BANCA COMERCIALA ROMANA: LEVERAGING THREATMARK TO COMBAT RAT FRAUD

Banca Comerciala Romana (BCR), a major Erste Group operation in Central and Eastern Europe, was hit by a surge in remote access attacks—putting customer funds and the bank's reputation on the line. By fully leveraging ThreatMark's Behavioral Intelligence Platform, the bank significantly reduced the volume and impact of this threat.

KEY CHALLENGES

Remote access tool (RAT) fraud

BACKGROUND AND CHALLENGES

Remote access attacks (RAT fraud) surged by 230% globally in 2022, with Romania hit especially hard. Shared language with neighboring Moldova made it a prime target for cross-border fraud. As attacks spiked, BCR faced growing pressure to protect its customers and reputation.

"When the wave of RAT fraud hit, we were handling hundreds of cases each week. Most involved fake investment offers on social media, luring victims with promises of sky-high returns. All they had to do was grant remote access to their device—and unfortunately, many did," explains Denis Adrian Bunda, Security Manager of the Department of Secure Management and Business Continuity in BCR.

Adding to the challenge was Romania's position at the forefront of these attacks, forcing the bank's fraud prevention team to rely on their own expertise while taking swift, decisive action to protect customers.

HOW DID THE BANK OVERCOME THESE CHALLENGES?

Recognizing the need for a strong response, BCR fully integrated the ThreatMark Platform to maximize its anti-fraud capabilities—especially in detecting and preventing RAT attacks. The ThreatMark Platform provides a comprehensive set of advanced tools designed to counter these sophisticated schemes.

"Even before the wave of RAT attacks, we had integrated the ThreatMark Platform into our operations, following a recommendation from colleagues at Erste Group. At first, we used it to detect malware and flag access from high-risk countries under AML regulations. But as threats grew more sophisticated, we saw the need to unlock its full potential—and enhanced our implementation to make the most of its capabilities," says the bank's Security Manager.

To combat RAT fraud, BCR adopted a two-layered approach. First, it flags the use of remote access applications as a risk factor. Second, it leverages the ThreatMark Platform's remote screen sharing detection—if screen sharing is active, the digital banking platform is immediately locked down, disabling both login and transaction functions.

Thanks to the ThreatMark Platform, BCR successfully reduced RAT fraud. The result? Higher customer satisfaction, a stronger reputation, and lower costs tied to victim compensation and potential litigation.

> *"ThreatMark helps us understand the threats we face, how to address them, and provides us with more options for tracking security issues as they arise."*
>
> **DENIS ADRIAN BUNDA**
> Security Manager at BCR

ADDITIONAL BENEFITS OF THE THREATMARK PARTNERSHIP

The bank also gained a deeper understanding of the evolving fraud landscape. "*The ThreatMark Platform helps us understand the threats we face, how to address them, and gives us more options for tracking security issues as they arise*," adds Denis Adrian Bunda.

This insight is crucial for the bank—not just for its anti-fraud strategy, but also in preparing for upcoming European legislation, PSD3. "*With PSD3 on the horizon and increasing fraud liability for financial institutions, having detailed data on specific fraud cases will be essential. ThreatMark is perfectly positioned to provide that*," says Bunda.

For Bunda, ThreatMark's integration has become more than just a business decision. "*ThreatMark has become a passion project for me because I see its direct impact on our customers. Knowing how much they're losing makes it more than just business—it's about protecting their money. You can truly see the difference ThreatMark makes in real life*," he emphasizes.

He also values ThreatMark's customer-centric mindset and its efforts to foster industry collaboration. "*Another aspect I appreciate is the Banking Fraud Summit initiatives. They've given me valuable insights and a chance to connect with others in the anti-fraud community. Sharing information helps everyone—at the end of the day, we're all in this together.*"

WHAT'S AHEAD FOR BANCA COMERCIALA ROMANA?

In the future, BCR plans to further automate fraud detection. This includes replacing phone calls with pop-up alerts to warn users about financial malware. The bank also aims to implement the ThreatMark Platform's active phone call detection during banking sessions to catch fraud without a remote access component—such as authorized push payment scams.

"*Looking ahead, our main concern is deepfakes and fraudsters using them to access accounts. This might happen at some point; we don't know when. Nevertheless, if new fraud vectors emerge, we will utilize the ThreatMark Platform to combat them*," concludes Denis Adrian Bunda.

WHAT ARE THE BANKING FRAUD SUMMITS?

Banking Fraud Summits are exclusive events where banking professionals connect in a secure, sales-free environment to discuss emerging fraud trends, share real-world insights, and collaborate on effective prevention strategies.

KEY RESULTS

- **Reduction in RAT attacks**
- **Improved insights comprehensive fraud data**
- **Improved customer satisfaction**

LEARN MORE ABOUT THE THREATMARK PLATFORM