



Presentation Outline

- ❖ LANDMARK – automated tradecraft to further expand CNE covert infrastructure





LANDMARK

- ❖ CSEC's Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration
- ❖ 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible





LANDMARK – the recent past....

- ❖ February 2010
- ❖ Operation encompassing the whole of LONGRUN solely using OLYMPIA (CSEC's network knowledge engine with automated tradecraft)
- ❖ 8 teams of 3 network exploitation analysts busy for 5-8 hours
- ❖ A list of 3000+ potential ORBs



LANDMARK today...

- ❁ Network analysis tradecraft to determine vulnerable devices has been encoded within OLYMPIA





GSM provider

- ✳ NSA TAO requested assistance gaining access to the network
- ✳ Network analysis using OLYMPIA:
 - ✳ DNS query to determine IP address
 - ✳ IP address to network range
 - ✳ Network range to port scan
 - ✳ Are there any vulnerable devices in that range?
- ✳ Duration: < 5 minutes