Maelstrom: Are you playing with a full deck?

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

Shane Steiger, Esq. CISSP

© 2016

DEF CON 24  #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

~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

Exfiltration

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!*

$ tortuosa concept–charting attacker’s progression

Recon
Weaponization
Delivery
Exploit
Install
C&C
Act on Objective

Attack Execution Over Time

What does this look like?
$ 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.

[Diagram showing the Project Management Triangle](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

Persistence Disruption

Attack Execution Over Time
$ tortuosa concept – charting attacker progression

Recon → Weaponization → Delivery → Exploit → Install → C&C → Act on Objective

Tool Unavailability

Attack Execution Over Time
$ tortuosa concept – charting attacker progression

Recon

Weaponization

Delivery

Exploit

Install

C&C

Act on Objective

Orchestrated False Targets

Attack Execution Over Time
$ tortuosa concept – attacking attacker’s plan

<table>
<thead>
<tr>
<th>Reconnaissance</th>
<th>Weaponization</th>
<th>Delivery</th>
<th>Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>List Timeframe, Successor/Predecessor</td>
<td>List Resource(s), Tools</td>
<td>List Tasks in Timeframe</td>
<td></td>
</tr>
</tbody>
</table>

**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/Predecessor
- List Resource(s), Tools
- List Tasks in Timeframe

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

***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

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

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

### Build Catalog of Attack Patterns – 8/2015

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

***[https://attack.mitre.org/wiki/Main_Page](https://attack.mitre.org/wiki/Main_Page)***
$ building the attacker deck
Build catalog of attack patterns – 8/2015

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

***https://attack.mitre.org/wiki/Main_Page***
### Building the Attacker Deck

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

<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Host Enumeration</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>C2</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Legitimate Credentials</td>
<td>Binary Padding</td>
<td>Credential Dumping</td>
<td>Account enumeration</td>
<td>Application deployment</td>
<td>Command Line</td>
<td>Commonly used port</td>
<td>Automated or scripted exfiltration</td>
</tr>
<tr>
<td>Accessibility Features</td>
<td>AddMonitor</td>
<td>DLL Side-Loading</td>
<td>Credentials in Files</td>
<td>File system enumeration</td>
<td>Exploitation of Vulnerability</td>
<td>File Access</td>
<td>Compressed data</td>
<td>Data compressed</td>
</tr>
<tr>
<td>DLL Search Order Hijack</td>
<td>New Service</td>
<td>Security Tools</td>
<td>Group permission enumeration</td>
<td>Group membership</td>
<td>Logon scripts</td>
<td>PowerShell</td>
<td>Encrypted data size limits</td>
<td>Data encrypted</td>
</tr>
<tr>
<td>Patch Interception</td>
<td>Scheduled Task</td>
<td>File System Logical Offsets</td>
<td>User Interaction</td>
<td>User Interaction</td>
<td>Pass the Hash</td>
<td>Process Hollowing</td>
<td>Data staged</td>
<td>Data staged</td>
</tr>
<tr>
<td>Service File Permission Weakness</td>
<td>BIOS</td>
<td>Process Hollowing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shortcut Modification</td>
<td>Hypervisor Rootkit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>=&gt; Exploitation of Vulnerability</td>
<td>DLL Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

---

[https://attack.mitre.org/wiki/Main_Page](https://attack.mitre.org/wiki/Main_Page)
$ do they win - building the defender deck

Defensive Strategies to Each ATT&CK Technique – Complimentary Cards

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

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

Front

Recon, Exploit, C2, Actions:
Lateral Movement - Application Deployment Software

Back

Upkeep: 3k/2nd

Front

Recon, Weaponize, Delivery, Exploit, install, C2, Actions:
Paging out to highest skilled resources for ad hoc tools, iOC creation and YARA rules

Back

Upkeep: -4/2nd
$ 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

$ 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)