ThreatMark

Our Fraud Detection Approach

ThreatMark

Our Fraud Detection Approach

Nowadays, neither traditional approach of rule-based transaction anomaly detection solution, nor IP and browser-based user identification techniques are sufficient. These strategies are ineffective against today's attackers, using cunning identity-theft and social engineering-based techniques to bypass all protective measures. Traditional solutions don't have enough relevant nor detailed data to be effective in detecting modern attacks. Moreover, the lack of detailed information and context results in a high number of false positive detections that need to undergo costly manual reviews.

To decrease the number of false positives, our Anti Fraud Solution (AFS) focuses on context. We developed a method**,** which considers all possible data – combining information about **threats** (threat detection), **transactions** (transaction risk analysis) and **behavior** (behavior profiling) **-** generating reliable user identity and **preventing fraud** at the same time.

Threat Detection

AFS observes and tests all data displayed by a browser as well as those hidden in the application code. The differences are tested automatically to see if they match known malware signatures and positive detections are reported. In case of unknown deviations, they are sent to our Security Operation Center (SOC) to further scrutiny. Our solution also detects insecure configurations and any non-human like behavior, which can be an early sign of financial malware trying to provide an automated transaction. Detection of phishing attacks is another feature that AFS has. Utilizing a sophisticated method of detection, our solution can reveal any attempts mimicking legitimate banking page for phishing purposes.

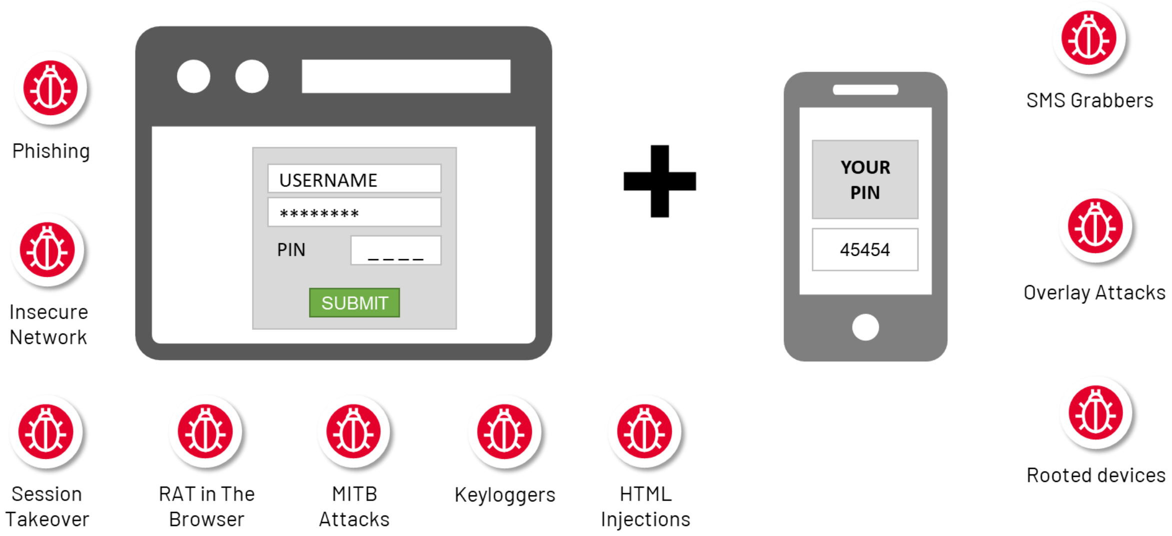

Figure 1 – Spectrum of cyber threats

Transaction Risk Analysis

User's spending behavior is tracked and analyzed, and it is compared to typical user behavior. Considered parameters include amount, frequency, time and other user entered values. All transactions are evaluated against various models. Every model includes a group of rules corresponding to a transaction type, the channel used, etc. AFS detection capabilities are not purely rule-based but are rather based on **advanced Machine Learning that canadapt to new fraudulent scenarios not covered by any rules.**

Behavioral Profiling

Everyone's behavior while interacting within the online application is unique. How one navigates throughout the application, how fast one clicks/taps/swipes or how one uses their keyboard, mouse or tap screen and other biometric markers. These markers are then augmented with user-specific information, such as location, device, time and date, navigation patterns and transaction behavior. Combined, these data deliver the best context-value resulting in decreased number of falsely rejected users and transactions while mitigating risk with a whole new level of precision.

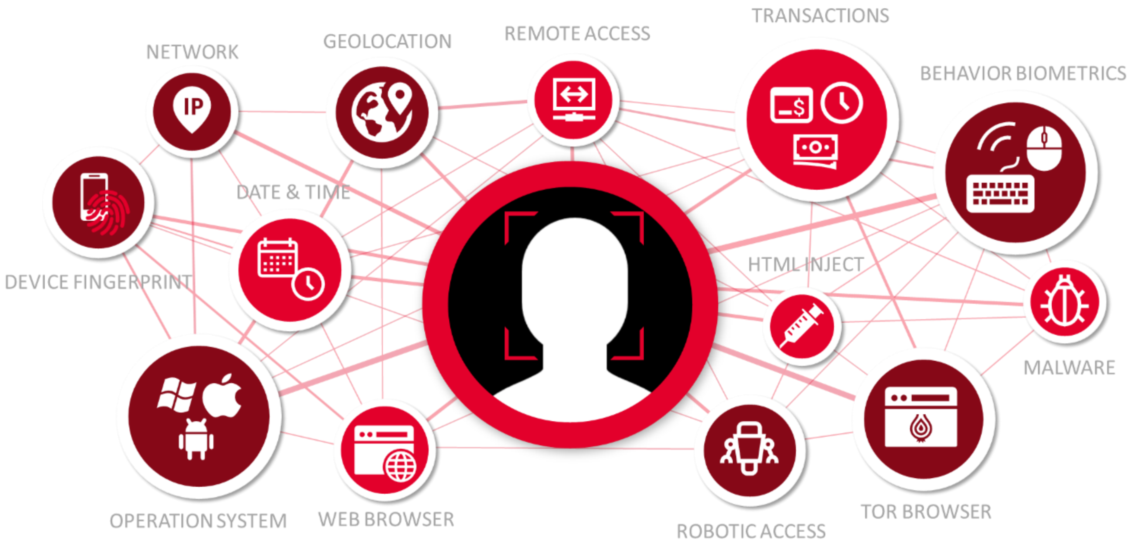

Figure 2 – ThreatMark's Trusted User Identity