
Mobile malware grew by 62% in 2017, as shown in the chart, leaving users vulnerable to both new and well-known threats.

- 80% growth in iOS
- 41% of Android devices are running security updates for the last major version, leading to more rapid patching
- 20% of iOS devices are running outdated versions

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.

SEP Mobile analyzes 1 million apps and more than 2 million unique networks worldwide. 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.

In organizations, Apps, are not identified by all mobile security solutions.

- 41% of Android devices can be identified by mobile security solutions.
- 30% of iOS devices can be identified by mobile security solutions.

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.

Over 40% of mobile devices are exposed to a medium-to-high risk of threats.

- Apps, are not identified by all mobile security solutions.
- Grayware, or Unwanted Software, may not be malicious, but introduces unnecessary risk to sensitive data.

Malware varied over the year. The third highest category is Grayware, which may not be malicious, but introduces unnecessary risk to sensitive data. Grayware, or Unwanted Software, may not be malicious, but introduces unnecessary risk to sensitive data.

41% of Android devices are coming security patches that are at least 3 months old.

- 20% of iOS devices are running outdated versions.
- 5.0.0
- 5.0.1
- 5.0.2
- 5.1.0
- 5.1.1
- 6.0.1
- 7.1.0
- 7.1.2
- 8.0.0
- 8.1.0

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, companies can take advantage of these known vulnerabilities.

This chart shows all of the published CVEs (Common Vulnerabilities and Exposures) for iOS and Android for the last several years.

According to the SEP Mobile Threat Intelligence Report, the biggest risk to mobile devices is 44% of systems with active vulnerabilities. These are systems that are currently under attack. The risk score of these devices currently under attack is high-risk, meaning they have 96% risk of being compromised. The risk score of all mobile devices is 21.2%.

Over 40% of mobile devices are exposed to a high risk of threats every 4 months.

By completing the Security Mastery Course, which includes nine video modules that can be completed in less than 2 hours, users can get a better understanding of how to protect their mobile devices.

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

Take the course!