C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

CS 668: Module 2
Lockheed-Martin Cyber Kill Chain

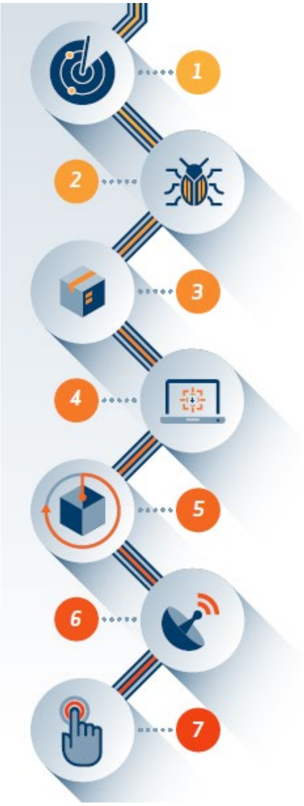
What is Cyber Kill Chain Framework

- The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity.
- The model identifies what the adversaries must complete in order to achieve their objective.
- Stopping adversaries at any stage breaks the chain of attack!
- Adversaries must completely progress through all phases for success;
    - this puts the odds in our favor as we only need to block them at any given one for success.
- Every intrusion is a chance to understand more about our adversaries and use their persistence to our advantage.

E. M. Hutchins, M. J. Cloppert, R. M.Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain” – Lockheed Martin Corp.

Cyber Kill Chain Steps

- The kill chain model is designed in seven steps:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control (C2)
  - Actions on Objectives
- Defender’s goal: understand the aggressor’s actions
  - Understanding is Intelligence
- Intruder succeeds if, and only if, they can proceed through steps 1-6 and reach the final stage of the Cyber Kill Chain®.



RECONNAISSANCE *Identify the Targets*

- ADVERSARY
  - *The adversaries are in the planning phase of their operation.*
  - *They conduct research to understand which targets will enable them to meet their objectives.*
    - Harvest email addresses
    - Identify employees on social media networks
    - Collect press releases, contract awards, conference attendee lists
    - Discover internet-facing servers

- **DEFENDER**
  - *Detecting reconnaissance as it happens can be very difficult, but when defenders discover recon – even well after the fact – it can reveal the intent of the adversaries.*
  - Collect website visitor logs for alerting and historical searching.
  - Collaborate with web administrators to utilize their existing browser analytics.
  - Build detections for browsing behaviours unique to reconnaissance.
  - Prioritize defences around technologies or people based on recon activity.

WEAPONIZATION *Prepare the Operation*

- Adversary
  - Obtain a weaponizer, either in-house or obtain through public or private channels
  - For file-based exploits, select “decoy” document to present to the victim.
  - Select backdoor implant and appropriate command and control infrastructure for operation
  - Designate a specific “mission id” and embed in the malware
  - Compile the backdoor and weaponize the payload

- Defender
  - Conduct full malware analysis – not just what payload it drops, but how it was made.
  - Build detections for weaponizers – find new campaigns and new payloads only because they reused a weaponizer toolkit.
  - Analyze timeline of when malware was created relative to when it was used. Old malware is “malware off the shelf” but new malware might mean active, tailored operations.
  - Collect files and metadata for future analysis.
  - Determine which weaponizer artifacts are common to which APT campaigns. Are they widely shared or closely held?

DELIVERY *Launch the Operation*

- Adversary
  - Adversary controlled delivery:
    - Direct against web servers
  - Adversary released delivery:
    - Malicious email
    - Malware on USB stick
    - Social media interactions
    - “Watering hole” compromised websites

- Defender
  - Analyze delivery medium – understand upstream infrastructure.
  - Understand targeted servers and people, their roles and responsibilities, what information is available.
  - Infer intent of adversary based on targeting.
  - Leverage weaponizer artifacts to detect new malicious payloads at the point of Delivery.
  - Analyze time of day of when operation began.
  - Collect email and web logs for forensic reconstruction. Even if an intrusion is detected late, defenders must be able to determine when how delivery began.

EXPLOITATION *Gain Access to Victim*

- Adversary
  - Software, hardware, or human vulnerability
  - Acquire or develop zero-day exploit
  - Adversary triggered exploits for server-based vulnerabilities
  - Victim triggered exploits
    - Opening attachment of malicious email
    - Clicking malicious link

- Defender
  - User awareness training and email testing for employees.
  - Secure coding training for web developers.
  - Regular vulnerability scanning and penetration testing.
  - Endpoint hardening measures:
    - Restrict admin privileges
    - Use Microsoft Windows Defender Exploit Guard
    - Custom endpoint rules to block shellcode execution
  - Endpoint process auditing to forensically determine origin of exploit.

INSTALLATION *Establish Beachhead at the Victim*

- Adversary
  - Install webshell on web server
  - Install backdoor/implant on client victim
  - Create point of persistence by adding services, AutoRun keys, etc.
  - Some adversaries “time stomp” the file to make malware appear it is part of the standard operating system install.

- Defender
  - HIPS to alert or block on common installation paths, e.g. RECYCLER.
  - Understand if malware requires administrator privileges or only user.
  - Endpoint process auditing to discover abnormal file creations.
  - Extract certificates of any signed executables.
  - Understand compile time of malware to determine if it is old or new.

COMMAND & CONTROL (C2)

Remotely Control the Implants

- Adversary
  - Open two way communications channel to C2 infrastructure
  - Most common C2 channels are over web, DNS, and email protocols
  - C2 infrastructure may be adversary owned or another victim network itself
- Defender
  - Discover C2 infrastructure thorough malware analysis.
  - Harden network:
    - Consolidate number of internet points of presence
    - Require proxies for all types of traffic (HTTP, DNS)
  - Customize blocks of C2 protocols on web proxies.
  - Proxy category blocks, including “none” or “uncategorized” domains.
  - DNS sink holing and name server poisoning.
  - Conduct open source research to discover new adversary C2 infrastructure.

ACTIONS ON OBJECTIVES *Achieve the Mission's Goal*

- Adversary
  - Collect user credentials
  - Privilege escalation
  - Internal reconnaissance
  - Lateral movement through environment
  - Collect and exfiltrate data
  - Destroy systems
  - Overwrite or corrupt data
  - Surreptitiously modify data

- Defender
  - Establish incident response playbook, including executive engagement and communications plan.
  - Detect data exfiltration, lateral movement, unauthorized credential usage.
  - Immediate analyst response to all CKC7 alerts.
  - Forensic agents pre-deployed to endpoints for rapid triage.
  - Network package capture to recreate activity.
  - Conduct damage assessment with subject matter experts.

Defenders must Continuously Analyze

- Analysis of multiple intrusion kill chains over time draws attention to similarities and overlapping indicators.
- Defenders learn to recognize and define intrusion campaigns and understand the intruder’s mission objectives.
- Identify patterns: what are they looking for, why are they targeting me?
  - Helps identify how to best protect yourself from the next attack.
- You can’t get ahead of the threat unless you understand the campaign.

Defenders must reconstruct Incidents

- Defenders must always analyze backward to understand earlier steps in the kill chain. The threats will come back again.
- Learn how they got in and block it for the future.
- Blocked intrusions are equally important to analyze in depth to understand how the intrusion would have progressed.
- Measure effectiveness of your defenses if it progressed.
- Deploy mitigations to build resilience for tomorrow.
- Cyber Kill Chain® analysis guides understanding of what information is, and may be, available for defensive courses of action.
- Stay focused on your threat landscape with vigilance.

RESILIENCE: *Defend against Advanced Persistent Threats*

- The antidote to APT is a resilient defense.
- Measure the effectiveness of your countermeasures against the threats.
- Be agile to adapt your defenses faster than the threats.

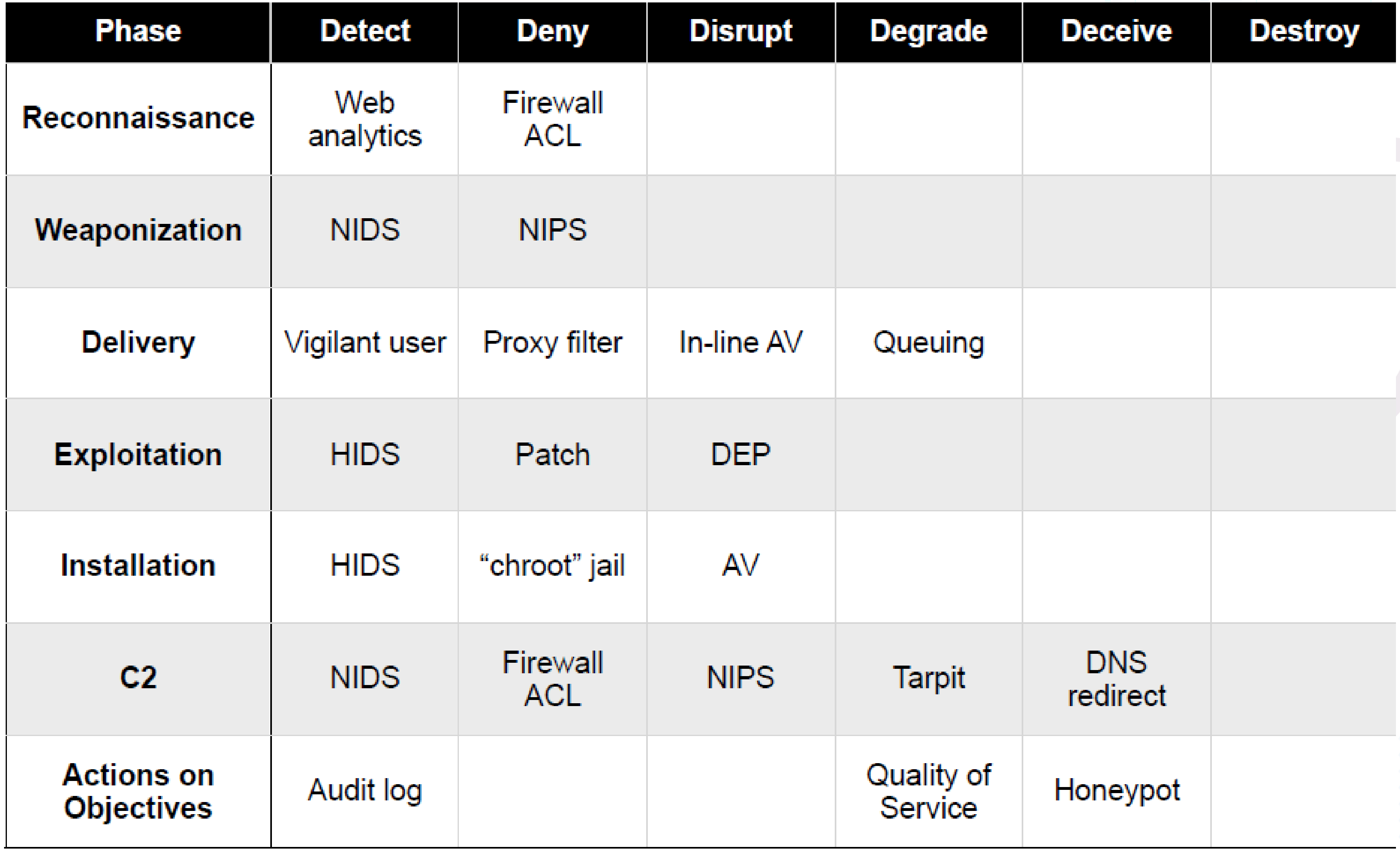
JUST ONE MITIGATION BREAKS THE CHAIN

- The defender has the advantage with the Cyber Kill Chain® solution.
- All seven steps must be successful for a cyber attack to occur.
- The defender has seven opportunities to break the chain.

Conclusion

- Defenders CAN have the advantage:
    - Better communicate and mitigate risks
    - Build true resilience
    - Meaningfully measure results
- Getting Started: Remember there is no such thing as secure, only defendable.
    - Start by thinking differently when you make changes to your processes, investments, metrics, communications with your team and leadership, staffing models, and architectures.
    - Know your threats…it’s not just about network defense anymore. it’s about defending much more like your platforms and mobile users.

Courses of Action Matrix



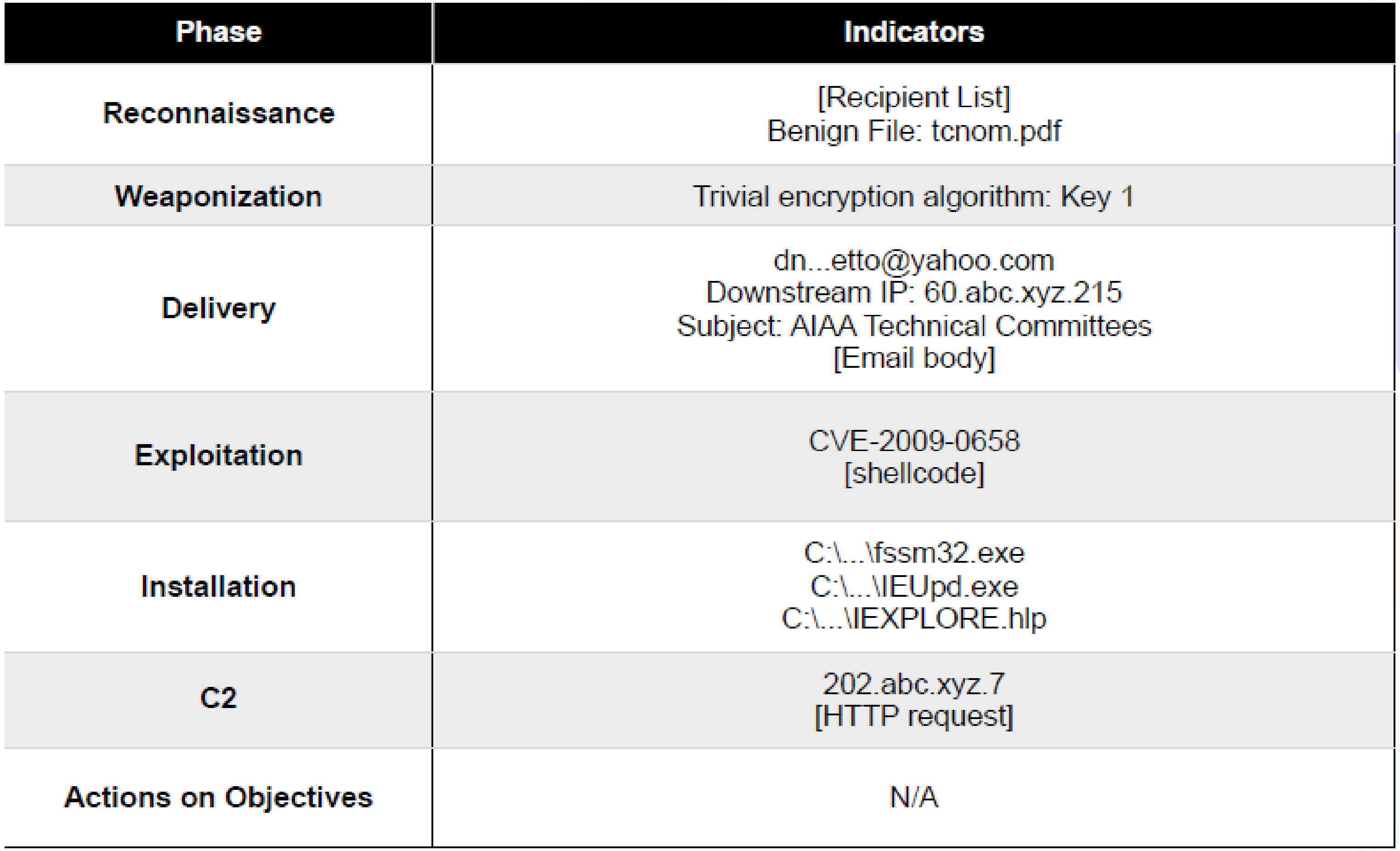
Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Example of Relative Effectiveness of Defenses Against Subsequent Intrusion Attempts

	December	March	June
Reconnaissance			
Weaponization	◇	→	◇
Delivery	◆	→	◆
Exploitation	→	◆ →	◆
Installation	◆ →	◆ →	◆
C2	◆ →	◆ →	◆
Actions on Objectives			

Legend ◇ *Detection* ◆ *Mitigation* → *Leverage new indicators*

Example Intrusion Stages



Phase	Indicators
Reconnaissance	[Recipient List] Benign File: tcnom.pdf
Weaponization	Trivial encryption algorithm: Key 1
Delivery	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]
Exploitation	CVE-2009-0658 [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp
C2	202.abc.xyz.7 [HTTP request]
Actions on Objectives	N/A