Android Malware

Przemysław Warias

Przemysław -> Przemek -> P-sh-em-eck

Background & Intro

- Android experienced 50% increase in Malware instances (2019)
- 10 Million Android Phones compromised (Grifthorse campaign)
- Greater adoption of BYOD leaves companies exposed

What Will I Be Studying?

- Compare and contrast the latest Android Malware strains
  - Rana
  - Sova
  - “System Updater”
  - Joker
  - GriftHorse
- Areas of analysis
  - Obfuscation
  - Purpose
  - C&C
  - Infection Vector

Motivation

- Android is everywhere!
- Open source nature makes analysis easier
- The public is becoming more and more concerned
  - https://www.msn.com/en-us/news/technology/this-new-android-malware-is-so-devious/ar-BB1f5Vah
  - https://www.forbes.com/sites/zakdoffman/2020/07/09/Idangerous-android-malware-warning-google-play-store-security/
- Previous Experience
- Understanding the gaps in our detection

Phases of Research

- Research of each malware strain
- Documentation of known mechanism of action
- Dynamic analysis and comparison of results
- Knowledge share!

Thank You!

Questions, comments, concerns?