# Mobile Intrusion:

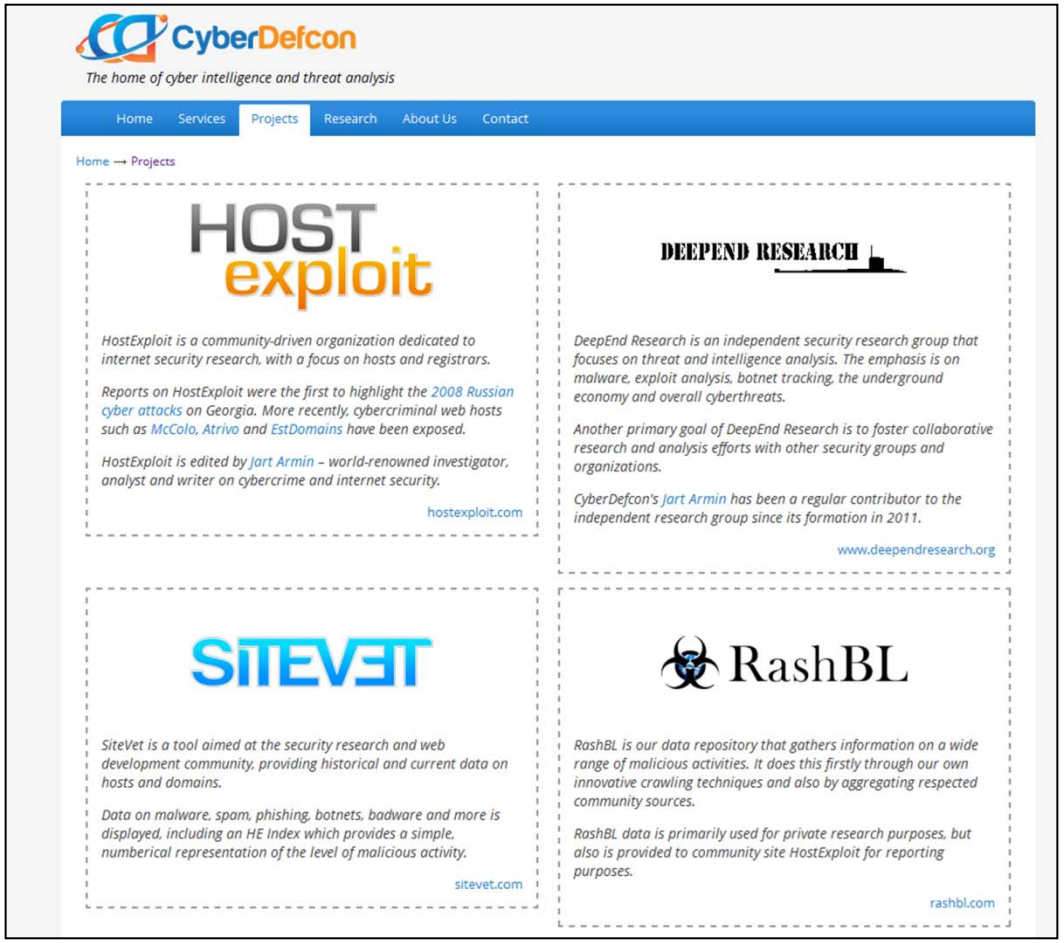
## From State Sponsorship to the Cybercrime Plexus


Jart Armin

HostExploit

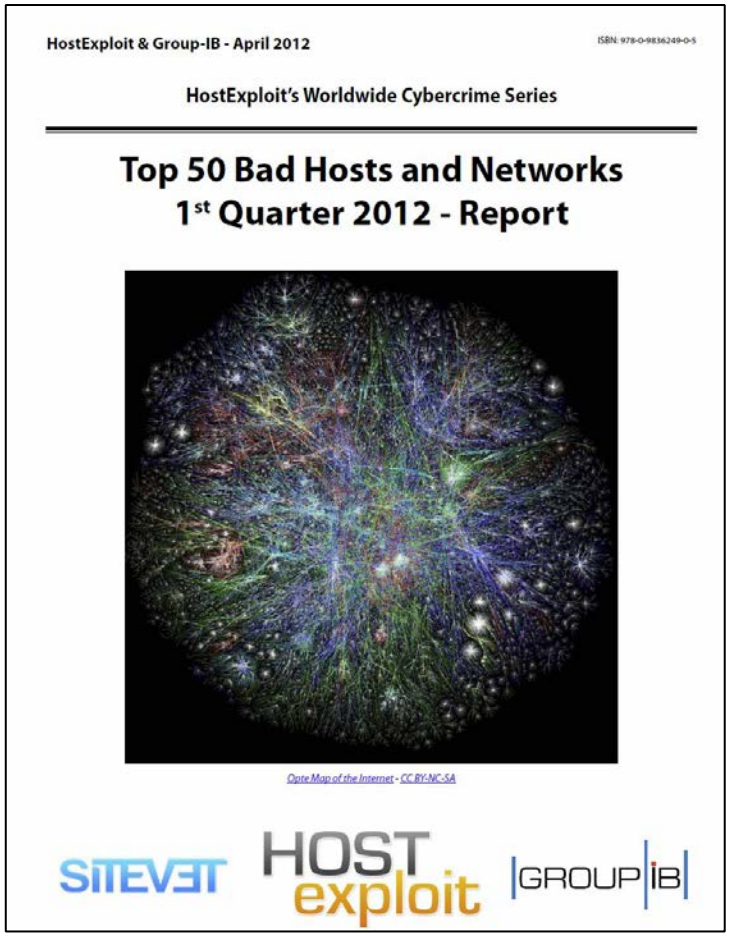
CyberDefcon Ltd


Specialist international team via HostExploit and CyberDefcon that provides cybercrime analysis and quarterly reports on all the world's hosts and Internet servers.




HOST exploit

SITEVET





# Mobile Intrusion – Define?

# Categorizing Mobile Intrusion – Bad?

- **Intrusion** - Any set of actions attempting to compromise the confidentiality, integrity or availability of the system by entering, seizing network data or violating a user's privacy. Classification of intrusion as an illegal act is country specific.

- **Spyware**- The gathering of information via a secret or duplicitous program to record a user's habits, browser and social networking activities, search history and preferred applications.

- **Phone Hacking** - The remote, unauthorised access of data stored in another person's phone, usually in order to manipulate, or listen to, voicemail messages. Defects in mobile chips or devices enables a hacker to then make calls for free or harvest personal information such as addresses and phone numbers.

# Categorizing Mobile Intrusion – Grey?

- **Monitoring** - Listening in to voice conversations or viewing the activity of phone calls, text messages, internet access, emails, by logging who sends what and when. Laws on monitoring vary according to state/country.

- **Mobile Tracking** – Attaining the current position of a mobile phone via its roaming signals, or via GPS. The collection and use of location data is limited according to country specific law, e.g. stingray .....

- **Pro-Active Mobile Forensics** - Strategies used to identify a risk profile based on rules applied to the data footprint of an organization's mobile devices or of BYOD (bring your own devices), forming the basis of an early warning system.

- **Tapping / Wiretapping** - The remote, unauthorised access of data stored in another person's phone, usually in order to manipulate, or listen to, voicemail messages. Defects in mobile chips or devices enables a hacker to then make calls for free or harvest personal information such as addresses and phone numbers.

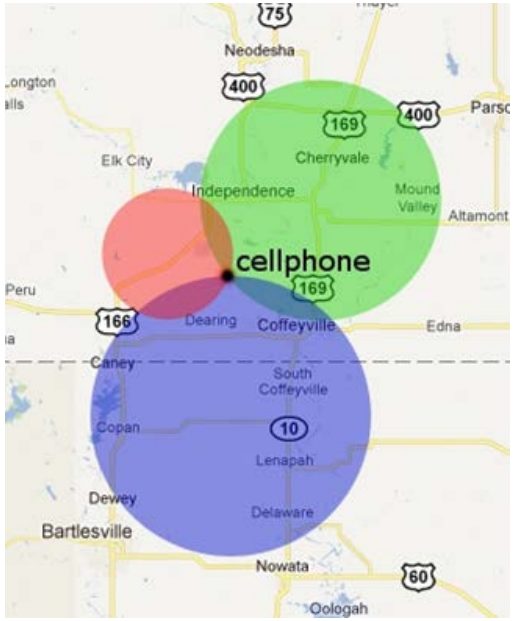
# Mobile Intrusion – Unlawful?

- Lawful intrusion – most countries
- US Federal Wiretap act

Note: The opinion holds that anyone can monitor the unencrypted Wi-Fi communications of anyone else without implicating the Wiretap Act.

- EU – many variations of lawful intrusion
- Example of Sweden – since 2009 log & store all SMS (consensus government)

# Examples – Tracking – 'Stingray'

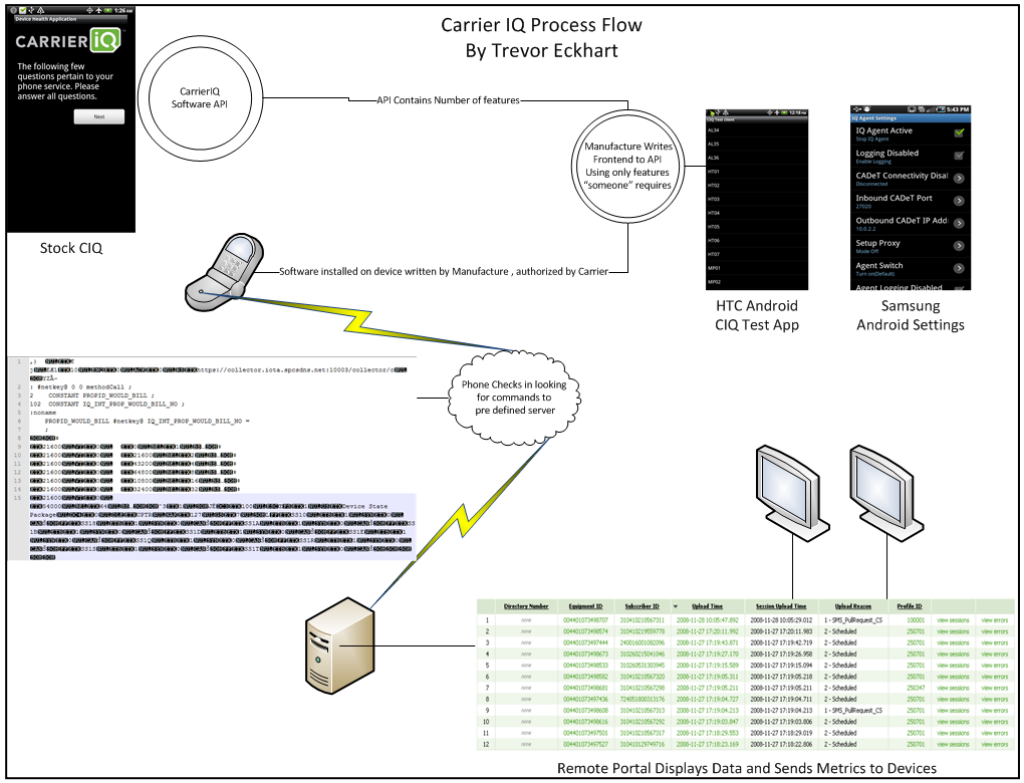




Mobile Phone tracking – cell tower mimicry – no warrant required

# Examples – Hijacking

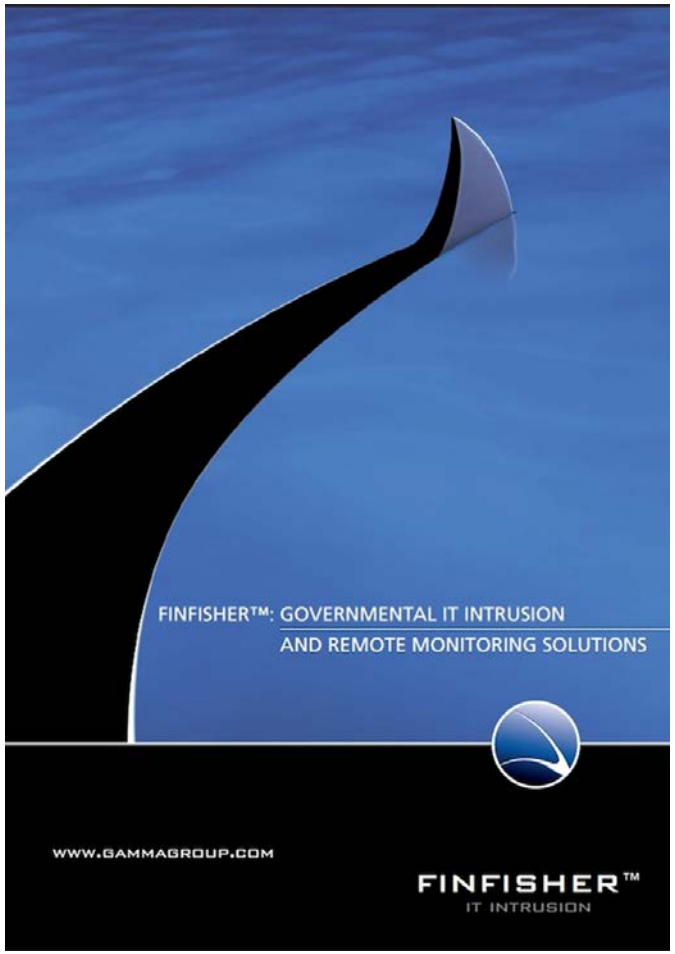

- **0wned / pwn3d – for fun and education**
- **Choose 'Jart's Super Free' Wi-Fi (would you ???? )**
- **28 workshops (5 to 30 participants) from: mil to kids**
- **99% successful on any mobile / smartphone**
- **Objective: 30 minutes from logon to stop re-broadcasting hub**
- **Simply grab the identifiers - acts as the ISP, operator, and finally simulates user actions**

# Examples – Monitoring – 'Carrier IQ'




- Trevor Eckhart – Android App to remove Carrier IQ from the Android smartphone
- Carrier IQ – cease and desist
- EFF – supported Eckhart and Carrier IQ dropped legal threat
- FBI uses for law enforcement purposes

# Examples – Intrusion – 'Finfisher'



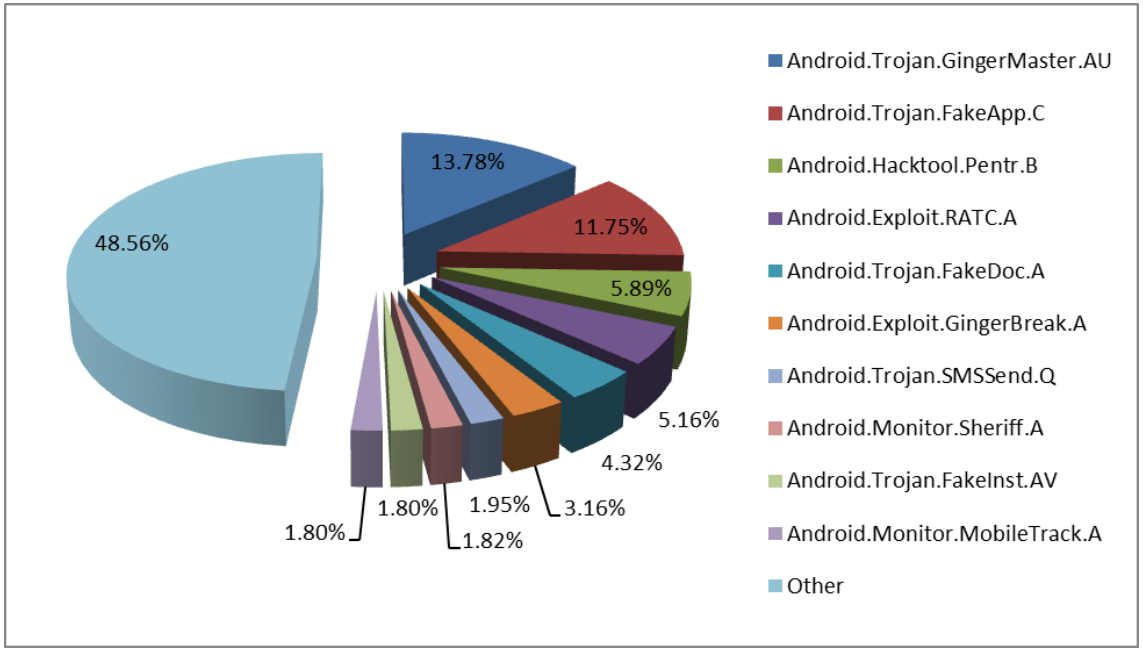

- Recording of common communications like Voice Calls, SMS/MMS and Emails
- Live Surveillance through silent calls
- File Download (Contacts, Calendar, Pictures, Files)
- Country Tracing of Target (GPS and Cell ID)
- Full Recording of all BlackBerry Messenger, iOS, & Android communications
- Covert Communications with Headquarters

# Examples – Monitoring Tool : Android/Flexispy.L


Flexispy.L - monitors the following activities on a compromised device:

- Incoming and outgoing call logs
- SMS messages
- Phonebook addresses
- E-mails
- Browsing history
- Photos

# Examples – Android Malware – Latest Rankings




- **Android.Trojan.GingerMaster.AU**
- The malware uses an exploit against Android 2.3 (known as Gingerbread) and comes bundled with multiple apps that attract unsuspecting users.
- When infected device is rebooted, it launches in background and broadcasts device ids, phone numbers and more by uploading them on a command and control server (Bitdefender)

## Crossover – to – Cybercrime “Who wants the data, where’s the $$$?”



# Smishing

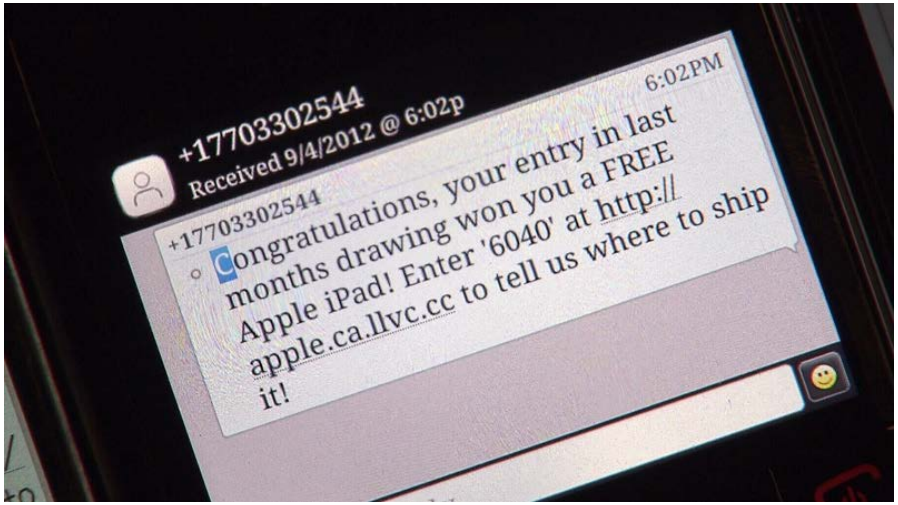
- **Smishing** – SMS based phishing

***ref: Cloudmark , about 30 million smishing messages are sent daily to cell phone users across North America, and Europe.***

- **Smishing** is part of the much larger SMS spam problem.

***In the US alone, there has been an almost 400 % increase in unique SMS spam campaigns in the first half of the year 2012 & 900% in September 2012.***

# Smishing




- Banking SMS
- Micro payments
- Secondary logins
- Online & mobile gaming
- Starbucks
- Coupons
- Webmaster
- Premium porn & SMS

# Smishing – In the Today's News

- **Oct 18th - A 20-year-old hacker has been arrested in northern France for spreading a virus via smartphone "apps" that defrauded thousands of victims.**
- **Prosecutors say he stole tiny sums from 17,000 people, amassing about 500,000 euros ($650,000) in 1 year.**
- **The virus sent a text message without the user's knowledge to a premium-rate number he had set up.**
- **There were also programmes that sent him the log-on codes for gaming and gambling websites to which the victims had subscribed.**

# The State – to – the cybercrime plexus



# Hacking the State

**If the state has the data its not so difficult to conceive its hackable? – One stop shopping?**

- **12 million unique Apple device identifiers – FBI –** (later claimed by 'Blue Toad publishing company' FL)
- **25,000 Euros paid to 0wn an EU police DB**

# Hacking the State



- 80% of LinkedIn = $300,000
- 60% of Facebook = $500,000

- Source of hack = governmental servers

## Conclusions - Discuss?



# Tech Conclusions v Mobile Intrusion

- The main effort for manufacturers is to prevent smartphones from becoming mini ISPs/re-broadcasting hubs.
- Avoid the unit becoming a router and using PPP (Point-to-Point Protocol); through using “mgetty” or similar commands; or in Microsoft Windows RAS (Remote Access Service).
- Best if the platform reveals the phone number of the device only to the smartphone’s modem
- Issue an IPv6 IP and public encryption for each smartphone

# Contact

- Contact presenter at jart@cyberdefcon.com