Symantec.

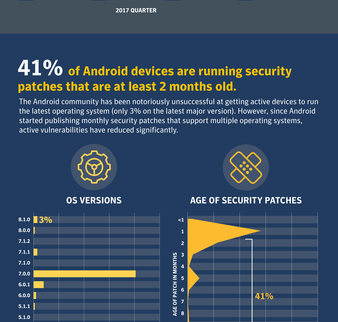
Mobile Threat Intelligence Report

2017: The Year In Review

This report reviews worldwide threat intelligence data collected by the SEP Mobile Research Team, from globally-deployed mobile security agents and millions of monthly security tests from January through December 2017.

Mobile malware variants increased by 54% in 2017,

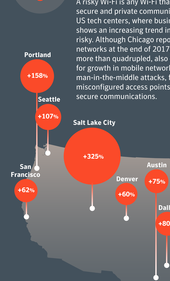
as compared to 2016. This chart shows how the frequency of different types of mobile malware varied over the year. Note the third highest category is Grayware, which may not be malicious, but introduces unnecessary risk to sensitive data. Grayware, or Unwanted Apps, are not identified by all mobile security solutions.



41% of Android devices are running security patches that are at least 2 months old.

The Android community has been notoriously unsuccessful at getting active devices to run the latest operating system (only 3% on the latest major version). However, since Android started publishing monthly security patches that support multiple operating systems, active vulnerabilities have reduced significantly.

OS VERSIONS



AGE OF SECURITY PATCHES

20% of iOS devices are running outdated versions.

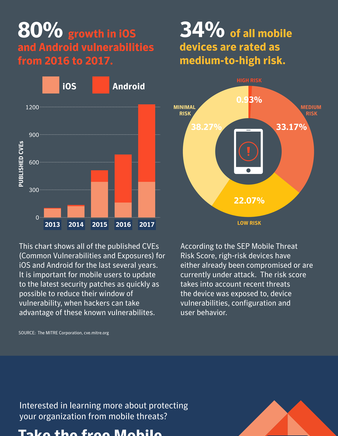
Unlike with Android, Apple controls the full distribution chain for its security updates, leading to more rapid patching and only 20% of iOS devices that are not on the last major version.

iOS VERSIONS

Data sampled on 1/1/2018

The number of risky Wi-Fi networks increased by 56% in 2017.

A risky Wi-Fi is any Wi-Fi that does not provide complete end-to-end secure and private communications, as requested. Looking at major US tech centers, where businesses rely heavily on user mobility, data shows an increasing trend in the number of networks identified as risky. Although Chicago reportedly had fewer risky Wi-Fi networks at the end of 2017, Salt Lake City numbers more than quadrupled, also earning them the top spot for growth in mobile network incidents, including man-in-the-middle attacks, fake networks and misconfigured access points that don't properly secure communications.



GROWTH ACROSS ALL US TECH CENTERS IN 2017

In organizations,

Over 40% of the mobile devices are exposed to a network threat every 4 months.

Regardless of how malicious the intent of the network threat is, individuals and organizations would be wise to avoid or protect themselves against risky networks.

Data averaged over 4 quarters.

80% growth in iOS and Android vulnerabilities from 2016 to 2017.

This chart shows all of the published CVEs (Common Vulnerabilities and Exposures) for iOS and Android for the last several years. It is important for mobile users to update to the latest security patches as quickly as possible to reduce their window of vulnerability, when hackers can take advantage of these known vulnerabilities.

SOURCE: The MITRE Corporation, cve.mitre.org

34% of all mobile devices are rated as medium-to-high risk.

According to the SEP Mobile Threat Risk Score, high-risk devices have either already been compromised or are currently under attack. The risk score takes into account recent threats the device was exposed to, device vulnerabilities, configuration and user behavior.

Interested in learning more about protecting your organization from mobile threats?

Take the free Mobile Security Mastery Course. Nine video modules that can be completed in less than 2 hours.

TAKE THE COURSE

About the Mobile Threat Intelligence Report

The Symantec Mobile Threat Intelligence Report reviews worldwide threat intelligence data, gathered by Symantec through the delivery of Symantec products and services. Today's report is based on millions of monthly security tests from January through December 2017 and includes both unmanaged devices and those under security management in enterprise organizations. Data includes SEP Mobile's proprietary Mobile Threat Risk Score, which acts as a credit score to measure the risk of threat exposure for mobile devices. For organizations, SEP Mobile condenses millions of data points to calculate a risk score so that IT can quickly discern the state of the overall system and the risk to each device. SEP Mobile analyzes 1 million apps and more than 2 million unique networks worldwide every year.

Symantec.