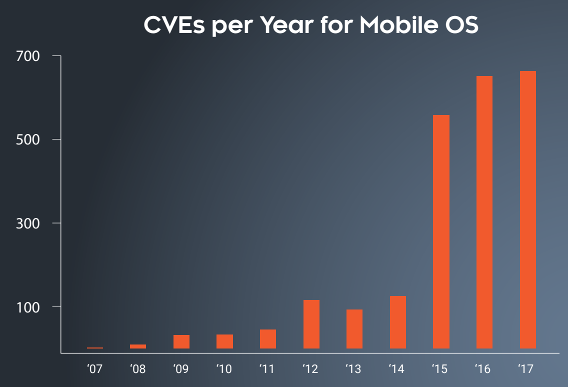
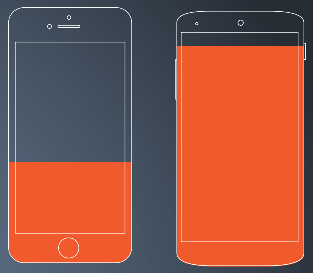
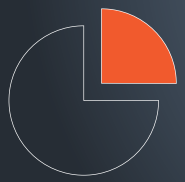
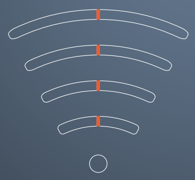
ZIMPERIUM®
MOBILE THREAT DEFENSE

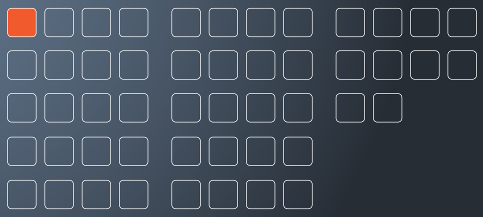
Zimperium Global Threat Report Q2-2017


CVEs per Year for Mobile OS




1 of 4 Devices Introduces Unnecessary Risk




1 out of 50 Apps Introduces Risk

Zimperium Global Threat Data

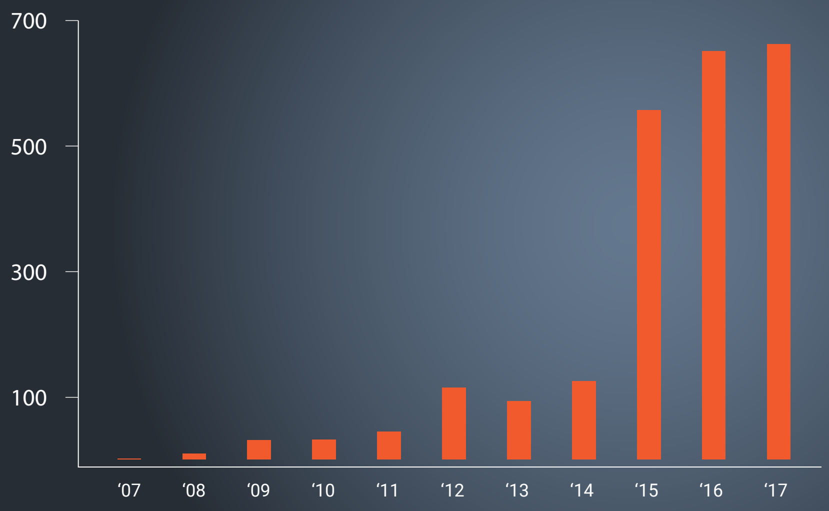
Businesses of all sizes use mobile devices as standard computing platforms in today's workplace. U.S. consumers now spend over 5 hours per day on mobile devices [1]. This number has continually increased every quarter since users prefer the ease of use and the flexibility to work wherever, whenever via their iOS-based and Android-based smartphones. As a result, personal and business data (e.g., emails, contacts, calendars, documents, photos, credentials) on mobile devices are exposed to threats now, more than ever.

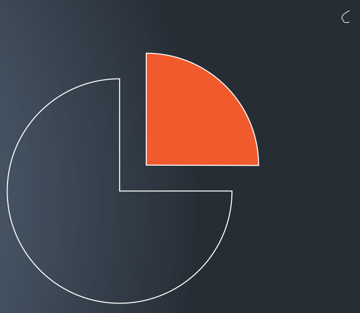
Cyber criminals are more likely to take the path of least resistance and enterprise data is most vulnerable via mobile devices since most of time spent is away from secure networks, on public Wi-Fi and on apps that IT and security do not control or administer. Security-conscious companies understand this is a serious threat and have installed mobile threat defense apps such as Zimperium zIPS on both corporate and BYO devices.

During the second quarter, April 1 - June 30, 2017, zIPS-protected devices detected several types of mobile device risks and threats around the world. We categorize the risks and threats as follows:

- **DEVICE THREATS AND RISKS** - Threats to the device or OS, including unpatched vulnerabilities
- **NETWORK THREATS** - Threats delivered to the device via the cell network or Wi-Fi
- **APP THREATS** - Mobile malware, spyware, adware, or "leaky apps" on devices

CVEs per Year for Mobile OS





1 of 4 Devices Introduces Unnecessary Risk

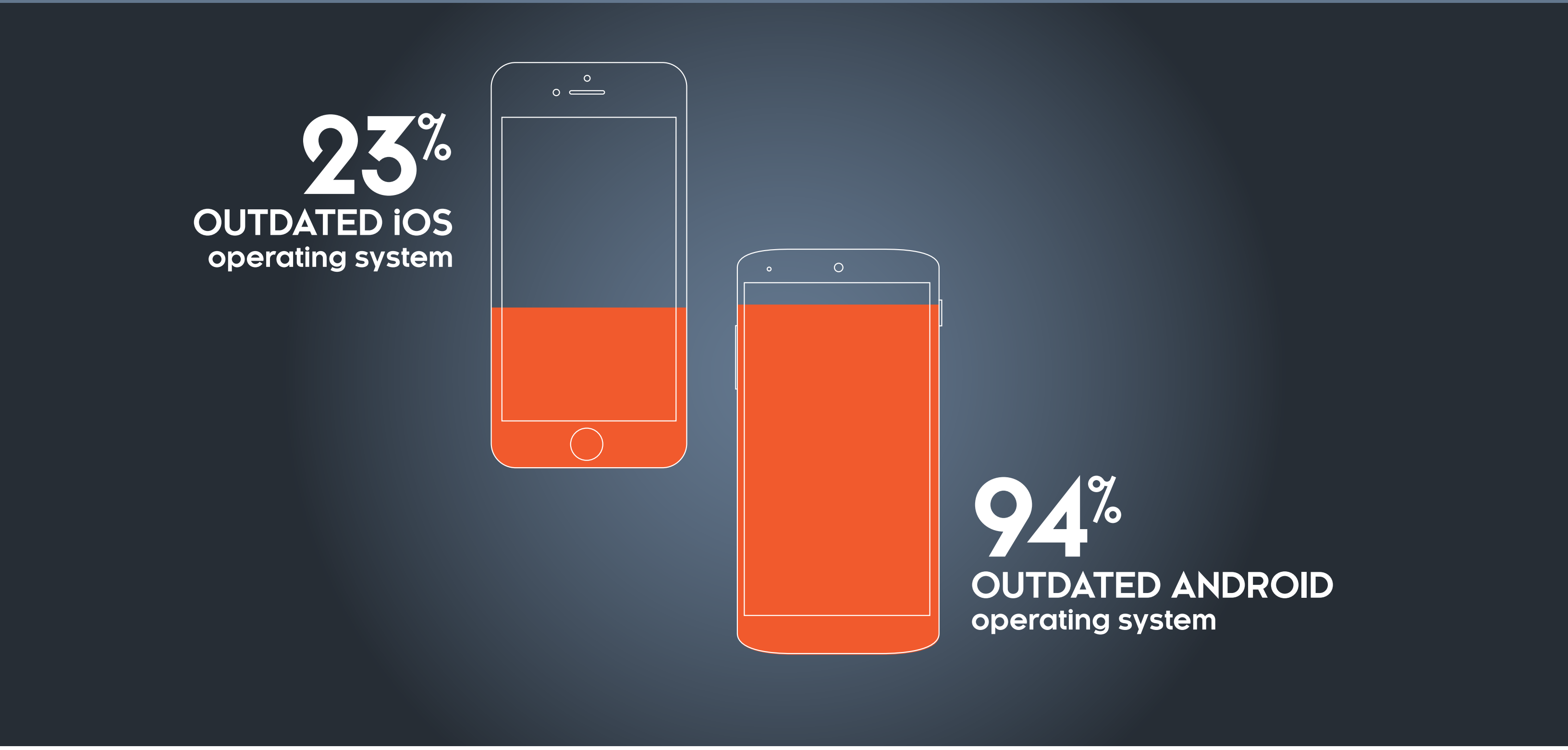
Device Threats and Risks

Attackers are constantly conducting research to uncover vulnerabilities and unique ways to exploit mobile operating systems. Sophisticated remote attacks sometimes do not require end-user interaction to install or detonate an attack in order to compromise a device. Therefore, silent remote attacks are difficult to detect during or after an attack without a mobile threat defense (MTD) solution monitoring the device's OS behaviors and file systems.

Since 2016 there have been over 600 common vulnerabilities and exposures (CVEs) registered for Android and 300 for iOS [2]. So far in 2017, there are more CVEs registered for Android and iOS than in all of 2016. The increase indicates the Android and iOS mobile operating systems are still maturing. New research both on current capabilities and on new features continues to be released and security researchers continue to disclose new bugs and vulnerabilities. While not all vulnerabilities are severe, there were still hundreds that enabled remote code execution (such as Stagefright and Pegasus) that forced the business world to pay attention to mobile device security.

So far in 2017, there are more **CVEs registered** for Android and iOS than in all 2016.

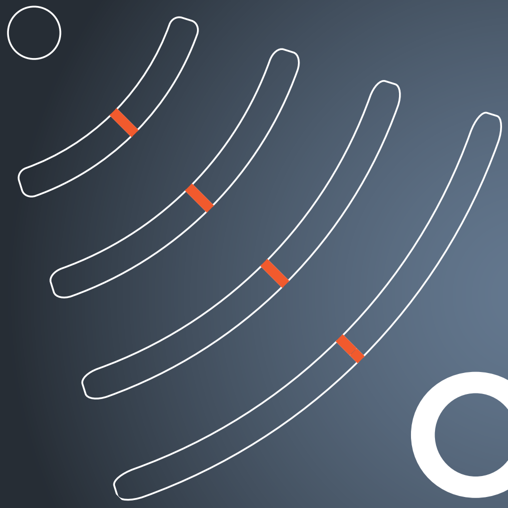
Zimperium collected device risk data from customer usage and reported it in the aggregate for mobile device misconfigurations, settings, and installed operating system versions. The risks are separated by operating system (Android and iOS) since each OS has its own software update ecosystem.



Device Threats and Risks

The fragmented Android update process is well documented, but a surprisingly high number of iOS devices were not running the latest version either. Over 23% of iOS devices were not running the latest version iOS 10.3.2 and hadn't received security updates as of June 30, 2017 [3]. Since Apple controls the OS and the process to update devices, many believe iOS devices are routinely updated in a timely fashion. However, our data shows that one in five iOS devices did not have an update that was readily available for over 45 days [4]. The most concerning risks associated with iOS devices were malicious configuration profiles and "leaky apps." These profiles can allow third parties to maintain persistence on a device, decrypt traffic, synchronize calendars and contacts, track the device's location and could allow a remote connection to control the device or siphon data from the device without the user's knowledge. These profiles were installed despite security policies in the MDM because they cannot be detected without MTD.

The most concerning risks associated with iOS devices were malicious configuration profiles and "leaky apps."



Over 5%

of all devices detected a reconnaissance scan from a network device or an attacker.

Network Threats and Attacks

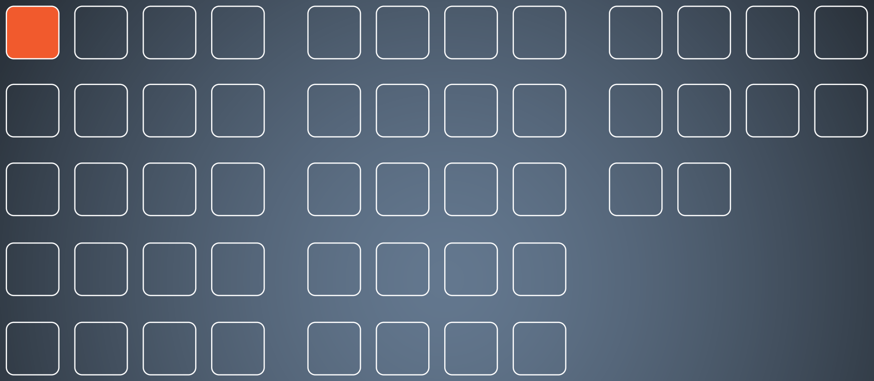
One of the most serious types of threats occurs when an attacker intercepts a mobile device's network traffic through techniques such as a man-in-the-middle (MITM) attack or a rogue access point. This gives the attacker the ability to read and capture credentials, emails, calendars, contacts and other sensitive data as a step in a more advanced attack.

For the second quarter of 2017, our data shows over 5% of all devices detected a reconnaissance scan from a network device or an attacker. Many of these devices experienced multiple scans over the quarter. Attackers scan networks to find victims and reroute traffic via an MITM attack in order to read and capture communications to and from the targeted device. zIPS detected a MITM attack on 80% of the devices that experienced a scan and simultaneously reported it to the customer's security team. This is the most severe type of network attack since it is usually invisible to a user. Unless a user has a mobile threat defense app that can detect the attack on his/her device in real-time (e.g., zIPS), their wireless connection can be rerouted to a proxy and their data may be compromised.

80%

of scanned devices detected a MITM attack.

Rogue access points, which are wireless access points that have been installed on a secure network without explicit authorization from a local network administrator, are another common type of network attack that reroutes traffic. Rogue access points can be placed anywhere and follow trusted naming conventions to capture traffic from potential targets. Nearly 1% of devices detected a rogue access point after a device connected to it. For example, one customer found a rogue access point placed in a legitimate public transportation vehicle in order to capture mobile user behavior. zIPS was able to detect these rogue networks, report back to the corporate security teams and automatically terminate the session if the security policy dictated and configured that action.



“1 out of 50 Apps contains Privacy or Security Issues”

iOS App Analysis

Apps can be used to deliver and execute malicious code to compromise a device, or to act as a proxy in a more sophisticated attack. Examples of app-based attacks include XcodeGhost on iOS and Gooligan, a family of Android-based malware.

Since Zimperium provides on-device detection, it doesn’t require signatures or hashes to detect malicious activity on the device. Zimperium monitors the OS behavior for anomalies using a machine-learning algorithm. zIPS, therefore, can detect attacks in real-time that would otherwise not be detected by only looking for malware signatures. Zimperium’s mobile application reputation service, z3A, scans apps installed on devices or in app stores and interrogates them for security issues and privacy abuse, enabling security teams to make informed decisions about the apps on users’ devices.

50,000
iOS Apps Analyzed

Zimperium analyzed 50,000 iOS apps present on enterprise users’ devices in the second quarter of 2017 to report on malware, security issues, and privacy abuse. Zimperium’s mobile application reputation service scans for dozens of app security and privacy issues, however, it focused on the seven most severe issues for this report.

7 Most Severe App Security Issues

MALWARE - This app contains known malware.

KEYCHAIN SHARING - This app has the functionality to share passwords from its keychain with other apps made by the same team.

MD2 ENCRYPTION - The app implements the Common Cryptographic library using MD2 for encryption features.

PRIVATE FRAMEWORKS - The app accesses frameworks that are located in PrivateFrameworks. Private Framework access is prohibited by Apple.

PRIVATE INFO URL - This app sends query parameters with private information such as the UDID of the device.

READING UDID - This app is reading the device UUID number.

STORED INFO OVER USB - Stored information can be retrieved without your knowledge during public USB recharge

Zimperium's application analysis on the sample set indicates malware is present on less than 1% of devices from which we collected data. While only 1% of Apple devices saw mobile malware, they have a greater percentage of suspicious profiles, apps using weak encryption and potentially retrieving private information from devices. The analysis found over 19% of apps had the capability of retrieving private information like passwords and device's Unique Device Identifier, UDID. Retrieving the UDID from devices has been prohibited by Apple since 2011 [5]. Approximately 3% of the apps were using weak encryption or hashing algorithms – like MD2 – and are not considered secure to pass private, payment data or in app purchases.

"Apps with security or privacy issues were downloaded over 50 million times"

The initial analysis sought to find a single issue inside each of the app bundles found on enterprise devices. Zimperium then sought out apps with more than one issue to identify the most abusive apps and therefore causing a huge mobile security and data leakage concern.

Of the 50,000 iOS apps scanned in the sample, 1,101 or 2.2% of the apps had at least one of the aforementioned security or privacy issues. This is a significant concern to enterprises since 1 of 50 apps is potentially leaking data to third parties. Enterprises have no way to detect this type of risk unless they are scanning apps for security or privacy issues. Through deep analysis, Zimperium researchers found the 1101 apps downloaded over 50 million times. Companies and individuals should be concerned if these iOS apps are on their devices and inside of their networks.

Further analysis of the most abusive and poorly constructed apps found several apps with 2 or more issues. Four apps had 5 issues and are considered highly dangerous and abusive. The most abusive and poorly constructed app had its latest version downloaded 850,000+ times. Twenty-one apps had 4 security concerns, seventy-four had 3 concerns, 174 had 2 issues and the remaining apps had a single security issue [6].

There are over 2.2 million apps in the Apple App Store downloaded 180 billion times [7]. These numbers represent a high number of variables to control and monitor by blacklisting or whitelisting different apps in order to reduce your data leakage via mobile devices. A simple way to enable informed decisions is to collect the app data in a central repository like Zimperium.

If you would like to monitor your actual mobile device risk, you need to implement a technology designed to be lightweight and unobtrusive to your user. Mobile threat defense technologies, like Zimperium are designed for mobile devices and their unique power and processing constraints. Please contact us to begin an evaluation for your organization.

SOURCES

1 - http://flurrymobile.tumblr.com/post/157921590345/us-consumers-time-spent-on-mobile-crosses-5

2 - https://cve.mitre.org/

3 - Zimperium, Inc.

4 - https://support.apple.com/en-us/HT207798

5 - https://techcrunch.com/2011/08/19/apple-ios-5-phasing-out-udid/

6 - Zimperium, Inc.

7 - https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

ZIMPERIUM®

Zimperium, the global leader in Mobile Threat Defense, offers real-time, on-device protection against both known and previously unknown threats, enabling detection and remediation of attacks on all three mobile threat vectors - Device, Network and Applications. Zimperium's patented z9™ detection engine uses machine learning to power zIPS™, mobile on-device Intrusion Prevention System app, and zIAP™, an embedded, In-App Protection SDK that delivers self-protecting iOS and Android apps.

CONTACT US

101 Mission Street
San Francisco, CA 94105
Main: (1) 844.601.6760
info@zimperium.com

www.zimperium.com