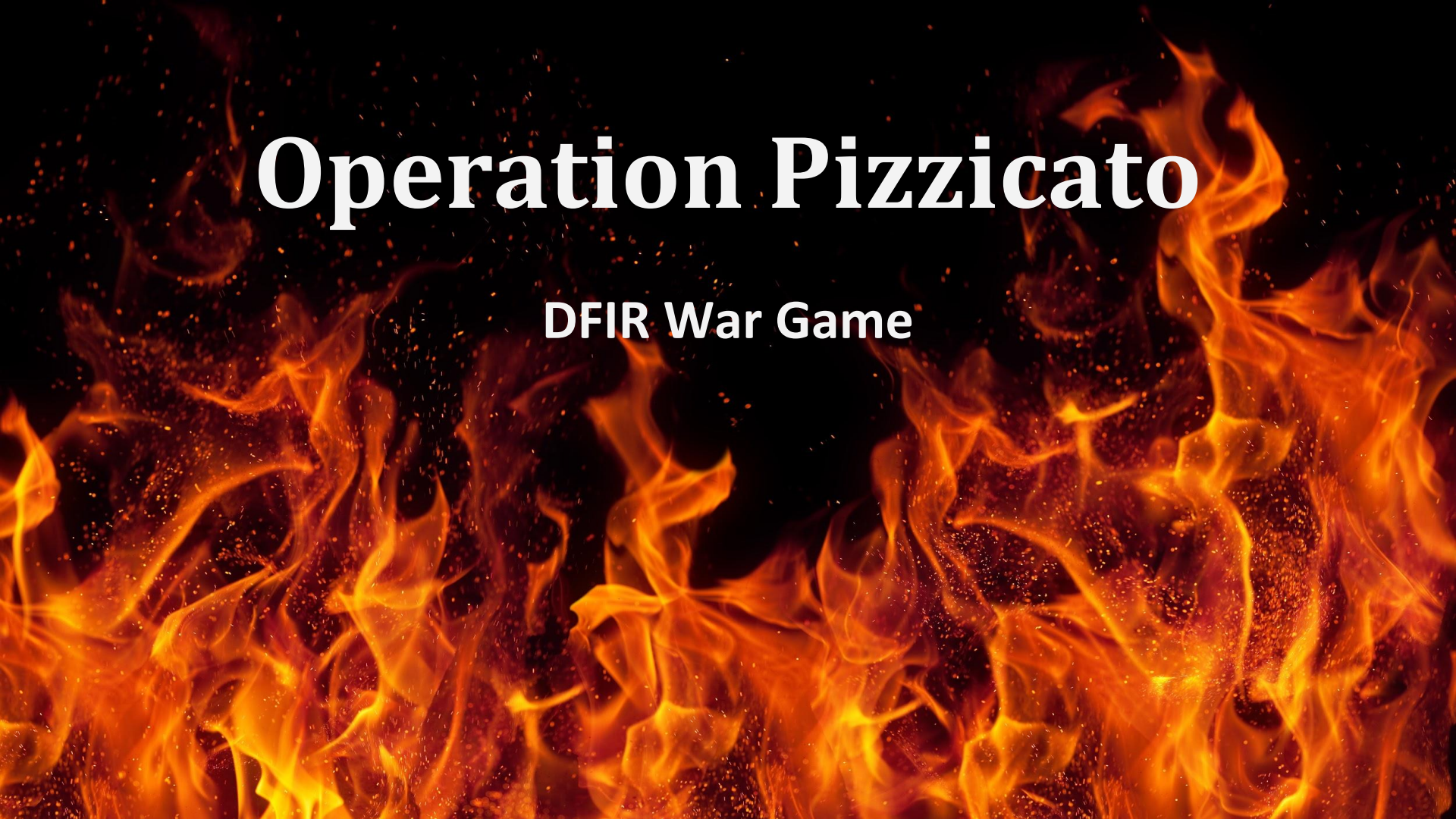

Operation Pizzicato
DFIR War Game

Operation Pizzicato

- Explore Disaster / Crisis in a safe way
- Identify trends in Response plans / procedures
- Interaction & Collaboration - diverse set of people
- Gain new perspectives/insights
- Explore various types of disaster testing
- Have a little fun

Mechanics of the Exercise

- **Tables of 8 - Diverse groups.** (Don’t sit with your friends!)
- **Scenario**
  - Decide what to do first. Start with the basics.
  - 15 minutes for table discussion
    - Plus 3-4 comments from entire room (keep comments short)
- **3 injects**
  - New information and advancements in the situation
  - Executives need info!
  - 15 minutes for table discussion
    - Plus 3-4 comments from entire room (keep comments short)
- **Post-Mortem: Take notes**

ICE-BREAKER (15 minutes)

- Select a “Table Lead”
- Every table get a “Capabilities Sheet” and pencil.
- Talk around the table
  - What capabilities do you have?
  - How much data / how long retained?
  - **BE HONEST!** This is a learning exercise and is not recorded.
- Table Lead:
  - Record the **low water mark** for each item at your table

Ground Rules!

- You'll have details about forensics, but this is an IR exercise
- Your capability "Low water mark" is what you've got to work with.
- If "Specific Tool X" would solve a problem, you can use it only if >50% of your team's members have it.
- If everyone at the table agrees an assumption is self-evident (eg, "We would have an expert on this in house") then you don't have to ask, just go with it.

During a production freeze before Cyber Monday at your company, a junior sysadmin is playing with nmap before their SANS Security class.

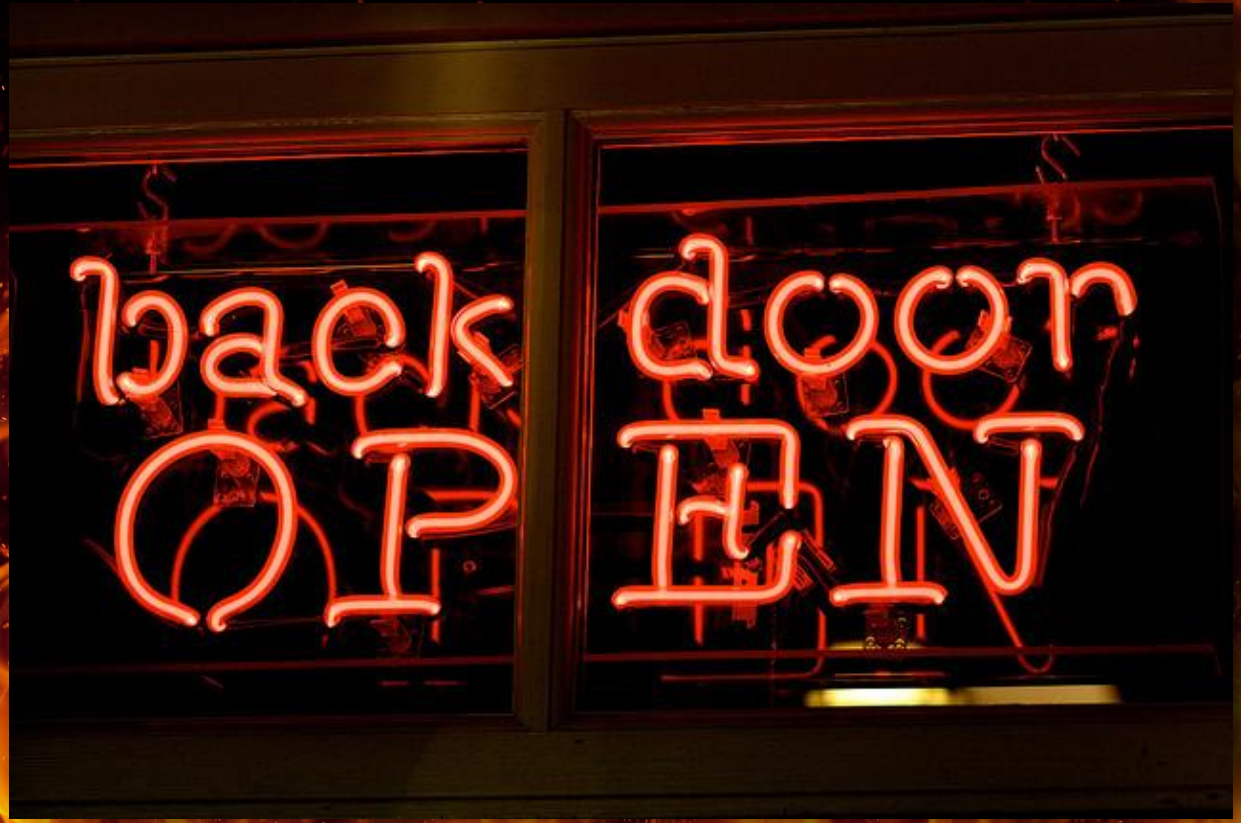
They've alerted you that the VNC server on their workstation allows for passwordless login.

Your company does not install VNC on workstations.

Wednesday afternoon Pacific Time

- You've validated that their Windows 10 system allows passwordless VNC
- She swears she didn't install it.
- System logs indicate that it was installed by her user account
- A potential artifact matching the install time was found in temp space (see: 'jquery.min.js.bat' on your unicorn head -- pass: 'UnicornsAreMagic')

Inject 1: This will not be comfortable.



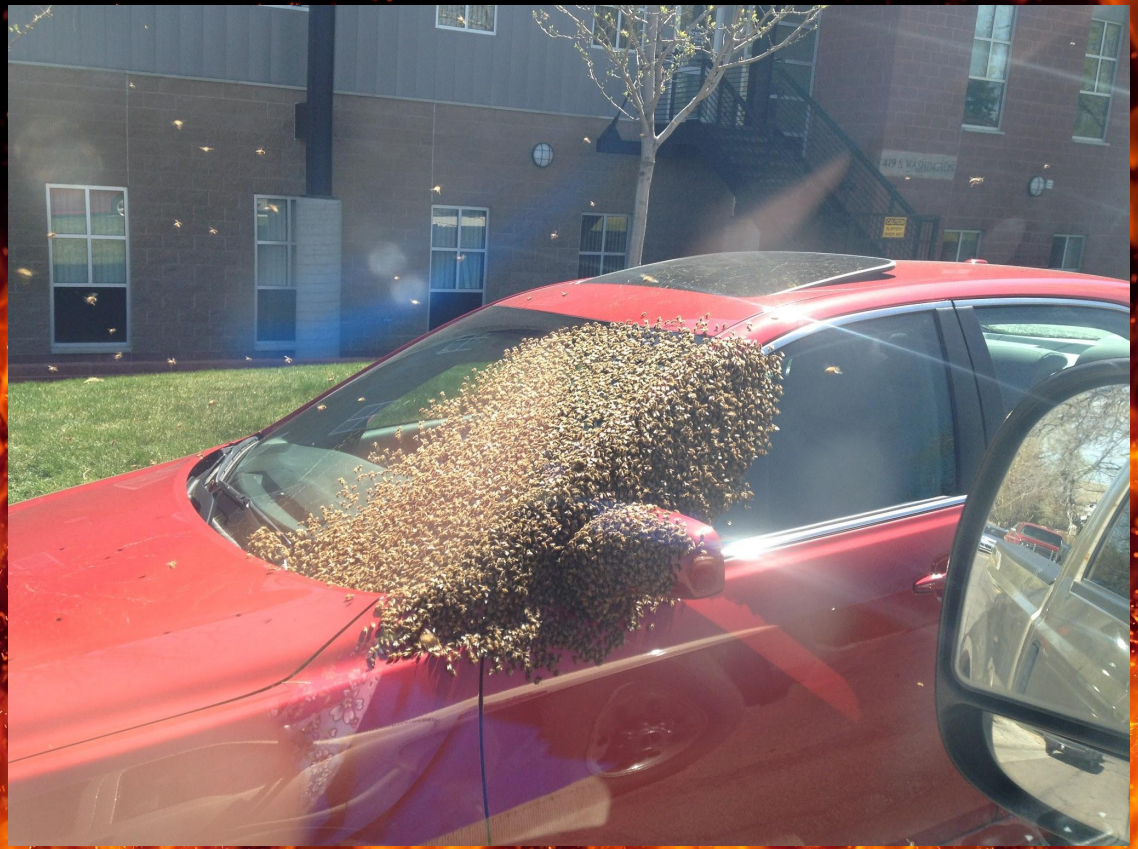
Wednesday evening, 6pm

- Analysis of the VNC server reveals a modified TightVNC
- Allows access to user screen regardless of what password is typed.

EXECUTIVE ASKS, Inject 1

- How did this get on the system
- How many systems is it on?
- What's it really doing?
- Is this contained yet? Why not? How soon?

Inject 2: OMG, BEES



Wednesday evening, 11pm

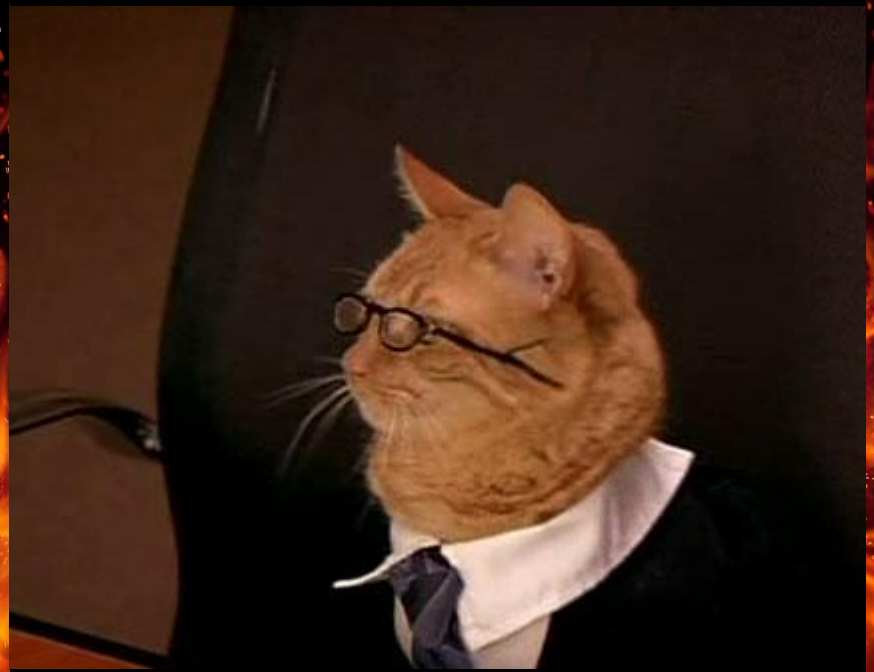
- Network PCAP is available on your unicorn head, titled “router_border.pcap” (pass: ‘NarwahlsAreMagicToo’)
- The pcap data was captured from your router’s WAN link
- Access to an internal company repo suggest attackers trying to locate backend databases w/ user data

EXECUTIVE ASKS, INJECT 2

- What to mitigate? When?
- What's the extent of the compromise?
- One of your executives is former Justice (Lawyer) & believes FBI Cyber would be helpful to get more support. She has a point of contact there for you. Do you contact them?

Inject 3: Lawyers make everything better

Sniffles G. Cattington III, Esq.



Attorney At Claw

Thursday morning, 10am

- Analysis of the backend databases suggests a breach of customer data
- An analyst reversing the malware finds a list of other targeted companies.
- [If you conduct business in Europe or California] - Your lawyers ask you to prove that no user data was accessed, or they want to notify regulators.

EXECUTIVE ASKS, INJECT 3

- Who did this?
- Can we clean it up?
- How can be sure of that?
- We make all our money in holiday season, what to do?
- Did we preserve evidence in case we get sued? How?
- Do we know which customers were affected?
- Are we going to tell the other companies? How? US-CERT? SIGs?

Review & Discussion

- What worked well?
- What do you wish you'd done differently at the outset?
- How did you manage communications w/ Lawyers, Execs, etc?
- Did you consider whether your IR infrastructure was affected?
- What decision points were involved in inviting the FBI, or not?
- How do you get hold of a lawyer / executive at an inopportune moment?