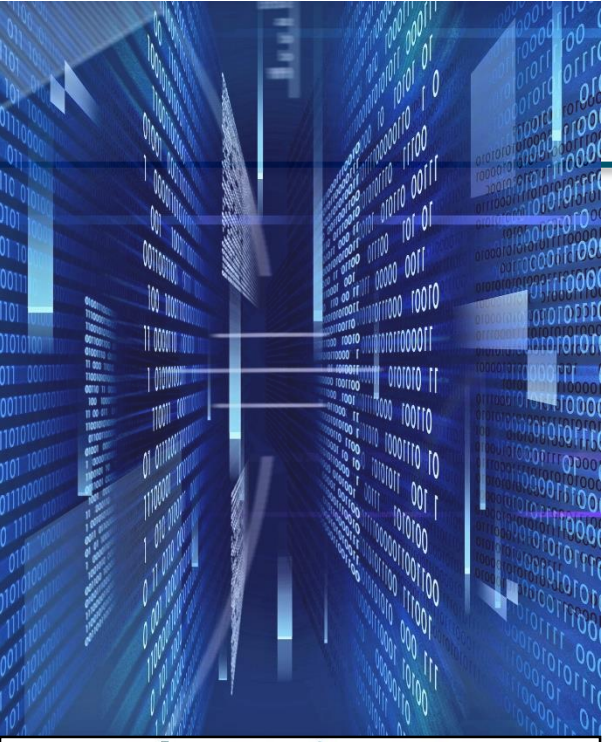


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Cyber Attack Life Cycle #2

Week 6 – Friday 8th November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Understand what a multi-step cyber-attack is
- LO2 Analyse a multi-step cyber-attack by using the Kill Chain model

Outline

- **Delivery vs Exploitation vs Installation**
- Multi-step Cyber-attacks
- Group Activity: analyse a multi-step cyber-attack using the Kill Chain

Delivery vs Exploitation vs Installation

UNIVERSITY OF Southampton

Equifax Data Breach

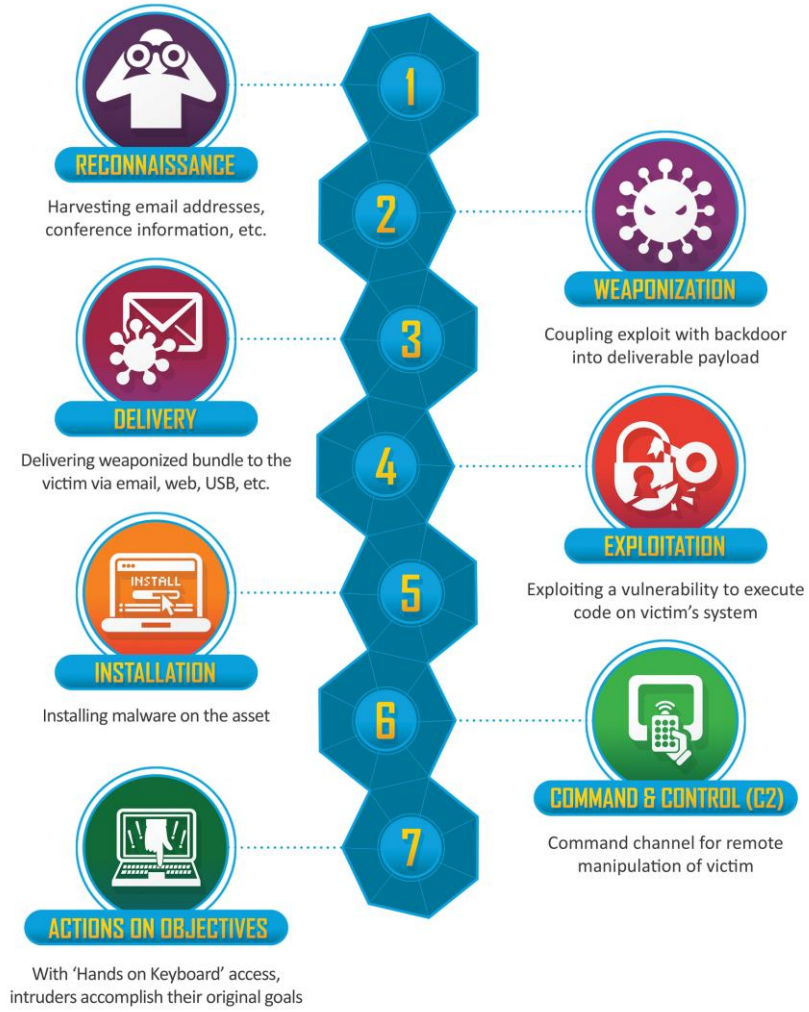
Equifax, the credit rating and scoring giant in America, was hacked back in March 2017. Vulnerabilities in third party open source software lead to hackers gaining access to critical systems via their online disputes portal (where customers dispute their credit report). Vulnerability CVE-2017-5638 in 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.

Delivery vs Exploitation vs Installation

- 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



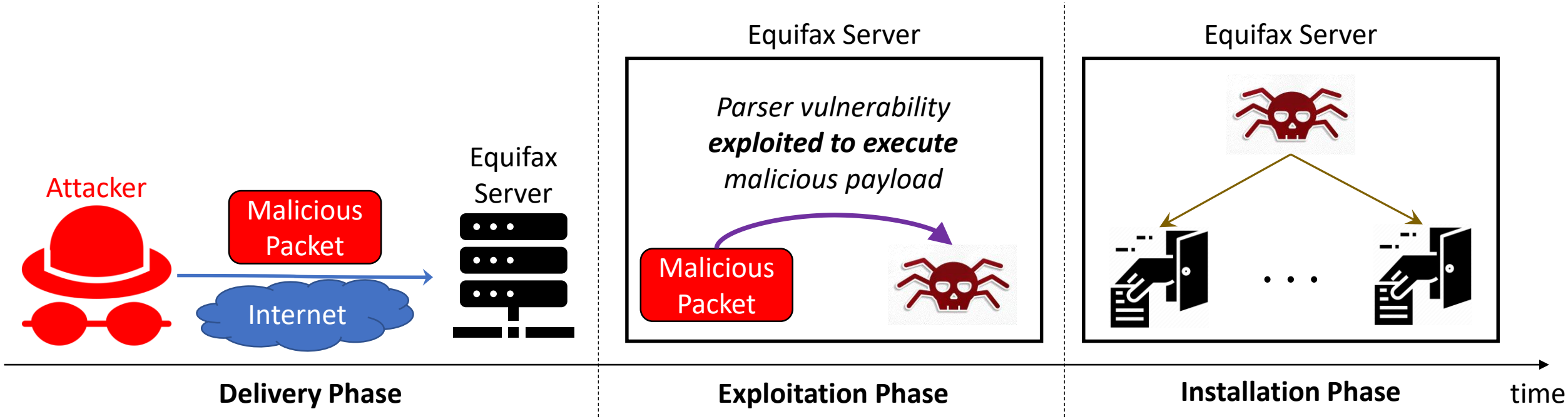
Lockheed Martin® Cyber Kill Chain

Delivery vs Exploitation vs Installation

UNIVERSITY OF Southampton

- CVE-2017-5638 (description available online https://nvd.nist.gov/vuln/detail/CVE-2017-5638)

  "The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which **allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header**, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string."



Outline

- Delivery vs Exploitation vs Installation
- **Multi-step Cyber-attacks**
- Group Activity: analyse a multi-step cyber-attack using the Kill Chain

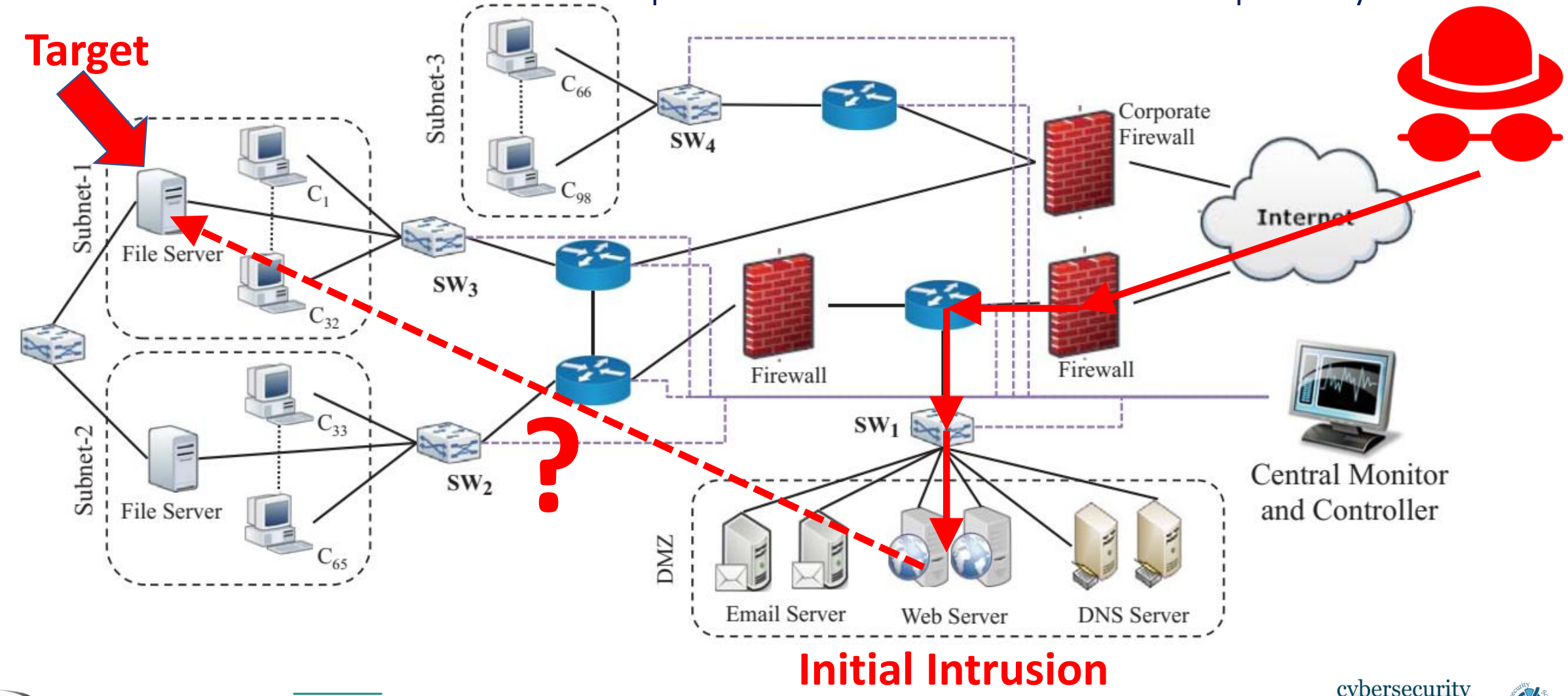
Multi-step Cyber-attacks

- According to the attack description:
  - “hackers gaining access to critical systems via their online disputes portal”
  - “attackers had made off with 145 million user’s personal details from databases within Equifax’s systems”

Do you notice anything missing in the analysis?

Multi-step Cyber-attacks

- "hackers gaining access to critical systems via their online disputes portal"
- "attackers had made off with 145 million user's personal details from databases within Equifax's systems"



Venkatesan, S., Albanese, M., Shah, A., Ganesan, R. and Jajodia, S., 2017, October. Detecting Stealthy Botnets in a Resource-Constrained Environment Using Reinforcement Learning. In Proceedings of the 4th ACM Workshop on Moving Target Defense (pp. 75-85).

Multi-step Cyber-attacks

- Initial Intrusion
  - As a result of a scanning (March 10, 2017), the adversary discovered a server housing Equifax's online dispute portal that was running a vulnerable software.
  - The adversary subsequently gained unauthorized access to the Equifax portal and confirmed that they could run commands. No data was taken at this time.
  - On May 13, 2017, in a separate incident following the initial unauthorized access, (other?) attackers gained again access to the online dispute portal.

United States Government Accountability Office. DATA PROTECTION - Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018. (https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf)

Multi-step Cyber-attacks

- Lateral Movement
  - The attackers used existing encrypted communication channels to the online dispute portal to send queries/commands to other systems and retrieve data.
  - The attackers issued queries to other databases to search for sensitive data.
  - They found a data repository containing personally identifiable information (PII), as well as unencrypted usernames and passwords that could provide access to several other Equifax databases.
  - The attackers expanded their access beyond the 3 databases associated with the online dispute portal, to include an additional 48 unrelated databases.

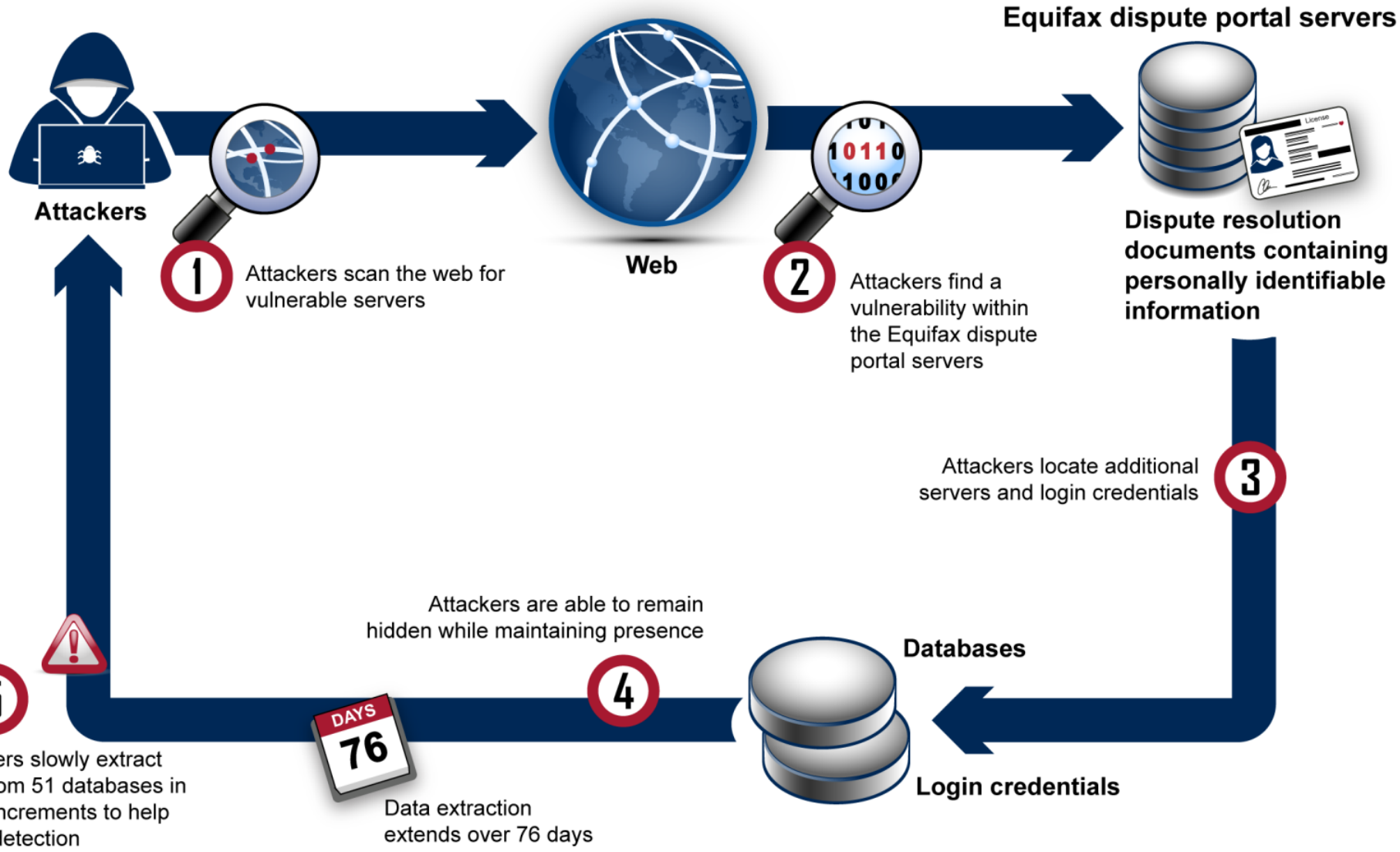
United States Government Accountability Office. DATA PROTECTION - Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018. (https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf)

Multi-step Cyber-attacks

- Data Exfiltration
  - The attackers then ran a series of queries in an effort to try to extract PII from the databases they had located.
  - They ran approximately 9,000 queries, a portion of which successfully returned data containing PII.
  - After successfully extracting PII from Equifax databases, the attackers removed the data in small increments, using standard encrypted web protocols to disguise the exchanges as normal network traffic.

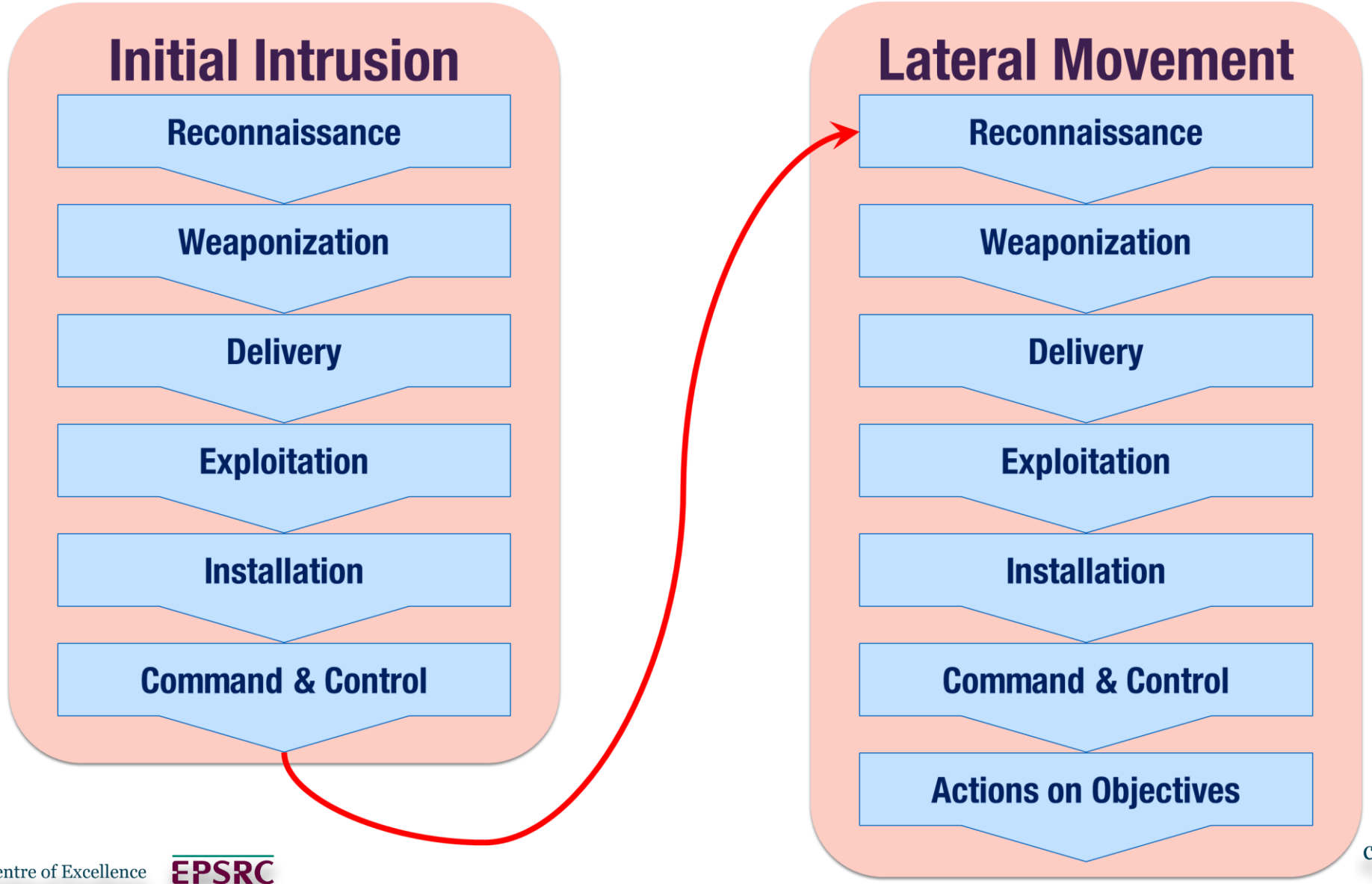
United States Government Accountability Office. DATA PROTECTION - Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018. (https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf)

Multi-step Cyber-attacks

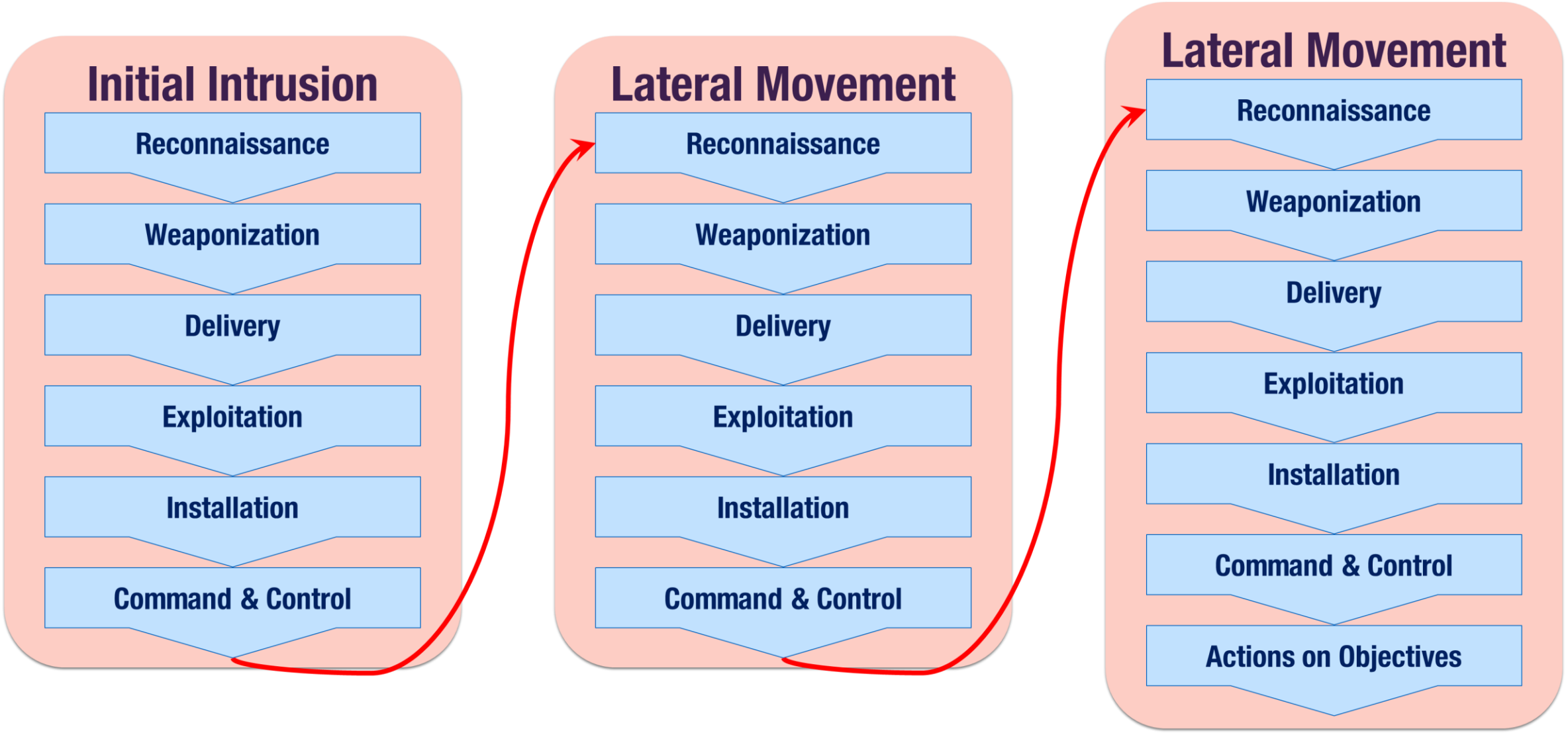


United States Government Accountability Office. DATA PROTECTION - Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018. (https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf)

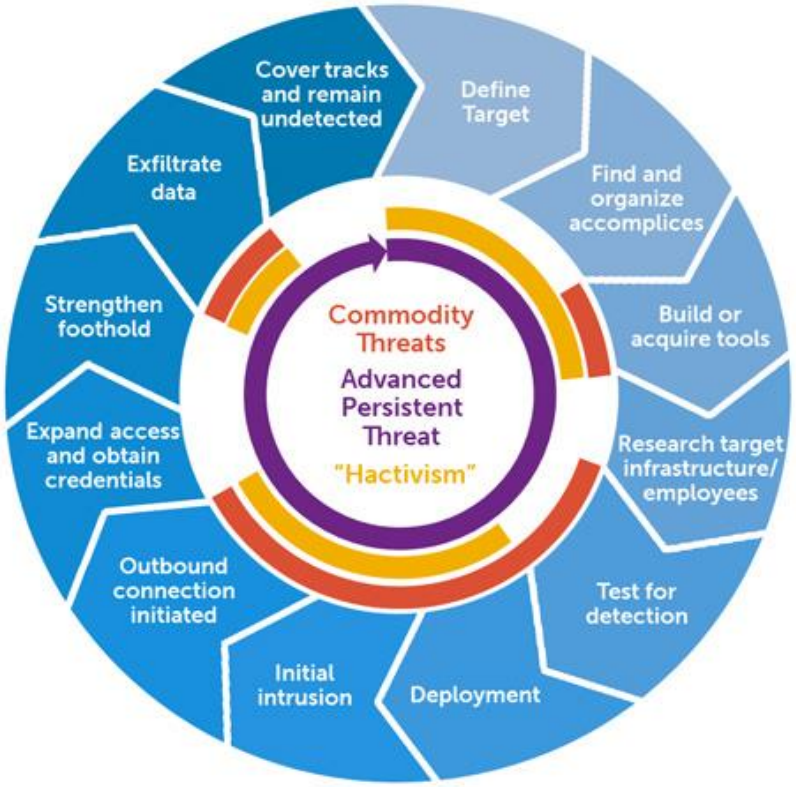
Multi-step Cyber-attacks



Multi-step Cyber-attacks



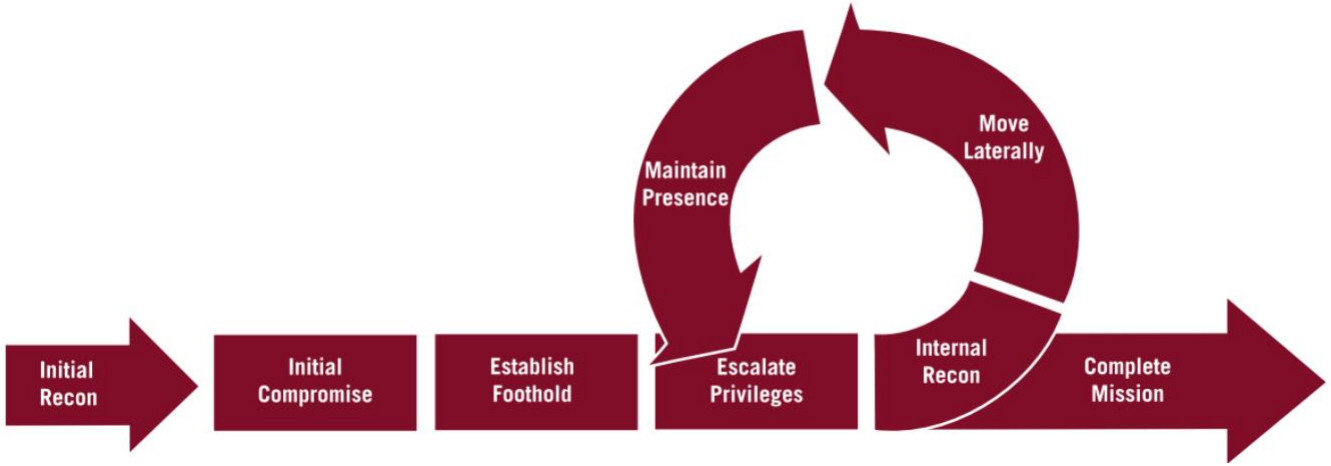
Multi-step Cyber-attacks



By Dell SecureWorks

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

Mandiant Cyber Attack Life Cycle



Outline

- Delivery vs Exploitation vs Installation
- Multi-step Cyber-attacks

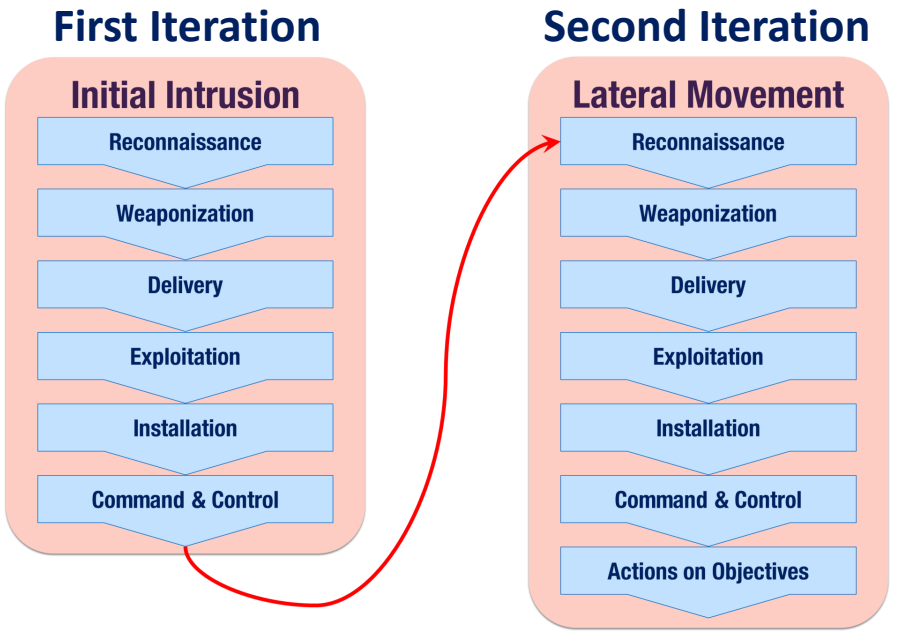
➢**Group Activity: analyse a multi-step cyber-attack using the Kill Chain**

UNIVERSITY OF Southampton

Equifax Data Breach

After the initial intrusion (i.e. in the second **iteration**), the attackers

- From the compromised online dispute portal, sent queries/commands to other systems
- Found a data repository containing personally identifiable information (PII), as well as unencrypted usernames and passwords
- Used those credentials to access other 48 DBs, which contained huge amounts of PII
- Extracted PII from those DBs



Kill Chain Analysis

- Split into groups of 4/5 students
- Discuss what might have happened in each phase
- Only analyse the second iteration of the attack
- 5 min group discussion
- 5/10 min open discussion

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

- Reconnaissance:
  scan systems connected to the online dispute portal, found credentials to other DBs
- Weaponization:
  in this case, the cyber weapons are the stolen credentials of those DBs
- Delivery: login attempt to those DBs
- Exploitation: successful login to those DBs
- Installation: not relevant (took place in the first iteration, through the web shells)
- C&C: issue SQL queries to collect confidential data (i.e. PII)
- Action on objectives: data exfiltration

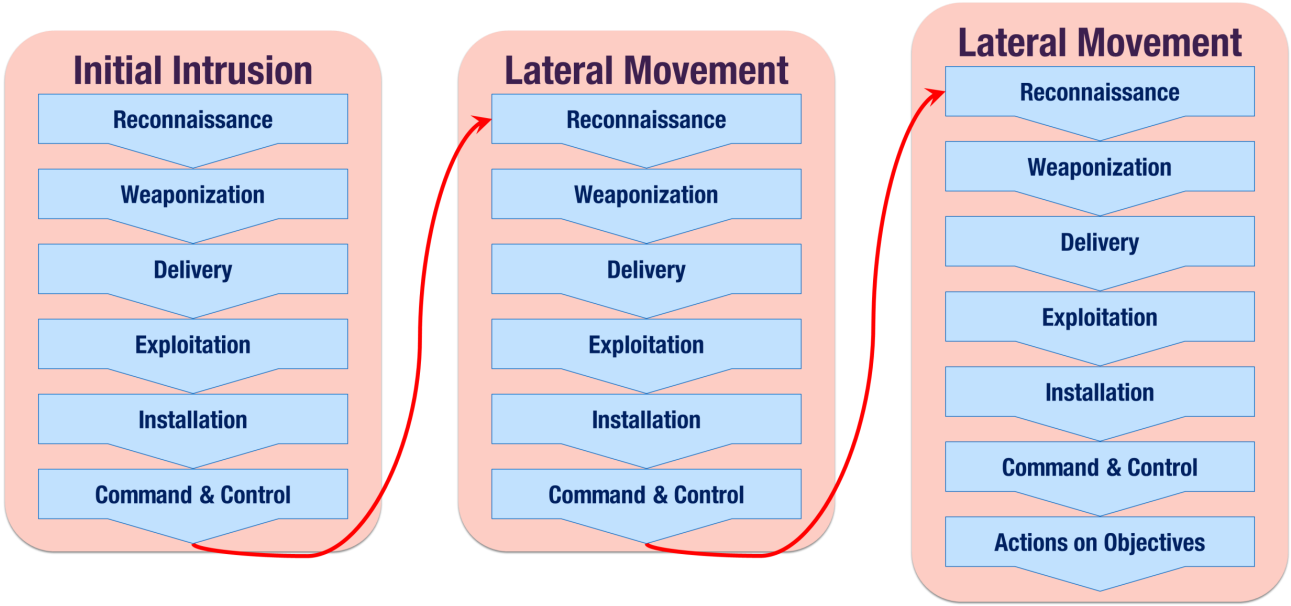
NB: the delivery and exploitation phases are trivial but still relevant

Cyber Attack Life Cycle #2 - Recap

UNIVERSITY OF Southampton

- Delivery vs Exploitation vs Installation

- Multi-step Cyber-attacks



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

Cyber Attack Life Cycle #2 - References

- United States Government Accountability Office. DATA PROTECTION - Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 2018.
  - Available online https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf