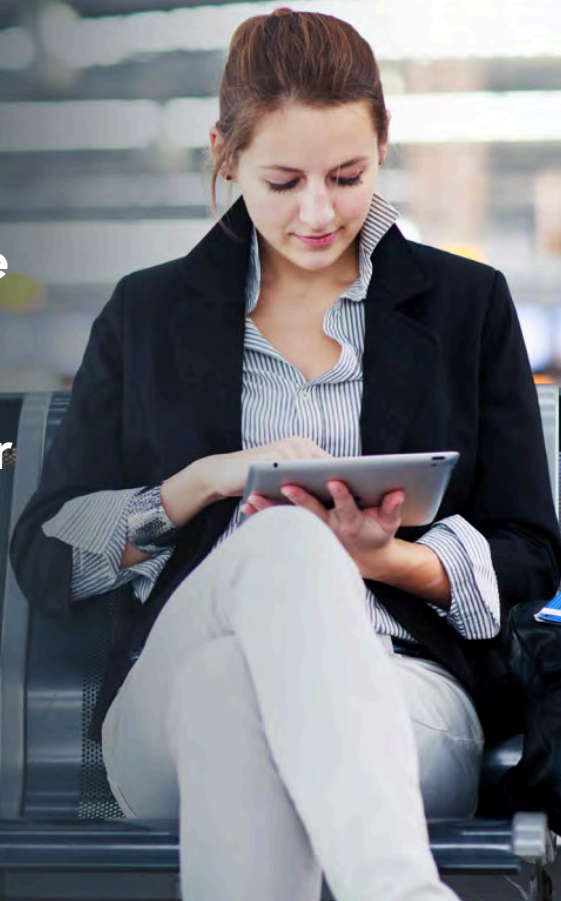




Zimperium Global Threat Report 1H-2018

Key Findings:

- ✓ Every customer sees mobile OS threats
- ✓ MITM attacks increased over last quarter
- ✓ One of every three devices detected a threat



Zimperium Global Threat Data

January 1 - June 30, 2018

During the first half of 2018, January 1 – June 30, zIPS-protected devices detected several types of mobile device risks and threats around the world. The risks and threats are categorized as follows (and often referred to as mobile threat “DNA”):

- **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



Mobile Threats Are Everywhere

Vulnerabilities Disclosed

Many times when mobile device vulnerabilities and malicious apps are disclosed, Zimperium receives frantic calls or emails. Inquirers ask, “Do you protect against BankBot, BroadPwn, KRACK, Meltdown, Spectre” and other attacks that get their own marketing campaigns. The answer has been consistently “yes” because our **z9 machine learning-based engine** detects attacks across all DNA vectors. Most mobile attacks are a combination of DNA vulnerabilities and techniques known as “kill chains”, and z9 has a proven track record of detecting these attacks at all three stages regardless of any creative ways they enter a device. If there is a hiccup in your OS, Zimperium will diagnose it immediately via our proprietary threat detection engine, z9.

This year, there have been several vulnerabilities disclosed to the market. Each was unique in how it enabled a sophisticated attacker to enter your device, app or grab your Wi-Fi traffic.

Meltdown and Spectre



Meltdown and Spectre

According to the team at Graz University of Technology that responsibly disclosed the new bugs, Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include passwords stored in a password manager or browser, personal photos, emails, instant messages and even business-critical documents.

Meltdown (CVE-2017-5754)

Meltdown is so named because the bug basically melts security boundaries which are normally enforced by the hardware. Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus data, of other programs and the operating system.

According to reports, every Intel processor since 1995 (except Intel Itanium and Intel Atom before 2013) are potentially affected by Meltdown. ARM processors are also affected, but AMD has stated there is "Zero AMD vulnerability due to AMD architecture differences."

Spectre (CVE-2017-5753 and CVE-2017-5715)

Spectre got its name from its root cause, speculative execution. As it is not easy to fix, its name implies that the researchers think it will haunt us for quite some time. Spectre breaks the isolation between different applications, and allows an attacker to trick error-free programs into leaking their data.

Almost every system is affected by Spectre. More specifically, Spectre vulnerability has been verified on Intel, AMD, and ARM processors. Additional exploits for other architectures are also known to exist. These include IBM System Z, POWER8 (Big Endian and Little Endian), and POWER9 (Little Endian).

How to protect mobile devices from Meltdown & Spectre vulnerabilities:

Operating System Patches

Apple and Google both stress that there are no known exploits impacting customers at this time.

To help defend against the bugs, Apple and Google have both released patches.

Apple users should be on iOS 11.2 to protect against Meltdown. According to Apple, while Spectre is extremely difficult to exploit, even by an app running locally on a Mac or iOS device, it can be potentially exploited in JavaScript running in a web browser. As a result, Apple plans to release mitigations in Safari to help defend against Spectre soon.

Android users should have security patch levels of 2018-01-05 or later, as documented on January 5 as part of the Android January 2018 security patch update.

Bluetoothd daemon

Vulnerabilities in Apple's bluetoothd daemon

As part of our platform research team in Zimperium zLabs, we investigated iOS mach message IPC, focusing on available services accessible from within the iOS sandbox. The goal of this effort was to assess potential opportunities to gain privilege escalation and escape the sandbox, which is a core part of a full iOS exploit chain.

We found 2 crucial vulnerabilities in the bluetoothd daemon on iOS, webOS and tvOS as part of CoreBluetooth. The first vulnerability is memory corruption in bluetoothd and the other is execution of arbitrary code on different crucial daemons.

The first vulnerability (CVE-2018-4095) is full relative (ASLR bypass) control on the stack in CoreBluetooth that leads to memory corruption over bluetoothd.

The second major vulnerability (CVE-2018-4087) leads to execution of arbitrary code on different crucial daemons in iOS by hijacking the session between each daemon and bluetoothd. Some of the impacted daemons are: SpringBoard, mDNSResponder, aggregated, wifid, Preferences, CommCenter, iaptransportd, findmydeviced, routined, UserEventAgent, carkitd, mediaserverd, bluetoothd, coreduetd and so on.

ZipperDown

ZipperDown Vulnerability: 100M iOS Users at Risk

Security researchers from iOS jailbreak firm, Pangu Lab, announced a vulnerability that they believe affects around 10% of all iOS apps. In a blog on its newly created information site, <https://zipperdown.org/>, Pangu stated that its researchers noticed “a common programming error, which leads to severe consequences such as data overwritten and even code execution in the context of affected Apps.” Pangu calculated that the infected apps may expose 100 million users or more. To avoid leaking the details of the programming error, Pangu named it “ZipperDown”.

What follows is a brief description of the vulnerability, and then a description of how zIPS (powered by the most effective and complete mobile machine learning engine in the world, z9) detects exploitation attempts on the device. The end result is that zIPS users are safe without any updates.

Preliminary ZipperDown Analysis

According to Pangu, “To protect the end-users, the detail of ZipperDown is not available to the public for now.” However, our researchers have discussed the vulnerability / programming error with Pangu, and believe that the issue lies in a 3rd party library that many apps are using. It is our team’s assessment that ZipperDown is not about malware, but about a vulnerability being exploited in several apps via a MITM on the network.

How Zimperium Helps Combat ZipperDown

Zimperium zIPS, powered by z9, detects MITMs and the exploits that can leverage ZipperDown, and can prevent them from executing via customer-defined policy enforcement.

Zimperium's on-device, machine learning-based detection has many advantages. One of which is Zimperium's full "kill chain" detection, wherein z9 detects attacks at multiple steps, without any updating or signatures. In this case, z9 detects MITMs and any exploits attempting to elevate privileges and compromise the device.



Update
on
Updates

For Apple, Google



Security Updates and Patches

During the first half of 2018, Apple released major and minor updates to iOS 6 times. Collectively, these security updates repaired 110 CVEs ranging from minor graphics updates to major browser and kernel updates. In 2017 there were 387 CVEs awarded. This matched the highest ever total for iOS in a single year (2015). Apple is very effective at pushing security updates to phones and making the latest patches available. However, users are still required to update to the latest version of the operating system.

Researchers from Zimperium's zLabs Team contributed several iOS updates in the first half of 2018. Adam Donenfeld and Rani Idan provided research in the graphics driver and core bluetooth resulting in patches being issued in the iOS 11.2.5 update.

Google released 6 Android Security Bulletins for the time period January 2018 through June 2018. Collectively there were updates to 495 CVEs with 48 of these deemed critical. Google notified users about security patches for Meltdown and Spectre in the [January 2018 update](#). This was a very critical update to fix CPU vulnerabilities and at the hardware level.

The [April 2018 update](#) included 311 CVEs including many dating back to 2014 for Qualcomm firmware. Updates to the vulnerabilities in the Qualcomm components were shared by Qualcomm with its partners through Qualcomm AMSS security bulletins or security alerts between 2014 and 2016. They were included in the April Android security bulletin in order to associate them with a security patch level.



Which Devices
Were Attacked?

How?
When?

Device Risks and Threats

We analyzed all of the mobile devices in our environments and have noticed enterprise customers continue to update devices with available security patches. We noticed fewer devices remain on older versions of each OS and vulnerable to known exploits than previous quarters. Even though many of our customers have EMM packages that monitor OS versions, they don't necessarily update the devices as soon as **security patches become available**.

We look at each OS separately since each has its own ecosystem and update schedule. iOS devices constitute the majority of our customers devices and we noticed the updates to these devices get delivered quickly. The latest major update to iOS is 11.4 release on May 29, 2018. Over half of iOS devices in our managed environments (51.9%) have the latest major update installed. The remaining devices are one or two versions behind the latest. There are 26.5% of iOS devices on version 11.3 with the remaining 21.5% on 11.2 or before.

Most of the Android devices in our environments run Android 6 (Marshmallow). Sixty-five (65.7%) percent of the devices are on Marshmallow followed by 16.4% on Android 7 (Nougat). Many analysts advise Marshmallow is the lowest version enterprises should allow inside the network. Thirteen percent (13.8%) of Android devices are on the latest version, Android 8 (Oreo). The remaining 4% of Android devices run Lollipop or prior versions of the operating system.

We look at how healthy these devices are in terms of how they are configured as well. We consider devices a high risk when **certain privacy and security settings are disabled**. Some of the high risk settings we investigate are whether or not Developer Options is enabled, whether a device is jailbroken or rooted, and necessary privacy settings remain on like encryption and PIN codes.

38%
of devices
introduce
unnecessary
risk.

Extremely risky devices disable code signing, allow apps from unknown sources or have malicious profiles on the device. Just over 1% of these devices were found to have malicious iOS configuration profiles that can manipulate the device to possibly steal data. We continue to see these profiles associated with apps deceiving users during installation in order to compromise the device or install RATs (Remote Access Trojans).

We measure static configuration risk and active threats independently since mobility teams often manage separate policies based on the device risk, user profiles, or roles. They want to know **whose devices are most risky** so they can put them in special groups or label them differently. Customers, of course, want to know **which actual devices were attacked, how and when**.

For the first half of 2018, customers recorded threats on 31% of active devices. Threat severity levels are configured by each customer based on their risk tolerance and are not called out in this report. One customer may remediate a threat automatically whereas another may mark it for further investigation. Alarming, we detected nearly 4% (3.5%) of devices containing apps scanning internal networks for surveillance reasons or had detected a rogue access point. These facts clearly state cyber criminals are increasingly using corporate mobile devices for surveillance purposes.



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 preliminary step in a more advanced attack.

For the first half of 2018, our data indicates one of every seven devices detected a MITM attack (14.88%). This is consistent with the rate we have recorded in other reporting periods in previous reports. Note, detecting a MITM does not indicate there was a successful attack. It does however, indicate a successful MITM attempt. Had the user not installed the ZIPS mobile threat defense app on their device, **the attack would not have been detected or recorded**. Unless users have a mobile threat defense app that can detect the attack on their devices in real-time (e.g., ZIPS), the wireless connections can be rerouted to a proxy and their data may be compromised. The compromised data can be used as part of an attack on the user, their employer or fraud.

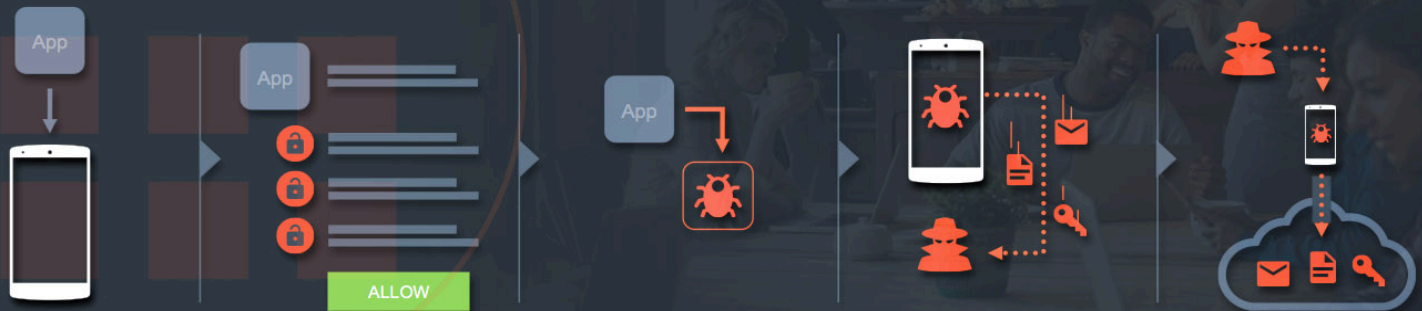
Rogue access points, which are wireless access points that have been installed on a secure network without explicit authorization from a local network administrator, are another common type of network attack that reroutes traffic. Rogue access points can be placed anywhere and typically follow trusted naming conventions to capture traffic from potential targets. For example, a rogue access point near a hotel or office location can mimic the actual name in order to deceive unsuspecting victims.

Nearly 2%
of devices
connected to a
rogue access
point during this
period.

zIPS is able to detect these rogue access points, report back to the corporate security teams and automatically terminate the session if the security policy dictated and configured that action.

Additional rogue access points were detected nearby but those mobile devices with zIPS did not actually connect. The security teams at each customer were notified there were rogue access points attempting to deceive corporate employees.

App Threats



App Threats

Enterprises and users continue to be concerned about mobile apps and mobile malware since they have been trained by legacy antivirus software packages. They scan and look for a known malware file and remove it.

The issue with this logic on mobile is the mobile operating systems **evolve and add features very rapidly**. The mobile operating systems add millions of lines of code in a year and therefore introduce unintended consequences, bugs and vulnerabilities. In 2017, there were more CVEs registered for Android and iOS than all of 2016 and 2015 combined. In 2017 there were 1228 CVEs awarded for the mobile operating systems. Over half of these CVEs received scores of 7+ or greater indicating the vulnerabilities are severe and exploitable. We expect this trend to continue into 2018 as the mobile operating systems continue to mature and more features are continuously being added.

Mobile malware and malicious apps are a high concern. However, they are the least prevalent threats amongst Zimperium customer environments.

Our customers are some of the most security conscious companies in the world in telecommunication, banking, financial services, management consulting, utilities, government and technology industries. These companies continuously refine their security policies and training programs to reduce IT risk. Despite all of the training and awareness programs, users still find routes around security policies and controls. For these reasons, our customers choose to reduce their risk posture by installing mobile security on employee and corporate-owned devices.

During the first half of 2018, Zimperium customers identified known malicious apps in their environments on **thousands of devices**. Android devices were more likely to have known malicious mobile malware on the devices. Malware inside apps was found on 3.5% of devices. Over 80% of the apps found with malware had access to internal networks and were scanning nearby ports. This type of surveillance is indicative of larger malware attacks.

In February 2018, a Zimperium customer downloaded a fake version of the legitimate BBC News app from Google Play. This app was previously unknown malware. Zimperium classified this app as malware via its threat detection technology and disclosed the findings on March 1, 2018.

iOS malware delivered via an app is less common at 0.1 % of total devices. iOS devices are more likely to have malicious profiles present on devices. These malicious profiles are often delivered to devices inside of free apps or disguised as companion apps. In late 2017, a Zimperium user paid \$15.95 for an app in the App Store that offered several games. After purchasing the app, this user received a prompt to download an "installer" or "helper" app in order to provision the games. This "installer" app was later found to be a malicious profile that compromised the device. The malicious profile enabled the device to download apps from outside the App Store without jailbreaking the device. The security team at this customer notified the user and provided him with instructions on how to remediate the attack.

The information provided in this report summarizes information on mobile threats detected and remediated with Zimperium technology. Each customer operates an independent environment and captures detailed forensics on each threat to their corporate or BYO devices. If you would like to collect similar data and gather intelligence on your mobile workforce, [contact us](#) today for an evaluation or an assessment of your company's mobile risk posture.

Sources:

Apple iOS 11.2.2 update

Apple iOS 11.2.5 update

Apple iOS 11.2.6 update

Apple iOS 11.3 update

Apple iOS 11.3.1 update

Apple iOS 11.4 update

Android Security Bulletin—January 2018 [https://source.android.com/security/](https://source.android.com/security/bulletin/2018-01-01)

[bulletin/2018-01-01](https://source.android.com/security/bulletin/2018-01-01) Android Security Bulletin—February 2018 [https://source.android.com/](https://source.android.com/security/bulletin/2018-02-01)

[security/bulletin/2018-02-01](https://source.android.com/security/bulletin/2018-02-01) Android Security Bulletin—March 2018

<https://source.android.com/security/bulletin/2018-03-01>

Android Security Bulletin—April 2018

<https://source.android.com/security/bulletin/2018-04-01>

Android Security Bulletin—May 2018

<https://source.android.com/security/bulletin/2018-05-01>

Android Security Bulletin—June 2018

<https://source.android.com/security/bulletin/2018-06-01>

CVE Details

https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

CVE Details

https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Zimperium, Inc.

<https://www.zimperium.com/>