Week 3 Workshop

Key knowledge/skills: Cyber Kill Chain & Cyber threats

Case study (as briefly discussed in the 2nd lecture) - "Company X and Company Y are competitors who both are bidding on a secret Government project. Staff A (attacker) from Company X learned from LinkedIn that Staff V (victim) is the lead architect in Company Y. A then crafted an email pretending from acquaintance of V with a malware attached. Note that A developed the malware by leveraging a recent Zero day vulnerability. V was lured to click on the malware in the email, which installed a backdoor, after successfully exploited the targeted vulnerability on Staff V's system. This gave A the remote control of Staff V's computer. After that, Staff A used a compromised server (C2 server) to issue commands to maintain the control of V's computer. One night, A started to upload key design documents from V's computer to a shared Cloud storage folder owned by Staff A."

Q1. Map the attack activities to Cyber Kill Chain (CKC)

Sample answer:

CKC1 – Staff A gathered information of Staff V via LinkedIn

CKC2 – Staff A developed customized malware

CKC3 – Malware was delivered via phishing email

CKC4 – Malware exploited targeted vulnerability on Staff V's system

CKC5 – Malware installed on Staff V's system and opened a backdoor

CKC6 – Staff A used a compromised server to control V's computer

CKC7 – Staff A started to copy documents from V's computer

Q2. Map the following technical controls to Cyber Kill Chain (CKC), e.g., 'Email Security: CKC3 Delivery'; and what other controls you can think of?

- Gateway controls such as Web Proxy, Email Security, DNS
- Network controls such as IPS (Intrusion Prevention System)
- Endpoint controls such as AV (Anti-Virus), HIPS (Host based IPS)

Sample answer:

Web Proxy – CKC6, 7
Email Security – CKC3
DNS – CKC6
IPS – CKC3, 6
AV – CKC3-5
HIPS – CKC3-7

Q3. Assuming you have access to all the logs / security alerts of the above controls during the event, what are the key information/attributes can help detect/stop the attack?

Sample answer:

Web Proxy – C2 server domain name/IP address, unknown Cloud storage link
Email Security – Phish email sender & malware signature
DNS – C2 server domain name
IPS – Malware signature, C2 domain name/IP address & communication pattern
AV – Malware signature
HIPS – Malware behaviour pattern, C2 communication pattern, unknown Cloud storage link