FEINTCLOUD – Laanwj's blog – Randomness

laanwj.github.io/2016/08/28/feintcloud.html

Laanwj's blog

Randomness

Blog About

FEINTCLOUD

In the Equation Group dump many of the implants can announce themselves with beacons, especially the BIOS implants. These beacons are disguised as normal network packets, likely directed at fake hosts, to be intercepted by intermediate infrastructure. The list in BLATSTING `beacon` listening post module gives a possible list of disguises:

```
FEINTCLOUD DNSDIRECT
FEINTCLOUD HTTP1
FEINTCLOUD NTP1
FEINTCLOUD PING-2
FEINTCLOUD PING_1_L
FEINTCLOUD TCPSYN
```

Beaconing would be silly when a host is implanted though remote exploitation as the target IP and the topology of their network is obviously known.

However I suppose that these are used when a host is implanted e.g. along the supply chain and it is unknown where it is going to end up on the network.

It would be interesting to look into this further to get an handle on which networks and hosts are infected. The above kinds of packets are typical ways to hide within a crowd on the internet, but periodical announcements with certain properties may stick out.

The “FEINTCLOUD” name doesn’t seem to turn up anything on Google. Has anyone encountered this project in one of the Snowden documents? It vaguely rings familiar.

Edit 2016-09-04: it looks like BBANJO (BANANABANJO?) in the BANANAGLEE framework is also a beaconing module, and various versions are available in the dump (`Firewall/BANANAGLEE/*/Install/LP/Modules/PIX/BBANJO-*`). May be interesting to reverse-engineer to get more insight. Could be fairly straightforward as local symbols such as `obfuscate_payload1` are still present.

Note: I’m continuing work on reverse-engineering the BLATSTING rootkit and reporting here.

Written on August 28, 2016

Tags: eqgrp malware
Filed under Reverse-engineering