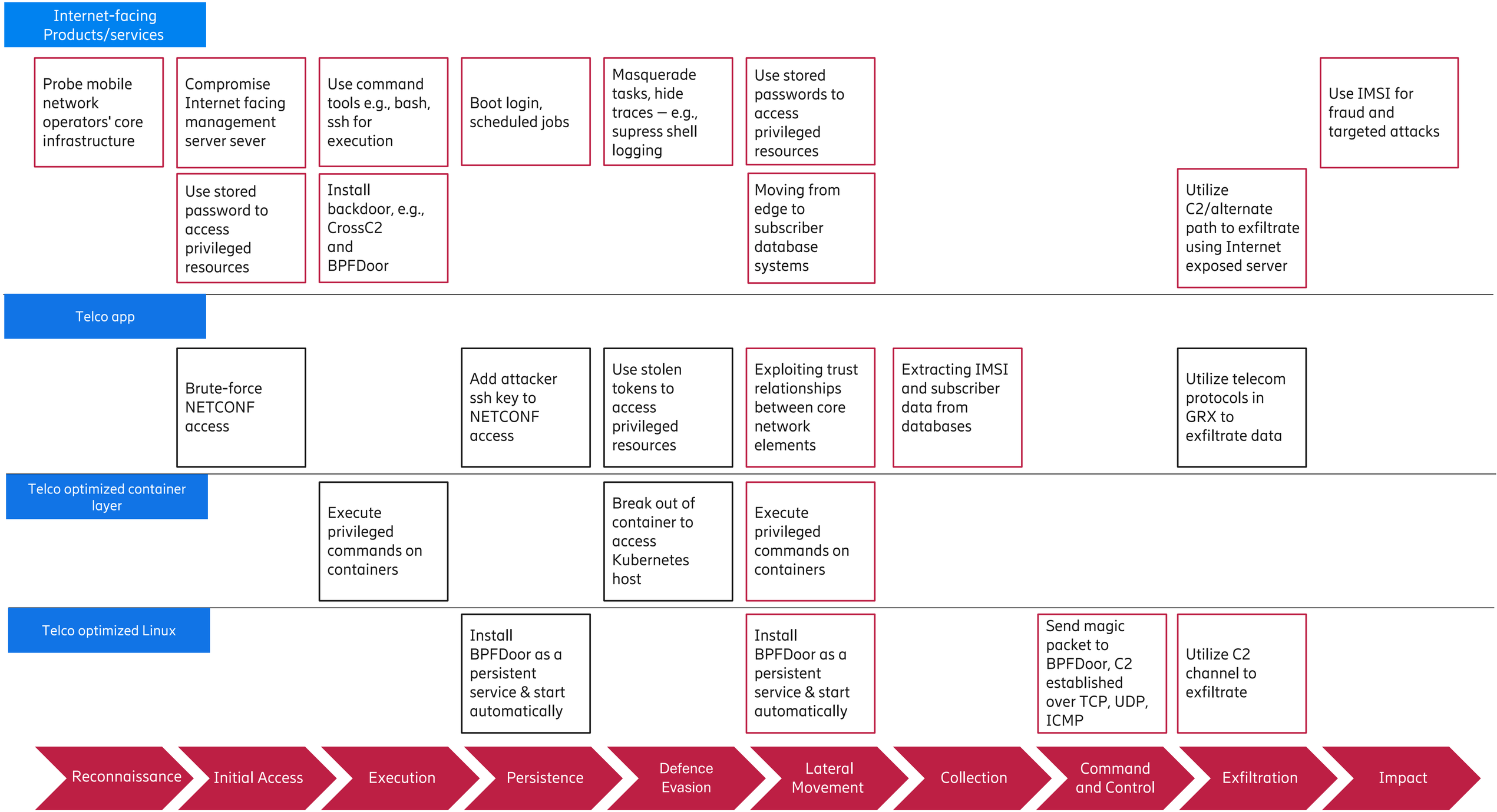
Internet-facing Products/services
Probe mobile network operators' core infrastructure
Compromise Internet facing management server sever
Use command tools e.g., bash, ssh for execution
Boot login, scheduled jobs
Masquerade tasks, hide traces – e.g., supress shell logging
Use stored passwords to access privileged resources
Use IMSI for fraud and targeted attacks
Use stored password to access privileged resources
Install backdoor, e.g., CrossC2 and BPFDoor
Moving from edge to subscriber database systems
Utilize C2/alternate path to exfiltrate using Internet exposed server
Telco app
Brute-force NETCONF access
Add attacker ssh key to NETCONF access
Use stolen tokens to access privileged resources
Exploiting trust relationships between core network elements
Extracting IMSI and subscriber data from databases
Utilize telecom protocols in GRX to exfiltrate data
Telco optimized container layer
Execute privileged commands on containers
Break out of container to access Kubernetes host
Execute privileged commands on containers
Telco optimized Linux
Install BPFDoor as a persistent service & start automatically
Install BPFDoor as a persistent service & start automatically
Send magic packet to BPFDoor, C2 established over TCP, UDP, ICMP
Utilize C2 channel to exfiltrate
Reconnaissance
Initial Access
Execution
Persistence
Defence Evasion
Lateral Movement
Collection
Command and Control
Exfiltration
Impact