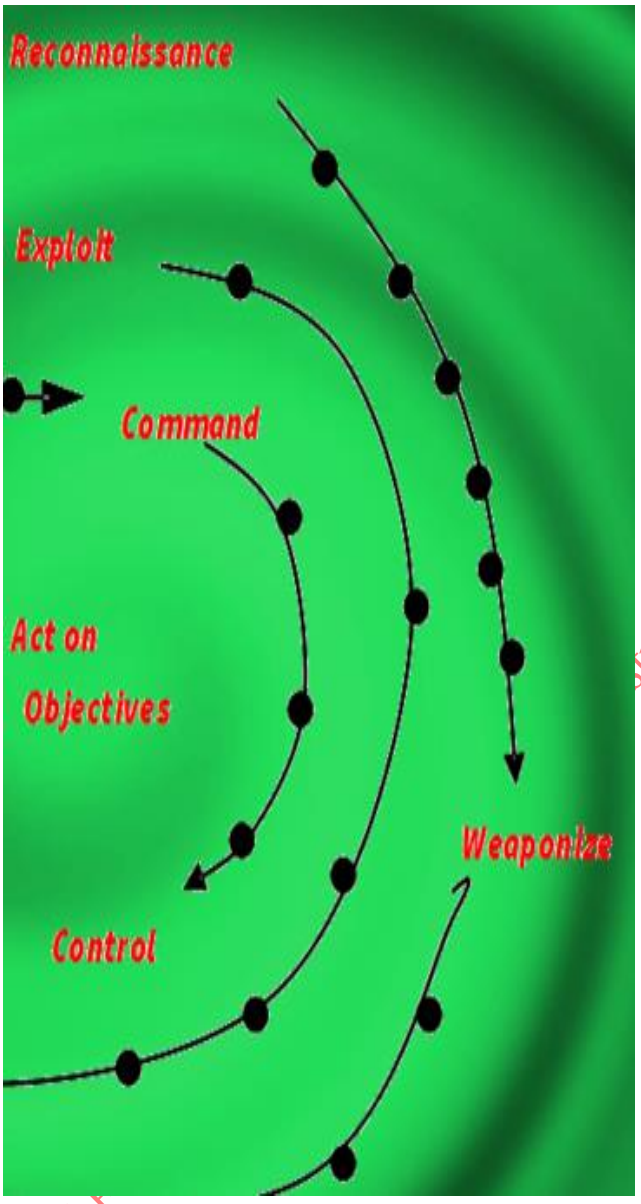

stromthegame/defcon24

MAELSTROM

'Are You Playing with a Full Deck?'

Shane Steiger

Attack Lifecycle Game Concept

version .8

© 2016

#cybermaelstrom

github.com/maelstromthegame

MAELSTROM: AN ATTACK LIFECYCLE GAME CONCEPT

Maelstrom is a game concept and model meant to enable Education, Demonstration and Evangelism within Cyber Security disciplines. The game concept is intended to span from the 8th grade levels to the cyber security Ninja (locked in his mom's basement). It is based on the Lockheed Martin Kill Chain Attack Lifecycle. The game also borrows concepts from several MITRE Frameworks, attack patterns mapped from previous cyber campaigns and from real 'cyber security life'. The Attacker's goal is to reach a progressive Action on Objective. The Defenders will play cards, tactics and strategies to prevent this progression.

Pick your side, pick your Actor and pick your Act on Objective, buy or build your own cards. Hope you don't lose! 'Are You Playing with a Full Deck?'

OFFICIAL RULES

CONTENTS: Include a game board (Figure 1), initial game cards for the red Attacker Deck, a blue Defender Deck (Figure 2), a green Act on Objective Deck, (optional Expansion packs of 'build your own' not shown), 2 dice, 9 Actor poker chip game pieces, tablets, pens and money.

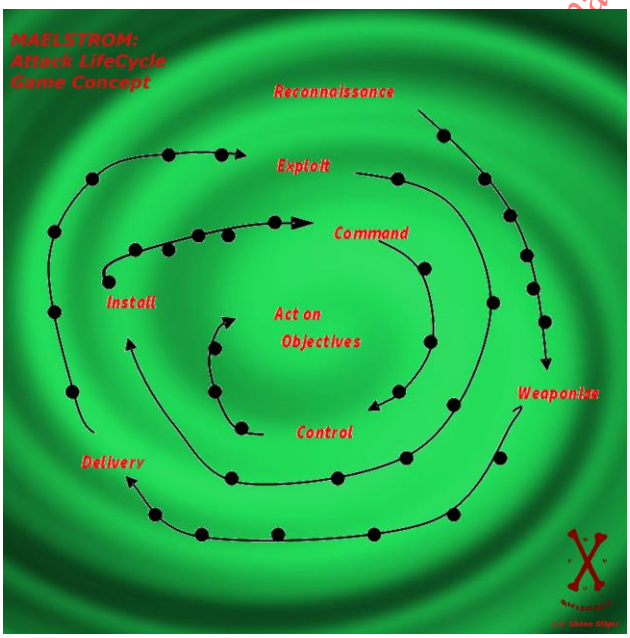

Figure 1 MAELSTROM Game Board

Anatomy of the Maelstrom board consists of multiple stages of an Attack Lifecycle (Lockheed Martin based in this case) where the start position for the Attacker is Reconnaissance. The 6 dots between phases indicate positions. Reconnaissance, Weaponization, Delivery, Exploit, Install, Command and Control (C2), Act on Objects are each phases in which on the appropriately labeled cards can be played.

GAME SETUP

FIRST:

Pick how many players Attackers

SECOND:

Attacker picks or draws their Threat Actor:

Pick from (12):

defcon24

LIST – State Actor, Ware Fighter, Freelance Spy, Script Kiddies, Political/Social, Insider Threat, Hacktivist, Disgruntled Employee, Corporate Spy, Criminal Organization, Criminal Freelance, Joker ☺

DRAFT – goto

Attacker does not reveal to the table the choice or draw and places the game piece face down on the board on Reconnaissance. Just like real life where you don't necessarily know the type of Threat Actor you are dealing with.

THIRD:

Attacker picks or draws their Act on Objective card

Pick from (11):

LIST – Humiliate, Pivot from Shared Space, Blackmail, Denial of Service/Cryptowall, Destroy, Data Disclosure, Exfiltration, Plant False Data/Information, Persistent Foothold for Future, Defacement/Vandelism, Pick any Act on Objectives Joke

Does not reveal to the table the choice or draw and places the game piece face down in the center of the board on Act on Objectives

Anatomy of Attacker and Defender Cards:

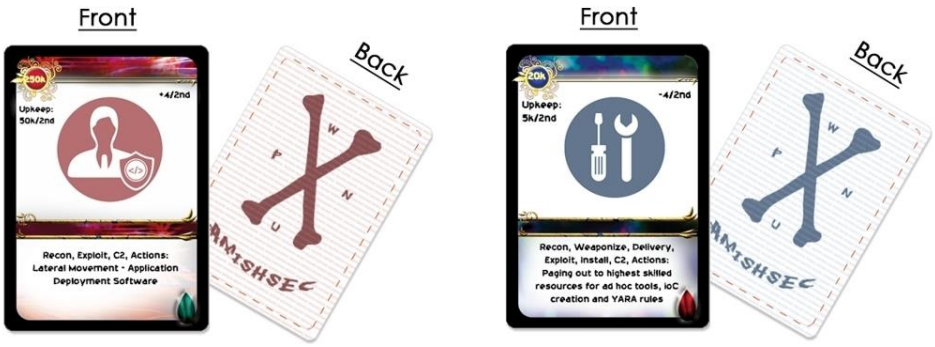

Figure 2 Example Attacker Card and Defender Card. Attacker cards are RED, Defender cards are BLUE.

Text of Card

The text indicates the phases in which a card can be played. This includes Reconnaissance, Weaponization, Delivery, Exploit, Install, Command and Control (C2) or Act on Objectives. For instance, this card indicates that it can only be played in the Reconnaissance (Recon), Exploit, C2 and Actions phases.

github.com/maelstromthegame/defcon24

Progression

A + or - indicates the progression and the number indicates the steps within a phase a player can advance their game piece(s).

For Ninja play, the players will need to buy their own cards according to a Cost.

Cost

For Ninja play, the players will need to maintain their budgets and pay upkeep of the value shown and the round frequency shown. For instance the card above is a $50k charge to the attacker for every second round of play to keep using the +4 progression through the phases.

DRAFT - goto https://www.github.com/maelstromthegame/defcon24

Upkeep is also meant for Ninja play.

DRAFT - goto https://www.github.com/maelstromthegame/defcon24

METHOD OF PLAY

Easy - 8th Grade Level – Quick and Fun!

2 Players – Role a single dice. The player with the highest roll decides to be the Attacker or Defender. The other player takes the opposite role. The Attacker then writes down an Action on Objectives (cards coming soon). The Attacker must build their cards only towards this Action on Objectives unless a card in play states otherwise. The Attacker plays with the Attacker cards only and the Defender plays with Defender cards only unless a card in play states otherwise ☺

The Object for the Attacker is to progress through the board until they reach and play the appropriate cards/story for their particular Act on Objectives.

Referring to the Anatomy of the cards,

7 cards are initially drawn by each player with the Attacker leading the first round. When a player plays a card, the opposite player can then play a follow on card. The player can discard if there are no playable cards in their hand or they wish to discard a card in exchange for another. The rounds continue as each hand is played.

Story of Play:

With each card played, the player must supply a one or two sentence description of the way in which the card is being played with some ‘fact fiction’ to create the story of play.

This does require the player to be somewhat versed in the usage and role of the card. It also makes for fun fact fiction!

Easy to Moderate – College Level – Tactical choices

Multiple players – Players choice on rolling dice or picking sides. Players also can pick the particular cards they would like in their deck for play. Keep in mind your opponent(s) may be picking tactical cards to defeat the cards you have so pick wisely.

- **Hard (Real Life) - Ninja Level**– Strategic choices coupled with realistic challenges

Multiple players – Players decide their role of Attacker or Defender. They are then given budgets to play with based on a dice role or as mutually (suggest realistically) decided between the players. The budget is a multiplier of 100,000 of the dice player's dice roll. For instance, if a player rolls a 3 then the budget = $300,000.

LATEST INFORMATION

Maelstrom github

- https://github.com/maelstromthegame/defcon24

Maelstrom twitter

- https://twitter.com/cybermaelstrom

REFERENCES

Lockheed Martin Cyber Kill Chain

- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

MITRE ATT&CK Framework

- http://attack.mitre.org/

MITRE CAPEC

- http://capec.mitre.org/

MITRE Cyber Resiliency Engineering Framework

- https://www.mitre.org/capabilities/cybersecurity/resiliency
- https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
- http://www2.mitre.org/public/industry-perspective/

DRAFT - goto https://www.github.com/maelstromthegame/defcon24