Cyber Kill Chain Methodology

Brian Wrozek, Managing Executive Director
Agenda

Threat Strategy
Use Cases
Final Thoughts

Kill Chain Components
Cautionary Notes
Threat Strategy
Security Strategy Development

- Research
  - New Threat Landscape
  - Compliance Requirements
  - External Factors

- Collaboration
  - New Business Priorities
  - New IT Priorities
  - Internal Factors

- Assessments
  - Program Improvements
  - Portfolio Gaps
  - Self-guided Factors

- Analysis and Planning
  - New Priorities
  - Updated Strategy
Threat Strategy Methodology

1. Determine Assets
2. Understand Actors & Vectors
3. Develop Threat Model
4. Counter-measure mapping
5. Positioning
6. Monitor and Repeat

Kill Chain
Kill Chain Components
F2T2EA Kill Chain

- **Find:** Locate the target
- **Fix:** Fix their location, make it difficult for them to move
- **Track:** Monitor their movement
- **Target:** Select an appropriate weapon or asset to use on the target to create desired effects
- **Engage:** Apply the weapon to the target
- **Assess:** Evaluate effects of the attack, including any intelligence gathered at the location

http://www.military-dictionary.org/F2T2EA
Traditional Kill Chain Model

Gather data and intelligence on target organization
Craft malicious payload, use exploits for vulnerabilities
Payload sent to target (phishing)
Compromise system
Install malware, obtain credentials and establish backdoors.
Navigate internal network and setup command and control
Ultimate goals achieved

[Diagram of the Kill Chain Model with stages: Recon, Weaponize, Deliver, Exploit, Install, C2, Actions]

Reconnaissance

Initial Planning Phase

- Threat perpetrator or actor researches target
- Analyze online activities and public presence
- Observe websites visited and social media networks used
- Harvest email addresses
- Collect publically available news
- Discover scanning for internet facing systems and applications
- Build a profile
Weaponization

Preparing and Staging the Attack

• Select appropriate malware payload based on research
• Reuse existing malware families – create slight variant
• Build the phishing email campaign
• Leverage exploit kits and botnets

https://blog.barkly.com/how-exploit-kits-work
Delivery

Launching the Attack

- Go live of the compromised website “watering hole”
- Delivery of the phishing email
  - Phishing is the most common attack vector especially for the US
- Distribution of infected USB sticks
- Execution of attack tools against servers and applications
Exploitation

Gain Access to Victim

- Exploited a hardware or software vulnerability
  - Zero days are rare
  - Most vulnerabilities exploited have known patches available
- Tricked a human being into providing access

Scanned websites with vulnerabilities

[Graph showing statistics of attacks per year]

229,000 Attacks / Day

Internet Security Threat Report from Symantec #22
Installation

Establish a Foothold in the Environment

• Installation of a persistent backdoor
• Utilize webshells on web servers
• Create additional accounts or services
• Leverage techniques to keep malware hidden and running
• Goal is to maintain access for an extended period of time

http://inkotech.co.id/what-is-web-based-malware-also-known-as-web-shell/
Command and Control (C2)

Establish Remote Control

- Use a two-way communication channel for remote control
- Common channels are web, email and DNS
- Often look to escalate privileges
- Move laterally internally
- Employ obfuscation (anti-forensics) techniques

https://logrhythm.com/blog/catching-beaconing-malware/
Actions and Objectives

Achieve the Goals of the Mission

• Successfully complete their end goal
• Steal data (IP, PII, $$)
• Corrupt, modify, destroy systems or data
• Use as a launching point to attack another
Use Cases
Controls Mapping
## Effectiveness Scorecard

### Seven ways to apply the cyber kill chain with a threat intelligence platform – LM
**Education and Awareness**

**ATTACK VECTORS:**

**INTERNET**
Social Media, P2P, Drive-By Download

**EMAIL**
Spear Phishing, Whale Phishing

**DEVICE**
USB Flash Drive, Phones, Tablets

1. Lure End-User to Download Exploit or Corrupt File
2. Exploit Executed
3. Inject Additional Code, Trojan or Backdoor
4. Establish Command and Control Channel
5. Explore and Move Laterally Within Organization
6. Steal and Transmit Target Data Out of Organization
7. Malware Becomes APT (Final Stage, Mutation)

Malware Injection
Inject Additional Code, Trojan or Backdoor
Establish Command and Control Channel
Explore and Move Laterally Within Organization
Steal and Transmit Target Data Out of Organization
Malware Becomes APT (Final Stage, Mutation)
Target Breach

Supplier portal and facilities management information publically available

Password logging malware embedded in email attachment (PDF or MS Office) sent to Fazio

Classic phishing campaign directed towards Fazio

Compromised a default password and moved internally around Target from external billing system to POS devices

RAM scrapping and data exfiltration malware loaded on POS devices at Target

Data exfiltrated in plain text to a server in Russia

Had access to internal systems for over a month

A kill chain analysis of the 2013 target data breach – UNITED STATES SENATE: COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
A kill chain analysis of the 2013 target data breach –
UNITED STATES SENATE: COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
Cautionary Notes
Many Similar Versions

Differences

• Change the wording
• Breakout specific actions into stages
• Combine different actions into stages
Limitations

External Intrusion-Centric
- Reinforces perimeter-focused mindset
- Predominately malware-prevention focused
  - Less effective for insiders and social engineering

Light on Recommendations
- Steps 1,2,3 have little defensive actions
- Steps 4,5 are classic protection solutions
- Steps 6,7 are more reactive solutions
Final Thoughts
Other Threat Modeling Approaches

**Attack Tree**

- Open Safe NSE/$20K
- Pick Lock SE/$30K
- Learn Combo NSE/$20K
- Cut Open Safe SE/$10K
- Install Improperly NSE/$100K
- Find Written Combo NSE/$75K
- Get Combo From Target NSE/$20K
- Threaten NSE/$80K
- Blackmail NSE/$100K
- Eavesdrop SE/$80K
- Bribe NSE/$20K

**SDLC**

## Actors – Intel Threat Agent Library

![Table Diagram](image)

Source: Intel IT Threat Assessment Group, 2007
Threat Modeling – Maturity Assessment
Battle Plan – Break the Kill Chain

Stop Attacker Here

Fallback Position

Last Stand

Update Resume