State of Enterprise Mobile Security Report

July 2019

EXECUTIVE SUMMARY

Mobile devices continue to be the target of attack at increasing rates. There is a relatively simple explanation for this - in a typical organization today, 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--they already are.

Mobile devices contain or have access to the same information as traditional endpoints. While billions of dollars have been spent protecting and securing traditional endpoints, very little has been invested to protect mobile device endpoints. Attackers work on the same model as any other business: where do they get the greatest return on their investment of time and resources. As a result, mobile devices have become a favorite attack target and that trend is not likely to decrease any time soon.

As the worldwide leader in mobile threat defense (MTD) protecting millions of enterprise mobile endpoints around the world, Zimperium is in a unique leadership position to deliver insight into how mobile endpoints are being targeted through device, network, app and phishing tactics.

This report examines "threats" and "attacks." "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 and most dangerous countries / cities. However, this report is primarily designed to provide enterprises and government agencies (Zimperium's customers) with the data they need to prioritize their security investments and efforts. This report, compiled from data from over 45 million endpoints around the world, is focused on answering the primary question organizations ask every day: *What percent of my devices are exposed to each type of threat and attack?*

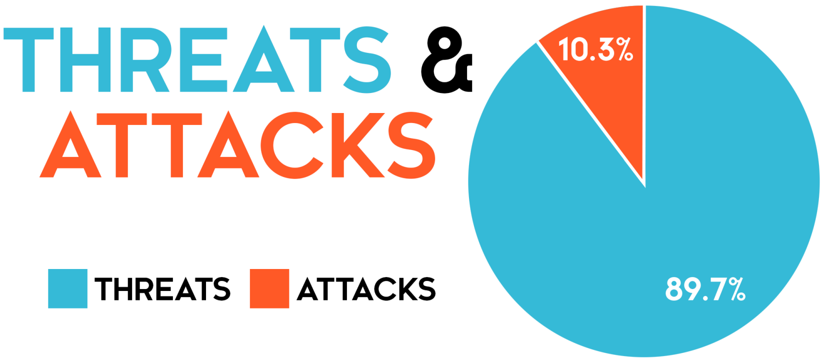
Key findings for threats and attacks across device, network and application vectors:

VECTOR	KEY FINDINGS
📱	*27% of enterprise mobile endpoints were exposed to device threats.*
📱	*Mobile OS vendors created patches for 440 security vulnerabilities.*
📱	*The majority of malicious profiles (68%) were considered "high-risk", meaning they had elevated access that could lead to data exfiltration or full compromise.*
📶	*32% of enterprise mobile endpoints encountered risky networks, and 7% of enterprise mobile endpoints were exposed to network attacks.*
📶	*ARP man-in-the-middle (MITMs) were attackers' favorite weapon with 48% of all network attacks and 45% of total attacks on enterprise endpoints.*
📶	*The number of network attacks detected in The Republic of Korea is slightly less than the total detected in the next four countries combined.*
□	*Zimperium's machine learning-based engine, z9, detected thousands of malicious apps that were not in VirusTotal or any other repository.*
□	*Malicious apps were 45% of Android attacks versus less than 1% of those detected on iOS. 98% of all detected malicious apps were on Android.*
□	*5% of enterprise mobile endpoints had sideloaded apps from sources outside the authorized and vetted Apple App Store or Google Play Store. 36% of the Android devices has sideloaded apps versus only 2% of iOS ones.*
□	*70% of iOS apps had advertising capabilities and iOS Bluetooth beacon usage exploded to 69% of apps (from 38% at the beginning of 2019).*
□	*24% of iOS apps passed sensitive information over the web unencrypted.*

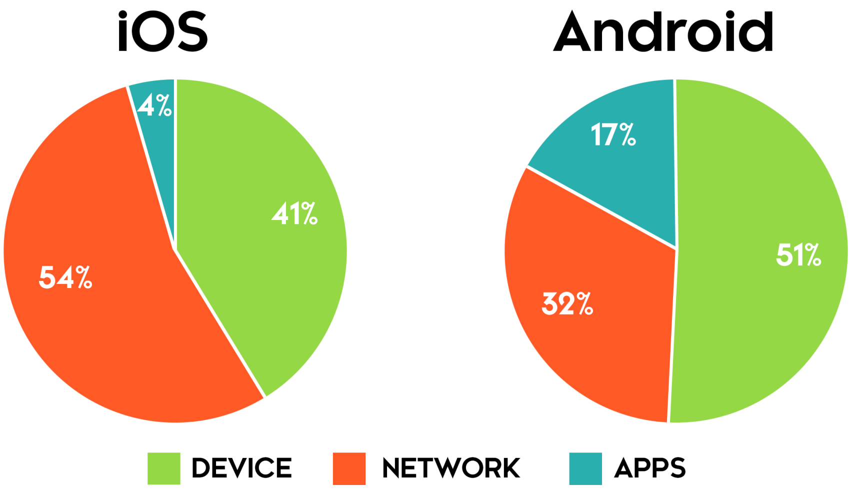
THE FOREST

Before diving into the details (the proverbial "trees"), it is helpful to frame things up with the big picture (the "forest").

As was previously mentioned, there are threats and attacks. Here is the high level breakdown of enterprise mobile endpoints detecting each:



Taking one step down, the breakdown of threats by iOS and Android provide some interesting insights. Given that Android has a more open third-party app environment, it is not surprising that apps have a relatively higher percent of the total threat for Android than we see in iOS. (However, this may be changing soon; please see the "Supreme Court Green Lights Suit Against Apple" sidebar story in the App Attack section for more information.)



Finally, here is the high level breakdown of iOS and Android attacks. For now, the overwhelming majority of iOS compromises occur via network attacks. While this is a clear nod to Apple's practice of vetting apps and developers, as well as its prohibition of third-party app stores, this very well may change - an unintended consequence of the recent United States Supreme Court ruling (which we mention in our "App Threats & Attacks" section). However, it's important to note that this does not mean iOS is free from attack. It simply means attackers look for the most optimal and efficient return on their time and for iOS, that attack path is through a network attack.

Similar to threats, Android's more open app environment, particularly the ease of accessing third party app stores, is evident in the larger percent of malicious apps:

ATTACKS	iOS	Android
DEVICE	0.2%	4%
NETWORK	99.7%	52%
APPS	0.1%	45%

Now that we have established the forest, let's dive into the trees. The next few sections outline the device, network, app and phishing threats and attacks detected across millions of endpoints.

DEVICE THREATS & ATTACKS

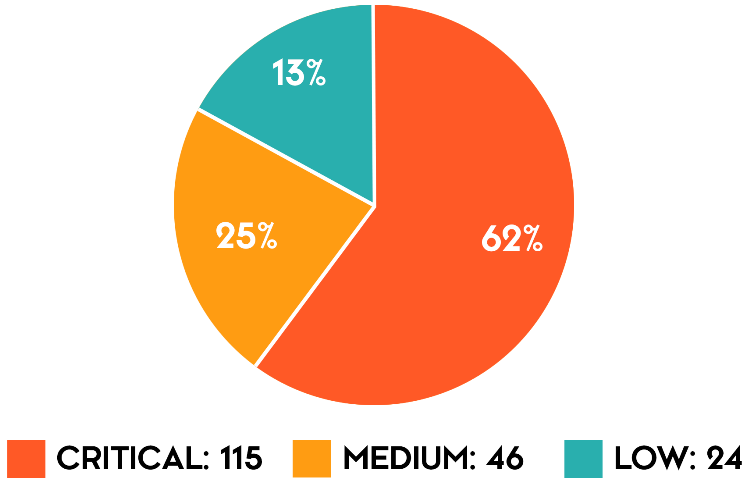
Many conditions increase the threat exposure of mobile endpoints--the majority of which stem from the fact that users are the admins on these devices. Users are the ones that choose whether or not to update the OS away from known vulnerable OS versions, to have a PIN code set, to jailbreak their device, etc. Here are some insights of the major device threats analyzed by Zimperium in 1H19:

Key Finding: *27% of enterprise mobile endpoints were exposed to device threats.*

Key Finding: *Mobile OS vendors created patches for 440 security vulnerabilities (a 30% increase over 1H2018), the majority of which were critical.*

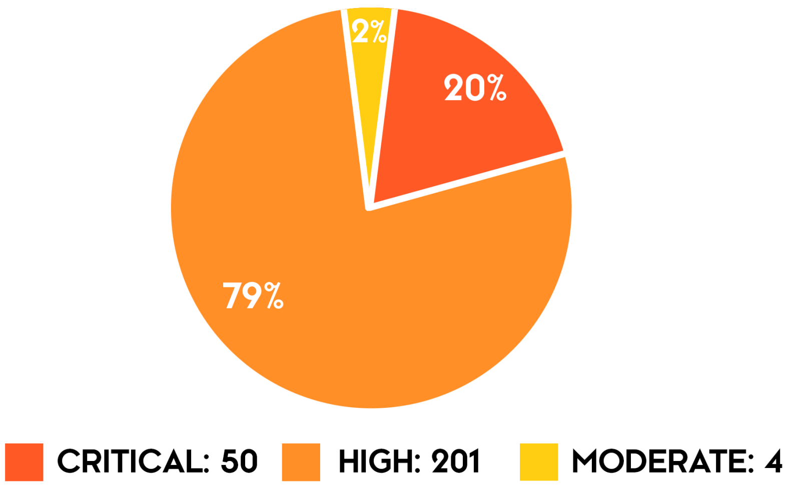
- iOS: In the 1H19, Apple patched 185 CVEs (Common Vulnerabilities and Exposures) compared to 120 during the same timeframe last year, or an increase of 54%. Over 60% of the 1H19 iOS CVEs were considered "critical" security threats.

iOS CVEs (1H2019)



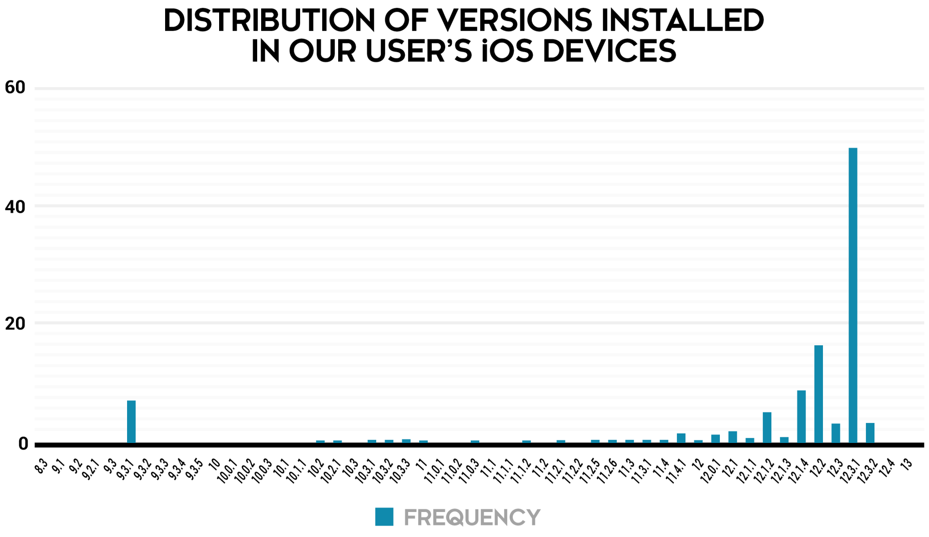
- Android: In the 1H19, Google patched 255 CVEs compared to 492 during the same timeframe last year, or a drop of 48%. 20% of the 1H19 Android CVEs were considered "critical" and another 79% were considered "high" security threats.

Android CVEs (1H2019)

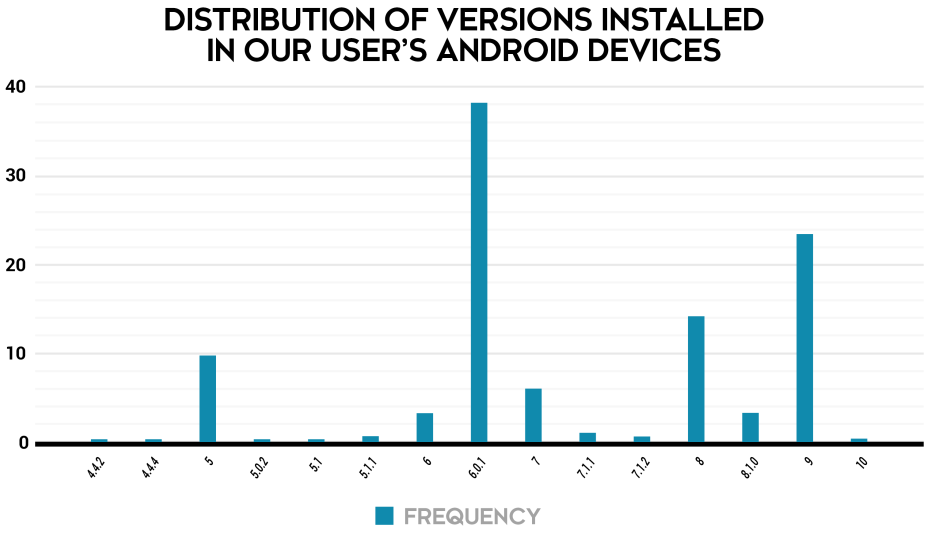


Key Finding: *When it comes to installing OS patches, Android devices continued to lag iOS ones. 60% of Android devices were more than five versions behind the latest release compared to only 28% for iOS.*

- iOS: Apple patches have been more frequent and granular than Android ones, so care should be taken in comparing the two. Having said that, less than 1% of iOS devices were one version behind the latest. In aggregate, only 28% of all iOS devices were more than five versions behind the latest.


DISTRIBUTION OF VERSIONS INSTALLED IN OUR USER'S iOS DEVICES

- Android: 24% of devices were one version behind the latest, but a staggering 38% were on version 6.0.1 which is seven versions behind. In aggregate, the majority (60%) of all Android devices were more than five versions behind the latest.


DISTRIBUTION OF VERSIONS INSTALLED IN OUR USER'S ANDROID DEVICES

MOBILE SECURITY NEWS

Apple Identifies and Patches iOS Flaws

Summary
Apple released a patch that rolled up more than 50 vulnerabilities, such as the ability to turn on an iPhone, iPad or iPod touch microphone without the user knowing

First Appearance
March 2019

Impacts and Consequences
Because users administer their own mobile devices, they typically do not apply patches and updates continuously and regularly, increasing potential risks

Sample Coverage:
The Register®
Biting the hand that feeds IT

Key Finding: *Most other device threats were consistent between enterprise and consumer users, reinforcing the reality that mobile blurs the lines between personal and professional lives.*

- **No PIN**: 525,000 endpoints were without a passcode, representing 1.1% of both enterprise and consumer endpoints.
- **No Encryption**: 110,000 endpoints had encryption disabled, representing a little over 0.2% of both enterprise and consumer endpoints.
- **Developer Options**: 170,000 endpoints were opened up to enable mobile app development. Enterprise devices were almost twice as likely as consumer ones to have had this threat (0.7% and 0.4%, respectively).[1]
- **USB Debugging**: 71,000 endpoints were opened up to enable USB debugging. Enterprise devices were more than twice as likely as consumer ones to have had this threat (0.5% and 0.2%, respectively).[2]

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 still 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 above 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 address device attacks on any mobile endpoint accessing corporate data and other systems. Here are some insights of the major device attacks analyzed by Zimperium so far in 2019:

MOBILE SECURITY NEWS

Cell Phone Belonging to Amazon CEO Compromised

Summary
Jeff Bezos alleged that a foreign government had compromised his cell phone and, at a minimum, had stolen photos from the device

First Appearance
March 2019

Impacts and Consequences
Device compromises can give cybercriminals access to all of the data on the device, including data that may be unencrypted

Sample Coverage:

CNN

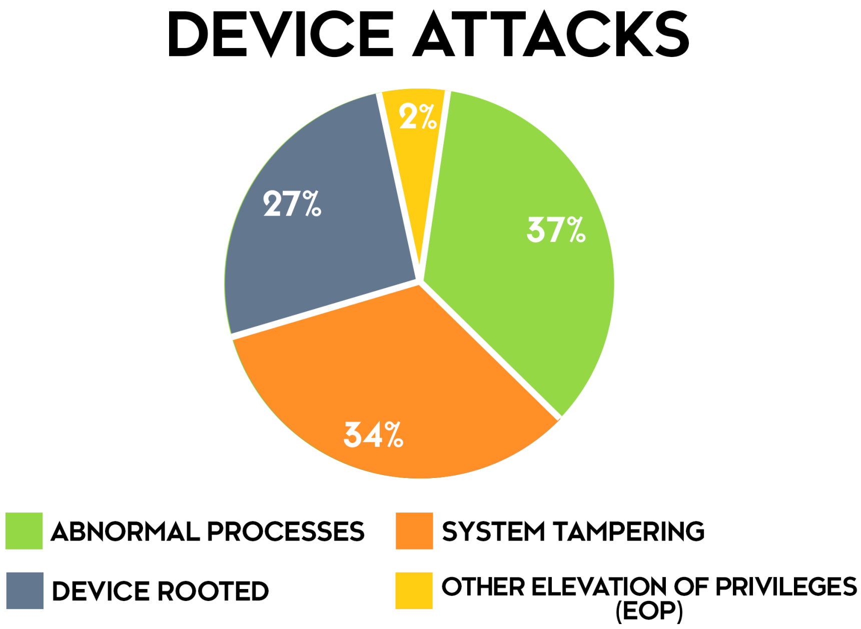
[1] Developer Options provides additional capabilities to assist in app development and testing, but can provide valuable information to assist in attacking the device (e.g., analyzing bug reports to find vulnerabilities).

[2] USB Debugging allows a user to actively debug an app. Attackers can use the same information to find vulnerabilities to exploit.

Key Finding: *0.1% of enterprise mobile endpoints detected compromise / elevation of access, but that number is a fraction of the real number of impacted devices in the wild.*

- 0.1% of enterprise mobile endpoints detected compromise attempts
- While device compromises are the ultimate goal, they are not the first/only step in a mobile attack "kill chain". In fact, the other mobile vectors (e.g., network, app and phishing attacks) all proceed and contribute to the delivery of device exploits. Since Zimperium solutions (powering this analysis) stop attacks at the first step in any kill chain, unprotected endpoints in the wild will have significantly more compromises.

Key Finding: *Three techniques accounted for 98% of attackers' device compromise attempts.*



Key Finding: *Malicious Profiles are more dangerous than malware on iOS[3]; profiles provide elevated access and are not vetted to the same extent as apps entering the App Store.*

MOBILE SECURITY NEWS

Facebook's WhatsApp Vulnerable to Remote Code Attack

Summary
A Facebook's WhatsApp vulnerability allows attackers to remotely run malicious code on a device without the user's permission or awareness

First Appearance
May 2019

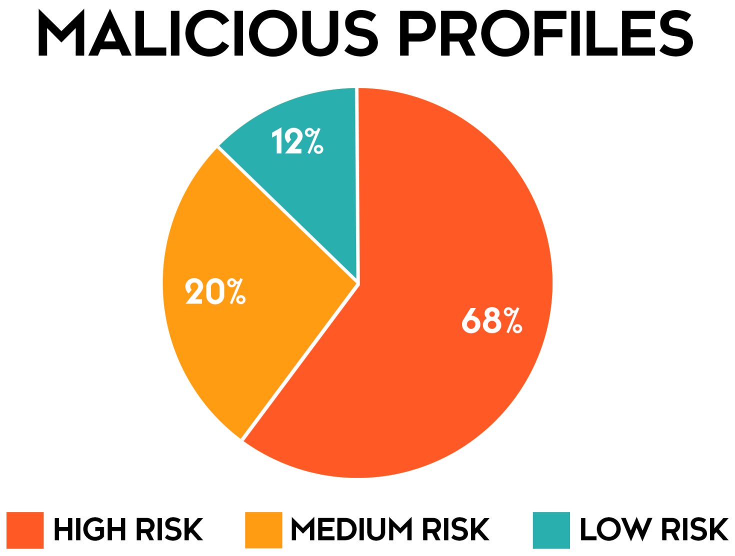
Impacts and Consequences
This type of device compromise allows attackers to control device functions such as microphone, camera, location and photos, creating serious privacy concerns

Sample Coverage:
ZIMPERIUM.

[3] This could be changing. Please see the "Supreme Court Green Lights Suit Against Apple" sidebar in the App Threat section.

- 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.

Key Finding: *In a sample of over 200K malicious profiles detected, the majority (68%) were considered "high-threat", meaning they had elevated access that could lead to data exfiltration or full compromise.*



MOBILE SECURITY NEWS

Hackers Abuse Legit Certificates to Compromise iOS

Summary
Cybercriminals lure iOS users into downloading a malicious profile, which the criminals then use to offer a whole store filled with compromised apps, bypassing Apple scrutiny

First Appearance
Feb 2019

Impacts and Consequences
Once installed, malicious profiles (enterprise certificates that are being abused) elevate privileges on an iOS device so hackers can do whatever they want

Sample Coverage:

THE VERGE

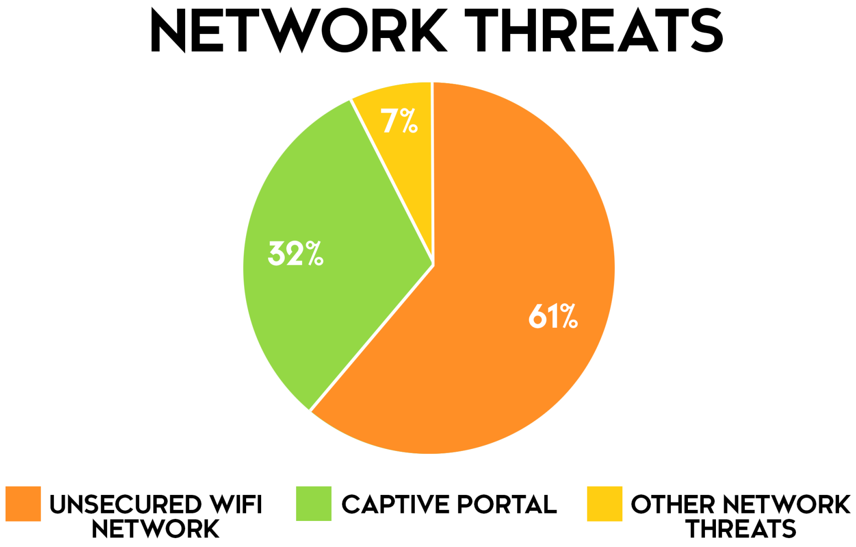
NETWORK THREATS & ATTACKS

Network Threats:

Risky networks and network activities can enable 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 so far in 2019:

Key Finding: *32% of enterprise mobile endpoints encountered risky networks.*

Key Finding: *61% of network threats were unsecured and unencrypted WiFi networks.*



Key Finding: *32% of network threats were captive portals that can be used to deliver exploits.*

Key Finding: *7% of network threats enabled reconnaissance scans of devices or attempted to redirect user traffic to unexpected (often dangerous) locations.*

Network Attacks:

As was mentioned in "The Forest" section above, network attacks dominated in 1H19. This is not surprising considering Zimperium's enterprise solutions stop attacks at the first step of the kill chain, which is a network attack in the majority of cases. Here are some insights of the major network attacks analyzed by Zimperium so far in 2019:

MOBILE SECURITY NEWS

Top Security Event Hit by ~4K Threats per Day

Summary
Zimperium detected more than 17,000 network-based threat events during the 2019 RSA conference in San Francisco

First Appearance
March 2019

Impacts and Consequences
Even tech-savvy and security-conscious mobile device users can fall prey to increasingly sophisticated and targeted attacks

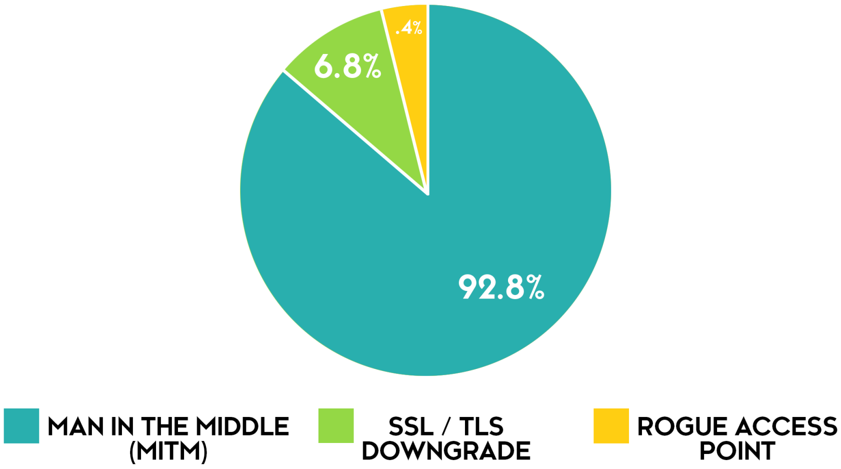
Sample Coverage:

ZIMPERIUM

Key Finding: *7% of enterprise mobile endpoints were exposed to network attacks.*

Key Finding: *93% of network attacks (and 86% of all attacks) were man-in-the-middle (MITM) variations wherein attackers hijack traffic to steal credentials/data or deliver exploits to compromise the device.*

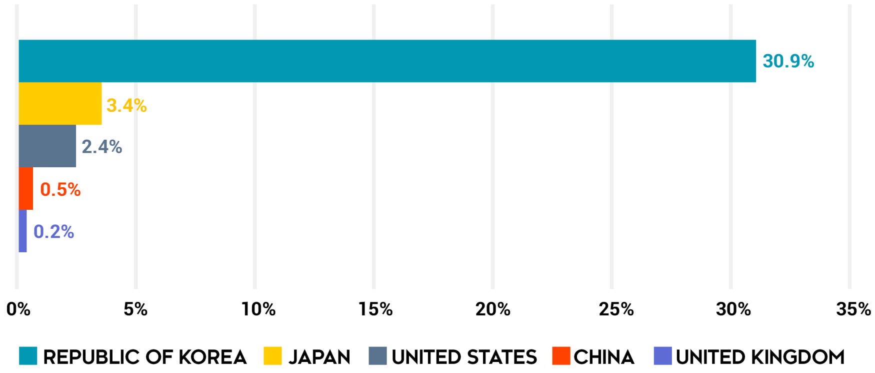
NETWORK ATTACKS



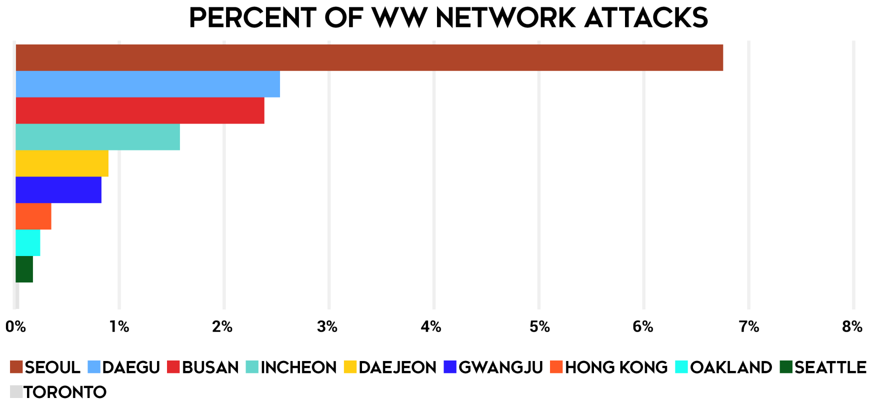
Key Finding: *ARP (Address Resolution Protocol) MITMs were attackers' favorite weapon with 48% of all network attacks and 45% of total attacks on enterprise endpoints.*

Key Finding: *31% of network attacks were detected in The Republic of Korea, demonstrating a heavy focus by a certain set of attackers. The remaining 69% were detected in dozens of other countries, showcasing the worldwide nature of the attacks.*

PERCENT OF WW NETWORK ATTACKS



Key Finding: *The Top 10 cities only accounted for 15% of total network attacks.*



APP THREATS & ATTACKS

App Threats:

Organizations are aware of malicious mobile app attacks, but fewer understand the threats that come from sideloaded apps or legitimate apps that have hidden security and privacy threats. With users being the admins of mobile endpoints, enterprises need a way to assess the threats of the installed mobile apps and create policies around their acceptable usage / existence. Here are some insights of the major app threats analyzed by Zimperium so far in 2019:

Key Finding: *5% of enterprise mobile endpoints had sideloaded apps from sources outside the authorized and vetted Apple App Store or Google Play Store. 36% of the Android devices had sideloaded apps versus only 2% of iOS ones.*

Key Finding: *70% of iOS apps had advertising capabilities and iOS Bluetooth beacon usage exploded to 69% of apps (from 38% at the beginning of 2019), both of which can lead to data leakage and other exploit opportunities.*

Key Finding: *24% of iOS apps passed sensitive information over the web unencrypted.*

Key Finding: *10% of analyzed apps leveraged external payloads not fully vetted by app stores.*

Key Finding: *16% of Android apps had hardcoded credentials to external systems.*

MOBILE SECURITY NEWS

Weather Channel App Allegedly Gathering Private Data

Summary
The city of Los Angeles filed suit claiming that the Weather Channel App covertly mined users' private data and resold it

First Appearance
Jan 2019

Impacts and Consequences
Enterprises must protect mobile users from mobile apps that can knowingly or unknowingly create security and privacy risks

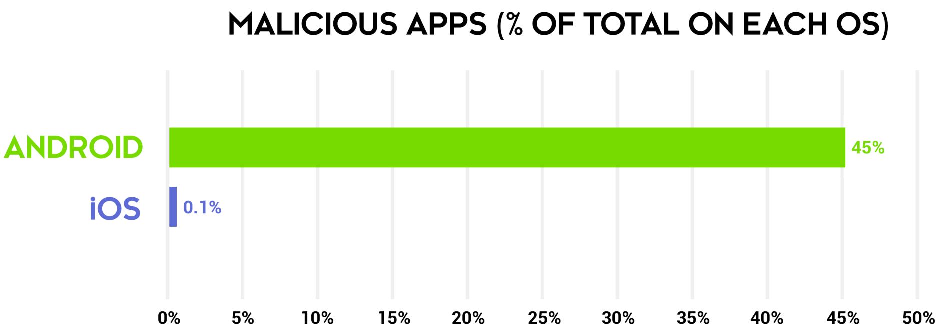
Sample Coverage:

App Attacks:

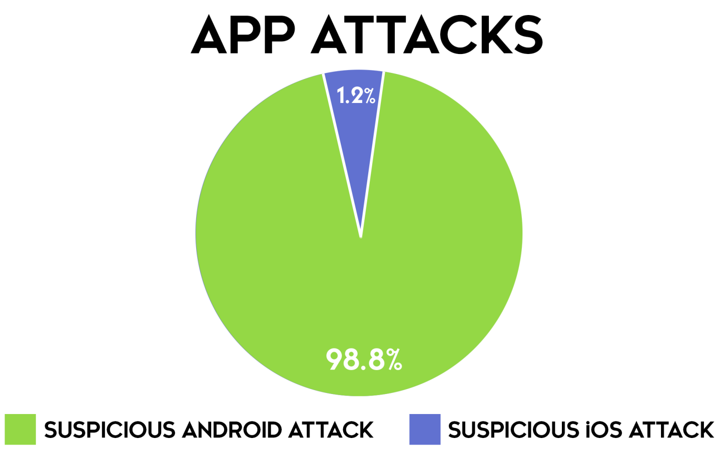
Because of the aforementioned unique architecture of mobile endpoints, the enterprise risk of malicious mobile apps are different than their counterparts on traditional endpoints. Because all mobile apps are in containers, they cannot interact with other apps to provide attackers with the coveted persistence discussed in the “Device Attack” section. The majority of malicious apps on mobile are designed for consumer fraud (e.g., BankBot and its variants). Even though malicious mobile apps are not the best way to attack an enterprise (that award goes to network attacks which 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. Here are some insights of the major app attacks analyzed by Zimperium so far in 2019:

Key Finding: *Zimperium’s machine learning-based engine, z9, detected thousands of malicious apps that were not in VirusTotal or any other repository.*

Key Finding: *Malicious apps were 45% of all attacks on Android versus less than 1% of ones detected on iOS.*



Key Finding: *98% of all detected malicious apps were on Android.*



MOBILE SECURITY NEWS

Scooters for Rent Vulnerable to Dangerous Hacks

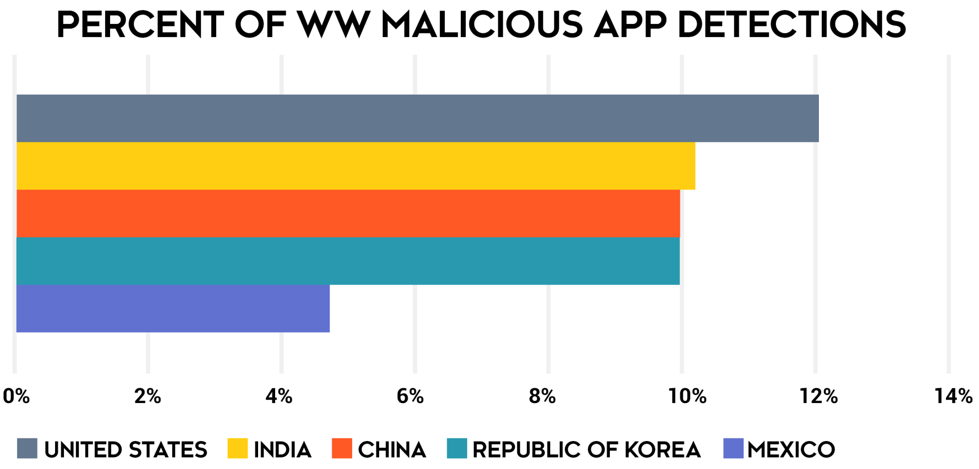
Summary
Scooters available to rent for use in urban areas are vulnerable to hacks that can make them accelerate and/or stop at dangerous speeds

First Appearance
2019

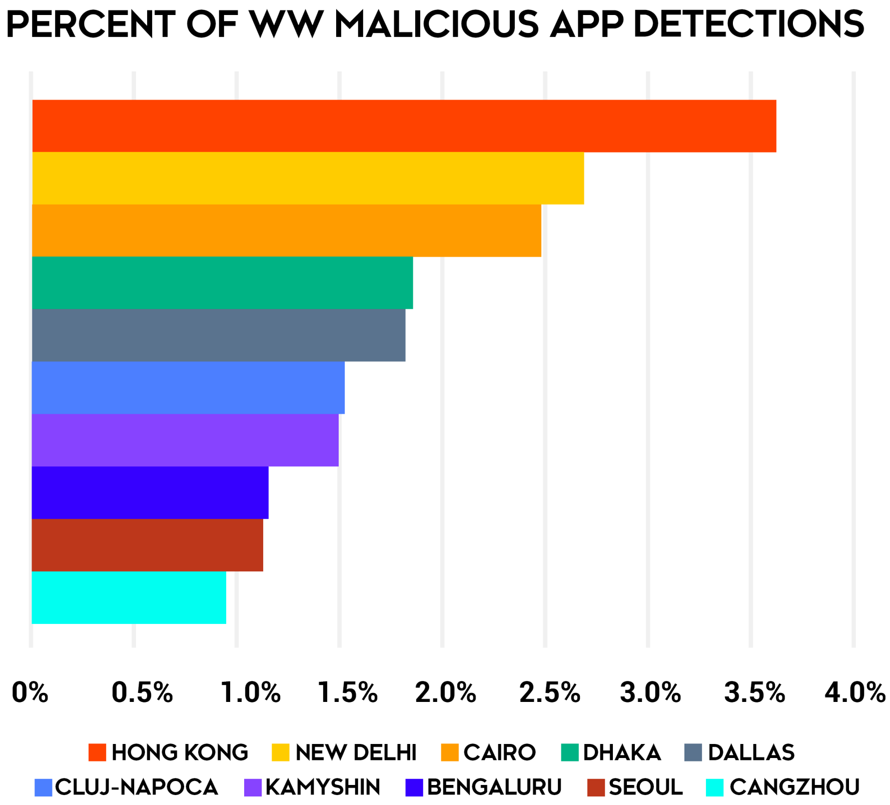
Impacts and Consequences
The intersection of Internet of Things and mobile devices is creating potential for mobile device compromises to initiate physical danger

Sample Coverage:
ZIMPERIUM.

Key Finding: *The top five countries accounted for almost half (47%) of mobile malware detections.*


PERCENT OF WW MALICIOUS APP DETECTIONS

Key Finding: Over *80% of the mobile malware detections occurred outside the top ten cities, reinforcing that mobile attacks are a worldwide epidemic.*


PERCENT OF WW MALICIOUS APP DETECTIONS

MOBILE SECURITY NEWS

Supreme Court Green Lights Suit Against Apple

Summary
A group of iPhone users won a decision for barring third-party apps on iOS

First Appearance
May 2019

Impacts and Consequences
If Apple is forced to allow third-party apps there will likely be a significant increase in malware; third party apps are the single largest source of malware for Android devices

Sample Coverage:

THE HILL

PHISHING THREATS & ATTACKS

According to the Verizon Data Breach Investigations Report[4], over 90% of all breaches begin with a phishing attack. Considering that almost two-thirds of emails are now read on mobile[5], mobile phishing is a real concern for enterprises. This is exacerbated by another factor: mobile endpoints are a primary place that users read their personal emails on systems 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 be diving even further into mobile phishing as our on-device, machine learning-based detections bring new insights.

CONCLUSION

Our research shows every organization that has protected its mobile endpoints with Zimperium has detected 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: *What percent of my devices are exposed to each type of threat and attack?* For the 1H of 2019, some of the more interesting findings included:

- 27% of enterprise mobile endpoints were exposed to device threats.
- Mobile OS vendors created patches for 440 security vulnerabilities. Apple patched 185 vulnerabilities compared to 120 during the same timeframe last year, an increase of 54%.
- 32% of enterprise mobile endpoints encountered risky networks, and 7% of enterprise mobile endpoints were exposed to network attacks.
- 36% of the Android devices has sideloaded apps versus only 2% of iOS ones.
- Malicious apps were 45% of Android attacks versus less than 1% of those detected on iOS. 98% of all detected malicious apps were on Android.

MOBILE SECURITY NEWS

Mobile-First Phishing Attack on Verizon Customers

Summary
Phishing links tailored to look like Verizon Customer Support emails sent to Verizon customers, complete with convincing landing page for click-throughs

First Appearance
April 2019

Impacts and Consequences
Attackers use phishing attacks to gain the target's login credentials and other data, including personally identifiable information (PII), creating both security and compliance issues

Sample Coverage:

threatpost

[4] Verizon Data Breach Investigations Report

[5] Adestra

The “State of Enterprise Mobile Security” Report will be updated quarterly 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 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.