ZIMPERIUM®
MOBILE THREAT DEFENSE

Zimperium z3A

Machine learning-based mobile app
risk and threat analysis for the enterprise

ZIMPERIUM Z3A

Enterprises are growing increasingly aware of the risks posed by mobile devices and apps. A 2019 survey[1] found that 83 percent of respondents said their companies were at risk from mobile threats, with 29 percent rating it a serious risk. Employee-owned mobile devices specifically were cited as the biggest enterprise security concern, followed by company-owned devices—ahead of even cloud and IoT concerns.

Enterprises have therefore begun implementing methods to mitigate that risk, but the adoption curve is steep, and even if an enterprise is taking effective steps to manage mobile device risk, the mobile apps on those devices can pose an entirely different attack vector. The risks can be substantial.

Here's why. Enterprises often have limited visibility into the mobile apps that their workforce is downloading. Many rely on antivirus solutions for app-focused security, potentially without realizing that some two-thirds of available mobile antivirus solutions have been demonstrated to be ineffective at best and fraudulent at worst[2].

Moreover, antimalware solutions do not offer protection against cases where legitimate and malware-free apps nevertheless include code or behave in ways that inadvertently create risk. Also known as riskware[3], such apps can expose enterprises to data leakage and other threats.

In practical terms, this means that even if you achieve some insight into the mobile apps that users are bringing into the enterprise via their devices, you still need a method of assessing the risks and threats those apps pose to the security and privacy of the workforce and to the business. Only with that knowledge can you set security policies to reduce that risk.

THE NUMBER OF MOBILE THREATS IS INCREASING

Mobile employees will account for 48% of the workforce by 2020[4], and over 60% of devices in an enterprise are now mobile. The combination of corporate-owned and BYOD devices in the enterprise will provide unprecedented opportunity for cybercriminals.

- At the end of 2018, total app downloads for the year passed **205 Billion**[5]
- As of February 2019, there were **2.2 Million**[6] apps in the Apple App Store, and as of Apr 2019 there were **2.6 Million**[7] apps on Google Play
- In the first quarter of 2019, mobile consumers spent an estimated **$19.5 billion**[8] globally on the App Store and Google Play (and this doesn't account for third party app stores)
- In Q1 2019, first-time app installs passed **28 billion**[9], with Google Play accounting for 3 out of every 4

Understanding and managing the risk that mobile apps pose to the enterprise has never been more important.

SECURITY AND PRIVACY RISK IDENTIFICATION WITH UNPRECEDENTED GRANULARITY

Zimperium z3A continually evaluates the risks posed by mobile apps that employees have downloaded to their devices. z3A shows you which apps are safe or risky. For all apps, z3A provides deep intelligence about app behavior with unprecedented granularity, including content (the app code itself), intent (the app's behavior), and context (the domains, certificates, shared code, network communications, and other data). z3A also provides privacy and security ratings, making it easy for you to set effective security policies to reduce an app's risk.

AUTOMATED, ONGOING DETECTION OF SECURITY AND PRIVACY RISKS IN INSTALLED APPS

z3A maintains continual awareness of the apps on mobile devices throughout your enterprise via a parallel processing engine that continuously collects and correlates data from multiple sources. z3A performs multivariate tests and validations to identify mobile app security and privacy risks before they become threats. The z3A engine constantly updates for new threats and the latest app risk behaviors.

The automation and analysis allows you to generate app security and privacy risk summary reports. The reports include app risk scoring, giving apps a Thumbs Up or Down, and details the app behaviors and context so that enterprise security teams can take action. Detailed technical journals in JSON help security teams further understand the Command and Control communications of malicious and risky apps.

RISK MITIGATION ACTIONS

Security administrators can set proactive app policies to mitigate app risks and reduce data exfiltration. Policies and risk mitigation are customizable so enterprises can tailor actions according to their risk tolerance. For example, you can restrict user access/privileges if users have installed risky apps on their devices based on criteria defined by you as an administrator. For example, some customers wish to restrict the use of applications that read SMS messages, use self signed certificates, and send sensitive information about the device over insecure communication channels or to unapproved cloud services. Application risk policies can be crafted to fit specific requirements, with over 100 application characteristics that can be used to create policies. This is powered by z3a's deep insight into application behavior and risks. z3A also allows for risk mitigation through customizable automated actions, such as sending an SMS when a risky app is discovered. Enterprises can also create distinct policies for different groups pulled from the enterprise's MDM solution.

GET STARTED TODAY

See how Zimperium z3A™ can help you manage mobile vulnerabilities across your enterprise. Contact us to get a free enterprise trial today.

ZIMPERIUM®

Sources

[1] ZDNet. Enterprises lax about mobile security as more threats loom. https://www.zdnet.com/article/enterprises-lax-about-mobile-security-as-more-threats-loom/#modal-absolute-0afb01bf-aeeb-4205-bdcb-a9c8c8f7c6fd

[2] ZDNet. Two-thirds of all Android antivirus apps are frauds. https://www.zdnet.com/article/two-thirds-of-all-android-antivirus-apps-are-frauds/

[3] MobileIron. Riskware vs. Malware. https://marketplace.mobileiron.com/servlet/servlet.FileDownload?file=00P3400000keRRrEAM

[4] Inbound Logistics. Mobile Trends Impacting the Enterprise Ecosystem in 2019. https://www.inboundlogistics.com/cms/article/mobile-trends-impacting-the-enterprise-ecosystem-in-2019/

[5] Statista. Number of mobile app downloads worldwide in 2017, 2018 and 2022 (in billions). https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

[6] LifeWire. How Many Apps Are in the App Store? https://www.lifewire.com/how-many-apps-in-app-store-2000252

[7] AppBrain. Android and Google Play statistics. https://www.appbrain.com/stats

[8] Sensor Tower. Global App Revenue Reached $19.5 Billion Last Quarter, Up 17% Year-Over-Year. https://sensortower.com/blog/app-revenue-and-downloads-q1-2019

[9] Sensor Tower. Global App Revenue Reached $19.5 Billion Last Quarter, Up 17% Year-Over-Year. https://sensortower.com/blog/app-revenue-and-downloads-q1-2019