



# IP Addresses Are Terrible Security Indicators

James Tucker



Un-Trusted Zone

Trusted Zone

# Where Am I right now?

The image is a composite of several elements:

- Terminal Window (Left):** Shows a series of commands and their outputs:

```
jjt@Epic -> % who
jjt
jjt@Epic -> % ifconfig
10.0.1.1
100.64.0
jjt@Epic -> % curl
147.161.
jjt@Epic -> % why
zsh: com
jjt@Epic -> % █
```
- Browser Window (Right):** Shows a Google search for "nordvpn.com/mrbeastgaming". The search results list several proxy servers:

Proxy Name	Count
ot for nexflix	8888
	889
's House	898
	233
	7535
xitPunkt (de)	7890
r Time Proxy	23456
- YouTube Video (Background):** A video player showing a man with a beard and headphones, wearing a blue t-shirt and a grey cap. The video title is "If You Build It, I'll Pay For It!". The channel is "MrBeast Gaming" with 37.3M subscribers. The video has 1.2M likes and a share button.
- Terminal Output (Bottom Left):** Shows the output of the terminal commands, including IP addresses and a list of proxy servers.

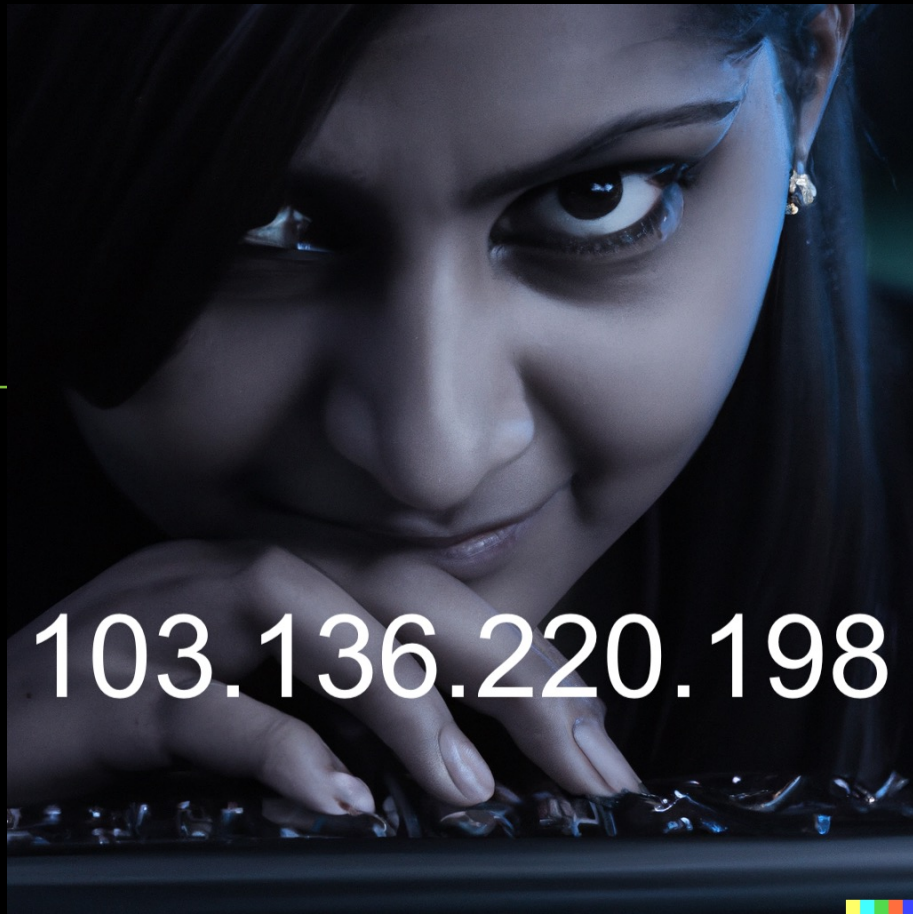
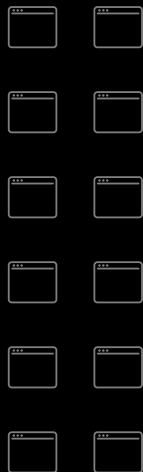
**GOOD LUCK**

**I'M BEHIND 7 PROXIES**

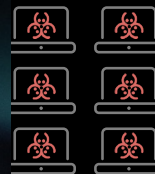
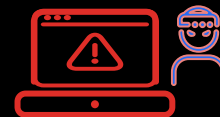


**DANGER**  
**ENTER AT**  
**OWN RISK**

# THE PROBLEM



103.136.220.198



**Distributes ransomware**  
Uses infrastructure to push ransomware org-wide



1

**Runs recon**  
Scopes environment to find vulnerable applications

# 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

The screenshot displays the Palo Alto Networks management console. The main window is titled "LOG DETAILS" and shows a security log entry. The entry is categorized as "Traffic" and shows a connection that was dropped. The log entry details are as follows:

Log Info	
Time	Today 16:39:31
Blade	Firewall
Product Family	Access
Type	Connection
Policy	
Action	Drop

The "Traffic" section provides further details about the connection:

Traffic	
Source	192.168.5.100
Destination	192.168.101.100
Service	TCP/10400
Interface Direction	inbound
Protocol	TCP (6)
Destination Port	10400
Source Port	54630

The "More" section shows additional context:

More	
Inzone	Internal
Message Information	Implied rule
Out-Zone	External

The interface also shows a "Tag Browser" with a table of tags and rules:

Tag(#)	Rule
none (4)	1-4

The bottom of the interface shows the "Object : Addresses" section with a list of IP addresses:

- 172.16.0.0-172.31.255.255
- 192.0.0.0-192.0.0.255
- 192.0.2.0-192.0.2.255

The interface includes navigation tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The user is logged in as "admin" and the last login time is 09/12/2016 06:04:49.

# 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.

