3. **Actionable Risk Score and Threat Indicators:** Real-time alerts are generated, activity is logged and visualized in the BioCatch Analyst Station.

BIOCATCH
Less Friction. Less Fraud.

www.biocatch.com info@biocatch.com @biocatch www.linkedin.com/company/biocatch

About BioCatch™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader. For more information, please visit www.biocatch.com