JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Defense Deception Methods

THREAT MANAGEMENT

Defense Deception Methods

- Cybersecurity professionals may want to go beyond just standard defense and attempt to lure an attacker to specific targets

- Examples:
  - Honeypots
  - DNS Sinkholes

Honeypot

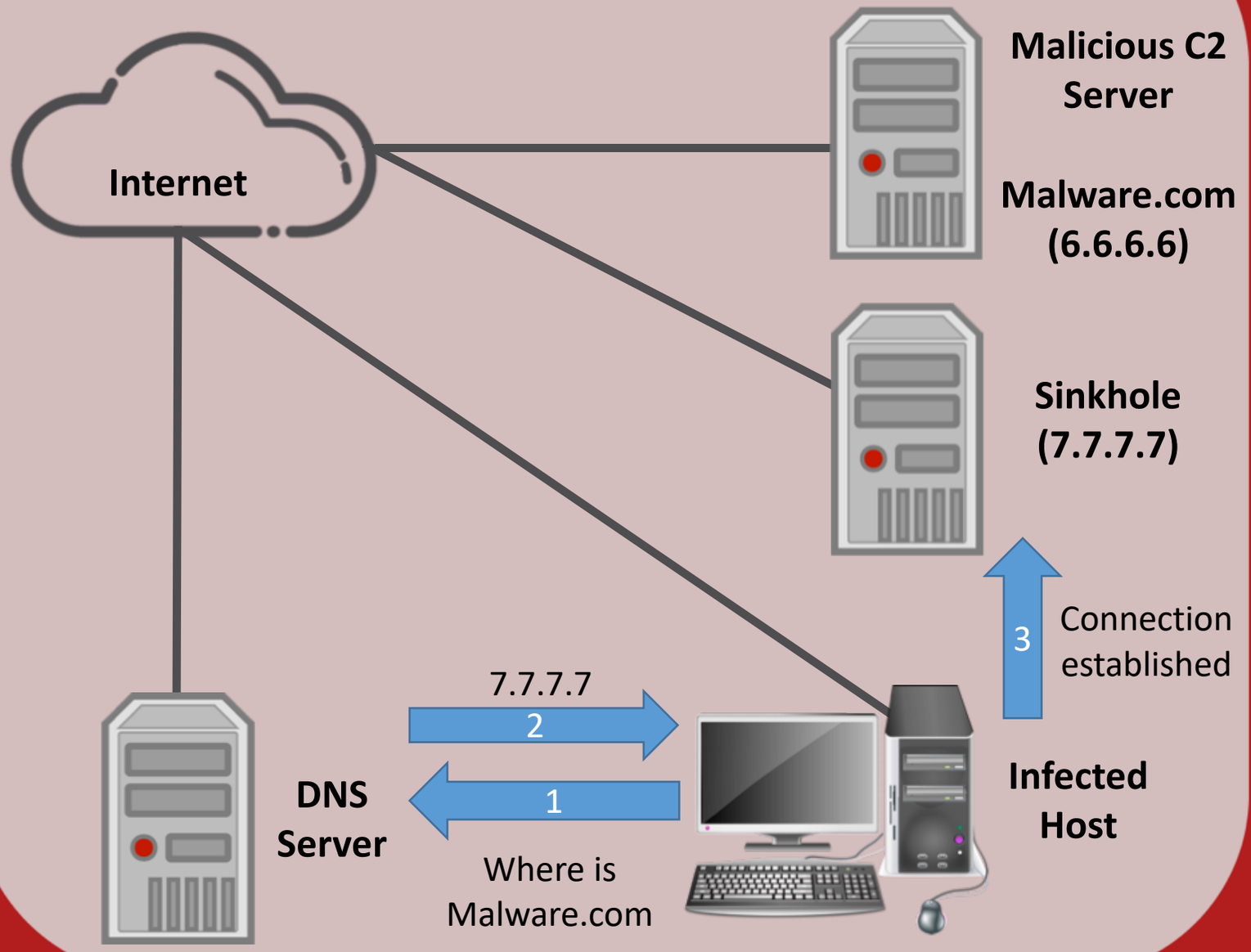
- System designed to look like a lucrative target due to the types of services being run or vulnerabilities contained
- In reality, honeypots are designed to falsely appear vulnerable and to fool malicious attackers to waste time going after them
- They simulate successful attacks and allow us to monitor attacker techniques

DNS Sinkhole

- Provide false DNS information to malicious software

- Compromised system requests DNS information from the server, but the server detects the suspicious request and gives the IP address of the sinkhole instead of the real Command and Control server

DNS Sinkhole



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE