Global Cybersecurity Firm BioCatch Granted Breakthrough Patent for Detecting Remote Access, Among the Most Persistent Cyber Threats Today

Latest Grant Extends the Company's Intellectual Property Portfolio to 23 Granted Patents and 25 More Pending

TEL AVIV, ISRAEL AND NEW YORK, NY (July 11, 2017) – BioCatch, the global leader in Behavioral Biometrics, announced today that it has been awarded a new patent entitled*, "Device, Method, and System of Detecting Remote Access Users and Differentiating Among Users."* The U.S. patent 9690915 detects the presence of remote access tools, in order to distinguish between genuine and malicious online behaviors, is the 23rd granted patent in the BioCatch intellectual property portfolio.

Remote Access Trojans (RATs) have traditionally come in a form of malware, that enable a fraudster to take over administrative control of a device. However, through social engineering techniques (such as phone-based vishing or SMS-based smishing), these attacks increasingly also involve humans who take over control of a victim's device via common remote access tools to gain access to victim accounts, stealing credentials, and intercepting and redirecting online activity.

RATs continue to be the attack vector of choice, because of the great difficulty in detecting them. Traditional malware detection tools are not capable of recognizing most RAT attacks, because fraudsters remotely take over a bona fide user's logged-in session, after the user has appropriately and correctly authenticated themselves, with no malware involved. Similarly, because by definition they usurp a user's login and device credentials, traditional device and geolocation verification tools are not effective in recognizing RATs either.

"Given the pace of continued cyberattacks, it is clear that current cybersecurity methods are insufficient. Today's cybercriminals are extremely savvy and patient, and have developed methods that kick into gear *after* a user authenticates themselves and is logged in. In working with our global customers - who have employed prior fraud prevention solutions - it has become clear that analyzing user behavior is the only way to effectively and consistently identify next-generation threats, such as RATs, without compromising the user's online experience. Rather than detect threats based on their origins which can be masked, BioCatch monitors the user's known behavior at the destination in the online session, and protects the user by detecting threats that exhibit anomalous user behavior, whatever their provenance may be. We are very proud to have been granted a patent for this approach, which further reflects the strong differentiation and value proposition that the BioCatch solution provides," said Avi Turgeman, Co-Founder and CTO of BioCatch.

With this latest award, BioCatch's intellectual property portfolio grows to a total of 48 granted and pending patents. In addition to the one announced today, many of the BioCatch patents center around the concept of Invisible Challenges™, which inject subtle tests in an online session in order to elicit subconscious responses that can be analyzed by the BioCatch system. Reflecting this innovative approach to cybersecurity and its market leadership, BioCatch was recently awarded the prestigious 2017 Global Frost & Sullivan Award for New Product Innovation and Red Herring's Top 100 awards in Europe and North America. The company monitors over 4 billion transactions per month.

About BioCatch
BioCatch is a cybersecurity company that delivers behavioral biometrics analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. 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.

###