CENSUS

IT Security Works

Known Beacons Wi-Fi Automatic Association Attack

George Chatzisofroniou

34C3 Chaos Communication Congress, Leipzig, 2017

www.census-labs.com

> Have you ever stayed in a popular hotel?

> Have you ever set-up a Chromecast device?

> Have you ever visited a hotspot that belongs to a Fon (or similar) network?

> Have you connected to the 34C3 Wi-Fi already?

> Well, it is very possible that your device is vulnerable to the Known Beacons attack.

> Known beacons attack

- We set-up a special AP that broadcasts dozens of beacon frames from a “dictionary” of popular **Open WLAN** ESSIDs.
- Victims will automatically connect to our rogue AP due to the “Auto-Connect” flag.

> Dictionary of popular ESSIDs

- Popular Networks
  - "Radisson_Guest", "Marriott_Guest", "hhonors", "Hilton Honors", "walmartwifi" are ESSIDs that exist in hotels and other places of public interest worldwide.
  - Fon-type networks where users share part of their bandwidth, so that they could connect to other members' hotspots.
  - "public", "airport", "test“ and other ESSIDs that are common in different setups across the world.
  - “ChromecastXXXX” where the last 4 digits can be brute-forced
  - Many others!
- Our dictionary is getting bigger and bigger thanks to the awesome contributions of the Wifiphisher community

> But isn't this KARMA?

- No! KARMA attack exploits the active scanning for networks the stations have associated with in the past
- Most Network Managers nowadays are protected by switching to passive scanning
- The Known Beacons attack exploits only the Auto-Connect flag
  - All modern Network Managers (except from Windows!) are vulnerable ☺

> Wifiphisher v1.4 coming!

- The new functionality will be incorporated to the new release
  - Comes with roguehostapd (specially patched hostapd for attack purposes)
  - “wifiphisher --knownbeacons”
- Many new features!
- Kudos to Wifiphisher core developers Brian Smith and Anakin Tung, as well as everyone else who helped!

Thank you!

CENSUS

IT Security Works