ARIZONA SMALL BUSINESS BOOT CAMP & COLLECTIVE

RESPOND → PLAN → RETURN STRONGER

CYBER SECURITY TRAINING AND CONSULTING LLC

# Packaged for Success

**PRESENTED BY**

Jeffrey Crump & Christopher Alexakis

# Learning objectives

1 Who the threat actors targeting SMBs are

2 How threat actors do what they do: Tactics, Techniques, and Procedures (TTPs)

3 Three types of controls needed to build a layered defense

4 The ~~weakest~~ strongest link in the security chain

# Threat Actors Targeting SMBs

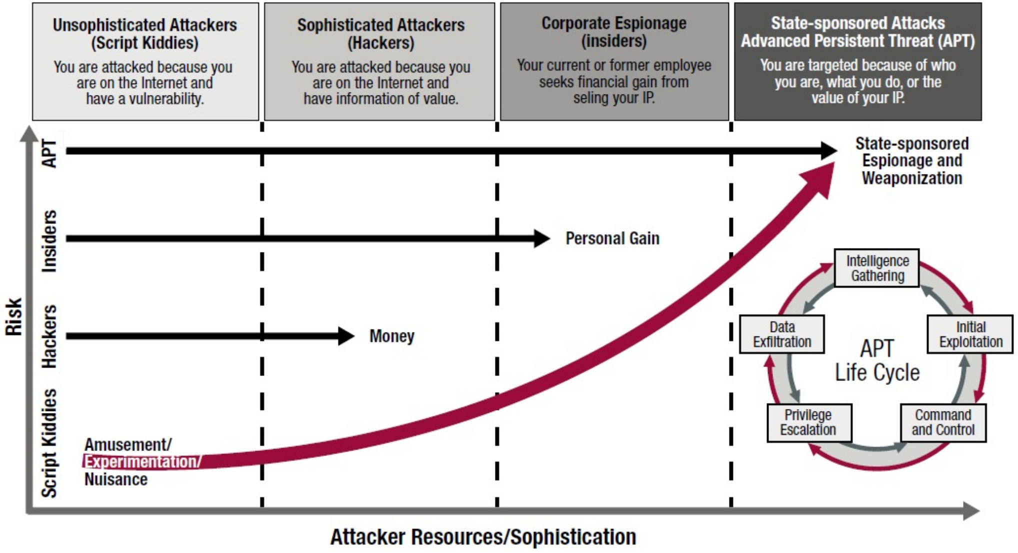
Who are your adversaries?

- Skill-based Considerations
- Motivations
  - Financially
  - Social Causes
  - Nationalism
- Employees & Trusted Third Parties

# Threat Actors: Skills Levels

- Script Kiddies
    - Low level of skill threat actors
        - Generally, use existing tools and technologies (e.g., Kali Linux)
            - Kali Linux provides 300+ free tools
        - Motivations may vary from just learning to causing mayhem

- APT (Advanced persistent threats)
    - Highly advanced skill sets
    - Well-financed
    - Generally, campaign-based
        - Data exfiltration
        - Observation for future action on objectives
        - Data destruction

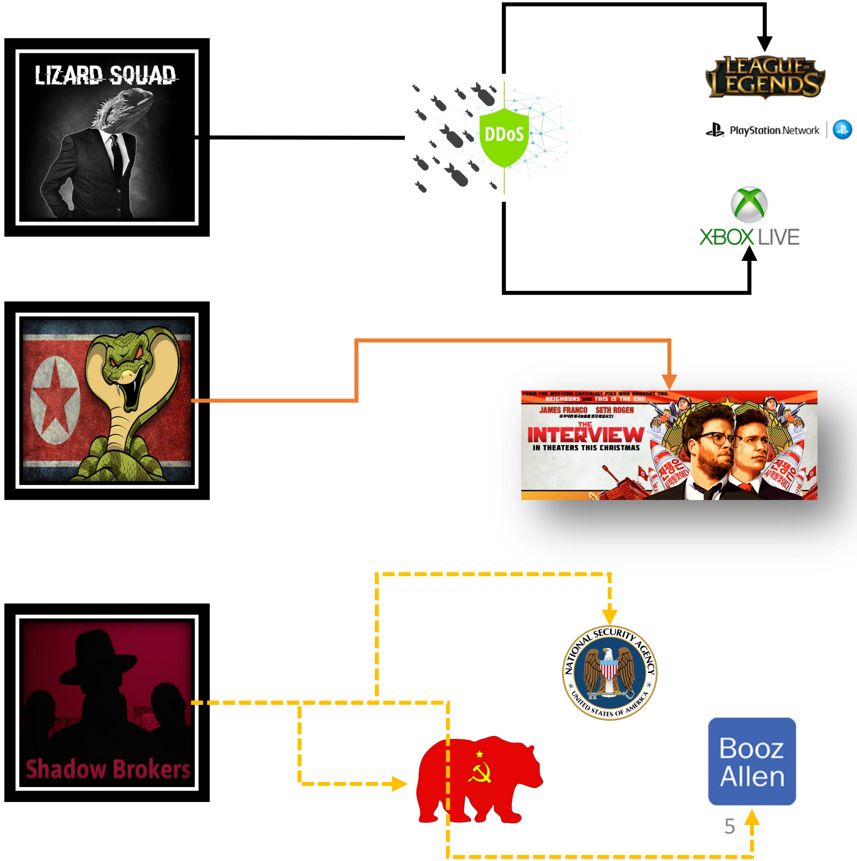


Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.
Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.
Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.
State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.
Risk
APT
Insiders
Hackers
Script Kiddies
State-sponsored Espionage and Weaponization
Personal Gain
Money
Amusement/ Experimentation/ Nuisance
Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
APT Life Cycle
Attacker Resources/Sophistication

Source: ISACA, Responding to Targeted Cyberattacks, USA, 2013

# Threat Actors: Financially Motivated

- Organized Cyber Criminals
  - Money motivated
  - Organized crime syndicates
    - Carbanak
    - Lizard Squad
    - Lazarus Group
    - Shadow Brokers



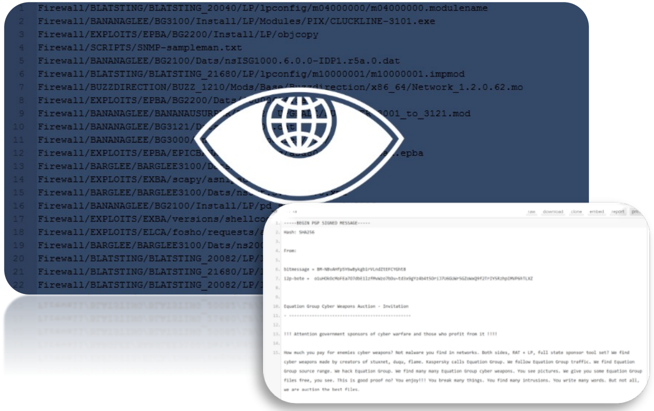
# Threat Actors: Social Cause Motivated

- Hacktivist
  - Civil disobedience using social engineering techniques

Anonymous

CyberBerkut

The Shadow Brokers

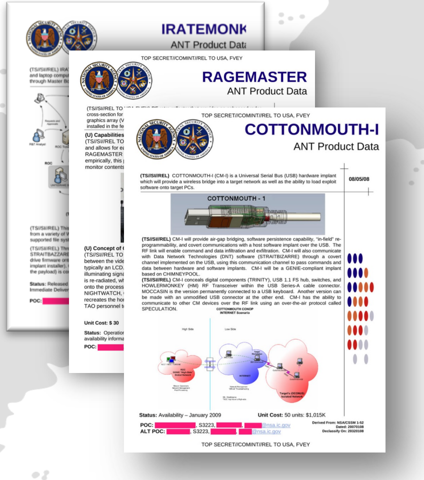


```
Firewall/BLATSTING/BLATSTING_20040/LP/lpconfig/m04000000/m04000000.modulename
Firewall/BANANAGLEE/BG3100/Install/LP/Modules/PIX/CLUCKLINE-3101.exe
Firewall/EXPLOITS/EPBA/BG2200/Install/LP/objcopy
Firewall/SCRIPTS/SNMP-sampleman.txt
Firewall/BANANAGLEE/BG2100/Dats/nsISG1000.6.0.0-IDP1.r5a.0.dat
Firewall/BLATSTING/BLATSTING_21680/LP/lpconfig/m10000001/m10000001.impmod
Firewall/BUZZDIRECTION/BUZZ_1210/Mods/Base/Buzzdirection/x86_64/Network_1.2.0.62.mo
Firewall/EXPLOITS/EPBA/BG2200/Dats/
Firewall/BANANAGLEE/BANANAUSURP
Firewall/BANANAGLEE/BG3121/D
Firewall/BANANAGLEE/BG3000/
Firewall/EXPLOITS/EPBA/EPICBA
Firewall/BARGLEE/BARGLEE3100/D
Firewall/EXPLOITS/EXBA/scapy/asn1
Firewall/BARGLEE/BARGLEE3100/Dats/ns
Firewall/BANANAGLEE/BG2100/Install/LP/pd
Firewall/EXPLOITS/EXBA/versions/shellco
Firewall/EXPLOITS/ELCA/fosho/requests/
Firewall/BARGLEE/BARGLEE3100/Dats/ns20
Firewall/BLATSTING/BLATSTING_20082/LP/
Firewall/BLATSTING/BLATSTING_21680/LP/
Firewall/BLATSTING/BLATSTING_20082/LP/
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

From:

bitmessage = BM-NBvAHfp5Y6wBykgbirVLndZtEFCYGht8
i2p-bote =  o1uHOk0cMoFEa707dbE1lzfMvWzo7bOu~td3x9gYz4b4tSOr137U6GLWr5GZoWxQ9f2TrIYSRzhpIMVP6hTLXZ


Equation Group Cyber Weapons Auction - Invitation
- ------------------------------------------------

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.
```

https://pastebin.com/M6haBeFw

# Threat Actors: Nation States/Nationalism



IRATEMONK
ANT Product Data

(TS//SI//REL) IRA
and laptop compu
through Master Bo

(TS//SI//REL) This
from a variety of W
supported file syst

(TS//SI//REL) Thro
STRAITBAZZARE
drive firmware ont
implant installer). 
the payload) is co

**Status:** Released
Immediate Deliver

**POC:** [redacted]

TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER
ANT Product Data

(TS//SI//REL TO
cross-section for
graphics array (V
installed in the fe

**(U) Capabilities**
(TS//SI//REL TO
and allows for ea
RAGEMASTER
empirically, this
monitor contents

**(U) Concept of**
(TS//SI//REL TO
between the vide
typically an LCD.
illuminating signa
is re-radiated, wh
onto the process
NIGHTWATCH,
recreates the ho
TAO personnel t

**Unit Cost: $ 30**

**Status:** Operation
availability informa

**POC:** [redacted]

TOP SECRET//COMINT//REL TO USA, FVEY

## COTTONMOUTH-I
ANT Product Data

**(TS//SI//REL)** COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

**(TS//SI//REL)** CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

**(TS//SI//REL)** CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario

High Side
Low Side
ROC
GENIE "High-Side" Global Network
INTERNET
Target Workstation
Target's (OCONUS) Isolated Network

**Status:** Availability – January 2009

**Unit Cost:** 50 units: $1,015K

**POC:** [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
**ALT POC:** [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

"The list reads like a mail-order catalog, one from which other NSA employees can order technologies from the ANT division for tapping their targets' data."

Der Spiegel

# Threat Actors: Insider Threats

Insiders were disgruntled and motivated by revenge for a negative work-related event.

Insiders exhibited concerning behavior prior to the attack.

Intentional threats exhibit malicious intent with what they are doing.

Insiders who committed IT sabotage held technical positions.

The majority of the insiders attacked following termination.

Unintentional threats have no real intent to harm, or even know what they are doing.

Carnegie Mellon University

No common demographic exists regarding age, gender, role or skill level.

Carnegie Mellon University, Software Engineering Institute, The CERT® Insider Threat Team (2013). Unintentional Insider Threats: A Foundational Study

# Tactics, Techniques, and Procedures (TTPs)

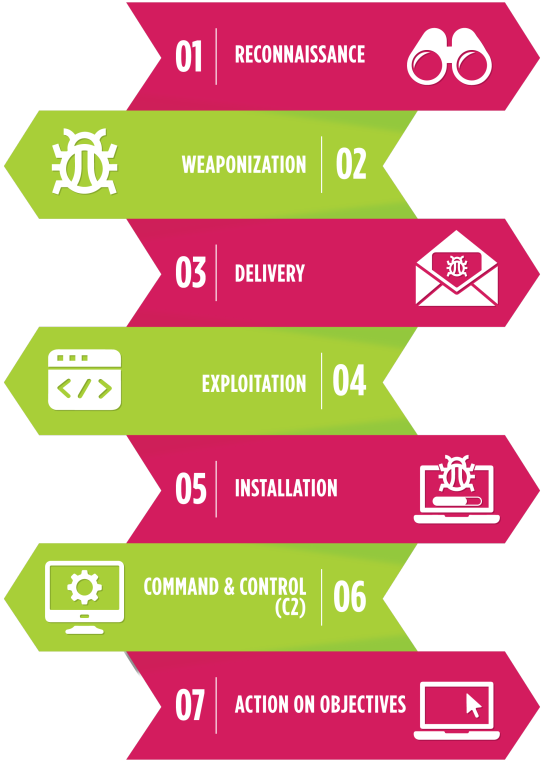
## What are TTPs?

The role of TTPs is to identify patterns of behaviors in a particular cyber threat.

- Tactics
  - General beginning-to-end strategies threat actors use to gain access and information
- Technique
  - What is being used to carry out attacks
- Procedure
  - The step-by-step guide on how to execute the attack or perform the technique

# TTPS: Cyber Kill Chain vs. MITRE ATT&CK

## Lockheed Martin Cyber Kill Chain



01 RECONNAISSANCE

02 WEAPONIZATION

03 DELIVERY

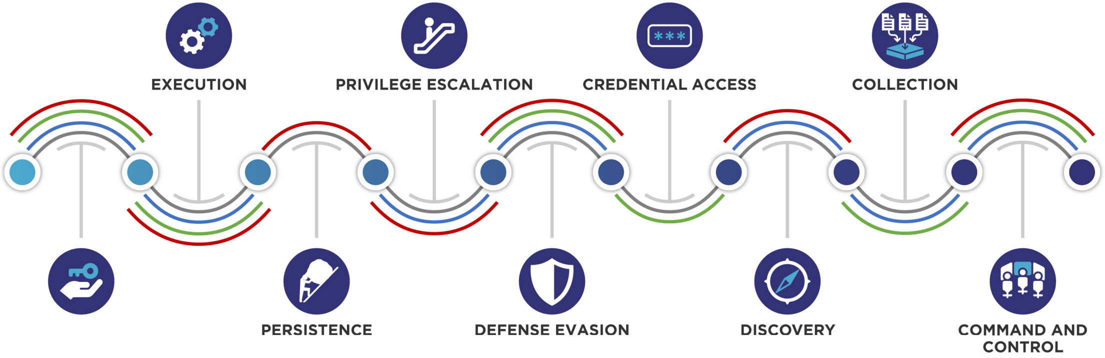
04 EXPLOITATION

05 INSTALLATION

06 COMMAND & CONTROL (C2)

07 ACTION ON OBJECTIVES

## Mitre ATT&CK



EXECUTION

PERSISTENCE

PRIVILEGE ESCALATION

DEFENSE EVASION

CREDENTIAL ACCESS

DISCOVERY

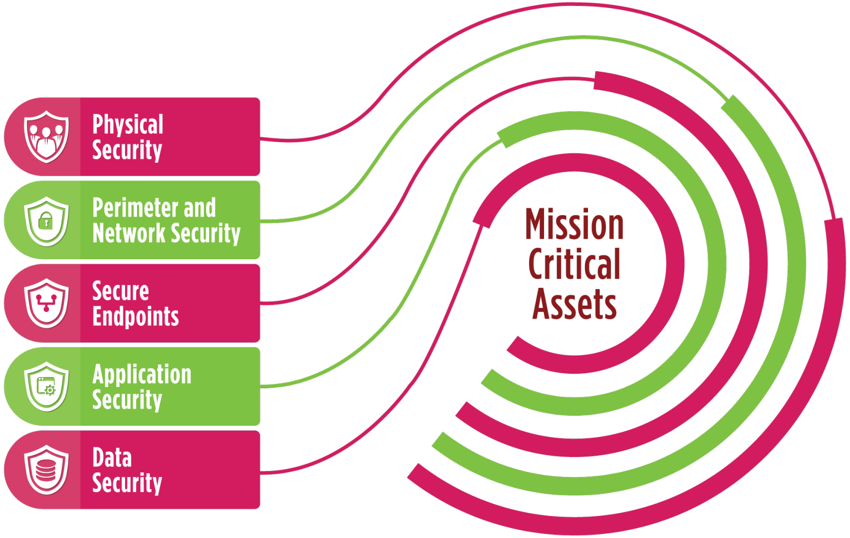
COLLECTION

COMMAND AND CONTROL

# LIVE DEMONSTRATION

# Defense in Layers

Layered Defense/Defense in Depth



(Proactive) Policy Management

(Reactive) Monitoring + Response

- Physical Controls
- Technical Controls
- Administrative Controls

# DEFENSE IN LAYERS: PHYSICAL CONTROLS

Anything that physically limits or prevents access to assets.

- CCTV Systems
- Guards
- Guard Dogs
- Biometric (Fingerprint, Voice, face etc.)
- Fences
- Passcode Door Entry
- Picture IDs

# DEFENSE IN LAYERS: TECHNICAL CONTROLS

Technical controls are hardware or software that's sole purpose is to protect assets

- Encryption
- Smart Cards
- Network Authentication
- Access Control Lists
- File Integrity Software
- Vulnerability Scanners
- One Time Passcodes

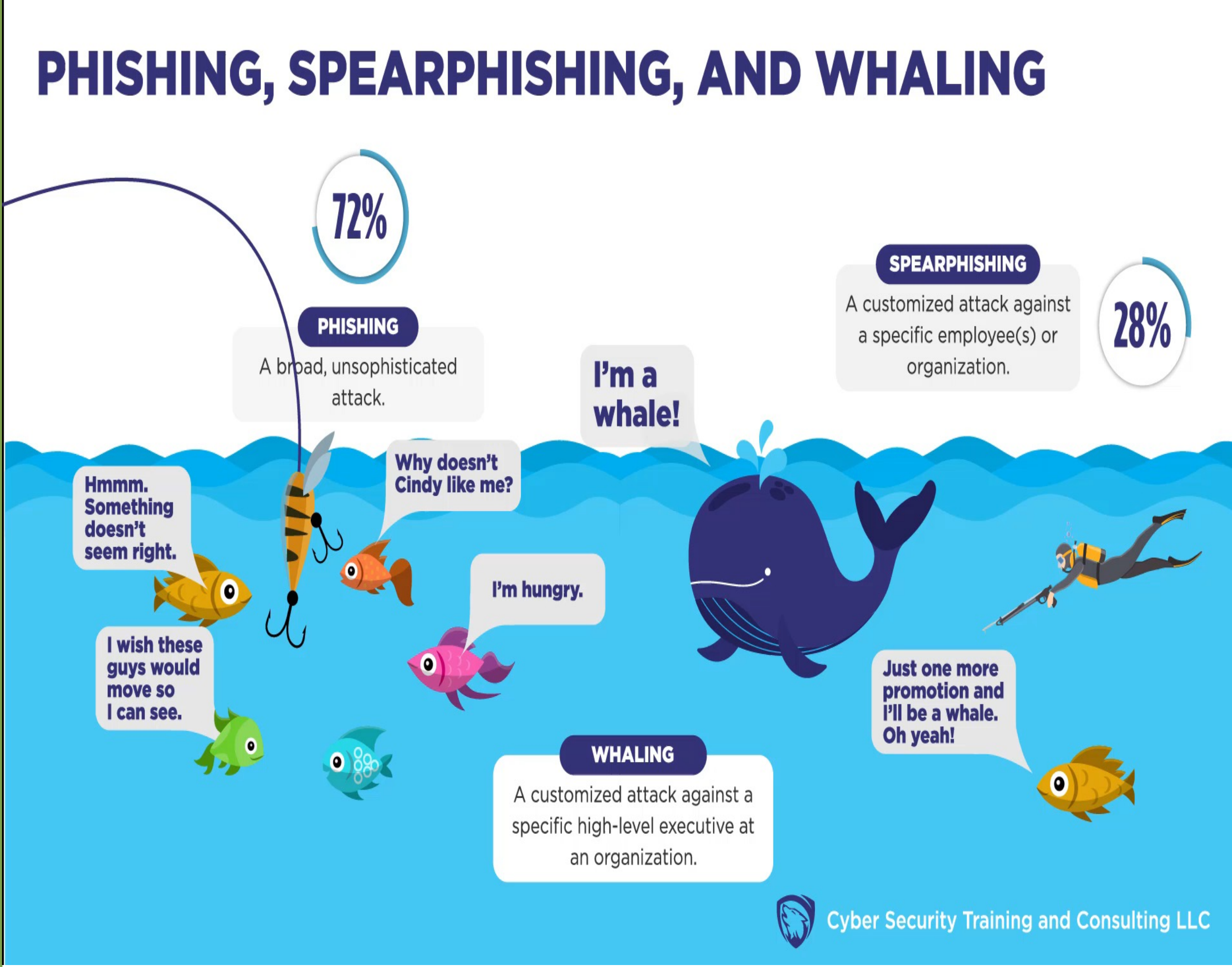
# DEFENSE IN LAYERS: ADMINISTRATIVE CONTROLS

Administrative controls are your human resources and security policies that help negate internal threats

- Hiring Practices
- Background Checks
- Data handling Procedures
- Security Requirements
- Security Policies
- Security Training

# Security Awareness

~~Weakest~~
Strongest link in the cyber security chain



## PHISHING, SPEARPHISHING, AND WHALING

72%

**PHISHING**
A broad, unsophisticated attack.

**SPEARPHISHING**
A customized attack against a specific employee(s) or organization.

28%

**WHALING**
A customized attack against a specific high-level executive at an organization.

I'm a whale!
Hmmm. Something doesn't seem right.
Why doesn't Cindy like me?
I'm hungry.
I wish these guys would move so I can see.
Just one more promotion and I'll be a whale. Oh yeah!
Cyber Security Training and Consulting LLC

# Q&A