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: WEB & CONTENT	APPS	DEVICE	NETWORK
THREATS	• Phishing • Drive-by-download • Malicious websites and files	• Spyware and surveillanceware • Trojans • Other malicious apps	• Privilege escalation • Remote jailbreak/root	• Man-in-the-middle • Fake cell towers • Root CA installation
SOFTWARE VULNERABILITIES	• Malformed content that triggers OS or app vulnerabilities	• Out-of-date apps • Vulnerable SDKs • Poor coding practices	• Out-of-date OS • Dead-end hardware • Vulnerable pre-installed apps	• Network hardware vulnerabilities • Protocol stack vulnerabilities
BEHAVIOR & CONFIGURATIONS	• Opening attachments and visiting links to potentially unsafe content	• Apps that leak data • Apps that breach company security • Apps that breach regulatory compliance	• User initiated jailbreak/root • No pin code/password • USB debugging	• Proxies, VPNs, root-CAs • Auto-joining unencrypted networks

MOBILE RISK PREVALENCE

203 OUT OF 1000 ENTERPRISE DEVICES ENCOUNTERED URL-BASED THREATS

203 out of 1000 enterprise devices (Android & iOS) encountered URL-based threats (Q1 - Q3 2021).

17% OF THE APPS ON ENTERPRISE DEVICES ACCESS THE DEVICE'S CONTACTS

On enterprise devices protected by Lookout Mobile Endpoint Security, 25% of apps access the camera, 38% access GPS, 2% access calendars, and 5% access the microphone. Across enterprise apps, 4% connected to Facebook and 2% connected to Twitter.

16 IN 1000 ANDROID ENTERPRISE DEVICES ENCOUNTERED APP-BASED THREATS

Across two quarters (Q1-Q3 2021) 16 out of 1000 Android enterprise devices encountered app-based threats.

58% OF iOS USERS HAVE NOT UPDATED THEIR OPERATING SYSTEMS ABOVE 15.0

From the release of 15.0 on September 20, 2021 to November 17, 2021 only 42% of users have updated to the last release.

2 OUT OF 1000 ENTERPRISE DEVICES ENCOUNTERED NETWORK-BASED THREATS

2 out of 1000 enterprise mobile devices encountered network-based threats over the last year.

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 January 1, 2021 and October 31, 2021. 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 185M devices worldwide. All data was pulled anonymously, and no corporate data, networks, or systems were accessed to perform this analysis.

ABOUT LOOKOUT:

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, VMware, Vodafone, Microsoft, Google, and Apple. 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 and follow Lookout on its blog, LinkedIn, and Twitter.