Behavioral Whitelists of Beaconing Activity

US-CERT: Brian Allen, Robert Annand

**What**

- Create whitelists of beacons for use in incident analysis.

**Why**

Threat Discovery

- "Is something malicious on my network phoning home?"
- Which hosts on my network are 0wn3d?

Situational Awareness

- "What are the normal things that beacon on my network?" Why?
- Need to understand normal to spot abnormal.

**How**

Two approaches

Start small, work up

- One hour, well-known network, specific services
- Pull outbound traffic sample
- Run beacon detection programs on sample
- Create, maintain whitelists
  - Very specific, will miss things

Start big, work down

- Pull large sample
- Run beacon detection programs on sample
- Identify all beacons
- Create and maintain whitelist
  - Lots of noise, false-positives

**Issues**

- Beacons within a single flow not visible
- Lots of beaconing over web ports
- Complete TCP connections
- Low and slow
- Talk to asset owners: policy? What's normal?

**So What?**

Finding malware beacons directly

- But may still need to validate with AV, C2 server lists, etc.
- Finding the normal (precursor for anomaly detection)
- NTP, AV updates, software updates, SNMP, regular data transfers...

This is one example of behavioral sets. Others might include

- Blacklists, High-Volume
- Web servers, destinations never seen before, proxies, clients, etc.

Enables analysts to ask questions like

- Tell me everything I know about this destination in terms of behavior over time.
- Volumes, times, services and behaviors-of-interest will vary.