



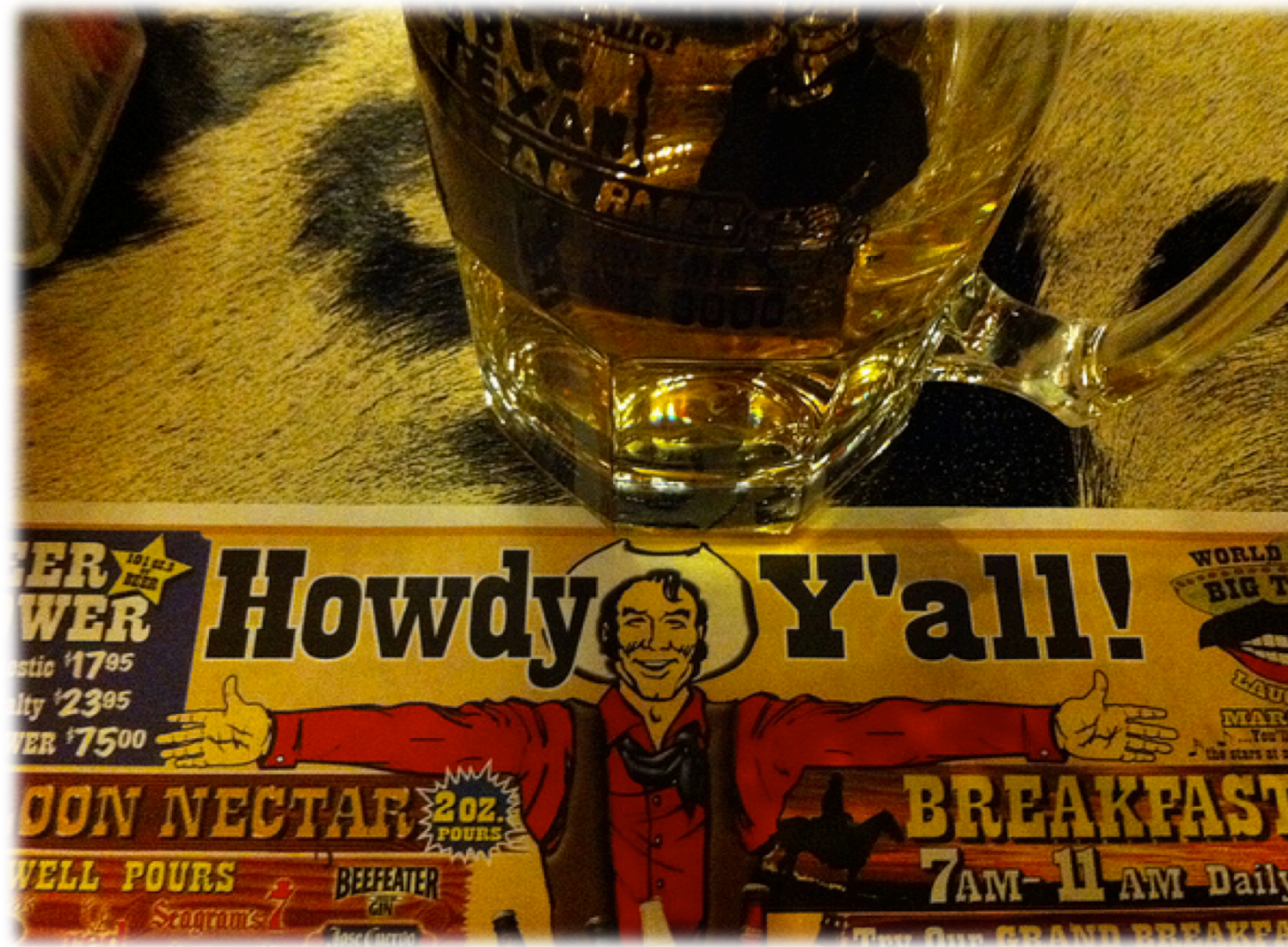
Mobile Snitch

CONFidence 2012

Pr
Luiz Eduar
le(at)trus

Agenda

- Intro
- Motivations
- Current "issue"
- Profiling
- Mitigation Tips
- Future



Whois Luiz Eduardo

Head of SpiderLabs LAC

Knows a thing or two about WiFi

Conference organizer (YSTS & SilverBullet)

Amateur photographer

le/at/ trustwave /dot/ com

@efffn



Whois Rodrigo Montoro

Security Researcher at Trustwave/Spiderlabs

- Intrusion Detection System Rules
- New ways to detect malicious activities
- Patent Pending Author for methodology to discover malicious digital files

Speaker

- Toorcon, SecTor, .FISL, Conisli, CNASI , OWASP Appsec Brazil, H2HC (São Paulo and México)

Member of Malwares-BR Group / Webcast Localthreats

Member and Coordinator

Support Brazilian Community

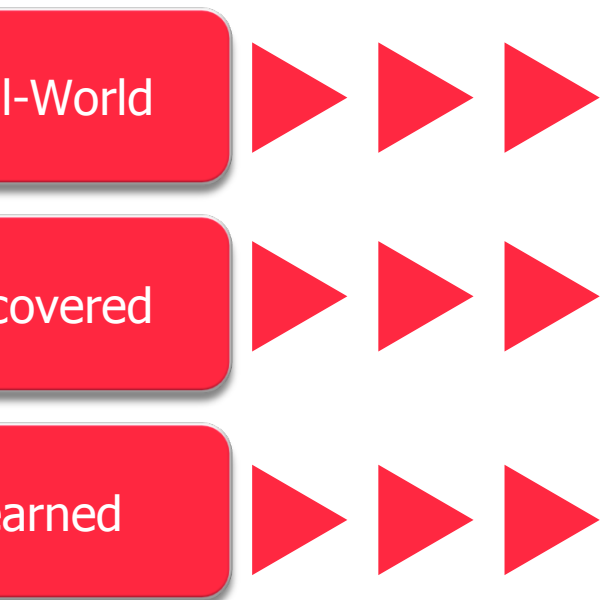
- Snort Rules Library for Brazilian Malwares



Trustwave SpiderLabs®

Trustwave SpiderLabs uses real-world and innovative security research to improve Trustwave products, and provides unmatched expertise and intelligence to customers.

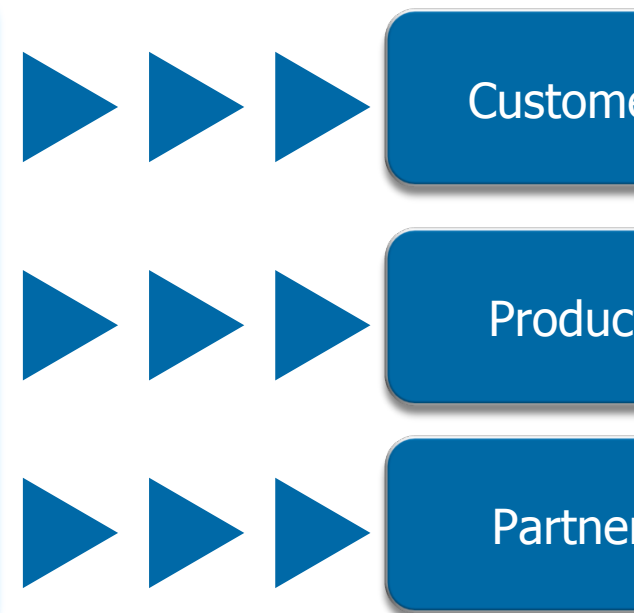
THREATS



Trustwave®
SpiderLabs®

Response and Investigation (R&I)
Analysis and Testing (A&T)
Research and Development (R&D)

PROTECTION



Goals of this Talk

Information about the data your mobile devices broadcast
Possible implications of that

Raise awareness of public in general in regards to mobile privacy

motivations

previous WiFi Research

patterns of travel

client-side / targeted attacks and Malware
spreading

very initial thoughts of this talk presented at
PlayThreat 2011

very very initial WiFi-based devices location at
FloorCon Seattle 2008)



Disclaimer

Definitive Goal

Ability to fingerprint a PERSON based on the **information** given by their mobile device(s)

Passive information gathering of

- Automatic "LAN/Internal" protocols
- Non-encrypted traffic analysis (security flaws / features / non-confidential info)



Current "issue"

Massive adoption of mobile devices

Usability vs. Security

- Networking Protocols
 - Broadcast / Multicast (and basic WiFi operation)
 - And...



MOD

BYOD

Security as we know it

- protect the infrastructure
- protect the user, once it's in the protected network

the newER buzzword: BYOD Security

doesn't solve the privacy issue

Privacy Matters?



can haz ZeroConfig

Used by most mobile devices

Discovery, Announcement & Integration with (mostly) home devices

- Multimedia products
- IP Cameras
- Printers

Yet, always on and automatic

Zero configuration networking allows devices such as computers and printers to connect to a network automatically without zeroconf, a network administrator must set up services..."

ZeroConfig Protocols

mDNS

UPnP SSDP (Simple Service Discovery Protocol)

SLP (Service Location Protocol)

PV6)

Work of
Monitoring
Protection
Knowledge
etc...

DNS is evil then?

o, how does it work?

Data Acquisition (Passive)

Filters

Compare with Existing Info

- First Search
 - Internet Search
 - Applications (Netbios / Services)

Third Party

- Arp Poisoning
- Extra pcaps
- Info correlation
- Additional Internet Search



Profile Creation

- Domain Request Info
- IP / Geolocation
- Locations (collection)
- Contacts
- Company info
- Personal Network
- Softwares
- etc

Data Acquisition (mdns - multicast)

port == 5353

Expression... Clear Apply

Time	Source	Destination	Protocol	Length	Info
19:40	10.0.204.228	224.0.0.251	MDNS	371	Standard query PTR _apple-mobdev._tcp
19:40	fe80::226:bbff:fe11:880d	ff02::fb	MDNS	391	Standard query PTR _apple-mobdev._tcp
19:40	fe80::462a:60ff:fe93:654	ff02::fb	MDNS	319	Standard query response PTR, cache fl
19:40	10.0.204.228	224.0.0.251	MDNS	81	Standard query PTR _sane-port._tcp.lo
19:40	fe80::462a:60ff:fe93:654	ff02::fb	MDNS	319	Standard query response PTR, cache fl
19:40	10.0.204.178	224.0.0.251	MDNS	320	Standard query response PTR, cache fl
19:40	10.0.204.178	224.0.0.251	MDNS	320	Standard query response PTR, cache fl
19:40	fe80::42d3:2dff:fed9:2e8e	ff02::fb	MDNS	340	Standard query response PTR, cache fl
19:40	10.0.204.100	224.0.0.251	MDNS	310	Standard query response PTR, cache fl
19:40	fe80::1a34:51ff:fe35:c9c9	ff02::fb	MDNS	330	Standard query response PTR, cache fl
19:40	fe80::654:53ff:fe5d:1c40	ff02::fb	MDNS	323	Standard query response PTR, cache fl
19:40	10.0.204.226	224.0.0.251	MDNS	303	Standard query response PTR, cache fl
19:40	fe80::654:53ff:fe5d:1c40	ff02::fb	MDNS	323	Standard query response PTR, cache fl
19:40	10.0.204.76	224.0.0.251	MDNS	136	Standard query PTR _airplay._tcp.local
19:40	fe80::cabc:c8ff:fe40:e2a6	ff02::fb	MDNS	156	Standard query PTR _airplay._tcp.local
19:40	10.0.204.76	224.0.0.251	MDNS	136	Standard query PTR _airplay._tcp.local

dns query

Time	Source	Destination	Protocol	Length	Info
08:44	fe80::5e59:48ff:fe45:dbfb	:::1	MDNS	341	Standard query response PTR, cache flush
08:44	192.168.33.106	224.0.0.251	MDNS	321	Standard query response PTR, cache flush

Additional RRs: 1

ies

Authoritative nameservers

Rodrigo-Montoro.local: type A, class IN, addr 192.168.33.106

Name: Rodrigo-Montoro.local

Type: A (Host address)

0000 0000 0000 0001 = Class: IN (0x0001)

..... = Cache flush: False

Time to live: 2 minutes

Data length: 4

addr: 192.168.33.106 (192.168.33.106)

Rodrigo-Montoro.local: type AAAA, class IN, addr fe80::5e59:48ff:fe45:dbfb

Name: Rodrigo-Montoro.local

Type: AAAA (IPv6 address)

0000 0000 0000 0001 = Class: IN (0x0001)

..... = Cache flush: False

Time to live: 2 minutes

mdns "passive port scan"

fe80::226:bbff:fe11:880d	ff02::fb	MDNS	312 Standard query ANY	[redacted]	_ssh
fe80::226:bbff:fe11:880d	ff02::fb	MDNS	312 Standard query ANY	[redacted]	_ssh
fe80::226:bbff:fe11:880d	ff02::fb	MDNS	312 Standard query ANY	[redacted]	_ssh

Protocol, Src Port: mdns (5353), Dst Port: mdns (5353)

System (query)

Transaction ID: 0x0000

Standard query

5

0

RRs: 5

RRs: 0

Active nameservers

_ssh._tcp.local: type SRV, class IN, priority 0, weight 0, port 22, target [redacted].local

_sftp-ssh._tcp.local: type SRV, class IN, priority 0, weight 0, port 22, target [redacted].local

_rfb._tcp.local: type SRV, class IN, priority 0, weight 0, port 5900, target [redacted].local

_net-assistant._udp.local: type SRV, class IN, priority 0, weight 0, port 3283, target [redacted].local

Data Acquisition (Netbios - Broadcast)

	Time	Source	Destination	Protocol	Length	Info
60	19:40	10.0.204.166	10.0.255.255	NBNS	92	Name query NB EDISONVERA-PC<20>
206	19:40	10.0.39.35	10.0.255.255	NBNS	92	Name query NB ISATAP<00>
213	19:40	10.0.204.166	10.0.255.255	NBNS	92	Name query NB EDISONVERA-PC<20>
214	19:40	10.0.39.35	10.0.255.255	NBNS	92	Name query NB ISATAP<00>
838	19:40	10.0.204.217	10.0.255.255	NBNS	92	Name query NB DCP<00>
1072	19:40	10.0.204.217	10.0.255.255	NBNS	92	Name query NB DCP<00>
1212	19:40	10.0.204.217	10.0.255.255	NBNS	92	Name query NB DCP<00>
2023	19:40	10.0.204.220	10.0.255.255	NBNS	92	Name query NB RECEPCION<20>
2236	19:40	10.0.204.220	10.0.255.255	NBNS	92	Name query NB RECEPCION<20>
2470	19:40	10.0.204.220	10.0.255.255	NBNS	92	Name query NB RECEPCION<20>
2524	19:40	10.0.202.116	10.0.255.255	NBNS	92	Name query NB MIL<1d>
2525	19:40	10.0.202.116	10.0.255.255	NBNS	92	Name query NB INICIOMS<1d>
2526	19:40	10.0.202.116	10.0.255.255	NBNS	92	Name query NB JUANCBOCANEGRA<20>
2652	19:40	10.0.202.116	10.0.255.255	NBNS	92	Name query NB JUANCBOCANEGRA<20>
2657	19:40	10.0.204.220	10.0.255.255	NBNS	92	Name query NB RECEPCION<20>
2806	19:40	10.0.202.116	10.0.255.255	NBNS	92	Name query NB SUDAMERICA<1d>

netbios query

Time	Source	Destination	Protocol	Length	Info
19:40	d0:c1:b1:f4:14:23	Broadcast	ARP	60	Who has 10.0.0.1? Tell 10.0.163.189
19:40	10.0.204.166	10.0.255.255	NBNS	92	Name query NB EDISONVERA-PC<20>

2: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)

Internet II, Src: IntelCor_aa:e4:3a (00:1c:bf:aa:e4:3a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 10.0.204.166 (10.0.204.166), Dst: 10.0.255.255 (10.0.255.255)

Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)

OS Name Service

Transaction ID: 0x9991

Flags: 0x0110 (Name query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

EDISONVERA-PC<20>: type NB, class IN

Name: EDISONVERA-PC<20> (Server service)

Type: NB

Class: IN

Key Information



First Search

Info: Rodrigo-Montoro.local,Rodrigo-Montoro.local

ating to Google (or any other search tool)

o Montoro inurl:facebook.com

o Montoro inurl:linkedin.com

o Montoro inurl:twitter.com

e images

o+Montoro

ro Rodrigo

ro

y other Google search for that matter.



Rodrigo Montoro inurl:facebook.com



quisar

Aproximadamente 15.600 resultados (0,22 segundos)

[Rodrigo Montoro | Facebook](#)

pt-br.facebook.com/montororodrigo

Participe do Facebook para se conectar com **Rodrigo Montoro** e outros que você talvez conheça. O Facebook oferece às pessoas o poder de compartilhar e ...

[Rodrigo Montoro Profiles | Facebook](#)

www.facebook.com/public/Rodrigo-Montoro

View the profiles of people named **Rodrigo Montoro** on Facebook. Join Facebook to connect with ... Search Results for **Rodrigo Montoro**. **Rodrigo Montoro**Add ...

[Rodrigo Montoro | Facebook](#)

pt-pt.facebook.com/people/Rodrigo-Montoro/100002442849439

at



-  Mural
-  Informações**
-  Fotos
-  Amigos

Amigos (710)

-  **Vitor Montoro**
-  **Daniel Ribeiro**
-  **Margarida Gutie...**


Rodrigo Montoro

 Trabalha na empresa **Casan**  Estudou na instituição de ensino **UFSC**

Trabalho e educação

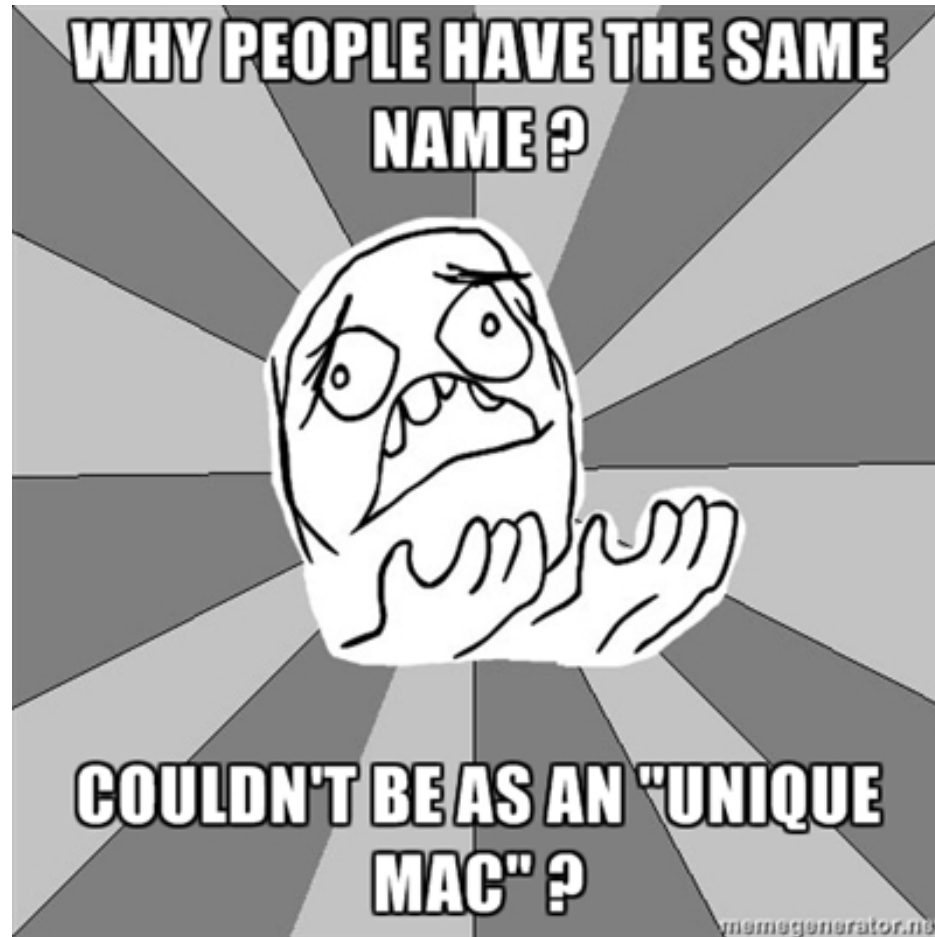
Empregadores  **Casan**

 **Universidade Federal de Santa Catarina**

Ensino superior  **UFSC**

Ensino médio  **Colegio Objetivo**

odrigo is not that famous (yet)...



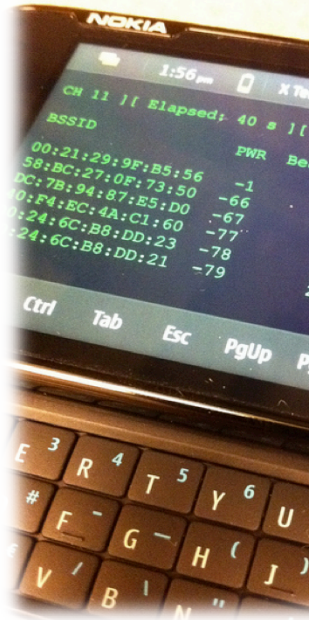
we could use third-party info

ARP Spoofing

new pcaps

in depth request analysis

- http objects rebuild (oh yeah)
- Plain-text request
- Who wants a cookie ?
- Usernames (we don't want passwords .. At least, not now)
- GeoIP / Domains
- SSIDs databases
- Image EXIF info



arp Spoofing



Difficult level: -10

```
# arpspoof -i eth0 192.168.0.1
```

* Don't forget to enable ip_forward

ew pcaps

Cloudshark

pcapr

Sniffing random locations

Create an online repository ?

-Agents (-e http.user_agent http.request.method == GET)

a/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.83 Saf

a/5.0 (Macintosh; U; Intel Mac OS X 10_6_7; en-us) AppleWebKit/533.21.1 (KHTML, like Gecko) Vers

Safari/533.21.1

vial/5.810

a/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A405

rForBlackBerry/2.1.0.28 (BlackBerry; U; BlackBerry 9300; es) Version/5.0.0.846

a/5.0 (Linux; U; Android 2.1-update1; es-ar; U20a Build/2.1.1.A.0.6) AppleWebKit/530.17 (KHTML, li

) Version/4.0 Mobile Safari/530.17 [FBAN/FB4A;FBAV/1.8.4;FBDM/

ty=0.75,width=320,height=240};FBLC/es_AR;FB_FW/1;FBCR/CLARO;FBPN/com.facebook.katana;F

FBSV/2.1-update1;]

We are the good guys ...

```
/var/log/snort/alert | grep "\[.*\]" | sort | uniq -c | sort -nr
```

```
[**] [1:100000236:2] GPL CHAT Jabber/Google Talk Incoming Message [**]
```

```
[**] [1:100000233:2] GPL CHAT Jabber/Google Talk Outgoing Message [**]
```

```
[**] [1:2010785:4] ET CHAT Facebook Chat (buddy list) [**]
```

```
[**] [1:2100538:17] GPL NETBIOS SMB IPC$ unicode share access [**]
```

```
[**] [1:2014473:2] ET INFO JAVA - Java Archive Download By Vulnerable Client [**]
```

```
[**] [1:2012648:3] ET POLICY Dropbox Client Broadcasting [**]
```

```
[**] [1:2011582:19] ET POLICY Vulnerable Java Version 1.6.x Detected [**]
```

```
[**] [1:2006380:12] ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
```

```
[**] [1:2002878:6] ET POLICY iTunes User Agent [**]
```

```
[**] [1:100000230:2] GPL CHAT MISC Jabber/Google Talk Outgoing Traffic [**]
```

Person "MACnification"

Mac Address

Username

Pictures

Facebook

LinkedIn

Twitter

Locations

Company

Softwares

Extras

Infected ?



next time we meet...



Mitigation" Tips

Name the device: Never use your name / last name in your device

Careful where you use your mobile

Turn off WiFi (BlueTooth and etc) when not using it

(Bonus!) Consider removing some SSID entries from your device.

But why?

onus!

Bring Your Own Probe Request
Bluetooth



Disconnected Devices & SSIDs

Company

People

SN #s

Hotel

School

Event

Airport

Lounges

. and

Free Public WiFi

```
C, SSID="Movistar-Vex", SSID="VENETO-W"  
C, SSID="IGNACIO7", SSID="WebSTAR"  
C, SSID="Movistar-Vex", SSID="SKOENEKA"  
C, SSID="IGNACIO7", SSID="GVT"  
C, SSID="Capri Polanco", SSID="SALON VIP LAN"  
C, SSID="INFINITUM3fd", SSID="WebSTAR"  
C, SSID="Capri Polanco", SSID="Edward"  
C, SSID="LT15i", SSID="Fiesta_Inn"  
C, SSID="default", SSID="Nexxt Solutions"  
C, SSID="V-Net de VIV", SSID="WiFi-Radisson 12"  
C, SSID="Radisson Res", SSID="Cabritos"  
C, SSID="HCB300", SSID="SALA VIP IBERIA"  
C, SSID="Connectify-IF", SSID="linksys"  
C, SSID="reforma410-16", SSID="Purcell-Rosas"  
C, SSID="INFINITUM3fd", SSID="Aeronet"  
C, SSID="Radisson Res", SSID="INFINITUM20F1CE"  
C, SSID="HCB300", SSID="link"  
C, SSID="Connectify-IF", SSID="Mangosplus"  
C, SSID="Capri Polanco", SSID="Taverna de Benni"  
C, SSID="INFINITUM3fd", SSID="Habitaciones Hot  
C, SSID="LT15i", SSID="link"
```

SSID="Toronto Pearson Wi-F

SSID="Fran Home"

SSID="mack"

SSID="DigitalCenterHotspot

SSID="paulistania"

SSID="Wsangari1"

SSID="ASAS"

SSID="home"

SSID="SurfNet"

SSID="WSangari1"

SSID="Toronto Pearson Wi-F

SSID="Fran Home"

SSID="mack"

SSID="jack-laptop-wireless

SSID="RedeWiFiInfraero"

SSID="DigitalCenterHotspot

SSID="Wsangari"

SSID="SurfNet"

SSID="WSangari1"

Careful with the New Features

It might affect (event more) your privacy....



uture ...

Website for profile feed collaboration?

- Macprofiling.com
- Whoisthismac.com
- Followthemac.com
- ISawYouSomewhereAlready.com

Social Engineer

- SET (Social Engineer Toolkit) integration
- Maltego

Others

Additional Resources

Download the Global Security Report: <http://www.trustwave.com/GS>

Read our Blog: <http://blog.spiderlabs.com>

Follow us on Twitter: @SpiderLabs / @efffffn / @spookerlabs