REPORT REPRINT

Cleafy targets website transaction fraud with web behavior analytics

ERIC OGREN

16 AUG 2017

The company, having developed its anti-fraud capability with the help of major Italian banks, has developed additional web behavior analytics capabilities in version 4.0 for web and mobile transactions.

Even an entry-level fraudster knows how to create malware injecting code into web pages to grab user credentials (account takeover) and to arm bots to impersonate valid users to extract money from online businesses. Even some advanced attack techniques like man-in-the-browser (MITB), man-in-the-middle (MITM), RAT-in-browser (remote access tool) and mobile app overlay are not effectively detected by web application firewalls. This places financial enterprises in a delicate situation – users resist having to install apps or anything else that degrades the experience, yet the business is responsible for ensuring the integrity of online transactions and indemnifying users against fraud. More and more enterprises are turning to vendors like Cleafy with real-time analytic approaches to protect their web and mobile services from advanced attacks for fraudulent purposes.

THE 451 TAKE

The challenge for application owners in fighting fraud is to avoid inhibiting user experiences and creating IT headaches with website changes for the sake of security. Cleafy attacks this problem by delivering a server-side engine that analyzes the application traffic in real time to detect violations of application integrity. Cleafy also documents detected threats by automatically extracting and classifying code fragments (web injects) from the attack. Security, anti-fraud and customer support teams can all work from a common view of the attack in coordinating remediation actions that are best for the business. In version 4.0, the product is extended to mobile applications for both native and hybrid apps running on Android and iOS devices, in order to detect mobile-specific threats such as app repackaging, SMS grabbing or app overlay. Cleafy presents a logical approach to securing online transactions as fraud rates, particularly those driven by automated software bots and based on advanced techniques, relentlessly climb.

CONTEXT

Cleafy is headquartered in Milan, Italy. The company started in 2014, and has since grown to just under 20 employees, with business offices in Italy and the US. The company is in the midst of expanding its operations to other EMEA markets, as well as US and APAC regions.

PRODUCTS

Cleafy Detect is designed to integrate into the application back-end without disrupting the business process. Cleafy integrates with application delivery controllers from F5 Networks BIG-IP and Citrix NetScaler to inspect the traffic between web application servers (or mobile API gateways) and the endpoints, without delaying the traffic. Cleafy integration does not require any change to the application code, the back-end infrastructure or the user endpoints.

The significant differentiator for Cleafy Detect is the ability to deterministically identify threats, since its approach is not based on signature and pattern matching, and to present evidence of an attack by extracting modified code fragments. When detecting discrepancies between generated and rendered DOM and XHR content, Cleafy increases the risk score of the session. Cleafy uses the logic involved in compiling a risk score to classify the attack and then extract relevant sections of code to help security and anti-fraud experts better understand the attack. It is this capability to group or cluster threats into families that provides insight into attack campaigns and trends that helps identify optimal remediation tactics.

Cleafy Detect comes with a comprehensive API, which can be leveraged to connect with anti-fraud consoles and SIEM systems. The API can provide access to risk scores and evidence (malicious apps and web injects) in real time to support graduated responses for cases where blocking or dropping the connection is too severe a response – typical actions include invoking step-up authentication to impede bots. In general, the API allows customers to implement remediation actions that are customized to their business requirements, which comes in handy for online transactions.

The business side is important when talking about anti-fraud. In addition to the API capability enabling technical integration, Cleafy's management console also includes features that allow security, anti-fraud and customer support teams to have full visibility into any event and session, endpoint characteristics, identified threat and attack evidence.

Cleafy says it also provides threat protection capabilities that enhance safe transactions from infected endpoints. Cleafy Protect leverages patented Real-time Dynamic Encryption technology that can be deployed when Cleafy detects an infected device accessing the online service. The idea is to deploy a 'secure box' that thwarts MITB and MITM attack when Cleafy Detect determines the user's device can no longer be trusted.

COMPETITION

The WBA market features larger, better-funded competitors. WBA is an emerging market as enterprises lament the limitations of web application firewalls. WBA, without the benefit of compliance mandates, is being adopted by enterprises protecting websites against bot-driven fraud, account takeover, data scraping and denial of service. It is a market where deal sizes above $500,000 are not uncommon.

There are WBA competitors that focus on identifying and thwarting automated bots attempting to perform unauthorized transactions on targeted websites. These vendors use all the behavior of the device and user they can find, such as device fingerprinting, browser configuration, mouse movement and typing patterns, to separate human users from bot users. Akamai, CloudFlare, Distil Networks, F5, PerimeterX, Shape Security, Unbotify and White Ops are all active WBA competitors. Most capture information from attacks to enhance detection algorithms in their products and services, and most include some sort of machine learning to detect inconsistent behavior indicative of an attack impersonating an authorized user or device.

SWOT ANALYSIS

STRENGTHS

Cleafy Detect collects evidence of fraud activity and presents the information to security, anti-fraud and customer support teams. There is a sensitivity to the business needs that comes from working closely with early customers.

WEAKNESSES

Cleafy Detect keys on discontinuities between actual and expected results in the HTML DOM, but could be stronger in recognizing and removing bot traffic.

OPPORTUNITIES

Cleafy is impressive in the way it has developed its Detect product with major Italian banks. The company has an opportunity to reduce fraud rates through website transactions for US financial markets.

THREATS

Switching costs for WBA are relatively low. All it takes is to remove Cleafy Detect from the ADC and direct traffic through a competitive product. Cleafy will have to prove itself every day against larger competitors.