Exfiltration

In the exfiltration phase, **attackers move the data they've collected out of the compromised environment to their own infrastructure**, allowing them to access and leverage the information externally. Exfiltration techniques vary depending on the attacker's goals, network controls, and the data's sensitivity. Common methods include using removable media, command-and-control (C2) channels and other covert communication paths, and scheduled transfers.

1. Removable Media/USB, Bluetooth Exfiltration

- **Removable Media (USB)**:
  - Definition: Attackers physically connect USB drives or other removable storage devices to the compromised system and copy data onto them.
  - Purpose: This method allows exfiltration without using the network, which can bypass network-based security tools.
- **Bluetooth Exfiltration**:
  - Definition: Bluetooth connections allow data transfer wirelessly over short distances. Attackers may use Bluetooth to exfiltrate data to nearby devices if USB access is restricted.
  - Security Implications: These methods are especially challenging to detect as they bypass network monitoring tools. USBs can contain large amounts of data, and Bluetooth transfers enable data to be shared quickly with nearby devices, potentially by insider threats or attackers who gained physical access.

2. C2 Channels, DNS Exfiltration, Web Services (Code Repos, Cloud Storage)

- **C2 Channels**:
  - Definition: Command-and-control (C2) channels used for communication between compromised systems and attacker-controlled servers can also serve as an exfiltration method.
  - Methods: Attackers may exfiltrate data over existing C2 channels, embedding data within normal C2 traffic to avoid detection. **Common C2 channels include HTTP(S), FTP, and IRC**.
- **DNS Exfiltration**:
  - Definition: DNS exfiltration **uses the DNS protocol to send data in small chunks**, often embedded in DNS queries, from the compromised system to the attacker's server.
  - Methods: Attackers encode data into DNS requests, with each request containing **a small piece of data** that is sent to a controlled DNS server, which reassembles it.
  - Security Implications: DNS exfiltration is difficult to detect because DNS traffic is often allowed and goes unmonitored by many network security solutions.
- **Web Services (Code Repositories, Cloud Storage)**:
  - Definition: Attackers use legitimate services like **GitHub, Google Drive, or Dropbox** to upload stolen data, leveraging these services' trusted nature to avoid detection.
  - Methods: Data may be disguised as legitimate files or code repositories, making it challenging for defenders to identify malicious activity.
  - Security Implications: Since organizations often allow access to these services, attackers can bypass network restrictions. The traffic to these services is often encrypted, limiting visibility into the data being exfiltrated.

3. Scheduled Transfers

- Definition: Attackers schedule data transfers to occur at specific times, typically when network activity is low (e.g., at night), to avoid detection and reduce the chance of triggering alerts.
- How It Works: Attackers may use built-in system scheduling tools, such as cron jobs on Linux or Task Scheduler on Windows, to automate exfiltration tasks.
- Example: Data can be transferred incrementally over time to avoid detection by data loss prevention (DLP) tools, with each transfer containing small batches of information.
- Security Implications: Scheduled transfers allow attackers to minimize the risk of detection by blending in with legitimate system activity. They may also bypass security alerts that trigger on large data transfers by using low and slow data transfer techniques.

Summary

- Removable Media/USB and Bluetooth Exfiltration allow attackers to move data physically without using the network, making it harder to detect via network security tools.
- C2 Channels, DNS Exfiltration, and Web Services are network-based exfiltration methods that take advantage of standard protocols and trusted services, allowing attackers to transfer data covertly.
- Scheduled Transfers enable attackers to exfiltrate data **at low-activity times or in small increments, helping them avoid detection by monitoring tools**.

Understanding these exfiltration methods enables organizations to monitor and control data flows effectively. Implementing data loss prevention (DLP), restricting access to external storage devices, monitoring DNS requests, and reviewing unusual network traffic patterns can help detect and prevent unauthorized data exfiltration.