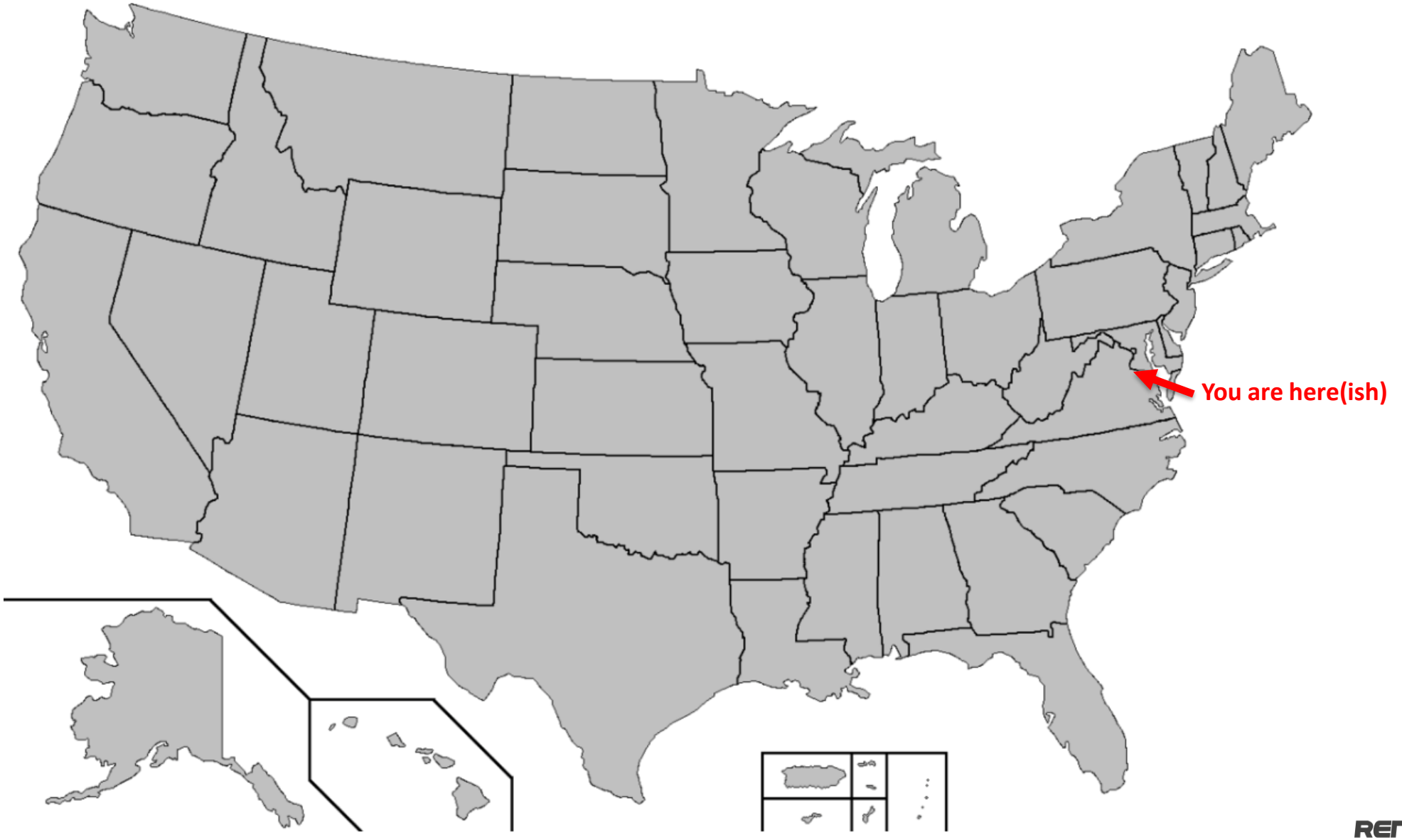
Supply Chain Summit Opener

Jake Williams (@MalwareJake)
Rendition Infosec
www.rsec.us
@RenditionSec

RENDITION INFOSEC
Cybersecurity by any legal means

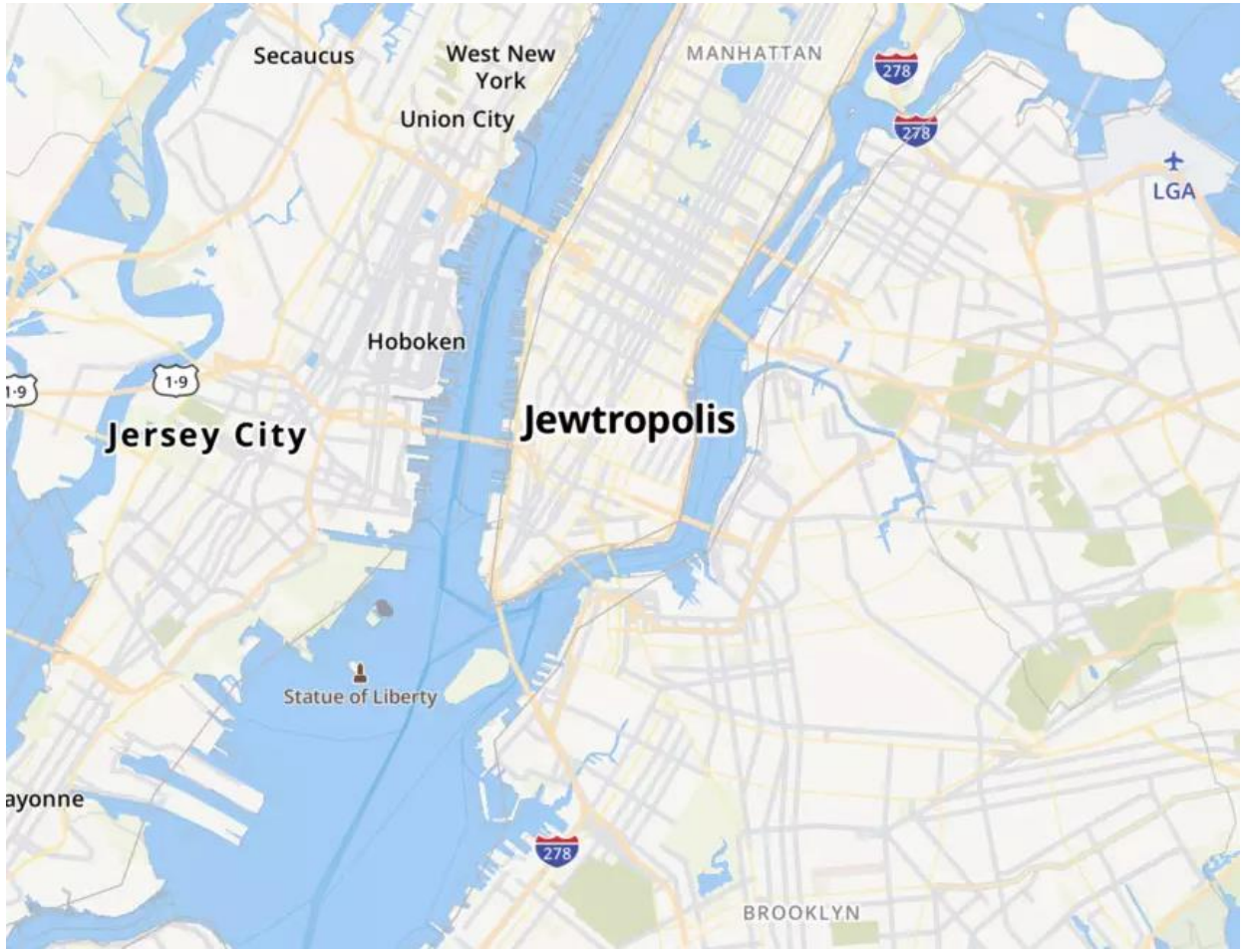
Who came the farthest to be here?



RENDITION INFOSEC
Cybersecurity by any legal means

Did anyone travel to the event from NYC? (or this place)

- Snapchat and others were victims of a supply chain attack in 2018 where Mapbox began mislabeling NYC



ShadowPad

- In 2017, Kaspersky discovered an attack on users of NetSarang server administration software
- Attackers distributed new digitally signed components with Xmanager, a program popular in SouthEast Asia
  - This may provide some clues as to targeting
- The new DLLs (digitally signed by NetSarang) were distributed via the company's own update channels

NotPetya

- Unless you were in a coma over the last two years, you've probably heard about the Russian attacks on Ukraine
  - Attacks impacted much of Eastern Europe, Maersk, etc.
- Russian APT compromised the tax software MeDoc and used their software update mechanism to spread malware
- Malware was deployed through software update mechanisms
  - Third party software update mechanisms are notoriously difficult to secure and most vendors get this VERY wrong

NotPetya – MeDoc Server Room

- It’s hard to imagine a company without adequate server room cooling (or fan covers) having invested in great security

- But when buying hardware, software, or services, we rarely get such an in-depth look at internal operations

- We need a supply chain risk evaluation framework

ShadowHammer

- In January 2019, Kaspersky discovered a supply chain attack targeting users of the ASUS Live Update program

- This attack was distinct from NotPetya in a number of ways:
  - Although all Live Update ran attacker controlled code, only a handful (~600) were targeted to download next stage implants
  - The goal of the operation appears to be espionage rather than destructive actions
  - Although it was a software attack, only users of specific hardware would have been impacted

Python PyPi

- In October 2018, attackers were able to get malicious code into the PyPI repository
- There's a legitimate (and popular) package named colorama
  - Attackers created a package named colourama
  - So close, and yet so very far apart…
- There were numerous installations of the malicious package, which was surprisingly only targeting Bitcoin transactions

Supply Chain Attacks – Here To Stay!

- With better endpoint and perimeter security, supply chain attacks are here to stay
- We must get better at evaluating the threat landscape around supply chain attacks
- Attackers will evolve to ensure they maintain access to our networks