Beholder

Nelson Murilo
nelson(at)pangeia.com.br

Luiz Eduardo
le(at)atelophobia.net
Agenda

- Who are we?
- Evolution of WiFi attacks
- Attack tools
- Threats
- Solutions
- The inner of Beholder?
- What does Beholder detect?
- What Beholder doesn’t do
- Scenarios
- Futures
Wi-Fi Attacks

beholder DefCon 16
WE RESERVE THE RIGHT TO REFUSE SERVICE TO ANYONE
MiTM
Impersonation

beholder

DefCon 16
Surveillance
Packet Injection
Crypto Cracking

- WEP
- WPA
Client-Side

- AdHocs Circa
Rogue APs

beholder

DefCon 16
Impersonation 2.0

- Evil-twin
- More rogue-aps
Drive-By Pharming
Faster Crypto-Cracking
Rogue Radius Servers
Tools
Solutions?

- Introduction to WIDS...
JUST KIDDING!
State of WIDS
(not the one below)
Any free tools at all?

- Roguescanner
- ??
Here comes Beholder

- No chipset or 802.11 standard limitations (yes, it works on 802.11n)
- Based beacon frames
802.11 Beacons

- (sometimes) more than you can expect
Beholder Detects and Reports

- Changes on AP (ESSID, MAC, Mode)
- Channel changes
- Huge signal level variations
- Missing Aps
- And more...
Your karma is leaking.
Other cool stuff
Things we DON’T do

• Sniffing on any interface types
• Put 802.11 interfaces in monitor mode (hence not checking for de-auths and such)
• WPA/WEP Cracking
• Detect client or AP authentication failed
(some of the) design challenges

• Easy to install and use
• Comprehensive
• Scanning time differences per adapter
• Madwifi “caching” issue
• Make it with as few dependencies as possible
• Written in a fast language
• C Ansi
Caveats

• For now...
Futures of Beholder

Try a Reading Yourself
1-800-997-5219

www.MISSCLEO.com
Karma Detection
Scenarios
checking for similar essids via RegEX

```
beholder -r "myne[t7]s.*" wifidev
```

Networks:
- mynets-wifi
- mynets
- mynets
- mynets
- default

Networks represented by routers and connected devices.
Scenarios
Huge environments

`beholder -s wifidev`

Syslog server

`swatch` calling email/sms/snmp trap/etc
Demo?
And remember

- Even great tools might not help in all situations
Beholder could help a bit though
What's next on wifi attacks?

- 802.11n rogue aps? Nahh
- 802.11n greenfield DoS type of attacks? (maybe)
Now available at

http://www.beholderwireless.org
thanks!