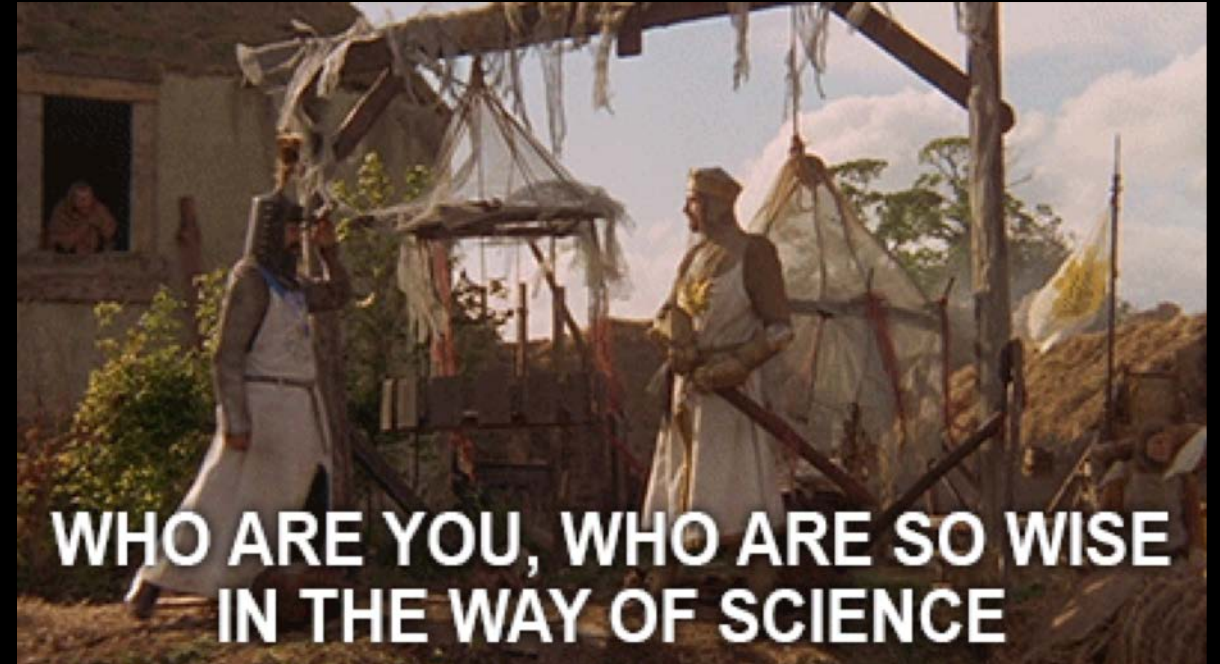


*Threat Hunting: The Incredible  
Journey*



# Who is this guy!?

- Just a security guy
- Security engineer past few years
- Systems engineer before that



What is this  
sorcery you  
speak of!?

- Proactively searching for anomalous activity
- It isn't just one thing
  - Theory/Intel based
  - Project/Digital Forensics based
- You might find something – be ready
  - Do you have a response plan or SOP

So... How do we get there?



# Threat Hunt Types

## Intelligence Based

- Short term – About a day
- Known IOC's and artifacts
- Intel based
  - Social Media/Blog posts/Your own idea...

## Project/Forensics based

- Long term – Multiple days, perhaps weeks
- Requires knowledge of tactics and tools
- Find unknown IOC's and unknown artifacts
- Planned and Documented
- Approvals received

# Where do I/we find these “threats”?

- Find / -name hackers
- ls -r / | grep tomfoolery
- Hey google, where are the bad guys(girls)?
  - Probably not the results you're looking for...



# Slow down champ

- You can't just start threat hunting
  - Where is the data
  - Where does it come from
  - Central point for data
- Enhance
  - Vision – Add more log sources



# The long and not so lonely road







Are you ready?

Do you...

- Have the right tools?
- Have the right data?
- Have the right people?
- Have the right training?

Have the right  
tools?

- Are you getting detection and protection where you need it
- Collection of events/data
- Presented in an easily readable format

Have the right  
data?

- Descriptive/informative data for events
- Does it answer who, what , where, when?  
("Why" will come from the analyst)

Have the right  
people?

- Not everybody has the investigatory mindset
- Or think like an attacker <- useful but not necessary

Have the right  
training?

- You/your people think the right way but don't know exactly how to use it
- They don't understand the data or its sources



# Incremental progression

- It's like a video game
  - Get an item/ability
    - Learn it, Know it, Love it
  - Tune that item/ability
  - Master the item/ability
  - Achieve next item/ability
- You could cheat (BUY EVERYTHING, INSTALL EVERYTHING)
  - but then “WTH is this thing!?”



# Knowing what you have

## Endpoint

- Anti-Virus –maybe
- PowerShell – Useful, lot's of data
- Event Logs – pertinent security events only

## IDS/IPS

- Are you logging this?

## Active Directory

- Are you logging this?

## Firewall

- Careful, have your storage ready

## EDR – Endpoint Detection and Response

- Are you... not really



# Security toilet



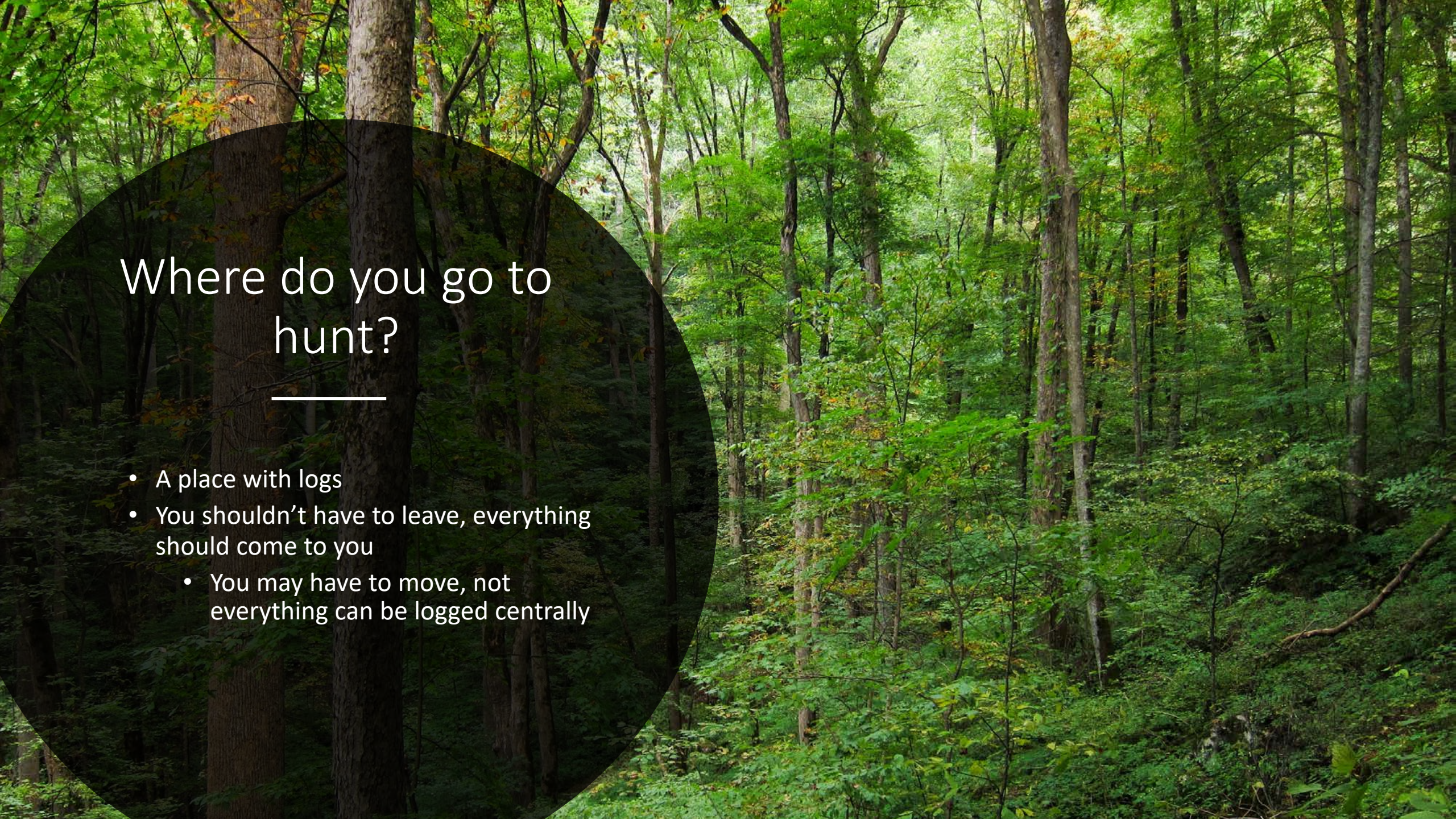
# The Fusion Center

Multiple security teams in one place

- They don't necessarily have to be geographically close
- Quick communication

You're security teams should all feed into each other


Allows you to accelerate organizational maturity



# Where do you go to hunt?

---

- A place with logs
- You shouldn't have to leave, everything should come to you
  - You may have to move, not everything can be logged centrally



# Where does all of this go?

---

- Log this to a centralized place
  - Aggregation
- SIEM is better (Security Information and Event Management)
  - Aggregation
  - Correlation
  - Applied intelligence
  - Alerts

**YAY!**



**ITS DONE!**

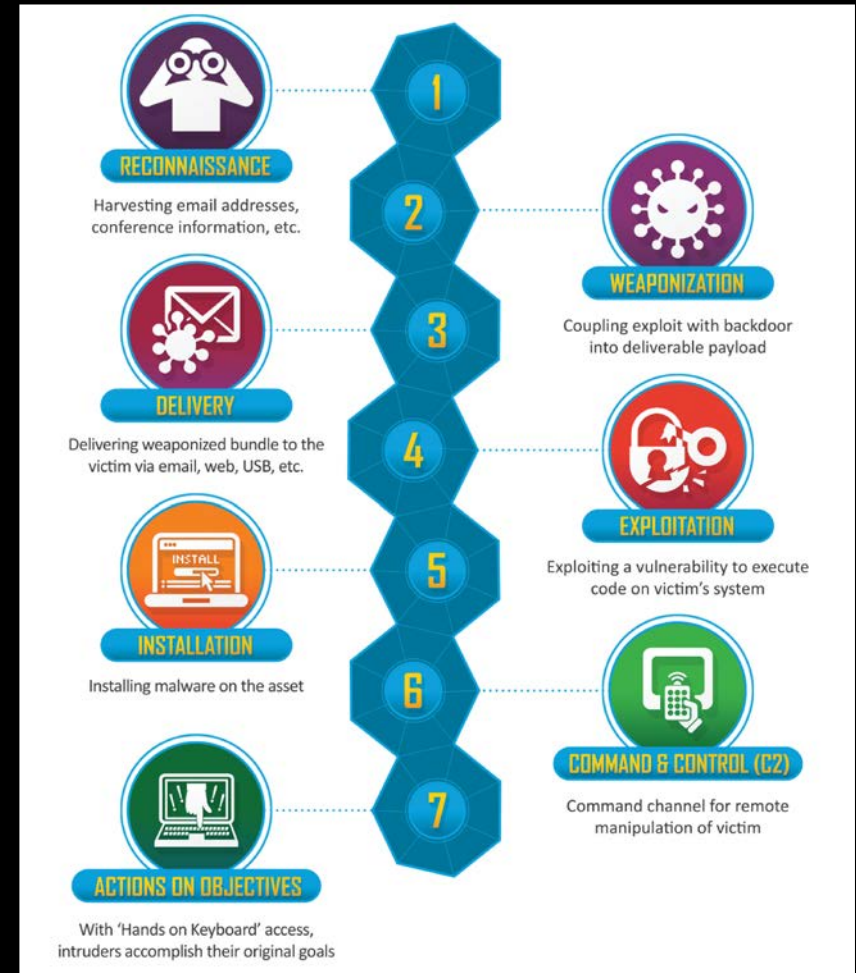
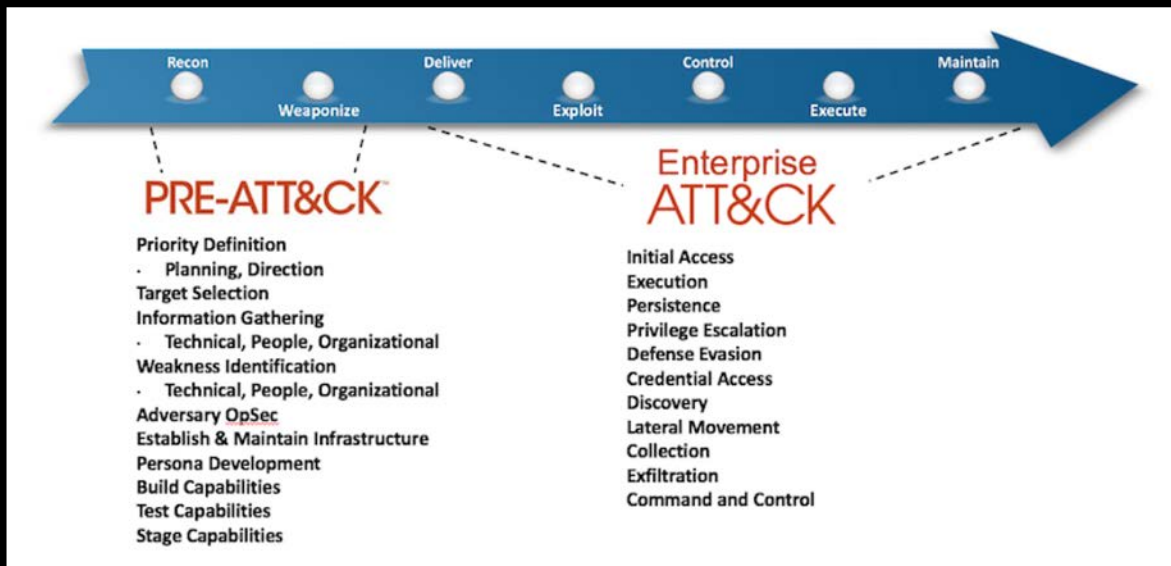
# What's your plan?

- What's your focal point?
  - User, workstation, network...
- I prefer the endpoint
  - It's where the user lives
  - Closest to most likely attack vector
  - Almost every external threat eventually becomes an internal threat
  - You have to win every time before compromise, but after compromise you only have to succeed once



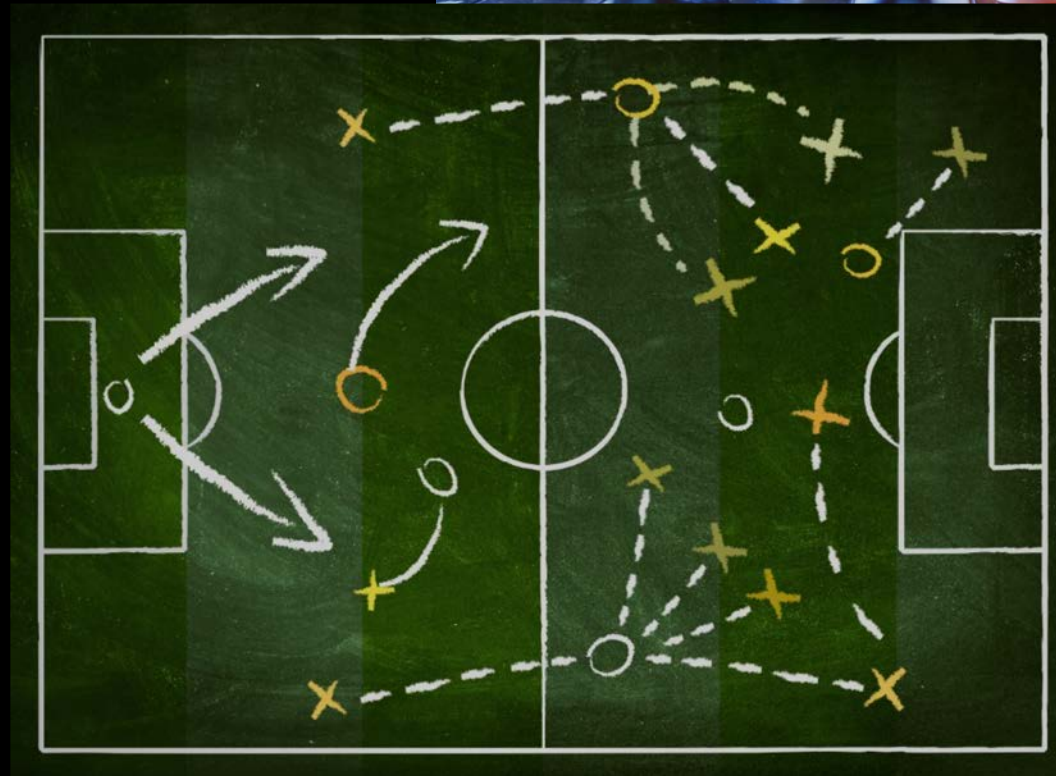
# Create a threat model

- Let's use US-CERT alert TA18-074A
- Model against a structured framework
  - Lockheed Martin Cyber Kill Chain
  - MITRE ATT&CK



# Key tactics of attack

- Spear phishing
- Compromised Credentials
- Maintain access
- Enumerate network
- Cover Tracks







## Spear Phishing

- **Highly targeted**
  - Advanced/complex emails – maybe
- **Malicious attachments**
  - Force SMB authentication to remote location



## Spear Phishing

- Detect Phishing
  - Mail rule for “kindly” – Half joking
  - Manual search for emails with attachments that appear anomalous
    - Maybe policy doesn’t allow
  - Check SMB authentication outbound NTLM
- Detect SMB authentication
  - Check SMB authentication outbound NTLM



Compromised  
Credentials

- Used against single factor logins



Compromised  
Credentials

- Detect harvested credentials
  - Authentication sources
    - Wildly different network locations
  - UBA?
  - Anomalous logins



Enumerate  
Environment

- Using PSEXec – renamed executable
- DNS
- Users
- Machines
- Screenshots



Enumerate  
Environment

- Detect
  - Process logs/PowerShell logs
    - Find use of PSEXEC
    - Registry edits



Maintain Access

- local administrators – language “aware”
- Disable firewall
- Enabled RDP
- WebShells on the external facing servers
- VNC



## Maintain Access

- Detect local administrators
  - Logs will show group membership changes
  - Force a policy check – If you have one
- Detect Disabled firewall
  - Configuration drift
- Enabled RDP
  - Configuration drift
  - Process logs/script logs
- WebShells on the external facing servers
  - Web app logs
  - Web connection
- VNC
  - Network logs





## Cover Tracks

- Uninstall applications
- Delete Logs
- Cleanup users created



## Cover Tracks

- Detect Uninstalled applications
  - Application logs - probably not centrally logged
  - Configuration drift
- Delete Logs
  - Security logs
- Cleanup users created
  - Security Logs



Command and  
Control

- User-agent entropy

It's a question slide

