Building the Perfect Evil Twin

Rich Mogull
Securosis, LLC
Aren't Evil Twins Old News?

Yes, but so is Jimmy Buffett and he still sells out more shows than god.
Evil Twin 101

1. Inject de auth
2. Overpower AP and MIM
3. Enjoy pwnage
Evil Twin 501

- Self contained
- High powered
- Drop and leave
- Multiple exploit options
Exploit Options

- Exploit browser on splash screen and install trojan for later access.
- Sniff/MITM traffic.
- Inject HTML
Why This Matters?

- There's nothing new here, but this attack will be effective for years to come.
- It's a great vector for any days or other exploit advancements.
- Enterprises are well protected, but distributed enterprises are more vulnerable.
- Own the consumer, eventually you own the enterprise.