PART 2: THE UNIFIED KILL CHAIN

Why Was It Created?

By 2017, cybersecurity professionals recognized that the original Cyber Kill Chain, while groundbreaking, had limitations. Paul Pols from Fox-IT and Leiden University developed the Unified Kill Chain to address these gaps.

Key limitations it addresses:

- The original is too linear (attackers don't always follow a straight path)
- Doesn't adequately cover insider threats
- Limited coverage of lateral movement and privilege escalation
- Not detailed enough for modern, complex attacks
- Doesn't reflect iterative, non-deterministic attack patterns

Structure: Three Cycles

The Unified Kill Chain organizes 18 attack phases into three cycles that can repeat and interconnect. Attackers may loop through these cycles multiple times.

CYCLE 1: IN (Initial Foothold)

This cycle focuses on gaining that crucial first access to the target environment.

1. Reconnaissance

Same as the original kill chain - researching targets, identifying vulnerabilities, and gathering intelligence.

2. Weaponization

Creating or acquiring the tools needed for the attack.

3. Delivery

Transmitting the attack tools to the target.

4. Social Engineering

What's new: This is now explicitly separated as its own phase because it's so critical to modern attacks.

Techniques:

- Phishing (email-based deception)
- Vishing (voice/phone-based)
- Smishing (SMS-based)
- Pretexting (creating false scenarios)
- Baiting (offering something enticing)
- Quid pro quo (offering service in exchange for information)
- Tailgating (physical access following authorized person)

Defenses:

- Comprehensive security awareness training
- Simulated social engineering campaigns
- Clear verification procedures
- Multi-person authorization for sensitive actions
- Psychological awareness training
- Reporting mechanisms that are easy and non-punitive

5. Exploitation

Triggering vulnerabilities to execute attacker code.

6. Persistence

What's new: Explicitly separated from installation to emphasize its importance.

Techniques beyond basic installation:

- Multiple persistence mechanisms (redundancy)
- Fileless malware (living in memory only)
- Registry-based persistence
- WMI event subscriptions
- Golden ticket attacks (Kerberos)
- Skeleton key attacks
- Cloud account creation

Defenses:

- Monitor all persistence mechanisms continuously
- Implement tamper protection on security tools
- Use Windows Attack Surface Reduction rules
- Credential guard and device guard
- Regular forensic analysis
- Golden image rebuilding for compromised systems

7. Defense Evasion

What's new: Recognizes that modern attackers actively work to avoid detection.

Evasion techniques:

- Disabling security tools
- Clearing logs
- Code obfuscation
- Timestomping (changing file timestamps)
- Process injection
- Living-off-the-land binaries (LOLBins) - using legitimate Windows tools
- Mimicking normal behavior
- Sandbox detection and evasion
- Polymorphic and metamorphic malware

Defenses:

- Tamper-proof security tools
- Write-once log storage (WORM)
- Behavioral detection (can't evade what you are)
- Memory analysis
- PowerShell logging and monitoring
- Endpoint Detection and Response (EDR) with behavioral analysis
- Deception technology (honeypots, honeytokens)
- Application whitelisting

8. Command & Control

Establishing communication channels with attacker infrastructure.

Cycle 1 Summary: At this point, the attacker has a foothold in your environment. They can communicate with their infrastructure and have mechanisms to maintain access. Now they typically move to Cycle 2.

CYCLE 2: THROUGH (Network Propagation)

This cycle represents the attacker moving through your network, escalating privileges, and spreading their access. This is where many modern attacks spend the most time.

9. Pivoting

What it means: Using the compromised system as a launching point to attack other systems. The initial compromised system becomes a "pivot point" for reaching deeper into the network.

Techniques:

- Port forwarding
- SSH tunneling
- VPN establishment
- Using compromised systems as proxy servers
- Jump boxes
- Protocol tunneling

Defenses:

- Network segmentation (critical!)
- Microsegmentation with Zero Trust
- Monitor for unusual internal network connections
- Detect tunneling protocols
- Restrict lateral network communication
- Internal firewalls between network zones

10. Discovery

What it means: Once inside, attackers map the internal environment to understand what's available.

What they look for:

- Network topology
- Active Directory structure
- User accounts and groups
- File shares and databases
- Backup locations
- Security tool placement
- High-value targets (crown jewels)
- Domain controllers
- Administrator accounts

Common tools:

- Network scanners (nmap, Angry IP Scanner)
- AD enumeration tools (BloodHound, PowerView)
- Built-in Windows commands (net view, nltest, dsquery)
- SMB enumeration
- LDAP queries

Defenses:

- Monitor for reconnaissance activity internally
- Honeypots and honeytokens inside the network
- Alert on AD enumeration activity
- Restrict LDAP queries
- Monitor for unusual network scanning
- Detect BloodHound and similar tool usage
- Segment administrative tools access

Detection indicators: Unusual DNS queries, port scans from internal hosts, AD enumeration commands, access to multiple file shares in short time, PowerView or BloodHound activity.

11. Privilege Escalation

What it means: Attackers gain higher-level permissions to access more sensitive resources.

Common techniques:

- Exploiting vulnerable services running as SYSTEM
- Kernel exploits
- DLL hijacking
- Token impersonation
- Credential dumping (Mimikatz)
- Pass-the-hash attacks
- Pass-the-ticket (Kerberos)
- Exploiting misconfigured services
- Abusing scheduled tasks
- SAM database extraction

Defenses:

- Principle of least privilege everywhere
- Remove local admin rights from users
- Patch privilege escalation vulnerabilities
- Credential Guard (Windows)
- LSA Protection
- Protected Users group in AD
- Admin Tier model (separate admin accounts for different privilege levels)
- Just-in-time administration
- Monitor for Mimikatz and similar tools
- Alert on suspicious privilege changes
- Application whitelisting

Detection indicators: Access token manipulation, LSASS memory access, SAM database access, new admin accounts created, users added to privileged groups, suspicious scheduled tasks.

12. Execution

What it means: Running additional malicious code and tools on compromised systems.

Techniques:

- PowerShell scripts
- Windows Management Instrumentation (WMI)
- Remote service execution
- Scheduled tasks
- Registry run keys
- DLL injection
- Process hollowing
- Scripting interpreters (Python, JavaScript)

Defenses:

- PowerShell logging (script block, module, transcription)
- Constrained Language Mode for PowerShell
- Application control policies
- Monitor WMI activity
- Code signing requirements
- Behavioral monitoring for execution patterns
- EDR solutions with execution tracking

13. Credential Access

What it means: Stealing usernames, passwords, hashes, and tokens to enable further access.

Techniques:

- Keylogging
- Credential dumping from memory (LSASS)
- Password spraying
- Brute force attacks
- Kerberoasting
- AS-REP roasting
- DCSync attacks
- NTDS.dit extraction
- Exploiting password storage (browsers, applications)
- Man-in-the-middle attacks
- Forced authentication

Defenses:

- Multi-factor authentication (MFA) everywhere
- Credential Guard
- Remote Credential Guard
- Protected Users security group
- Disable NTLM authentication
- Service account password rotation
- Managed service accounts (gMSA)
- Password managers (reduces credential reuse)
- Monitor for Mimikatz, Kerberoasting, DCSync
- Honeypot credentials (never used legitimately)
- Disable WDigest authentication
- Monitor authentication logs for anomalies

Detection indicators: LSASS process access, suspicious authentication patterns, Kerberos ticket anomalies, DCSync activity, multiple failed logins followed by success.

14. Lateral Movement

What it means: Moving from one compromised system to others within the network.

Techniques:

- Remote Desktop Protocol (RDP)
- SMB/Windows Admin Shares (C$, ADMIN$)
- PsExec and similar tools
- WMI remote execution
- PowerShell remoting
- Pass-the-hash
- Pass-the-ticket
- Overpass-the-hash
- Remote services
- Exploitation of trusted relationships

Defenses:

- Network segmentation (cannot emphasize enough)
- Disable NTLM where possible
- Local Admin Password Solution (LAPS)
- Restrict RDP access
- Disable SMB v1
- Monitor for lateral movement tools
- Require MFA for administrative access
- Use Jump servers/Privileged Access Workstations (PAW)
- Network access control
- Monitor for Pass-the-Hash indicators
- Detect unusual logon patterns (user logs into 50 systems)

Detection indicators: Same user accessing many systems rapidly, administrative tools used from unexpected locations, unusual RDP connections, WMI/PowerShell remoting from non-admin workstations, PsExec execution.

Cycle 2 Summary: The attacker has now spread through your network, escalated their privileges, stolen credentials, and can access multiple systems. They're positioned to achieve their objectives. This leads to Cycle 3.

CYCLE 3: OUT (Actions on Objectives)

This cycle represents the attacker achieving their actual goals.

15. Collection

What it means: Gathering the data or resources that the attacker actually wants.

Techniques:

- Automated data collection scripts
- Staged collection (gathering data to a central location before exfil)
- Screen capture
- Keylogging
- Audio recording
- Clipboard data
- Email collection
- Database queries
- Cloud service access
- Archive file creation (compressing stolen data)

Defenses:

- Data Loss Prevention (DLP)
- File access monitoring
- Abnormal access pattern detection
- Database activity monitoring
- Monitor for staging locations
- Email monitoring for bulk downloads
- Cloud Access Security Brokers (CASB)
- User behavior analytics

Detection indicators: Accessing many files rapidly, database dumps, large archive file creation, unusual file copying, access to files outside normal scope.

16. Exfiltration

What it means: Transferring collected data outside the organization.

Techniques:

- HTTPS uploads (encrypted, looks legitimate)
- DNS tunneling
- Email with attachments
- Cloud storage services
- FTP/SFTP
- Physical media
- Steganography (hiding data in images)
- Out-of-band channels
- Scheduled transfers during off-hours

Defenses:

- Data Loss Prevention (DLP) with content inspection
- Egress filtering
- Monitor for large outbound transfers
- DNS query analysis
- Cloud service monitoring
- Email attachment scanning
- USB device control
- Bandwidth monitoring
- Time-based alerting (large transfers at 3 AM)
- Encrypt sensitive data (makes exfiltration less valuable)

Detection indicators: Large outbound data transfers, connections to file-sharing sites, unusual DNS query volumes, encrypted channels to unknown destinations, data transfers during off-hours.

17. Impact

What it means: Actions that disrupt, destroy, or alter systems and data.

Types of impact:

- Data destruction
- Ransomware encryption
- Defacement
- Denial of service
- Data manipulation/integrity attacks
- Firmware corruption
- Resource hijacking (cryptomining)
- Supply chain poisoning

Defenses:

- Immutable backups (offline, air-gapped)
- Snapshot technologies
- File integrity monitoring
- Backup testing (verify you can restore)
- Incident response capabilities
- Automated containment
- System hardening
- Change management controls
- Digital signatures for critical files

Detection indicators: Mass file modifications, file encryption, shadow copy deletion, backup deletion, system performance degradation, unexpected shutdowns.

18. Objectives

What it means: The final realization of the attacker's goals - whether that's financial gain, espionage, sabotage, or something else.

This is where you assess the full scope of damage and begin recovery.