BIOCATCH
Less Friction. Less Fraud.

Detecting Remote Access (RAT) Attacks on Online Banking Sites

A BioCatch White Paper

www.biocatch.com

Document Overview

Remote Access Tools (RATs) allow an attacker to take control over a desktop and use it remotely, opening any application and operating the PC as if the fraudster was sitting next to it. RATs have been used by nation states and hacktivists for many years, but only recently[1][2] have we seen this remote access attack vector migrate to online banking fraud, where the main use is to neutralize all device-related defenses such as device recognition, IP geo-location, and proxy detection. Existing fraud detection solutions that attempt to identify unknown or infected devices are not designed to spot RATs, leaving banks vulnerable to remote access attacks.

Instead of examining device data, BioCatch takes a different approach. It monitors and analyzes user behavior. BioCatch's Cognitive Behavioral Analysis tracks interaction traces, and injects subtle, invisible challenges to capture the user's response.

This technology enables BioCatch to instantly detect abnormal user behavior consistent with the use of RAT, MITB and other threats, as well as biometrically authenticate users who have been profiled. The Java Script-based detection is extremely accurate, real-time, and focused only on the computers where a live attack is observed – making it much more actionable than malware detection tools that report thousands of infected PCs, only a fraction of which will actually experience fraud.

What are RATs?

RATs or Remote Access Tools started as harmless software used by a remote helpdesk or IT administrators to take over a user PC in order to understand what issues they were experiencing and to offer immediate assistance. Cybercriminals quickly recognized the effectiveness of RATs and began leveraging these capabilities. State-sponsored attackers and hacktivists often use modified RATs, such as PoisonIvy, for controlling employee PCs connected to sensitive networks. Recently, the RAT capability has been adopted by financial cybercriminals.

---

[1] http://nakedsecurity.sophos.com/2013/03/26/slovenians-arrested-2-5m-banking-fraud/

[2] http://www.infosecurity-magazine.com/view/33911/rat-drains-california-escrow-firm-out-of- business/

Today re- purposed RATs are sold in the cyber underground as standalone malware (e.g. DarkComet, ProRat) or as cheap plug-ins to common financial trojans such as Zeus, SpyEye and Citadel. Based on remote access protocols like VNC or RDP, these RATs offer an easy way to remotely control a user PC.

Cybercriminals use RATs to circumvent existing online banking fraud prevention solutions such as device recognition, device malware infection detection, proxy detection, and IP geo- location. RAT lets the attackers remotely control the victim's device, providing them access to any application.

RATs fool device recognition (often the basis of Adaptive Authentication solutions) since the device originating the login and money transfer is the real user device. The bank will see a 100% genuine user device fingerprint, no traces of proxy, no JavaScript code injections, no automated code, no malware infection, and of course, same IP and geo-location. Device certificates will also automatically work. This is as close as it comes to a full 'cloaking device'.

RATs are now part of every main Trojan kit, or sold separately for up to $400. For example, Citadel offers a RAT add-on based on VNC (see images below, source: RSA Cyber Labs). It allows full remote control over PCs infected with Citadel.

Figure 1: A screen capture of the Citadel (financial Trojan) VNC add-on console

BIOCATCH
Less Friction. Less Fraud.

How Do Fraudsters Perpetrate RAT Online Banking Fraud?

As with other types of malware, RAT infections are typically a product of vulnerabilities in operating systems, browsers and popular software such as Flash, Acrobat PDF and Java. Most infections nowadays use a method called Drive by Download where fraudsters randomly hack into a large number of websites and direct all user traffic to an infection point running a commercially available exploit pack. Once accessed, the malicious code scans for browser vulnerabilities and infects the device with a Trojan dropper making it part of a bot network. Later, bot devices are sold in the underground market to cybercriminals that install their weapon of choice – RATs – to later perform the remote access attack. Some RAT infections are more targeted; either using a specific "waterhole", a site or web service where the targets are likely to browse, or sending spear-phishing emails with a link leading to the infected site.

Once installed, the RAT can be used as long as the user is connected to the Internet and without the user suspecting anything. Fraudsters may also leverage Man-in-the-Browser (MitB) technology and remote access as part of the single attack flow. In a combined MitB/RAT attack, the malware informs the attacker that the user just logged into the online banking site and provides the login credentials. The attacker suspends the user's session, opens an invisible browser on the victim's device, and logs into the bank. They proceed with a money transfer and should the bank ask for any out-of-band or two-factor authentication, they use the suspended session with the user to ask them to go through the authentication process and provide the resulting one-time code, which the attacker then feeds to the live session completing the fraud. The use of RAT makes the attack completely invisible to any device recognition, IP geo location, or proxy detection tool.
There are more simple ways to gain remote access to a user device, using social engineering. Some fraudsters simply call users, impersonating as "IT Admins" or "Microsoft Representatives", and ask to get remote access for "security reasons".

In a recent remote access attack[3], the fraudster went so far as to ask the victim to turn off the monitor while they performed the task.

BIOCATCH
Less Friction. Less Fraud.

How does BioCatch detect a RAT?

BioCatch monitors how users interact with online banking applications and introduces small, subtle, invisible challenges to track the users' responses. Using machine-learning techniques, BioCatch models different types of genuine and malicious behavior. During a user's online banking session, the actual monitored behavior is compared with modeled behavior to detect fraudulent activity.

Users operating remotely on an online banking site respond differently than those working locally on their PC. In RAT sessions, interaction data travels over the web (typically through a proxy server) and triggers a screen refresh that travels back to the remote PC. Due to web network latency, BioCatch will observe sluggish responses, overshoots, and delayed corrections that are very characteristic of remote access. Simply put, remote responses to the BioCatch invisible challenges are distinctively different than responses in local sessions.

Easy Integration

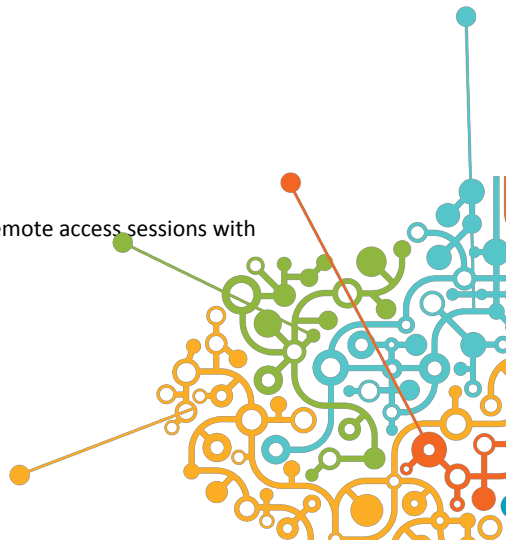
BioCatch is a cloud-based service that collects behavioral data via a small JavaScript snippet embedded into the onlinebaking site. Once remoteaccess is detected an alert is sent to the bank to take mitigating action. No learning period is required for RAT detection.

RAT Detection with BioCatch

Detects 100% of Malicious RAT attacks – such as DarkComet, ProRat, VNC and RDP Add-ons to Zeus and Citadel

Catches RAT in the act: unlike solutions that detect malware infections, a majority of which are NOT targeting the online banking site. BioCatch will alert in real time as the remote access occurs, allowing you to handle the few real fraud attempts instead of thousands of "genuine" sessions.

5 BioCatch has tested multiple RAT types and configurations and found to detect all remote access sessions with no false positives (never identified a local session as remote).



Lightning-fast integration: embedding a small JavaScript on the online banking web site.

Not just RATs: BioCatch can detect "in the act" other forms of advanced cyber threats including automated MITB and manual MITB (also known as Human in the Middle). BioCatch also offers behavioral biometric authentication for online and mobile applications.

About BioCatch

BioCatch is a leading provider of behavioral authentication and threat detection solutions for mobile and Web applications. Available as a cloud-based solution, BioCatch proactively collects and analyzes more than 400 bio-behavioral, cognitive and physiological 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 Remote Access (RAT) 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.