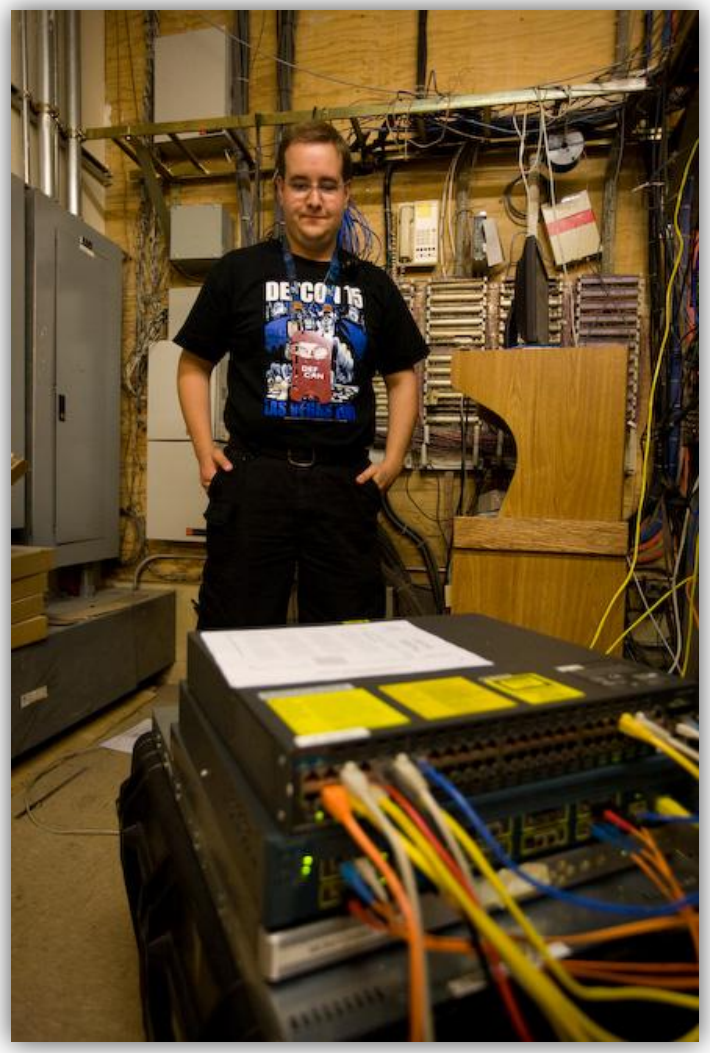
Cloud Computing

A Weapon of Mass Destruction?

netSPI
RISK COMPLIANCE SECURITY

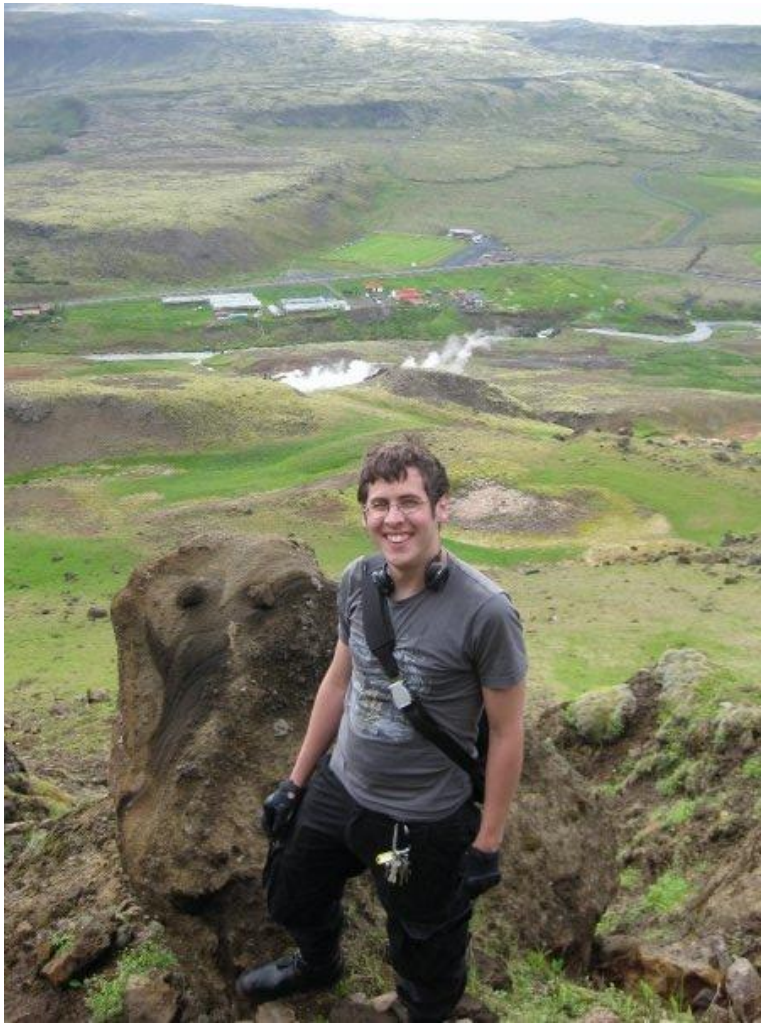
David M. N. Bryan - CISSP

- Technology Enthusiast (Aka “Hacker” or VideoMan)
- Security Consultant (Other Company)
- dave@drstrangelove.net
- PGP Key on key servers



Michael Anderson - Newb

- Security Consultant (NetSPI)
- michael.anderson@netspi.com
- cpt.fury@gmail.com



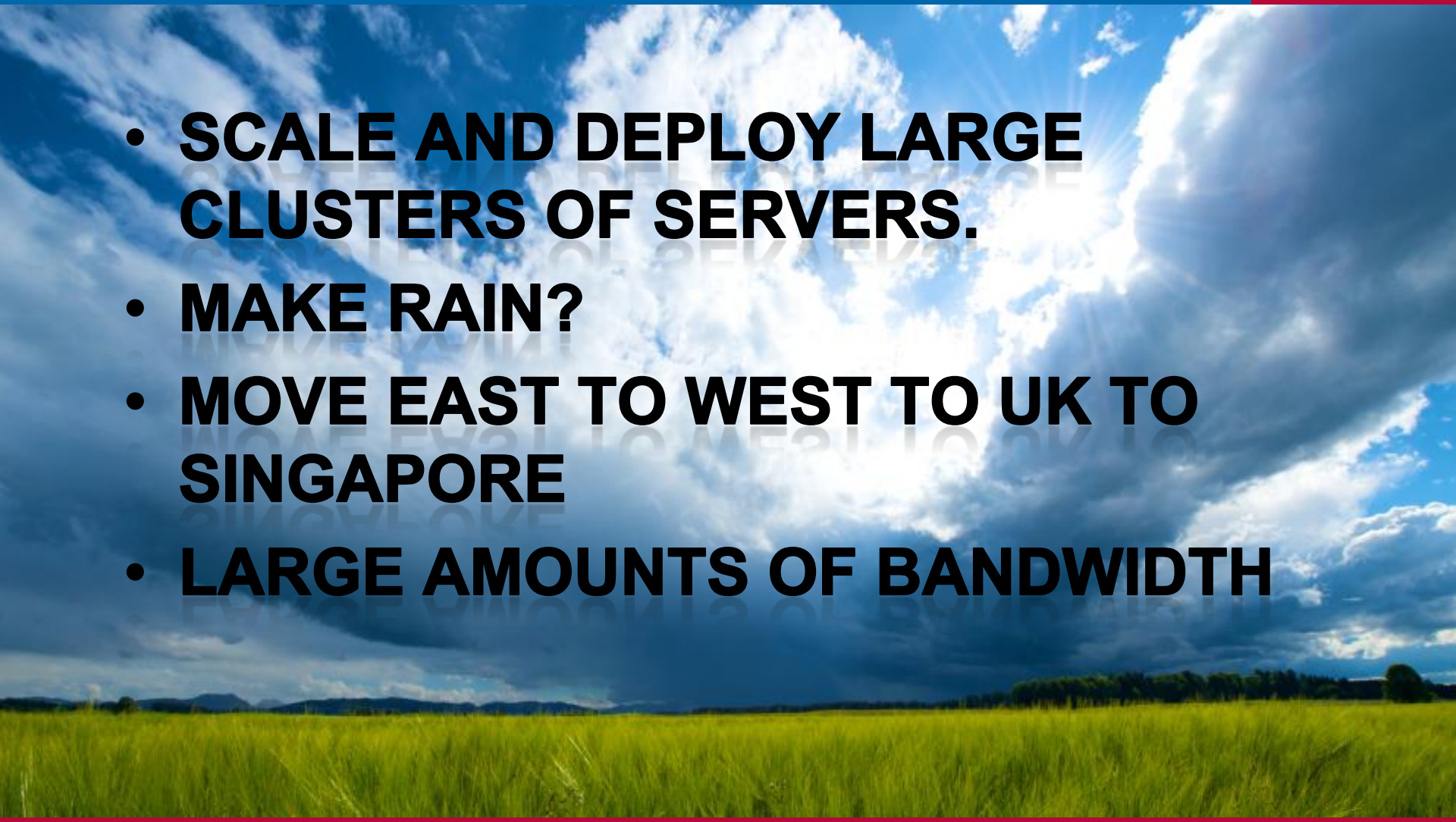
NetSPI

- Founded in 2001
- Exclusive Focus: Information Security Consulting
  - Security & compliance assessments, security program development
  - Vendor neutral – services only
- PCI QSA, ASV, and PA-QSA Certifications
- Government Clearances
- Industry Focus:
  - Retail / payment apps
  - Financial services
  - Healthcare
  - Energy & Power

What is the “Cloud”

- CUSTOM SERVER IMAGES
- CENTRAL STORAGE
- CENTRAL MANAGEMENT
- NO PHYSICAL SYSTEMS TO WORRY ABOUT
- USES CUSTOM APIS
  - STORAGE, QUEUING, WEB SERVING, ETC.

What can I do in the cloud?



- SCALE AND DEPLOY LARGE CLUSTERS OF SERVERS.
- MAKE RAIN?
- MOVE EAST TO WEST TO UK TO SINGAPORE
- LARGE AMOUNTS OF BANDWIDTH

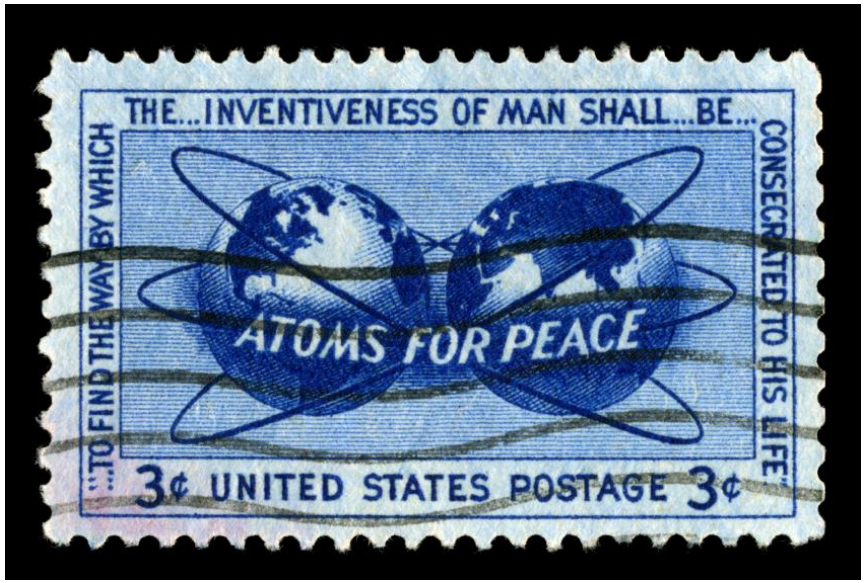
What's required to start?

- **EMAIL ADDRESS**
- **CREDIT CARD**
- **CURSORY REVIEW OF API**

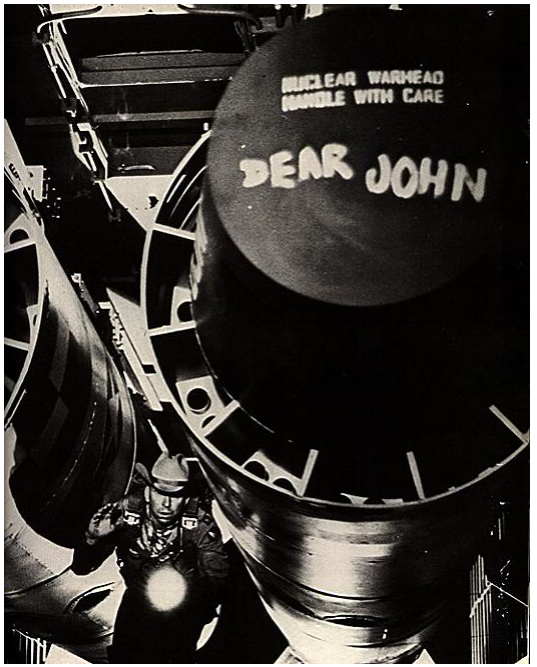
- **CONTRACTS?**

Cloud Computing?

- Is it a useful tool?



- Or a WMD?



Cloud Computing WMD

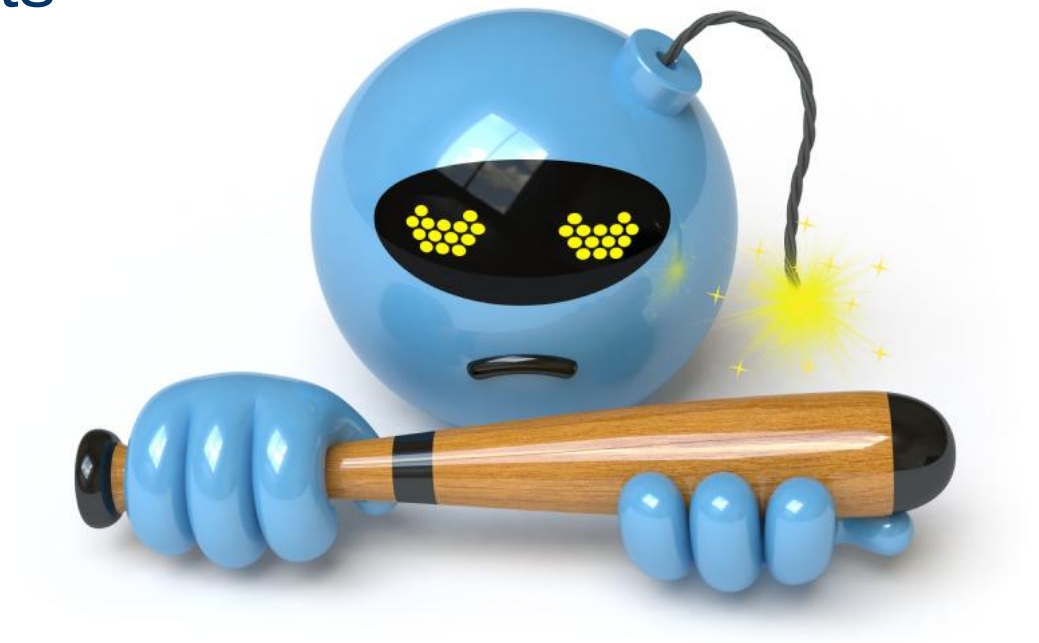
- Outline
- Threat Agents
  - Who and why?
- Attacks
  - Command and Control
  - Attack Types
  - Results
- Defenses
  - Incident Response

Threat Agents

- Who are they?
  - Business Rivals
  - Organized Crime
  - Foreign Powers

Motivates

- What do they want?
  - Bragging Rights
  - Money
  - Power



Power

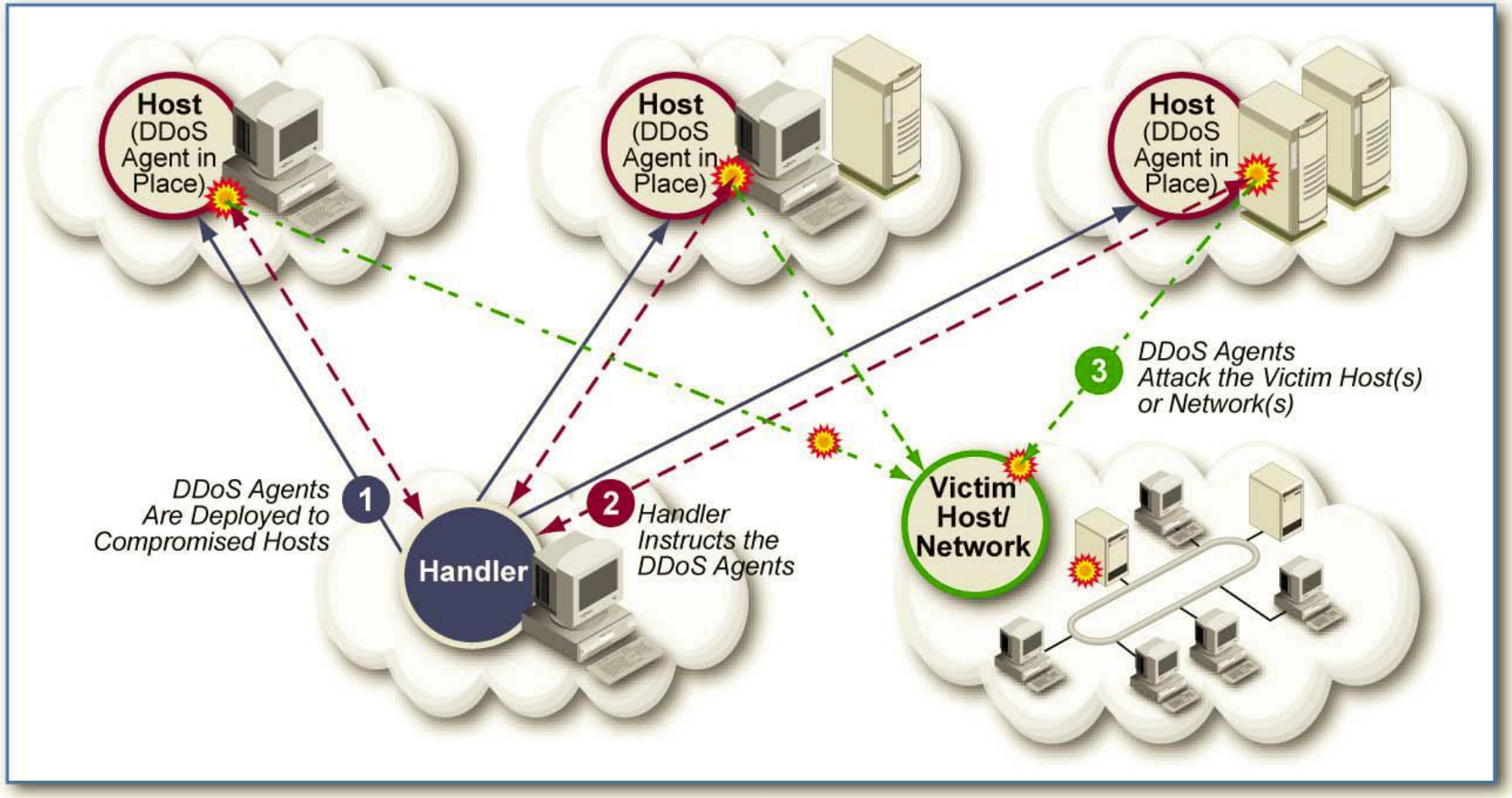
Terms

- DDoS
  - Distributed Denial of Service Attack
- Fragmentation Attack
- TCP Syn Flood
  - Sending packets with only the Syn bit set, and not listening for a response

Typical Command And Control

- Who is your herder?
  - Typical CNC
  - Herder
    - Controller or Scripts
  - Bots
    - Infected Clients
    - Lots of Hosts (Millions?)
    - Requires lots of time
    - Most systems are Windows

Command And Control



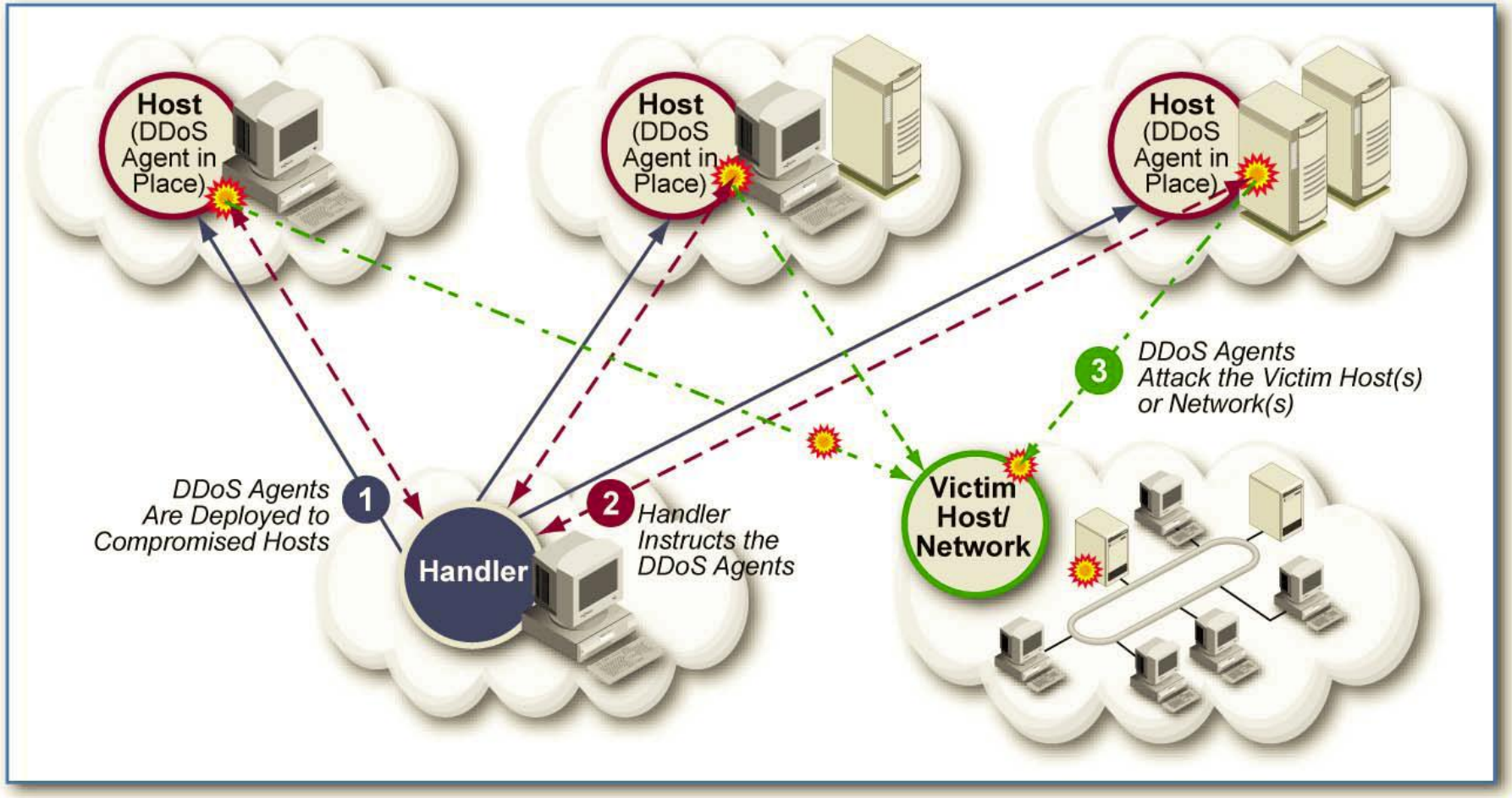
Thunder Clap

- Its a proof of concept
- Run DDoS attacks from the cloud
- Can use social media as herder
- Rapid deployment and ramp up of systems

New Command And Control

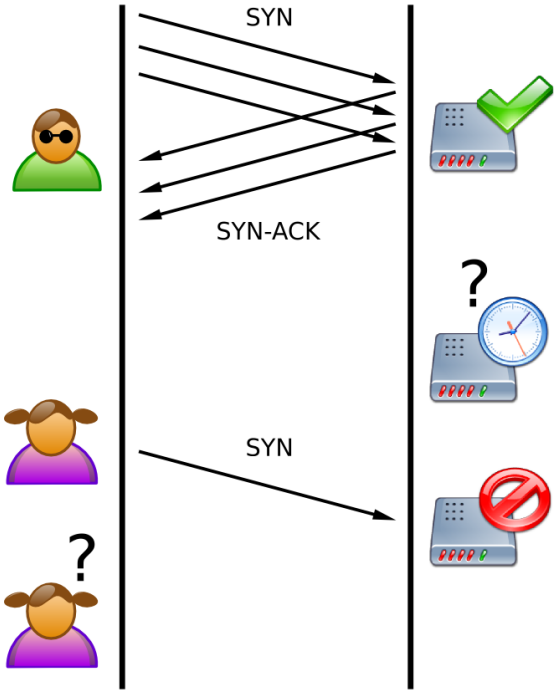
- Who is your herder?
  - Cloud is Herder and Botnet
  - Bandwidth is plentiful
    - Less dispersed
    - Little prep time
  - Control of attack
    - Social Media
    - Anonymous
    - Hard to track

Command And Control



Attack Types

- TCP Full Connection
  - Could be less effective; not stealthy
- Packet Fragmentation
  - Not implemented in proof-of-concept
- TCP Syn Flood
  - Dangerous, but requires some serious bandwidth



What can we do with this?

- Target a website, server, or service
- Target multiple components or sites
- Potentially target distributed systems
- Run a lowlife blackmail scheme (we won’t but, organized crime might)
- Sell DDoS services to your competitors
- Ensure your website is down, for good.

Outcome

- Threat agents can hold your environment hostage
  - Easily
  - Cheaply
  - Who watching again?

ThunderClap

Create Environment

- Get credit card
- Create machine image
  - Include dependencies
- Deploy zombies

Development

- Create tools
  - Scapy
  - Hping
  - Libdnet
- Develop attacks
  - TCP Full
  - Syn No Data
  - Random Source IP?

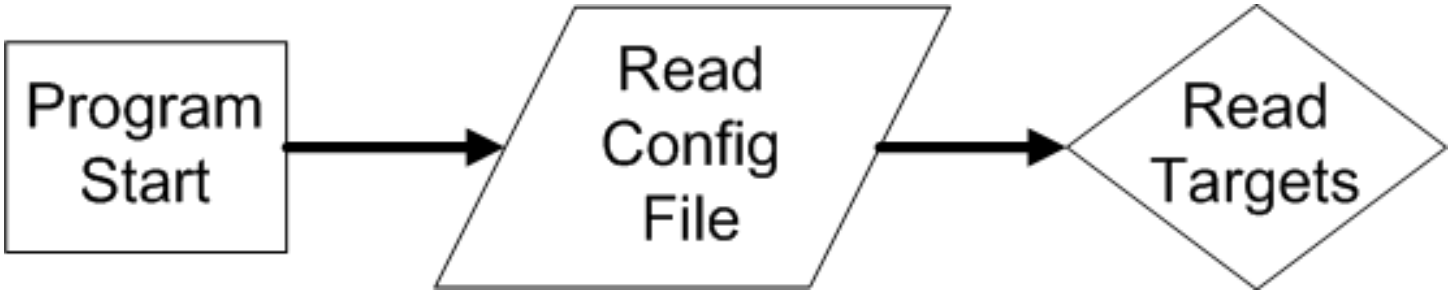
Boom – pwnt!

D00D, we is 1337

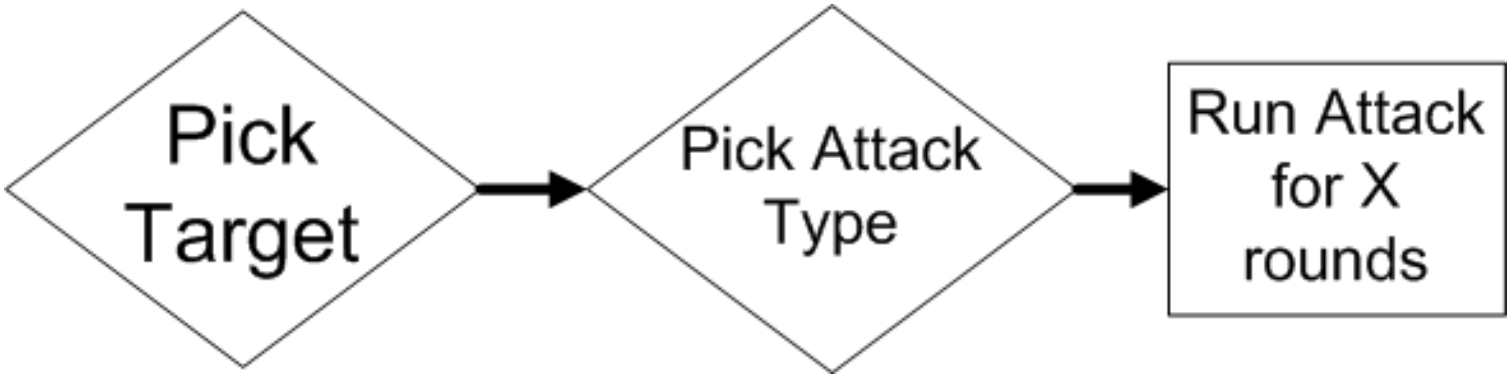
Outcome?

- Profit
- A series of tubes…

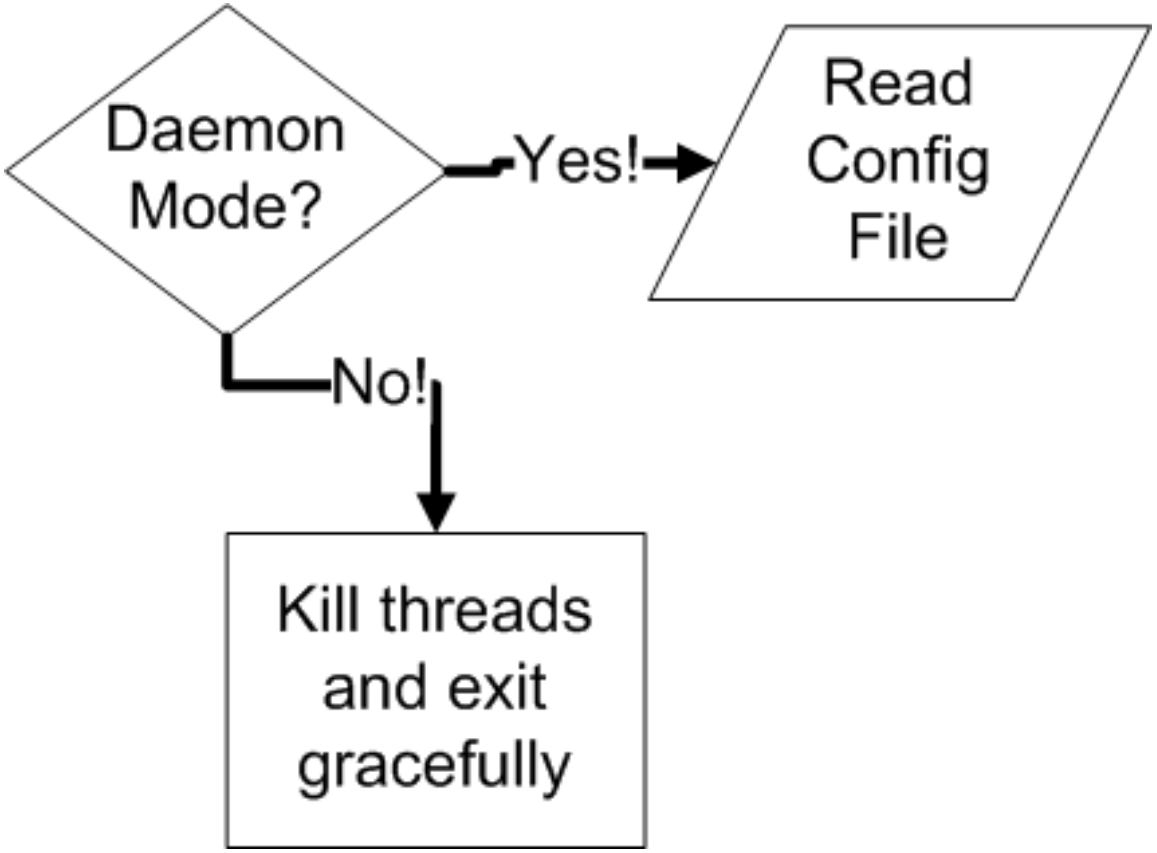
Inter workings of TC



Attack!



Work to be done?



Defense?

- How can you protect yourself?

Incident Response

- CSIRT Teams?
- NIST 800-61 Incident Response

Could Computing Pros

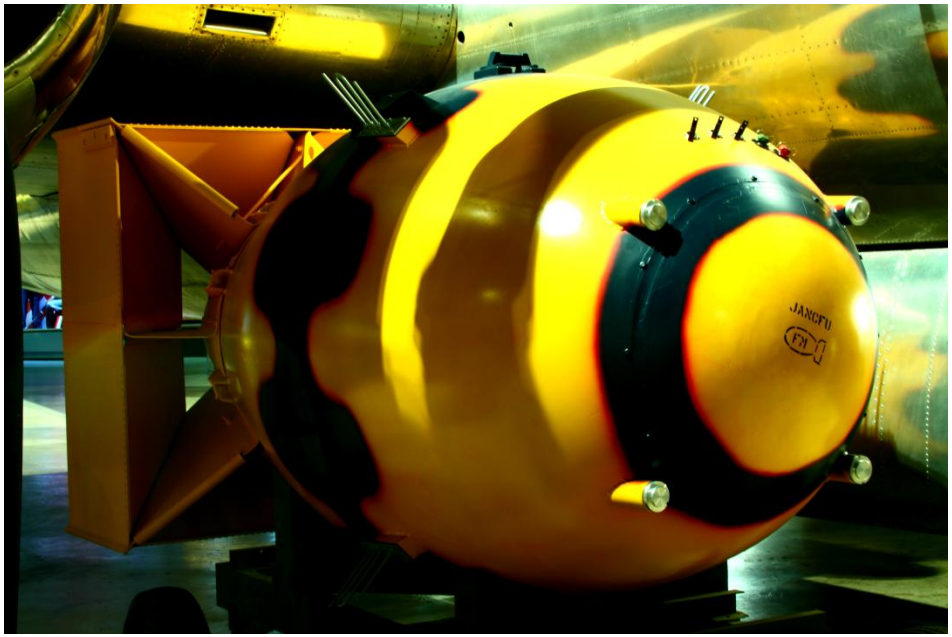
- Cloud computing is nimble
  - Provides agility to start ups
  - Easy to deploy large numbers of servers
  - Cost effective for small company
  - Only requires a credit card
  - Storage, CloudFront, Queues, etc

Cloud Computing Cons

- "*Storing data yourself, on your own computers—without relying on the cloud—is the most legally secure way to handle your private information, generally requiring a warrant and prior notice. The government asserts that it can subpoena your data from cloud computing providers, with no prior notice to you.*“ -Granick and Opsahl, EFF
- No monitoring or response
- Quick and nimble server deployment
- Low cost to run effective DDoS
- Use stolen credit card for environment

Unmonitored…

- We could end up with the next large scale attack in the clouds.



Conclusion

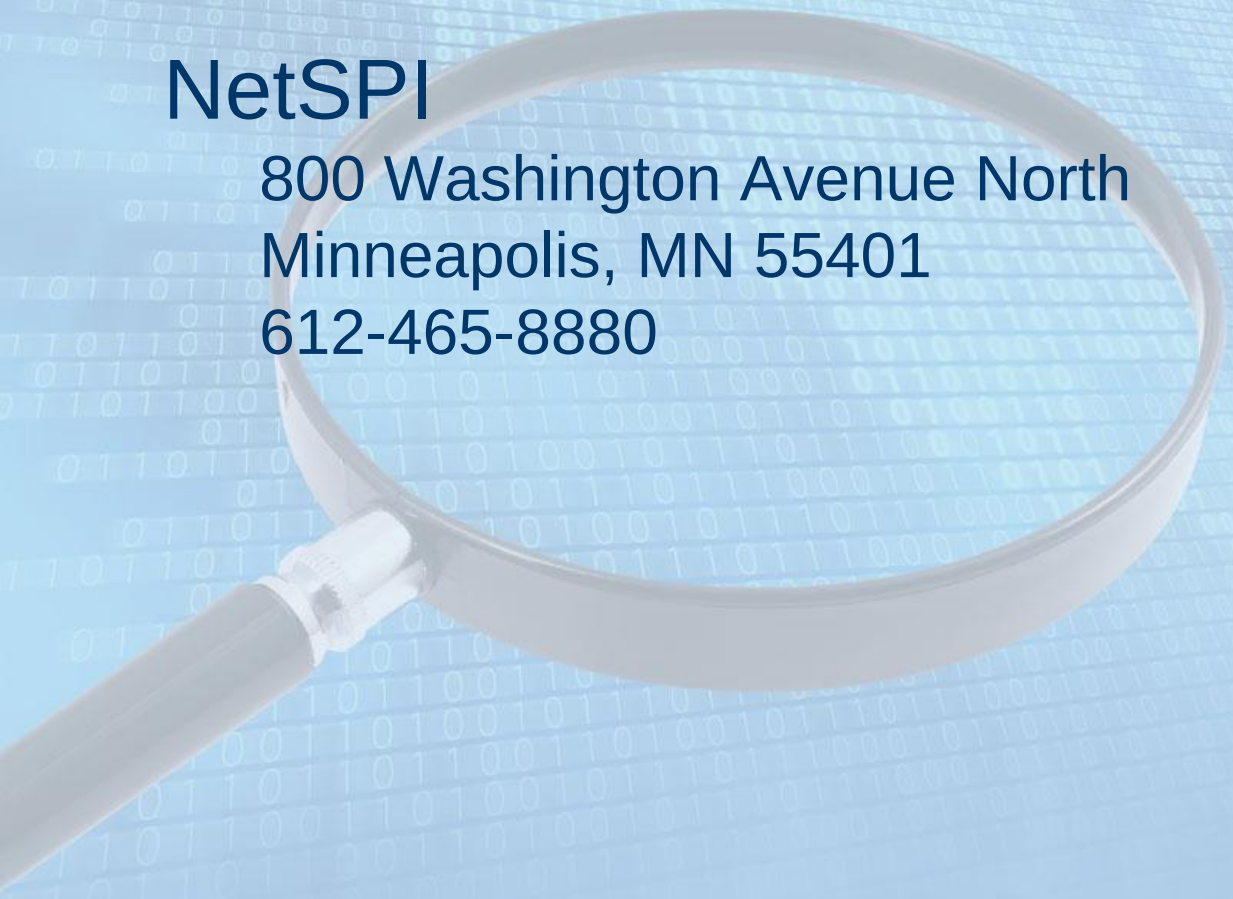
- Unmonitored – IDS/IPS?
- Cloud allows for quick and nimble deployments
- Reduce your server costs
- Your data can be subpoenaed with our your consent or knowledge
- What about logging?

Q and A

Thank You

NetSPI

800 Washington Avenue North
Minneapolis, MN 55401
612-465-8880



netSPI
RISK COMPLIANCE SECURITY


netSPI
RISK COMPLIANCE SECURITY

References

- http://zvis.com/nuclear/detonation/ctyankee/ctyankee.shtml
- http://www.indelibleinc.com/kubrick/films/strangelove/images/kingkong.jpg
- http://commons.wikimedia.org/wiki/File:Tcp_synflood.png
- http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
- http://upload.wikimedia.org/wikipedia/commons/7/71/AirForceMuseum_FatManReplica.jpg
- http://www.strangeloveforcongress.com/o/30070/images/warroom.jpg
- http://www.eff.org