Winning the RAT Race

How Banks Can Get Ahead of Remote Access Attacks and Account Takeover Fraud

BioCatch

WHITE PAPER

Executive Summary

The use of remote access tools (RAT) is hardly new and have been used by IT departments for decades to connect remotely to computers, servers and networks to diagnose and solve technical issues. Globalization combined with an extended remote workforce have made remote access a necessity for every IT department to ensure business operations.

It wasn't long before fraudsters also recognized the power of RATs. Their use in Help Desk and tech support scams are almost as old as phishing itself. Remote access capabilities in banking Trojans can be traced back to as early as 2007 when the Zeus Trojan emerged and slowly migrated to mobile malware as mobile banking grew in popularity. The technology works so well that modified RATs continue to be sold in underground forums as standalone tools or as cheap plug-ins to common banking Trojans. Legitimate remote access software, such as TeamViewer and AnyDesk, are also exploited by fraudsters.

RATs continue to be a popular attack choice for fraudsters to take over user accounts. BioCatch data indicates a RAT is present in one out of every 12 confirmed fraud cases, and nearly two-thirds of those cases originate in the mobile channel.

While the use of RATs in the perpetration of financial crime is not a new threat, they continue to pose significant challenges to fraud fighters. When a RAT is present on a user's device, the bank's systems detect a genuine device fingerprint, with no traces of proxy, code injections, or malware, and with the proper IP and geo-location. When used in a social engineering scam, the same is true as it's the legitimate user being guided by a fraudster to conduct a transaction.

As legacy fraud prevention tools have been deemed nearly ineffective in detecting account takeover fraud that leverages remote access capabilities, new approaches are required to protect customers and their accounts from this persistent threat. Behavioral biometrics provide unique insights to detect patterns that a user's account has been taken over – whether from malware or a social engineering scam.

This white paper will examine the common and emerging fraud methods that leverage RATs, where legacy fraud controls are falling short, and how behavioral biometrics can provide the additional visibility banks need to prevent these attacks.

Common and Emerging Remote Access Attacks

The use of popular software and platforms in the commission of cybercrime is not new. Fraudsters use legitimate job sites to recruit money mules and social media sites to sell and exchange stolen information. The same is true for remote access software. The common ways fraudsters use these tools for illicit purposes include:

Remote access scams. The use of legitimate remote access tools, such as TeamViewer and AnyDesk, in a variety of social engineering scams is growing. Impersonation scams and Help Desk scams are some of the more popular schemes where remote access tools are used to convince unknowing victims to provide the fraudster remote access to their device to execute a payment.

Banking Trojan. Most banking Trojans leverage remote access capabilities, and once a device is infected, tools are installed that provide remote access to the device. Most fraudsters do not have the technical capability to develop advanced Trojans and instead pay a nominal fee to other criminals on the dark web who "rent" access to botnets that distribute the malware. Once a user is infected, a fraudster is able to perpetrate on-device fraud by remotely controlling the compromised device.

Passive Remote Access: Uncovering an Emerging Mobile Attack

Fraudsters have pivoted remote access scams from the online channel to the mobile channel. BioCatch data indicates that about two out of every three fraud cases where a RAT is detected originates in the mobile channel. Consolidating the attack onto a single platform makes sense in a scam scenario where the fraudster is typically calling the victim on a smartphone device.

The challenge for fraudsters with mobile remote access scams is that not all mobile operating systems (specifically iOS) allow a user to enable remote access to their device. Therefore, if the victim is an iPhone user, the fraudster can't take direct control of the phone.

In late 2021, BioCatch customers in Asia were seeing an increase in remote access fraud cases being reported on iOS devices. After additional research, BioCatch discovered that fraudsters were getting victims to use legitimate remote access tools to share the screen (view only) of their iOS device so they could more effectively coach the victim through the scam. BioCatch dubbed this attack type as *passive remote access*. Over 80% of all fraud cases reported from an iOS device had a positive screen broadcast feature.

The use of passive remote access in impersonation scams across the globe is growing. Several U.S. banks have reported this method being used to steal money from victims via the popular P2P payment network, Zelle. One bank saw costs from impersonation scams involving passive remote access become so prohibitive that it eclipsed traditional ATO losses by nearly five times and resulted in losses of over $400,000 USD in only one month.

> Impersonation scams involving passive remote access eclipsed traditional ATO losses by nearly five times.

Behaving Like a RAT

The challenge with detecting remote access attacks is that device, IP, and geo-location checks will appear genuine as the request is coming from the legitimate user's device. In the case of financial malware, the RAT will open a browser or app from within the user's device. In the case of an impersonation scam, the fraudster does not interact directly with the banking platform and instead convinces the victim to execute the payment themselves.

Legacy-based fraud prevention measures are no longer a match on their own for fraudsters who have learned to easily spoof them. New approaches that leverage behavioral analysis to provide deeper visibility into risk across a digital session are required to detect remote access attacks.

There are several behavioral patterns that can be observed to differentiate between a human user and a RAT. Behaviors such as mouse movements, keyboard interaction device movements, and swipe patterns are used to detect active remote access in a session. These behaviors – both genuine and fraudulent – are explored in more detail below.

Mouse movements

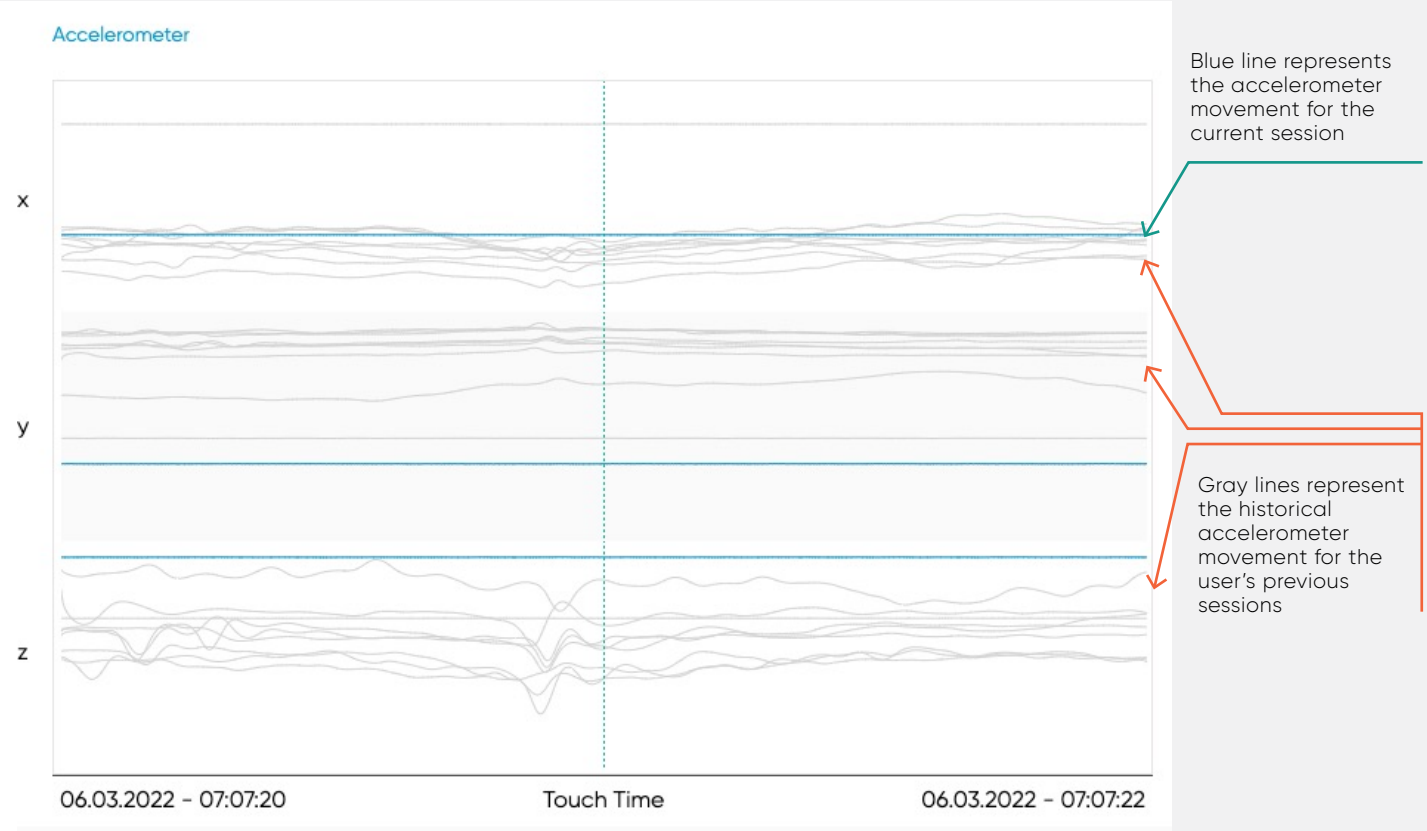
Mouse movements from a human will appear with curves, shakes and imprecise movements. Mouse interaction when a RAT is enabled will appear much differently. It is common to see near-perfect straight lines due to latency caused by the remote connection, movements originating from a single point, and activity concentrated on a specific area of the page. An example of these behaviors can be observed in the session below.

Keyboard interaction

As with mouse movements, latency on the keystrokes can be used to identify the presence of a RAT. This is done by analyzing the time between the press and release of individual keys. Repeated presence of quick intervals between these actions can indicate latency suggesting the use of remote access. BioCatch data shows that 94% of all fraud cases where a RAT is detected present this behavior.

Device movements

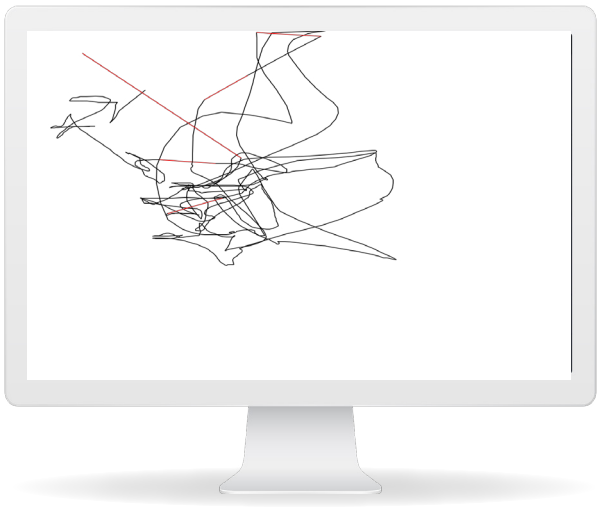
Data collected from a mobile device's accelerometer and gyroscope can provides additional data points on device movement to determine whether a RAT is being used in a session. For example, the image below shows historical accelerometer movement from the user's previous sessions represented by the gray lines. This shows natural movement of the device as a result of shaking, vibrations from pressing, device movement, and other expected human interactions. The blue lines represent the current session showing no movement in any direction indicating the device is likely flat.



Summary: current session shows no movement in any direction – ***device is likely flat***

Swipe patterns and other touch events

Swipe patterns and other touch events on a mobile device are often very different in a session where remote access is present compared to genuine user activity. For example, when a RAT is detected, swipe patterns tend to be precise with perfectly straight lines and movement often starts at the center of the screen. An example of this is illustrated below.



NORMAL

- **Human-like interaction**, with curves, shakes and imprecise movements.

RAT

- **Lots of straight lines** (marked in red) due to **latency** caused by the remote connection.
- Very few **genuine movements**, and all **concentrated** in specific areas.
- Screen size appears limited.

There are numerous other behavioral indicators that can indicate the presence of a RAT as part of an account takeover such as dead time ratio, the presence of developer tools, and time to add a new payee or submit a payment. Each indicator on its own does not imply fraud, but when combined with hundreds of other data points and compared against the norms of the genuine user population, these insights are highly accurate in detecting account takeover by remote access.

> In a remote access scam, it takes an average of 17 minutes to submit a payment - a significant time delay compared to historical genuine sessions.

Conclusion

Remote access attacks are increasing globally. While remote access capabilities are present in most banking Trojans, the use of malware in account takeover is not very common. Most fraud cases where remote access is present is perpetrated through social engineering scams. Unfortunately, seniors and the elderly are particularly vulnerable to these attacks; 85% of fraud cases involving remote access impact individuals over the age of 60, according to BioCatch data.

The use of remote access tools in account takeover also leaves the issue of liability for fraud losses up for debate. In most countries, this type of fraud is often classified as an "authorized" payment as it appears to come from the genuine user's device or may have even been initiated by a victim acting under the guidance of a fraudster. Thus, customer reimbursement might not be mandatory by regulation and open to the discretion of the bank.

Even if not designated by law, most banks take the loss from these types of attacks in order to maintain good customer relationships and negative impacts on their reputation. As the incidence of fraud from scams, including remote access scams, now outpace other types of fraud, this can become very costly to banks. Legacy controls still work, but behavioral biometrics is needed to provide continuous visibility beyond login to detect remote access attacks.

About BioCatch

BioCatch is the leader in Behavioral Biometrics, a technology that leverages machine learning to analyze an online user's physical and cognitive digital behavior to protect individuals online. BioCatch's 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.

Today, BioCatch counts over 25 of the top 100 global banks as customers who use BioCatch solutions to fight fraud, drive digital transformation and accelerate business growth. BioCatch's Client Innovation Board, an industry-led initiative including American Express, Barclays, Citi Ventures, and National Australia Bank, helps enable BioCatch to identify creative and cutting-edge ways to leverage the unique attributes of behavior for fraud prevention. With over a decade of analyzing data, more than 70 registered patents, and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems.

For more information, please visit www.biocatch.com

BioCatch

www.biocatch.com
E: info@biocatch.com
@biocatch
/company/biocatch