ZIMPERIUM®
MOBILE THREAT DEFENSE

Zimperium Global Threat Report Q3-2017

Zimperium Global Threat Data

July 1 - September 30, 2017

During the third quarter of 2017, July 1 - September 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

24% of organizations suffered a mobile security breach, primarily driven by malware and malicious Wi-Fi

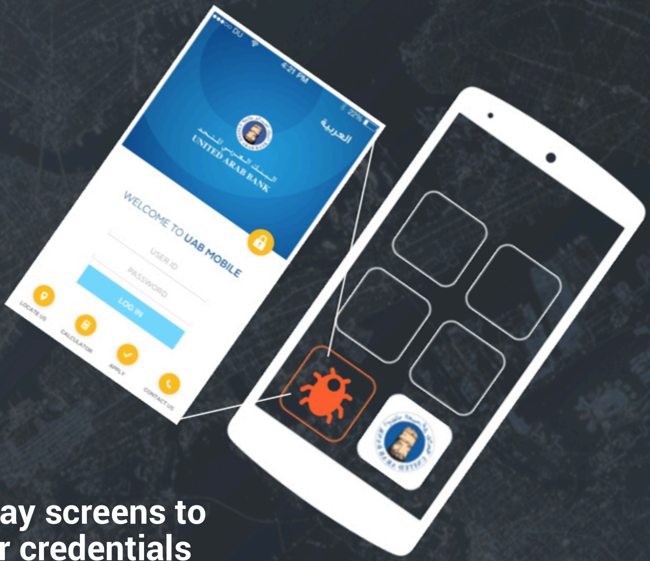
43% were unsure if mobile security incidents had occurred[1]

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 anomaly 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 was very unique in how it enabled a sophisticated attacker to enter your device, leverage an app or listen to your Wi-Fi traffic.

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.[2]

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

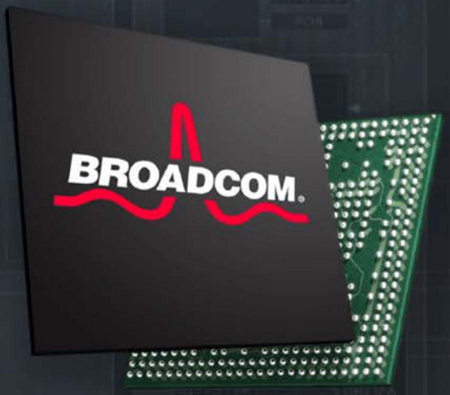
1. **The running environment is a real device.**
2. **The device location is not in Commonwealth of Independent States (CIS) countries.**
3. **An app of a targeted bank is installed on the device.**

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).

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.

Devices Need Protected from Broadpwn



BroadPwn

Broadpwn is a vulnerability (CVE 2017-9417) in the Broadcom Wi-Fi chip used in all iPhones and most Android phones. Security researcher, Nitay Artenstein, discovered a crucial bug in Broadcom's "association" process, which allows phones to search for familiar Wi-Fi networks before they connect to one. The bug allowed an attacker to corrupt the handshake process **between the device and the access point**. With a carefully crafted response, the access point could send data that corrupts the module's memory, overflowing into other parts of the memory to run as commands.[3, 4]

How to protect your devices from Broadpwn vulnerability

Both Apple and Google have updated iOS and Android operating systems for CVE 2017-9417. You should update your iOS and Android devices to the latest version to remove this vulnerability from your devices. For more information you can refer to the July 2017 Android Security Bulletin and Apple's Security update for iOS 10.3.3.[5, 6]

No app, including zIPS, can detect the actual attack on the Wi-Fi hardware itself since apps do not have privileged access to device hardware. However, zIPS detects sophisticated exploitation attempts on the device via its behavioral based threat detection technology.

Since there is no access to the system log, security apps like zIPS cannot view Wi-Fi diagnostic messages that could lead to detecting anomalous behavior. Detecting an abnormal change in the Wi-Fi connection could be another possible way to determine if a potential exploitation is in progress. However, we have not seen that sort of abnormal change occur.

Again, this applies to the exploit itself. If an attacker wants to compromise a device, then there are additional steps required--**steps that zIPS' on-device detection of DNA (device, network and app) threats will detect** in order to activate remediation procedures. As just one example, a kernel exploit would trigger a "System Tampering" warning since an attacker will normally disable code signing during the exploit attempt.

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 .[7, 8]

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.

Update on Updates

For Apple, Google

Security Updates and Patches

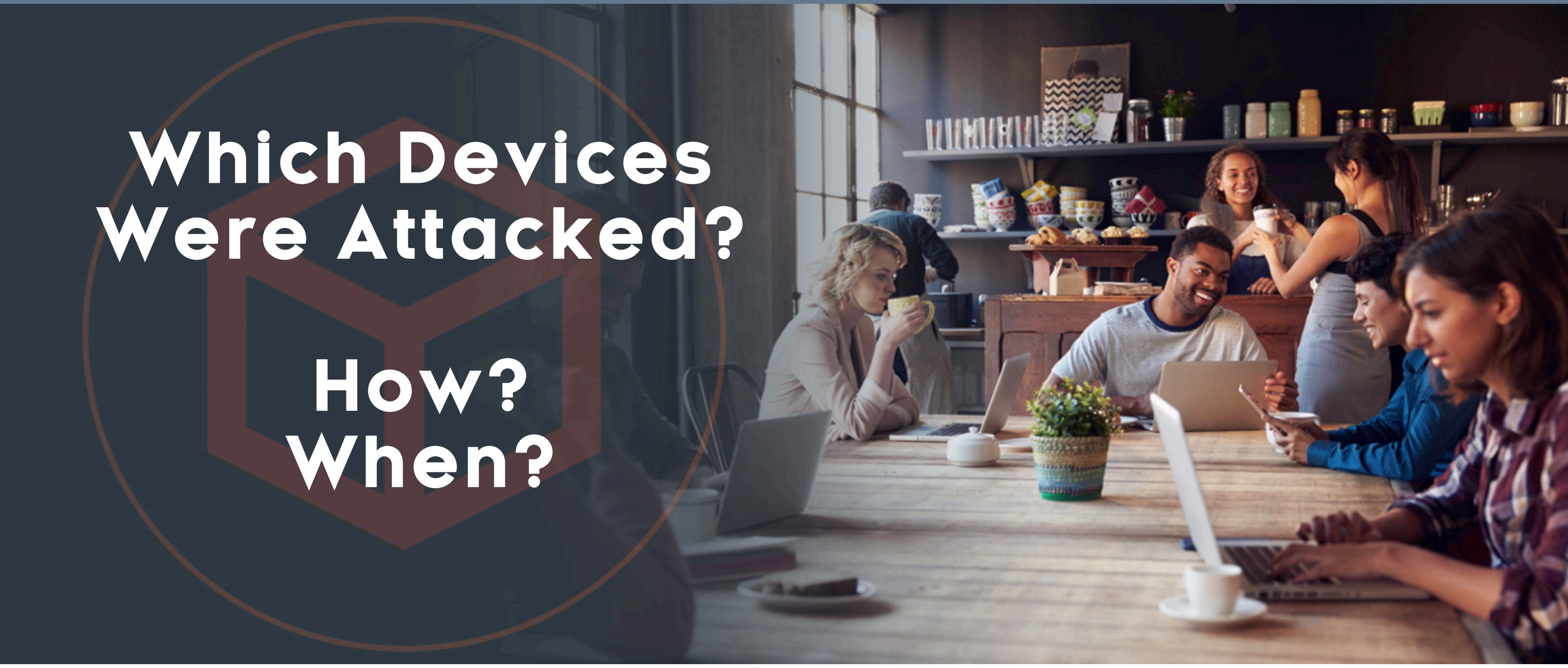
Apple and Google both updated their mobile operating systems multiple times from July through September. Apple released 3 updates in the quarter in iOS versions 10.3.3, 11.0, and 11.0.1 to patch over one hundred vulnerabilities. In total, there were 139 individual CVEs patched in these three security updates.

The most significant update according to Zimperium researcher, Adam Donefeld, is the 11.0 update. "It is extremely important to update to 11.0 to avoid Wi-Fi bugs discovered by Google's Project Zero. Google Project Zero also released an exploit for several of the vulnerabilities, which means anyone can attack iPhones up to version 10.3.3." The update was to patch the BroadPwn vulnerability mentioned earlier. Updating your devices to 11.0 removes the chances your devices can be exploited via BroadPwn.

The monthly security updates from Google on Android for the third quarter collectively contained updates for 281 CVEs. In the July bulletin there are updates to Qualcomm closed source vulnerabilities going back to 2015. Other updates in the August and September bulletins patched many Broadcom components (BroadPwn).[9, 10, 11]

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 are cleaning up their devices. 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 iOS and Android separately since each has it's 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 11.0 which was released on September 19, 2017. At the end of the quarter, we took a snapshot to identify which devices were current and which remained on older versions. We found 39.2% of devices had installed security patches inside of the 11 days after 11.0 became available. Almost half of iOS devices (49.3%) remained on 10.3.X versions and the remaining 11.5% of the devices were on versions prior to 10.3.

Most of the Android devices in our environments run Android 6 (Marshmallow). Eighty-two (82.1%) percent of the devices are on Marshmallow followed by 11.5% 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%) 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, 8.4% of devices 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 active devices reported threats deemed extremely risky. These devices were found to have malicious iOS configuration files that can manipulate the device to possibly steal data. We continue to see these files associated with third party VPN apps. Users download free third party VPN apps to circumvent security and compliance policies.

We **measure risk and active threats** since customers ask us to break it down like this 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 third quarter we saw active threats on 58.6 % of active devices. Our threat 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 found Elevation of Privilege (EOP) and System Tampering threats on over 2% of devices.[12]

Wi-Fi MITM
Attacks are Real
coffee_wifi
CONNECTED!
LOGIN

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 third quarter of 2017, our data shows over 9% of devices detected a MITM attack. This is double the rate over last quarter. In the second quarter of 2017, 4% 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.[12]

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.

Nearly 1%
of devices detected a rogue access point after connecting to it.

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.

App Threats are Real

App Threats

We get a lot of questions about mobile app security. Enterprises and users are concerned about mobile apps because they have been trained over the years 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**. In the first 3 quarters of 2017, there have been more CVEs registered for Android and iOS than all of 2016. We expect this trend to continue for years as more features are being added to maturing mobile OS platforms.

Mobile malware is the least prevalent threat 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 several malicious apps in their environments on **thousands of devices**. Android devices were more likely to have malicious mobile malware on the devices. Mobile malware inside apps was found on 4.4% of android devices. iOS malware delivered via an app is less common at 0.1 %. iOS devices are more likely to have malicious profiles present on devices. These malicious profiles are often delivered to devices inside of free apps like the VPN apps mentioned earlier.[12]

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

1 -2017 Mobile Security Spotlight

2 -http://blog.trendmicro.com/trendlabs-security-intelligence/bankbot-found-google-play-targets-ten-new-uae-banking-apps/

3 - https://blog.exodusintel.com/2017/07/26/broadpwn/

4 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9417

5 - https://source.android.com/security/bulletin/2017-07-01

6 - https://support.apple.com/en-us/HT207923

7 - https://www.krackattacks.com/

8 - https://www.cnet.com/au/news/krack-wi-fi-attack-patch-how-microsoft-apple-google-responding/

9 - The Mitre Corporation, Common Vulnerabilities and Exposures (CVE®)

10 - Apple, Inc.

11 - Google, Inc.

12 - Zimperium, Inc.

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