Lookout®

A Beginner's Guide to Android Malware Analysis

#BlackHoodie18

Kristina Balaam | @chmodxx, Security Intelligence Engineer

$whoami

KRISTINA BALAAM

Toronto, Canada

- Security Intelligence Engineer @ Lookout
- Formerly Application Security Engineer @ Shopify
- MSc. Student in Information Security Engineering, SANS Tech

@CHMODXX_ @CHMODXX blog.chmodxx.net

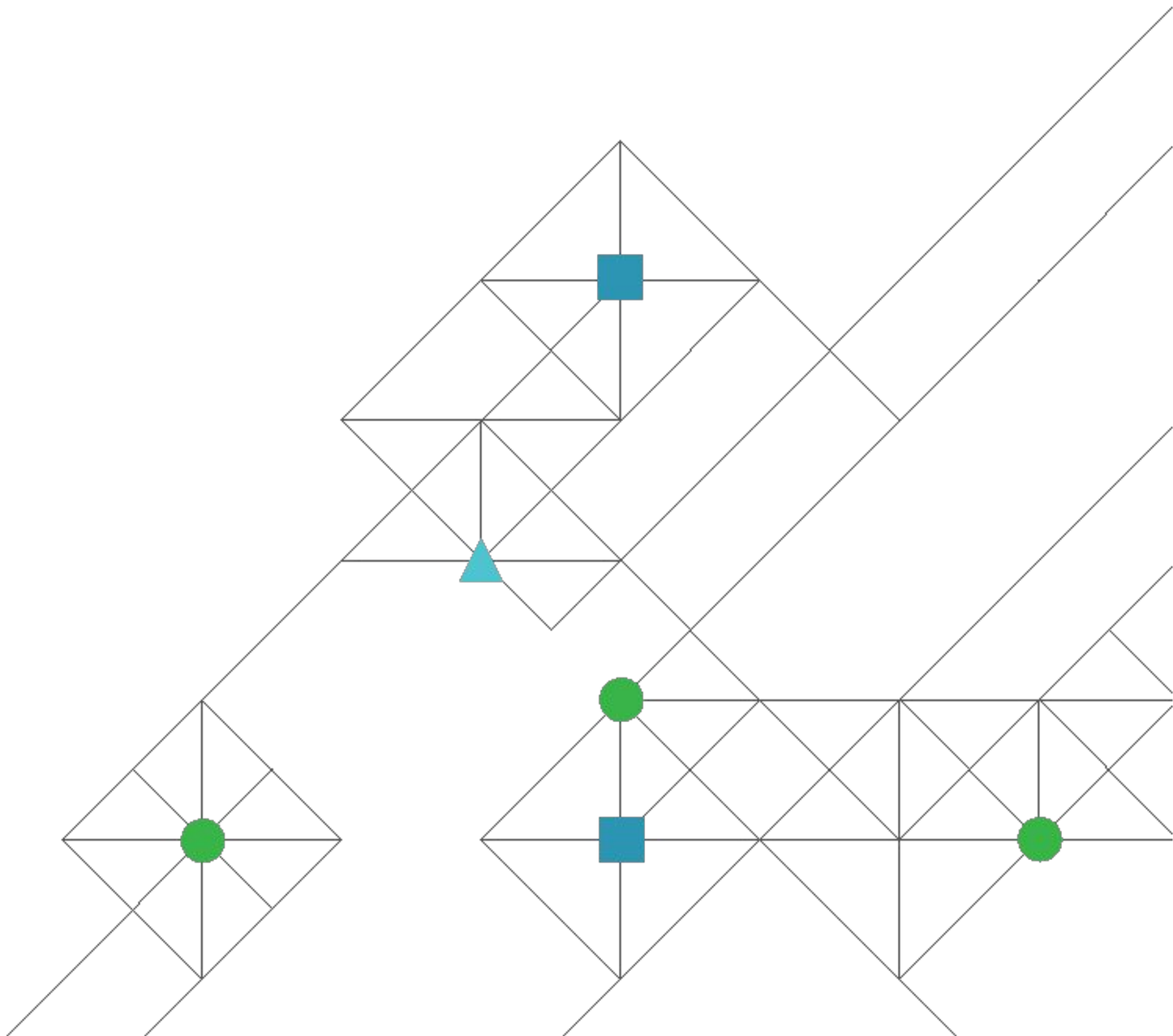
AGENDA

1. Android Malware 101
2. Tools
3. Finding Malicious Samples
4. Analyzing Samples
5. Resources

DISCLAIMER

- ✓ The information provided is intended to educate!
- ✓ Use these techniques to help find & remove malicious applications online, or to learn how to protect your *own* applications under development.
- ✓ If you want to hack for $$ and fame, *please* join a bug bounty program like **HackerOne** or **BugCrowd**.
- ✓ ***Be responsible and disclose vulnerabilities*** □

Mobile Malware Basics



Prevalence

- Gartner predicts that 80% of worker tasks will take place on a mobile device by 2020.

  Gartner, "Prepare for Unified Endpoint Management to Displace MDM and CMT" June 2018

- 95% of Americans now own a cellphone; 77% own a smartphone
- ⅕ Americans are “smartphone-only” internet users
- ¼ American adults say they are “almost constantly” online

  http://www.pewinternet.org/fact-sheet/mobile/ | Pew Research Center, Washington DC 02/18

Rank	Total Population	Online Population	Smartphone Penetration
1	United Arab Emirates	9,543,000	82.2%
2	Sweden	9,987,000	74.0%
3	Switzerland	8,524,000	73.5%
4	South Korea	50,897,000	72.9%
5	Taiwan	23,611,000	72.2%
6	Canada	36,958,000	71.8%
7	United States	328,836,000	71.5%
8	Netherlands	17,085,000	71.0%
9	Germany	80,561,000	71.0%
10	United Kingdom	65,913,000	70.8%
11	Belgium	11,513,000	69.7%
12	Spain	46,117,000	69.5%
13	Australia	24,967,000	69.3%
14	Azerbaijan	10,070,000	69.1%
15	Italy	59,788,000	68.5%

https://en.wikipedia.org/wiki/List_of_countries_by_smartphone_penetration

The Perfect Espionage Platform

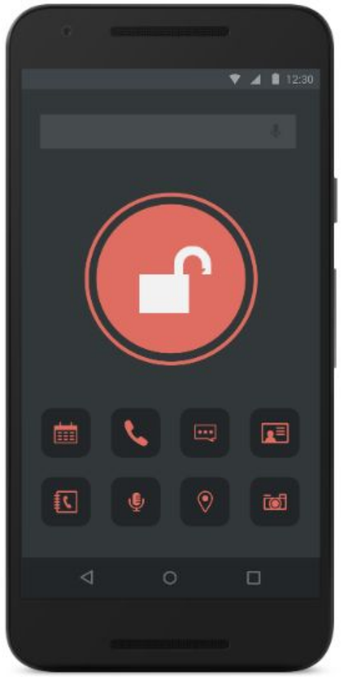
Always Connected

- Voice
- Camera
- Email
- Location
- Passwords & MFA
- Contact lists
- and more…

Malware Trends:

multi-platform campaigns

Means of Propagation



Phishing

- Email
- SMS / Text
- Social media

Gain Access

- Dropper installs, or
- Exploit, or
- Victim clicks thru for install

Elevate Privilege

- Install payload or
- Rootkit or
- Dropped apps, or
- Exploit vulns

Perform Espionage

Receive commands to:

- Send / exfiltrate private data, pictures, camera, audio

Common Types of Mobile Malware

SPY/
SURVEILLANCE

ADWARE/
CHARGEWARE

TROJAN
VIRUS

BOT

Important Terms

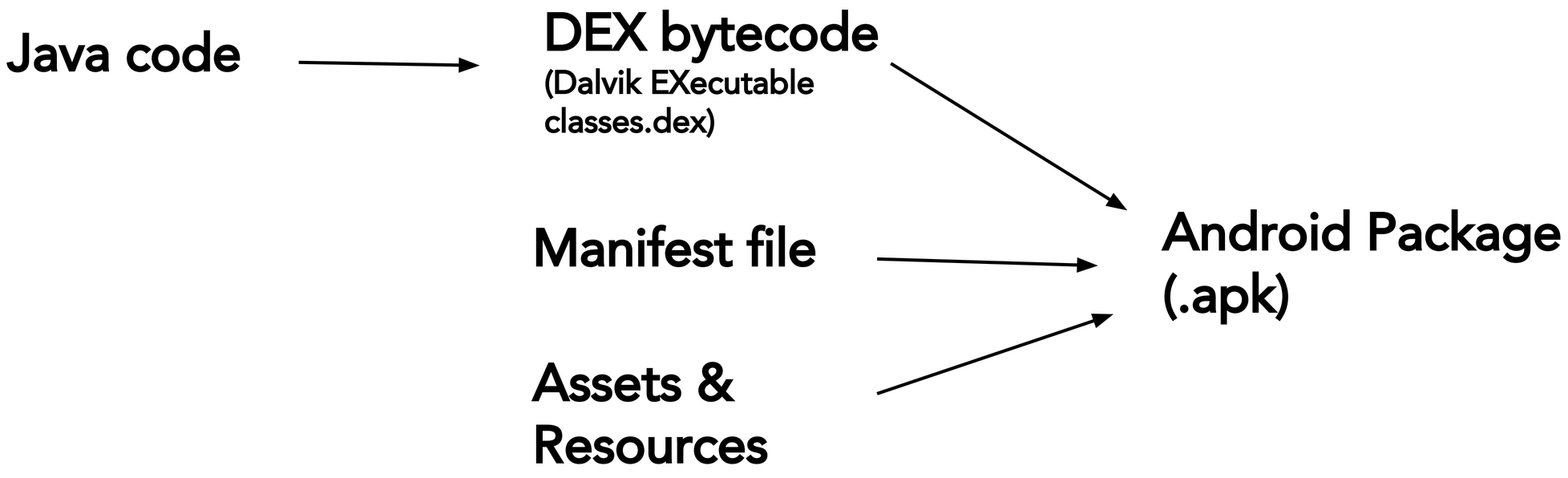
IOC (Indicators of Compromise): *an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion…Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers. (Wikipedia)*

C2 Server (Command & Control Server): *controlled by the malicious actor to either send remote commands to an application, or receive data collected by that application.*

Malware Family: *programs similar in functionality that can be seen as iterations on earlier versions of the malicious software.*

Heuristics: *elements of a malicious application common across families that can be used to detect similar/related applications.*

Packaging Android Applications



Reversing Android Applications

apktool → .apk → SMALI classes, Manifest file, Assets, META, Libraries & Resources

dex2jar → .jar (Compiled Java class files)

JD-GUI → .class (Pseudo-Java class files)

unzip → .apk → ~~Bytecode classes, Manifest file, Resources~~

Not human readable!

Is It Malware?

Popular IOCs

- ✓ *Domains*
- ✓ *IP Addresses*
- ✓ *Unique strings*
- ✓ *Unique files*
- ✓ *Signatures*

Potentially Malicious Behaviours

- ✓ *TONS of useless packages*
- ✓ *Extensive permissions*
- ✓ *Multi-DEX (eg. classes2.dex)*
- ✓ *Hiding the launch icon (!!!)*
- ✓ *Sketchy naming conventions (eg. com.services.android)*

Tools