



ZIMPERIUM[®]
MOBILE THREAT DEFENSE

2019 “State of Enterprise Mobile Security” Report

EXECUTIVE SUMMARY












As the worldwide leader in mobile threat defense (MTD), Zimperium solutions protect millions of mobile endpoints around the world against device, network, phishing and malicious app threats and attacks. This report contains 2019 data from over 45 million endpoints from enterprises in a variety of industries and both local and national government agencies.

For purposes of this report, “threats” are conditions that increase the likelihood of a device being attacked or enable attacks to be made more efficiently. “Attacks” are actual attacks against mobile endpoints.

For some threats and attacks, we provide data about total detections; however, this report is primarily designed to provide businesses and government agencies of all sizes (Zimperium’s customers) with the data they need to prioritize their mobile device security efforts.

In a typical organization today, 60% of the endpoints containing or accessing organizational data are mobile... and most of these endpoints do not have a security solution that can provide protection and visibility. This report is intended to answer the primary question organizations ask every day: *How many and how are my mobile endpoint devices being attacked?*

Here are a few key findings across the threat and attack vectors:

VECTOR	KEY FINDINGS
	Mobile OS vendors created patches for 1,161 security vulnerabilities.
	24% of enterprise mobile endpoints were exposed to device threats not including outdated operating systems.
	68% of malicious profiles were considered “high-risk”, meaning they had elevated access that could lead to data exfiltration or full compromise.
	Over half of all enterprise mobile endpoints encountered risky networks.
	Zimperium detected over 3 million risky networks in 2019.
	Network attacks accounted for 92% of all attacks covered in this report.
	19% of enterprise mobile endpoints experienced network-based attacks.
	13% of enterprise Android devices detected malicious apps. Of all enterprise endpoints with malicious apps, 86% were Android-based and 14% were on iOS.
	48% of the Android devices had sideloaded apps versus 3% of iOS devices.
	85% of iOS apps and 21% of Android apps failed to receive a passing privacy grade.
	71% of iOS apps and 68% of Android apps failed to receive a passing security grade.

DEVICE THREATS & ATTACKS

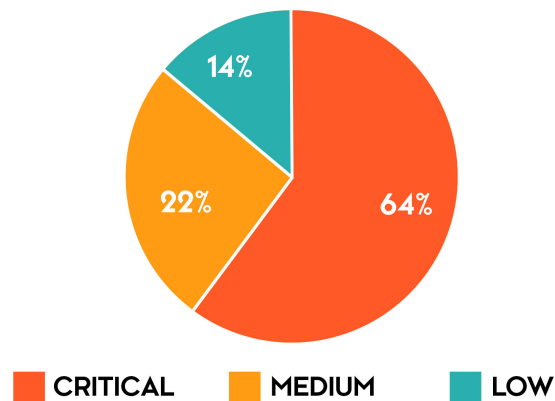
Device Threats

Many conditions increase the threat exposure of mobile endpoints - the majority of which stem from the fact that users are the admins on these devices. Users are the ones that choose whether or not to update the OS away from known vulnerable OS versions, to have a PIN code set, to jailbreak their device, etc. Here are some insights of the major device threats analyzed by Zimperium in 2019:

Key Finding: *Mobile OS vendors created patches for 1,161 security vulnerabilities.*

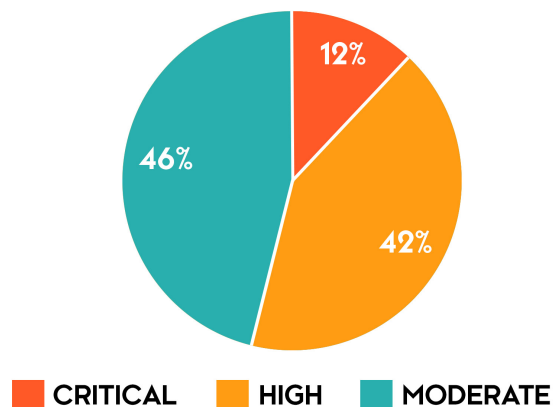
- iOS: In 2019, Apple patched 306 CVEs (Common Vulnerabilities and Exposures), 64% of which were considered "critical" security threats.

iOS CVEs (2019)



- Android: In 2019, Google patched 855 CVEs, the majority of which (54%) were considered "critical" or "high" security threats.

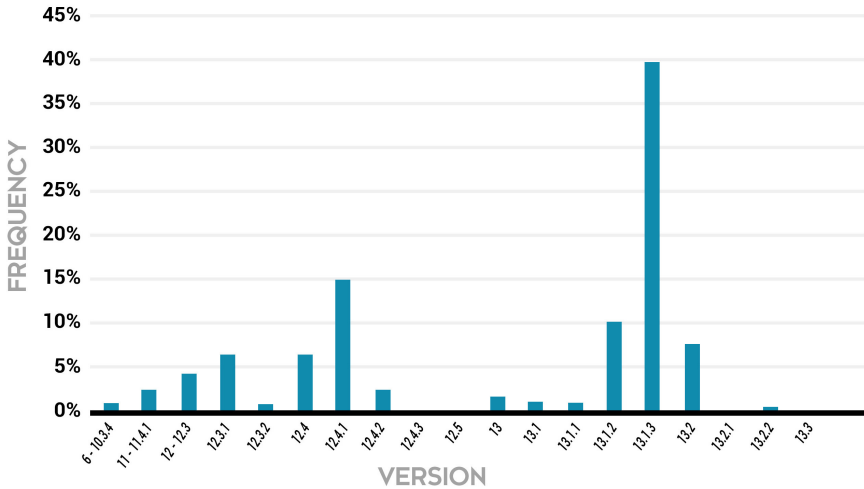
Android CVEs (2019)



Key Finding: Both mobile operating systems had a single version with significantly more users than any other. 40% of iOS devices were on a version four behind the latest (13.1.3) while the largest cluster of Android devices (58%) were on a version two behind the latest (9).

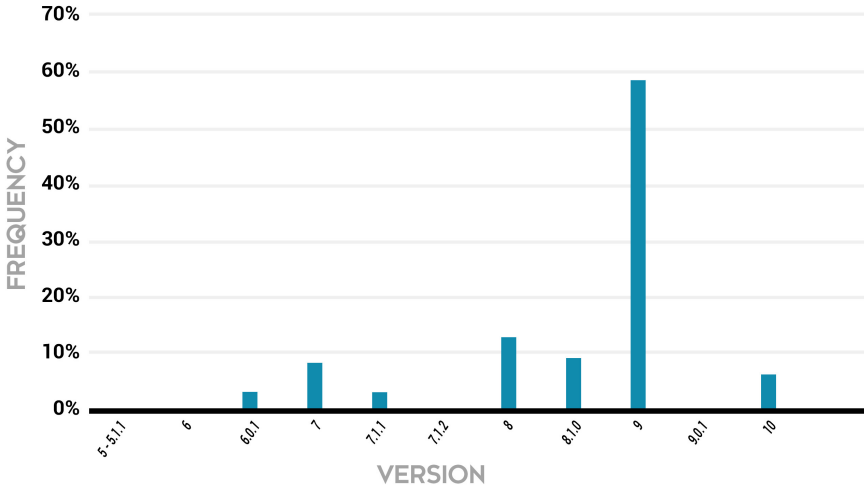
Key Finding: At the end of 2019, 48% of iOS devices were more than four versions behind the latest. The following charts show all the versions for active devices.

iOS VERSION FREQUENCY



- Android: While 6% of Android enterprise endpoints were on the current version at the end of 2019, 58% of Android devices were more than two versions behind the latest.

ANDROID VERSION FREQUENCY



Key Finding: 24% of enterprise mobile endpoints were exposed to device threats not including outdated operating systems.

- **No PIN:** 15% of enterprise endpoints had no PIN codes set.
- **Unknown Sources Enabled (Android):** 9.1% of enterprise Android endpoints enabled downloads from sources other than Google Play Store.

Device Attacks

For decades, hackers have worked hard to establish and maintain a persistent hold on every endpoint they compromise (e.g., servers, desktops, laptops, point of sale (POS) terminals, SCADA systems). By remaining persistent, attackers can not only steal data and credentials from the captured endpoint, but they can weaponize it and use it as a stepping stone to move to other systems (“land and expand”).

When attackers target mobile endpoints, the goal is the same. Given the unique architectural design of mobile endpoints (e.g., all apps being in containers, kernel being locked down), compromising the device and/or elevating privileges higher in the stack than app containers are the only ways to remain persistent and use the device for additional expansion. Simply put, compromising a mobile endpoint is the primary objective. Organizations must understand and protect against device attacks on any mobile endpoint containing or accessing corporate data and other systems.

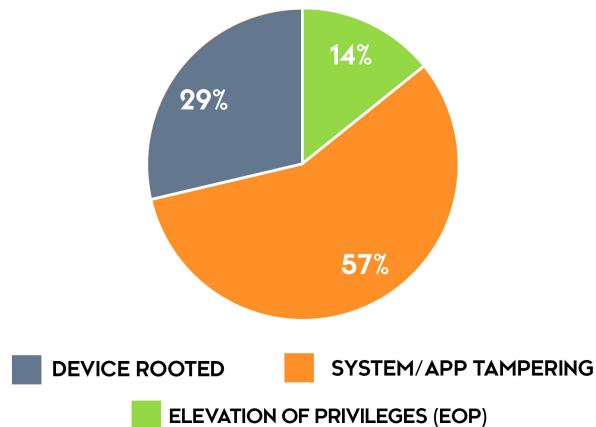
CAVEAT: Before diving into the device attacks, it is important to understand that Zimperium’s primary mission is to protect our customers at the earliest step in the attack “kill chain,” not to produce threat reports. Other attacks, predominantly network attacks, always proceed a device attack. Since Zimperium’s solutions stop the attack at the earliest part of the kill chain, *device attacks are significantly underreported compared to devices in the wild*. And it’s important to note that a single mobile device compromise puts an entire organization at risk.

Here are some insights of the major device attacks analyzed by Zimperium in 2019:

Key Finding: *Attempts to tamper with the system or apps (which requires having compromised the device) accounted for 57% of detected device attacks in 2019.*



DEVICE ATTACKS (2019)



Key Finding: 68% of malicious profiles were considered “high-risk”, meaning they had elevated access that could lead to data exfiltration or full compromise.

- Some of the dangerous iOS profiles detected include:
 - **“Sideload” AppStores:** Enables installing apps from non-Apple app stores; apps could have been created or manipulated to steal information, deliver exploits, etc.
 - **WiFi/Proxy Configurations:** Can secretly route traffic to malicious hosted proxies where traffic and data is captured.
 - **Personal VPN Profiles:** Users installing these profiles can go around corporate controls (e.g., DLP), but they often send traffic to foreign countries, etc.
 - **“Jailbreak” Profiles (CA/store/exploit):** User trusts/allows new jailbreaks and associated apps from a jailbreak developer.
 - **Unmanaged Root CA Certificates:** A cert that could be used to allow software to be installed and/or allow an already installed app to decrypt traffic on the device.

NETWORK THREATS & ATTACKS

Network Threats:

Risky networks can lead to data loss and are often precursors to actual network attacks. Enterprise network threats are completely user-driven since they are the ones deciding which networks to access. Here are some insights of the major network threats analyzed by Zimperium in 2019:

Key Finding: Over half of all enterprise mobile endpoints encountered risky networks.

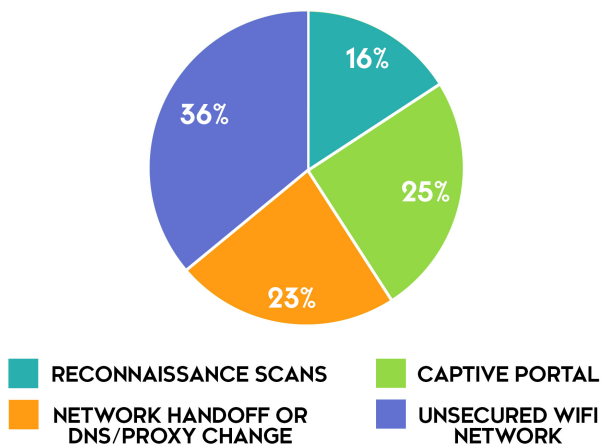
Key Finding: *Zimperium detected over 3 million risky networks in 2019.*

Key Finding: *While unsecured and unencrypted WiFi networks were the top network threats in 2019, the most interesting trend is the rise of network handoffs... from less than 1% of devices in 1H19 to 14% by the end of the year.*

- **Unsecured & Unencrypted Networks:** 22% of enterprise mobile endpoints attempted to connect to unsecured and unencrypted networks, which can lead to data loss.
- **Captive Portals:** 15% of enterprise mobile endpoints encountered captive portals, which can be utilized to deliver device exploits.
- **Network Handoffs:** 14% of enterprise mobile endpoints experienced a network handoff to redirect, which can take users to malicious websites where exploits can be delivered.
- **Reconnaissance Scans:** 10% of enterprise mobile endpoints experienced reconnaissance scan attempts wherein the attacker scans the device for known vulnerabilities that can be exploited.

Key Finding: *36% of network threats were through unsecured or unencrypted WiFi networks, followed by captive portals (25%) and network handoffs (23%).*

NETWORK THREATS (2019)



Network Attacks

Network-based attacks dominated in 2019. This is not surprising considering Zimperium's enterprise solutions stop attacks at the first step of the kill chain, which is a network-based attack in many cases. Here are some insights of the major network attacks analyzed by Zimperium in 2019:

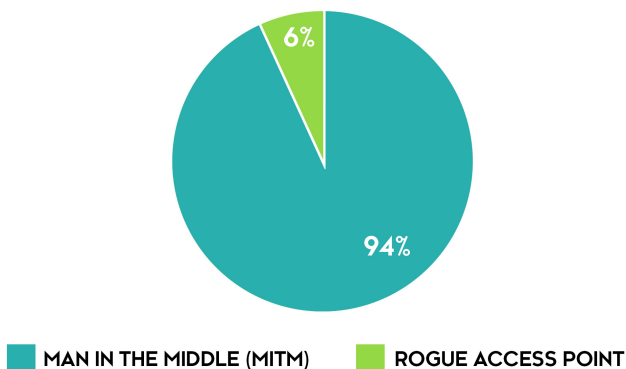
Key Finding: *Network attacks accounted for 92% of all attacks covered in this report.*



Key Finding: 19% of enterprise mobile endpoints experienced network-based attacks.

Key Finding: 94% of network attacks were man-in-the-middle (MITM) variations wherein attackers hijack traffic to steal credentials/data or deliver exploits to compromise the device.

NETWORK ATTACKS (2019)



APP THREATS & ATTACKS

App Threats

Organizations are aware of malicious mobile apps, but few understand the threats that come from sideloaded apps or legitimate apps that have hidden (and often completely unintended) security and privacy threats. Since users are the admins of mobile endpoints, organizations need a way to assess the threats of the installed mobile apps in their environments and create policies around their acceptable usage/existence. Below are insights of the major app threats analyzed by Zimperium in 2019:

Key Finding: 48% of the Android devices had sideloaded apps versus 3% of iOS devices.

Zimperium analyzed over six hundred thousand applications that were installed on enterprise endpoints to understand the security and privacy risks. The results are derived from Zimperium's advanced application analysis solution, z3A. As part of our study, mobile security researchers from the award-winning zLabs team assigned each application a pass or fail grade. A "passing" grade means that the app has very few security or privacy risks and does an above average job of protecting user data.

Key Finding: 85% of iOS apps and 21% of Android apps failed to receive a passing privacy grade.



Key Finding: *The most critical **privacy** risks in apps are those that capture data (which may include PII) and can send it off the device or inadvertently share it with other apps without user knowledge/consent.*

- Some of the most critical privacy risks in iOS apps include:
 - **System Logging:** App logs information into a system console; system log files (which may include PII) are accessible to any app.
 - **UI Screenshotting:** App can take screenshots of the full UI, enabling an attacker to understand everything from installed apps to credentials.
 - **Pasteboard Monitoring:** App is actively monitoring and can retrieve iOS Pasteboard data contents, exposing any captured data to theft.
 - **UX Tracking:** App includes the AppSee SDK which captures user activities using screenshots; screenshots and data (which may include PII) can be sent off of the device without the user being notified.
 - **Photo Enumeration:** App implements a direct Photo Library enumeration functionality that is prohibited by Apple.
- Some of the most critical privacy risks in Android apps include:
 - **Unprotected Data Publishing:** Data being published by the app is not protected with permissions and any app who is listening can intercept it.
 - **Vulnerable Facebook SDK:** The Facebook SDK embedded in the app is a version which is vulnerable to session hijacking.
 - **Insecure Content Provider:** App uses an insecure content provider; this allows other applications (e.g., a malicious app) on the device to request and share data.
 - **SMS Monitoring:** App can read SMS messages stored on the device or SIM card, regardless of content or confidentiality.
 - **Beacon Utilization:** App uses beacons to send information (potentially including PII) to nearby devices, often without user knowledge.

Key Finding: *71% of iOS apps and 68% of Android apps failed to receive a passing security grade.*

Key Finding: *The most critical **security** risks in apps are those that allow the installation of unapproved code/functionality or the execution of injected code.*

- Some of the most critical security risks in iOS apps include:



- **Swizzling API:** App implements Swizzling API calls which may impact the app's ability to trust security decisions that are based on manipulated/swizzled output.
 - **Unsafe Authentication:** App has an authentication method that can be used to override SSL and TLS chain validation.
 - **Over-the-air Installations:** App implements an over-the-air app installation method which circumvents Apple's review process and can install unapproved functionality.
 - **Vulnerable OpenSSL:** App was bundled with a vulnerable version of the OpenSSL library; an attacker can gain access to data being transmitted from the app to the server.
 - **Insecure Cloud Storage:** App contains references to cloud storage locations with viewable file/directory index listings, which could lead to data leakage of PII information.
- Some of the most critical security risks in Android apps include:
 - **JavaScript Execution:** App enables WebView to execute JavaScript code. This could potentially allow an attacker to introduce arbitrary JavaScript code to perform malicious actions.
 - **OS Level Commands:** App can execute commands at the OS level such as launching other applications and processes.
 - **Blind Method Loading:** App uses methods to blindly load all apps and JAR files located in a directory, enabling abuse by malicious parties.
 - **Java Object Injection:** App has methods of injected Java objects that are enumerable from JavaScript.
 - **Remote Code Retrieval:** App has functionality to retrieve apps, Java code and DEX files from remote locations; allows the application to update and introduce additional code at any time.

App Attacks

Because of the unique architecture of mobile endpoints, the malicious app threat to enterprises is different than the threat to traditional endpoints. Because mobile apps are in containers, they cannot interact with other apps to provide attackers with the coveted persistence discussed in the "Device Attack" section (a technique often used on traditional endpoints). The majority of malicious apps on mobile target consumers (e.g., BankBot and its variants) which leads to large fraud expenses to organizations.



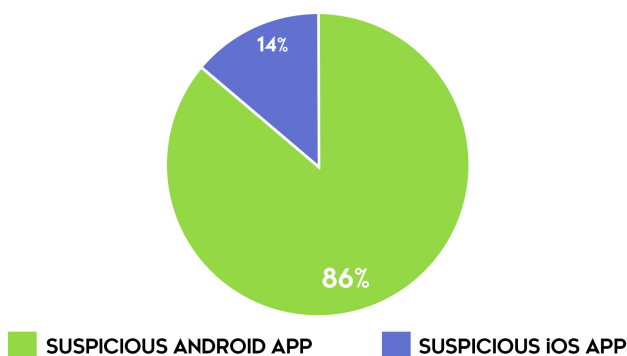
Even though malicious mobile apps are not the most effective way to attack an enterprise (network-based attacks are a far more efficient means to target a specific organization), they can still deliver exploits that can lead to loss of data/credentials or complete device compromise/weaponization. Below are some insights of the major app attacks analyzed by Zimperium in 2019:

Key Finding: *App attacks accounted for 5% of all attacks covered in this report. Like device attacks that were prevented earlier in the kill chain by Zimperium's machine learning-based detection, the percentage is much higher on unprotected devices in the wild.*

Key Finding: *13% of enterprise Android devices had malicious apps installed, compared to 0.2% of iOS devices detecting the same.*

Key Finding: *Of all enterprise endpoints with malicious apps, 86% were Android-based and 14% were on iOS.*

APP ATTACKS (2019)



PHISHING THREATS & ATTACKS

According to the Verizon Data Breach Investigations Report¹, over 90% of all breaches begin with a phishing attack. Considering that almost two-thirds of emails are now read on mobile², mobile phishing is a real concern for enterprises. This is compounded by another factor: mobile endpoints are a primary place that users read personal emails and instant messages/texts that are not protected by enterprise mail gateways with phishing protections. In addition to credential loss, when a user simply accesses a phishing site on mobile, an exploit can be delivered that compromises the device as discussed above.

In future reports, we will examine and provide analysis of mobile phishing threats and attacks. Our on-device, machine learning-based anti-phishing technology is currently collecting data on phishing threats and attacks.

¹ [Verizon Data Breach Investigations Report](#)

² [Adestra](#)



CONCLUSION

60% of the endpoints containing or accessing enterprise data are mobile; the majority of which do not have any security protection today. It is no longer a matter of if or when an enterprise's mobile endpoints are at risk of being attacked - they already are. Our research shows that 100% of the organizations that have protected their mobile endpoints with Zimperium have detected and prevented threats and attacks. As attackers continue to get more creative and take advantage of the lack of mobile security/visibility, mobile threats and attacks are increasing in both quantity and impact.

Zimperium's "State of Enterprise Mobile Security" Report is designed to answer the primary question organizations ask every day: *How many and how are my mobile endpoint devices being attacked?* For 2019, some of the most interesting findings include:

- Mobile OS vendors created patches for 1,161 security vulnerabilities.
- 24% of enterprise mobile endpoints were exposed to device threats not including outdated operating systems.
- Malicious Profiles are more dangerous than malware on iOS; profiles provide elevated privileges and are not vetted to the same extent as apps entering the App Store.
- 68% of malicious profiles were considered "high-risk", meaning they had elevated access that could lead to data exfiltration or full compromise.
- Over half of all enterprise mobile endpoints encountered risky networks.
- Zimperium detected over 3 million risky networks in 2019.
- Network attacks accounted for 92% of all attacks covered in this report.
- 19% of enterprise mobile endpoints experienced network-based attacks.
- 13% of enterprise Android devices detected malicious apps. Of all enterprise endpoints with malicious apps, 86% were Android-based and 14% were on iOS.
- 48% of the Android devices had sideloaded apps versus 3% of iOS devices.
- 85% of iOS apps and 21% of Android apps failed to receive a passing privacy grade.
- 71% of iOS apps and 68% of Android apps failed to receive a passing security grade.

The "State of Enterprise Mobile Security" Report will be updated semiannually to provide updated information and trending.



ABOUT ZIMPERIUM

Zimperium, the global leader in mobile device and app security, offers real-time, on-device protection against Android and iOS attacks. The Zimperium platform leverages our award-winning machine learning-based engine - z9 - to protect mobile data, apps and sessions against device compromises, network attacks, phishing attempts and malicious apps. To date, z9 has detected 100% of zero-day device exploits in the wild without requiring an update or suffering from the delays and limitations of cloud-based detection - something no other mobile security provider can claim.

Headquartered in Dallas, TX, Zimperium is backed by Sierra Ventures, Samsung, Telstra, Warburg Pincus and SoftBank. Learn more at www.zimperium.com or our official blog at <https://blog.zimperium.com>.

Zimperium detects mobile device, network, app and phishing threats and attacks via two solutions that utilize our core z9 detection engine:

- [zIPS](#): Zimperium's stand-alone app that provides persistent, on-device protection for mobile endpoints and data in a manner analogous to next-generation antivirus on traditional endpoints. For app threat analysis, zIPS customers also can receive detailed privacy and security threat information for any app through Zimperium's [z3A](#) capability.
- [zIAP](#): A software development kit (SDK) that quickly embeds z9 into any mobile app, immediately protecting the app and all of its sessions from attacks.

If you are interested in learning more about our research and how Zimperium can help protect enterprise mobile endpoints, please [contact](#) us or visit www.zimperium.com.

Zimperium, the Zimperium name and logo, Powered by Zimperium, zIPS, zIAP and z9 are registered trademarks or trademarks of Zimperium, Inc. in the US and other countries.

