### **Practical #3 Cyber Attack Techniques and how the attack unfolds**

Team #1

Yash Rustagi

Aditya Chawla

Pranav Sahni

Abhishek Madaan

### **Top 5 cyber attacks of 2024**

1. **Watering Hole Attacks** Attackers compromise websites frequently visited by target organizations and insert malicious scripts. When a user visits the site, malware is silently downloaded or executed. This attack is difficult to detect because it uses legitimate websites. Indicators include unusual network requests, suspicious scripts on endpoints, and unexpected downloads.
2. **DNS Tunneling** DNS Tunneling encodes data in DNS queries to exfiltrate sensitive information. It bypasses traditional firewall rules because DNS traffic is normally trusted. Detection requires monitoring for abnormal DNS request patterns, unusually large or frequent queries, and unexpected domain resolutions.
3. **Living off the Land (LotL) Attacks** In LotL attacks, attackers use built-in tools like PowerShell, Windows Management Instrumentation (WMI), or shell scripts to execute malicious actions. Since these tools are legitimate, signature-based security often misses them. Detection relies on monitoring unusual command-line activity, high-frequency administrative tool usage, and abnormal process behaviors.
4. **Credential Stuffing** Attackers use leaked usernames and passwords from one breach to access other accounts or systems. Unlike brute force, this relies on reused credentials. Signs include failed login spikes, logins from unusual locations, or multiple accounts being accessed in a short time. Multi-factor authentication and anomaly detection reduce risk.
5. **Supply Chain Attacks** Attackers compromise third-party software or services, which then infects the target organization. Detection is challenging since updates or vendors appear legitimate. Indicators include unexpected outbound connections, unverified software updates, and unusual process activity.

### **Detecting and Mitigating Attacks Using the Kill Chain**

1. **Watering Hole Attacks**

* **Reconnaissance:** Monitor external scanning and unusual web traffic to find compromised sites.
* **Weaponization:** Detect suspicious scripts or exploit code prepared on endpoints.
* **Delivery:** Inspect browser requests for malicious payloads.
* **Exploitation:** Identify execution of malware scripts or drive-by downloads.
* **Installation:** Check for new persistent processes or unauthorized files.
* **Command & Control (C2):** Monitor network traffic to suspicious external domains.
* **Actions on Objectives:** Audit data exfiltration or lateral movement within the network.

1. **DNS Tunneling**

* **Reconnaissance:** Monitor DNS traffic for unusual domain requests.
* **Weaponization:** Detect encoded payloads in DNS query patterns.
* **Delivery:** Identify endpoints making repeated, irregular DNS queries.
* **Exploitation:** Observe abnormal data movement via DNS channels.
* **Installation:** Check for installation of scripts or agents using DNS for communication.
* **C2:** Track DNS-based communication with attacker-controlled servers.
* **Actions on Objectives:** Audit exfiltrated sensitive data and stop further transfers.

1. **Living off the Land (LotL) Attacks**

* **Reconnaissance:** Detect scanning and probing activity by insider or attacker-controlled processes.
* **Weaponization:** Monitor scripts or PowerShell commands built for attacks.
* **Delivery:** Identify execution of legitimate tools with unusual parameters.
* **Exploitation:** Check for abnormal privilege escalation or file access.
* **Installation:** Monitor new scheduled tasks or service modifications.
* **C2:** Detect unusual remote access or remote execution activities.
* **Actions on Objectives:** Audit data access, lateral movement, or configuration changes.

1. **Credential Stuffing**

* **Reconnaissance:** Monitor for credential dumps from public sources.
* **Weaponization:** Detect lists of credentials being prepared for automated login attempts.
* **Delivery:** Identify login attempts from unknown IPs or multiple accounts.
* **Exploitation:** Track successful logins using reused credentials.
* **Installation:** No software installation, but monitor session creation or token generation.
* **C2:** Not typically applicable; focus on monitoring access channels.
* **Actions on Objectives:** Monitor data access, unauthorized transactions, and account changes.

1. **Supply Chain Attacks**

* **Reconnaissance:** Monitor vendor activity and third-party communications.
* **Weaponization:** Detect malicious updates or software packages.
* **Delivery:** Identify updates or services deployed in the environment.
* **Exploitation:** Monitor execution of tampered software.
* **Installation:** Audit for new processes, services, or scheduled tasks.
* **C2:** Track outbound connections from compromised vendor software.
* **Actions on Objectives:** Observe unauthorized data access, exfiltration, or system modifications.