Maelstrom: Are you playing with a full deck?

Using an Attack Life Cycle Game to Educate, Demonstrate and Evangelize

Shane Steiger, Esq. CISSP

$ whoami

~ messing with computers since 1989 - TIN, PINE, yTalk, Lynx, MUDs, etc.

~ 8 years in a large food manufacturer helping to build and secure SCADA/ICS systems across 90+ food manufacturing plants in the US.

~ 6 years building out a security function in one of the largest pharmaceutical drug distributors in the US.

~ currently Chief Endpoint Security Architect in a large tech company building out the roadmaps for desirable Cyber Resiliency techniques in the endpoint space.

~ much better than family law! I am more of a geek.

$ disclaimer

~the views and opinions are purely my own based on time in the industry and experience. They don't necessarily reflect the views, positions or policies of my employer.

~oh yeah....this presentation and discussion is not intended to give legal advice nor form any kind of attorney/client relationship. I am not your attorney and some of the things you might find interesting may require consultation with your own attorney (not me ☺).

$ agenda

~journey picking strategies - who wins?
~attack life cycle primer
~why study attack lifecycles?
~what do effective defensive strategies look like?
~exercises in building out your defensive strategies
~...maybe there is something more here...

$ strategy journey

~from a past life, I was asked by a CIO ‘do they win?’

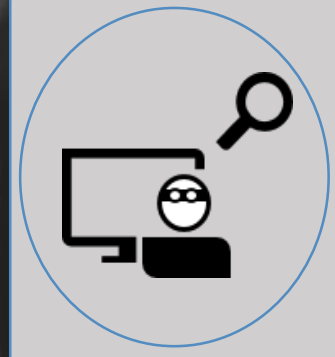
~later, asked to look at a solution for over 300k endpoints

~like most folks – look at requirements, functions, capabilities and operationalization

~hmmmm....wow I got a pretty heat map that doesn’t seem very useful in terms of selecting things at large scale

~‘do they win’ stuck with me to develop better strategic choices

$ Lockheed Martin Kill Chain Phases ™

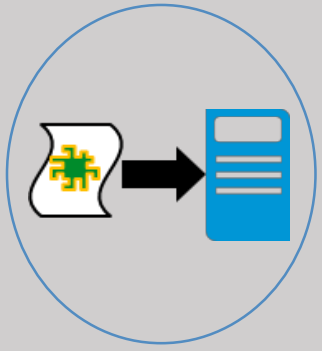


Reconnaissance

- Research, ID/selection of targets
  - Email addresses
  - Social relationships
  - Target technology & topology

Weaponization

- Combining an exploit with a payload to establish/maintain access by attacker



Delivery

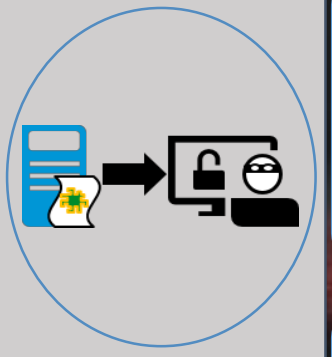
- Transmission of weapon to target environment

Exploitation

- Exploit is triggered on target

Installation

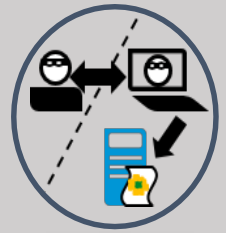
- Payload is executed



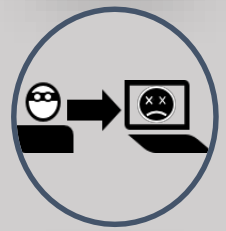
Command and Control

- Communication and control is established between attacker and target

Act on Objectives



Recon/Pivot



Destruction

Exfiltration

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

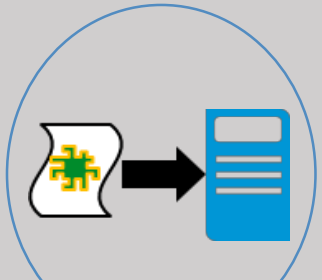
$ Lockheed Martin Kill Chain Phases ™ *misnomer

Reconnaissance

- Research, ID/selection of targets
  - Email addresses
  - Social relationships
  - Target technology & topology

Weaponization

- Combining an exploit with a payload to establish/maintain access by attacker



Delivery

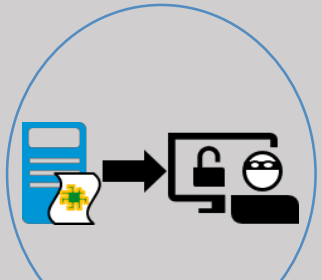
- Transmission of weapon to target environment

Exploitation

- Exploit is triggered on target

Installation

- Payload is executed

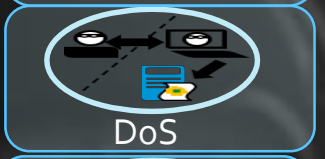


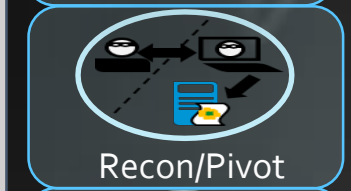
Command and Control

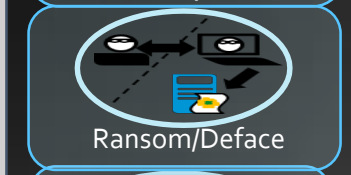
- Communication and control is established between attacker and target

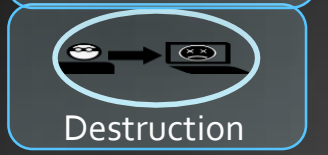
*defender is the actor in a kill chain!

Act on Objectives



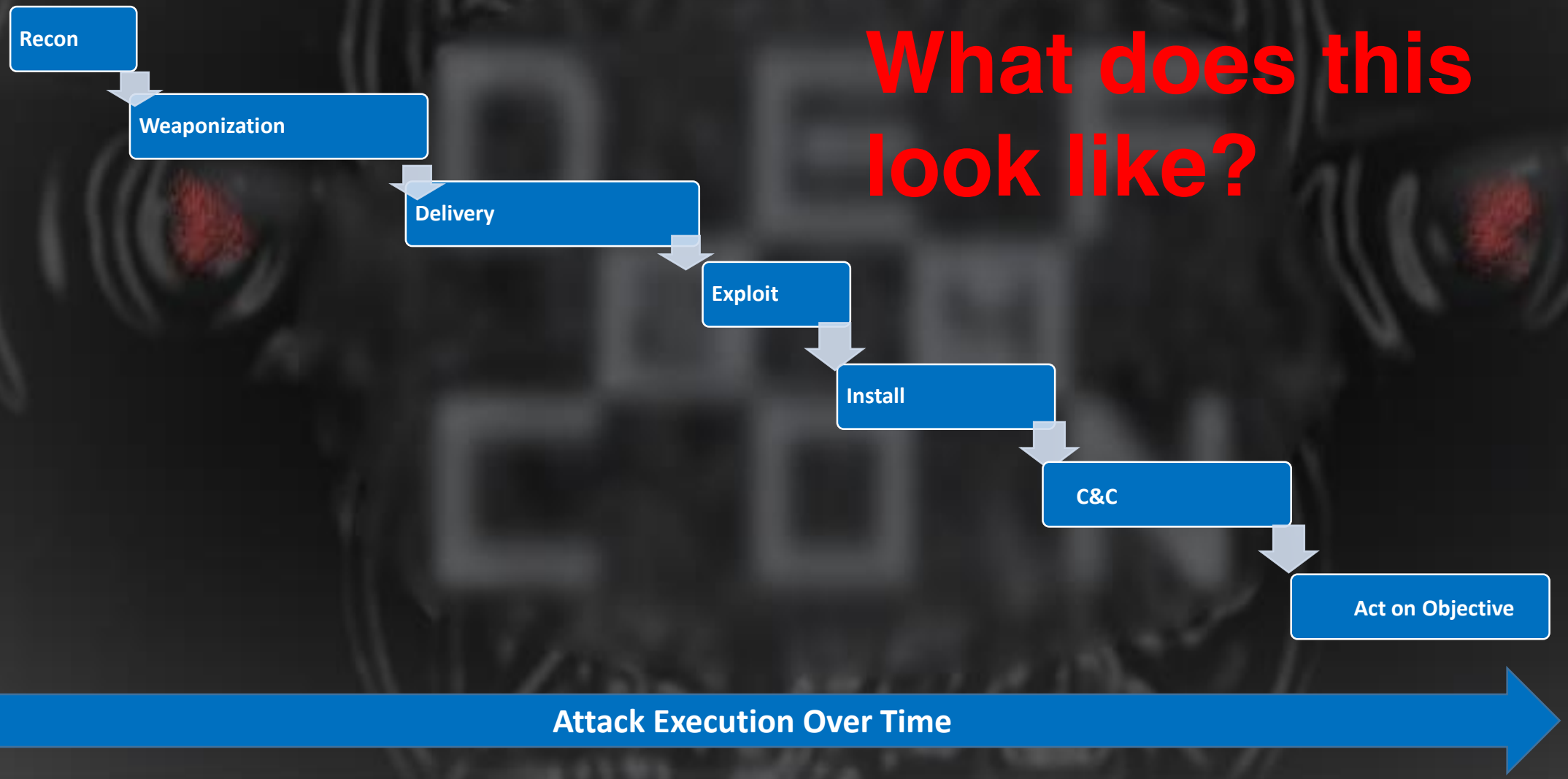






http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

$ tortuosa concept–charting attacker's progression



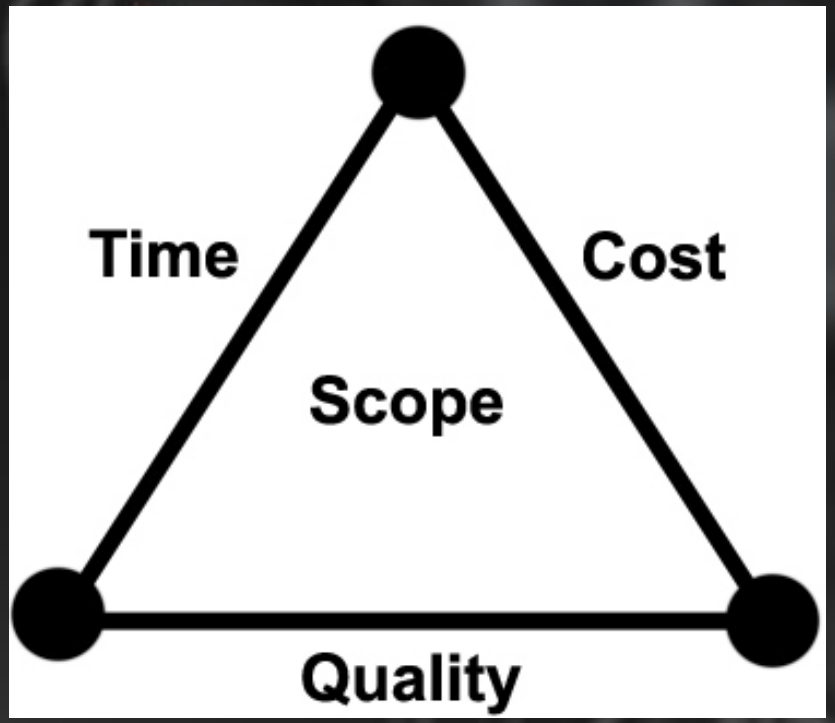
$ tortuosa concept – attacking the attacker's plan

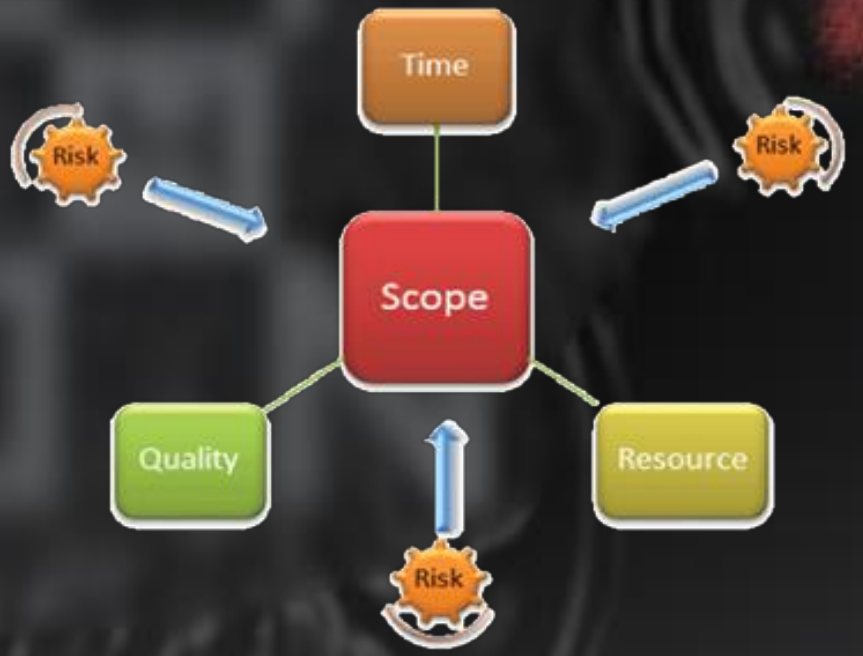
- ~what does this look like?
  - Looks like a ***Gantt Chart! A project plan!***
  - Attackers are organized indicating plan progression for campaigns
- ~what other evidence have we seen to indicate the attackers seem to follow a plan if not a traditional project plan?
  - Different time schedules indicating 'shift work'
  - Different skill levels from the same attackers indicating different 'resources or teams'
  - Different teams using different tool sets
  - Follow scripts and make mistakes redoing work or retrying task

$ tortuosa concept – attacking the attacker's plan

Attack the Attackers' Project Plan!

IT organizations are experts at messing up project plans. Mapping these plans can reveal weakness in the attackers' plan.





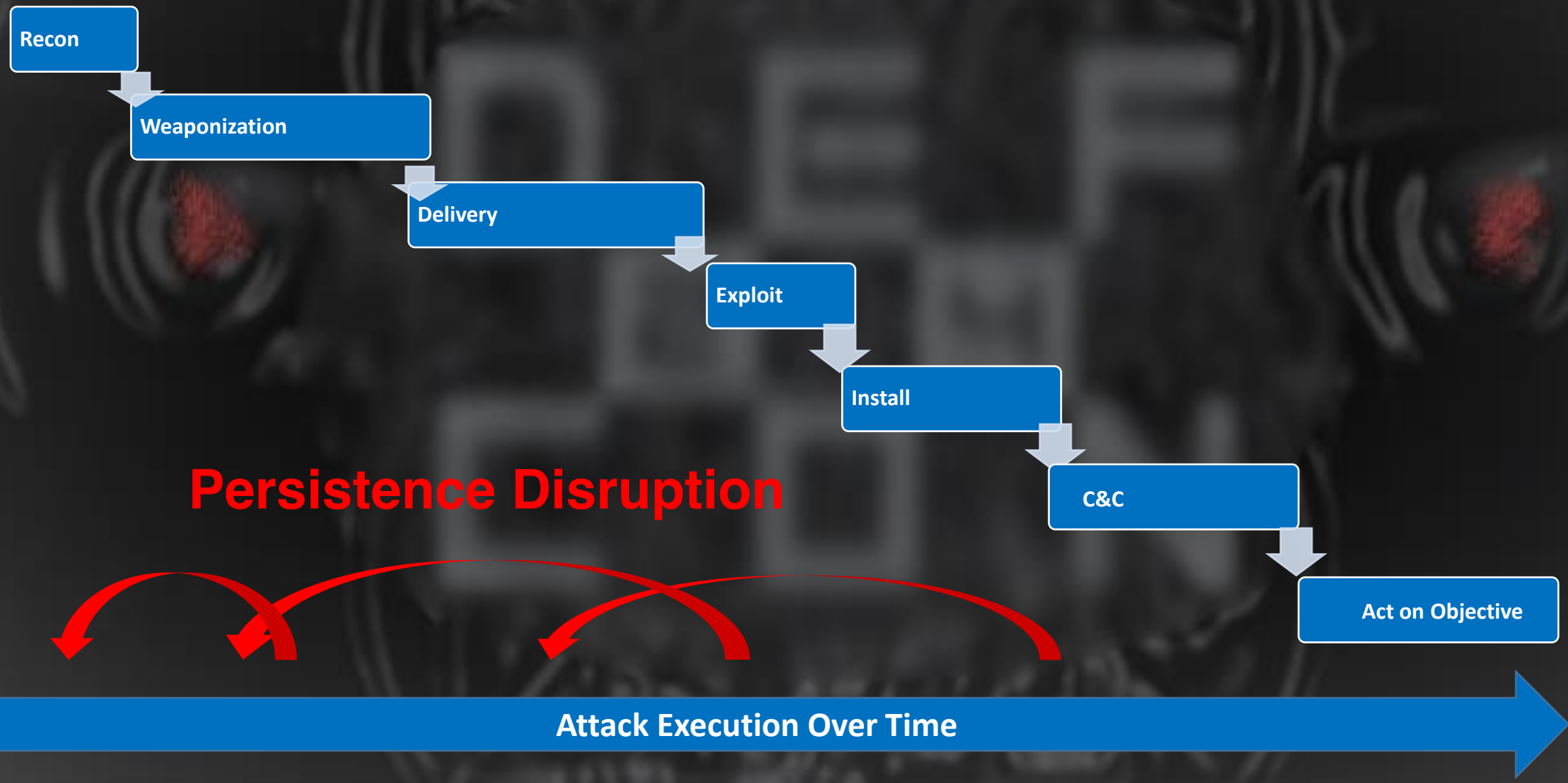
https://en.wikipedia.org/wiki/Project_management_triangle

$ tortuosa concept – attacking attacker's plan

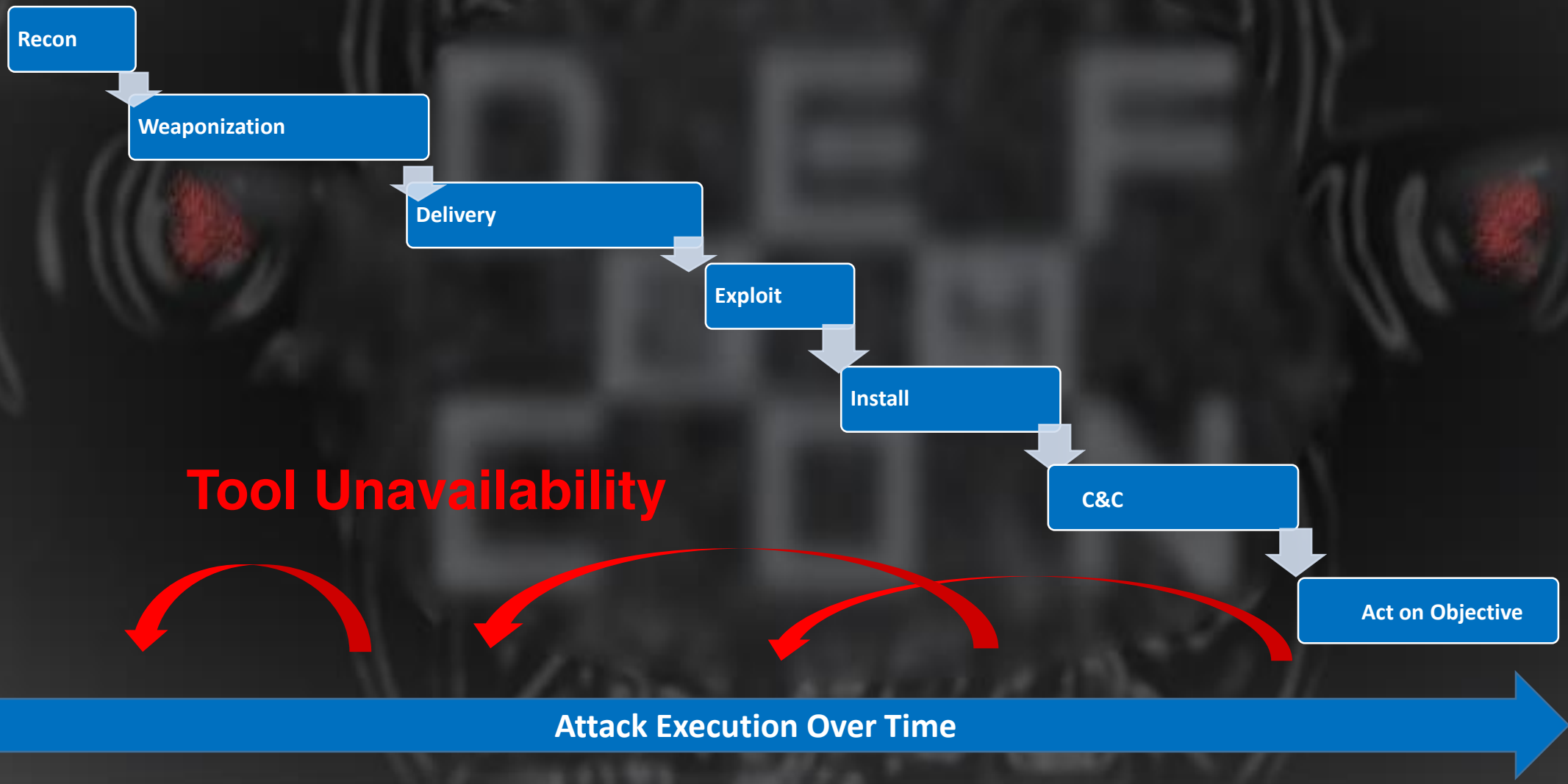
What can we do to disrupt the attacker's project plan?

- ~ Time: Strategies to attack – 'assumed linear time'
  - Replays
  - Snapshots
  - Predecessors and Successors – feigning completion
- ~ Resources and Tools: Attack the 'shift work'
  - Create resource unavailability – maybe APT Team F uses Cloudflare (during Team F stage block Cloudflare)
  - Create resource contention – flood targets?
  - Different teams using different tool sets
- ~ Scope: Create scope creep utilizing deception with fake targets or tarpits
- ~ Cost: Increase setting the attacker back in progression increases cost to them thereby decreasing cost to defender to remediate
- ~ Quality: Create noise and anomalies – attackers, automation and scripts are disrupted

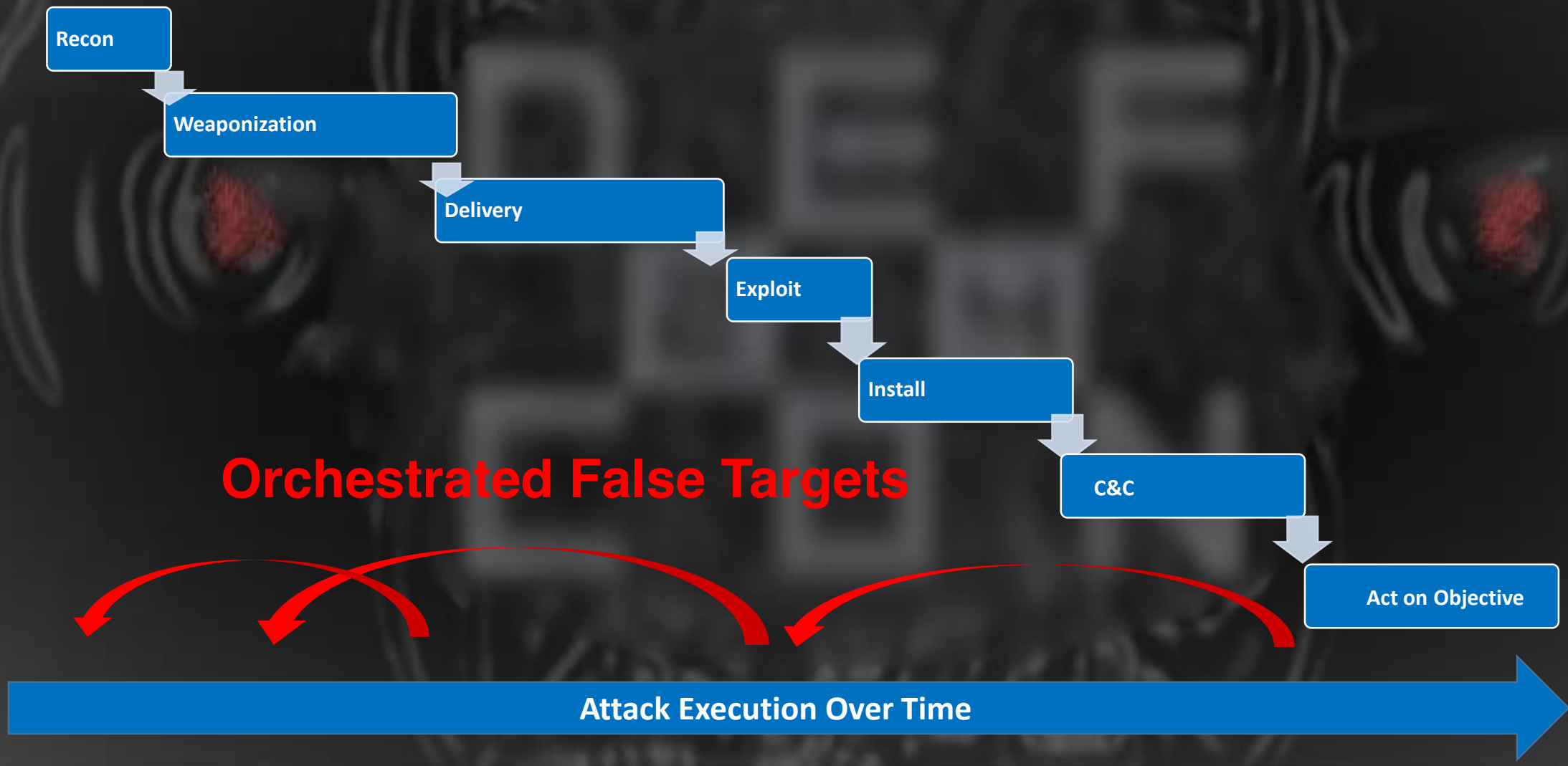
$ tortuosa concept – charting attacker progression



$ tortuosa concept – charting attacker progression



$ tortuosa concept – charting attacker progression



$ tortuosa concept – attacking attacker's plan

Reconnaissance	Weaponization	Delivery	Exploit	Inst
Reconnaissance				
List Timeframe, Successor/Predecessor				
List Resource(s), Tools				
List Tasks in Timeframe				
	Weaponization			
	List Timeframe, Successor/Predecessor			
	List Resource(s), Tools			
	List Tasks in Timeframe			
		Delivery		
		List Timeframe, Successor/Predecessor		
		List Resource(s), Tools		
		List Tasks in Timeframe		
			Exploit	
			List Timeframe, Successor/Pred	
			List Resource(s), Tools	
			List Tasks in Timeframe	

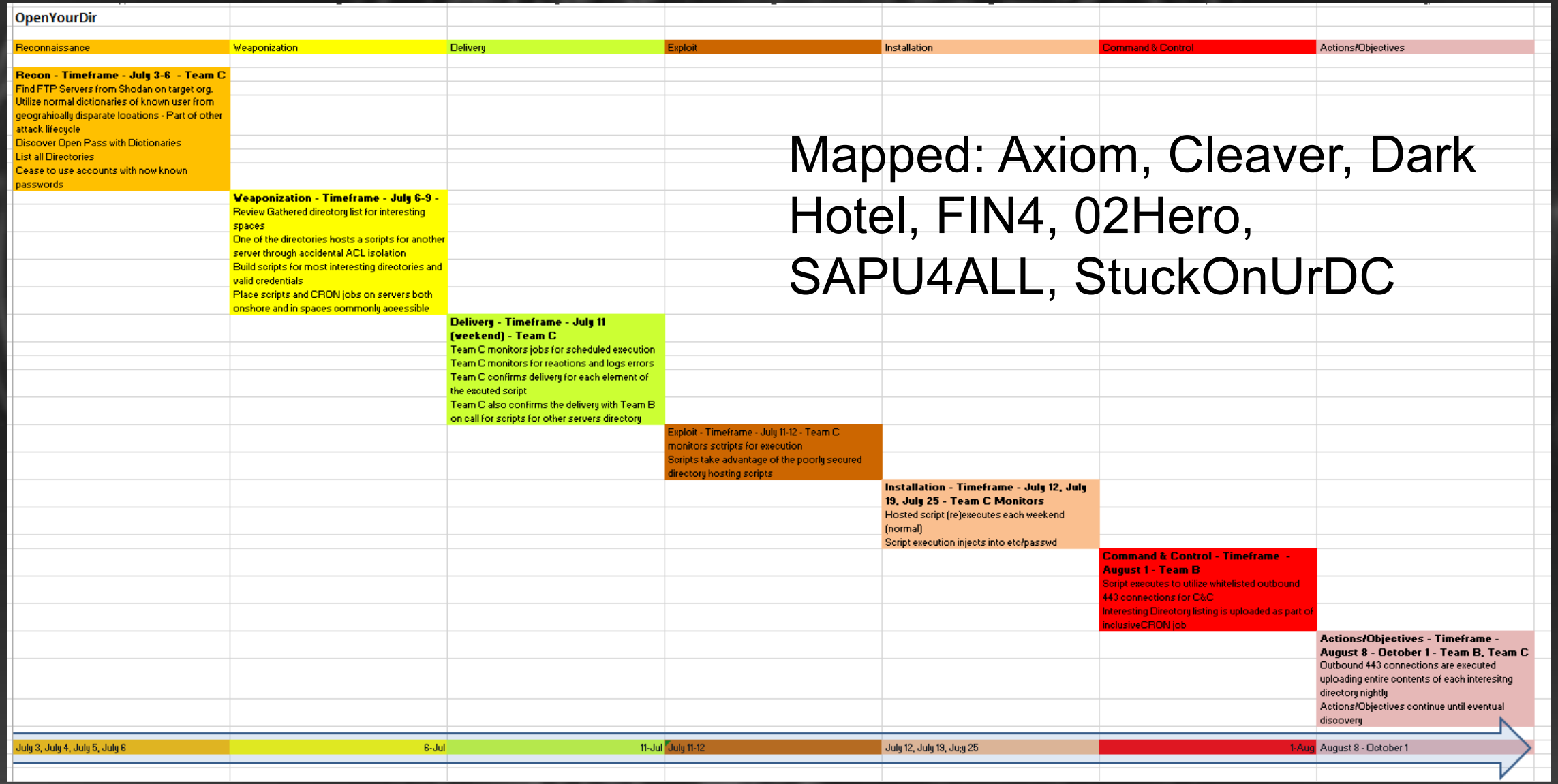
Targets:
Assumed Linear Timeline Disruptions
Resource/Tool - Contention/Unavailability
Scope Creep - Scope Expansion - Adversary Target Deception
Fight Organization - Chaotic Randomness
Predecessors, Successor
Disrupt Deliverables

Cyber Resiliency Techniques

- Adaptive Response
- Analytic Monitoring
- Coordinated Defense
- Deception
- Diversity
- Dynamic Positioning
- Dynamic Representation
- Non-Persistence
- Privilege Restriction
- Realignment
- Redundancy
- Segmentation
- Substantiated Integrity
- Unpredictability

***https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

$ tortuosa concept – attacking attacker's plan



Mapped: Axiom, Cleaver, Dark Hotel, FIN4, 02Hero, SAPU4ALL, StuckOnUrDC

$ got the plans, let's build catalog of attack patterns

Recon	Weaponize	Delivery	Exploit	Install	C&C	A/O
Exploratory Phishing Attacks	Custom Toolset/0-day exploit	RCE on internet facing host	Buffer Overflow	Executed dropper pulls rootkit code	SSL connection over arbitrary port	(Pivot & Recon) controlled host used to scan for open fileshares
Port Scans	Criminal Commodity Framework	Malicious email attachment	Privilege Escalation	Installation of new backdoor via inline-code	HTTP/HTTPS posts back to attacker C&C host	(Destruction) drive of controlled host is wiped
Google/Shodan Search	Metasploit Module/PoC toolset	Malicious URL	Malicious leverage of user's rights	Initial exploit modifies existing service/code	Data xfer via DNS query	(Exfiltration) documents found on controlled host are sent back to attacker

$ build catalog of attack patterns – light ‘em up

Recon	Weaponize	Delivery	Exploit	Install	C&C	A/O
Exploratory Phishing Attacks	Custom Toolset/0-day exploit	RCE on internet facing host	Buffer Overflow	Executed dropper pulls rootkit code	SSL connection over arbitrary port	(Pivot & Recon) controlled host used to scan for open fileshares
Port Scans	Criminal Commodity Framework	Malicious email attachment	Privilege Escalation	Installation of new backdoor via inline-code	HTTP/HTTPS posts back to attacker C&C host	(Destruction) drive of controlled host is wiped
Google/Shodan Search	Metasploit Module/PoC toolset	Malicious URL	Malicious leverage of user’s rights	Initial exploit modifies existing service/code	Data xfer via DNS query	(Exfiltration) documents found on controlled host are sent back to attacker

$ building the attacker deck

Build catalog of attack patterns – 8/2015***

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	OS/Software Weakness	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration	Indicator removal	Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration	Indicator blocking	Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit			Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				Scheduled transfer
AT / Schtasks / Cron			File system enumeration				

***https://attack.mitre.org/wiki/Main_Page

$ building the attacker deck

Build catalog of attack patterns – 8/2015***

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	OS/Software Weakness	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration	Indicator removal	Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration	Indicator blocking	Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit			Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				Scheduled transfer
AT / Schtasks / Cron			File system enumeration				

***https://attack.mitre.org/wiki/Main_Page

$ building the attacker deck

Build catalog of attack patterns – Updated 10/2015, more coolness coming 7/2016 ***

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Indicator blocking on host		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Indicator removal from tools		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Indicator removal from host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Masquerad-ing		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Bypass UAC	NTFS Extended Attributes		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Obfuscated Payload			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Rootkit			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Rundll32			Windows admin shares			
Mod. Exist'g Service		Scripting						
Registry Run Keys		Software Packing						
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

***https://attack.mitre.org/wiki/Main_Page

$ do they win - building the defender deck

Defensive Strategies to Each ATT&CK Technique – Complimentary Cards

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	OS/Software Weakness	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration	Indicator removal	Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration	Indicator blocking	Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit			Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				Scheduled transfer
AT / Schtasks / Cron			File system enumeration				

Fight Persistence!		
Time Disruptions		
Intro Scope Creep		
Increase Cost		
Fight Oranization		
Eviscerate Quality/Intro Friction		
		New Services
		Whitelisting
		Blacklisting
		Service Start Failures/Dependancies
		Snapshotting
		Stop all Services, Start all Services
		3rd party certs for start*?
		Modify Existing Services
		Dependacies for Modifications
		Whitelisting Modifications Settings*?
		Blacklisting Modifcation Settings*?
		Disposable Services*?
		Snapshotting
		DLL Proxying*?
		Lookup Friction
		Snapshotting
		Disposable DLLs*?
		Whitelisting*?
		BlackListing*?
		Hypervisor Rootkit
		Host Profile
		Whitelisting
		Blacklisting

***https://attack.mitre.org/wiki/Main_Page - 8-2015

$ tortuosa concept – attacking attacker's plan

While Mapping Noticed Something

~ Some defensive techniques appear most often – Invest!!!!
    Progression disruption – Time
    Build anomalies and fake targets with trips – Scope Creep
    Deception of phase exit – Predecessor/Successor
~ Some strategies seem to have little payoff but high investment
    Don't bang head here!!!!
~ This made sense! Spending time buried in Cyber Resiliency Engineering Framework – This validated the findings and was common sense
    https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
    http://www2.mitre.org/public/industry-perspective/

$ tortuosa concept – attacking attackers' plan

Noticed something more…

~ ….maybe a game?

Got an Attacker Deck

Got a Defender Deck

Got a Progressive Board with Lockheed Martin Attack Lifecycle

$ maelstrom – are you playing with a full deck?

Board Game Mock Up – Attacker Red Deck – Defender Blue Deck

$ maelstrom – are you playing with a full deck?

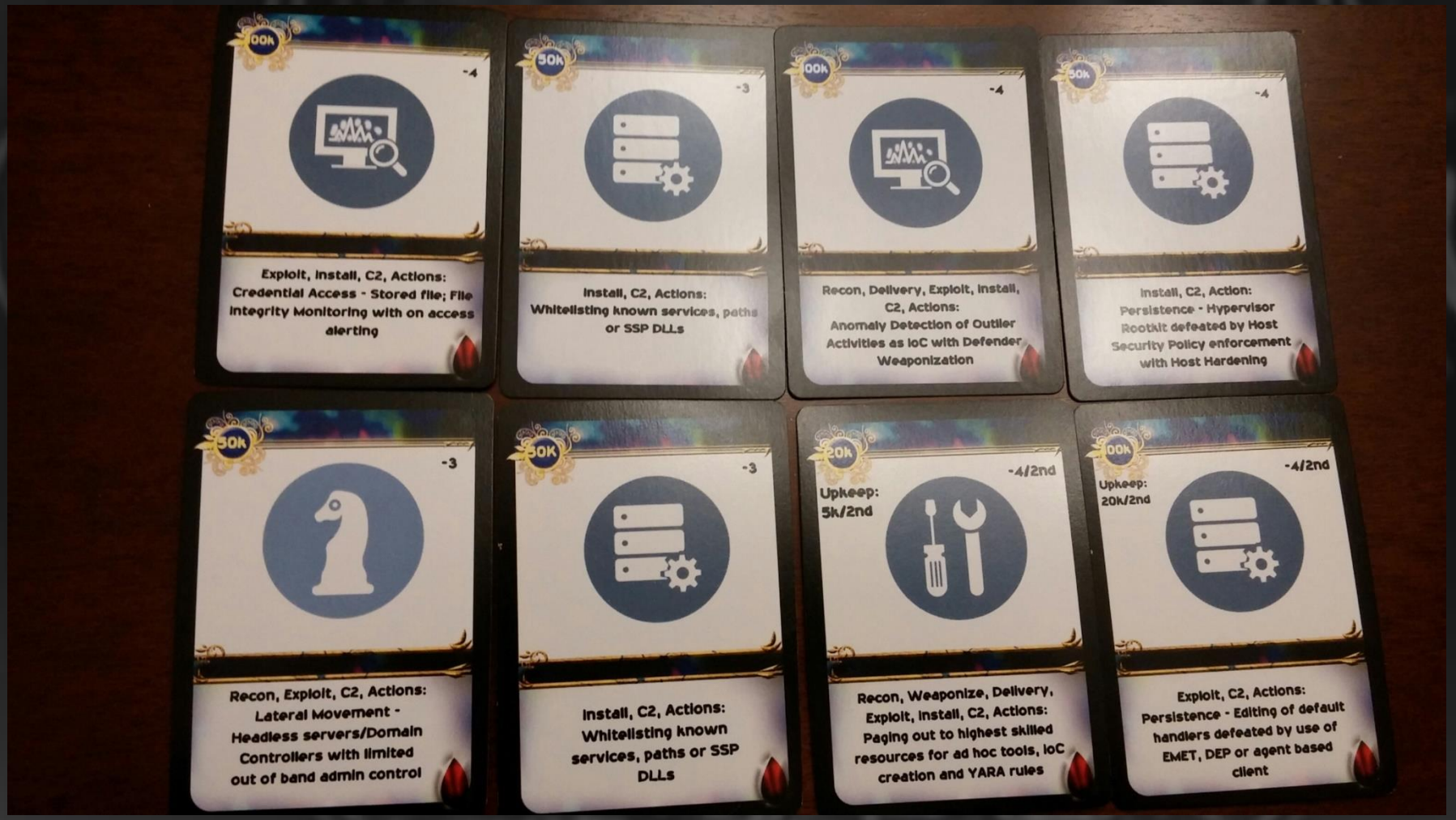
Card Anatomy – Progression, Cost, Upkeep, Usage – Build a Story

$ maelstrom – are you playing with a full deck?

60+ unique attacker cards and 70+ unique defender cards

$ maelstrom – are you playing with a full deck?

60+ unique attacker cards and 70+ unique defender cards



$ maelstrom – are you playing with a full deck?

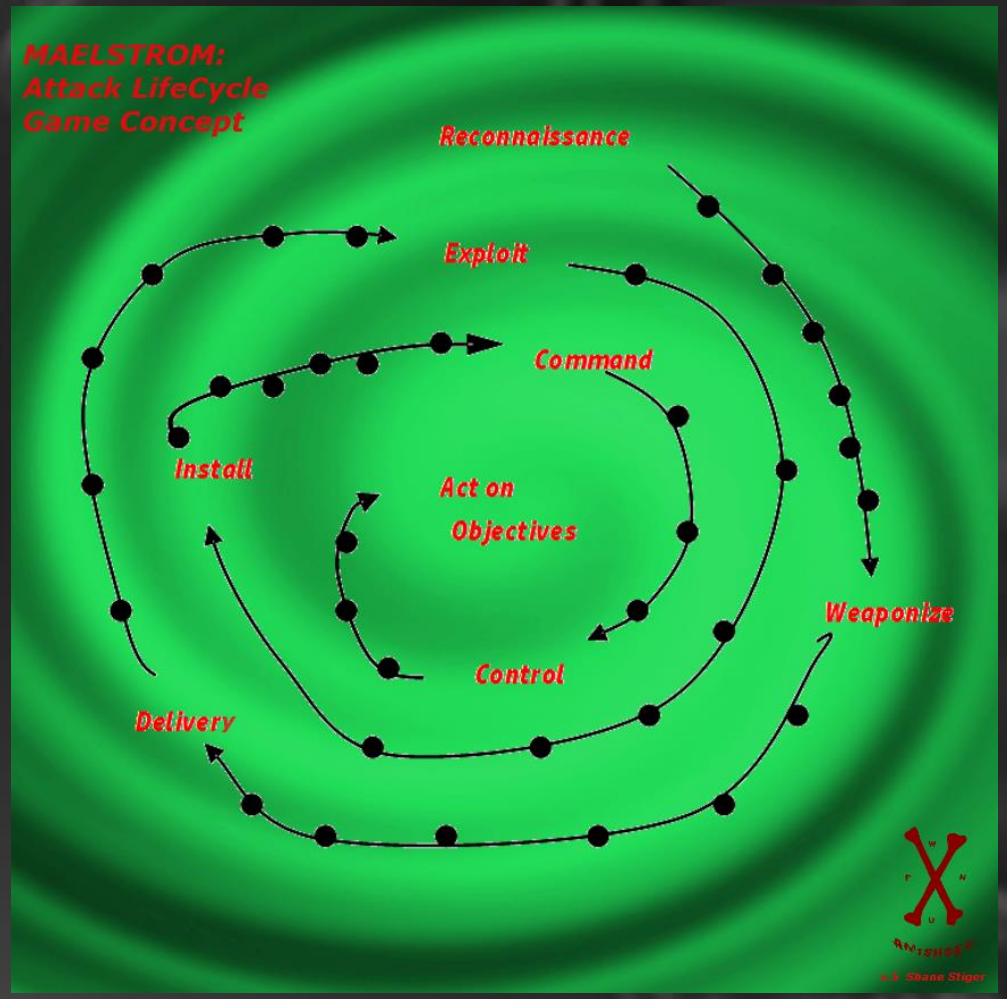
12 unique threat actor chips – face down

$ maelstrom – are you playing with a full deck?

11 unique act on objectives – face down in middle

$ maelstrom – are you playing with a full deck?

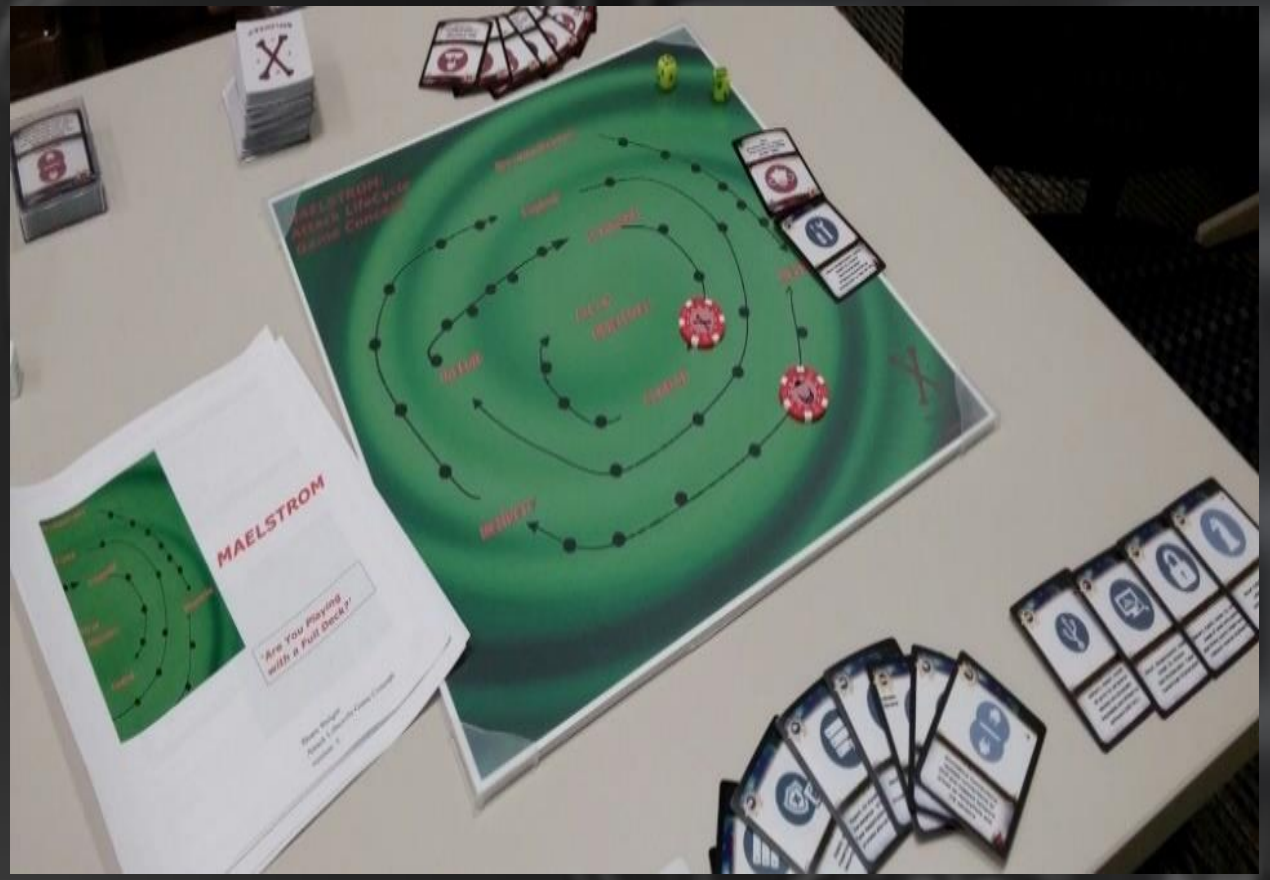
Game Board Mockup – General Rules



- ~ 3 Versions – Easy, Tactical, Strategic
- ~ Dealt cards (easy), actively pick cards (tactical) or buy cards (strategic)
- ~ Choose number of attacker players
- ~ Attackers choose their Threat Actor
- ~ Attackers choose their Act on Objectives
- ~ Attackers seek to get to Act on Objectives through progression to win
- ~ Defenders prevent progression from Act on Objectives
- ~ Defender wins if sets the attacker pieces back to Delivery 3 times or Recon 2 times

$ maelstrom – are you playing with a full deck?

Game Board Mockup – Game Play – Yeah its playable!!!



$ maelstrom – are you playing with a full deck?

Use Cases

- **Education**
  - Learn an Attack Life Cycle concept and make it part of a vocabulary
  - Build a security mindset in defenders who don't do offense
- **Demonstration**
  - Mini table top exercises
  - Defender practice - Investigator pattern recognition
  - Analysis and strategies for choosing technologies to win
  - Cost/Benefit analysis
- **Evangelism**
  - Gamification as marketing
  - Helps to get the message to non security folks

$ build catalog of attack patterns – get more…

Mockup Done – Now Game Tweaks

~ **Official Rules**

Have general rules and game play

~ **More Cards**

Missing certain cards in certain phases

More Opportunistic cards

~ **Rationalization**

Progression steps in a 1-6 effectiveness – Picked 6 because of a dice

Cost rationalization based on a 1000 seat company

~ **Prior Art**

Hacker, Hacker II, Ctrl-Alt-Hack, Elevation of Privilege, Exploits, STIXITS, Cyber Attribution Dice

No one has an Offensive and Defensive game play with a progressive board based on research

$ maelstrom – are you playing with a full deck?

Reaping Benefits Now

- **Example play for**
  - MITRE and Mini Table Tops – MITRE's 5th Cyber Resiliency Invitational (5/2015)
  - Current incidents with investigators
  - Mapping defensive strategies to technology choices – use case validation and development
- **Predicted products and spaces**
  - Ramp up to PoC for startups coming out of stealth
  - Input for development work
- **Educational mechanism for some new team members – expanding concept**
- **Built rich discussion for vendor feedback on products and feature requests**

$ build catalog of attack patterns – get more…

Next Steps

- **Pursue**
  - Submit work for upcoming CON talks, get input
- **Map to current attack patterns and developing patterns and play games**
  - Played multiple rounds with investigators, red team members, engineers and others
  - Produce lessons from games
- **Digitizing and creating open source framework*** (wanna help?)**
- **Expansion packs**
- **Non-technical game development for kids (Spyder)**
- **Let others play and update their decks, watch their decks and collect strategies ;)**
- **LASTLY, digitize and let the ‘Machine Rise and Play Itself’…**

$ where to get maelstrom stuff

Contribute, follow, volunteer, get the latest developments!

For DEF CON CD/Archive viewers, go to these links for all updates…

- **twitter.com/cybermaelstrom**
- **github.com/maelstromthegame/defcon24**
- **to print your copy of the game**
  - **cards, poker chips - makeplayingcards.com (working on getting a sku with the vendor to print)**
  - **game board – download the file from github above and print at FedEx**
- **adding cards – use twitter above for peer review ;) and possible addition**
- **watch twitter and github for digitized version (contact twitter to volunteer to help)**

$ credits

~ ATT&CK Framework
  - https://attack.mitre.org

~ Cyber Resiliency Engineering Framework
  - https://www.mitre.org/capabilities/cybersecurity/resiliency
  - http://www2.mitre.org/public/industry-perspective/

~ Gerard Laygui

~ Garrett Adler

~ Collin Frietzsche

~ Brent Thibido

~ Jerry Decime

~ Cale Smith

~ Tom Van Setten

~ George Mckee

~ Logan Browne

~ Darlene Leong

$ sources

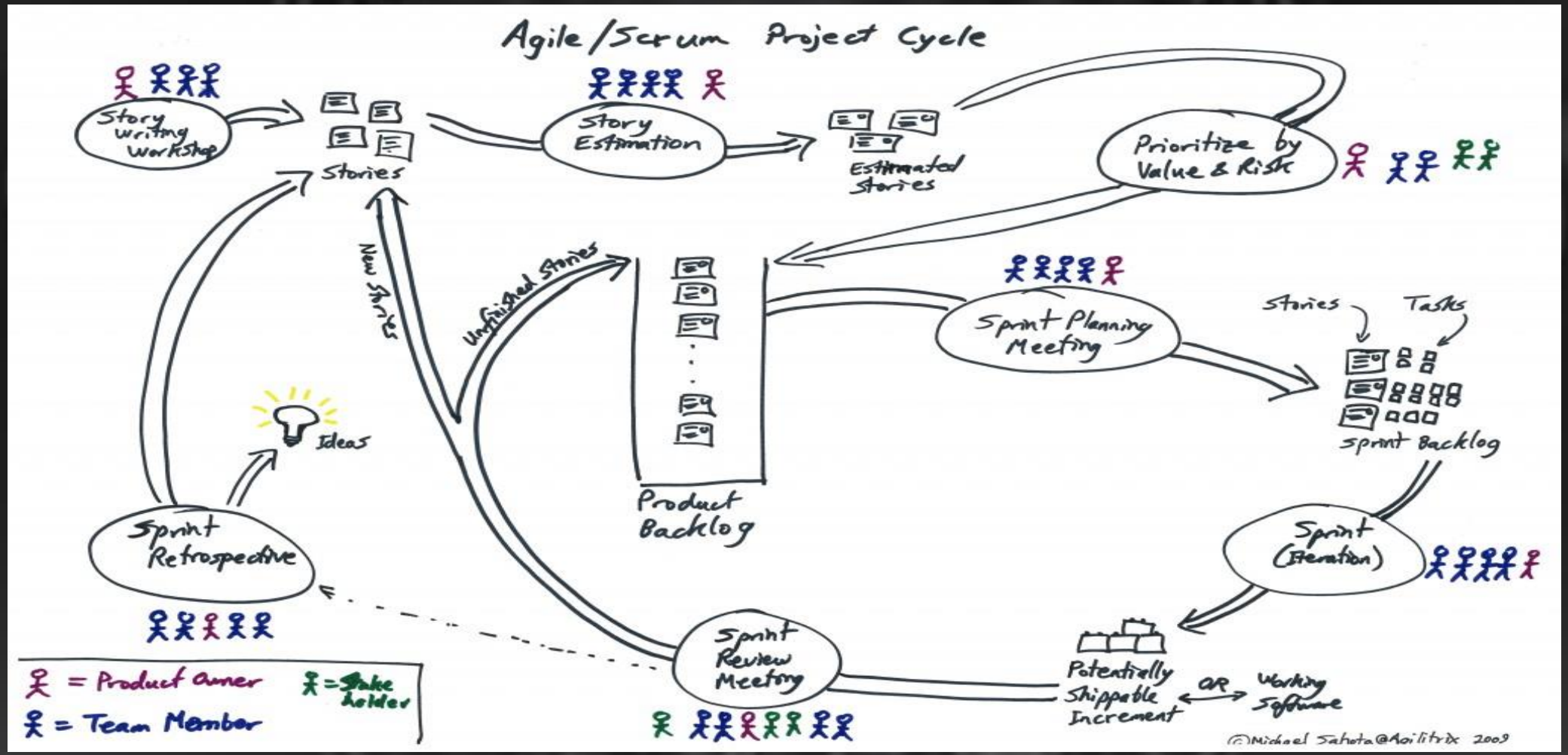
- [1] https://www.dhs.gov/what-security-and-resilience
- [2] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- [3] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- [4] https://en.wikipedia.org/wiki/Cyber_Resilience
- [5] https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
- [6] https://www.mitre.org/sites/default/files/pdf/11_4436.pdf
- [7] https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-aid-the-updated-cyber-resiliency
- [8] https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf
- [9] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ScotlandNCSS.pdf
- [10] https://www.axelos.com/best-practice-solutions/resilia
- [11] https://blogs.microsoft.com/cybertrust/2016/02/11/working-to-increase-the-cyber-resilience-of-cities-around-the-globe/
- [12] http://www2.mitre.org/public/industry-perspective/index.html
- [13] http://www2.mitre.org/public/industry-perspective/guidance-executives.html
- [14] http://www2.mitre.org/public/industry-perspective/guidance-architects.html
- [15] http://www2.mitre.org/public/industry-perspective/slicksheets/disrupting_the_attack_surface.html
- [16] http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
- [17] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- [18]http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- [19] http://mena.boozallen.com/content/dam/MENA/PDF/resilience-in-the-cyber-era.pdf
- [20] https://www.hexiscyber.com/news/hot-topics/pt-2-integration-automation-key-achieving-cyber-resilience

$ questions?

$ backup slides if anyone goes there

$ tortuosa concept – attacking attackers' plan

~…so agile you say



$ tortuosa concept – attacking attacker's plan

~ what can we do to disrupt the attacker's project plan?

Agile SCRUM Methodology

Stories:

- Replays
- Snapshots
- Predecessors and Successors – feigning completion

Sprints :

- Create resource unavailability – Maybe APT Team F uses AWS (during Team F stage block AWS)
- Create resource contention – Flood targets?
- Different teams using different tool sets

- Build Project Backlog:
- Change Priorities:
- Cost: Increase Time and Backlog

https://en.wikipedia.org/wiki/Scrum_(software_development)