JUICE JACKING UNEARTHED

August 2013 | Def Con 21

Robert Rowley
VP of Security Researcher

Trustwave®
Smart security on demand

SUMMARY

1 Introduction and History of Juice Jacking
2 Prevention methods
3 Device Specific issues
4 Advanced Topics
5 Summary

Trustwave®

Introduction and History

Trustwave®

What is Juice Jacking?

- To break in and violate someone's lunchable for the sole purpose of consuming the delicious juice pouch.

Trustwave®

What is Juice Jacking?

- The utilization of a charging kiosk for malicious actions against mobile devices, under the ruse of providing a free charge.

Trustwave®

The Build

Hardware

- Computer
- Box
- Lots of USB cables

Software

- Linux (liveCD)
- USButils package
- Custom shell scripts

Trustwave®

First you hack

Trustwave®

Put it in a box

Trustwave®

Put the box out in public

Trustwave®

The software

- Puppy Linux Customized Image
  - Remove USBHID from the kernel
  - Include images/libraries
  - Custom scripts for managing screen

Trustwave®

The software

```
#!/bin/bash
base_count=`/sbin/lsusb | wc –l`;
last_count=$base_count;
interval=2;
while ( sleep $interval; ) do
  count = `/sbin/lsusb | wc –l`;
  if [ $last_count != $count ] && [ $count != $base_count ]
    then
  # Do your code here
  fi
done
```

Trustwave®

The software

```
#!/bin/bash
base_count=`/sbin/lsusb | wc –l`;
last_count=$base_count;
interval=2;
while ( sleep $interval; ) do
  count = `/sbin/lsusb | wc –l`;
  if [ $last_count != $count ] && [ $count != $base_count ]
    then
  # Do your code here
  fi
done
```

Trustwave®

The software

```
#!/bin/bash
base_count=`/sbin/lsusb | wc –l`;
last_count=$base_count;
interval=2;
while ( sleep $interval; ) do
  count=`/sbin/lsusb | wc –l`;
  if [ $last_count != $count ] && [ $count != $base_count ]
    then
  # Do your code here
  fi
done
```

Trustwave®

The software

- Update Image shown on screen

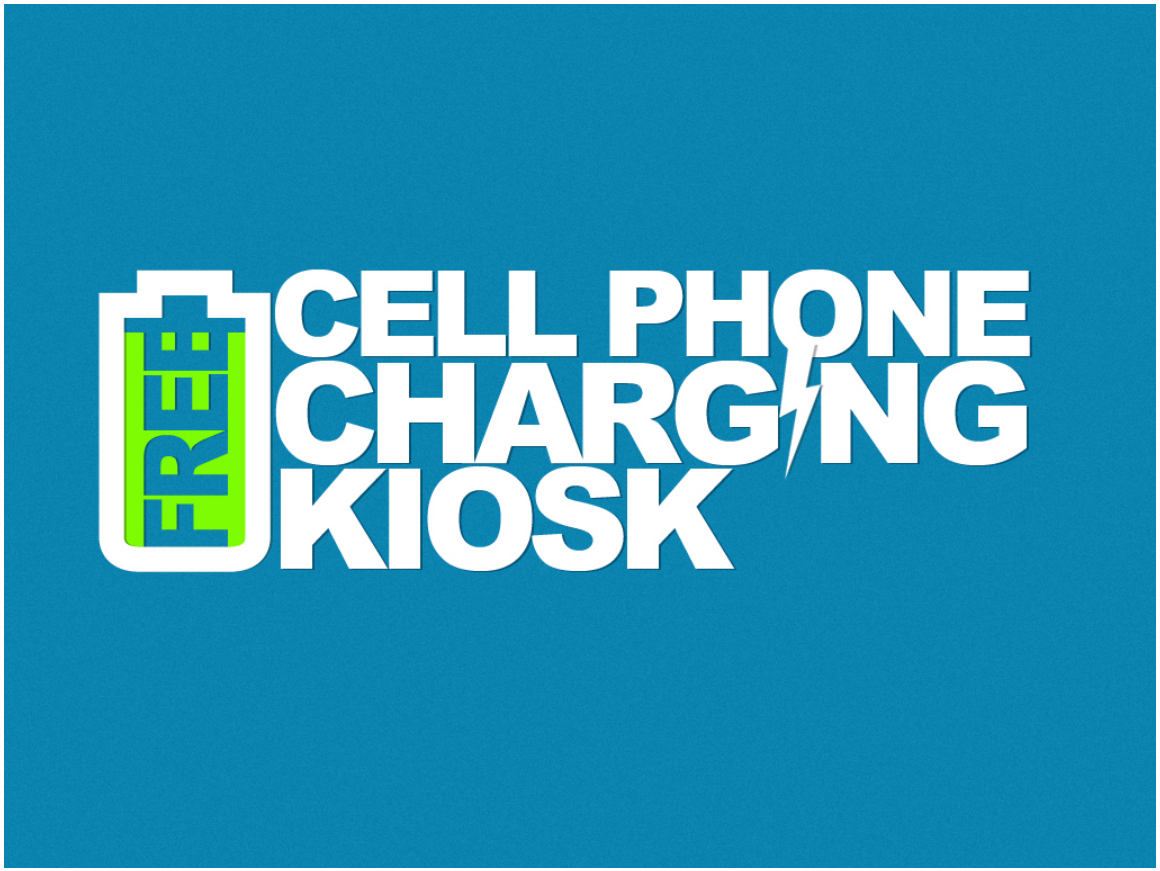
```
…
while ( sleep $interval) do
 count=`/sbin/lsusb | wc -l`;

 if [ $last_count != $count ] && [ $count != $base_count ]
 then
   /usr/bin/xsetroot -solid \#a30909;
   killall viewnior:
   viewnior --slideshow yourestupid.jpg;
    sleep 5;
   viewnior --slideshow chargestation.jpg;
fi
…
```

Trustwave®

The software

- Update Image shown on screen



Trustwave®

The software

- Update Image shown on screen

Trustwave®

The software

- Update Image shown on screen
- Track USB device information
  - Unique device identifier
  - How long they were plugged in

Trustwave®

The software

- Update Image shown on screen
- Track USB device information
- Download data from the DCIM folder

Trustwave®

The software

- Update Image shown on screen
- Track USB device information
- Download data from the DCIM folder
- Upload images to the DCIM folder

Trustwave®

The software

- Update Image shown on screen
- Track USB device information
- Download data from the DCIM folder
- Upload images to the DCIM folder
- “be malicious” Install software, root device etc…

Trustwave®

The Deployment @ Defcon 19

Largest Hacker Conference.

Attendees treat it a lot like the wild west.

– This means the kiosk will now become a target.

Trustwave®

The Deployment @ Defcon 19

Largest Hacker Conference.

Attendees treat it a lot like the wild west.

– This means the kiosk will now become a target.

Hundreds of people plugged in

Trustwave®

Defcon

Trustwave®

Next up … Toorcon

New kiosk, new tricks.

Similar/Same attendees.

The idea has already been published.

Trustwave®

Next up … Toorcon

New kiosk, new tricks.

Similar/Same attendees.

The idea has already been published.

People still plugged in

Trustwave®

Toorcon

Trustwave®

ThotCon

Trustwave®

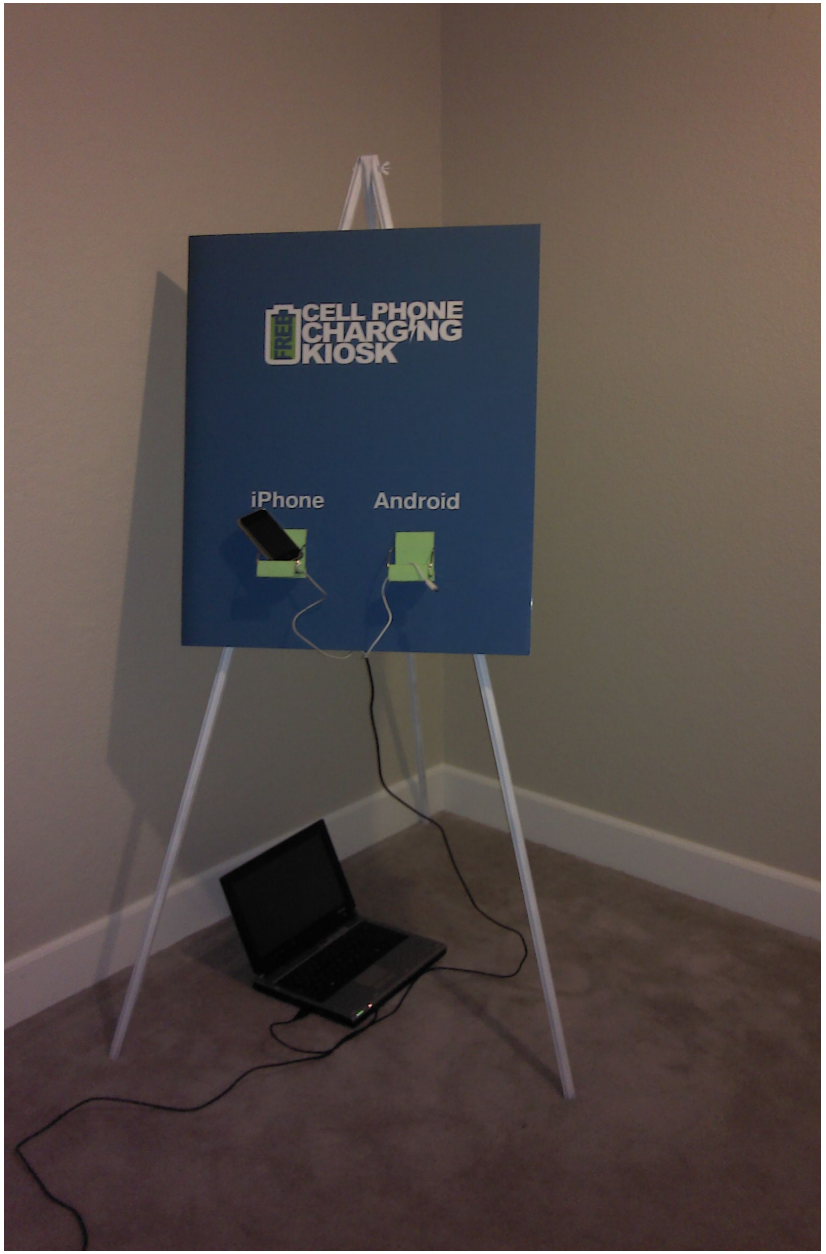
ThotCon

Trustwave®

Layer 1

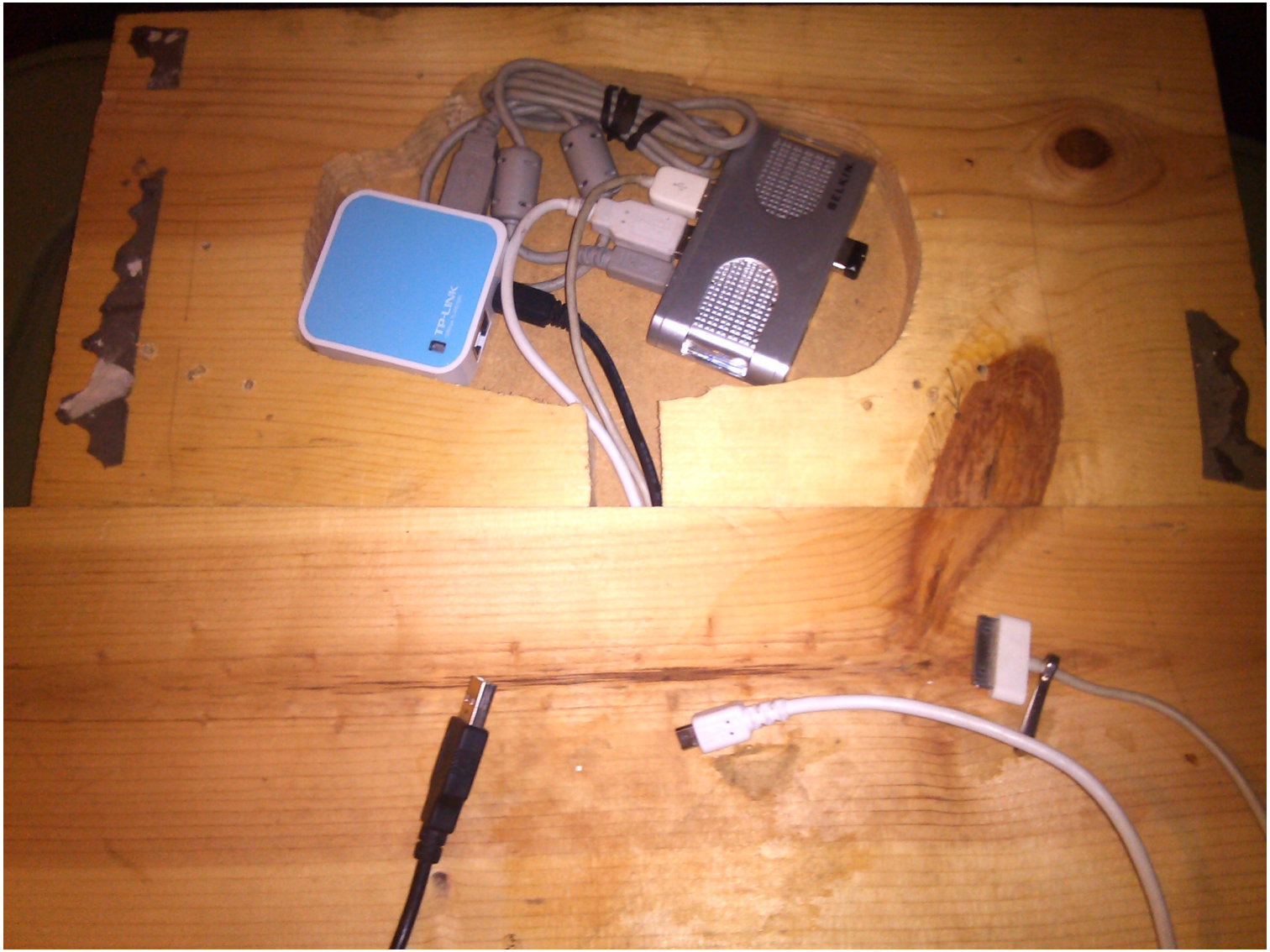
Trustwave®

Layer 1



Trustwave®

Layer 1



Trustwave®

The Media

Beware of Juice-Jacking

376 tweets
TOP ★1K
retweet

You're out and about, and your smart
an airport, hotel, or shopping mall. Yo
the device, but you do have a USB co
spot an oasis: A free charging kiosk.
to this unknown device that could be configured to read most of the data on your phone, and
perhaps even upload malware?

The answer, for most folks, is proba
people I've asked while researchin
they u
while
time
ramifi
securit

TODAY @ PCWORLD

Charging Stations May be 'Juice-Jacking' Data from Your Cellphone

By Brennon Slattery, PCWorld Aug 19, 2011 10:35 AM

» JUICE JACKING

TECHNOL

Facebook, iPhone, Twitter an
tech reporters and editors loo

↓ About this blog ↓ Archives

How to avoid smartphone juice jacking

Posted *3 weeks* ago by **Trent Nouveau**

Have you every heard of smartphone juice jacking? No? Well, don't worry, because you aren't alone.

4 comments belo

18 Aug 2011 1:36pm, EDT

Watch out! Charging stations could be stealing your data

By Rosa Golijan

Trustwave®

The Media

- Krebs on Security

Beware of Juice-Jacking

376 tweets TOP ★1K retweet

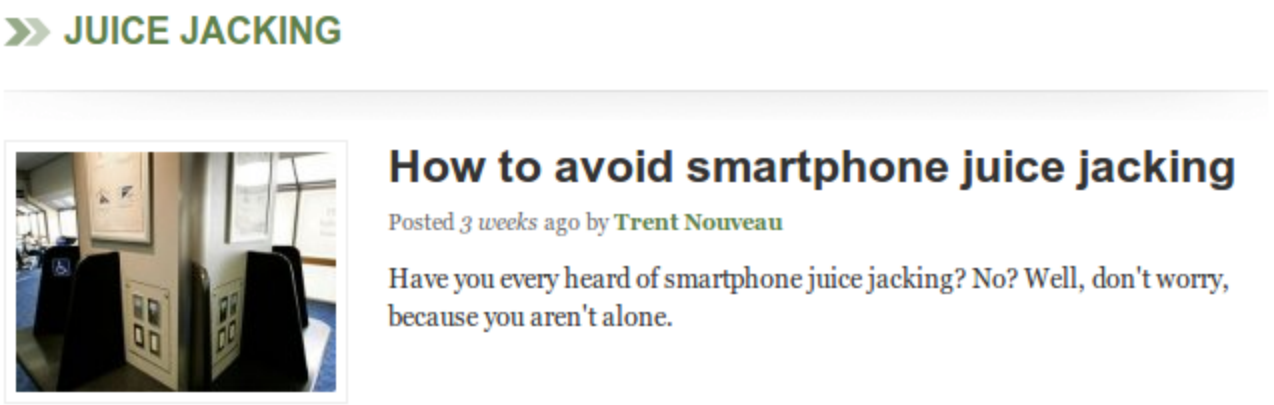
You're out and about, and your smartphone's battery is about to die. Maybe you're at an airport, hotel, or shopping mall. You don't have the power cable needed to charge the device, but you do have a USB cord that can supply the needed juice. Then you spot an oasis: A free charging kiosk. Do you hesitate before connecting your phone to this unknown device that could be configured to read most of the data on your phone, and perhaps even upload malware?

The answer, for most folks, is probably not. The few people I've asked while researching this story said they use these charging kiosks all the time (usually while on travel), but then said they'd think twice next time after I mentioned the possible security ramifications of doing so. Everyone I asked was a security professional.

Trustwave®

The Media

- Krebs on Security
- TG Daily



Trustwave®

The Media

- Krebs on Security
- TG Daily
- CNET -- “the 404” podcast

Trustwave®

The Media

- Krebs on Security
- TG Daily
- CNET -- “the 404” podcast
- MSNBC -- Technolog

rustwave®

The Media

- Krebs on Security
- TG Daily
- CNET -- “the 404” podcast
- MSNBC -- Technolog
- PC world


TODAY @ PCWORLD

Charging Stations May be 'Juice-Jacking' Data from Your Cellphone

By Brennon Slattery, PCWorld Aug 19, 2011 10:35 AM

Trustwave®

The Media

- Krebs on Security
- TG Daily
- CNET -- “the 404” podcast
- MSNBC -- Technolog
- PC world
- Twitter / Facebook / Social Networking

Trustwave®

Preventing Juice Jacking

Trustwave®

Don't get jacked.

Ideas?

???

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)
- Powering off the device

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)
- Powering off the device
- Confirmation required for mounting/debug access

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)
- Powering off the device
- Confirmation required for mounting/debug access
- Bring a backup battery!

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)
- Powering off the device
- Confirmation required for mounting/debug access
- Bring a backup battery!
- Bring your own charger; only plug into wall sockets (110v AC).

Trustwave®

Don't get jacked.

- USB cable neutering (removing data pin)
- Powering off the device
- Confirmation required for mounting/debug access
- **Bring a backup battery!**
- **Bring your own charger; only plug into wall sockets (110v AC).**

Trustwave®

My 0.02

- For business it's a matter of policy.
- For users it's a matter of not forgetting.

- Remember your charger or backup power source/battery.

Trustwave®

The gov'ment

Security Configuration Recommendations for Apple® iOS 5 Devices

Revision 0

March 28, 2012

The Mitigations Group

of the

Information Assurance Directorate

Trustwave®

The gov’ment

Security Configuration Recommendations
for
Apple® iOS 5 Devices

Revision 0

March 28, 2012

“Don’t plug in”

The Mitigations Group
of the
Information Assurance Directorate

Trustwave®

The Devices

Trustwave®

Devices
Android

Majority of roms ship with the “ask before mounting” option.
– This differs from rom to rom (check your device.)
OS designed with strict security permissions on applications and filesystem.
Battery accessible, you can bring another battery or replace the stock battery.

Unique risks:
– Android debugger
– Rooted phones
– psneuter
– Summed up very well by @theKos in “Physical Drive-By” presentation

Devices

iPhone

- Auto-sync
- Design for usability first
- No battery replacements
- Proprietary connector
- Strict after-market control
- “Mactans”

Trustwave®

Advanced Topics

Trustwave®

Juice Jacking 201
Advanced Topics

mmHrmm there is more here.

Trustwave®

Roll your own kiosk

- Push malware to phones
- Pull data from phones
- Foot traffic monitoring (device ID)
- People tracking (device ID)

Trustwave®

Attack Existing Kiosks

- Complicated PIN/Video systems likely means a CPU is in the box
- USB interface
- Discrete attack (just plugging in your phone!)
- Requires a detailed knowledge of the Kiosk

Trustwave®

Beyond the Kiosk

- Forget everything about the Kiosk.
- Transfer the attacks to a Laptop/PC.
- Use infected phones to spread Malware.
- Everyone brings their phones to work, plenty of those people will 'charge' at their desk.
- Minipwner/RasPi/Beagle Board powered

Trustwave®

Other similar work

- Kos's p2p-adb -- "Drive by Download"
  - github.com/kosborn/p2p-adb
- Jonathan Zdziarski's Talks about iOS forensics
  - zdziarski.com
- Billy Lau, YeongJin Jang, and Chengyu Song
  - MACTANS (released at BlackHat)

Trustwave®

Summary

Trustwave®

Summary

- The core threat isn't the kiosk, it is:
  - A design that chose usability over security.
  - Data transfer and charging happen on the same port.

Trustwave®

Summary

- The core threat isn't the kiosk, it is:
  - A design that chose usability over security.
  - Data transfer and charging happen on the same port.
- The complexity goes beyond the Kiosk.
  - Malware infecting PCs/Laptops used to infect phones.
  - Phones used to infect PCs/Laptops and Kiosks.

Trustwave®

Summary

- The core threat isn't the kiosk, it is:
  - A design that chose usability over security.
  - Data transfer and charging happen on the same port.
- The complexity goes beyond the Kiosk.
  - Malware infecting PCs/Laptops used to infect phones.
  - Phones used to infect PCs/Laptops and Kiosks.
- It is not just phone malware.
  - Monitoring/Tracking people based on USB device ID
  - Stolen personal information, Blackmail, etc...

Trustwave®

Thank You!

- Wall of Sheep
- Iggy, Riverside, Cedoxx and the other sheep shepherds
- Irvine Underground

Contact Information:

Email: rrowley@trustwave.com
Twitter: @iamlei
Github: rawrly

Trustwave®