Maelstrom: Are you playing with a full deck?

Using an Attack Lifecycle Game to Educate, Demonstrate and Evangelize

Shane Steiger, Esq. CISSP

DEF CON 24

Shane Steiger © 2016

#cybermaelstrom

$ 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

~unexpected journey to a cyber attack lifecycle game

~research that took me on that journey

~maelstrom the game

$ strategy journey

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

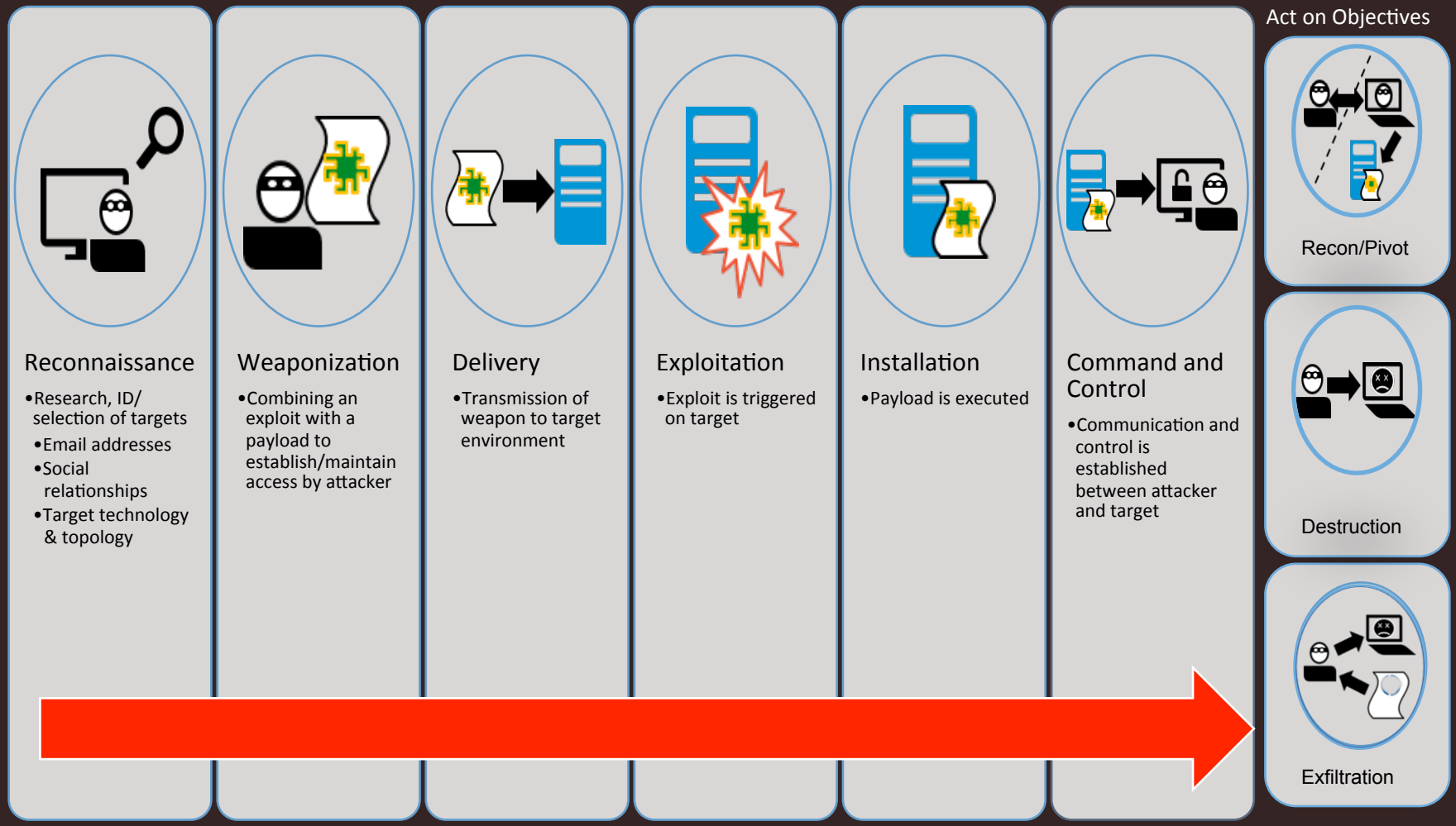
~later, asked to look at a solution for over 300k endpoints

~like most folks – look at requirements, functionality, 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

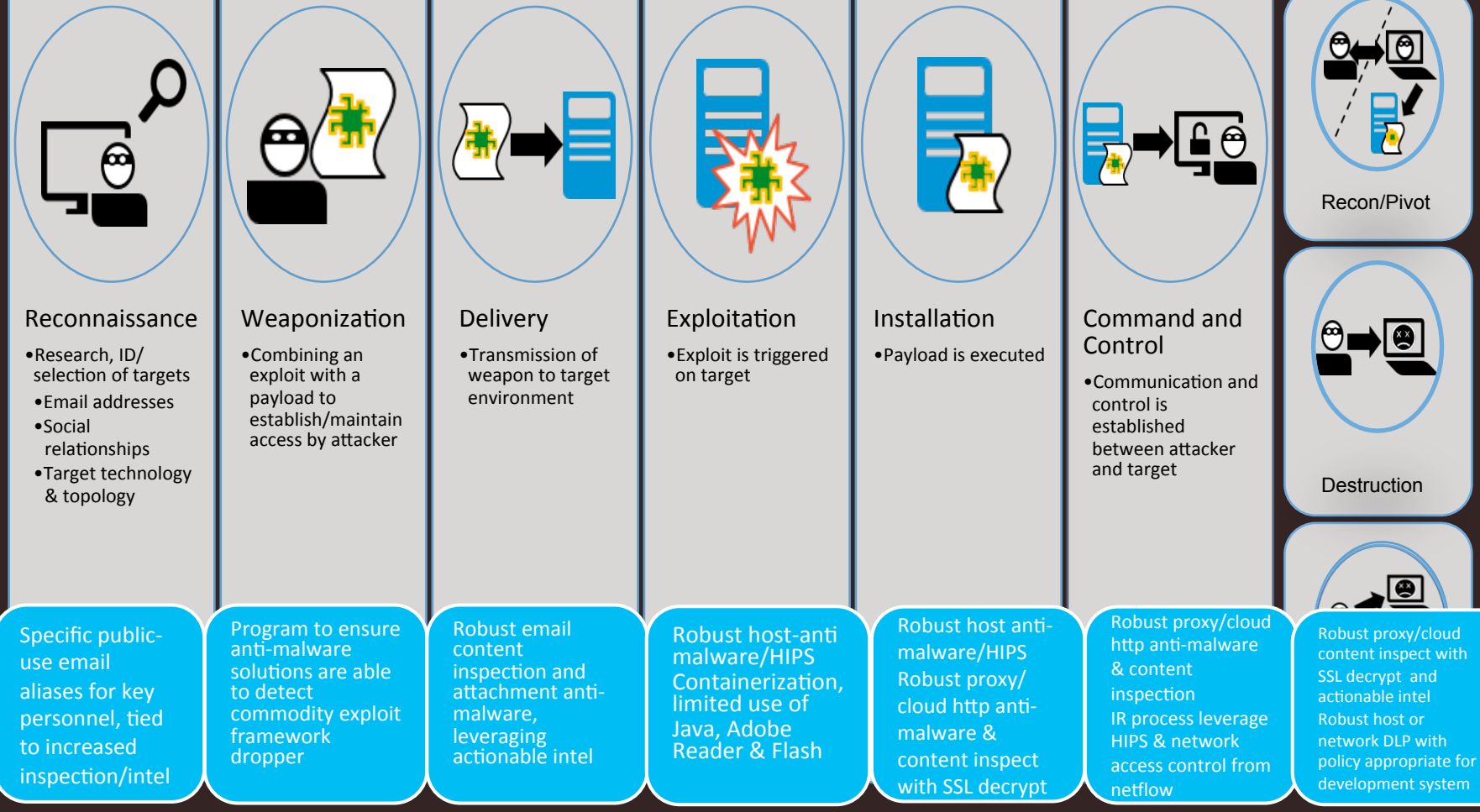
~‘do they win’ stuck with me; find a way to develop better strategic choices

$ Lockheed Martin Cyber Kill Chain®



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

$ Lockheed Martin Cyber Kill Chain®



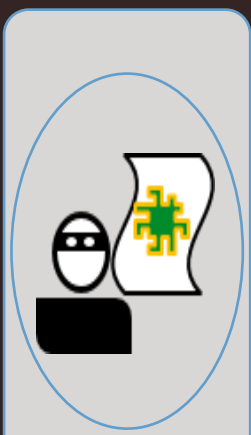
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

$ Lockheed Martin Cyber Kill Chain®*misnomer



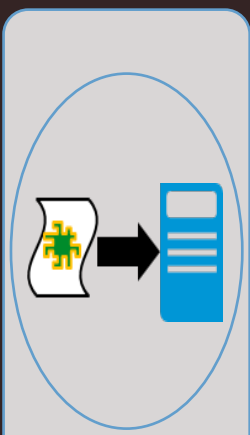
Reconnaissance

- 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



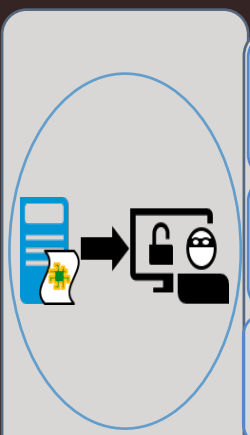
Exploitation

- Exploit is triggered on target



Installation

- Payload is executed



Command and Control

- Communication and control is established between attacker and target

Act on Objectives



Exfiltration



DoS



PlantInfo



Humiliate



Recon/Pivot



Ransomware



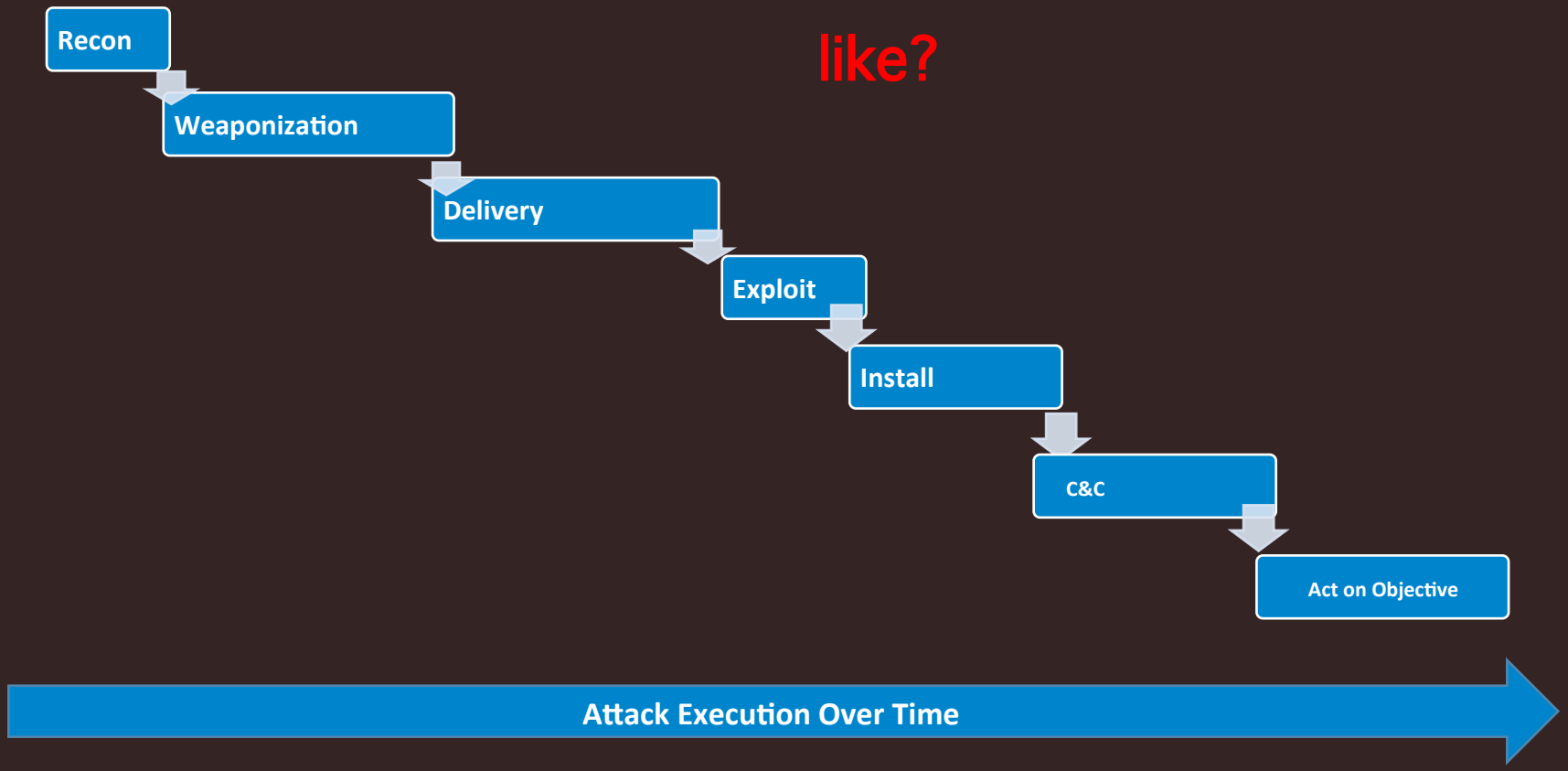
Destruction

defender is the actor in a kill chain!

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

$ charting attacker's progression

What does this look like?



$ charting attacker's plan

~looks like a *Gantt Chart! A project plan!*

- Attackers are organized indicating plan progression for campaigns

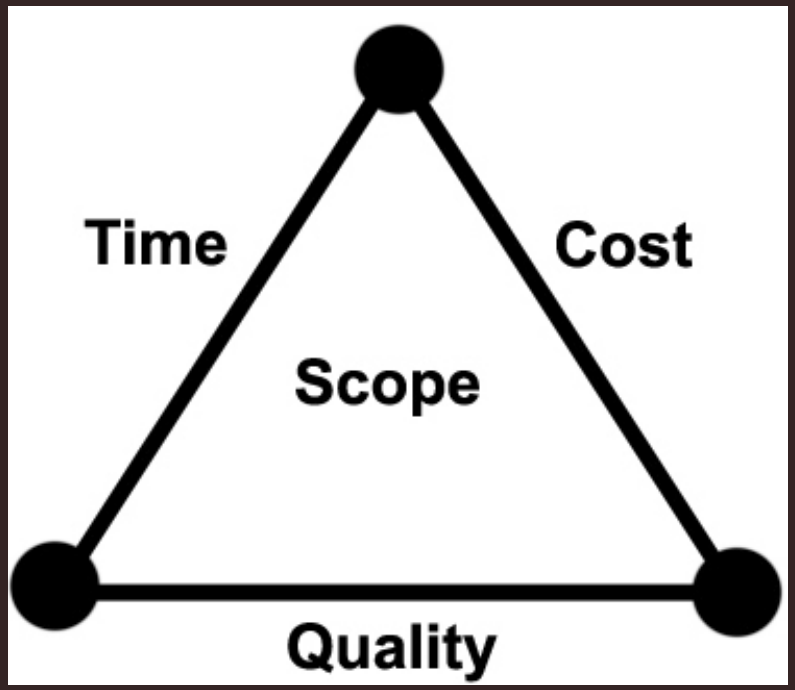
~what other evidence have we seen to indicate the attackers seem to follow a plan if not a traditional project plan?

- Different skill levels from the same attackers indicating different 'resources or teams'
- Different teams using different tool sets
- Different time schedules indicating 'shift work'
- Follow scripts and make mistakes redoing work or retrying task

$ tortuosa concept – attacking attacker's plan

~what can defenders do? attack the project plan!!!

IT organizations are experts at messing up project plans! They do it like it is there job! They even have a methodology!!!



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 techniques can disrupt the attacker's project plan?

~ **Time:** Strategies to attack – 'assumed linear time'
  - Replays – only accept replayed web sessions with an additional token
  - Snapshots – use virtualized environments; revert unpredictably
  - Predecessors and Successors – feigning completion

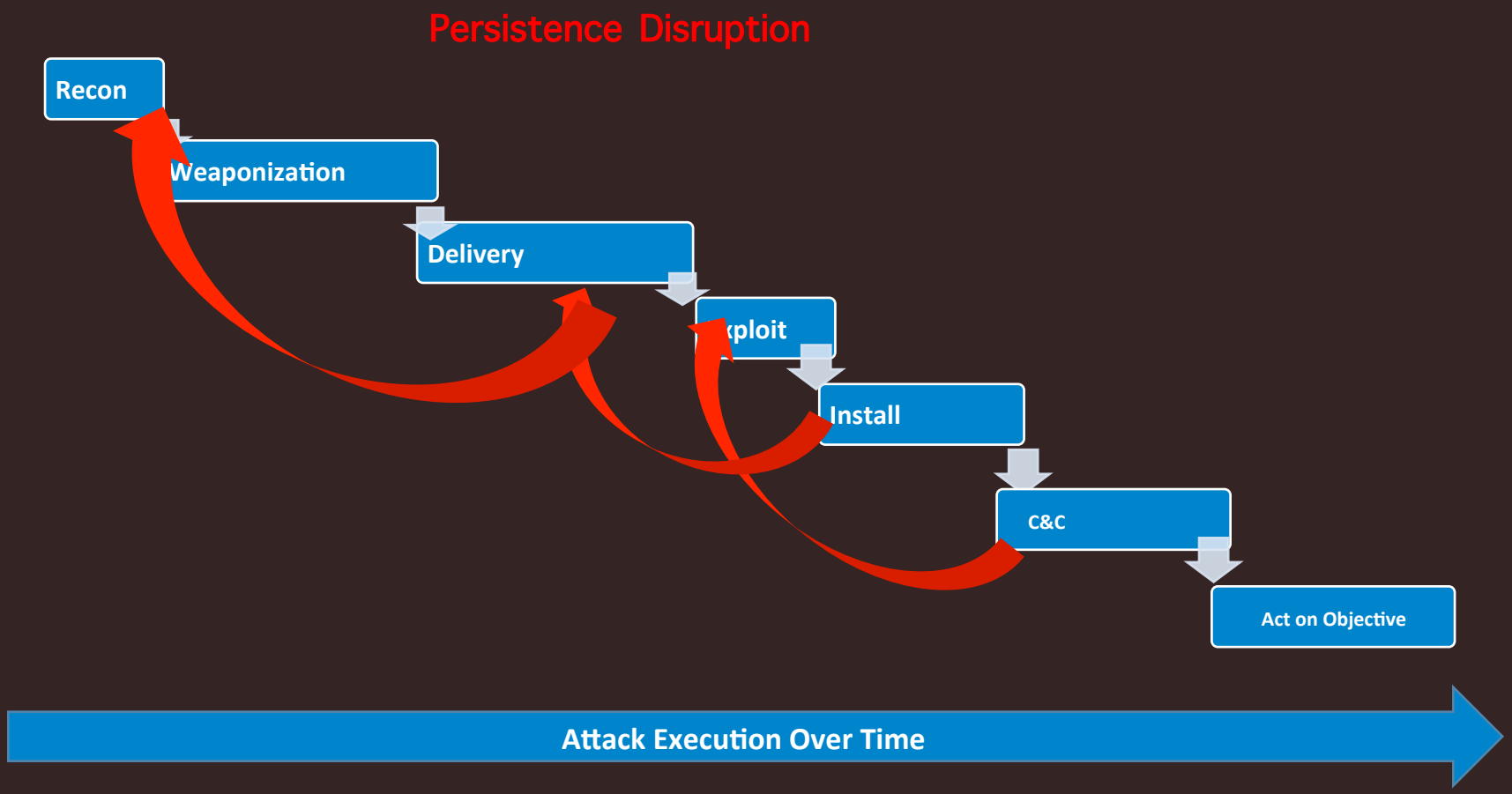
~ **Resources and Tools:** Attack the 'tools or shift work'
  - Create resource unavailability – APT Team F uses Cloudflare; during Team F stage block Cloudflare thereby forcing Team F to page out find another team or resource
  - Create resource contention – flood your own machines; sacrificial lambs
  - Different teams using different tool sets – remove PSEXEC, WMI, PowerShell; your management tools that are used against you

~ **Scope:** Create scope creep utilizing deception with fake targets or tarpits

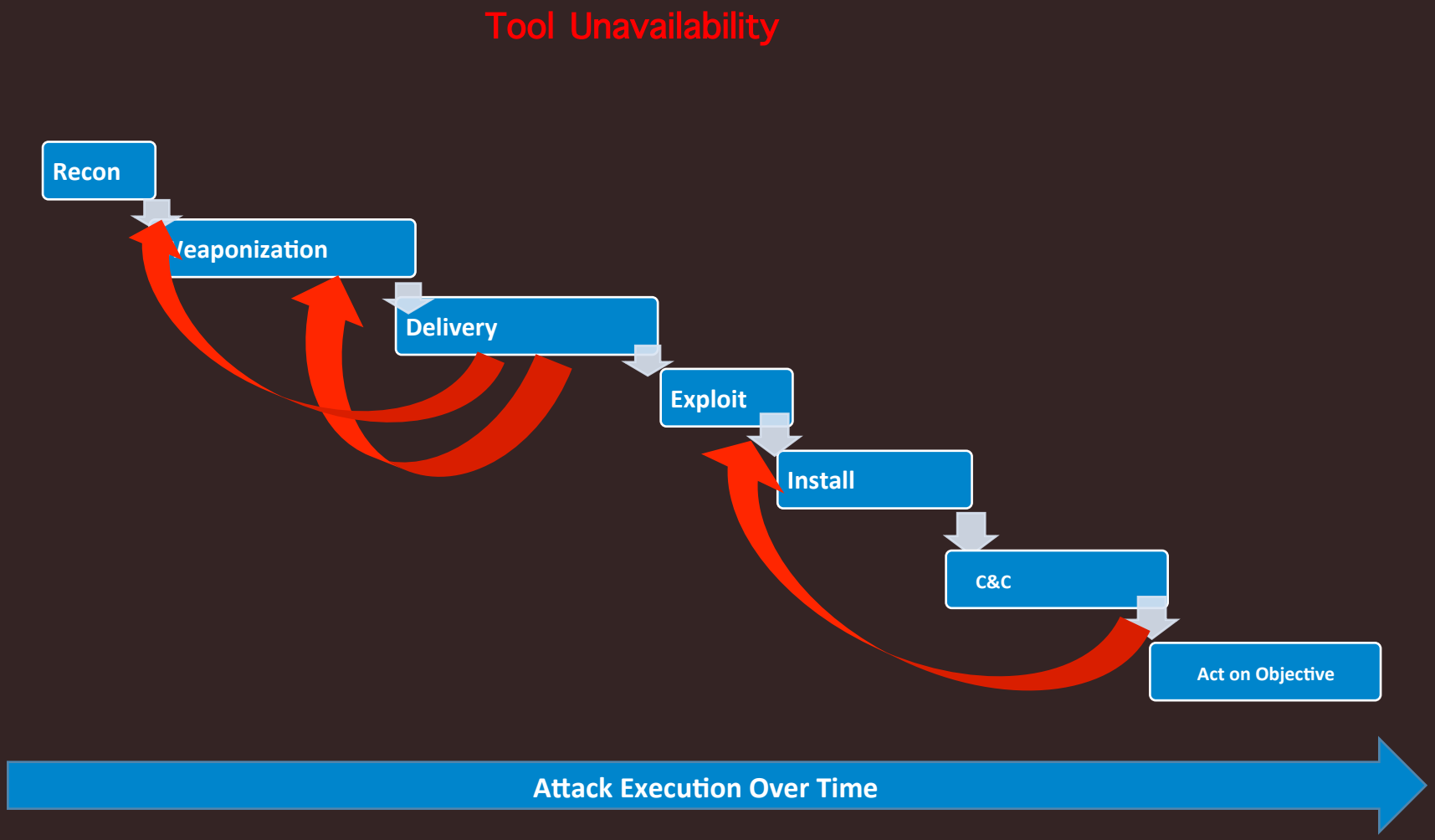
~ **Cost:** Increase costs by setting the attacker back in progression increases cost to them thereby decreasing cost to defender to remediate

~ **Quality:** Create noise and anomalies – attackers, automation and scripts are disrupted

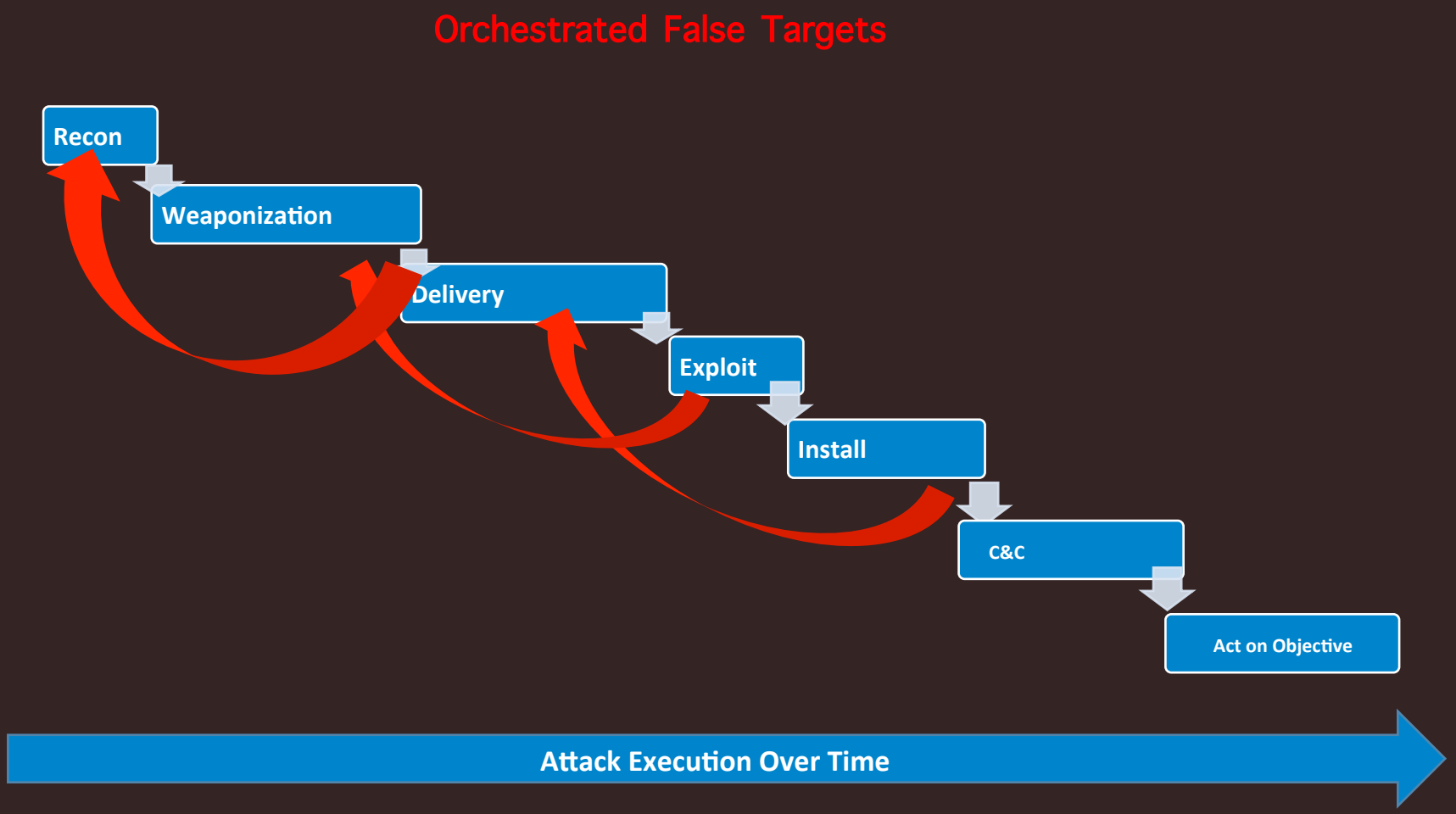
$ tortuosa concept – attacking attacker's plan



$ tortuosa concept – attacking attacker's plan



$ tortuosa concept – attacking attacker's plan



$ 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:

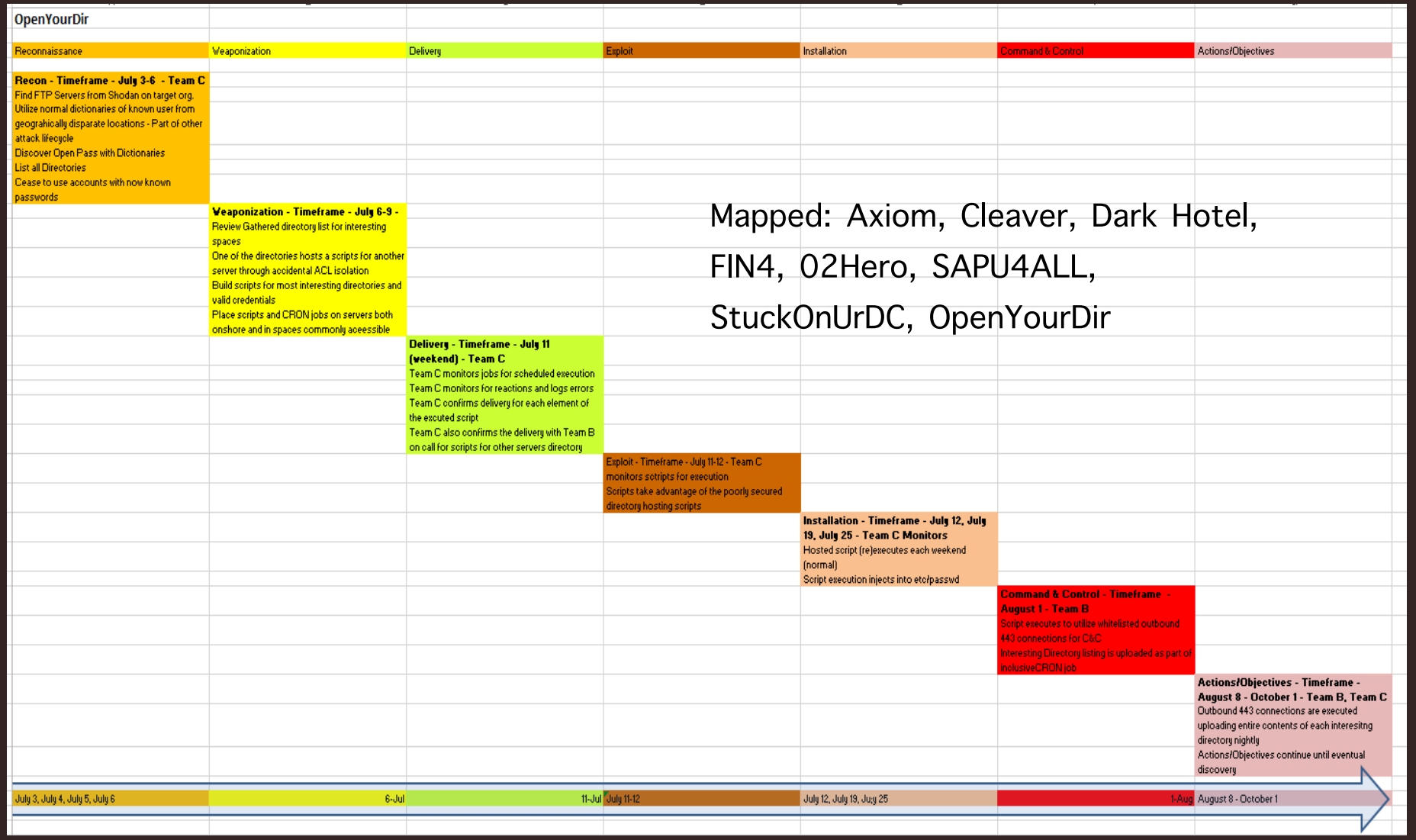
- Assumed Linear Timeline Disruptions
- Resource/Tool - Contention/Unavailability
- Scope Creep - Scope Expansion - Adversary Target Deception
- Fight Organization - Chaotic Randomness
- Predecessors, Successor
- Disrupt Deliverables

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

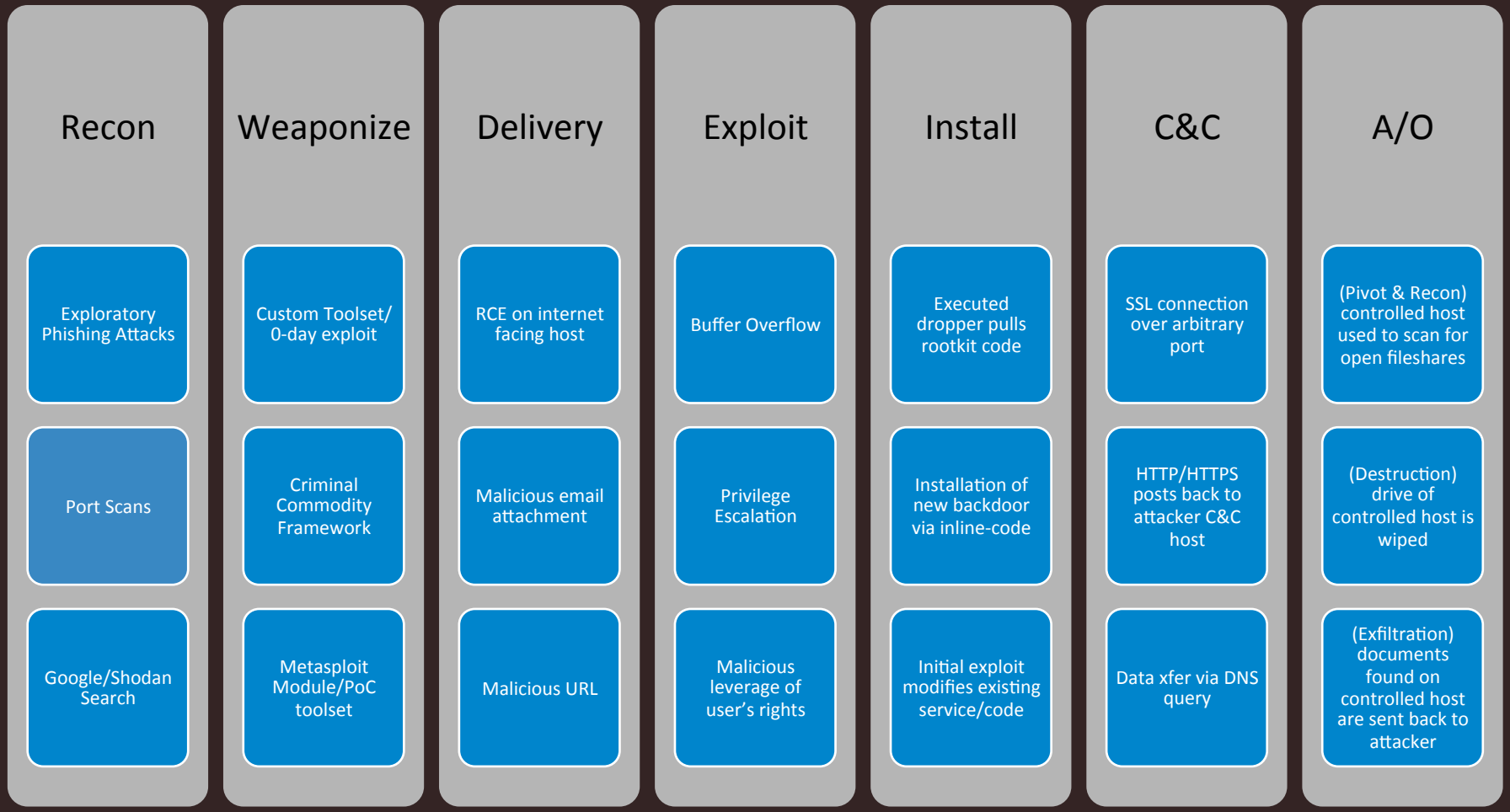
***https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

$ tortuosa concept – attacking attacker's plan

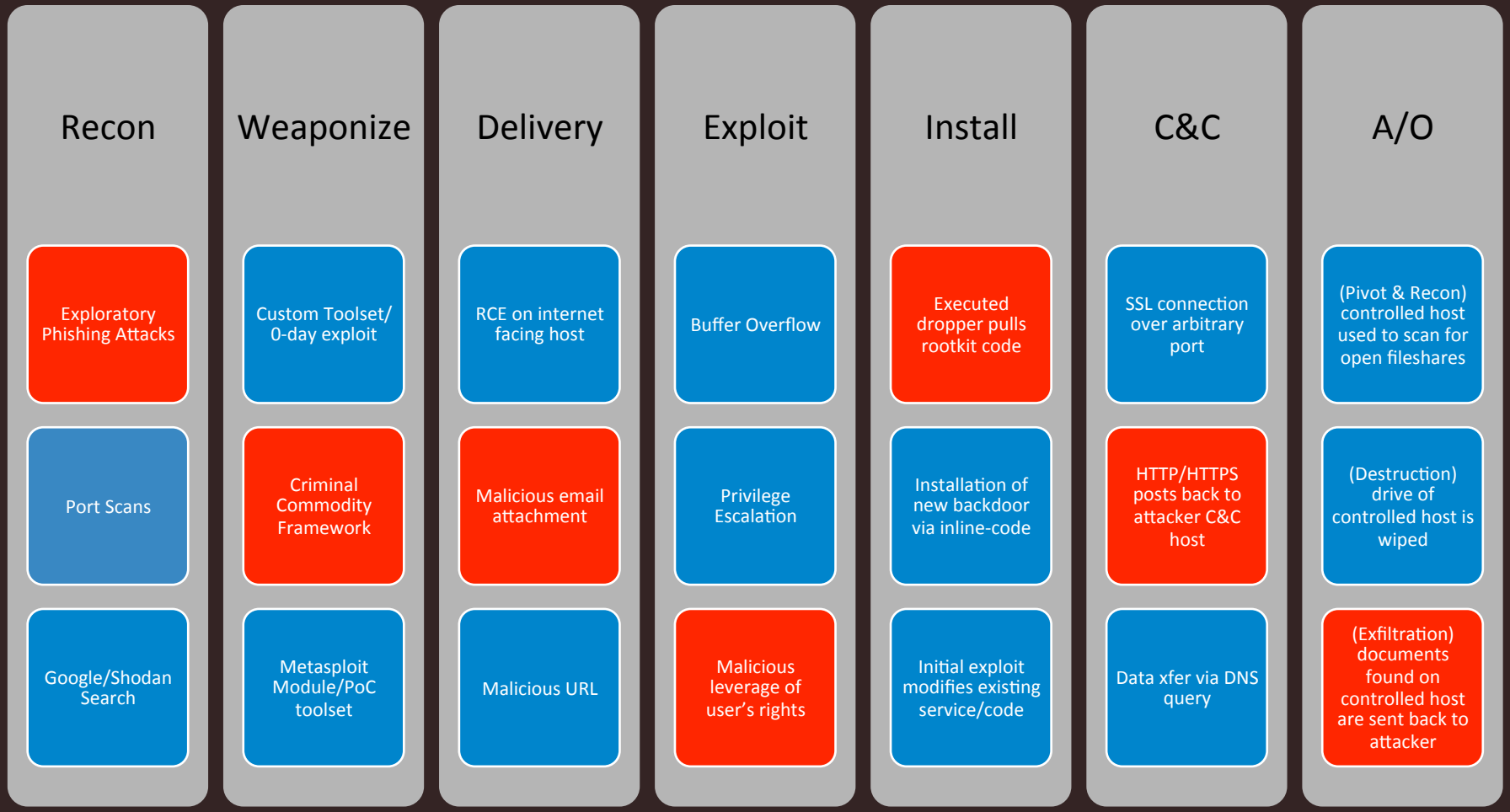


Mapped: Axiom, Cleaver, Dark Hotel, FIN4, 02Hero, SAPU4ALL, StuckOnUrDC, OpenYourDir

$ let's build a catalog of attack patterns



$ let's build a catalog of attack patterns



$ research based attack catalog techniques

~ MITRE's CAPEC (Common Attack Patterns and Enumeration Catalogue)



- 500+ techniques
- Slightly unmanageable for my needs

~ MITRE's ATT&CK Framework (Adversarial Tactics, Techniques & Common Knowledge)

- 68 techniques!
- More manageable
- Attack lifecycle map
- Win!



$ building the attacker deck

Build catalog of attack patterns – MITRE ATT&CK Framework – 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 - 8-2015

$ building the attacker deck

Build catalog of attack patterns – MITRE ATT&CK Framework – 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 - 8-2015

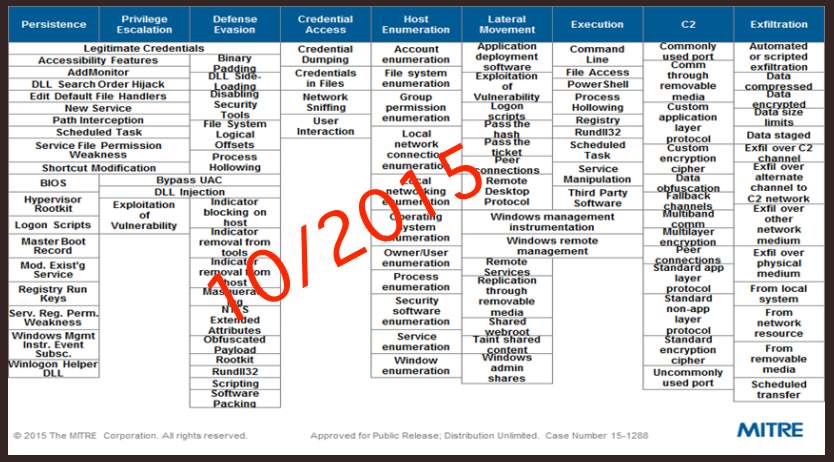
$ building the attacker deck

Build catalog of attack patterns – Updated 7/28/2016 ***



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 load	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				

2/2015



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

© 2015 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case Number 15-1288 MITRE

10/2015



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Change Default File Association	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Rundll32	Man in the Browser	Scheduled Transfer	Multiband Communication
Local Port Monitor	Path Interception	File Deletion		Query Registry	Shared Webroot	Scheduled Task	Screen Capture		Multilayer Encryption
Logon Scripts	Scheduled Task	File System Logical Offsets		Remote System Discovery	Taint Shared Content	Scripting	Video Capture		Remote File Copy
Modify Existing Service	Service File Permissions Weakness	Indicator Blocking		Security Software Discovery	Third-party Software	Service Execution			Standard Application Layer Protocol
New Service	Service Registry Permissions Weakness	Indicator Removal from Tools		System Information Discovery	Windows Admin Shares	Third-party Software			Standard Cryptographic Protocol
Path Interception	Web Shell	Indicator Removal on Host		System Owner/User Discovery	Windows Remote Management	Windows Management Instrumentation			Standard Non-Application Layer Protocol
Redundant Access		InstallUtil		System Service Discovery		Windows Remote Management			Uncommonly Used Port
Registry Run Keys / Start Folder		Legitimate Credentials							Web Service
Scheduled Task		Masquerading							
Security Support Provider		Modify Registry							
Service File Permissions Weakness		NTFS Extended Attributes							
Service Registry Permissions Weakness		Obfuscated Files or Information							
Shortcut Modification		Process Hollowing							
Web Shell		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

7/28/2016

***https://attack.mitre.org/wiki/Main_Page - 1-2015, 10-2015, 7/28/2016

$ building the attacker deck

v·d·e	Adversary Techniques
Persistence	Winlogon Helper DLL · Local Port Monitor · Accessibility Features · Basic Input/Output System · Shortcut Modification · Modify Existing Service · Path Interception · Logon Scripts · DLL Search Order Hijacking · Change Default File Association · Service File Permissions Weakness · **New Service** · Scheduled Task · Service Registry Permissions Weakness · Registry Run Keys / Start Folder · Hypervisor · Bootkit · Legitimate Credentials · Windows Management Instrumentation Event Subscription · Web Shell · Security Support Provider · AppInit DLLs · Redundant Access · Component Firmware
Privilege Escalation	Local Port Monitor · Accessibility Features · Path Interception · DLL Search Order Hijacking · Service File Permissions Weakness · **New Service** · Scheduled Task · DLL Injection · Service Registry Permissions Weakness · Exploitation of Vulnerability · Legitimate Credentials · Bypass User Account Control · Web Shell · AppInit DLLs
Credential Access	Credential Dumping · Network Sniffing · Input Capture · Exploitation of Vulnerability · Credentials in Files · Credential Manipulation · Brute Force · Two-Factor Authentication Interception
Discovery	System Service Discovery · Application Window Discovery · Query Registry · Local Network Configuration Discovery · Remote System Discovery · System Owner/User Discovery · Network Service Scanning · Local Network Connections Discovery · Process Discovery · Security Software Discovery · Permission Groups Discovery · System Information Discovery · File and Directory Discovery · Account Discovery · Peripheral Device Discovery
Defense Evasion	File System Logical Offsets · Binary Padding · Rootkit · Obfuscated Files or Information · Masquerading · DLL Search Order Hijacking · Software Packing · Indicator Blocking · DLL Injection · Scripting · Indicator Removal from Tools · Exploitation of Vulnerability · Indicator Removal on Host · DLL Side-Loading · Legitimate Credentials · Rundll32 · Bypass User Account Control · Disabling Security Tools · Process Hollowing · NTFS Extended Attributes · Timestomp · File Deletion · Redundant Access · Component Firmware · Modify Registry · Code Signing · Regsvr32 · InstallUtil · Regsvcs/Regasm
Lateral Movement	Application Deployment Software · Remote Services · Windows Remote Management · Logon Scripts · Shared Webroot · Exploitation of Vulnerability · Third-party Software · Pass the Hash · Remote Desktop Protocol · Windows Admin Shares · Taint Shared Content · Replication Through Removable Media · Pass the Ticket · Remote File Copy
Execution	Windows Remote Management · Service Execution · Windows Management Instrumentation · Scheduled Task · Command-Line Interface · Graphical User Interface · Scripting · Third-party Software · Rundll32 · PowerShell · Process Hollowing · Execution through API · Regsvr32 · InstallUtil · Regsvcs/Regasm
Collection	Data from Local System · Data from Removable Media · Data from Network Shared Drive · Input Capture · Data Staged · Screen Capture · Email Collection · Clipboard Data · Automated Collection
Exfiltration	Data Compressed · Exfiltration Over Other Network Medium · Automated Exfiltration · Data Encrypted · Scheduled Transfer · Data Transfer Size Limits · Exfiltration Over Command and Control Channel · Exfiltration Over Alternative Protocol · Exfiltration Over Physical Medium
Command and Control	Data Obfuscation · Fallback Channels · Custom Cryptographic Protocol · Multiband Communication · Standard Cryptographic Protocol · Commonly Used Port · Uncommonly Used Port · Standard Application Layer Protocol · Multilayer Encryption · Connection Proxy · Communication Through Removable Media · Custom Command and Control Protocol · Standard Non-Application Layer Protocol · Web Service · Multi-Stage Channels · Remote File Copy

Categories: Persistence | Privilege Escalation | Technique

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

$ 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.

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

$ tortuosa concept – attacking attacker's plan

Noticed something more…

Got an Attacker Deck

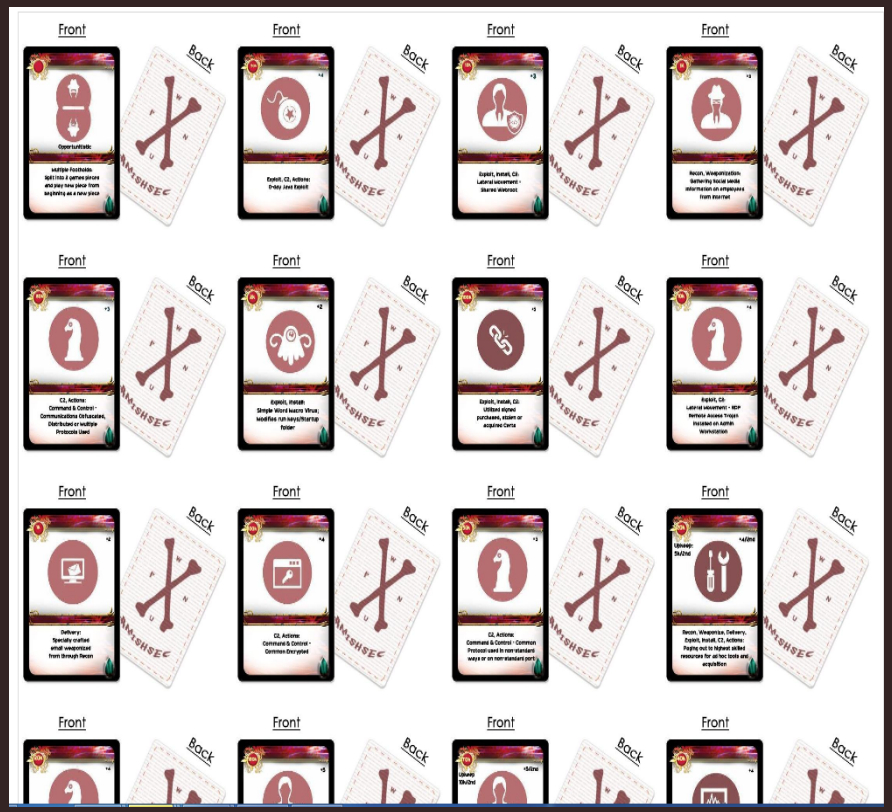
Got a Defender Deck

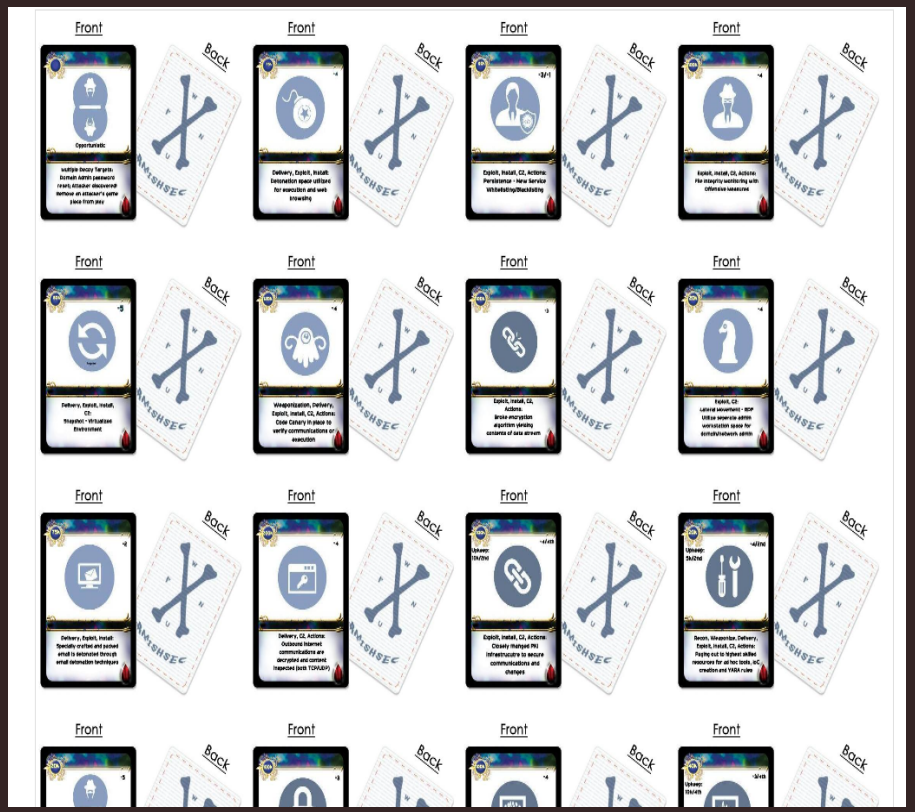
Got a Progressive Board

…maybe a game?

$ maelstrom – are you playing with a full deck?

Game Mock Up – Attacker Red Deck – Defender Blue Deck





$ maelstrom – are you playing with a full deck?

Game Board – Give and take between attacker and defender



$ maelstrom – are you playing with a full deck?

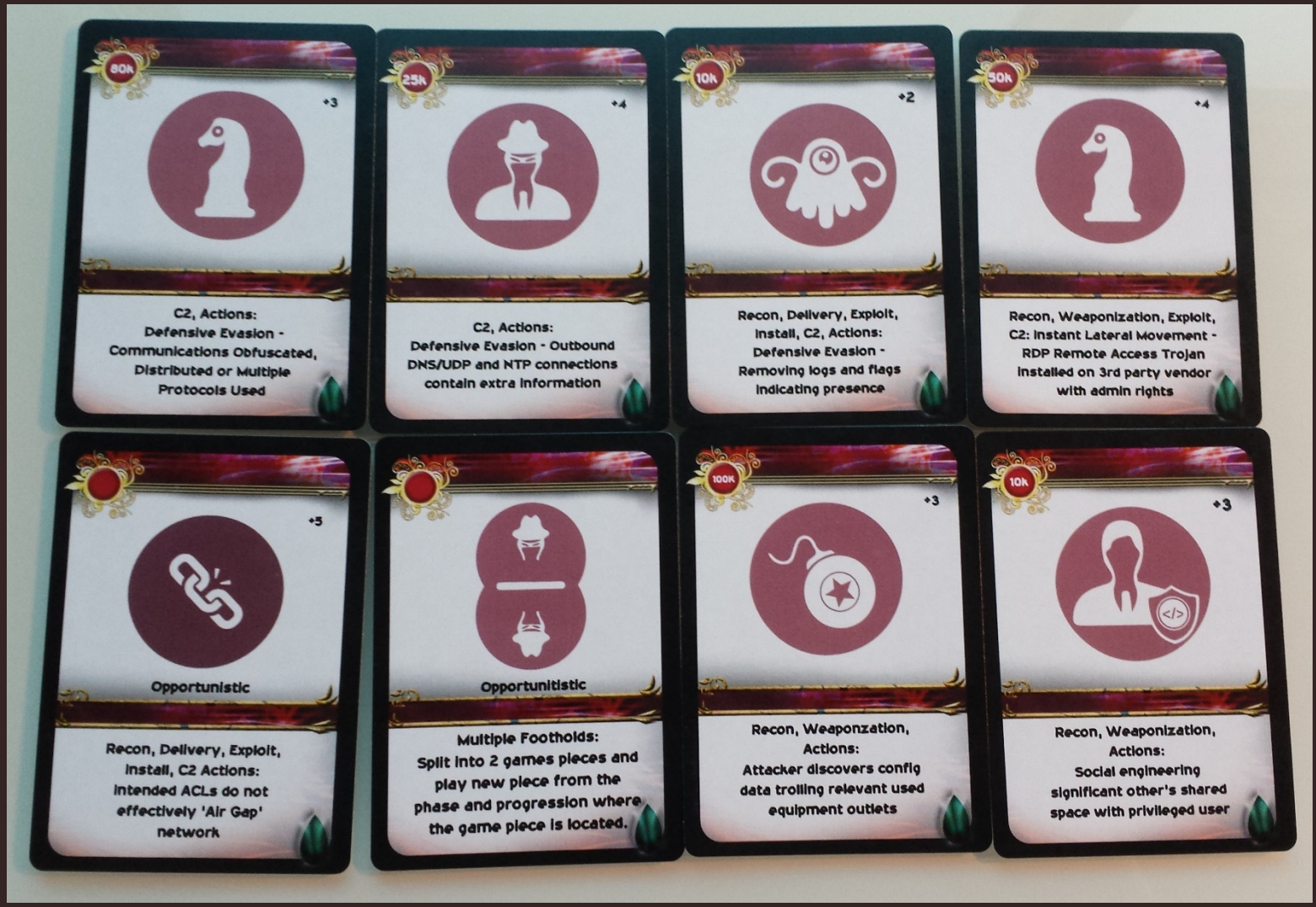
Card Anatomy – Progression, Cost, Upkeep, Usage – Build a Story





$ maelstrom – are you playing with a full deck?

60+ unique attacker cards



$ maelstrom – are you playing with a full deck?

70+ unique defender cards



$ maelstrom – actor game pieces

12 unique threat actor chips – face down



$ maelstrom – act on objective cards

11 unique act on objectives – face down in middle



$ maelstrom – methods of play

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

Rules located here…

github.com/maelstromthegame/defcon24

$ maelstrom – is it playable?

game board mockup – game play – yeah its playable!!!



sample video of game play - https://vimeo.com/177304576

$ maelstrom – are you playing with a full deck?

Use Cases

~ Education

- Learn an attack lifecycle 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…

~ **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, Game of PWNs, Breaches, 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?

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!

~ twitter.com/cybermaelstrom
~ github.com/maelstromthegame/defcon24
~ to print your copy of the game – coming very soon
  - cards, poker chips – watch twitter for vendor information (working on getting a sku with the vendor to print)
  - game board – download the file from github above and print at FedEx or through vendor
~ 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

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

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

~Lockheed Martin – Cyber Kill Chain ®
- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

~ Gerard Laygui

~ Garrett Adler

~ Collin Frietzsche

~ Brent Thibodo

~ Jerry Decime

~ Cale Smith

~ Tom Van Setten

~ George Mckee

~ Logan Browne

~ Darlene Leong

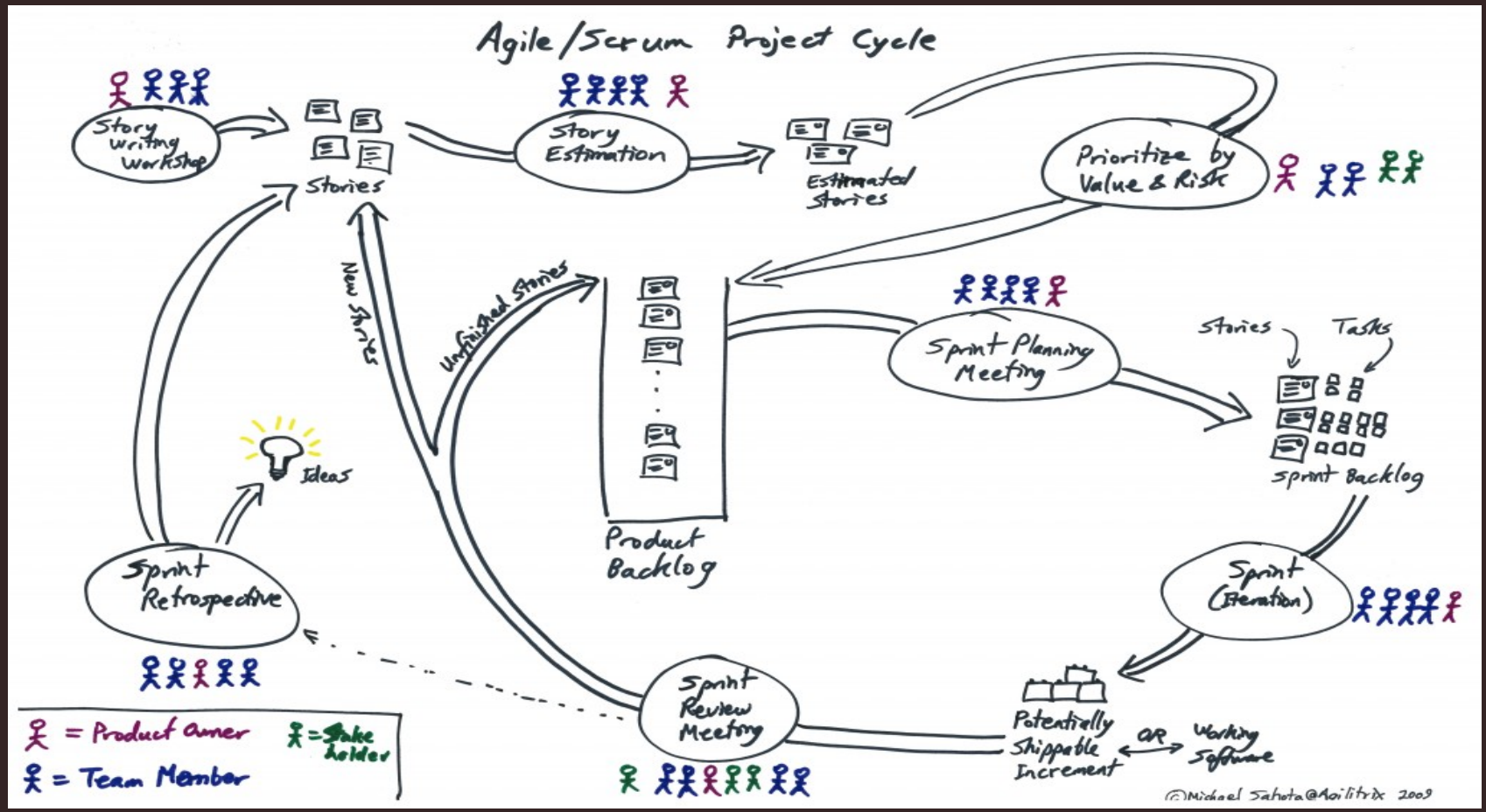
~ JR

$ questions?

$ backup slides if anyone goes there

$ tortuosa concept – attacking attacker's plan

~…so agile you say



$ tortuosa concept – attacking attacker's 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)

$ 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