Cyber Kill Chains, Diamond Models and Analysis Methods.
Understanding how Intelligence works.

David Peers
Bournemouth OWASP, 2019
Who am I?
Royal Corps of Signals
Microsoft
CREST
GCHQ

What am I?
dpeers@protonmail.com
• Jargon
• Intelligence Cycle
• Typical installation of malware
• Cyber Kill Chains
• Diamond Model
• Threat actor types
• 3 Scenarios
Jargon

- Events and Incidents
- IoA
- IoC
- IoT
- TTP
- Bias
- Risk
- Black Swan
- Hypothesis
- APT
- Assets
- Asset
- Adversary
- Adversary Operator
- Adversary Customer
- Attack
- Campaign
- Cyber (enabled) crime
Intelligence Cycle

Consumption of Intelligence

1 Planning and Direction

2 Collection

3 Processing

4 Analysis

5 Delivery

Generation of Intelligence

Consumes Data

Creates Information

Creates Data

Creates Intelligence

Creates Decisions

RFI
Typical Installation of Malware

1. Download
2. Email
3. Play Store
4. Boom!
5. User Impact
Cyber Kill Chain

7 step process, developed by Lockheed Martin, to breakdown the process of intrusion and compromise.

- **Reconnaissance**
  - Harvesting email addresses, conference information, etc

- **Weaponization**
  - Coupling exploit with backdoor into deliverable payload

- **Delivery**
  - Delivering weaponized bundle to the victim via email, web, USB, etc

- **Exploitation**
  - Exploiting a vulnerability to execute code on victim system

- **Installation**
  - Installing malware on the asset

- **Command & Control**
  - Command channel for remote manipulation of victim

- **Actions on Objectives**
  - With “Hands on Keyboard” access, intruders accomplish their original goal
Diamond Model #2

Adversary

Uses

Infrastrucure

Connects to

Capability

Develops

Exploits

Victim
Threat Actor Types

State
Sponsored
Organised Crime
Criminal Hacktivists
Disgruntled Employees
Script Kiddies

Impact
National Infrastructure, Elections
Fraud, Identity, Espionage
Brand, Reputation
DoS, Data Breech
Nuisance

Ability
Low
High
Low

Population, Commitment, Time
Stealth, Knowledge, Funding
Scenarios 1, 2 & 3

Let’s have some fun!
Questions?

Why ask?  To learn!