Detecting and Defending Against State-Actor Surveillance
Introduction
CONTENTS

1. Introduction
2. Goals and Intent
3. Surveillance Catalog Leaks
   - Hardware
   - Software
   - Wifi
   - Cellular
4. Conclusions
Who is involved

- Those that spy.
- Those that get spied on.
Why do Spies Spy?

- Information has value.
  - Moral values:
    - Protect people from harm
    - Progress society
  - Immoral values:
    - Blackmail
    - Profiteering
Full Disclosure

I loath tin foil hats and conspiracy theories.
Story time!

- 2010, someone working on their car finds a GPS unit
- Law enforcement and FBI show up shortly after it is removed, asking for their device back.
- www.wired.com/2010/10/fbi-tracking-device/
2010, someone working on their car finds a GPS unit

Law enforcement and FBI show up shortly after it is removed, asking for their device back.

This is the only major story that discusses a tracking device being found.
Story time!

- 2010, someone working on their car finds a GPS unit

- Law enforcement and FBI show up shortly after it is removed, asking for their device back.

- www.wired.com/2010/10/fbi-tracking-device/

- This is the only major story that discusses a tracking device being found.

- No agency admits involvement
What is the “Surveillance Catalog”? 
Surveillance Catalog leaks

- Der Spiegel and 30c3 in December 2013
- Tons of details regarding how spying agencies are 'bugging' computers, cell phones and more.
- They do not credit a source.
Introducing Surveillance Sam!
Hardware Bugs

Retro Reflectors

RAGEMASTER

LOUDAUTO

TAWDRYYARD

SURLYSPAWN
Hardware Bugs

RF Bug Detection
Hardware Bugs
RF Bug Detection
Hardware Bugs

RF Bug Detection

Software Defined Radio
Hardware Bugs

Data Exfiltration

COTTONMOUTH

HOWLERMONKEY

GINSU

FIREWALK
Hardware Bugs

Persistant Compromise

A device by any of these names

- GODSURGE, JETPLOW
- HEADWATER, HALLUXWATER
- SCHOOLMONTANA, SIERRAMONTANA, STUCCOMONTANA
- FEEDTROUGH, GOURMETTROUGH, SOUFFLETROUGH

Just means hardware for persistent compromise
Detecting Persistent Compromise Devices

By looking inside
Detecting Persistent Compromise Devices

By looking inside
Detecting Persistent Compromise Devices

By looking inside
Detecting Persistent Compromise Devices
Connected to JTAG, XDP, ITP, etc…
Detecting Persistent Compromise Devices
Connected to JTAG, XDP, ITP, etc…
Which one of these does not belong?
Software Exploits

IRATEMONK SWAP

WISTFULTOLL DIETYBOUNCE
BIOS/Firmware/CF Card Hacked?

Re-Flash Devices
BIOS/Firmware/CF Card Hacked?

Re-Flash Devices

TPM Trusted Platform Module
BIOS/Firmware/CF Card Hacked?

TPM
WIFI Devices
Wifi Devices

NIGHTSTAND

SPARROW
Cell Phone Bugs
Cell Phone Bugs

Base Stations

CYCLONE CROSSBEAM, EBSR, ENTOURAGE, NEBULA, TYPHO

Intelligence

GENESIS, WATERWICH, CANDYGRAM
Cell Phone Bugs
OPSEC
At All Times
Conclusions

- Enjoy the thought experiment and discussion.
- Bugs are detectable
  - Many are based on attacks covered in Hacker cons
- Hard evidence is better than Hearsay
  - I want to hear from the first person who finds one!
- Tin-Foil hats are not stylish
Further Reading & Sources

- SpiderLabs Blog (blog.spiderlabs.com)
- Michael Ossmann (ossmann.blogspot.com)
- Trusted Computing Group (trustedcomputinggroup.org)
- http://leaksource.files.wordpress.com

Find me on Twitter: @iamlei
Spiderlabs on Twitter: @SpiderLabs
THANK YOU