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



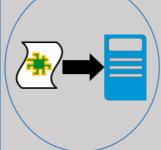
Reconnaissance

- 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



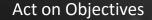
Installation

• Payload is executed



Command and Control

 Communication and control is established between attacker and target





Recon/Pivot



Destruction



\$ Lockheed Martin Kill Chain Phases ™ *misnomer

Act on Objectives



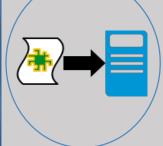
Reconnaissance

- 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



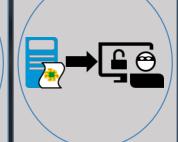
Exploitation

 Exploit is triggered on target



Installation

Payload is executed



Command and Control

 Communication and control is established between attacker and target







Humiliate



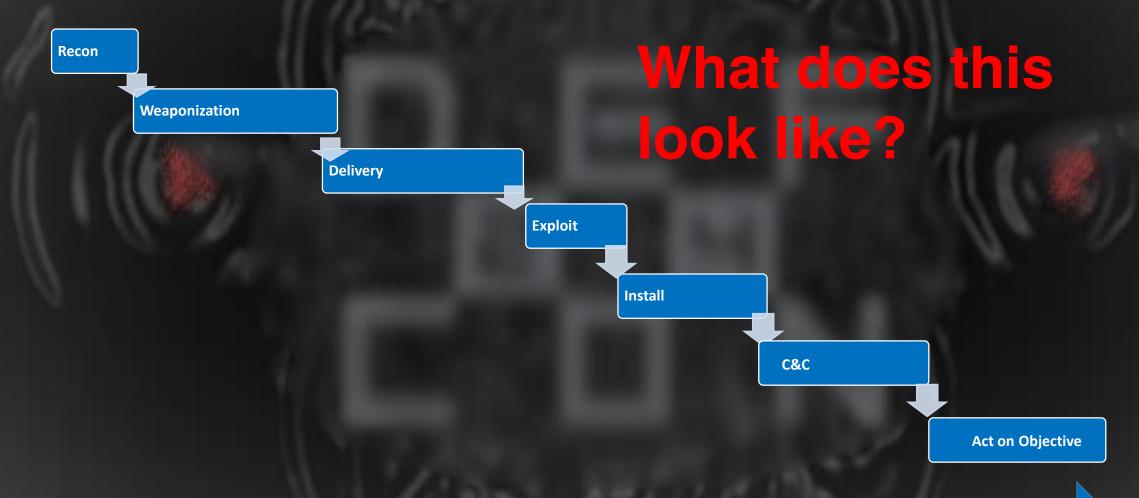
Recon/Pivot





*defender is the actor in a kill chain!

\$ tortuosa concept—charting attacker's progression



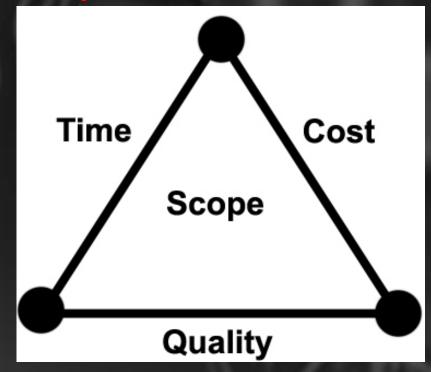
\$ tortuosa concept — attacking the attacker's plan

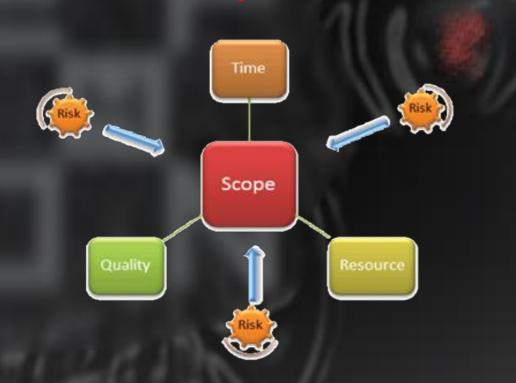
- ~what does this look like?
 - Looks like a Gantt Chart! A project plan!
 - Attackers are organized indicating plan progression for campaigns
- ~what other evidence have we seen to indicate the attackers seem to follow a plan if not a traditional project plan?
 - Different time schedules indicating '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.



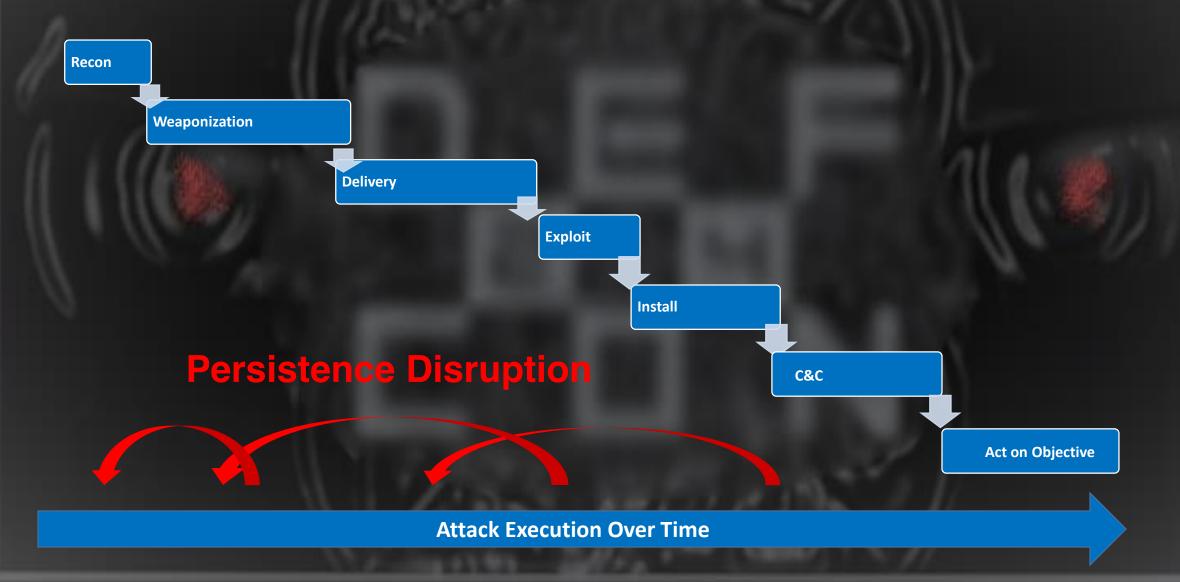


\$ tortuosa concept – attacking attacker's plan

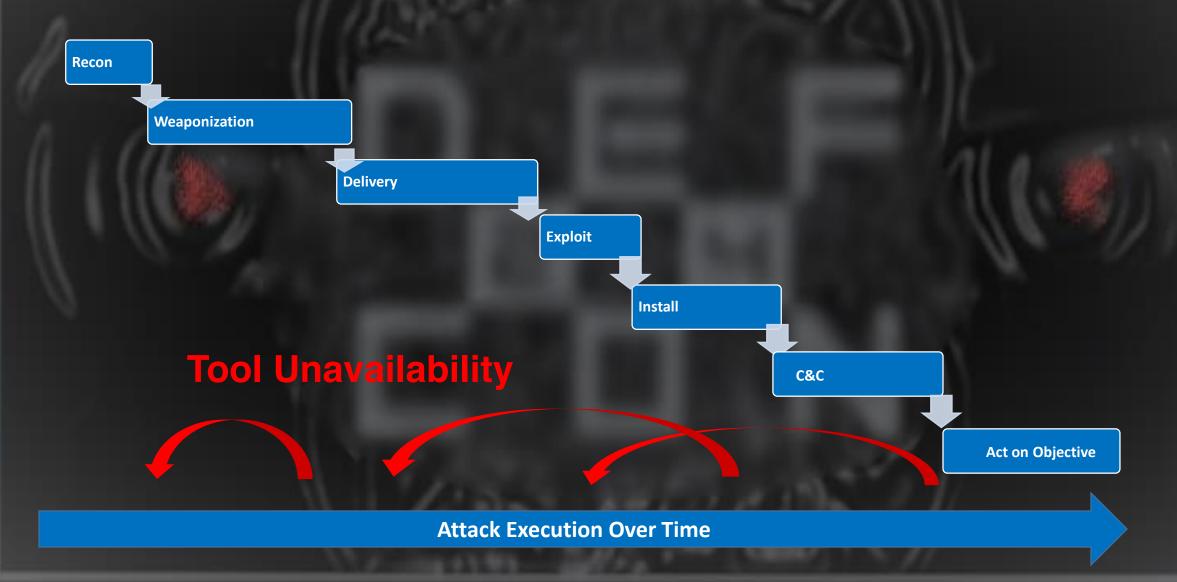
What can we do to disrupt the attacker's project plan?

- ~ 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

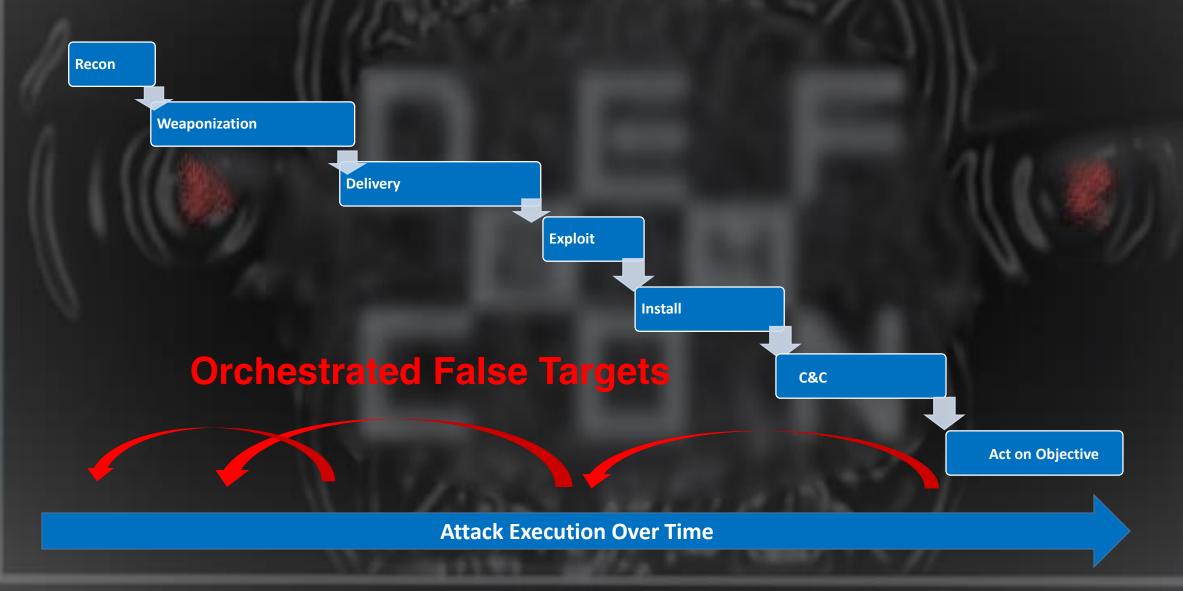
\$ tortuosa concept – charting attacker progression



\$ tortuosa concept – charting attacker progression



\$ tortuosa concept – charting attacker progression



\$ tortuosa concept – attacking attacker's plan

- 4	A	В	L		U				
1	Reconnaissance	Weaponization	Delivery	Exploit			Inst		
2					Targets:				
3	Reconnaissance						line Disrupti		
4	List Timeframe, Successor	/Predecessor			_		ention/Unav		Target Deception
5	List Resource(s), Tools				-		haotic Rand	-	raiget Deception
Č	List Tasks in Timeframe					ors, Success		011111033	Cyber
Ь	List rasks iii riiiieiraiiie	Mananination				eliverables		Resilie	ncy Techniques
7		Weaponization	'		-			Adap	otive Response
8		List Timeframe, Successor/	/Predecessor				- 000	Analy	rtic Monitoring
9		List Resource(s), Tools					- 800	Coord	linated Defense
10		List Tasks in Timeframe							Deception
11			Delivery					17	Diversity
12			List Timeframe, Successor/F	redecesso	or				mic Positioning
13			List Resource(s), Tools						ic Representation
14			List Tasks in Timeframe					Noi	n-Persistence
15				Exploit				Privil	ege Restriction
16				List Time	frame, Su	ccessor/F	red	R	ealignment
17				List Reso	urce(s), To	ools		R	edundancy
18				List Tasks	s in Timefi	rame		Se	gmentation
h			100 July 2017 4 17	100	770.	- 41	la et	Substa	ntiated Integrity
	***https://www.n	nitre.org/publications/	technical-papers/cyber-	resilienc	y-engine	ering-fr	amewor	k Uni	predictability

\$ tortuosa concept – attacking attacker's plan

OpenYourDir						
Reconnaissance	Weaponization	Delivery	Exploit	Installation	Command & Control	Actions/Objectives
Daniel Timefrance Into 0.0 Table 0.0						
Recon - Timeframe - July 3-6 - Team C Find FTP Servers from Shodan on target org.	<u></u>					
Utilize normal dictionaries of known user from						
geographically disparate locations - Part of other						
attack lifecycle						
Discover Open Pass with Dictionaries			NAOR	nod: Avia	m Cloove	or Dork
List all Directories	<u></u>		IVIAL	ped: Axio	III. Cleave	a. Daik
Cease to use accounts with now known passwords					,	, <u> </u>
passwords	Veaponization - Timeframe - July 6-9 -					
	Review Gathered directory list for interesting		Hote	SI LINIA N	17Hara	
	spaces			el, FIN4, 0	ZIICIU.	
	One of the directories hosts a scripts for another			, · ·	· ·	
	server through accidental ACL isolation		_ ^ ^ =			
	Build scripts for most interesting directories and valid credentials		$oxed{\Box}$	U4ALL, S	iturk()nl li	/I)(
	Place scripts and CRON jobs on servers both			UHALL, C	luckOnoi	
	onshore and in spaces commonly accessible			, -		
		Delivery - Timeframe - July 11				
		(weekend) - Team C				
		Team C monitors jobs for scheduled execution				
		Team C monitors for reactions and logs errors				
		Team C confirms delivery for each element of				
		the excuted script Team C also confirms the delivery with Team B				
		on call for scripts for other servers directory				
		,	Exploit - Timeframe - July 11-12 - Team C			
			monitors setripts for execution			
			Scripts take advantage of the poorly secured			
			directory hosting scripts			
				Installation - Timeframe - July 12, July 19, July 25 - Team C Monitors		
				Hosted script (re)executes each weekend		
				(normal)		
				Script execution injects into etc/passwd		
					Command & Control - Timeframe -	
					August 1 - Team B	
					Script executes to utilize whitelisted outbound	
					443 connections for C&C Interesting Directory listing is uploaded as part of	
					interesting Directory listing is uploaded as part or inclusiveCRON job	
						Actions/Objectives - Timeframe -
						August 8 - October 1 - Team B, Team C
						Outbound 443 connections are executed
						uploading entire contents of each interesiting
						directory nightly
						Actions/Objectives continue until eventual discovery
						and the same of th
July 3, July 4, July 5, July 6	6-Jul	11-Jul	July 11-12	July 12, July 19, Ju;y 25	1-Aug	August 8 - October 1
						V

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

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

\$ build catalog of attack patterns — light 'em up

Weaponize Delivery Exploit C&C Recon Install RCE on internet Custom Toolset/0-**Executed dropper Exploratory Buffer Overflow** Phishing Attacks day exploit facing host pulls rootkit code

Port Scans

Google/Shodan

Search

Metasploit Module/PoC toolset

Criminal

Commodity

Framework

Malicious URL

Malicious email

attachment

Privilege **Escalation**

Malicious leverage of user's rights

Installation of new backdoor via inline-code

Initial exploit modifies existing service/code

SSL connection over arbitrary port

HTTP/HTTPS posts back to attacker C&C host

Data xfer via DNS query

A/O

(Pivot & Recon) controlled host used to scan for open fileshares

(Destruction) drive of controlled host is wiped

(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
reisistence	Trivinege Escalation	Creacitial Access	1103t Enameration	Defense Evasion	Euteral Wovellient	command and control	Extitution
		OS/Software		Software			
New service	Exploitation of vulnerability	Weakness	Process enumeration	packing	RDP	Common protocol, follows standard	Normal C&C channel
				pg	1121	,	
	Service file permissions						
Modify existing service	weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C\$, ADMIN\$)	Common protocol, non-standard	Alternate data channel
					, , ,	•	
	Service registry permissions					Commonly used protocol on non-	Exfiltration over other network
DLL Proxying	weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	standard port	medium
			Local network				Exfiltration over physical
Hypervisor Rookit	DLL path hijacking	Stored file	connections	DLL loading	Remote vulnerability	Communications encrypted	medium
				Standard			
Winlogon Helper DLL	Path interception		Window enumeration	protocols	Logon scripts	Communications are obfuscated	Encrypted separately
				016			
Dath Interception	Modification of shortcuts		A	Obfuscated	Application deplement astronom	Distributed communications	Communicated communicated
Path Interception	iviodification of shortcuts		Account enumeration	payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys /				Indicator			
Startup folder addition	Editing of default handlers		Group enumeration	removal	Taint shared content	Multiple protocols combined	Data staged
				Indicator	Access to remote services with valid		Automated or scripted data
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration	blocking	credentials		exfiltration
			Operating system				
MBR / BIOS rootkit			enumeration		Pass the hash		Size limits
- 1101 - 6 1 6 5							
Editing of default			Security software				Cab a dada dawa wafa
handlers			enumeration				Scheduled transfer
AT / Schtocks / Cross			Eilo system enumeration				
AT / Schtasks / Cron			File system enumeration				

\$ 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				

\$ 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
	gitimate Credentia ty Features onitor Order Hijack File Handlers ervice erception ed Task Permission mess lodification Bypas DLL In Exploitation of Vulnerability	als Binary Padding DLL Side- Loading Disabling Security Tools File System Logical Offsets Process Hollowing	Credential Dumping Credentials in Files Network Sniffing User Interaction	Account enumeration File system enumeration Group permission enumeration Local network connection enumeration Local networking enumeration Operating system enumeration Owner/User enumeration Process enumeration Security software enumeration Service enumeration Window enumeration	Application deployment software Exploitation of Vulnerability Logon scripts Pass the hash Pass the ticket Peer connections Remote Desktop Protocol	Command Line File Access PowerShell Process Hollowing Registry Rundll32 Scheduled Task Service Manipulation Third Party Software nanagement entation s remote	Commonly used port Comm through removable media Custom application layer protocol Custom encryption cipher Data obfuscation Fallback channels Multilayer encryption Peer Connections Standard app layer protocol Standard non-app layer protocol Standard encryption cipher Uncommonly used port	Automated or scripted exfiltration Data compressed Data encrypted Data size limits Data staged Exfil over C2 channel Exfil over alternate channel to C2 network Exfil over network medium Exfil over physical medium From local system From network resource From removable media
		Software Packing					useu port	Scheduled transfer

MITRE

\$ do they win - building the defender deck Defensive Strategies to Each ATT&CK Technique -Complimentary Cards

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

П			
2	Fight Persistence!		
9	Time Disruptions		
ı	Intro Scope Creep		
5	Increase Cost		
5	Fight Oranization		
7	Eviscerate Quality/Intro Friction		
3		New Services	
9		Whitelisting	
0		Blacklisting	
1		Service Start Failures/Dependancies	
2		Snapshotting	
3		Stop all Services, Start all Services	
4		3rd party certs for start*?	
5		Modify Existing Services	
6		Dependacies for Modifications	
7		Whitelisting Modifications Settings*?	
8		Blacklisting Modifcation Settings*?	
9		Disposable Services*?	
0		Snapshotting	
1		DLL Proxying*?	
2		Lookup Friction	
3		Snapshotting	
4		Disposable DLLs*?	
5		Whitelisting*?	
6		BlackListing*?	
7		Hypervisor Rootkit	
8		Host Profile	
9		Whitelisting	
0		Blacklisting	

\$ 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/

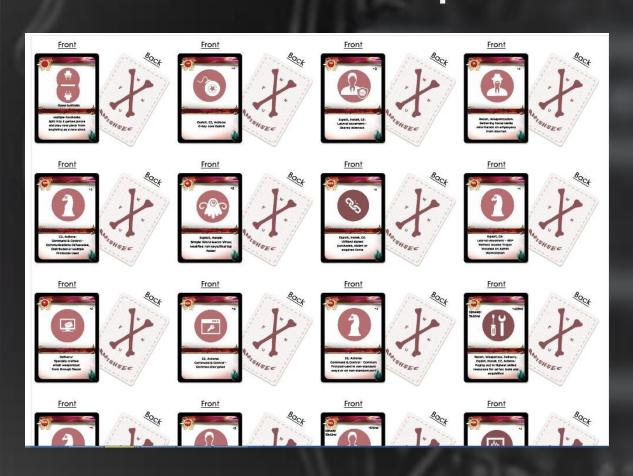
\$ tortuosa concept – attacking attackers' plan

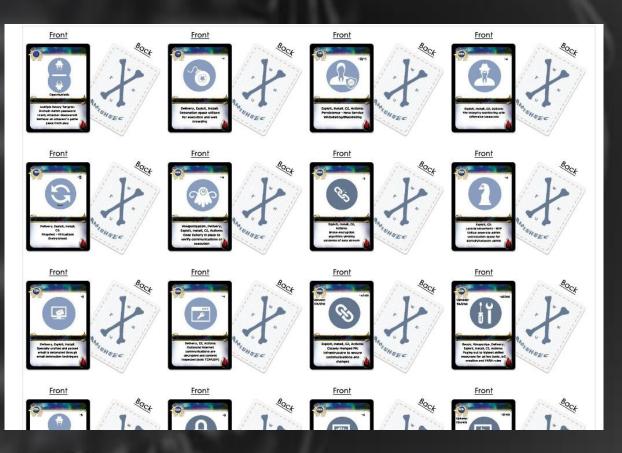
Noticed something more...

~maybe a game?

Got an Attacker Deck
Got a Defender Deck
Got a Progressive Board with Lockheed
Martin Attack Lifecycle

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





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

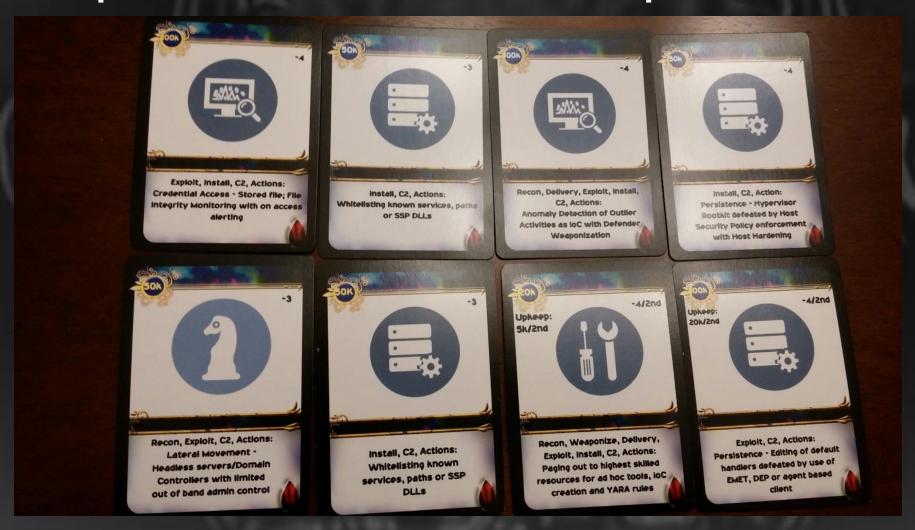




\$ maelstrom — are you playing with a full deck? 60+ unique attacker cards and 70+ unique defender cards



60+ unique attacker cards and 70+ unique defender cards



12 unique threat actor chips – face down



11 unique act on objectives – face down in middle



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

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





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

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/cyberse curity/resiliency
 - http://www2.mitre.org/public/industryperspective/
- ~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-pressoffice/2013/02/12/presidential-policy-directive-criticalinfrastructure-security-and-resil
- [3] http://www.whitehouse.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity
- [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] <u>https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ScotlandNCSS.pdf</u>
- [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/

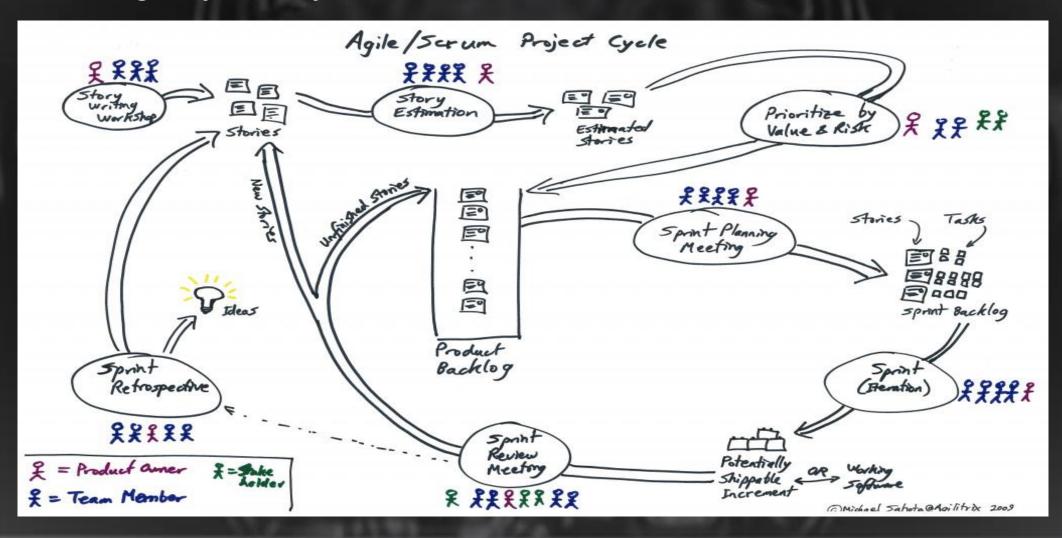
- [12] http://www2.mitre.org/public/industry-perspective/index.html
- [13] http://www2.mitre.org/public/industry-perspective/guidance-executives.html
- [14] http://www2.mitre.org/public/industry-perspective/guidancearchitects.html
- [15] http://www2.mitre.org/public/industryperspective/slicksheets/disrupting_the_attack_surface.html
- [16] http://csrc.nist.gov/publications/drafts/800-160/sp800 160 draft.pdf
- [17] <u>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf</u>
- [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



\$ 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)