ZIMPERIUM®
MOBILE THREAT DEFENSE

Zimperium Global Threat Report Q4-2017

Key Findings:

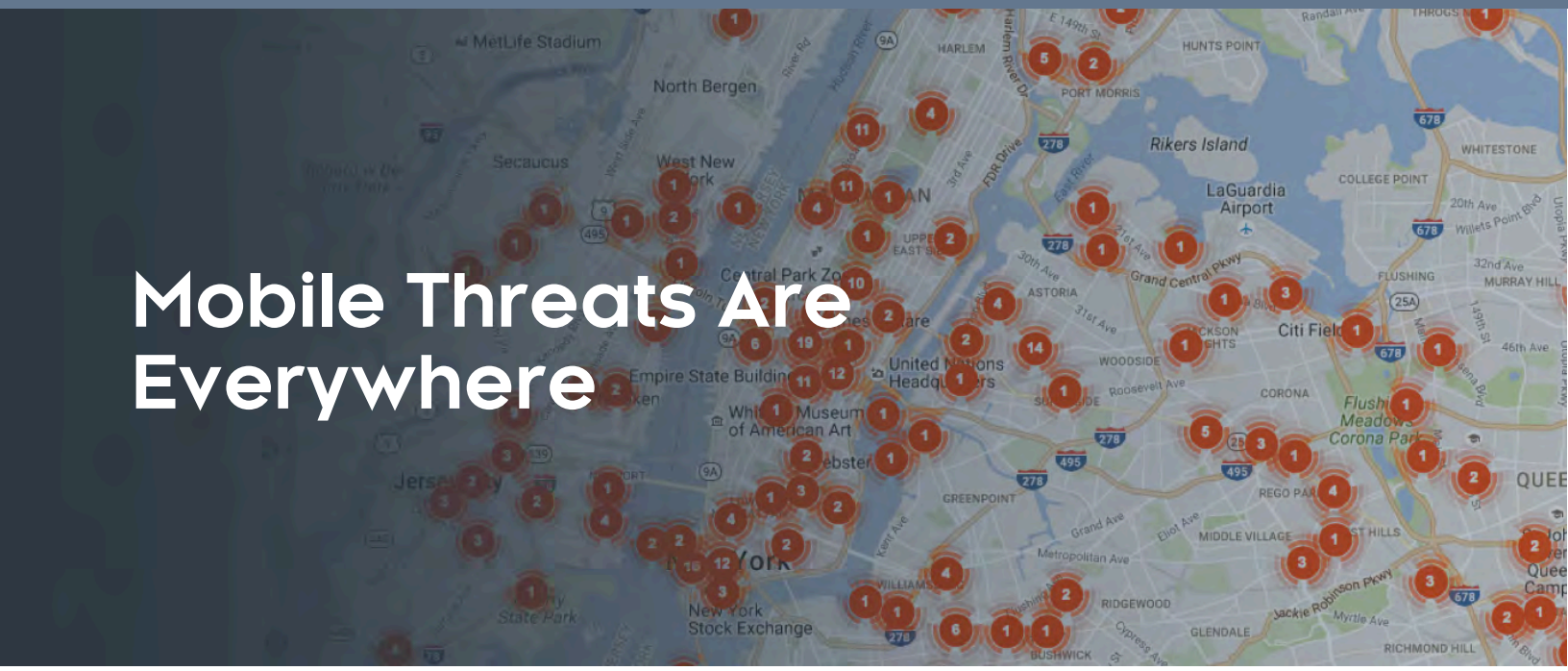
- ✓ Every customer sees mobile OS threats
- ✓ More mobile OS vulnerabilities in 2017 than 2016 and 2015 combined
- ✓ MITM attacks increased by 15% over last quarter

Zimperium Global Threat Data

October 1 - December 31, 2017

During the fourth quarter of 2017, October 1 - December 31, 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. They'll ask, "Do you protect against BankBot, BroadPwn, KRACK," and other attacks that get their own marketing campaigns. The answer has been consistently "yes" because of our **z9 machine learning-based engine** that 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 an hiccup in your OS, Zimperium will diagnose it immediately via our proprietary threat detection engine, z9.

Last quarter, there were several vulnerabilities disclosed to the market. Each were very unique in how it enabled a sophisticated attacker to enter your device, app or grab your Wi-Fi traffic.

BankBot Steals Mobile Banking Credentials

Android-targeting malware uses fake overlay screens to mimic existing banking apps and steal user credentials

BankBot

Distributed as benign apps in Google Play, BankBot is Android-targeting malware that uses fake overlay screens to mimic existing banking apps and steal user credentials. Earlier in 2017, more than 20 BankBot-infected apps were detected posing as entertainment and online banking apps. The newest BankBot variants targeted over 150 legitimate apps including apps from banks based in 27 different countries.

The latest version of BankBot operates if the device meets three conditions:

1. **The running environment is a real device.**
2. **The device location is not in Commonwealth of Independent States (CIS) countries.**
3. **An app of a targeted bank is installed on the device.**

Once it is installed and running on the device, BankBot phishes user credentials by:

- Checking the package information of apps installed on the device for one of the targeted bank apps.
- If one is found, BankBot connects to its C&C server, uploads the target's package name and label and sends a URL for the library that contains files used for the overlay webpage.
- BankBot monitors the device for the launch of any target bank app. The malware **displays the overlay page on top of the legitimate app** when the app runs.
- The overlay tricks the user into believing they are using the legitimate app, and phishes/ steals the user's credentials.
- BankBot has a unique variation for UAE banking apps. Before it shows the overlay page, BankBot requests the user's phone number, and the C&C server sends a pin code to the victim. After entering the pin, the victim is instructed to input bank details (two times, to make sure the attacker has valid credentials).

zIPS detects the BankBot malware, and can prevent it from executing via customer-defined policy enforcement.

An app containing our threat detection SDK, zIAP, could immediately terminate a user's session and/or flag the account for high fraud risk after the BankBot malware is detected or when there is an active attack from another threat vector.

KRACK Attacks

KRACK

KRACK (Key Reinstallation attaCKs, KRACKs) is a serious weakness in the WPA2 protocol. WPA2 secures all modern protected Wi-Fi networks including those used by smartphones. Attackers within physical range of a Wi-Fi network can exploit protocol weaknesses by using key reinstallation attacks. The attack works against all modern protected Wi-Fi networks and can be used to steal sensitive information such as usernames, passwords, messages, emails, photos, calendaring, and contacts information.

The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected.

How zIPS Helps

Zimperium customers can detect MITMs like KRACK through various detection techniques. With zIPS on your Android and iOS devices, **you will be notified if an attacker intercepts your Wi-Fi traffic** in order to read traffic.

If an attacker inserts himself between your device and your access point and attempts to decrypt your traffic, zIPs will alert you via standard MITM detection. Standard MITM detection in zIPS that apply to KRACK include but are not limited to:

- **Fake SSL Certificate MiTM** – Attack using a fake certificate where an attacker can hijack traffic and steal credentials or deliver malware to the device.
- **SSL Strip** – Man-in-the-Middle attack using SSL stripping allowing a malicious attacker to change HTTPS traffic to HTTP to hijack traffic, steal data or deliver malware to the device.
- **Traffic Tampering** – Man-in-the-Middle attack allowing a malicious attacker to change the content of the network traffic and deliver malware to the device.

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.

Skygofree

Skygofree

According to the researchers that disclosed the malware, here are the salient points of Skygofree:

- Only select individuals in Italy are being targeted, as are the malware's developers. Users are lured to a website where they're asked to update or configure their device configuration, allowing the malware to be dropped in the process.
- Skygofree offers attackers 48 different commands, enabling access to all services and information on the infected device.
- One advanced feature is the ability to use location services to use the device's microphone when the user is in a specific place.
- Contains the features and root access privileges of other spyware, e.g., capturing photos, contacts, text messages and monitoring the user's location.
- If the user has chosen to run battery-saving measures, Skygofree is able to add itself to the list of 'protected apps' in order to ensure it can carry on its malicious activity, even when the screen is off or the phone isn't active.
- The last known evidence of attacks is in October 2017.

How Zimperium Helps Defeat Skygofree

Zimperium zIPS, powered by our core machine learning-based engine, z9, detects the Skygofree malware, and can prevent it from executing via customer-defined policy enforcement. Additionally, exploits used by the malware to escalate privileges on the device are also correctly detected by z9.

Security Updates and Patches

During the fourth quarter 2017 and the first two months of 2018, Apple updated iOS 10 times. Collectively, these security updates repaired 72 CVEs. One of the most severe vulnerabilities updated included CVE-2017-13077 which allowed an attacker in Wi-Fi range to force nonce reuse in WPA unicast/PTK clients (Key Reinstallation Attacks - KRACK). Apple also provided security patches for CVE-2017-5754 (Meltdown). This allowed an application to possibly read kernel memory.

Researchers from Zimperium's zLabs Team contributed. Adam Donefeld 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 5 Android Security Bulletins for the time period October 2017 through February 2018. Collectively there were updates to 161 CVEs. Google notified users about security patches for KRACK in the November 2017 update and for Meltdown and Spectre in the January 2018 update.

Device Risks and Threats

We analyzed all of the mobile devices in our environments and have noticed enterprise customers continue 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 most important update to iOS is 11.2. This was a critical update since it fixed, KRACK, Meltdown and the 11.1.2 and below bugs that allowed exploits published by Google Project Zero and also made jailbreaks like LiberiOS and Electra possible. The 11.2 update was released on December 2, 2017. As of December 31, 2017, we found just over half of iOS devices (53.76%) had received this update. The remaining 46.24% of devices are considered vulnerable to known exploits and should be immediately updated.

Most of the Android devices in our environments run Android 6 (Marshmallow). Nearly seventy-five (74.9%) percent of the devices are on Marshmallow followed by 12.7% on Android 7 (Nougat). Many analysts advise Marshmallow is the lowest version enterprises should allow inside the network. There is a very small percentage (1.75%) of Android devices on the latest version, Android 8 (Oreo).

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.

Last quarter, there were 8.52% of devices that had at least one of the aforementioned concerns.

Extremely risky devices disable code signing, allow apps from unknown sources or have malicious profiles on the device. Just over 2% of all of the monthly active devices reported threats deemed extremely risky. 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 risk and active threats** since customers ask us to clarify these states in their mobile threat defense dashboards. 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 fourth quarter we saw active threats on 45.83% of active devices. Threat severity levels are configured by each customer based on their risk tolerance. One customer may remediate a threat automatically whereas another may mark it for further investigation. Alarmingly, we detected 2% of devices having access to internal networks for surveillance or had detected a rogue access point. These facts clearly state that cyber criminals are increasingly using corporate mobile devices for surveillance purposes.

Network Threats and Attacks

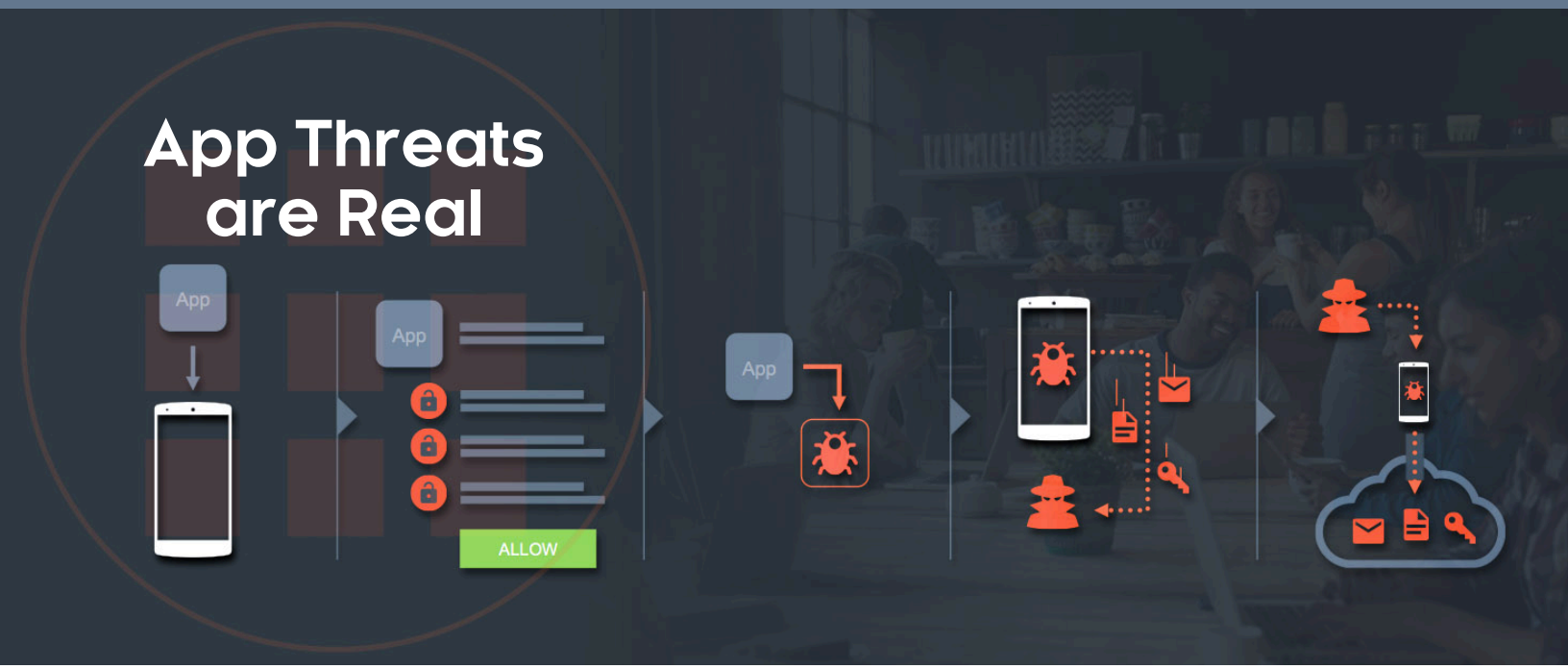
One of the most serious types of threats occurs when an attacker intercepts a mobile device's network traffic through techniques such as a man-in-the-middle (MITM) attack or a rogue access point. This gives the attacker **the ability to read and capture credentials, emails, calendars, contacts** and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

For the fourth quarter of 2017, our data shows over 10.35% of devices detected a MITM attack. This is a 15% increase over last quarter. In the third quarter of 2017, 8.95% of all devices detected a MITM. 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 zIPS Mobile Threat Defense on their device, **the attack would not have been noticed or recorded**. Unless users have a mobile threat defense app that can detect the attack on their devices in real-time (e.g., zIPS), their 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 1%
of devices connected to a rogue access point during this period.

zIPS was 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. Several more 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 are rogue access points attempting to deceive corporate employees.



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. 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 have been more CVEs registered for Android and iOS than all of 2016 and 2015 combined. In 2017 there were 1229 CVEs awarded. Over half of these CVEs received scores of 7 or greater indicated the vulnerabilities are severe and exploitable. We expect this trend to continue as the mobile operating systems continue to mature and more features are continuously being added.

Mobile malware and malicious apps are the least prevalent threats amongst Zimperium customer environments. Our customers are some of the most security conscious companies in the word in telecommunication, banking, financial services, management consulting and technology.

Over the last quarter, 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 2.2% of Android devices. In February 2018, a Zimperium customer downloaded a fake version of a BBC News app. 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. In late 2017, a Zimperium customer paid $15.95 for access to iOS games. After purchasing access to the games this user received a prompt to download the “installer” app in order to provision the games. This “installer” app later was found to be a malicious profile that compromised the device. The security team at this customer notified the user and provided him with instructions on how to remediate the attack.

If you would like to obtain forensic detail like the above for your enterprise devices, please contact us to set up the appropriate steps.

Sources:

Apple 11.0.2 update
Apple 11.0.3 update
Apple 11.1 update
Apple 11.1.1 update
Apple 11.1.2 update
Apple 11.2 update
Apple 11.2.1 update
Apple iOS 11.2.2 update
Apple iOS 11.2.5 update
Apple iOS 11.2.6 update
Android Security Bulletin October 2017 https://source.android.com/security/bulletin/2017-10-01
Android Security Bulletin November 2017 https://source.android.com/security/bulletin/2017-11-01
Android Security Bulletin December 2017 https://source.android.com/security/bulletin/2017-12-01
Android Security Bulletin January 2018 https://source.android.com/security/bulletin/2018-01-01
Android Security Bulletin February 2018 https://source.android.com/security/bulletin/2018-02-01
Zimperium, Inc.