Lookout

THE SPECTRUM OF MOBILE RISK

Understanding the full range of risks to enterprise data from mobility

Lookout has developed the Mobile Risk Matrix to help organizations understand the components and vectors that make up the spectrum of mobile risk – and to provide data that will help enterprises gain a deeper understanding of the prevalence and impact of mobile threats and vulnerabilities.

THE MOBILE RISK MATRIX

Components of Risk / **Vectors**

Components of Risk	APPS	DEVICE	NETWORK	WEB & CONTENT
THREATS	**App threats** 1 Malicious apps can steal info, damage devices, and give unauthorized remote access.	**Device threats** Device threats can cause catastrophic data loss due to heightened attacker permissions.	**Network threats** 5 Data is at risk of attack via Wi-Fi or cellular network connections	**Web & content threats** Threats include malicious URLs opened from phishing emails or SMS messages.
SOFTWARE VULNERABILITIES	**App vulnerabilities** Even well known software development companies have been found to release apps that contained security flaws, putting corporate and user data at risk.	**Device vulnerabilities** 2 Enterprise devices are at risk during "vulnerability windows," the amount of time it takes from the release of a new patch to adoption of that update.	**Network vulnerabilities** Mobile devices encounter many more hostile networks than laptops, and don't have the same level of protection.	**Web & content vulnerabilities** Malformed content, such as web pages, videos, and photos, can enable unauthorized device access.
BEHAVIOR & CONFIGURATIONS	**App behaviors & configurations** 3 Mobile apps have the potential to leak data such as contact records.	**Device behaviors & configurations** 4 Behaviors like enabling USB debugging for Android or installing apps from non-official app stores put enterprise data at risk.	**Network behaviors & configurations** Connecting to a misconfigured router, unknown captive portal, or a network that decrypts traffic for content filtering.	**Web & content behaviors & configurations** Visiting "low reputation" websites that don't encrypt credentials, leak enterprise data, and increase the likelihood of malicious activity.

MOBILE RISK PREVALENCE

47 IN 1000 ANDROID ENTERPRISE DEVICES ENCOUNTERED APP-BASED THREATS

Across two quarters (4Q16-1Q17) 47 out of 1000 Android enterprise devices protected by Lookout Mobile Endpoint Security encountered app-based threats. 1

57% OF iOS USERS HAVE NOT UPDATED THEIR OPERATING SYSTEMS ABOVE 10.3

From the release of iOS 10.3 on March 27, 2017 to April 14, 2017 only 43% of users updated to the latest version of iOS. This is concerning because 10.3.1 patches a code execution flaw that could be exploited via Wi-Fi. This data point is based on iOS users of Lookout Personal. 2

30% OF APPS ON ENTERPRISE iOS DEVICES ACCESS THE DEVICE'S CONTACTS

On enterprise iOS devices protected by Lookout Mobile Endpoint Security, 75% of apps access the camera, 38% access GPS, 8% access calendars, and 10% access the microphone. Across iOS enterprise apps, 43% connected to Facebook and 14% connected to Twitter. 3

5 IN 1000 ENTERPRISE ANDROID DEVICES ARE ROOTED

Only 1 in 1,000 of enterprise iOS devices are jailbroken. 4

UP TO 1% OF ENTERPRISE MOBILE DEVICES ENCOUNTERED NETWORK-BASED THREATS

Lookout research shows that slightly less than 1% of enterprise mobile devices encountered network-based threats over the last year. 5

ABOUT THE DATA:

The analyzed data came from a large global subset of Lookout personal and enterprise protected devices, and the time periods ranged between April 15, 2016 and April 16, 2017. The enterprise data includes both Android and iOS devices from financial institutions, healthcare organizations, government agencies and other industries. The personal data includes both Android and iOS devices from consumers around the globe, consisting of over 100M devices worldwide. All data was pulled anonymously, and no corporate data, networks, or systems were accessed to perform this analysis.

ABOUT LOOKOUT:

Lookout is a cybersecurity company that makes it possible for tens of millions of individuals, enterprises and government agencies to be both mobile and secure. Powered by a dataset of virtually all the mobile code in the world – 40 million apps and counting – the Lookout Security Cloud can identify connections that would otherwise go unseen and predict and stop mobile attacks before they do harm. The world's leading mobile network operators, including AT&T, Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile and Telstra, have selected Lookout as their preferred mobile security solution. Lookout is also partnered with such enterprise leaders as AirWatch, Ingram Micro, Microsoft, and MobileIron. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com, subscribe to the Lookout newsletter, and follow Lookout on Facebook, Twitter and LinkedIn.