Mobile App Profiler^{TM} Technology

Mobile Apps – the new threat frontier

Mobile apps used in enterprise environments represent a fundamental shift in endpoint computing. Enterprises are used to being in control of their endpoints and the applications running on them. Applications used to be written by well-known vendors like Oracle, SAP, Microsoft and Siebel. The browser used to be the single outlet to the Internet from a user's computer. Deploying web security provided the enterprise protection from Internet-based threats and helped meet compliance needs.

With mobile apps, there has been a fundamental shift in the ownership model of applications. Few mobile apps are written by the traditional application owners – like SAP, Microsoft or Oracle. Employees can download apps from authorized as well as 3rd party/ underground market places. When employees use their personal smartphones and tablets on the corporate network, personal apps on the devices piggyback itself onto the corporate network. This bypasses traditional on-premise security mechanisms deployed as appliances or PC software by allowing unauthorized and potentially malicious apps onto the corporate network.

Identifying and Profiling Mobile Apps using Mobile App Profiler

Identifying mobile apps cannot be done based on just a URL or two being accessed over the network. Mobile apps rarely communicate with just 1 or 2 domain. In fact, traffic patterns from most mobile apps like Facebook and LinkedIn look entirely different from that generated by a browser connecting to the same applications. Mobile app identification requires redesigned and improved technology over traditional app identification mechanisms that might work on PCs and Macs.

Zscaler Mobile App Profiler is a technology designed from the ground up to identify mobile apps and the originating mobile platform based on the network traffic patterns they generate. Mobile App Profiler's "fingerprinting" technique transcends URL-based detection, identifying and classifying apps based on persistent visibility to the traffic generated by the app. It also provides information about the associated mobile platforms, such as Apple iOS, Google Android or Windows 8 Pro.

Protecting the mobile user with Mobile App Profiler

This technology enables Zscaler to apply its expertise in web security to mobile app traffic. For instance, based on the mobile traffic pattern, Zscaler can identify mobile apps making calls to malicious URLs like phishing websites or Command-and-control servers on the Internet. It also identifies apps leaking information to remote servers that may be sensitive to the user or device, such as device identifiers, user's calendar or contacts, or other personally identifiable information (PII).

Zscaler's Data Loss Prevention (DLP) solution protects customers from loss of information subject to compliance requirements such as PCI, HIPAA or SOX, as well as information patterns deemed confidential by the administrator. When combined with Mobile App Profiler, customers can detect DLP in mobile apps, identifying mobile applications that may jeopardize their compliance posture or confidential data.