Saal:	10:30	00:30	Day: 2	Track: Security & Hacking	nA
Simulacron-3					

Title: **Understanding Open Proxies**

Subtitle:

Speaker: **Will Scott**

Short: *Proxies have been around for a while now, but remain poorly understood. I'll share some data on how they are used, what they are used for, and who uses them. To understand open proxies, I've scanned the Internet to track their prevalence, and monitored public statistics interfaces to understand the machines hosting them. 220 TB of traffic flows through open proxies each day, making them one of the largest overlay networks in existence - especially since most operators appear to be running them unintentionally.*

Long: This work is meant to convey some understanding about what's going on with open proxies. These proxies are ubiquitous, but unfortunately not particularly secure. In that capacity, they provide a rare glimpse at what the usage patterns of other indirection systems look like, so that we can learn from their mistakes. This work began by monitoring open proxy aggregators to understand the churn and distribution of proxies. We contacted operators in several countries to understand their intentions in running these services, and ended up helping them fix their configurations. We also monitored the public statistics interfaces provided by squid and polipo proxies, and used them to record a sample workload experienced by open proxies. From this, we are able to understand the distribution of client locations, characterize the size and cache-ability of requests, and pull out high-level observations on the use of automated versus manual traffic.