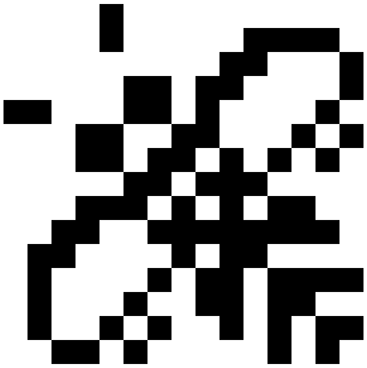
BLATSTING FUNKSPIEL

laanwj.github.io/2016/08/22/blatsting.html



Laanwj's blog

Randomness

Blog About

I’ve done a bit of reverse-engineering on the BLATSTING “modular rootkit” implant which was part of the recent Equation Group leak. I find it interesting as it injects into the Linux kernel, intercepts network traffic, and even injects packets as to redirect browser users to a site with pre-packaged exploits.

There’s probably something to be learned from state sponsored Linux malware, even though the code and the kernels it targets seem to be fairly old.

The details can be found in a gist on github here. I’ll keep this up to date when I find more information. Please suggest changes if you find anything out that I haven’t noticed yet.

(FUNKSPIEL, literal translated “RADIO PLAY”, is the name of a WW2 operation in which Nazis impersonated specific radio operators to send false messages. This was used in the plot of Cryptonomicon by Neal Stephenson. I don’t think MiTM attacks existed back then.)

Written on August 22, 2016

Tags: eqgrp malware

Filed under Reverse-engineering