CHAPTER 1

The Threat Landscape

Chapter Overview

01

Attacker Motivations

IP theft, financial fraud, espionage, hacktivism, and more

02

Attack Methods

DoS/DDoS, ransomware, phishing, web & wireless attacks

03

Anatomy of an Attack

Recon → Exploitation → Expansion → Exfiltration → Clean-Up

04

The Modern Adversary

Credential theft and advanced persistent threats

Attacker Motivations

Why do threat actors attack?

Attacker Motivations — Overview

Attribution is difficult — motivations often unclear during response

Three broad categories: intelligence (espionage), financial gain, disruption

Understanding motivation predicts attacker behavior and TTPs

Nation-states, organized crime, and insiders all present threats

IP Theft & Supply Chain Attacks

Intellectual Property Theft

Targets trade secrets, proprietary tech, recipes

Stolen IP sold to competitors or used by nation-states

Attacker may extort victim to prevent disclosure

Common target: R&D organizations

Supply Chain Attack

Attack the vendor/supplier, not the final target directly

Embed malware in trusted software updates

NotPetya: via accounting software → $10B+ damages

Also: corrupting manufactured components

Financial Fraud & Extortion

Financial Fraud

Theft of credit card / banking credentials

Phishing of online banking logins

Compromise of ATM and SWIFT systems

One of the oldest and most persistent motivations

Extortion

Ransomware: encrypt data, demand payment

DDoS threats: pay or be taken offline

Sextortion: intimate photos obtained via RATs

Any sensitive data can be an extortion vehicle

Espionage & Power

Espionage

Nation-state or corporate intelligence gathering

Target: proprietary tech, customer data, strategies

Nation-states maintain profiles of critical systems

Insider threats: disgruntled employees selling data

Power

Cyber power used alongside kinetic warfare

Disrupting communications and infrastructure

Threat to electric grids as conflict deterrent

Real-world examples: Estonia, Ukraine attacks

Hacktivism & Revenge

Hacktivism

Cyberattacks as political protest

Website defacement to express views

DDoS attacks to take targets offline

Publishing embarrassing or incriminating info

Revenge

Disgruntled or former employees

Insiders with deep knowledge of systems

Personal grievances against individuals or orgs

Often publicized on social media before/after

Attack Methods

How do attackers reach their goals?

DoS/DDoS & Worms

DoS and DDoS

Deny service to legitimate users

Distributed: coordinated from many systems (botnets)

Used for extortion, hacktivism, competitive disruption

Overwhelms bandwidth, CPU, or application layers

Worms

Self-replicating — spreads without user action

Exploits vulnerabilities to propagate across networks

Can carry ransomware, backdoors, or wipers as payload

Example: WannaCry used the EternalBlue exploit

Ransomware & Phishing

Ransomware

Encrypts files; demands payment for decryption key

Targets individuals, hospitals, governments, enterprises

Double extortion: encrypt AND threaten to publish data

RaaS (Ransomware-as-a-Service) lowers skill bar

Phishing & Spear Phishing

Deceptive emails to steal credentials or deliver malware

Spear Phishing: targeted, highly personalized messages

Vishing (phone) and **Smishing** (SMS) variants exist

Primary delivery mechanism for most malware

Ransomware attack screen — a common endpoint for web-based attack chains

Watering Hole & Web Attacks

Watering Hole: compromise websites that targets frequently visit

Drive-by downloads infect visitors without interaction

SQL Injection: extract or modify database content via crafted queries

Cross-Site Scripting (XSS): inject malicious scripts into web pages

Compromised web apps provide persistence and lateral movement

Wireless & Network Attacks

Wireless Attacks

Rogue access points mimic legitimate Wi-Fi

WPA2 handshake capture for offline cracking

Evil twin attacks intercept wireless traffic

Deauth floods disconnect legitimate users

Sniffing & Man-in-the-Middle

Passive: capture unencrypted network traffic

Active MitM: insert attacker between client and server

ARP spoofing redirects traffic on local network

SSL stripping downgrades HTTPS to HTTP

Crypto Mining & Password Attacks

Crypto Mining (Cryptojacking)

Hijack victim's CPU/GPU to mine cryptocurrency

Silent — victim sees only degraded performance

Delivered via malware, browser scripts, or cloud compromise

Password Attacks

Brute force: try all combinations

Credential stuffing: reuse known breached passwords

Password spraying: common passwords across many accounts

Kerberoasting: request service tickets for offline cracking

Anatomy of an Attack

The five stages of a modern intrusion

Attack Lifecycle Overview

Modern attacks follow predictable, repeatable stages

Understanding stages helps defenders detect and interrupt attacks early

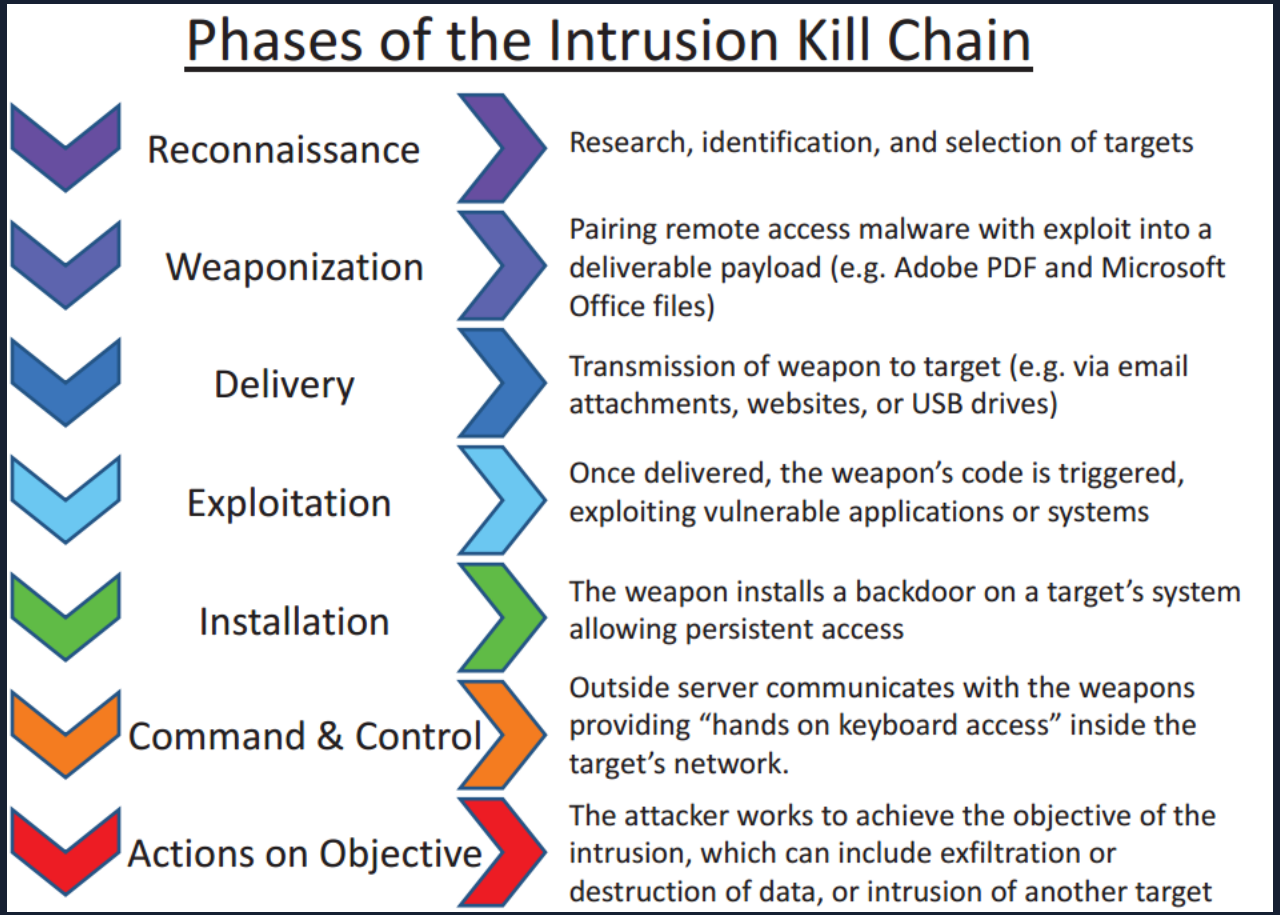
Stage 1: **Reconnaissance** — gather information about the target

Stage 2: **Exploitation** — gain initial access

Stage 3: **Expansion/Entrenchment** — grow foothold and persist

Stage 4: **Exfiltration/Damage** — achieve mission objectives

Stage 5: **Clean Up** — erase evidence of intrusion



Intrusion Kill Chain — Hutchins, Cloppert & Amin (Lockheed Martin, 2011)

Reconnaissance & Exploitation

Reconnaissance

Passive: OSINT, DNS, LinkedIn, job postings

Active: port scans, vulnerability scans, web crawling

Goal: identify targets, tech stack, personnel, vulns

More recon = more targeted and effective attack

Exploitation

Leverage discovered vulnerability to gain access

Methods: phishing, unpatched CVEs, web app flaws

Often targets the weakest link — users

Initial foothold may be low-privilege; escalation follows

Expansion/Entrenchment & Exfiltration

Expansion / Entrenchment

Lateral movement: pivot from beachhead to other systems

Privilege escalation: gain admin or domain admin rights

Persistence: backdoors, scheduled tasks, registry keys

Goal: own the domain, maximize access and resilience

Exfiltration / Damage

Steal sensitive data: IP, credentials, PII

Deploy **ransomware** across the environment

Destructive **wipers** (e.g., NotPetya, Shamoon)

Achieve the mission objective

Clean Up

Sophisticated attackers remove evidence of their presence

Delete log entries, shell histories, malware artifacts

Modify timestamps to confuse forensic timelines

Remove persistence mechanisms after objective achieved

Incident responders must preserve evidence early — memory is volatile

Collect memory and logs before remediation begins

The Modern Adversary

Sophisticated, persistent, credential-focused

The Modern Adversary

Nation-state and organized crime TTPs have converged

Code from attack campaigns is routinely reused by other threat actors

Attacks shifted from static malware to living-off-the-land (LotL)

Living off the Land

Attackers use built-in OS tools: PowerShell, WMI, PsExec

Behavioral detection is critical — signatures miss modern threats

Persistent access maintained for months before detection

Credentials: The Keys to the Kingdom

Credentials are the #1 target of modern attackers

Valid credentials bypass most security controls invisibly

Password hashes allow lateral movement without knowing plaintext

Pass-the-Hash, Pass-the-Ticket, Kerberoasting all target credentials

Multi-factor authentication (MFA) is the most impactful defensive control

Privileged accounts (Domain Admin) are the highest-value targets

Conclusion

Every organization is a potential target — size doesn't provide protection

Attackers are motivated by espionage, financial gain, and disruption

Modern attacks follow predictable stages: recon → exploitation → clean-up

Credentials are the primary target of modern adversaries

Understanding attacker methods helps defenders prepare and respond

Knowledge Check