Lecture 2: Threat Landscape and Attack Vectors

Theme: Information Security Fundamentals
Technical University of Moldova
Lecturer: Maxim Masiutin, Associate Professor

Introduction

Welcome back. In our previous lecture, we established the fundamental concepts of information security, including the CIA Triad, assets, threats, vulnerabilities, and risks. Today, we will take a deep dive into the threat landscape, examining who attacks our systems, why they do it, and how they carry out their attacks.

Understanding your adversary is essential for effective defense. As Sun Tzu wrote in "The Art of War," if you know the enemy and know yourself, you need not fear the result of a hundred battles. In cybersecurity, we must understand threat actors, their motivations, their capabilities, and their methods.

The threat landscape has evolved dramatically in recent years. According to the 2025 Global Threat Report by CrowdStrike, a cybersecurity company, cloud intrusions increased 136 percent in the first half of 2025 compared to all of 2024. Interactive intrusions, where attackers operate hands-on-keyboard, increased 27 percent year-over-year, and remarkably, 81 percent of these intrusions were malware-free. Attackers are becoming more sophisticated, relying less on traditional malware and more on living-off-the-land techniques.

Let us begin by classifying the actors who pose threats to our organizations.

Part 1: Threat Actor Classification

A **threat actor** is any individual or group that poses a potential threat to an organization's security. Threat actors vary widely in their motivations, capabilities, resources, and targets. Understanding these differences helps us anticipate and defend against their attacks.

Nation-State Actors

Nation-state actors are government-sponsored groups that conduct cyber operations for political, economic, or military objectives. They represent the most sophisticated and well-resourced threat actors.

Characteristics:

- Virtually unlimited resources (funding, personnel, time)
- Access to advanced tools, including zero-day exploits
- Long-term, patient operations lasting months or years
- Sophisticated operational security to avoid attribution
- State-level legal protection

Motivations:

- Espionage (stealing government secrets, intellectual property)
- Sabotage (disrupting critical infrastructure)
- Influence operations (manipulating public opinion)
- Economic advantage (stealing trade secrets)

Examples by MITRE ATT&CK groups classification:

- **APT28 (Fancy Bear)**: Associated with Russian military intelligence, targeted US elections, Olympic committees, and NATO countries
- **APT41**: Chinese state-sponsored group that conducts both espionage and financially motivated operations
- **Lazarus Group**: North Korean group known for the Sony Pictures hack and WannaCry ransomware
- **APT33**: Iranian group targeting aerospace and energy sectors

The term APT stands for **Advanced Persistent Threat**. APT groups are characterized by their advanced capabilities and their persistence in pursuing objectives over extended periods. They often maintain access to compromised networks for years before being detected.

There are no groups explicitly classified as North American or Western European government-sponsored in MITRE ATT&CK. This asymmetry exists because MITRE ATT&CK is built from open-source Western threat intelligence reporting. Western vendors and governments publish extensive reports attributing adversary activity to Russian, Chinese, Iranian, and North Korean state actors often backed by indictments and sanctions. Comparable public attribution of US, UK, or other Five Eyes offensive operations is almost nonexistent in the CTI ecosystem, despite well-documented capabilities (Shadow Brokers leaks, Snowden disclosures, Vault 7, etc.). So the framework reflects what gets publicly reported and attributed, not the actual distribution of state-sponsored cyber operations globally.

Not explicitly attributed by MITRE can be the following examples:

- **Equation (G0020)**: widely attributed by Kaspersky, a cybersecurity and antivirus company, and other researchers to the US NSA/TAO (Tailored Access Operations). MITRE's description deliberately omits any government attribution, saying only "a sophisticated threat group that employs multiple remote access tools."
- **Strider / ProjectSauron (G0041)**: suspected by researchers of being linked to a Western intelligence agency (possibly US or allied). Again, MITRE provides no government attribution.

Cybercriminals

Cybercriminals are motivated primarily by financial gain. They range from individual hackers to organized crime syndicates with business-like structures.

Characteristics:

- Financially motivated
- Opportunistic target selection (low-hanging fruit)
- Use of criminal infrastructure (bulletproof hosting, money laundering)
- Increasingly professional operations
- May purchase tools and services from other criminals

Common activities:

- **Ransomware**: Encrypting victim data and demanding payment
- **Business Email Compromise**: Tricking employees into transferring funds
- **Credit card theft**: Stealing and selling payment card data
- **Credential harvesting**: Stealing and selling login credentials
- **Cryptojacking**: Using victim systems to mine cryptocurrency

The cybercrime economy has become highly organized. There are marketplaces where criminals buy and sell stolen data, hacking tools, and even access to compromised systems. Ransomware-as-a-Service operations provide ransomware to affiliates who conduct the attacks, splitting the proceeds.

Hacktivists

Hacktivists are individuals or groups who use hacking to promote political or social causes. The term combines "hacker" and "activist."

Characteristics:

- Ideologically motivated
- Seek publicity for their cause

- Variable technical capabilities
- Often loosely organized
- May have broad target selection

Common activities:

- Website defacement to spread messages
- DDoS (Distributed Denial of Service) attacks to disrupt operations
- Data leaks to embarrass targets
- Doxing (revealing private information about individuals)

Examples:

- **Anonymous**: Decentralized collective known for attacks on governments and corporations
- **LulzSec**: Group that targeted Sony, CIA, and other organizations
- Various groups active during geopolitical conflicts

Insider Threats

Insider threats come from individuals within the organization who misuse their authorized access. They may be current or former employees, contractors, or business partners.

Types of insiders:

- **Malicious insiders**: Deliberately cause harm for revenge, financial gain, or ideology
- **Negligent insiders**: Accidentally cause harm through carelessness or lack of awareness
- **Compromised insiders**: Have their credentials stolen by external attackers

Characteristics:

- Already have authorized access
- Know organizational systems and processes
- Can bypass many security controls
- Actions may appear legitimate
- Difficult to detect

According to the Verizon 2024 Data Breach Investigations Report, insider threats are involved in approximately 20-30 percent of data breaches, but they often cause the most damage because insiders know where valuable assets are located.

Script Kiddies

Script kiddies are inexperienced attackers who use pre-built tools without understanding how they work. Despite their limited skills, they can still cause significant damage.

Characteristics:

- Low technical sophistication
- Use readily available tools
- Often motivated by curiosity or desire for recognition
- Opportunistic target selection
- May accidentally cause more damage than intended

While individual script kiddies pose limited threats, their large numbers mean they collectively conduct many attacks. They often serve as a gateway for developing more sophisticated attackers.

Competitors

Competitor espionage involves businesses spying on rivals to gain competitive advantage.

Activities:

- Stealing trade secrets and intellectual property
- Obtaining customer lists and pricing information
- Monitoring strategic plans
- Hiring employees to extract knowledge

This threat is often underestimated but can cause significant business harm.

Part 2: Attack Vectors

An **attack vector** is the path or method an attacker uses to gain access to a target system. Understanding attack vectors helps us implement appropriate defenses.

Network-Based Attacks

Network attacks target the communication infrastructure connecting systems.

External network attacks:

- Port scanning to identify running services

- Exploitation of vulnerable network services
- Man-in-the-middle attacks on network traffic
- DNS (Domain Name System) attacks (spoofing, cache poisoning)
- DDoS attacks to overwhelm network resources

Internal network attacks:

- ARP (Address Resolution Protocol) spoofing to redirect traffic
- VLAN (Virtual Local Area Network) hopping to access segmented networks
- Rogue devices on the network
- Unauthorized network sniffing

Wireless attacks:

- Evil twin access points
- WPA2/WPA3 cracking attempts
- Bluetooth attacks
- RF jamming

Application-Based Attacks

Application attacks target software vulnerabilities.

Web application attacks:

- SQL injection: Inserting malicious database queries
- Cross-site scripting (XSS): Injecting malicious scripts
- Cross-site request forgery (CSRF): Forcing authenticated users to perform actions
- Remote code execution: Exploiting flaws to run arbitrary code
- Path traversal: Accessing unauthorized files

API (Application Programming Interface) attacks:

- Broken authentication
- Excessive data exposure
- Mass assignment vulnerabilities
- Injection attacks

Software vulnerabilities:

- Buffer overflows
- Use-after-free bugs
- Integer overflows
- Race conditions

Physical Attacks

Physical attacks require physical presence at or near the target.

Examples:

- Stealing devices (laptops, phones, USB drives)
- Shoulder surfing to observe passwords
- Dumpster diving for discarded documents
- Tailgating through secure doors
- Installing hardware keyloggers
- USB drop attacks (leaving malicious USB drives)

Physical security is often overlooked but remains critical.

Social Engineering Attacks

Social engineering exploits human psychology rather than technical vulnerabilities. We will cover this in detail in a later lecture, but key vectors include:

- Phishing emails
- Voice phishing (vishing)
- SMS phishing (smishing)
- Pretexting and impersonation
- Baiting

Supply Chain Attacks

Supply chain attacks compromise an organization by attacking its suppliers, vendors, or software providers. These attacks have increased dramatically in recent years.

Types:

- **Software supply chain**: Compromising software during development or distribution
- **Hardware supply chain**: Implanting malicious components in hardware
- **Service provider attacks**: Compromising managed service providers to reach their clients

Famous examples:

- **SolarWinds (2020)**: Attackers compromised the Orion software update from SolarWinds, an IT infrastructure management company, affecting 18,000 organizations including US government agencies

- **Kaseya (2021)**: Ransomware distributed through compromised remote management software from Kaseya, an IT management software provider
- **Log4Shell (2021)**: Vulnerability in widely-used logging library affected countless applications

A new framework called **OSC&R (Open Software Supply Chain Attack Reference)** has been created specifically to address software supply chain security threats. It provides an MITRE ATT&CK-like approach for understanding attacker behaviors in supply chain contexts.

Cloud-Based Attack Vectors

As organizations move to the cloud, new attack vectors emerge.

Cloud-specific attacks:

- Misconfigured cloud storage (exposed S3 buckets)
- Compromised cloud credentials
- Insecure APIs
- Cross-tenant attacks in multi-tenant environments
- Serverless function vulnerabilities
- Container escapes

Cloud intrusions have increased dramatically. Many attack sequences now unfold in cloud control planes rather than on traditional endpoints, requiring new defensive approaches.

Part 3: The Vulnerability Lifecycle

Understanding how vulnerabilities are discovered, disclosed, and exploited helps us manage risk effectively.

Vulnerability Discovery

Vulnerabilities may be discovered by:

- Security researchers (ethical)
- Product vendors
- Government agencies
- Cybercriminals
- Bug bounty hunters

Responsible Disclosure

When researchers discover vulnerabilities, responsible disclosure practices suggest:

1. Report the vulnerability privately to the vendor
2. Give the vendor reasonable time to develop a patch (typically 90 days)
3. Coordinate public disclosure after a patch is available
4. If the vendor fails to act, disclose to protect the public

Zero-Day Vulnerabilities

A **zero-day vulnerability** is a flaw unknown to the vendor or public. Zero-day exploits target these vulnerabilities before patches exist.

Zero-days are highly valuable:

- Nation-states stockpile them for offensive operations
- Cybercriminals pay hundreds of thousands of dollars for them
- Bug bounty programs offer substantial rewards

Once a zero-day is discovered and used, it becomes known and eventually patched, losing its value.

CVE System

The **Common Vulnerabilities and Exposures (CVE)** system provides standardized identifiers for known vulnerabilities.

Format: CVE-YEAR-NUMBER (e.g., CVE-2024-12345)

CVE records include:

- Description of the vulnerability
- Affected products and versions
- References to advisories and patches

The CVE database is maintained by MITRE Corporation and is freely accessible at cve.org.

CVSS Scoring

The **Common Vulnerability Scoring System (CVSS)** provides numerical scores indicating vulnerability severity.

CVSS 3.1 scores range from 0.0 to 10.0:

- 0.0: None

- 0.1-3.9: Low
- 4.0-6.9: Medium
- 7.0-8.9: High
- 9.0-10.0: Critical

CVSS considers factors including:

- Attack vector (network, adjacent, local, physical)
- Attack complexity
- Privileges required
- User interaction required
- Impact on confidentiality, integrity, availability

Organizations use CVSS scores to prioritize patching efforts, though scores should be considered alongside contextual factors specific to each environment.

Part 4: MITRE ATT&CK Framework

The **MITRE ATT&CK framework** is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge.

Framework Structure

ATT&CK organizes adversary behavior into:

Tactics: The "why" of an attack, the adversary's objective

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection

- Command and Control
- Exfiltration
- Impact

Techniques: The "how" of an attack, the specific methods used

Sub-techniques: More specific implementations of techniques

Procedures: Detailed descriptions of how specific groups implement techniques

Using ATT&CK

Organizations use ATT&CK for:

- **Threat intelligence**: Understanding how specific groups operate
- **Detection**: Developing detection capabilities for known techniques
- **Assessment**: Evaluating security coverage against the framework
- **Red teaming**: Planning realistic attack simulations
- **Training**: Educating security teams about adversary methods

ATT&CK Matrices

MITRE provides several matrices:

- **Enterprise**: Windows, macOS, Linux, cloud, network, containers
- **Mobile**: iOS and Android
- **ICS**: Industrial control systems

Recent Updates

As of late 2025, MITRE released ATT&CK version 18, which introduced:

- Detection Strategies and Analytics objects
- Structured, behavior-focused detection guidance
- Expanded cloud-based attack techniques
- New tactics related to AI-driven attacks
- Supply chain compromise techniques

The 2025 ATT&CK evaluations focused on attacks by Scattered Spider (cybercrime group) and Mustang Panda (Chinese state-sponsored actor), with increased emphasis on cloud infrastructure attacks and protection capabilities.

Part 5: Emerging Threats in 2025-2026

Let us examine the most significant emerging threats that security professionals must address.

AI-Powered Attacks

Artificial intelligence is transforming the threat landscape:

- **AI-generated phishing**: Large language models create highly convincing phishing content
- **Automated vulnerability discovery**: AI systems find and exploit vulnerabilities faster
- **Deepfakes**: Realistic audio and video for impersonation attacks
- **Adaptive malware**: Malware that modifies behavior based on environment
- **AI-assisted social engineering**: Personalized manipulation at scale

Quantum Computing Threats

While practical quantum computers capable of breaking current encryption do not yet exist, organizations must prepare:

- **Harvest now, decrypt later**: Attackers steal encrypted data now to decrypt when quantum computers become available
- **Cryptographic migration**: Planning transition to post-quantum algorithms
- **Timeline uncertainty**: Estimates range from 5 to 15+ years

Supply Chain Attacks

Supply chain attacks continue to grow:

- Compromised software development tools
- Malicious code in open-source dependencies
- Attacks on managed service providers
- Hardware implants
- Compromised update mechanisms

Organizations must verify the integrity of their entire software supply chain.

Cloud-Native Threats

As workloads move to cloud:

- Misconfiguration remains the leading cause of cloud breaches
- Container and Kubernetes-specific attacks
- Serverless function vulnerabilities
- Cross-tenant attacks
- Cloud credential theft

Identity-Based Attacks

Attackers increasingly target identity:

- Credential phishing and theft
- MFA (Multi-Factor Authentication) bypass techniques
- Session hijacking
- Privilege escalation
- Identity federation attacks

Malware-Free Attacks

A significant trend highlighted by the CrowdStrike 2025 Global Threat Report: 81 percent of intrusions were malware-free:

- Living-off-the-land techniques using legitimate tools
- Fileless attacks residing only in memory
- Abuse of trusted applications
- PowerShell and script-based attacks
- Harder to detect with traditional antivirus

Part 6: Threat Intelligence

Threat intelligence is evidence-based knowledge about threats that helps organizations make informed security decisions.

Types of Threat Intelligence

Strategic intelligence: High-level information about trends and risks for executives

Tactical intelligence: Information about attacker tools, techniques, and procedures for security teams

Operational intelligence: Details about specific attacks, campaigns, or actors

Technical intelligence: Indicators of compromise (IOCs) for detection systems

Indicators of Compromise (IOCs)

IOCs are artifacts indicating potential malicious activity:

- IP addresses
- Domain names
- File hashes
- URLs
- Email addresses
- Registry keys
- Mutex names

Security tools use IOCs to detect known threats.

Threat Intelligence Sharing

Organizations share threat intelligence through:

- Information Sharing and Analysis Centers (ISACs)
- Government programs (CISA (Cybersecurity and Infrastructure Security Agency), FBI)
- Commercial threat intelligence feeds
- Open-source intelligence (OSINT)
- Industry groups and partnerships

Sharing improves collective defense but requires careful handling of sensitive information.

Part 7: Practical Exercise

Let me walk through a real-world scenario to illustrate these concepts.

Scenario: The SolarWinds Attack

In December 2020, the SolarWinds supply chain attack was discovered. Let us analyze it using our framework:

Threat Actor: APT29 (Cozy Bear), associated with Russian intelligence

Motivation: Espionage, access to US government networks

Attack Vector: Supply chain (compromised software update)

Initial Access (ATT&CK): Supply Chain Compromise (T1195.002)

Techniques Used:

- Trojanized software update
- Stealthy command and control
- Extensive reconnaissance
- Credential harvesting
- Lateral movement
- Data exfiltration

Impact:

- 18,000 organizations received compromised update
- Major US government agencies breached
- Multiple private companies affected
- Months of undetected access

Lessons:

- Supply chain security is critical
- Nation-states have extensive capabilities
- Detection of sophisticated actors is extremely difficult
- Vendor trust must be verified

Conclusion

Today we explored the threat landscape in depth:

1. **Threat actors**: Nation-states, cybercriminals, hacktivists, insiders, and others have different motivations and capabilities
2. **Attack vectors**: Network, application, physical, social engineering, supply chain, and cloud attacks
3. **Vulnerability lifecycle**: Discovery, disclosure, patching, and the CVE/CVSS systems
4. **MITRE ATT&CK**: Framework for understanding adversary behavior
5. **Emerging threats**: AI-powered attacks, quantum threats, supply chain, cloud-native, and malware-free attacks
6. **Threat intelligence**: Using evidence-based knowledge for defense

In our next lecture, we will examine malicious software in detail, including malware types, infection methods, and defensive technologies.

Discussion Questions

1. How should organizations prioritize defenses against different threat actors?
2. What are the ethical implications of government stockpiling zero-day vulnerabilities?
3. How can organizations verify the security of their software supply chain?

Thank you for your attention. See you in our next session.

Review Questions

1. Identify and compare the six main categories of threat actors. What distinguishes their motivations and capabilities?
2. What is a zero-day vulnerability, and why is it particularly dangerous?
3. Explain the CVE system and how CVSS scoring helps organizations prioritize vulnerability remediation.
4. Describe the MITRE ATT&CK framework. How is it organized, and how can defenders use it?
5. What are the primary attack vectors through which organizations are compromised?
6. How do supply chain attacks differ from direct attacks, and why are they difficult to defend against?
7. What types of threat intelligence exist, and how should each be used in an organization?
8. Explain the concept of responsible disclosure and its role in the vulnerability lifecycle.

Key Terms

- **AI-Powered Attack**: A cyberattack that uses artificial intelligence to automate vulnerability discovery or enhance attack capabilities

- **APT**: Advanced Persistent Threat, a prolonged and targeted cyberattack by a sophisticated adversary
- **Attack Vector**: The path or method used by an attacker to gain access to a target
- **CVE**: Common Vulnerabilities and Exposures, a system for identifying known vulnerabilities
- **CVSS**: Common Vulnerability Scoring System, a framework for rating vulnerability severity
- **Cybercriminal**: An individual or group that commits crimes using computers or networks for financial gain
- **Hacktivism**: Hacking motivated by political or social causes
- **Harvest Now, Decrypt Later**: A strategy where attackers collect encrypted data now with the intention of decrypting it when quantum computers become available
- **Indicator of Compromise (IOC)**: Evidence that a security breach has occurred
- **Insider Threat**: A security risk originating from within the organization
- **MITRE ATT&CK**: A knowledge base of adversary tactics, techniques, and procedures
- **Nation-State Actor**: A government-sponsored threat actor conducting cyber operations
- **Responsible Disclosure**: The practice of privately reporting security vulnerabilities to vendors before making them public
- **Software Bill of Materials (SBOM)**: A comprehensive inventory of all components and dependencies in a software product
- **Supply Chain Attack**: An attack that targets less-secure elements in a supply chain
- **Threat Actor**: An entity responsible for an event or incident that impacts the security of another entity
- **Threat Intelligence**: Evidence-based knowledge about existing or emerging threats
- **Zero-Day**: A vulnerability unknown to the vendor with no available patch

References and Further Reading

- MITRE ATT&CK Framework (attack.mitre.org)
- NIST National Vulnerability Database (nvd.nist.gov)
- Verizon Data Breach Investigations Report
- ENISA Threat Landscape Report

- Mandiant M-Trends Report
- CrowdStrike Global Threat Report
- CISA Known Exploited Vulnerabilities Catalog