
Detecting and Defending
Against State-Actor Surveillance
Trustwave®
SpiderLabs®

Introduction

CONTENTS

Who is involved

- Those that spy.
- Those that get spied on.

Trustwave® SpiderLabs®

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.

Trustwave® SpiderLabs®

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/

Trustwave® SpiderLabs®

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.**

Trustwave® SpiderLabs®

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**

Trustwave® SpiderLabs®

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.

Trustwave® SpiderLabs®

Introducing Surveillance Sam!

Trustwave® SpiderLabs®

Hardware Bugs

Hardware Bugs

Retro Reflectors

Trustwave® SpiderLabs®

Hardware Bugs

RF Bug Detection

Trustwave® SpiderLabs®

Hardware Bugs

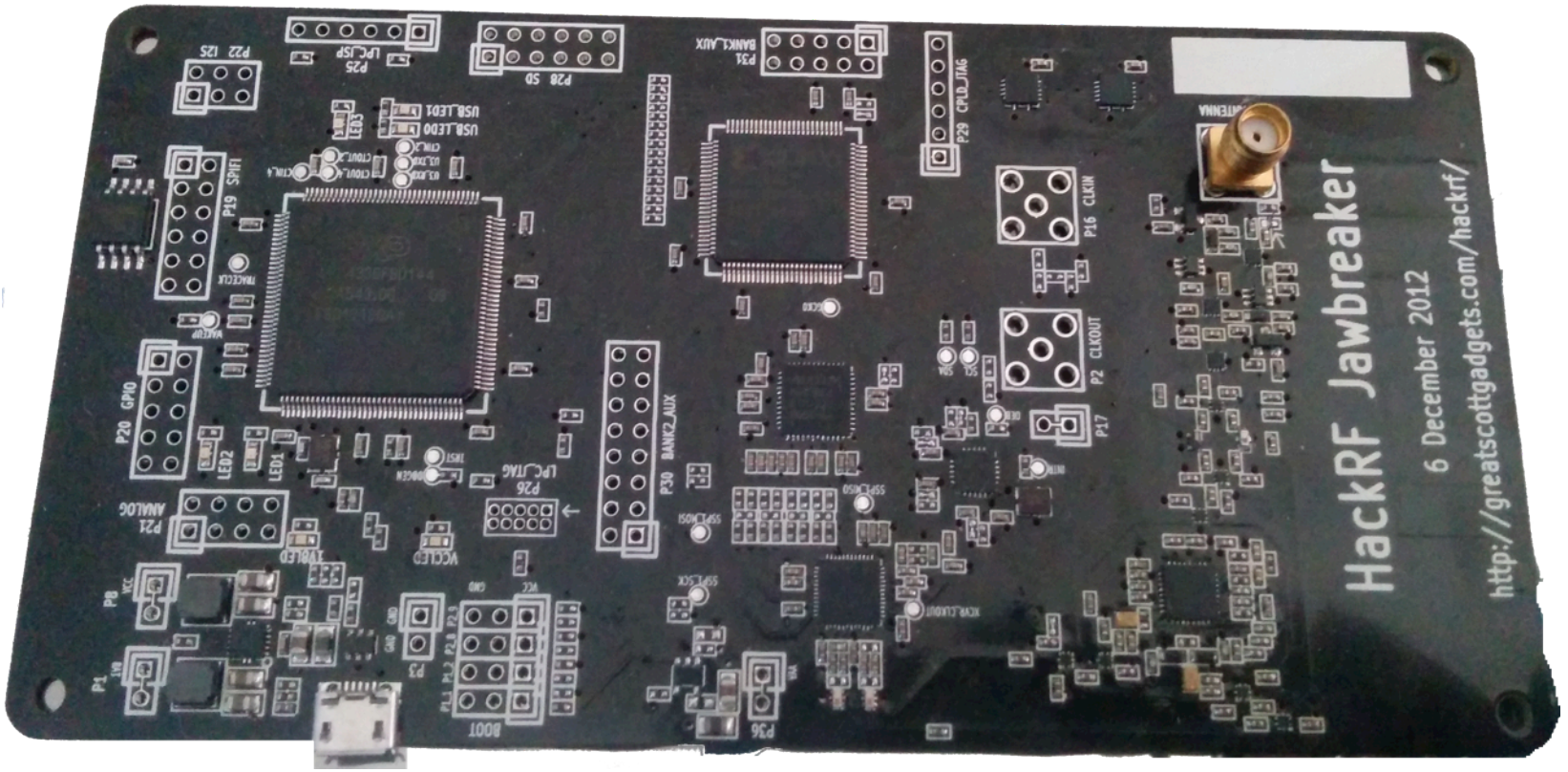
RF Bug Detection

Trustwave® SpiderLabs®

Hardware Bugs

RF Bug Detection

Software Defined Radio



Trustwave® SpiderLabs®

Hardware Bugs

Data Exfiltration

Trustwave® SpiderLabs®

Hardware Bugs

Persistant Compromise

A device by any of these names

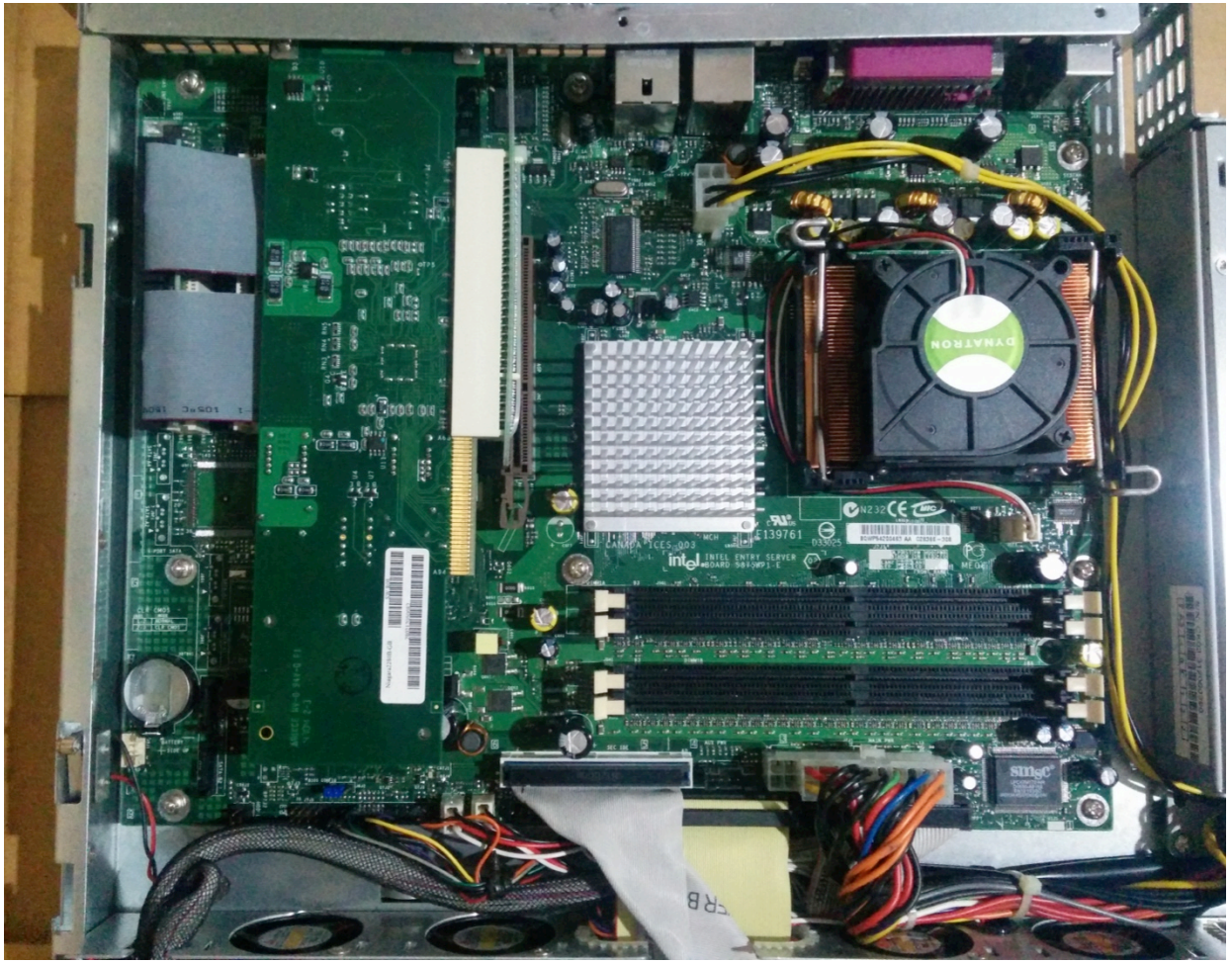
- GODSURGE, JETPLOW
- HEADWATER, HALLUXWATER
- SCHOOLMONTANA, SIERRAMONTANA, STUCCOMONTANA
- FEEDTROUGH, GOURMETTROUGH, SOUFFLETROUGH

Just means hardware for persistent compromise

Trustwave® SpiderLabs®

Detecting Persistent Compromise Devices

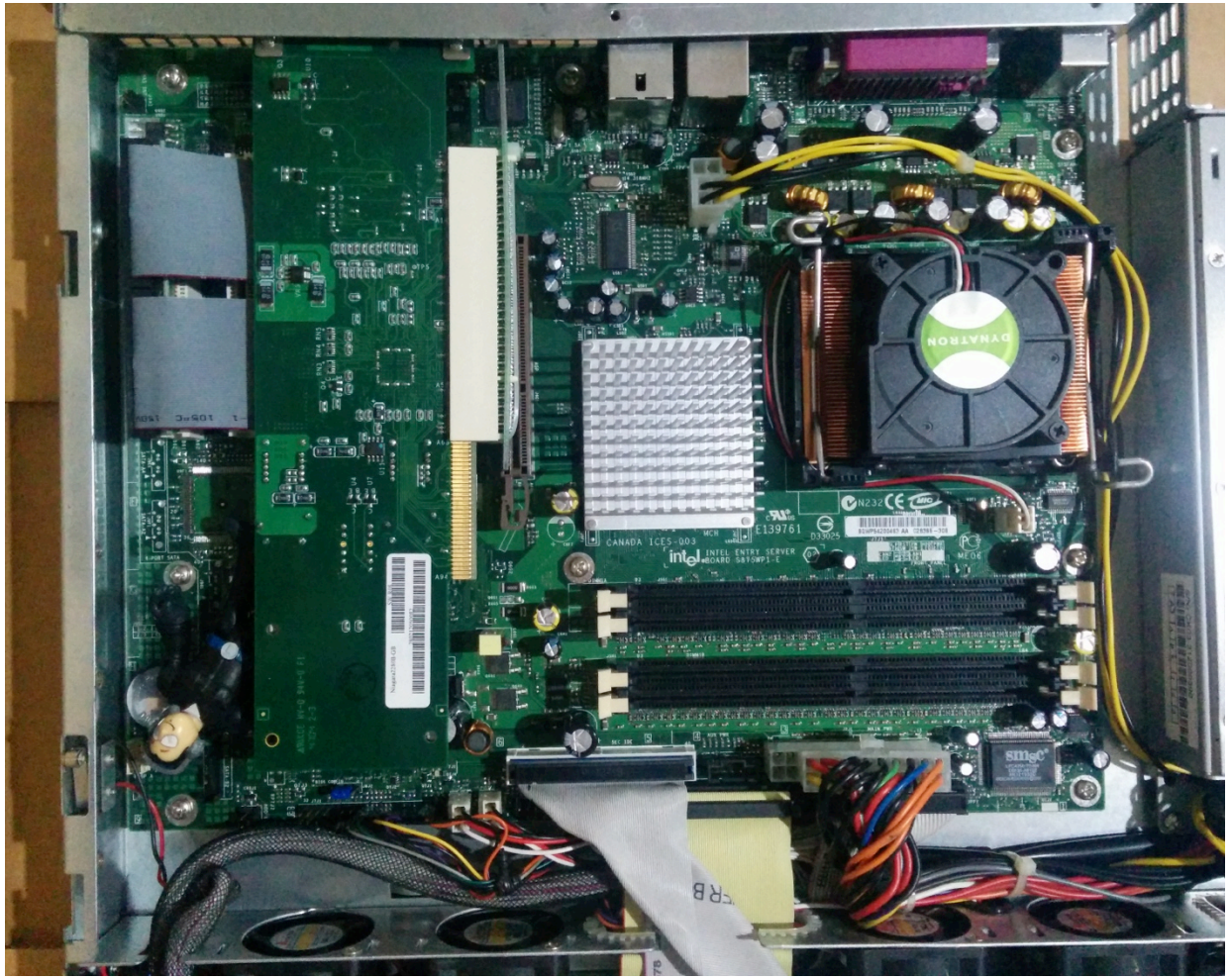
By looking inside



Trustwave® SpiderLabs®

Detecting Persistent Compromise Devices

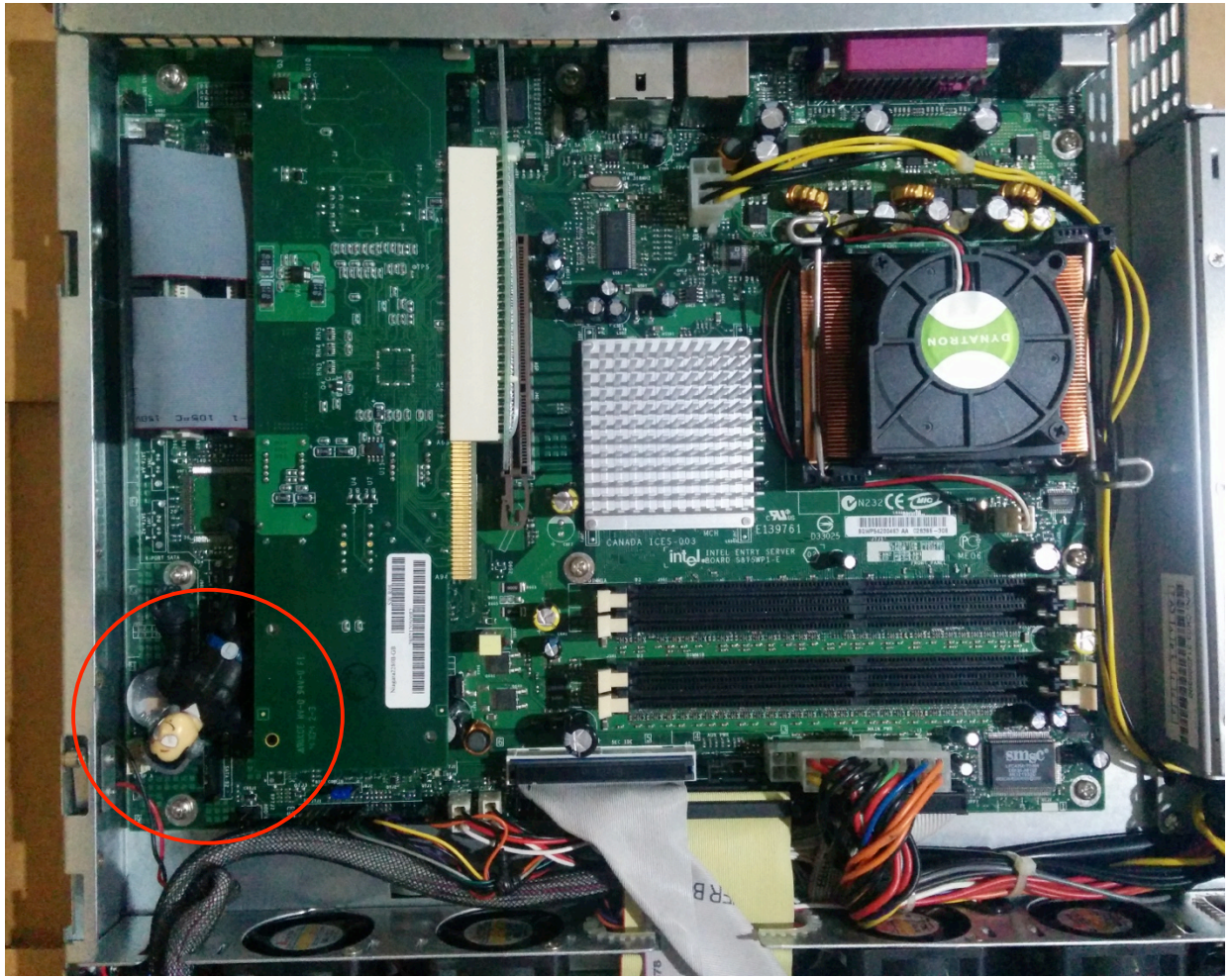
By looking inside



Trustwave® SpiderLabs®

Detecting Persistent Compromise Devices

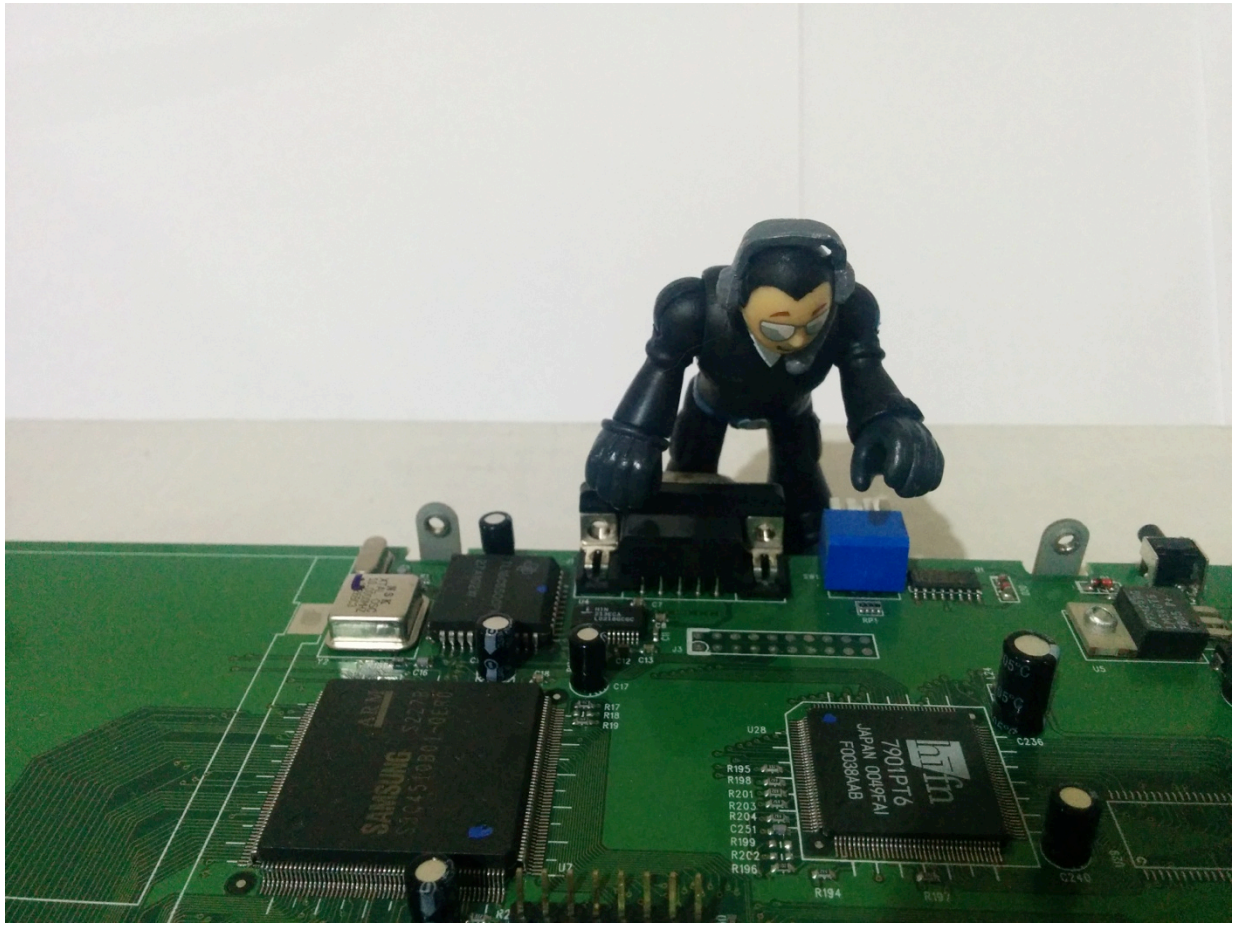
By looking inside



Trustwave® SpiderLabs®

Detecting Persistent Compromise Devices

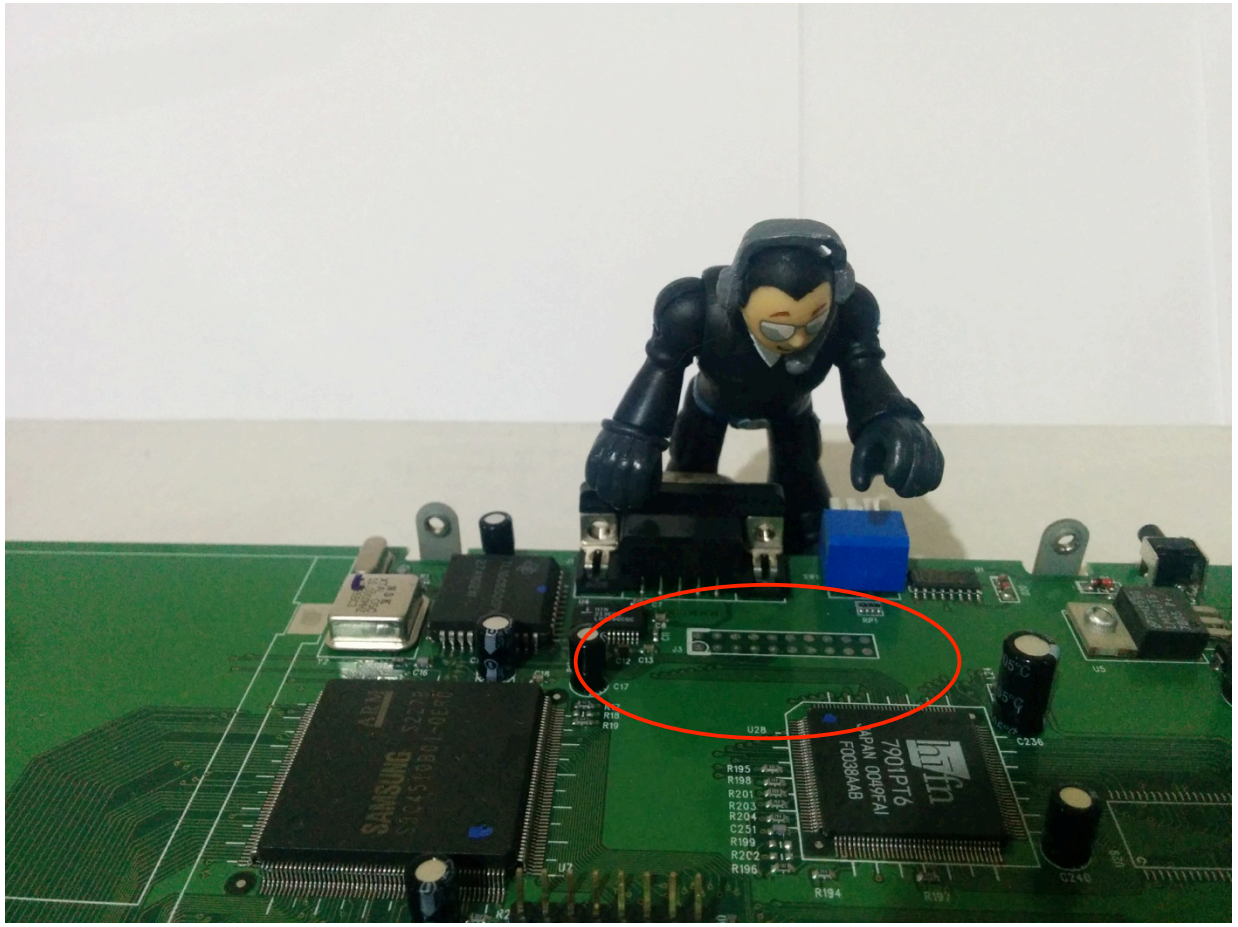
Connected to JTAG, XDP, ITP, etc…



Trustwave® SpiderLabs®

Detecting Persistent Compromise Devices

Connected to JTAG, XDP, ITP, etc…



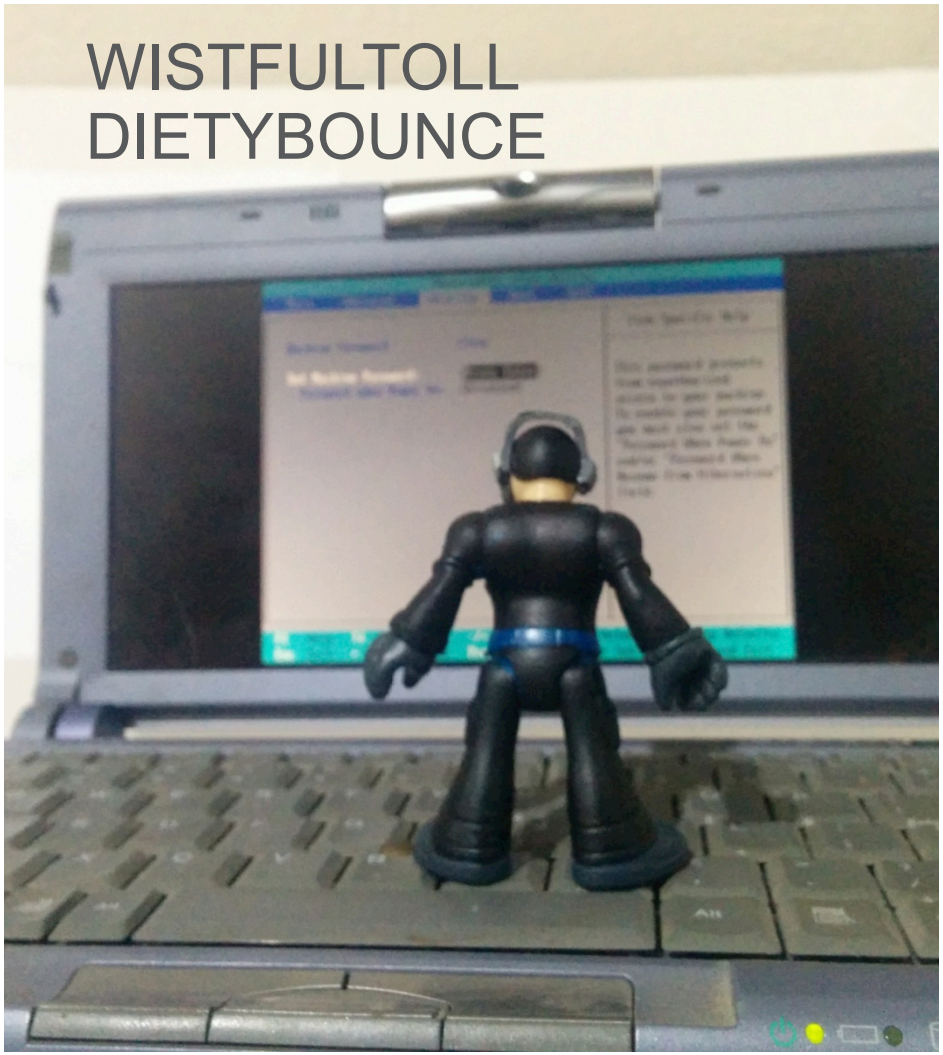
Trustwave® SpiderLabs®

Which one of these does not belong?

Trustwave® SpiderLabs®

Software Compromises

Software Exploits



Trustwave® SpiderLabs®

BIOS/Firmware/CF Card Hacked?

Re-Flash Devices

Trustwave® SpiderLabs®

BIOS/Firmware/CF Card Hacked?

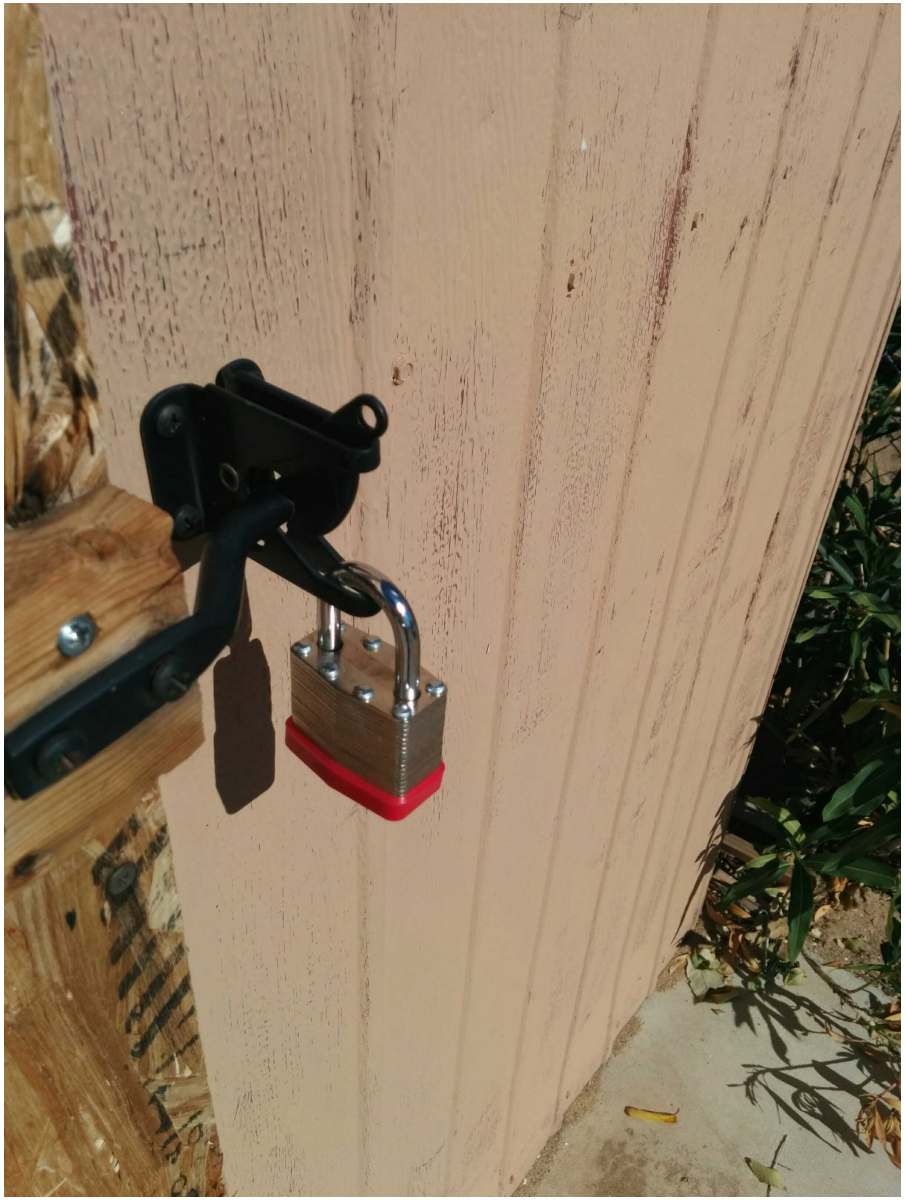
Re-Flash Devices

TPM Trusted Platform Module

Trustwave® SpiderLabs®

BIOS/Firmware/CF Card Hacked?

TPM



Trustwave® SpiderLabs®

WIFI Devices

Wifi Devices

Trustwave® SpiderLabs®

Cellular Networks

Cell Phone Bugs

Trustwave® SpiderLabs®

Cell Phone Bugs

Base Stations

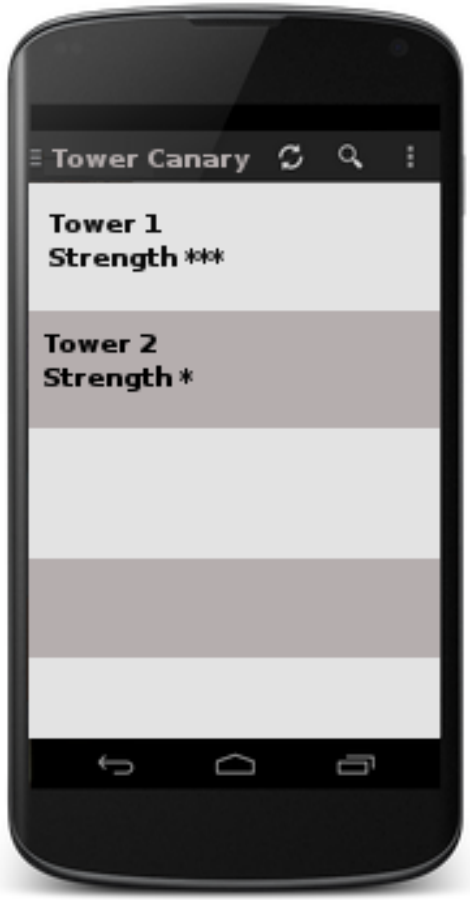
CYCLONE CROSSBEAM, EBSR, ENTOURAGE, NEBULA, TYPHO

Intelligence

GENESIS, WATERWICH, CANDYGRAM

Trustwave® SpiderLabs®

Cell Phone Bugs



Trustwave® SpiderLabs®

OPSEC
At All Times

Trustwave®
SpiderLabs®

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

Trustwave® SpiderLabs®

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

Trustwave® SpiderLabs®


THANK YOU
Trustwave®
SpiderLabs®