Pokemon League

<https://attack.mitre.org/>  
<https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0050%2FG0050-enterprise-layer.json>

Defense

* Vulnerability Cards
  + Related to mitre attack
* Inject Cards

Offense

* APT Cards
  + Related to Mitre
* Inject Cards

Money cards? Buy new defenses/buy new attacks

Things to do:

1. Create rules for game
   1. What can defense do?
   2. What can offense do?
   3. How do we determine a winner?
   4. Point system?
   5. Tournament system?
2. Create card front and back lol
3. How do we determine who is on defense and who is on offense?
4. Is this one team vs one team or multiple teams?
5. Do we want defense to have to figure out who the enemy is?
6. Announce a few times over the next week
7. Create intro for game - make a presentation about APTs and explain a few thangs
8. Create Poster for knowing and get to secretaries

Kedric

1. Presentation about APT
2. Create Defense cards - done
3. Make a back for the cards - done

Jared

1. vulnerability cards/tools
2. Work on marketing
   1. Carson
   2. Aaron about printing
3. Speaks with the printing center

End goal: teach about APTs and how to defend against

Back doors and breaches?

Rules/Gameplay

* APT assign HP
  + - They can either use an attack or use their ability
  + Their goal is to reach impact
    - To define impact:
  + Pick one of 3 to start
  + Leave another 3 out in their market
    - If want to purchase: prove why the groups would work together
* Defender:
  + Have researchers trying to identify APTs
  + Gain money each round
  + Start off with a company - like APT except defense

Cards

* Inject cards :
  + Block attack
  + Gain new attack on privilege escalation
  + Something bad happens such as losing money
  + Something good happens such as gaining money
  + gain/lose HP
  + Lose a tool
  + Go back a step
  + Reveal APT to defense
  + Reveal weakness of defense to offense
* defense/attack cards
  + Set price on hirelings
  + Purchase firewall, SOC, new equipment, etc
  + Attacks can purchase a new tool if APT is blocked
    - General tool and they have to tell us what and why - convince us
  + Give defense a starter pack

Logistics:

* Split teams by tables/divider
* 2-3 min timer : keep on screen
* Offense wins by reachings impact
* Defense wins by offense reaching zero
  + Offense loses HP by rolling
* Penalties for not keeping with the timer
  + Offense: defense gets a successful block = losing hp
  + Defense: successful attack = offense moves one step
  + 60 more seconds; if not then lose turn
* Give recommendations for team setup
* defense : random vulnerabilities is random - draw from a pile
  + Turn all vulnerabilities into cards
* Team limit: we will figure it out

Defense cards:

|  |  |
| --- | --- |
| **Front (Question)** | **Back (Answer)** |
| Defender Inject | Instant: Block an incoming attack |
| Defender Inject | Instant: Stop the attacker from gaining a market card |
| Defender Inject | Instant: Remove all market cards and replace them with new ones |
| Defender Inject | Event: You hear about a hacker group that might be targeting you next. Research an APT that performed espionage on the DNC in the 2016 election and give 3 techniques they used. You have until your next turn to present.  Success: You thwart their attacks, gain a market card for free.  Failure: They post one of your vulnerabilities on the internet. The attackers learn one vulnerability. |
| Defender Inject | Event: A new zero day has emerged, find a recent zero day and give a 30s-1m presentation next turn  Success: Patch a vulnerability  Failure: A hacker takes advantage of the zero day, the hackers gain $100 |
| Defender Inject | On Your Turn: Reveal the persistence technique the attackers have |
| Defender Inject | Event: You were attacked! You have until your next turn to find the APT responsible based on the following: Zyxel Router, Denmark  Success: You replace your Zyxel router, remove one vulnerability with the word "Network"  Failure: Your Zyxel router gets taken over, add a vulnerability card. |
| Defender Inject | Event: Your CEO wants you to stop the most common technique for APTs to get initial access? What do you stop? Report to your CEO on your next turn.  Success: The CEO finally realizes that more budget = less security incidents. Gain $200  Failure: The CEO gets hacked, lose $300 |
| Defender Inject | Event: You are purchased by a company, gain $300, your decision maker is laid off (decision maker is silent until next round) |
| Defender Inject | Event: You didn't save backups and got hit by ransomware. Lose $100 and gain a vulnerability card. |
| Defender Inject | Event: Researchers join a union and start protesting their pay. (Researchers are silenced until your next turn) |
| Defender Inject | Event: Choose 1: Lose this turn or remove 1 market card permanently |
| Defender Inject | Event: You have an insider! Select one person to show two vulnerabilities to the attackers. |
| Defender Inject | Event: Bonuses! You gain $500 |
| Defender Inject | Event: Company vacation to Hawaii for Cybermoncon! Lose this turn, but gain 1 market item for free. |
| Defender Inject | Event: The attackers messed up and let you know their technique! Reveal 1 technique from the APT |
| Defender Inject | Event: The government increases their Cybersecurity spending, add 2 items to the market this turn, remove 2 at the end of this turn. Pay the government $100 (does not apply to Government Agency). |
| Defender Inject | Event: You let half of your team go because of the recession, gain $300, but silence half of your team. |
| Defender Inject | Event: You get into a debate about who should be the decision maker, choose a new decision maker. You may choose to buy another inject this turn. |
| Defender Inject | Instant: Gain a market card for free |
| Defender Inject | Instant: Draw the top 3 market cards, pick one and discard the rest |
| Defender Inject | Instant: Add 2 minutes to your turn |
| Defender Inject | Instant: Stop a negative inject card from happening |
| Defender Inject | On Your Turn: Gain intel on a vulnerability that the attackers can attack |
| Defender Inject | On Your Turn: Discard another inject card and $1,000 to learn about an attack the APT has done to another company/government |
| Defender Inject | On Your Turn: View the attackers market and remove one item |
| Defender Inject | On Your Turn: Remove two minutes from the attackers turn, you may buy a market card |
| Defender Inject | On Your Turn: Draw two inject cards or gain $300 |
| Defender Inject | On Your Turn: Hack back (not ethical), deal damage to the attackers |
| Defender Inject | On Your Turn: Choose 2 vulnerabilities to turn into honey pots, if the attackers attack that vulnerability, you gain $200 and a market card (they still advance in MITRE). |
|  |  |
|  |  |

| **Front (Question)** | **Back (Answer)** |
| --- | --- |
| Attacker Inject | Instant: Bypass the defenses of the opposing team for your attack |
| Attacker Inject | Instant: Stop the defender from gaining a market card |
| Attacker Inject | Instant: Remove all market cards and replace them with new ones |
| Attacker Inject | Event: You hear about a hacker group that might be targeting you next. Research an APT that performed espionage on the DNC in the 2016 election and give 3 techniques they used. You have until your next turn to present.  Success: You thwart their attacks, gain a market card for free.  Failure: They post one of your signature attacks on the internet. The defenders learn one of your signatures. |
| Attacker Inject | Event: A new zero day has emerged, find a recent zero day and give a 30s-1m presentation next turn  Success: Gain advantage on exploiting the zero day and gain $100  Failure: The defenders patch the zero day and gain $100 |
| Attacker Inject | On Your Turn: Reveal the most recent defense purchased by the defenders |
| Attacker Inject | Event: You were attacked! You have until your next turn to find the APT responsible based on the following: Zyxel Router, Denmark  Success: You replace your Zyxel router, remove gain $200  Failure: Your Zyxel router gets taken over, go down one tier on the Mitre Attack Matrix |
| Attacker Inject | Event: Your Team Leader wants to manipulate the most common technique for APTs to get initial access? What is this? Report to your Team Leader on your next turn.  Success: The Team Leader starts to appreciate your efforts. Gain $200  Failure: The Team Leader dislikes you, lose $300 |
| Attacker Inject | Event: You are hired by a 3rd party, gain $300. You cannot attack the defenders for one round because of your side gig. |
| Attacker Inject | Event: You didn't save backups and got hit by ransomware. Lose $100 and go down one tier in the Mitre Attack Matrix. |
| Attacker Inject | Event: Researchers are upset and start protesting their pay. (Researchers are silenced until your next turn) |
| Attacker Inject | Event: Choose 1: Lose this turn or remove 1 market card permanently |
| Attacker Inject | Event: You have a double agent! Select one person to show the defenses a signature |
| Attacker Inject | Event: Bonus! You gain $500 |
| Attacker Inject | Event: Group vacation to Hawaii for Cybermoncon! Lose this turn, but gain 1 market item for free. |
| Attacker Inject | Event: The defenders messed up and let you know their vulnerabilities! Reveal 1 company vulnerability |
| Attacker Inject | Event: The government increases their Cybersecurity spending, add 2 items to the market this turn, remove 2 at the end of this turn. Pay the government $100 |
| Attacker Inject | Event: You fire ½ your team because they suck, gain $300, but silence half of your team. |
| Attacker Inject | Event: You get into a debate about who should be the Team Leader, choose a new Team Leader. You may choose to buy another inject this turn. |
| Attacker Inject | Instant: Gain a market card for free |
| Attacker Inject | Instant: Draw the top 3 market cards, pick one and discard the rest |
| Attacker Inject | Instant: Add 2 minutes to your turn |
| Attacker Inject | Instant: Stop a negative inject card from happening |
| Attacker Inject | On Your Turn: Gain intel on a vulnerability that the defenders have patched |
| Attacker Inject | On Your Turn: Discard another inject card and $1,000 to learn all the vulnerabilities the defense has in a tier of the Mitre Attack Matrix of your choice |
| Attacker Inject | On Your Turn: View the defenders market and remove one item |
| Attacker Inject | On Your Turn: Remove two minutes from the defenders turn, you may buy a market card |
| Attacker Inject | On Your Turn: Draw two inject cards or gain $300 |
| Attacker Inject | On Your Turn: Remove the most recent defense purchased by the defenders |
| Attacker Inject | On Your Turn: Choose 2 vulnerabilities to turn into honey pots, if the defenders patch that vulnerability, you gain $200 and a market card (they still successfully patch). |

Game Setup

1. For teams - assigned at door
2. For role: draw 3, pick one
   1. Remove stage 1
3. For defense: draw ½ of cards per vulnerability tier
4. Assign team roles
5. Setup market: 3 per side
6. Assign starting cash - $1000
7. Lower dividers and put timer/rules on screens
8. Each team assigned a moderator (watches the cash flow and helps you out if needed)
9. Offense - setup APT market (3 random)
10. Defense knows what the possible apts are

Game Rules:

1. Defense goes first
2. 3min timer per turn - bonus 2min if go over
   1. Offense: defense gets a successful block = losing hp
      1. 20 sided die to decide loss
   2. Defense: successful attack = offense moves one step
3. Team team has a set income per round (updates later in game)
   1. Defense: 200$
   2. Offense: $100
4. Per turn(one action):
   1. Action one
      1. Pay $100 to draw an inject card
      2. Play inject card
      3. Pay $100 to reset market
      4. Defense: purchase tool
   2. Action two
      1. Defense: pay double for a custom tool
      2. Card abilities
      3. Market card purchase (everyone)
5. Required to develop resources for offense to make initial attack
   1. Also when purchase new APT to join team
   2. If fail initial access, required to develop a new resource to try new attack
6. Reconnaissance - both roll 20d
   1. Defense: plus tier level
   2. If critical success for offense then get to see ½ of vulnerabilities
   3. If fail for offense then detected and lose health
   4. If normal success then get one of vulnerability
   5. If critical success for defense then roll 2 d20
7. Winning:
   1. Offense reaches impact
   2. Defense defeats APT -aka lose all health
      1. Successfully block attack or detect active scan