Networking Equipment is Critical

- It forms a technological foundation for communication
- It contributes to the economy
- Vital for national security
Backdoors, exploits and 0days in Networking Equipment

Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon.
Backdoors in SDN equipment

• Does that introduce new attacks?
• Can we detect backdoor activity?
Software Defined Networking (SDN) is a networking paradigm

- Separated planes
- Centralized model
SDN Teleportation: An attack previously not possible

Traditional Networks

Software Defined Networks

Teleportation

Control plane

Data plane
SDN Teleportation poses several threats

- Bypass security mechanisms
- Attack coordination
- Exfiltration
- Eavesdrop
The Teleportation Model

1) Switch to Controller
2) Controller to Switches
3) Destination Processing
Teleportation Techniques

- Out-of-band Forwarding
- Flow (re-)configurations
- Switch Identification
Out-of-band Forwarding Teleportation

- Complete packets from one switch are teleported to another switch
Flow (Re-)Configuration Teleportation

- Exploit the controllers centralized control to reconfigure the network when a host moves across the network.
Switch Identification Teleportation

- Impersonate the Datapath-ID to communicate information

Diagram showing the teleportation process with arrows indicating features request and reply messages with DPID=1.
Attacks using Teleportation

- Bypass firewalls, IDS and IPS
- Exfiltration
- Man-in-the-middle
- Rendezvous/Attack coordination
Teleportation Bandwidth
Countermeasures

- Packet-in-Packet-Out Watcher
- Audit-Trails and Accountability
- Enhanced IDS with Waypoint Enforcement
Conclusions

- Introduced a conceptually novel SDN attack
- Teleportation enables several attacks
- Teleportation has high quality and throughput
- Suggested Teleportation countermeasures
Questions