Evil Twin Wireless Attack

Sam Gaudet


MTUG
Peers & Beers!
Co-sponsored by:
aruba
NETWORKS
an HP company

$ whoami

Disclaimer

Do not use this information against others.

Do not perform these types of attacks
on equipment you do not own.

Be cognizant of the law (FCC).

Evil Twin

MTUG
txpower 15

MTUG

MTUG
txpower 30
wifijammer.py

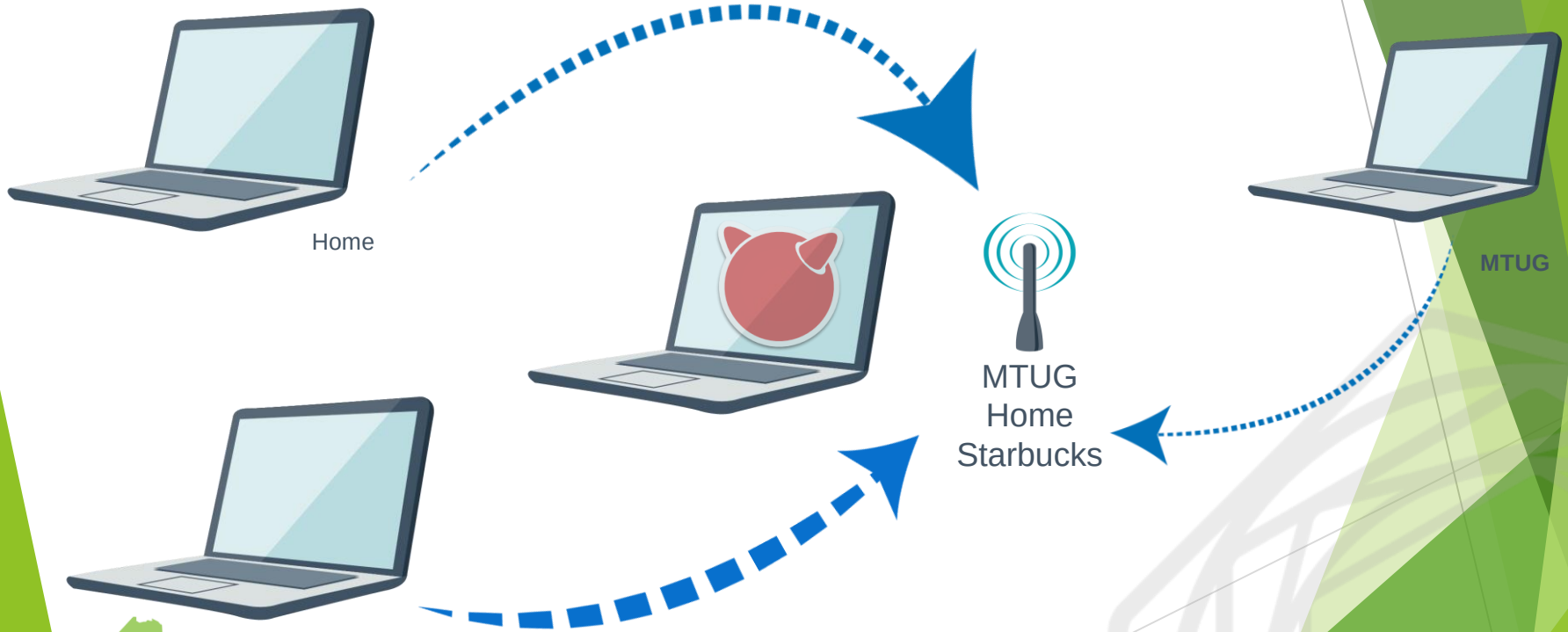
MTUG

Demo

Other attacks

- Ettercap
- sslstrip
- Evilgrade (fake updates)
- Credential harvesting
- Social-Engineer Toolkit (SET)

Karma



Commercial implementations

Mitigations and safeguards

- 802.1x / NAC
- VPN
- Common sense
  - Context of SSID
  - Nmap the gateway
    - Is 192.168.1.1 Windows/Linux?

Mitigations and safeguards, cont.

- PCI wireless auditing
  - PCI DSS Req. 11.1 & 12.9
- Aruba
  - AirWave RAPIDS
- Nessus & SecurityCenter

Tools used

- Airbase-ng
  - airbase-ng -e MTUG -c 11 -v wlan0
- Ettercap
  - ettercap -i EvilAP -T -q -P dns_spoof -M ARP:remote //192.168.1.103/ //192.168.1.1/
- Urlsnarf
  - urlsnarf -i EvilAP

MTUG

Thank you!

sgaudet@tenable.com

https://www.tenable.com/careers