INSIGHT

Check Point Adds Analytics, Mobile Threat Prevention with Lacoon Acquisition

Robert Westervelt
Stacy K. Crook
Charles J. Kolodgy

IDC OPINION

Check Point Software Technologies' acquisition of Lacoon Mobile Security bolsters Check Point's enterprise mobile security portfolio by adding a unique approach to mobile threat prevention. In addition:

- The acquisition of Lacoon allows Check Point to round out its mobile security strategy by adding mobile threat prevention to its existing data and network protection capabilities and its mobile suite, named Check Point Capsule.
- Lacoon's threat intelligence data and risk analysis engine may add contextual data that could be used across Check Point's mobile security product portfolio.
- Lacoon provides risk scores for mobile applications and suspicious threats. Its threat emulation sandbox for mobile applications adds to Check Point's suspicious file analysis emulation sandbox technologies, providing behavioral analysis of suspicious mobile applications.

IN THIS INSIGHT

This IDC Insight covers the recent acquisition of Lacoon Mobile Security by Check Point Software Technologies. Check Point announced its intention to acquire Lacoon, a mobile security start-up based in Tel Aviv, Israel, that has gained attention for its strong research team and the ability to spot zero-day threats associated with targeted attack and nation-state espionage activity on mobile devices. Lacoon management is being brought into Check Point, and Lacoon's core technologies will be integrated into the Check Point mobile security offerings. This Insight examines Check Point's acquisition and provides analysis of the potential for further M&A activity in the mobile security market.

SITUATION OVERVIEW

Check Point Software Technologies is adding endpoint visibility and security analytics to its mobility portfolio with the announcement this month of its acquisition of Lacoon Mobile Security. The move further transforms Check Point's mobile approach from one of data protection and network security to a more comprehensive strategy that also includes threat prevention.

Based in Tel Aviv, Israel, Lacoon takes a three-pronged approach to mobile security. Through an agent deployed on the mobile device, it sends metadata about the device (OS), applications, and networks to Lacoon's cloud-based Behavioral Risk Engine (BRE) to detect and mitigate mobile threats.

April 2015, IDC #255625

Since the BRE performs its analysis in the cloud, Lacoon claims it can eliminate unnecessary battery drain and performance issues on the device.

According to Check Point, Lacoon's BRE uses a number of patent-pending, proprietary techniques to identify vulnerabilities and threats. The BRE's behavioral app analysis identifies suspicious patterns and behaviors over time by sandboxing apps in an emulator to understand exactly how they interact with specific device types and the risks these interactions may pose. With advanced static code analysis, the BRE detects on-device and network event anomalies by identifying patterns that might otherwise evade detection, such as malicious command and control behaviors or data leakage by unknown malware. The BRE's real-time risk assessment also identifies changes in configurations or device states that may indicate exploitation of vulnerabilities, including phony certificates, unusual configuration profiles, and network setting changes. To prevent data theft, the BRE can then quarantine the device by blocking all network connections until the threat has been removed.

By acquiring Lacoon, Check Point adds a strong security engineering and research team dedicated to mobile security. Check Point also gains Lacoon's threat intelligence data and risk analysis engine, which can be fed into Check Point's current mobility offerings. Lacoon's technology includes a threat emulation sandbox to analyze the behavior of mobile applications and calculate a risk score based on characteristics and behavior.

Lacoon has been especially strong in identifying techniques that would be used in targeted attacks conducted in nation-state cyberespionage or corporate espionage activity. Researchers previously demonstrated a way to remotely steal login credentials and other sensitive data by using a malicious configuration profile that could be delivered through a compromised WiFi hotspot. They also developed a proof-of-concept man-in-the-middle attack to hijack and screen scrape data from a VDI session.

IDC expects the Lacoon acquisition to be quickly integrated into Check Point's mobile security products. The offering will become a core component of Capsule, Check Point's flagship mobile security suite. Today, Capsule includes the ability to encrypt documents, a containerized workspace environment, and protection for network traffic. In addition, the capabilities will be included in Capsule Cloud, a lightweight SaaS-based version of Capsule offered in small and medium-sized businesses and enterprise versions. Capsule Cloud tunnels mobile devices and laptops through its inspection service to conduct URL inspection, antivirus, antibot, threat emulation, intrusion prevention, and HTTPS inspection capabilities. Capsule Cloud was only introduced six months ago, but Check Point executives tell IDC it is experiencing significant growth, with about 10% of the customer base currently subscribing to the service. Capsule Cloud supports Windows clients and Android and iOS devices. Check Point also offers a Mobile Access Blade for remote access through an SSL VPN.

Lacoon has had a close partnership with Check Point on collaborative research. Lacoon used Check Point's global infrastructure to analyze the amount of mobile remote access trojans that exist in corporate environments. Lacoon recently expanded its platform from detecting advanced threats to include other inspecting file attachments and enable IT teams to remotely investigate threats and integrate with some mobile device management suites.

FUTURE OUTLOOK

IDC expects to see more M&A activity in the mobile security market as vendors seek to provide customers with better visibility over mobile activity and control oversensitive data.

In this market, there are three groupings of vendors that are likely acquirers of mobile security technology:

- Large security companies and enterprise mobility management (EMM) vendors are some of the most obvious acquirers of mobile security technology because of the increasing convergence between the EMM and mobile security markets. In fact, the majority of large security vendors now offer some level of EMM functionality. While all leading EMM products provide policy management for devices, applications, and data, we believe the ability to offer innovative security techniques within the areas of data protection, identity, and threat prevention will provide an important basis for differentiation in the market.
- Mobile device and OS providers such as Apple, Microsoft, Google, and BlackBerry have acquired and will continue to make acquisitions in this space. These technology purchases range from biometrics to encrypted voice communications to the ability to create a virtual barrier between work and personal information on the device, among others.
- Independent software/SaaS vendors are also making smaller, point acquisitions to bolster security. In March, enterprise cloud storage service Box acquired Subspace, a small mobile security start-up that offered a containerized Web browser to secure corporate data in transit and on the endpoint. Meanwhile, salesforce.com announced on April 1 its intention to acquire Toopher, a multifactor authentication service that uses a device's location as the second factor when a user logs into an application or a service.

Lacoon is one of a number of vendors that are addressing the changing nature of applications from merely on-premise deployments into the cloud and the potential weaknesses that they may introduce to mobile devices. IDC also anticipates phishing attacks designed to steal log-in credentials will increase steadily on mobile devices. Having endpoint visibility is essential, but IDC predicts that the network security will play an increasingly important role in reducing the attack surface of mobile devices by performing access control, traffic encryption, and traffic inspection.

Lacoon also has a sales office in San Francisco, the heart of several mobile security start-ups attempting to capture the enterprise market with alternative approaches. These start-ups' unique approaches and strong executive teams make them possible acquisition targets. One notable start-up, Bluebox, is headed by Caleb Sima, a noted software security expert who was founder and CTO of Web application security testing firm SPI Dynamics (acquired by HP) and most recently had headed Armorize Technologies (acquired by Proofpoint). Bluebox focuses on separating corporate and personal data on mobile devices. Its technology creates self-defending applications, dynamically wrapping them to give organizations the ability to create and enforce policies. Lookout Inc., also based in San Francisco, got its start on the consumer side, establishing strong market share adoption of more than 60 million users from which it is pulling in threat data. The company announced its expansion plans in November 2014 to bring to market an enterprise-grade mobile security platform. It also created Lookout Federal Systems to sell into government agencies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com
