Exfiltration Over Physical Medium

The attackers use a USB drive, printouts, or even socks... yes, socks, as a way to get data out of a network. This requires an accomplice on the inside or it can be used with the Insider Threat (Initial Compromise) card.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Security Guard
User Awareness Training
Video Surveillance

TOOLS

USB drive/socks and a dream... a dream of evil.

EVIL SOCKS

EXPV1_0421

Backdoors & Breaches

C2 and EXFIL