



BioCatch Detects New Vulnerability Making its Way to Mobile

The rise in mobile banking has made mobile payments and wallets a prime target for Remote Access Attacks

Tel-Aviv, IL – February 18, 2016 – [BioCatch](#), the global leader in Behavioral Authentication and Malware Detection, announced today that its behavioral authentication platform is the first to successfully detect Remote Access and RAT-in-the-Mobile (RitM) malware, in real time. As the adoption of mobile banking continues to grow, attacks on mobile devices are rapidly increasing, with remote access trojans (RATs) becoming the primary tool of attack for fraudsters to gain access to users' online mobile banking accounts. A recent discovery by BioCatch researchers, which exposed a vulnerability in one of the top-three online payment services in the world, demonstrates the need for the rapid adoption of RAT detection software.

The past year has seen a rise in the use of RAT access technology and financial malware such as, Dyre, Dridex, and Neverquest that gives criminals the ability to access a user's browser, login to their account and submit fraudulent transactions. This variant of remote access attack, [RAT-in-the-Browser \(RitB\)](#), has gained steady popularity among fraudsters due to low detection rates. Security teams have a difficult time detecting fraudulent activity, as sessions can continue to look normal without raising red flags. Existing fraud detection solutions are ineffective at detecting RitB attacks, since both device and network are recognized and trusted and there are no signs of automated scripts.

BioCatch has been invited to present these new findings on stage at the RSA Conference 2016, to take place from February 29-March 4 at the Moscone Center in San Francisco, CA.

Oren Kedem, VP of Product Management, will open the week with a presentation and video on Mobile RATs at the eFraud forum on February 29th. Uri Rivner, Head of Cyber Strategy, will also be giving a presentation entitled, "Dyre Times: Into the Mind of a RAT Operator," on March 3rd from 10:20-11:10 am in room 3009.

About BioCatch™

BioCatch™ is a leading provider of Behavioral Biometric, Authentication and Malware Detection solutions for mobile and web applications. Available as a cloud-based solution, BioCatch proactively collects and analyzes more than 500 cognitive parameters to generate a unique user profile. Organizations use the platform to continuously

authenticate users during their online sessions, protecting against cyber threats and fraudulent activity, such as account takeover and RAT-in-the-Browser (RitB).

The Company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-Commerce websites across North America, Latin America and Europe, monitoring over 1 billion transactions per month. For more information, please visit www.biocatch.com.

#

Media Contact:
Rachel Glaser
GKPR for BioCatch
rachel@gkpr.com
+972 54 250 9439