ACHILLES: SMALL CHIP, BIG PERIL

New Vulnerabilities Found by Check Point <research>

Tomas Vobruba | Check Point SE Slovakia

cp<r>
CHECK POINT RESEARCH

WHAT IS CP<R>?

Trends

Research and analysis of trends and technical developments in the cyber threat landscape

Detection

Improving detection of ongoing threats and alerting of future ones

Analysis

Advising product teams through analysis of malicious artifacts.

Spread The Word

Spreading the word of cybersecurity in Check Point

CPR'S LATEST FINDINGS IN THE MOBILE WORLD

Coronavirus-related mobile malware

Lucy's Back: Ransomware goes Mobile

MDM used to distribute Cerberus malware

SandBlast Mobile keeps you protected

WHAT WE FOUND

cp<r>
CHECK POINT RESEARCH

Over 400 vulnerabilities on Qualcomm's Chipset threaten mobile phones' usability worldwide

SAMSUNG

LG

SONY

xiaomi

ONEPLUS

Lenovo

Google Pixel

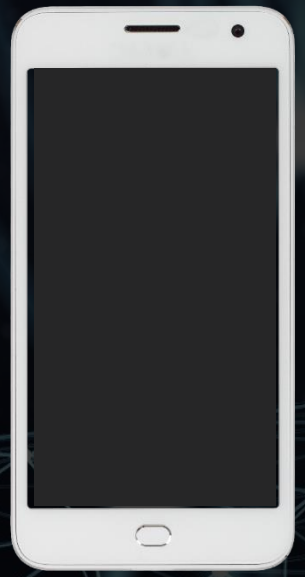
WHAT ARE THE RISKS?

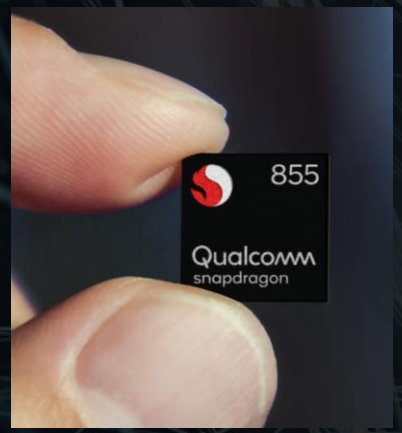
Turn the phone into a spying tool

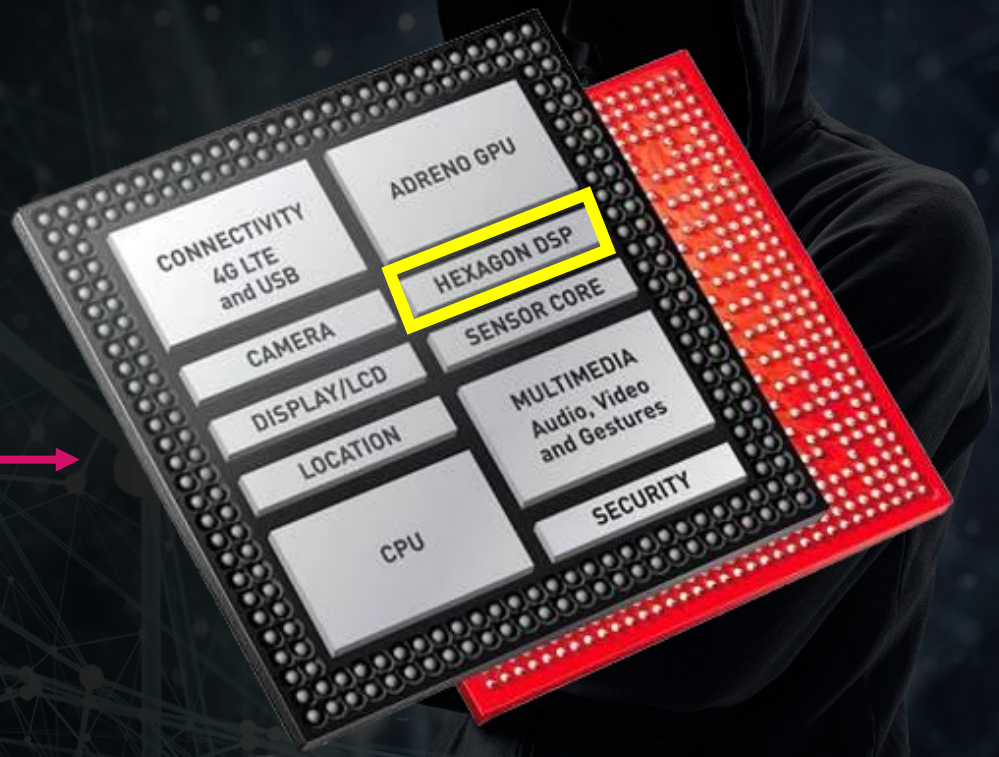
Render the phone unresponsive

Malicious code can hide activities and become un-removable

QUALCOMM SoC (System on Chip)



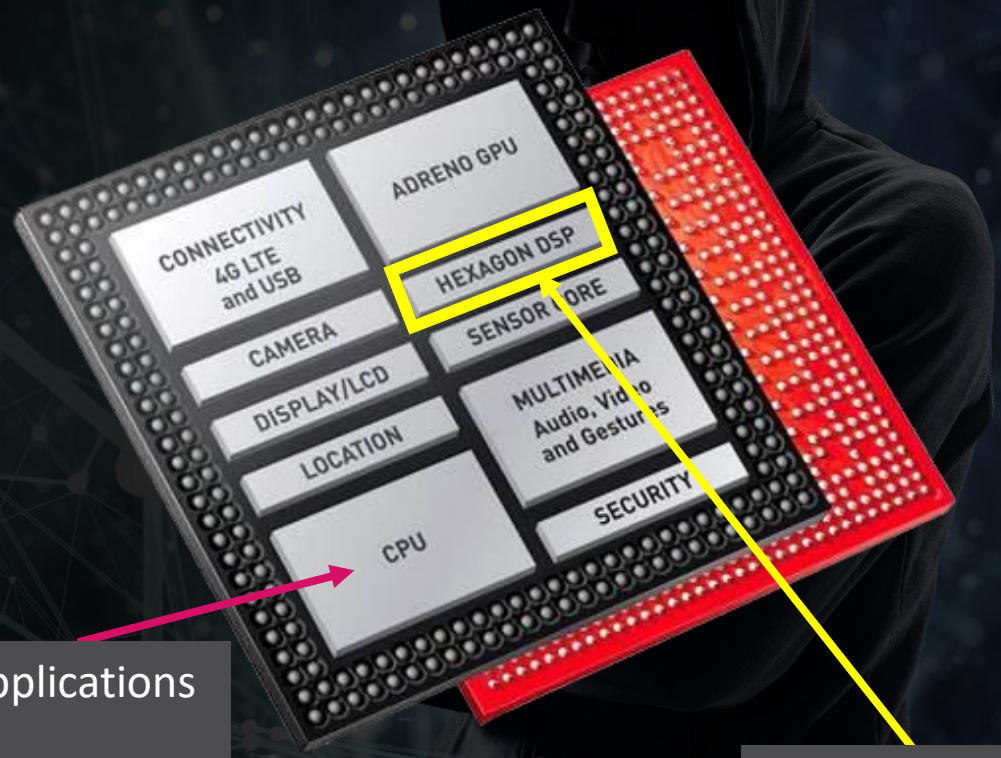




https://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/

WHAT IS A DSP?

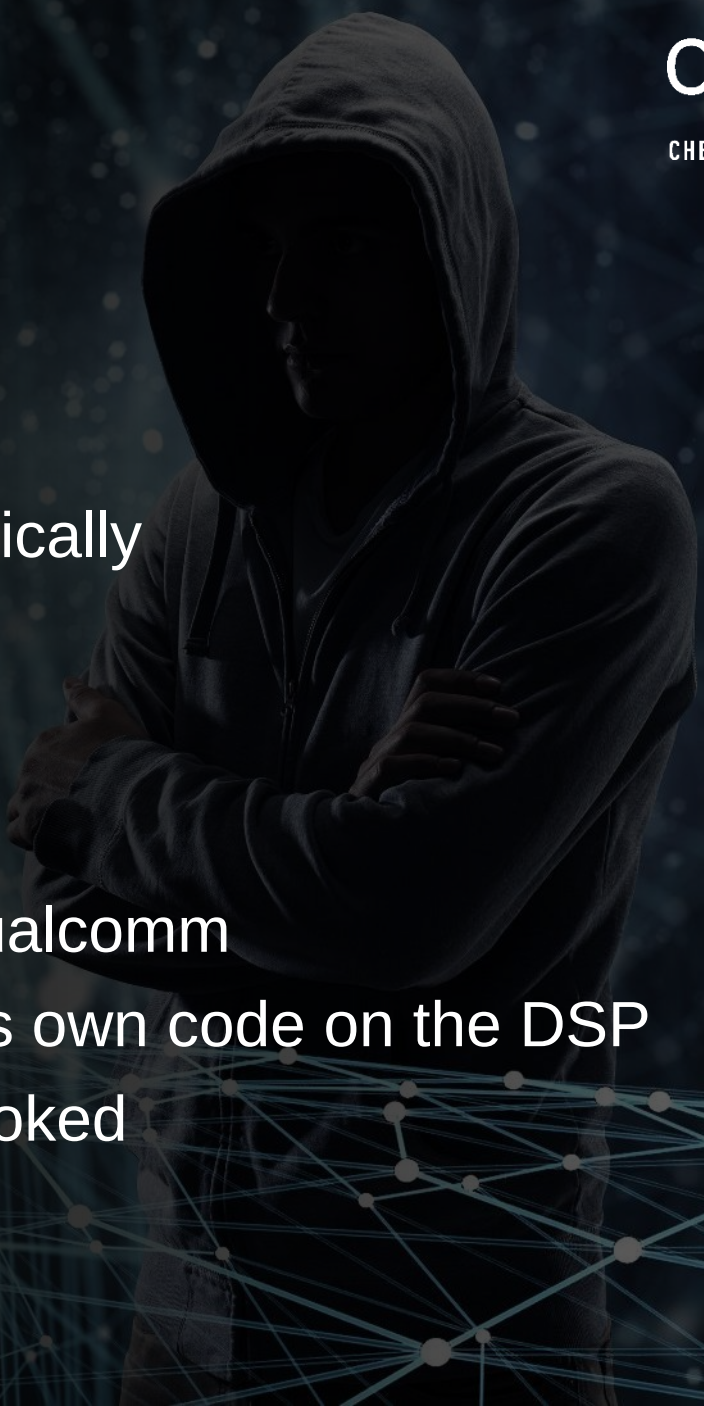
- **What is a DSP?**
  - Digital Signal Processor
- **What is Hexagon?**
  - A HW architecture like x86, MIPS, ARM
- **Does it have its own OS?**
  - Yes, QuRT
- **What is it used for?**
  - Computer vision tasks
  - Camera streaming
  - Machine learning-related calculations
  - Low-power processing of audio/voice data



Android applications run here

Only Qualcomm signed code can run here

Who can run code on DSP?



- Can I compile my own DSP library? Yes
  - Hexagon SDK is publically available
  - *Stub* and *skel* code will be generated automatically

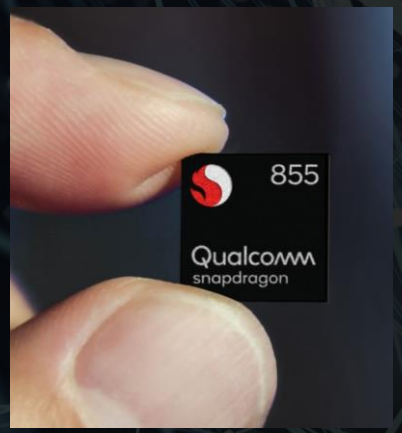
- Can I execute this library on DSP? No
  - DSP is licensed for programming by OEMs
  - The code running on the DSP is signed by Qualcomm
  - Android app has no permissions to execute its own code on the DSP
  - Only prebuilt DSP libraries could be freely invoked

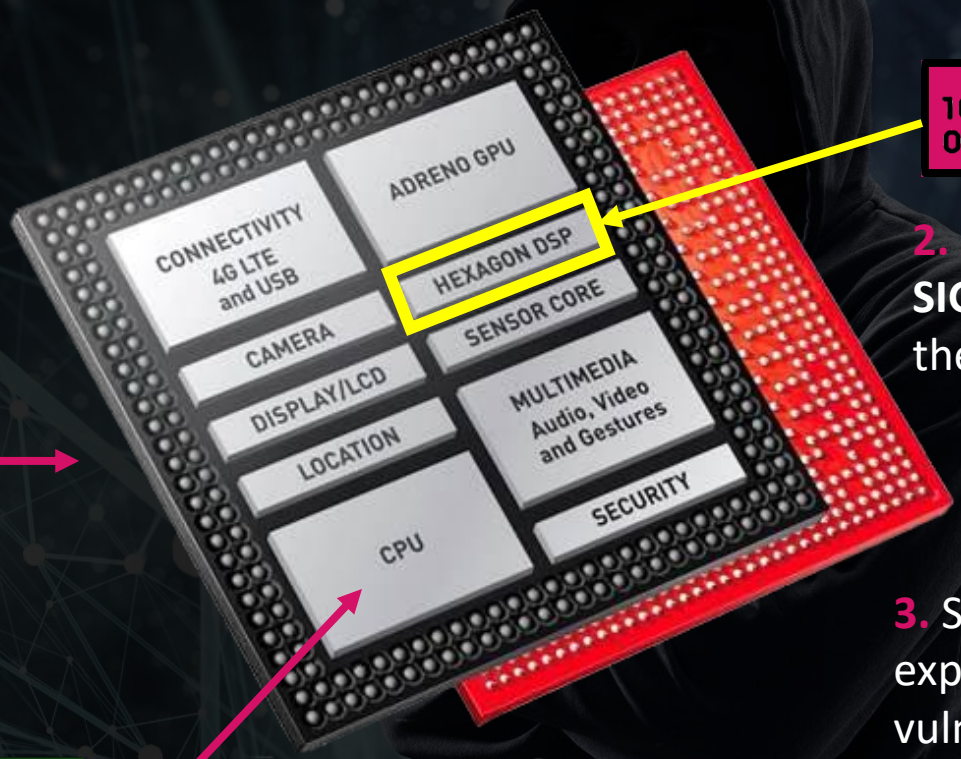
How does Achilles work?

- We cannot sign a skeleton library, but…
- We can execute a signed one
- No version check
- No per-device limitation

Downgrade vulnerability
(CVE-2020-11209)

How does it work?





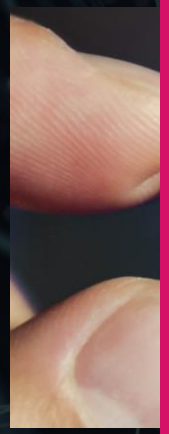
1. Application runs here

2. App loads old **SIGNED** library to the DSP

3. Sending payload exploiting the vulnerable skeleton lib running code on the DSP

4. Exploiting DSP driver to gain system privileges

How does Achilles work?



CVE-2020-11201

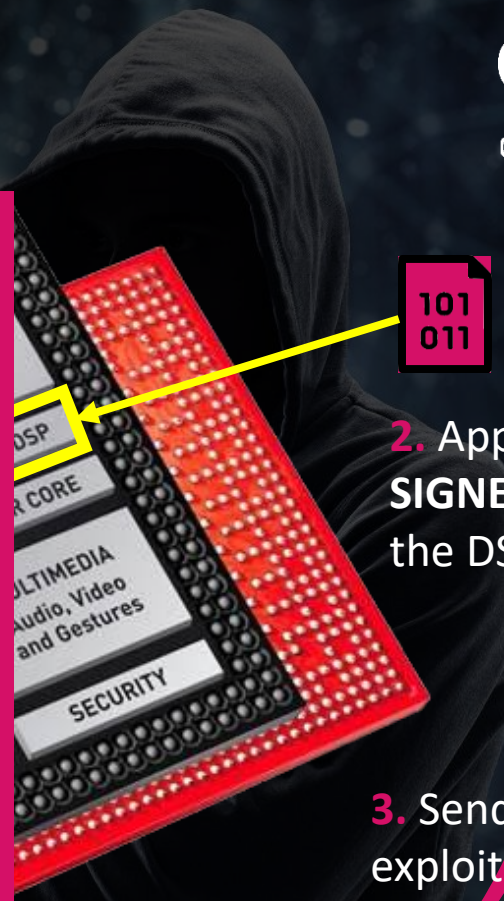
CVE-2020-11202

CVE-2020-11206

CVE-2020-11207

CVE-2020-11208

CVE-2020-11209



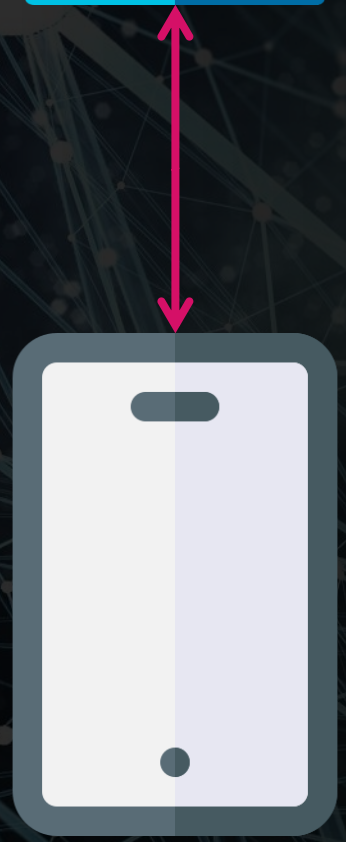
2. App loads old **SIGNED** library to the DSP

3. Sending payload exploiting the vulnerable skeleton lib running code on the DSP

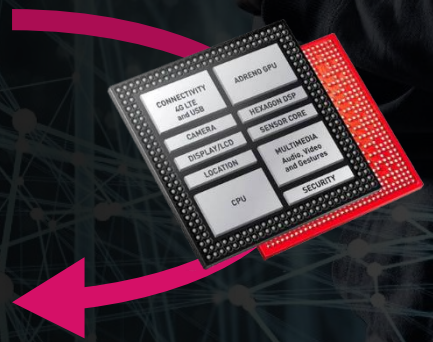
THE VULNERABILITIES WE FOUND ENABLE RUNNING CODE ON THE DSP!

ATTACK FLOW

1. User downloads innocent app from market or other web link



2. Application sends malicious payload to DSP exploiting Achilles



3. Application gains persistency, higher privileges, can steal data and crash device.

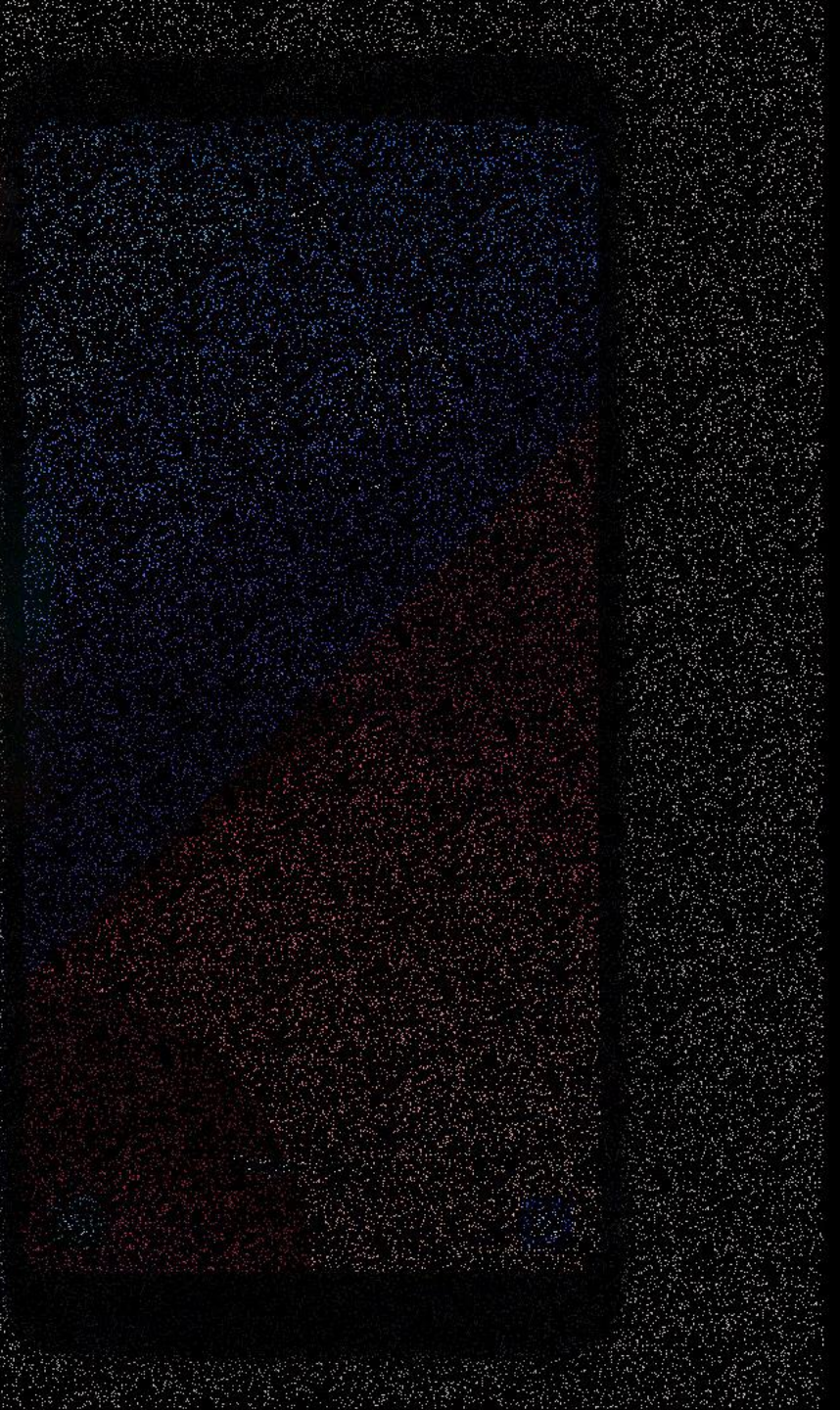
cp<r>
CHECK POINT RESEARCH

More Details – DefCon Talk


cp<r>
CHECK POINT RESEARCH
DEMO

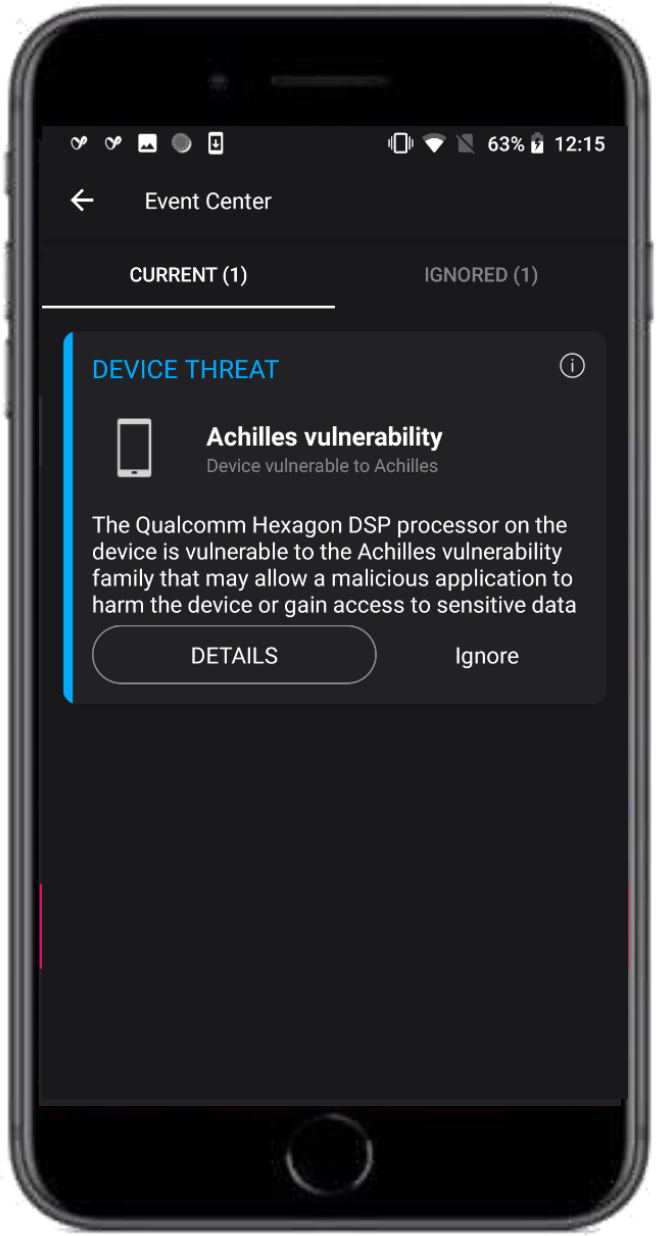
DEMO PART 2

The only way to restore the device is to wipe it via boot menu (factory reset)



Is my device vulnerable?

Check Point SandBlast™ MOBILE



SANDBLAST MOBILE
Preventing mobile cyber attacks

01. Prevents malicious app downloads

02. Prevents phishing across all apps

03. Prevents MitM attacks

04. Blocks access of infected devices to corporate apps

05. Prevents OS exploits

KEY BENEFITS

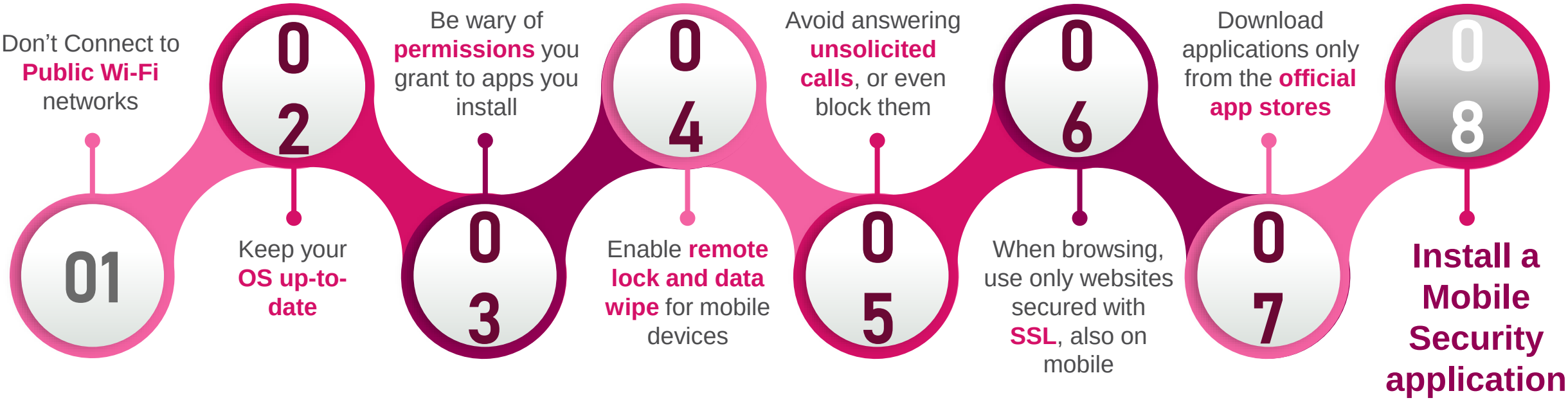
Ensures data regulatory compliance

Easy to deploy and to integrate

Leverages world's largest threat intelligence engine, ThreatCloud

Full visibility on incoming threats

BEST PRACTICES FOR MOBILE SECURITY HYGIENE




cp<r>
CHECK POINT RESEARCH
THANK YOU