University of
South Wales
Prifysgol
De Cymru

The Little Phone That Could Ch-Ch-Chroot (Some Trains Included)

Jack Whitter-Jones

bsides@exit.wtf

@Jack_WJ

Mathew Evans

bsides@nop.ninja

@MuNK__

Introduction

- Jack Whitter-Jones
  - Also known as eXit
  - PhD Student from the University of South Wales
    - Security Operations, Network Monitoring and PHP

- Mathew Evans
  - Also known as MuNk
  - PhD Student from the University of South Wales
    - Big Data, Lua and Hadoop

debian
tiny
core
micro

The Ideal Device

- Cheap
- Deniable
- Rootable
- Easy to use
- Android

Rooting the Device

- Mobile OS
  - Ubuntu Touch
  - Lineage OS (Successor of Cyanogen)
  - Sailfish
- CyanogenMod 13
  - It still has its place
  - Common for mobile enthusiasts
  - Provide a base for further dev work

CPIO & Chroot….. So what?

- CPIO and Chrooting is far from new
  - Kali NetHunter
    - Debian
  - Firmware Packages
    - CPIO Archiving

- Drawbacks regarding NetHunter
  - 1GB in Size (Tools + Debian)
  - Packet full of pen testing tools
  - **Noticeable**

Our Approach

- TinyCore
  - Tinycore:16mb,
  - Core: 11mb
  - Ours: 32mb
    - Python
    - VPN
  - Large amounts of packages
  - Can build and deploy remotely
- CPIO
  - Supported by Android, not supported by most forensic tools
  - GZ Compression to protect against data carvers
  - Can hide on the end of a file

So What do we have

- We have an extreme small operating system
- Can put the entire operating system at the end of a file
- Can load and hide the running operating system in the memory of the device
- No physical impact on the device while running
- Can use androids functionality

Functionality

ID	Functionality	Reason	Outcome
1	USB Tethering	Looks like you are charging your phone, but can provide the network adapter	The phone was adapted to look as if it is charging when the USB tethering is in place
2	VPN	Built in VPN that can hide traffic in and out of the phone	Using OpenVPN we can utilise backend infrastructure
3	Gesture Reader	This is how we can capture the devices gesture movement to indicate whether we take a photo	Using Androids operating system we can capture the screen movement when an operator touches the screen
4	Photo	Demonstration that we can hide an image that was taken by the underlying Android OS	We can take an image both via the gesture and via the VPN connection

Demonstration – USB Tethering

- VIDEO Charging + Video Windows Adapter

Demonstration – Photo

- Video of photo remotely

Anti-Forensics

- Typically in a forensic investigation we aim to achieve integrity when imaging a device
  - While this can be done, an investigator must have some form of understanding on where an integrity change may occur
  - We therefore, introduce an integrity changer within the hidden partition of the device to skew the imaging of the phone

- The next-phase of an investigation would be to do a live analysis of the phone
  - When an investigator places a phone in a faraday cage, the phone will not load the CPIO image
  - In addition, if the operator disconnects from the phone, the image is unloaded, requiring a restart

- Finally, an investigator would be required to carry out destructive analysis of the device
  - So we glued the chips to the back of the phone as to destroy the device

What have we learnt

- For anyone that has used Android for security research
  - SELINUX is **NOT YOUR FRIEND**

- There are particular areas of memory that are reserved for the Android operating system, but can be used for hiding small partitions and operating systems

- We can do a lot more offensive development regarding embedded devices.

Further Information

- A guide has been written and all the code for the device is place on our githubs:
  - https://github.com/ExitSec/
  - https://github.com/munk/

- We also wrote a paper which can be found at:
  - arXIv

University of
South Wales
Prifysgol
De Cymru

Thanks for listening!

Jack Whitter-Jones

bsides@exit.wtf

@Jack_WJ

Mathew Evans

bsides@nop.ninja

@MuNK__