Cyber Kill Chain Controls

Boris Kogan, CISSP

Solution Architect

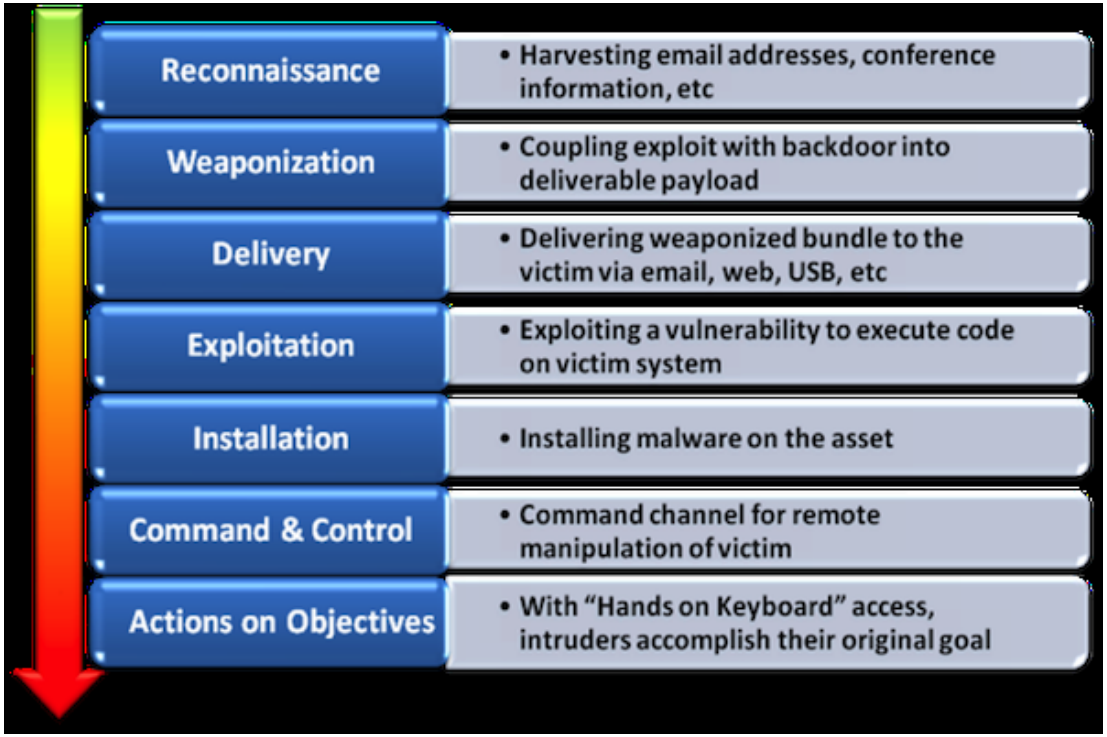
matrix | 2B SECURE@matrix

Introduction

- Created by defense giant Lockheed Martin, the term "Cyber Kill Chain" has been widely used by the security community to describe the different stages of cyber attacks.

- The following presentation will show each stage of the cyber kill chain, what are the defender objectives and what are the recommendations and actions that should be taken.

“Cyber Kill Chain”



Cyber Kill Chain Phase 1- Reconnaissance

Definition:

this phase in the Cyber Kill Chain consists of activities related to:

"Research ,identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies"

Defender Objective

> Limit Reconnaissance and reduce the attacker's ability to enumerate the target's footprint.

Targeted and Disruptive Countermeasures:

1. Determine focus of reconnaissance activity
2. Use search engines to ensure private information has not been publicly disclosed
3. Manage thresholds for source volume traffic and type
4. Perform proactive penetration testing
5. Identify internal reconnaissance

Standard Recommendations

1. Monitor external exposure
2. Install, configure and manage host and network based IDS/IPS
3. Update and maintain proper ACLs

Cyber Kill Chain Phase 2- Weaponization

Definition:

this phase consists of activities related to:

"coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.9"

Defender Objective

Interpret potential weaponization based on available information to disrupt future stages.

Targeted and Disruptive Countermeasures:

1. Application of threat intelligence
2. Use honeypots for protection and detection signatures
3. Train the incident response team to be prepared for the unexpected
4. Determine what reconnaissance took place
5. Identify weaponization characteristics

Standard Recommendations:

1. Implement a configuration management program
2. Perform formal risk assessments
3. Implement robust log monitoring
4. Actively enable internal communication

Cyber Kill Chain Phase 3- Delivery

Definition:

the Delivery phase in the Cyber Kill Chain consists of activities related to:

"Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, are email attachments, websites, and USB removable media"

Defender Objective

Identify activity as hostile and interrupt the delivery of malicious content, forcing the attacker to change tactics.

Targeted and Disruptive Countermeasures:

1. Manage browser security
2. Enable whitelist management
3. In-line anti-virus
4. Effective configuration and management of Web application firewall (WAF)
5. Automatic device fingerprinting
6. Implement a secure Web gateway (SWG)

Standard Recommendations:

1. Enable verbose logging
2. Manage peripheral security
3. Assess physical security
4. Implement professional security awareness and training
5. Implement email filtering and sanitization
6. Perform proper blacklist management
7. Install in-line anti-virus
8. Develop secure Web applications
9. Implement and maintain sound identity access management

Cyber Kill Chain Phase 4- Exploitation

Definition:

the Exploitation phase definition is:

“After the weapon is delivered to victim host, exploitation triggers intruders’ code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature which auto-executes code.”

Defender Objective:

Focus controls to minimize exploitation opportunities, reducing vulnerabilities, forcing the attacker into alternate or noisier attacks.

Targeted and Disruptive Countermeasures:

1. Implement application/process sandboxing
2. Perform proactive penetration testing
3. Remove externally facing remote administration consoles for Web applications
4. Use purpose-built tools such as the Enhanced Mitigation Experience Toolkit (EMET)
5. Implement application whitelisting
6. Implement Data Execution Prevention (DEP)
7. Perform address space layout randomization

Standard Recommendations:

1. Implement multifactor authentication
2. Eliminate unneeded services and protocols
3. Implement a patch management process
4. Implement a vulnerability management program
5. Use secure host baselines for system deployment
6. Create and test incident response plans ahead of time
7. Perform formal risk assessments

Cyber Kill Chain Phase 5- Installation

Definition:

the Installation phase definition is:

“Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.”

Defender Objective:

Inhibit the installation of malware and other actions, interfering with the attacker's ability to establish and maintain persistent access.

Targeted and Disruptive Countermeasures:

1. Only enable command-line based tools and features when necessary
2. Implement user behavior monitoring and behavioral detection/prevention capabilities
3. Implement file execution restrictions
4. For Windows environments, configure User Account Controls (UAC)
5. Configure and manage multi-layered firewalls (MLF)

Standard Recommendations:

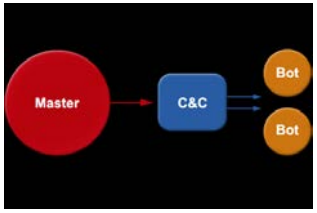
1. Enforce “least privilege” settings
2. Ensure processes and batch jobs do not use hard coded credentials
3. Assess system and database user account security

Cyber Kill Chain Phase 6- Command and Control (C2)

Definition:

the C&C phase definition is:

"Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have 'hands on the keyboard' access inside the target environment."



Defender Objective:

Disrupt the attacker's ability to retain long-term remote access, and end his hostile access.

Targeted and Disruptive Countermeasures:

1. Ensure proper network segmentation
2. Revert to disruptive tactics from reconnaissance
3. Restrict peer-to-peer (P2P) traffic
4. Set thresholds for DNS queries by a single machine
5. Block communication to the external C2 server
6. Use DNS sinkholes
7. Implement aggressive domain categorization blocking

Standard Recommendations:

1. Implement ingress and egress monitoring
2. Implement auditing/traffic logging
3. Implement log monitoring
4. Implement authenticated proxies

Cyber Kill Chain Phase 7- Actions on Objectives

Definition:

the A&O phase definition is:

“only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.”

Defender Objective:

Disrupt the attacker's ability to locate, access and extract sensitive information.

Targeted and Disruptive Countermeasures:

1. Restrict access to shared folders containing sensitive information
2. Enforce Identity Management
3. Implement Data Access Controls
4. Implement controls to detect and mitigate unauthorized lateral movement

Standard Recommendations:

1. Update the organization's **risk profile**
2. Ensure proper network **segmentation**
3. Perform regular data and **system backups**
4. Maintain layers of security for all **databases**
5. If a **DDoS** occurs be aware of other malicious activity
6. Password protect **Web application** directories
7. Implement diverse **log monitoring**

Thank You!

Boris Kogan, CISSP

Borisko@2bsecure.co.il

+972-3-6492007

matrix

2B SECURE@matrix