BIOCATCH
Less Friction · Less Fraud

BioCatch's Fraud Detection Platform is First Solution Capable of Detecting Dyre and RAT-in-the-Browser (RitB) Malware in Real Time

In a new campaign, BioCatch detects Dyre and Dridex with Behavioral Biometrics

Tel-Aviv, IS – October 20, 2015 -- BioCatch, the global leader in Behavioral Authentication and Malware Detection, announced today that its fraud detection platform is the first that can successfully detect RAT-in-the-Browser (RitB) malware such as Dyre and Dridex in real time. While identity theft is a well document security threat in online banking, the use of Remote Access Trojans, or "RATs," such as Dyre and Dridex, has become the primary tool of attack for fraudsters to gain access to users' online banking accounts.

Nowadays all serious malware kits, including Zeus, Dyre, Neverquest and Dridex, feature RAT capabilities, demonstrating the popularity of RitBs among fraudsters. When fraudsters deploy RAT-in-the-Browser (or RitBs), banks have a more difficult time suspecting fraudulent activity, as a session can continue to look perfectly normal without raising red flags. For example, the device is trusted, there is a known IP Address, and there are no signs of automated scripts.

BioCatch's patented technology analysis hundreds of user interaction parameters enabling the creation of a specific model that separates between users who directly control their device and users that remotely control the device over the Internet. Moreover, each Trojan operator has its unique traces left in the fraudulent session, while using the RitB capabilities.

Additionally, BioCatch researchers have identified a new variant of RitB fraud attacks on online banking – Social RitB, with a unique modus operandi. You can read about Social RitB here.

"BioCatch consistently works to stay ahead of the game in combating fraud," said Oren Kedem, VP Products of BioCatch. "With each attempted malware attack caught by BioCatch, we are able to derive valuable information that helps us identify and defend against new threats, providing the most sophisticated up-to-date protection for our customers."

BioCatch "RAT Wars" campaign is available here.

###

About BioCatch

BioCatch is a leading provider of Behavioral 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. Banks and eCommerce websites and mobile apps use BioCatch to significantly reduce friction associated with risky transactions and protect users against cyber threats, such as Account Takeovers, Man-in-the-Browser (MitB) Malware and RAT-in-the-Browser (RitB) attacks. Additionally, BioCatch provides an enterprise tool that improves the employee authentication experience while protecting access to critical IT assets. The Company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks, eCommerce sites and enterprises across North America, Latin America and Europe. For more information, please visit www.biocatch.com.