Zimperium

Machine Learning-Based Mobile Security

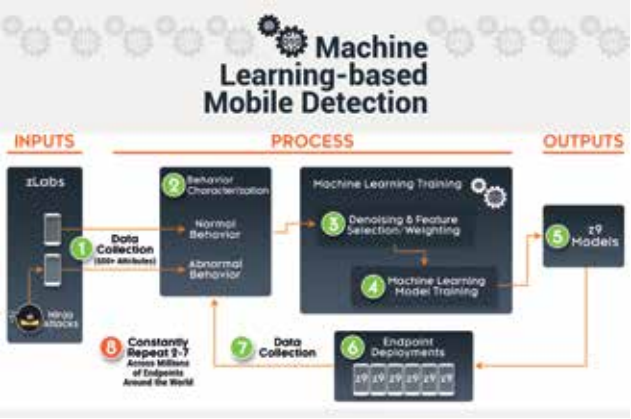
Organizations often lack the visibility needed to understand where the main vulnerabilities and risks lie in their mobile infrastructure, leaving them blind and unable to defend against cyber attacks. As a global leader in enterprise mobile security, Zimperium addresses these issues by offering comprehensive and continuous visibility into advanced mobile threats to provide protection against network, device and application-based threats by leveraging machine learning.

Initially, Zimperium used machine learning to detect network threats such as man-in-the-middle attacks. As the company evolved, z9—Zimperium's patented machine learning-based engine—was designed to detect host or device threats such as system or kernel vulnerabilities that allow remote takeover and control. Additionally, z9 uses static analysis and creates behavioral patterns of applications to detect anomalies in real time. Esteban Pellegrino, Chief Scientist of Zimperium, states, "z9 allowed us to mitigate every zero-day exploit to date without requiring any updates."

Most security solutions block malicious applications and other attacks by creating signatures of previously discovered threats, which is ineffective against unknown malware and zero-day threats. Moreover, the "containerization" approach followed by many security solutions—which effectively involves sandboxing to mitigate possible threats—is complex to roll-out, disruptive for the end user and can be circumvented.

On the other hand, Zimperium provides continuous on-device monitoring and analysis to detect mobile cyber attacks in real time with its Mobile Threat Defense platform. z9's machine-learning models were developed and refined through years of threat intelligence research; z9 accurately identifies malicious attacks regardless of the entry point. Zimperium runs locally on devices, is platform agnostic and does not require signatures, cloud-based sandboxes or even an internet connection, further ensuring users are always protected. "Our on-device architecture enables mobile devices to become powerful sensors that alert users and management about enterprise threats from endpoints across your organization," adds Pellegrino.

Zimperium's solutions, collectively called the Zimperium 5.0, include four key offerings designed to meet the needs of security-savvy enterprises. zIPS, a standalone on-device application, leverages machine learning-based detection to



provide persistent protection for mobile devices and data in a manner analogous to next-generation antivirus on traditional endpoints. The zIAP software development kit (SDK) quickly embeds z9 into any mobile app. Zimperium's reporting and management console, zConsole, features threat forensics, policy administration and integrates with EMM and SIEM solutions. To further enforce mobile security, z3A provides detailed privacy and security risk analytics for every app across company employees and their devices.

In 2016, Zimperium discovered Stagefright, a critical exploit in the Android operating system. After Stagefright, the company formed the Zimperium Handset Alliance, an association of different parties interested in exchanging information and receiving timely updates on Android's security-related issues. "We also released a Stagefright Detector tool to help users identify if they were vulnerable," states Pellegrino. Zimperium users were also protected from Quadroot vulnerabilities since the solution continuously monitors for any anomalous behavior using z9 to detect attacks from local escalation privileges and malicious applications. z9 also detected a malicious sample with a suspicious package in the Google Play Store, which was disguised as the official BBC app, in an attempt to scam users into downloading it.

Moving forward, Zimperium is expanding its mobile threat detection to cover IoT and other connected devices. "We want to continue our goal of addressing potential issues quickly and efficiently to help combat today's advanced mobile threats without compromising user experience," concludes Pellegrino. CA