BioCatch

WHITEPAPER

Winning the Malware Arms Race

An Innovative and Effective Approach to Managing Automated Attacks

WHITEPAPER

Winning the Malware Arms Race

Table of Contents

Copyright

Traditional Approach to Combat Online Banking Malware

Many financial institutions are struggling with various types of malware such as Trojans that install themselves on the customer's devices and perform a variety of malicious activities. These activities range from phishing of user's credentials and credit card information, to opening backdoors within an authenticated online sessions, allowing bad actors to take over the session and perform payments. Some automated trojans don't even need humans to be present to transfer money to mule accounts, which are used to funnel the money to adversaries.

Detecting Trojans and other forms of malware can be a tricky task. Security researchers have been studying Trojan modes of operation in order to create solutions to detect and prevent Trojan attacks. Some solutions take the approach of creating a honeypot to lure Trojans to attack the protection layer itself, posing as a banking session with several "payee" and "amount" type fields embedded. This is a nice approach; however, it must be tailored to the specific modes of operation a Trojan has. The reality is that there are many types of Trojan families, and endless variants. In essence, this is an arms race, and whenever the Trojan capabilities evolve, the solutions need to be redesigned to catch up.

As soon as security researchers understand one Trojan family, a new, smarter and more sophisticated one is released. Therefore, a comprehensive solution must not be tied to what some Trojan malware does today, but what Trojans would look like when new methods and variants are created.

Other solutions take an approach that is similar to anti-virus software, requiring end users to install some software on their device. The software will look for known Trojan patterns and will need to update itself occasionally. This approach might work for enterprise users, however, in the case of consumer financial users, it is very hard to get a high percentage of users willing to download software to their personal devices, which vastly limits the effectiveness of such a solution. In addition, the approach itself is problematic because the financial institutions take responsibility of the user's computer hygiene, however, they don't want to be an anti-virus vendor.

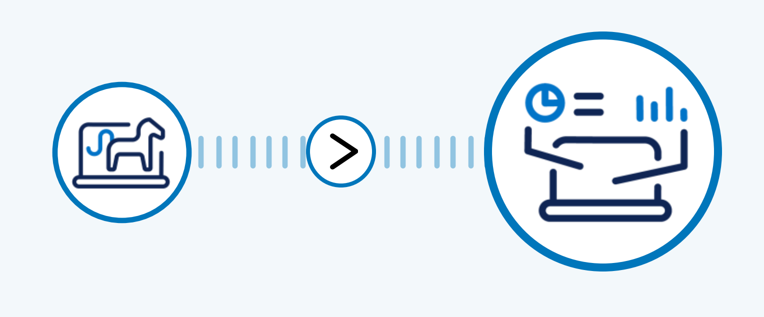
In an era where liability is mostly on the side of the financial institution, this type of approach is not good enough because you need visibility into all user activities. And still, relies much on known attacks.

Finally, these solutions cannot detect alternative types of attacks such as redirection, Remote Access Tools (RATs), TeamViewer, and Social Engineering attacks.

Did You Know?

- 25% of all cases reported as Malware, were detected as RAT (Remote Access Tool), which would likely bypass traditional malware detection. BioCatch detects these attacks due to indication of subtle RAT features in the human interactions
- Modern malware uses human-like interactions in most cases (keypress down/up, times "clicks") so if the solution simply looks for these indicators without deeper analysis, the Trojans will not be detected.
- BioCatch detects keypress events that are anomalous compared to the population and looks for movement that is similar to genuine user movement

The question becomes: do we need to keep up with this arms race? Is it realistic to stop Trojans from being installed on end user devices? What is the ultimate goal?



The goal is to stop fraud, improve end user experience and minimize operational costs, while satisfying regulatory requirements.

BioCatch takes a different approach to solve the Trojan predicament. Rather than detecting a specific Trojan variant, wouldn't it be better to detect all types of malicious actors, be it Trojans, bots or other adversaries? And what if we could not only protect against current, known, threats, but also future, unknown modes of operation? And finally, what if this detection can be truly continuous, easy to integrate with and deploy, with tools that provide visibility into the user activity?

BioCatch has reframed the problem by taking an approach that singles out any deviation from the legitimate user's behavior by applying behavioral biometric analysis to all activities. With BioCatch you can detect when it's not the user performing an activity such as a login, payment or account opening, detecting all types of attacks including bot activity, Trojans and other adversaries. In other words, the BioCatch platform makes the Trojans attack ineffective due to its' ability to detect indicators of abnormal activity for any user, leveraging innovative technology that is powered by Machine Learning and takes into account user behavior traits and cognitive thinking insights. The BioCatch platform selects a set of unique features out of 2,000+ behavioral profiling metrics to create a user profile which is based on physical factors, including left/right handedness, press-size, hand tremors, and pressure, as well as cognitive factors, such as eye-hand coordination, usage preferences, familiarity with data and device interaction patterns.

The technology analyzes user behaviors in context and session data is compared to the genuine user's profile. Finally, leveraging BioCatch's Policy Manager, analysts can create rule to trigger the desired action in real time based on the BioCatch risk score which can be used as a standalone factor or in conjunction with other indicators.

Trojan malware doesn't know which behavioral traits act as indicators and therefore cannot trick the detection mechanism, unlike the honeypot approach which is visible to Trojans.

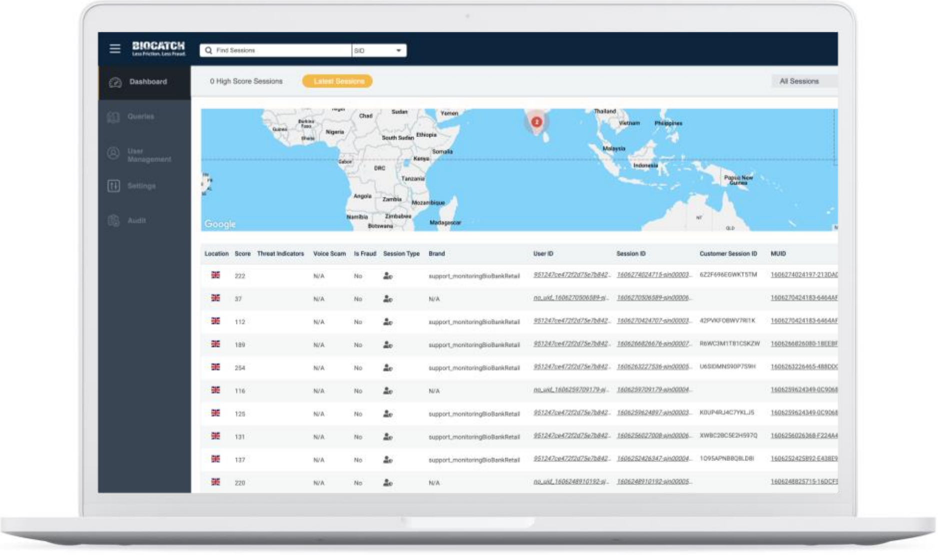
Although BioCatch platform can detect automated script attacks, Man in The Browser (MITB), social engineering malware, bots, RATs, Data Switching, the detection capabilities are much broader and provide more holistic coverage. This innovative approach can detect both known and unknown attacks and can provide more comprehensive protection than point solutions that are designed to target the Trojan problem only. In addition, using BioCatch technology, digital teams also benefit from the ability to reduce false positives (in the form of declining genuine user legitimate activity) for both account opening and other activities, by taking BioCatch scores that indicate low risk as input in the decision-making process.

WHEN THE RUBBER MEETS THE ROAD: COST AND EFFECTIVENESS

Operational considerations play an important role when selecting a solution to mitigate malware and other types of fraud.

To implement the honeypot approach:

The trojan activity indicators need to be collected and the methods of collection of data rely on highly customized JavaScript to specifically "trap" the attackers. In addition, sophisticated and heavy lifting integration points are required with multiple API calls, causing financial institutions to go through cumbersome costly deployments. Finally, the ability to analyze what really happens in the user session is cumbersome due to partial data and limited data points.



Location	Score	Threat Indicators	Voice Scam	Is Fraud	Session Type	Brand	User ID	Session ID	Customer Session ID	MUID
🇬🇧	222		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606274024715-sin00003...	6Z2F696EGWKT5TM	1606274024197-213DAC
🇬🇧	37		N/A	No	👤	N/A	no_uid_1606270506589-s|...	1606270506589-sin00006...		1606270424183-6464AF
🇬🇧	112		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606270424707-sin00003...	42PVKFOBWV7RI1K	1606270424183-6464AF
🇬🇧	189		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606266826676-sin00007...	R6WC3M1TB1CSKZW	1606266826080-18EEBF
🇬🇧	254		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606263227536-sin00005...	U6SIDMNS90P7S9H	1606263226465-488DDC
🇬🇧	116		N/A	No	👤	N/A	no_uid_1606259709179-s|...	1606259709179-sin00004...		1606259624349-0C9068
🇬🇧	125		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606259624897-sin00003...	K0UP4RJ4C7YKLJ5	1606259624349-0C9068
🇬🇧	131		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606256027008-sin00006...	XWBC2BC5E2H597Q	1606256026368-F224A4
🇬🇧	137		N/A	No	👤	support_monitoringBioBankRetail	951247ce472f2d75e7b842...	1606252426347-sin00004...	1O95APNBBQ8LD8I	1606252425892-E438E9
🇬🇧	220		N/A	No	👤	N/A	no_uid_1606248910192-s|...	1606248910192-sin00005...		1606248825715-16DCF5

Analyst Station Dashboard

Conversely, to implement BioCatch's approach,

A single API is used to collect lightweight data in multiple point and in a continuous manner, providing not only lighter and more cost-effective operational aspects, but actually improving fraud detection due to the continuous collection and hidden logic. **BioCatch's Analyst Station** tool provides step by step visibility into the online session and simplifies analysis for the fraud teams.

BioCatch

BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch

Tel Aviv | New York | Boston | London | São Paolo | Santiago | Mexico City | Melbourne | Mumbai | Singapore