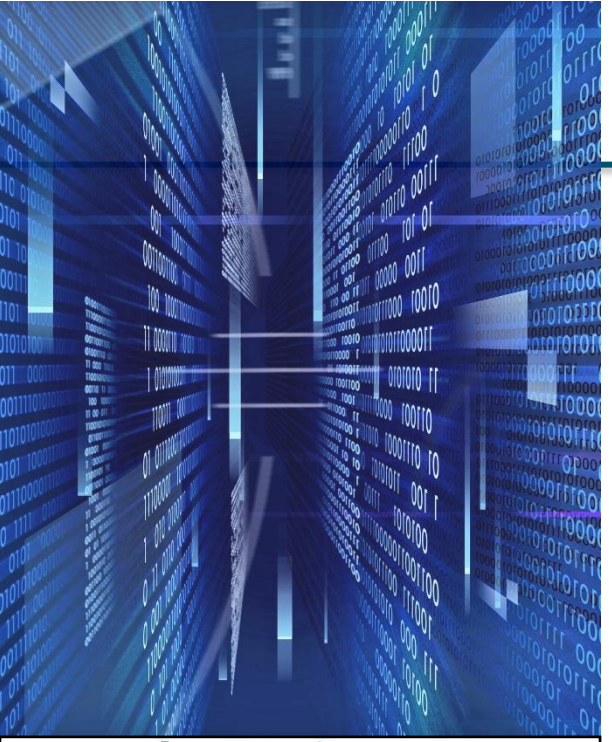


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Cyber Attack Life Cycle #1

Week 6 – Wednesday 6th November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Link with previous lectures

UNIVERSITY OF Southampton

Cyber Security

- . . .
- . . .

Access Control

Confidential/anonymous data/communication

Authentication (include passwords)

Cryptography

Applications

Data at rest

Data in transit

Machines

Network

. . .

. . .

. . .

Pervasive Passive Monitoring

Cyber Attack Life Cycle

. . .

. . .

. . .

Law

Cyber Space

Cyber Attacks

Cyber Actors

Multi-disciplinary Aspects

Learning Outcomes

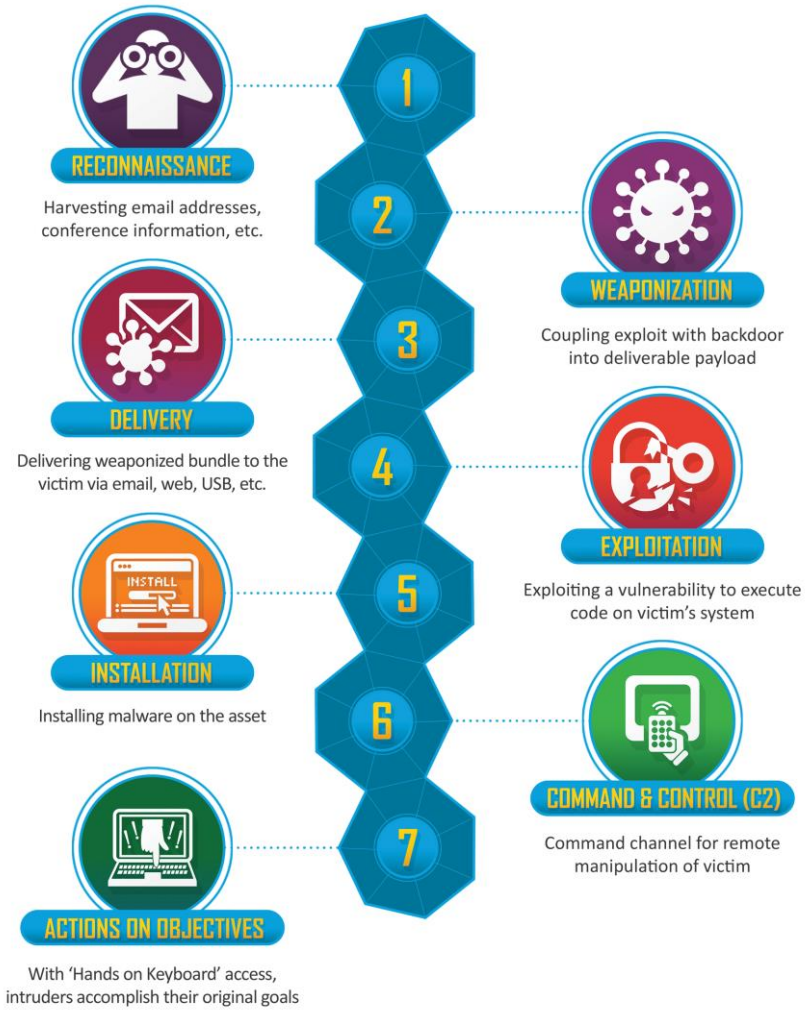
At the end of this lecture you should be able to

- LO1 Explain what the Kill Chain model is and describe its phases
- LO2 Analyse a cyber-attack by using the Kill Chain model

Outline

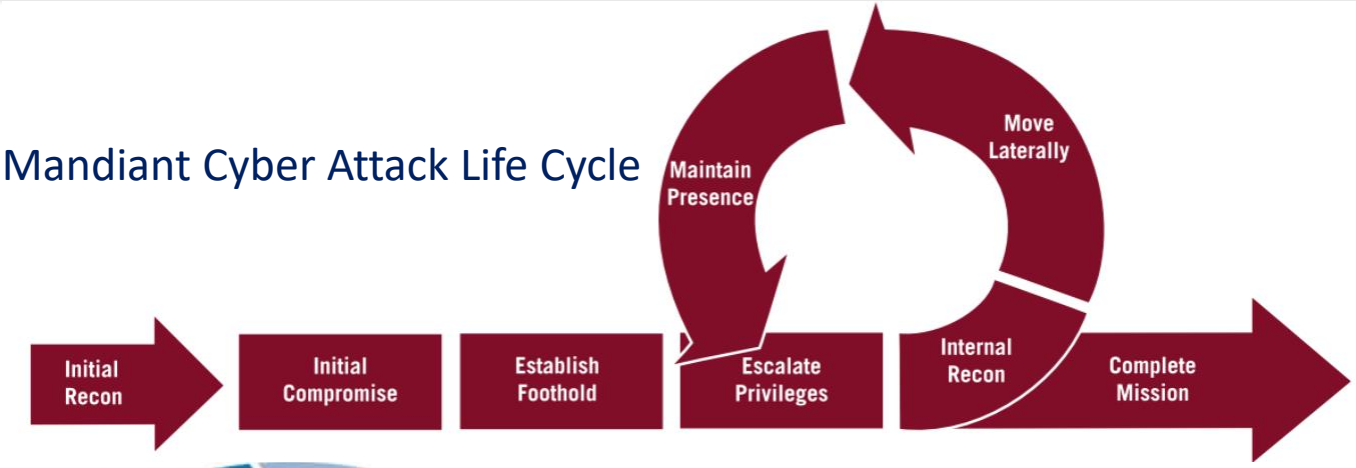
- **Cyber-attack Life Cycle Models**
- Lockheed Martin's Kill Chain Model
- Group Activity: analyse a cyber-attack using the Kill Chain

Cyber-attack Life Cycle Models



Lockheed Martin® Cyber Kill Chain

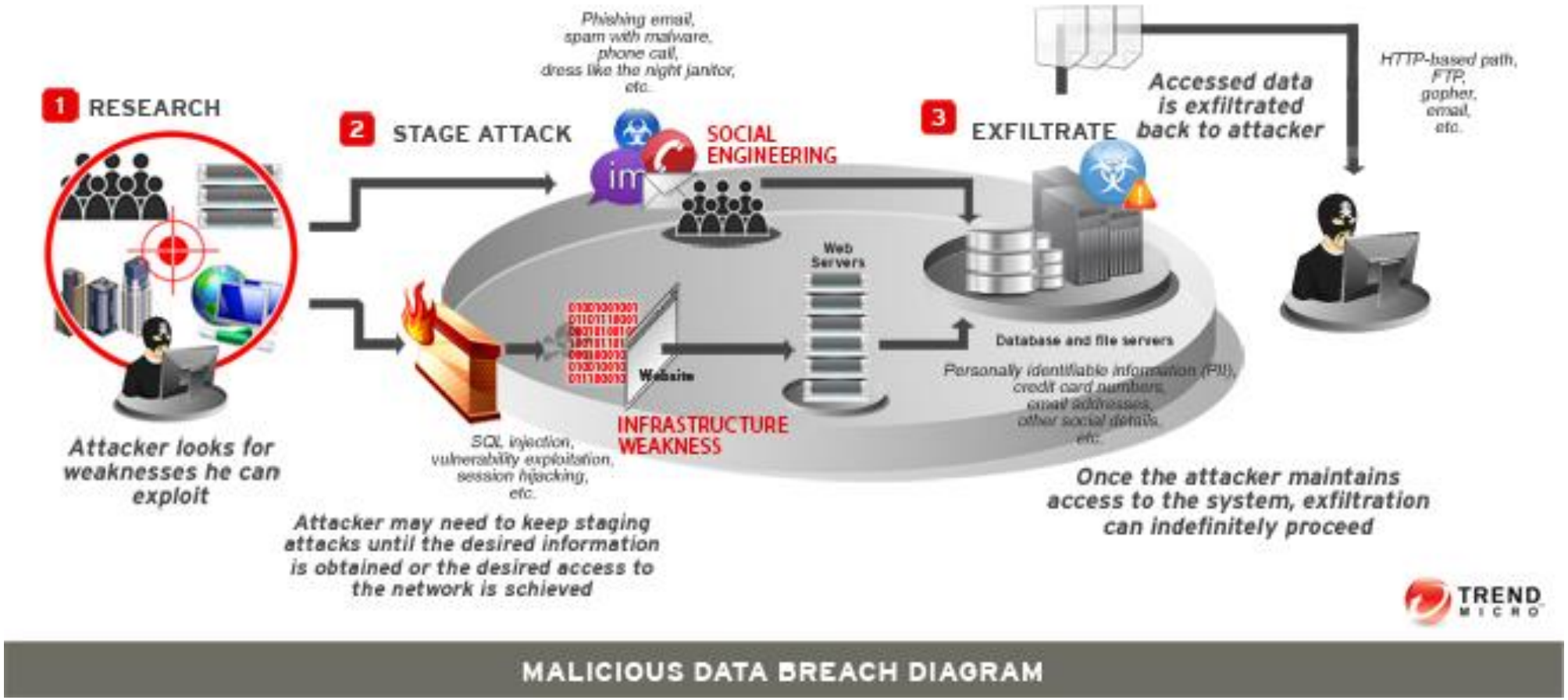
Mandiant Cyber Attack Life Cycle



By Dell SecureWorks

https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

Cyber-attack Life Cycle Models



https://www.trendmicro.com/vinfo/my/security/news/cyber-attacks/data-breach-101

Cyber-attack Life Cycle Models

- Empirical models representing the sequence of steps that cyber attacks go through

- Provide a framework to better understand cyber attacks to
  - Figure out why past attacks succeeded
  - Develop a structured knowledge base on past attacks
  - Identify convenient and effective ways to protect assets
  - Forecast potential next steps of a possibly ongoing attack

Outline

- Cyber-attack Life Cycle Models
- **➢Lockheed Martin's Kill Chain Model**
- Group Activity: analyse a cyber-attack using the Kill Chain

Lockheed Martin's Kill Chain Model

UNIVERSITY OF Southampton

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

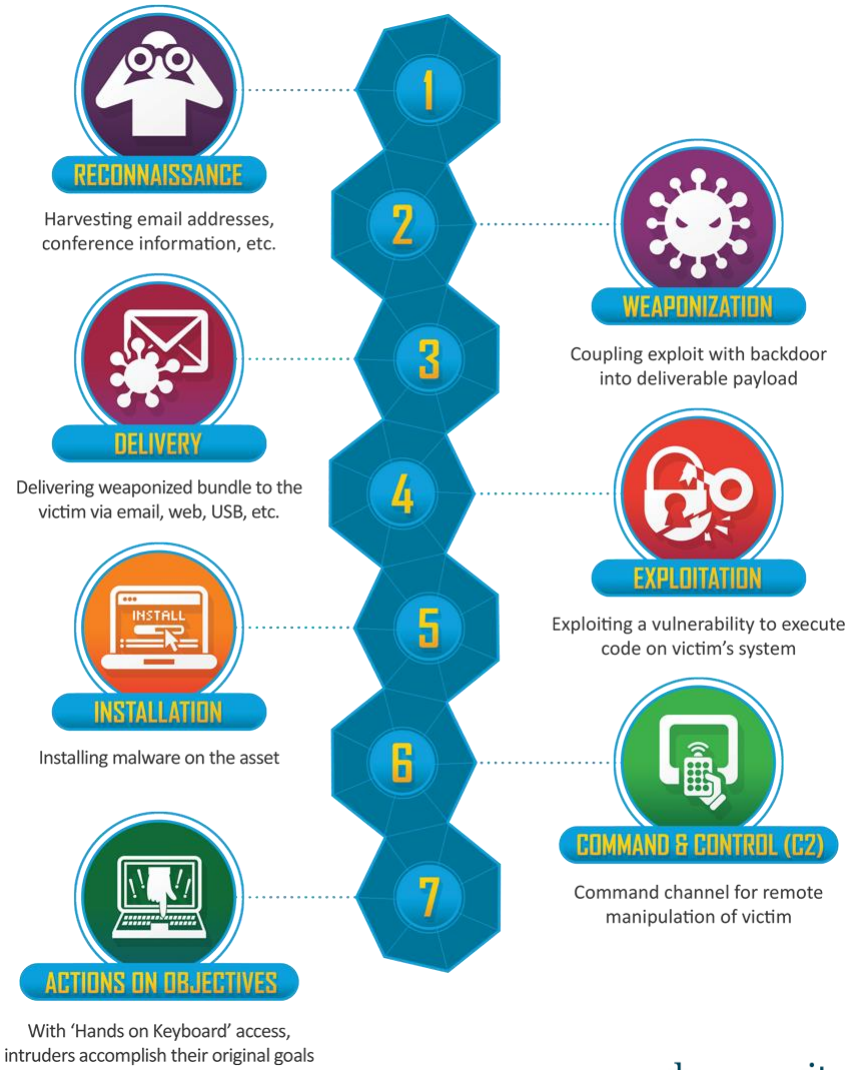
Eric M. Hutchins*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡

Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

Keywords: incident response, intrusion detection, intelligence, threat, APT, computer network defense



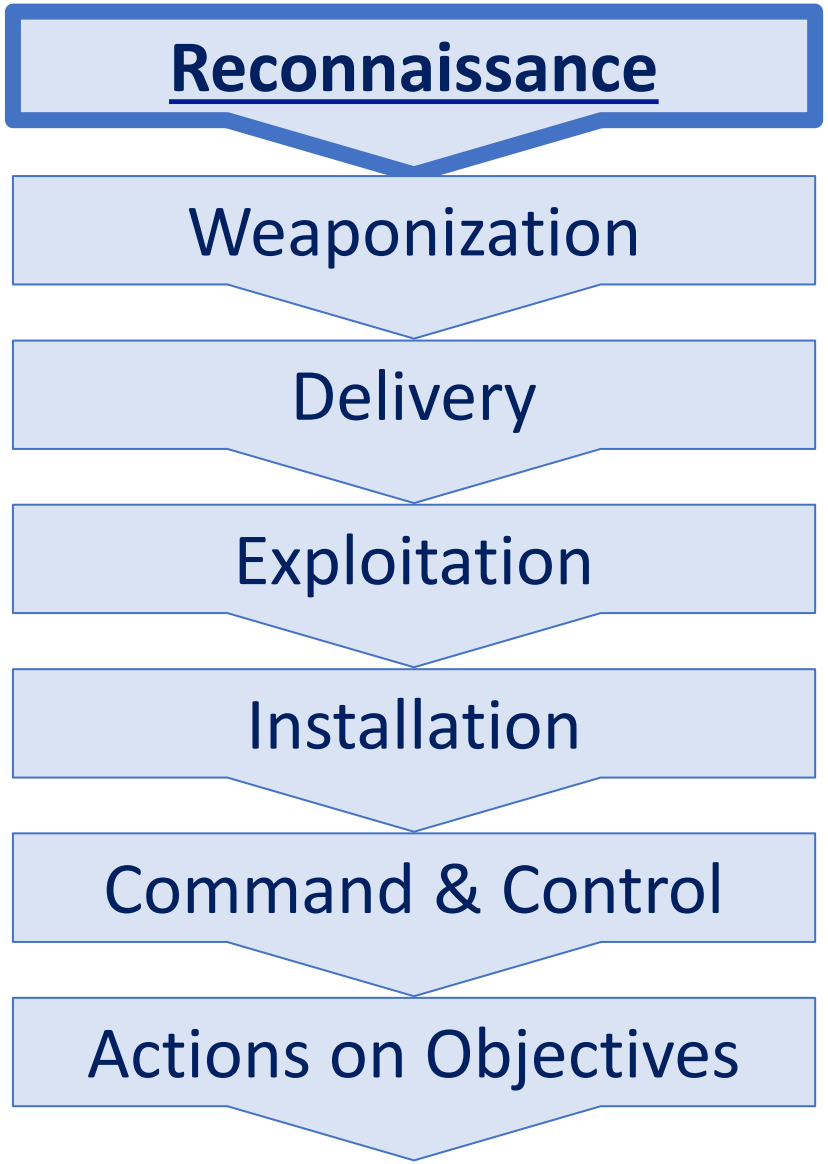
GCHQ Academic Centre of Excellence EPSRC

cybersecurity southampton

Lockheed Martin's Kill Chain Model

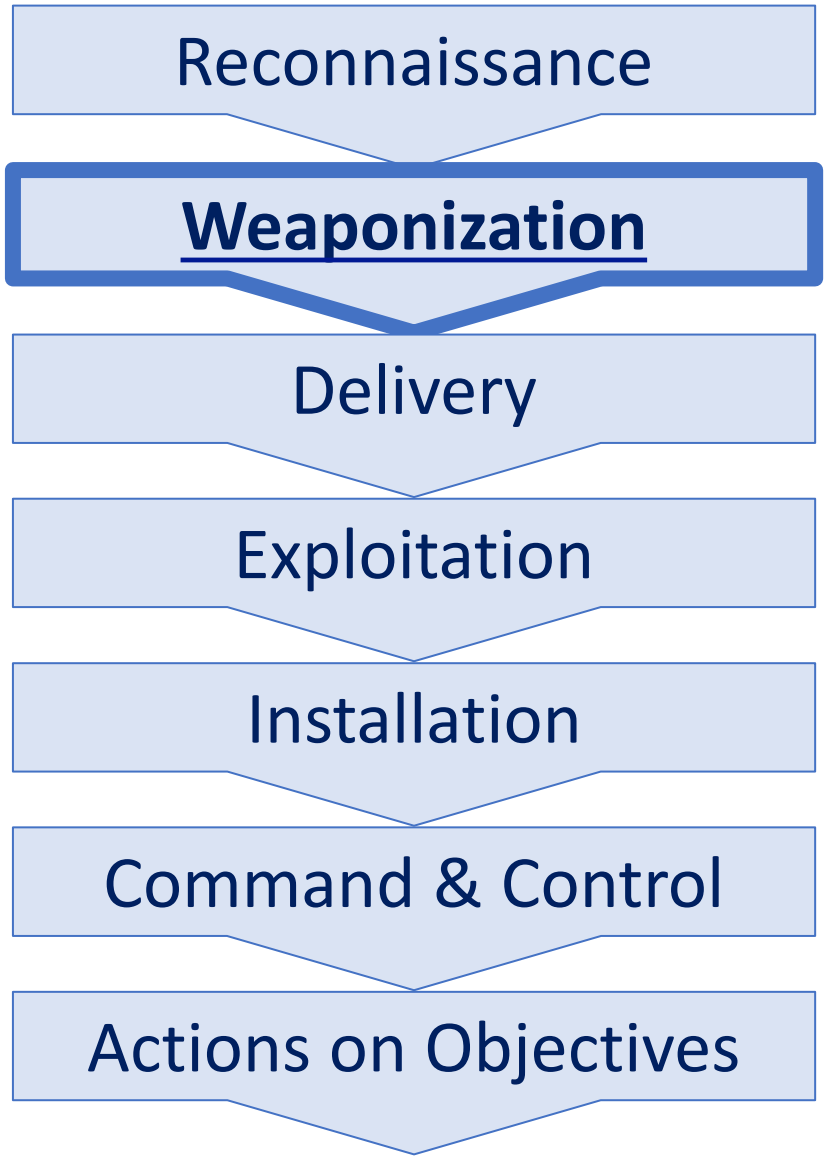
- Basic idea: *better understanding of adversarial strategy, in order to enhance countermeasures*
- Methodology to retrace attack phases through aggregation of intelligence information produced by distinct sources
  - IDS/FW/IPS alarms
  - Malware/Traffic analysis
  - Technical reports
- The kill chain represents the sequence of phases executed by the attacker
- This model is mainly thought for complex cyber intrusion
  - In particular, it nicely fits with Advanced Persistent Threats (APTs)
  - Some phase may not take place for simpler attacks

Lockheed Martin's Kill Chain Model



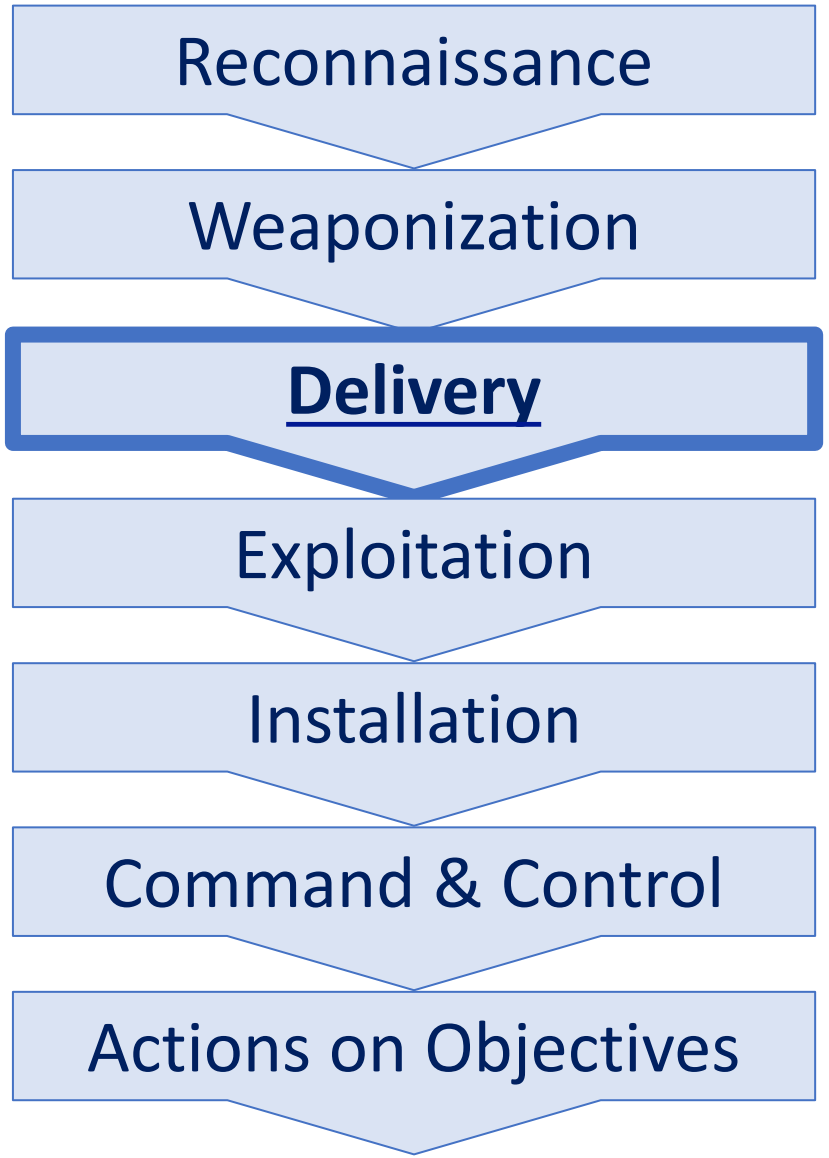
- Target research and selection
- Examples
  - Crawling of web sites to gather email addresses
  - Scans and probes to identify the security means used by the target

Lockheed Martin's Kill Chain Model



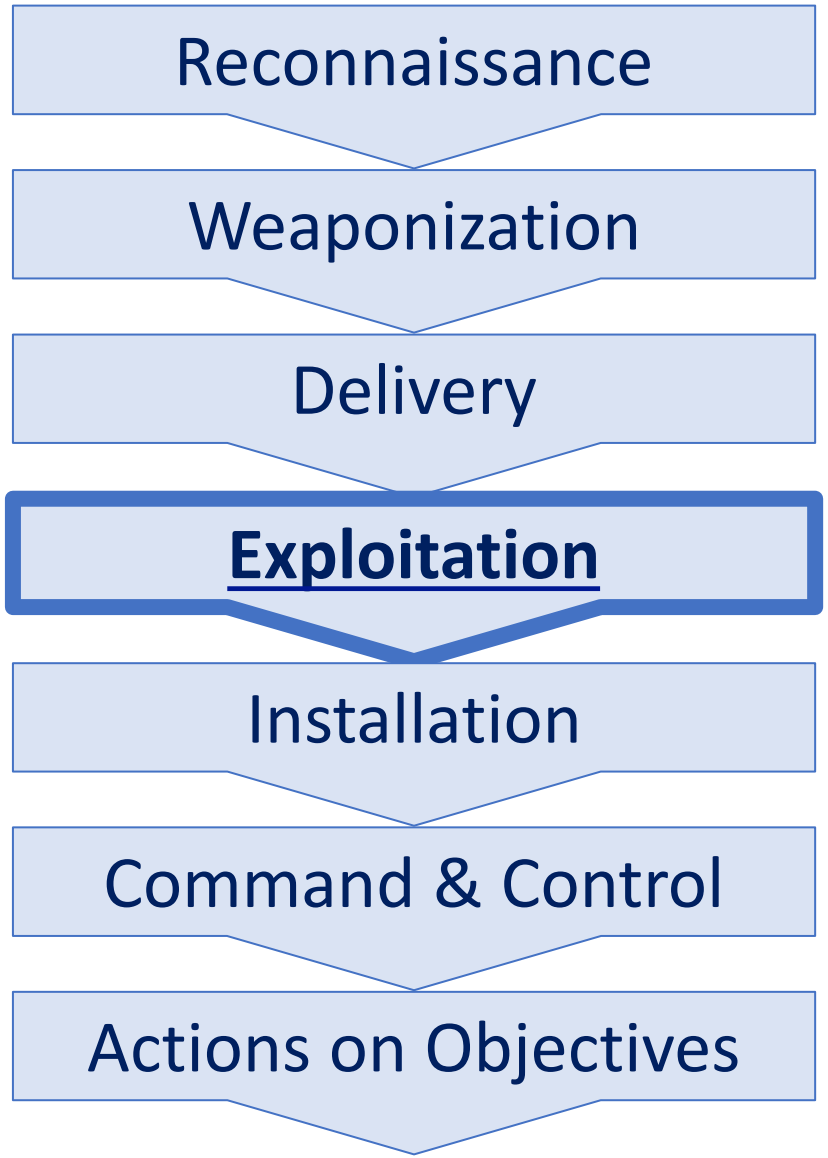
- Development of required cyber weapons, e.g. malicious payload, pairing it with an exploit
- Examples
  - PDF or Microsoft Office documents with embedded malicious scripts
  - Remote Access Trojan (RAT)

Lockheed Martin's Kill Chain Model



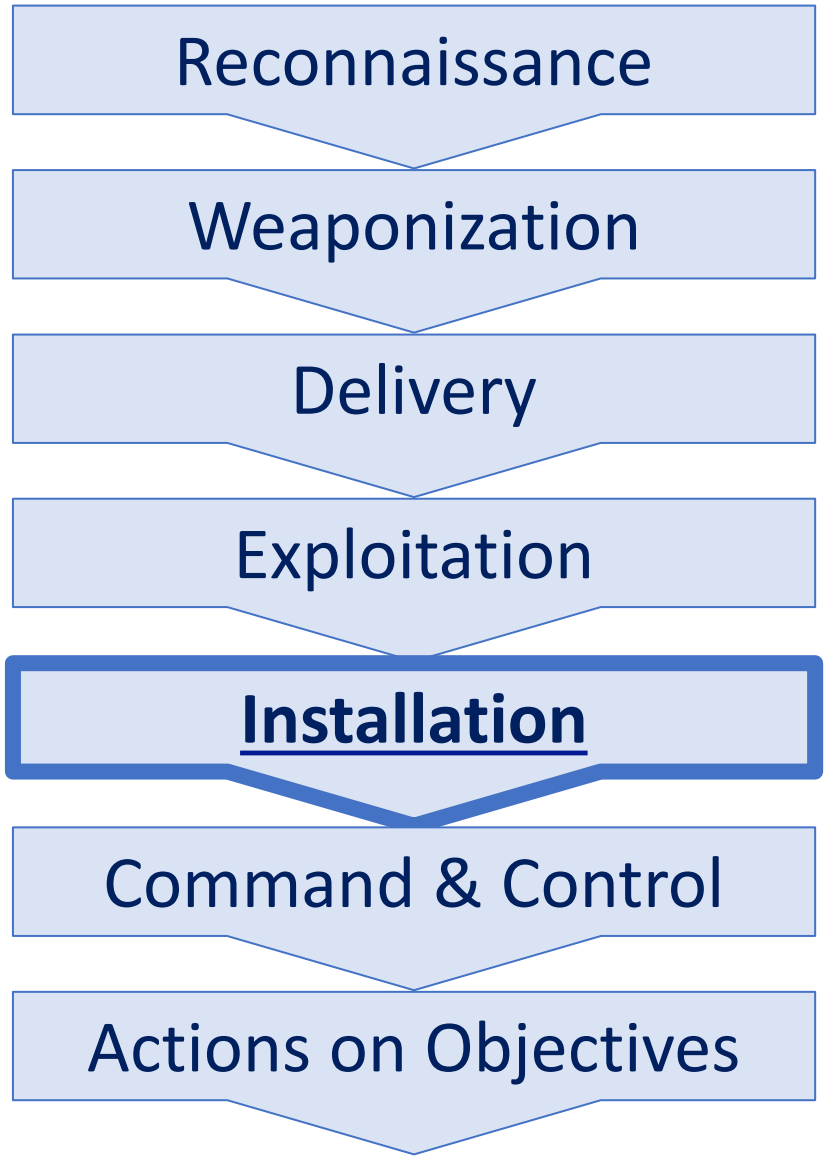
- Delivery of the payload to the target
- Examples
  - Download from web site
  - Email attachment
  - USB stick

Lockheed Martin's Kill Chain Model



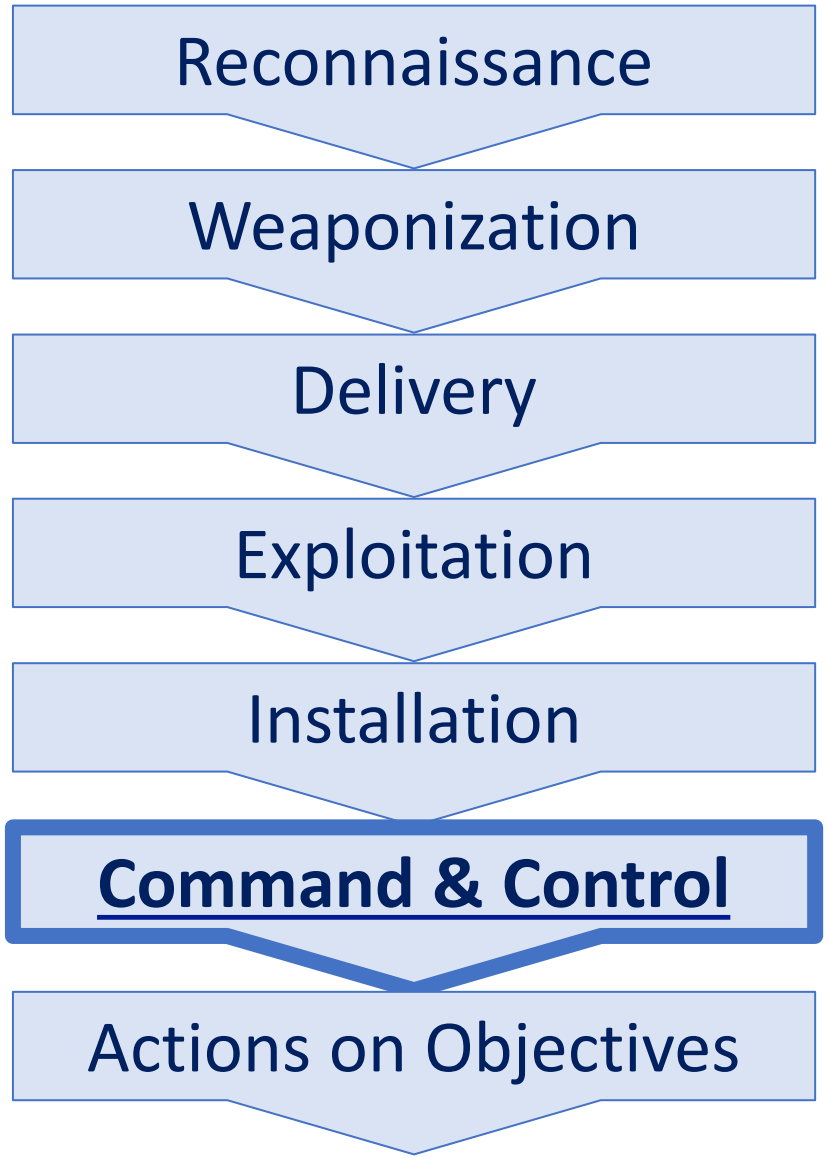
- Execution of the payload, e.g. through the exploit
- Examples
  - Exploit of known vulnerabilities of the target
  - Exploit of OS auto-start feature
  - User deception

Lockheed Martin's Kill Chain Model



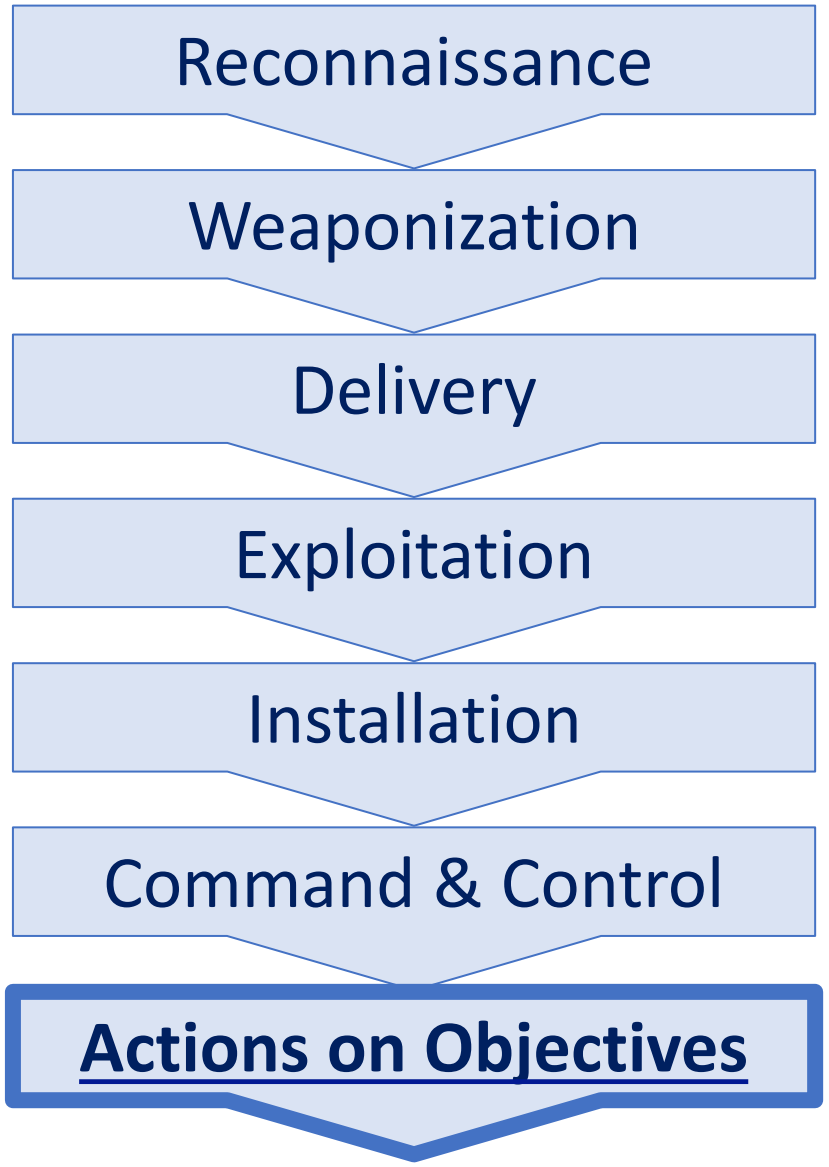
- Ensure payload persistence within the target
- Examples
  - Inject the malicious payload inside an OS process (e.g., explorer.exe)
  - Register the malicious payload as OS service with auto-start mode

Lockheed Martin's Kill Chain Model



- Establish a communication channel with an external command and control (C2) server
- Examples
  - Ciphered connection over HTTPS
  - Information exchange through public, beyond suspicion channels (e.g., on Twitter through tweets having specific hashtags)

Lockheed Martin's Kill Chain Model



- Execution of desired actions within the target, depending on the commands from C2
- Examples
  - Data exfiltration
  - Disruption

Outline

- Cyber-attack Life Cycle Models
- Lockheed Martin's Kill Chain Model
- **Group Activity: analyse a cyber-attack using the Kill Chain**

Group Activity: analyse a cyber-attack using the Kill Chain

UNIVERSITY OF Southampton

Equifax Data Breach

Equifax, the credit rating and scoring giant in America, was hacked back in March 2017. Vulnerabilities in third party open source software lead to hackers gaining access to critical systems via their online disputes portal (where customers dispute their credit report). Vulnerability CVE-2017-5638 in Apache Struts 2 was used to gain entry. However, the security breach comes down to the poor practices of Equifax's security team whose protocols did not update the vulnerability and left the 'gateway' open for months. Equifax then noticed and patched the software vulnerability but not after the hackers had installed more than 30 web shells (backdoor connections to the server).

One month later Equifax found the web shells via unusual network activity and pulled the site offline, crippling the attackers connection. By that point, however, the attackers had made off with 145 million user's personal details from databases within Equifax's systems. Once the attack was noticed both the FBI and Mandiant (forensic consulting firm) were called in to investigate the breach. Finally Equifax released a statement about the data breach and some help channels to help the effected population.

Kill Chain Analysis

- Split into groups of 4/5 students
- Discuss what might have happened in each phase
- 5 min group discussion
- 5/10 min open discussion

Group Activity: analyse a cyber-attack using the Kill Chain

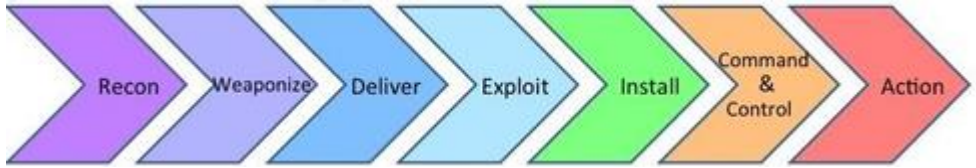
- Reconnaissance: look for vulnerable Apache Struts 2 servers
- Weaponization: obtain vulnerability exploit, develop/configure web shells, prepare C&C infrastructure
- Delivery: send crafted message to vulnerable Apache Struts 2
- Exploitation: exploit that vulnerability
- Installation: place 30 web shells
- C&C: remote connection through the web shells
- Action on objectives: data exfiltration

NB: the delivery phase is trivial but still relevant

Cyber Attack Life Cycle #1 - Recap

- Cyber-attack Life Cycle Models
  - Empirical models to represent the anatomy of cyber attacks

- Lockheed Martin's Kill Chain Model



Source: "A 'Kill Chain' Analysis of the 2013 Target Data Breach," March 26, 2014; US Senate Committee on Commerce, Science, and Transportation

- Group Activity: analyse a cyber-attack using the Kill Chain
  - Given a partial description of a cyber attack, deconstruct it using the kill chain

Cyber Attack Life Cycle #1 - References

- Hutchins, E.M., Cloppert, M.J. and Amin, R.M., 2011. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**. *Leading Issues in Information Warfare & Security Research*, 1(1), p.80.