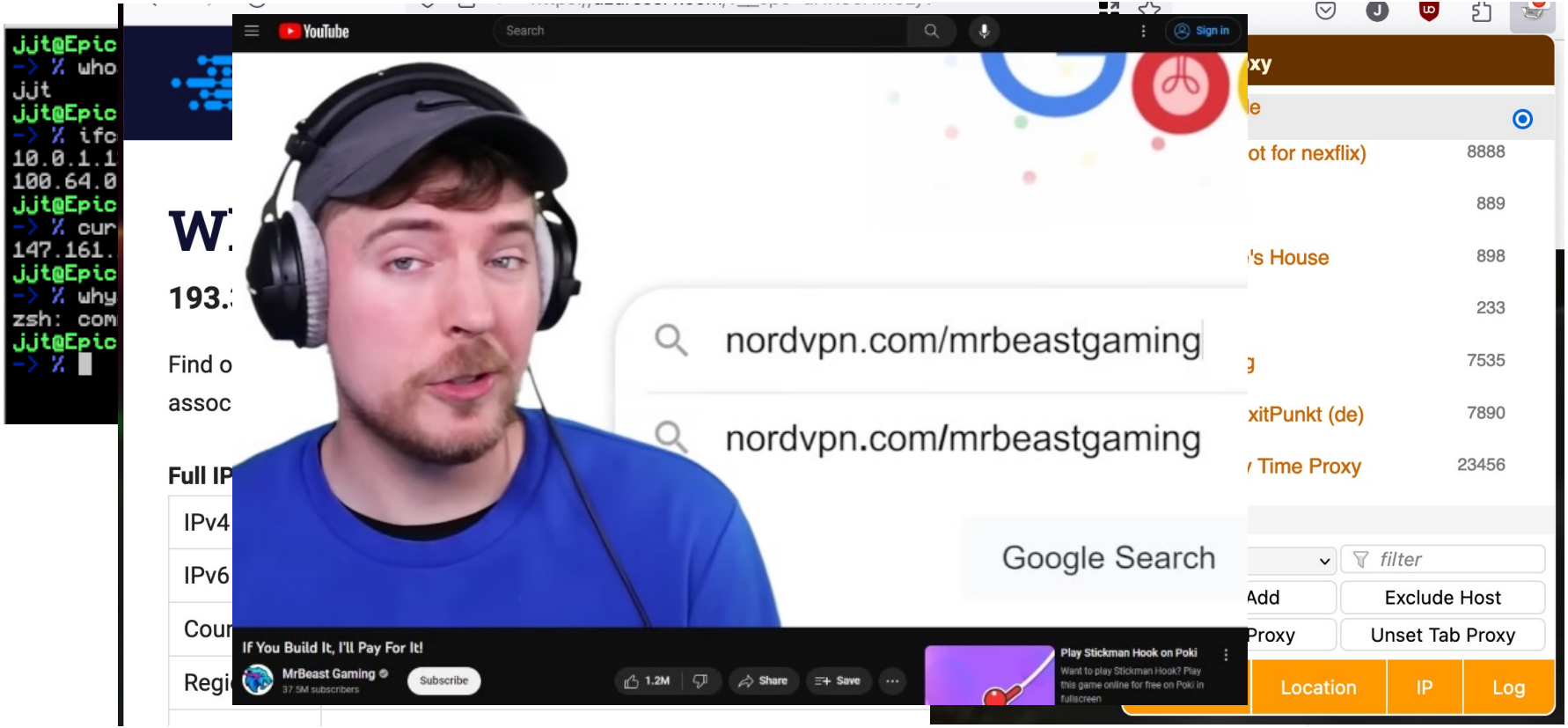
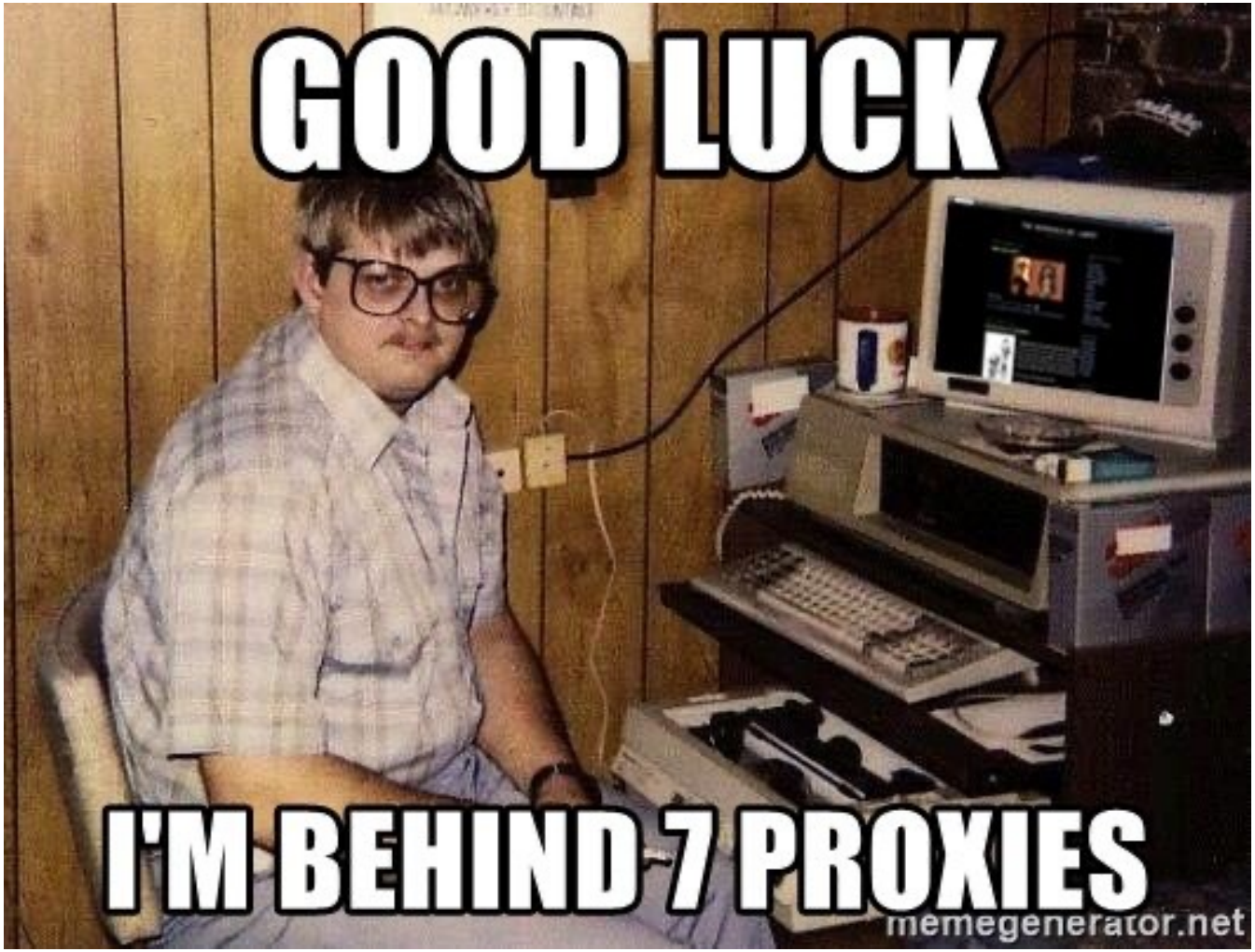
IP Addresses Are Terrible Security Indicators

James Tucker


UNTRUSTED
CONSOLE
DC POWER
5V 1.5A
Un-Trusted Zone
Trusted Zone

Where Am I right now?




GOOD LUCK
I'M BEHIND 7 PROXIES
memegenerator.net


DANGER
ENTER AT
OWN RISK

THE PROBLEM

Runs recon
1 Scopes environment to find vulnerable applications

Distributes ransomware
Uses infrastructure to push ransomware org-wide

IDENTITY

- A foundation of ZTNA
- Could be a Human, a machine, or a workload.
- Location is secondary and contextual

External Attackers

- IP is an inverse measurement for trust. (AS6939, I’m looking at you)
- Usually background noise
  - Geo Blocking
  - Individual IPs Block - and move on.
- Nation State Actors

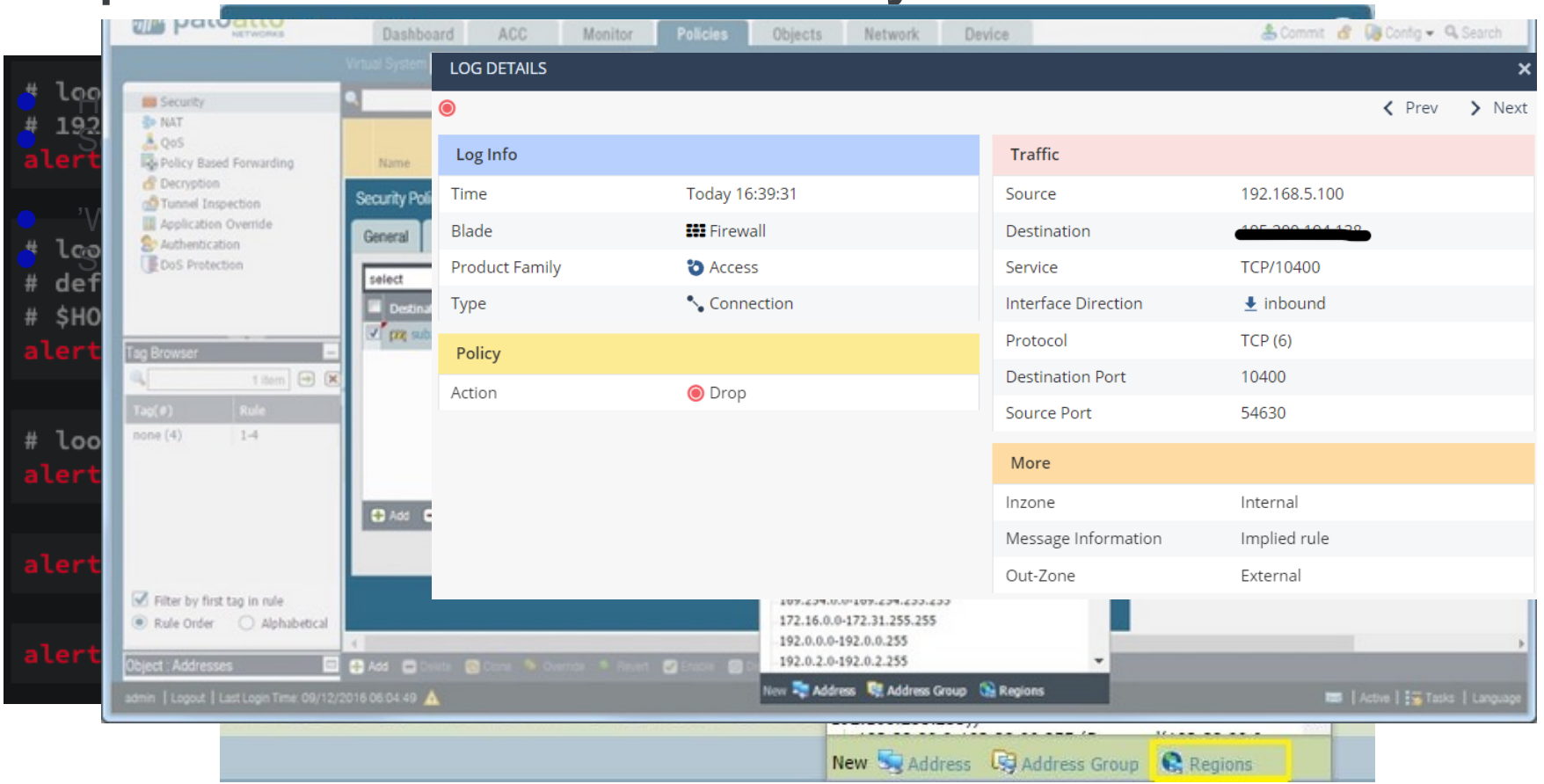
Internal Attackers

- First What is ’Inside’
- Your Users, workloads, and third parties are the perimeter

- We have the advantage of more tooling, more control as defenders.
  - Identity, Access Context, and Device Context provides more.

- ZTNA provides a way to limit attack surface, reduce blast radius and minimize attack windows.

The problem of Zero Trust in Security Incidents



Final Thoughts

- There is no such thing as a ‘trusted network’
- Zero Trust is simply the recognition of this
- Starting with Identity will provide more meaningful security outcomes.
- Separating your network and your security will provide better results, and greater operational flexibility.