Closing the Loop:
RE, IR, & the Kill Chain

Bryan Nolen

About Me

- Worked in IT/InfoSec for the last 10+ years
- Cyber Security Incident Analyst at a Multinational Financial Company, providing priority coverage of EU/ASPAC

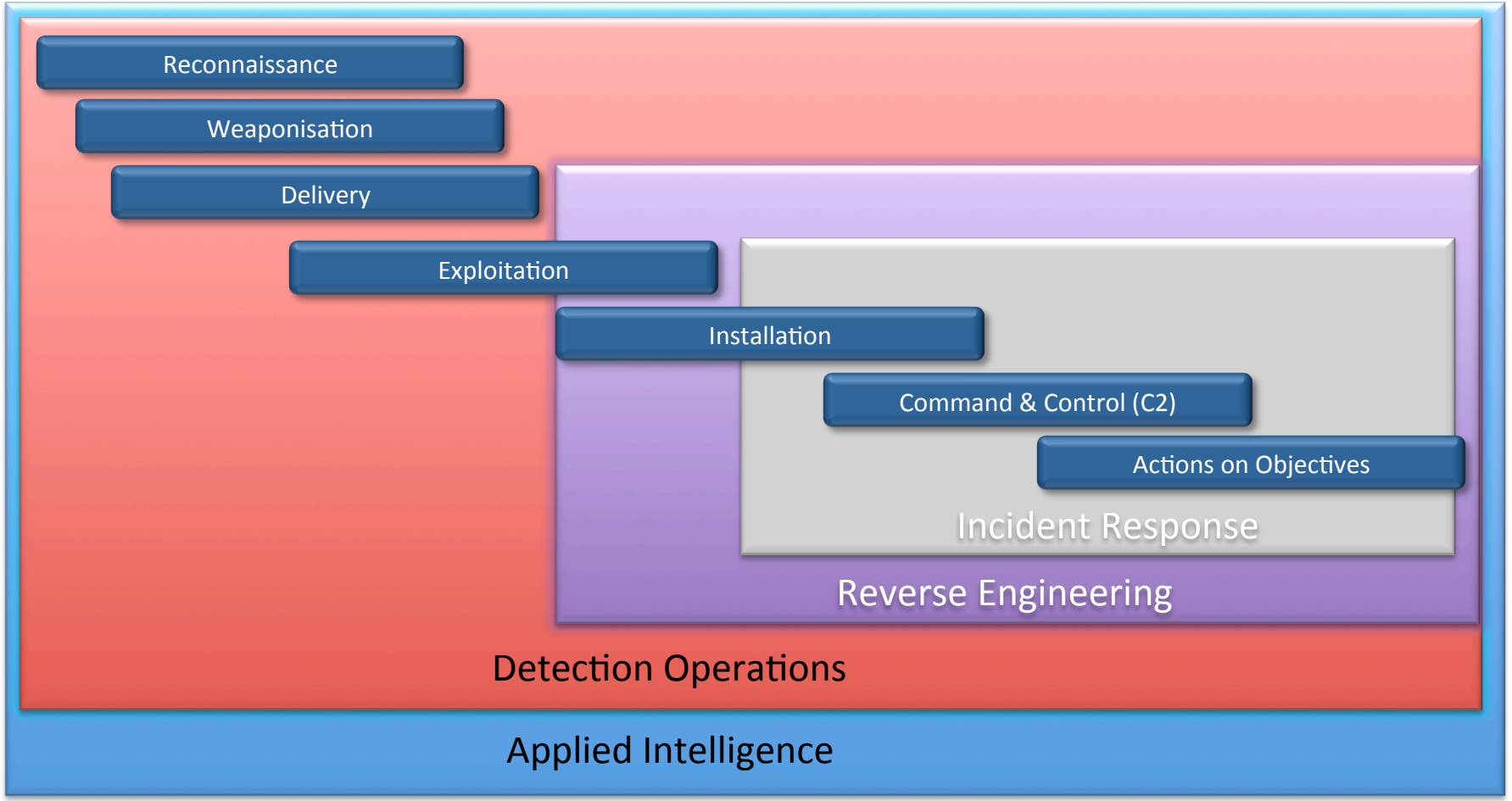
Kill Chain Intro

- Developed at Lockheed Martin in 2011
- Depicts common stages involved in an attack, mainly from the viewpoint of the attacker

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

The Kill Chain

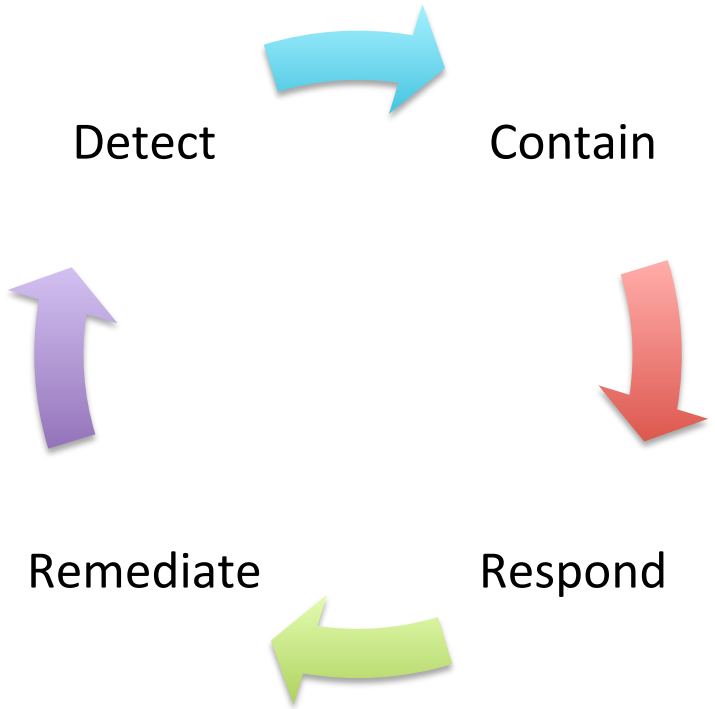
Reconnaissance	Research, identification, and selection of targets
Weaponisation	Developing exploit with payload creation, malware, delivery system, decoys
Delivery	Delivering weaponised bundle to the victim via email, web, USB, etc.
Exploitation	Exploiting vulnerability to execute intruder's code on target
Installation	Malware execution on target
Command & Control (C2)	Command channel established back to attacker
Actions on Objectives	Expand compromise, consolidate persistence, identify further targets, data exfiltration


Reconnaissance
Weaponisation
Delivery
Exploitation
Installation
Command & Control (C2)
Actions on Objectives
Incident Response
Reverse Engineering
Detection Operations
Applied Intelligence

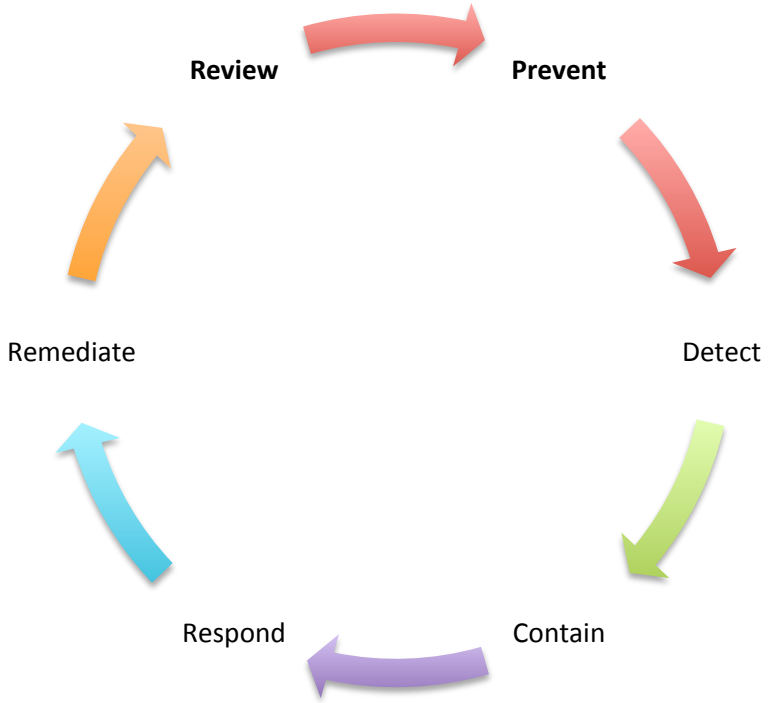
IR Cycle

- Similar to the Kill Chain, the IR Cycle depicts the stages of an attack, but from the defender’s vantage point

IR Cycle (base form)



IR Cycle (mature)



Case Study One

- Small company – 50 employees, just 2 in IT
- Email sent to their accountant (Alice)
- … who opened it, but did notice some odd behavior after *
- Reported to IT a few days later, who then scanned the box with their AV product

The Next Day…

- AV detected it as “erydza”
- Employees noticed their pay had not been processed
- Determined that the malware must have injected into the browser and intercepted/ rerouted the payroll transfer

Lessons – IR Cycle

Prevent	Failed – AV did not detect the malware until days after infection
Detect	User self-reported to AV, on-demand AV scan to detect
Contain	Machine Powered Off
Respond	No significant investigation, finance transactions investigated at the bank.
Remediate	Machine Reformatted, insurance claim lodged for the lost money
Review	N/A

Lessons – Kill Chain

Recon	Not easy to determine, requires outside intelligence in cases like this
Weaponisation	Embedded shellcode linked to multi stage installer
Delivery	Email as attachment with appropriate lure text
Exploitation	Macro enabled word document with embedded shellcode to download malware from a distribution point
Installation	Malware stage one is downloaded and executed by macro, stage two decrypted and copied to disk, persistence via Registry run key
C2	SSL traffic to multiple dynamic DNS domains
AoO	Injects into active browser sessions targeting financial transactions

Case Study Two

- Multinational company – 30,000 employees, 2,000 in IT
- Fully in-house SOC & CIRT
- Centralised 24x7 monitoring and analysis teams

Case Study Two cont.

- 5 employees in the same branch receive an email, which contained a specific, targeted, lure. Embedded within is a link to an EXE on a popular sharing site
- 2 members of the group click the link
- Of the 2, only 1 actually runs the EXE

Meanwhile in the SOC…

- Details of the email, and embedded link are recorded in the SIEM
- Details of the accesses to the link and the subsequent download are also recorded
- No Alerts are raised

Some time later…

- Routine AV scan detected the downloaded EXE, and the payload, and removes them.
- Detection is classified PUA/PUP, not a high severity threat

- Too bad it was a fairly capable keylogger

Three Weeks Later…

- Member of the Hunter team, acting on a hunch, searches for PUA/PUP activity on high value assets
- Given the value of the data on this asset, formal Incident Response Process was invoked

Containment

- Asset was logically isolated
- Number of important forensic artifacts were collected using specially designed scripts – i.e. memory, MFT, page files, USNJournal, etc.
- Thus contained, initial analysis was conducted

Response

- Collected artifacts were processed using a number of tools looking for known indicators of badness
- Memory analysis was also undertaken, but of limited value in this case given the lag between infection and collection
- Static and Dynamic file analysis however, provided solid evidence

Reversing FTW

- By submitting the quarantined files to proper static, and dynamic, reverse engineering, the capabilities of the malware were uncovered
- Based on the encryption details revealed, the collected log file remnants were able to be decrypted and potential exposure determined accurately
- Network IOCs and hunting signatures were able to be developed to search for any possible exfiltration

Lessons – IR Cycle

Prevent	Failed – Host based IPS and App Whitelisting should have prevented the initial execution, but did not – why?
Detect	AV detection did occur, but at the wrong severity, based on business risk
Contain	Logical Isolation
Respond	Evidence Collection and Analysis. Bulk data collection uncovered, but no successful exfiltration outside the controlled network (secondary controls worked as planned)
Remediate	Machine reimage, preventative proxy blocks implemented, user phishing training mandated
Review	Hunters add more similar edge cases to their workbooks, TPP/IOC shared with community

Lessons – Kill Chain

Recon	As with the other example, recon is not immediately evident, but no industry partners reported being hit by similar malware (post review)
Weaponisation	-
Delivery	Phish email with industry targeted lure, malicious exe hosted on a “trusted” site
Exploitation	User Behavior – users click things they should not click
Installation	Normal program execution via explorer
C2	None Observed, but not required for data collection
AoO	Keystrokes, screenshots, and browsing activity collected and stored in encrypted files on compromised server. No exfiltration.

TL;DR

- Reversers help Responders (e.g extracting encryption keys to decode collected files)
- Responders help Reversers (e.g. extra context on observed behaviors)
- Using Kill Chain and IR Cycle to speed up the analysis/review phases helps everyone

- Any Questions?