PART 1: THE ORIGINAL CYBER KILL CHAIN

Historical Context & Purpose

In 2011, Lockheed Martin's Computer Incident Response Team published a groundbreaking paper that changed how we think about cyberattacks. They adapted military targeting doctrine (the F2T2EA model used for physical attacks) to cyber operations, creating what we now call the Cyber Kill Chain.

The Core Insight: Every successful cyberattack follows a sequence of stages. If defenders can break the chain at any single point, the entire attack fails. This shifted security thinking from purely reactive ("we got hacked, now what?") to proactive and intelligence-driven.

The Seven Stages Explained

Stage 1: Reconnaissance

What happens: Attackers research their target to find weaknesses. This is the planning phase where they select targets, identify employees, map network infrastructure, and search for vulnerabilities.

Common techniques:

- Harvesting email addresses from LinkedIn, company websites, WHOIS databases
- Port scanning to identify open services
- Google dorking to find exposed documents or systems
- Social media research on employees
- Dumpster diving for physical documents
- Identifying third-party vendors and partners

Real example: Before the Target breach, attackers researched their HVAC vendor relationships and identified Fazio Mechanical as having weaker security but network access to Target's systems.

Defensive strategies:

- Minimize your digital footprint (what information is publicly accessible?)
- Employee security awareness training about oversharing on social media
- Monitor for reconnaissance activity using honeypots or web analytics
- Implement network monitoring to detect scanning activity
- Regular external vulnerability assessments to see what attackers see
- OSINT (Open Source Intelligence) audits on your own organization

Detection indicators: Unusual scanning patterns, multiple failed login attempts from unfamiliar sources, increased traffic to public-facing websites, suspicious DNS queries.

Stage 2: Weaponization

What happens: Attackers create the actual weapon they'll use. This typically means coupling a remote access tool (RAT) or malware with an exploit, then packaging it into a deliverable format like a malicious PDF, Office document with macros, or infected software installer.

Common techniques:

- Creating malicious documents with embedded macros
- Developing exploit kits targeting specific vulnerabilities
- Backdooring legitimate software
- Creating watering hole attack infrastructure
- Generating polymorphic malware to evade signatures

Critical understanding: This phase happens outside your network and is therefore largely invisible to you. You cannot directly detect or prevent this stage.

Defensive strategies:

- Participate in threat intelligence sharing communities
- Monitor malware repositories and dark web marketplaces
- Maintain aggressive vulnerability patching programs (remove targets from weaponization)
- Use threat intelligence feeds to understand emerging attack tools
- Conduct malware analysis in sandboxed environments
- Research adversary TTPs (Tactics, Techniques, Procedures)

Why this matters: While you can't stop weaponization, understanding common attack tools helps you prepare defenses for the next stages. If you know attackers are weaponizing CVE-2024-XXXXX, you can prioritize patching that vulnerability.

Stage 3: Delivery

What happens: The attacker transmits the weapon to the target. This is the moment of initial contact where the malicious payload moves from attacker-controlled infrastructure to your environment.

Common delivery methods:

- Email attachments (still the #1 method)
- Malicious links in emails or messages
- Compromised websites (watering holes)
- USB drives left in parking lots
- Malvertising (malicious advertisements)
- Supply chain compromises (software updates)
- Exploit kits on compromised websites

Real example: The Sony Pictures hack began with a phishing email containing a malicious link. The WannaCry ransomware spread via network exploitation of SMB vulnerabilities.

Defensive strategies:

Email security:

- Advanced email filtering and anti-spam solutions
- Attachment sandboxing (detonate attachments in isolated environments before delivery)
- Email authentication protocols: SPF, DKIM, DMARC
- Link analysis and URL rewriting
- User training to recognize phishing attempts
- Implement banners for external emails

Network security:

- Web filtering and reputation services
- Intrusion Prevention Systems (IPS)
- Network segmentation to limit blast radius
- Application whitelisting (only approved applications can run)
- USB device controls and restrictions
- Secure web gateways

Endpoint protection:

- Anti-malware solutions
- Host-based firewalls
- Browser isolation technology
- Software restriction policies

Detection indicators: Emails from unusual senders, suspicious attachments with double extensions, shortened URLs, requests for urgent action, grammatical errors in communications, requests to enable macros.

Key principle: This is one of the best stages to break the kill chain. If the weapon never reaches the target, the attack fails immediately.

Stage 4: Exploitation

What happens: The delivered weapon now executes, triggering the attacker's code. This exploits a vulnerability in the system, application, or even the human (social engineering). The vulnerability could be technical (unpatched software) or procedural (user clicks malicious link).

Common exploitation types:

- Software vulnerabilities (buffer overflows, SQL injection, remote code execution)
- Zero-day exploits (unknown vulnerabilities)
- Social engineering (tricking users into executing malware)
- Credential exploitation (using stolen or weak passwords)
- Misconfiguration exploitation (default passwords, open ports)

Real example: EternalBlue exploit (used in WannaCry) exploited Windows SMB vulnerability CVE-2017-0144. The Equifax breach exploited Apache Struts vulnerability CVE-2017-5638.

Defensive strategies:

Vulnerability management:

- Rigorous patch management programs with SLAs
- Vulnerability scanning (authenticated and unauthenticated)
- Virtual patching for systems that cannot be immediately patched
- Asset inventory management (you can't patch what you don't know about)
- Prioritize patches based on threat intelligence

Exploit prevention technologies:

- Data Execution Prevention (DEP)
- Address Space Layout Randomization (ASLR)
- Control Flow Guard (CFG)
- Sandboxing and containerization
- Application isolation

Access controls:

- Principle of least privilege
- Multi-factor authentication (MFA)
- Network segmentation
- Application-aware firewalls
- Disable unnecessary services and features

User security:

- Security awareness training
- Simulated phishing exercises
- Clear reporting procedures for suspicious activity

Detection indicators: Unexpected application crashes, unusual system behavior, new processes running, registry modifications, attempts to disable security tools, exploit attempt signatures in IDS/IPS logs.

Stage 5: Installation

What happens: The malware establishes a foothold by installing itself on the victim's system. This usually involves creating persistence mechanisms so the malware survives reboots and can maintain access even if initially discovered.

Common installation techniques:

- Registry key modifications (Run keys, services)
- Scheduled tasks creation
- DLL hijacking
- Rootkit installation
- Boot sector modification
- Creating new user accounts
- Web shell installation on servers

Real example: The Carbanak malware created Windows services for persistence. APT groups commonly install remote access trojans (RATs) like Cobalt Strike beacons.

Defensive strategies:

Endpoint Detection and Response (EDR):

- Monitor file system changes
- Track process creation and execution
- Detect persistence mechanism creation
- Behavioral analysis of endpoint activity
- Automated threat hunting on endpoints

System hardening:

- Application whitelisting (only approved applications can install)
- Disable PowerShell for regular users
- Implement AppLocker or similar tools
- Restrict admin privileges
- Enable Windows Defender Application Control

Monitoring:

- File Integrity Monitoring (FIM)
- Registry monitoring
- Service creation alerts
- Scheduled task monitoring
- User account creation logging
- Host-based Intrusion Detection Systems (HIDS)

SIEM correlation:

- Aggregate logs from multiple sources
- Create correlation rules for suspicious installation patterns
- Alert on known malware signatures
- Baseline normal system behavior

Detection indicators: New services created, registry modifications, new scheduled tasks, unexpected file drops in system directories, new user accounts, changes to startup folders, unsigned drivers loading.

Critical concept: If you catch the attack here, you prevent the attacker from achieving persistence. Without persistence, they lose access if the system reboots or the initial process terminates.

Stage 6: Command & Control (C2)

What happens: The installed malware "phones home" to establish communication with attacker-controlled infrastructure. This channel allows attackers to send commands, receive stolen data, update malware, and control the compromised system remotely.

Common C2 techniques:

- HTTP/HTTPS beacons (looks like normal web traffic)
- DNS tunneling (hiding data in DNS queries)
- IRC or custom protocols
- Social media platforms (Twitter, Reddit for covert channels)
- Cloud services (Dropbox, Google Drive for dead drop storage)
- Fast Flux networks (rapidly changing IP addresses)
- Domain Generation Algorithms (DGA) for backup C2 domains

Real example: Emotet malware uses HTTPS for C2 communication, making it harder to detect. APT29 (Cozy Bear) has used legitimate cloud services for C2 to blend with normal traffic.

Defensive strategies:

Network security:

- Egress filtering (control outbound traffic, not just inbound)
- DNS filtering and sinkholes
- Proxy servers with SSL/TLS inspection
- Firewall rules blocking unusual outbound connections
- Network segmentation preventing unauthorized outbound connections

Detection and analysis:

- Network behavior analysis tools
- Beaconing detection (regular, periodic communications)
- DNS query analysis for suspicious patterns
- Monitoring for connections to recently registered domains
- Tracking connections to high-risk countries/regions
- Protocol analysis (detecting non-HTTP traffic on port 80)

Threat intelligence:

- Maintain blocklists of known C2 infrastructure
- Subscribe to threat intelligence feeds
- Participate in information sharing organizations (ISACs)
- Implement STIX/TAXII threat intelligence platforms

Network Detection and Response (NDR):

- Deep packet inspection
- Traffic pattern analysis
- Encrypted traffic analysis
- Lateral movement detection

Detection indicators: Regular beaconing patterns, connections to unusual ports, DNS queries to algorithmically generated domains, large data uploads, connections to newly registered domains, traffic to known malicious IPs.

Key insight: Breaking the C2 link severely limits the attacker. Without command and control, they cannot exfiltrate data, move laterally, or adjust their tactics. Many sophisticated attacks can be neutralized at this stage.

Stage 7: Actions on Objectives

What happens: The attacker finally accomplishes their goal. This could be data theft, system destruction, ransomware deployment, cryptocurrency mining, espionage, or using your system as a launching pad for further attacks.

Common objectives:

- Data exfiltration (intellectual property, customer data, credentials)
- Financial theft or fraud
- Ransomware encryption
- System destruction or sabotage
- Cryptocurrency mining
- Establishing persistence for future operations
- Lateral movement to other systems
- Privilege escalation
- Creating backdoors for other threat actors

Real example: In the Target breach, attackers exfiltrated 40 million credit card numbers. NotPetya ransomware caused $10 billion in damages through system destruction. APT groups often spend months conducting espionage before exfiltration.

Defensive strategies:

Data Loss Prevention (DLP):

- Monitor and block sensitive data leaving the network
- Classify data by sensitivity
- Encrypt sensitive data at rest and in transit
- Monitor for large file transfers
- Block unauthorized cloud storage usage
- Email DLP scanning

Access controls:

- Least privilege principle strictly enforced
- Segregation of duties
- Multi-factor authentication everywhere
- Privileged Access Management (PAM) solutions
- Just-in-time access provisioning

Lateral movement prevention:

- Network microsegmentation
- Disable NTLM and use Kerberos
- Remove local admin rights
- Implement jump servers/bastion hosts
- Application-level segmentation

Detection and response:

- User and Entity Behavior Analytics (UEBA)
- Abnormal data access patterns
- Unusual login times or locations
- Mass file modifications (ransomware indicator)
- Database query anomalies
- Privilege escalation attempts

Backup and recovery:

- Immutable backups (cannot be encrypted by ransomware)
- Offline backup copies
- Regular backup testing
- Disaster recovery planning
- Snapshot technologies

Incident response:

- Documented playbooks
- Incident response team ready
- Forensic tools prepared
- Legal and communication plans
- Automated containment capabilities

Detection indicators: Large data transfers, accessing files outside normal patterns, privilege escalation attempts, shadow copy deletion (ransomware), mass file encryption, unusual database queries, connections to file-sharing sites.