CCDC Inject

INJECT NAME	Find Beaconing Malware
INJECT ID	SOCS06A

INJECT DESCRIPTION:
Malware often reaches out to the external network looking to locate its command-and-control server, or to exfiltrate information. Develop a technique to detect these beacons.

INJECT DELIVERABLE
Respond with a business memo which provides:

1. What tool, process, feature etc… are you using to know when these beacons are present and potentially understand how they are functioning.
2. Monitor for a period of time, and filter and distill a presentation that shows these beacons (packets) in the network. Explain how they work.
3. Provide evidence of your work using screen shots.