

Impact with Slowloris

Impact with Slowloris



Pinal Dave

Technology Evangelist

@pinaldave

<https://blog.sqlauthority.com>



Slowloris



Slowloris

Creator: Gokberk Yaltirakli

Slowloris is an HTTP Denial of Service attack that affects threaded servers. This exhausts the servers thread pool and the server can't reply to other people.



Slowloris

Impact tool using DDoS methodology

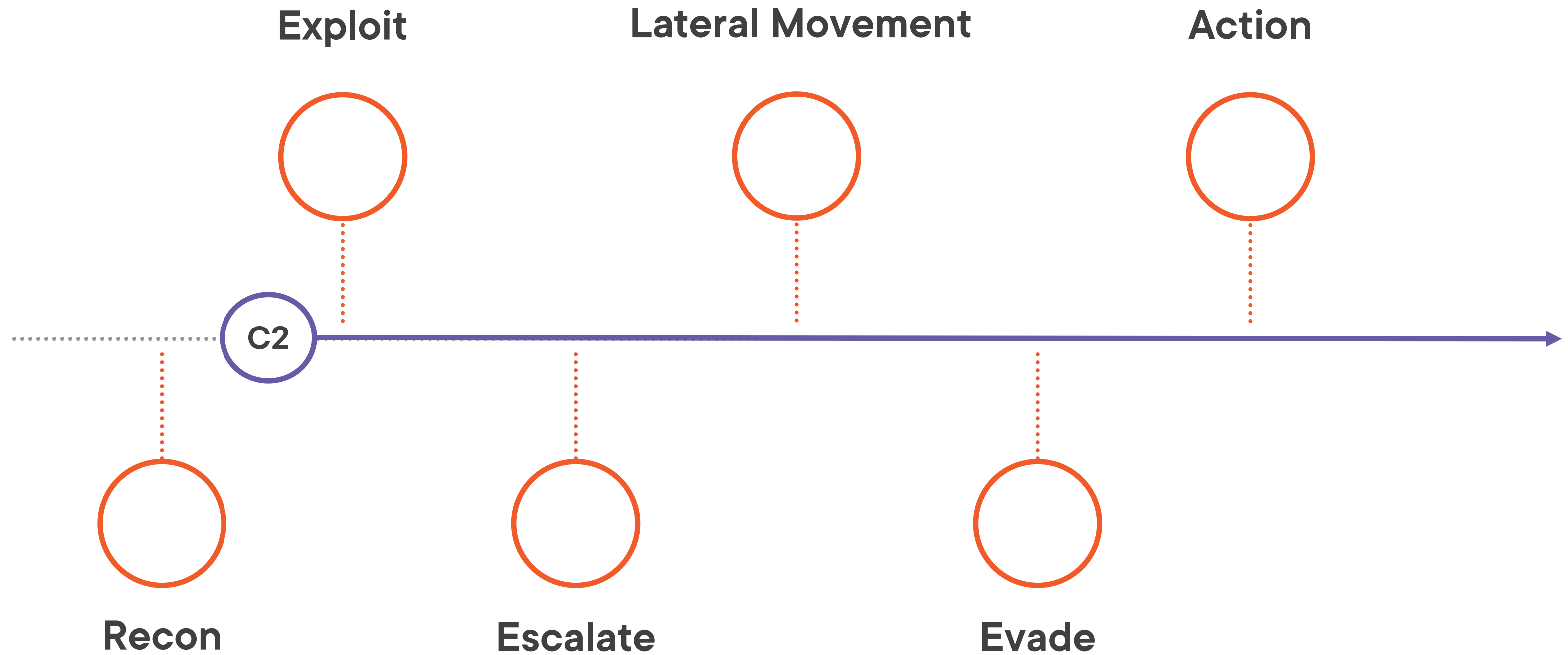
DDoS – Distributed Denial of Service

Difficult to differentiate from legit traffic

- Keeps connections open
- Randomizes user-agents
- Time to sleep between header sent



Kill Chain



MITRE ATT&CK

Tactics

Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact



MITRE ATT&CK

Tactics

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1498:

Network Denial of Service

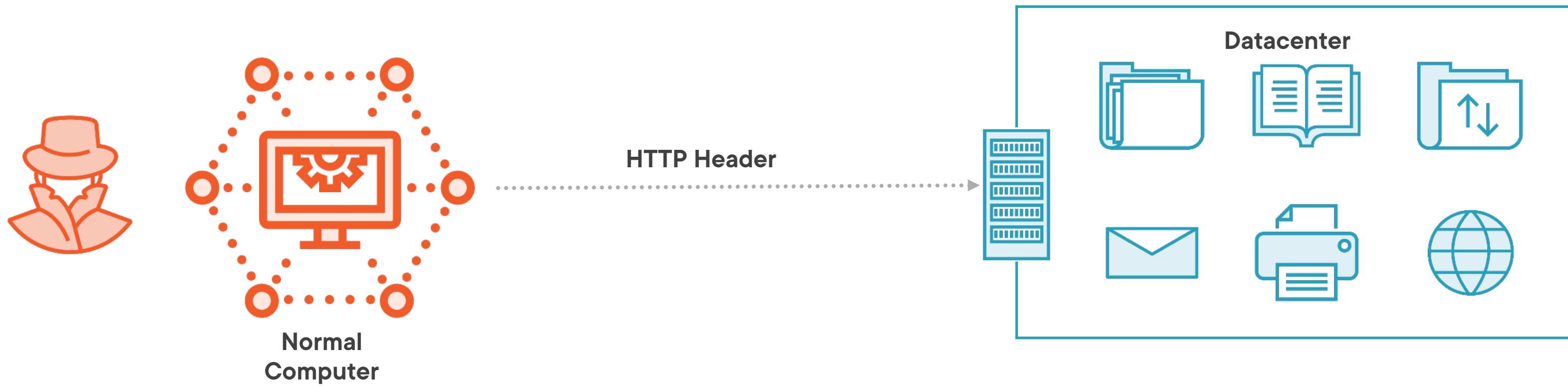
T1499:

Endpoint Denial of Service



Staying Legal

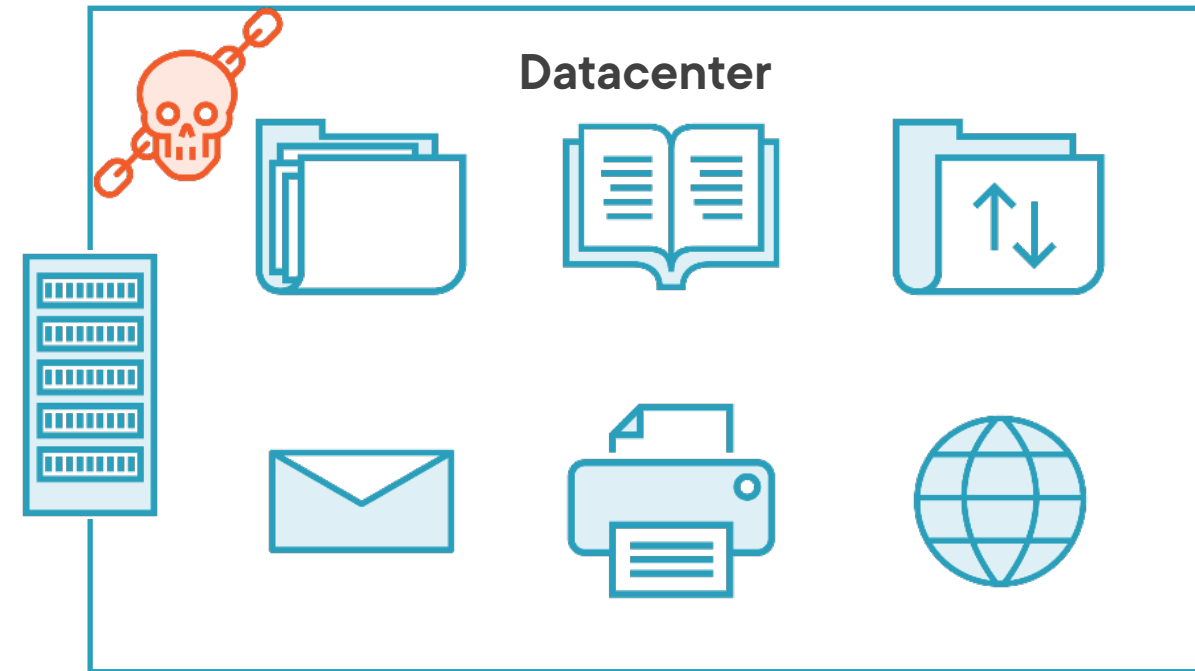
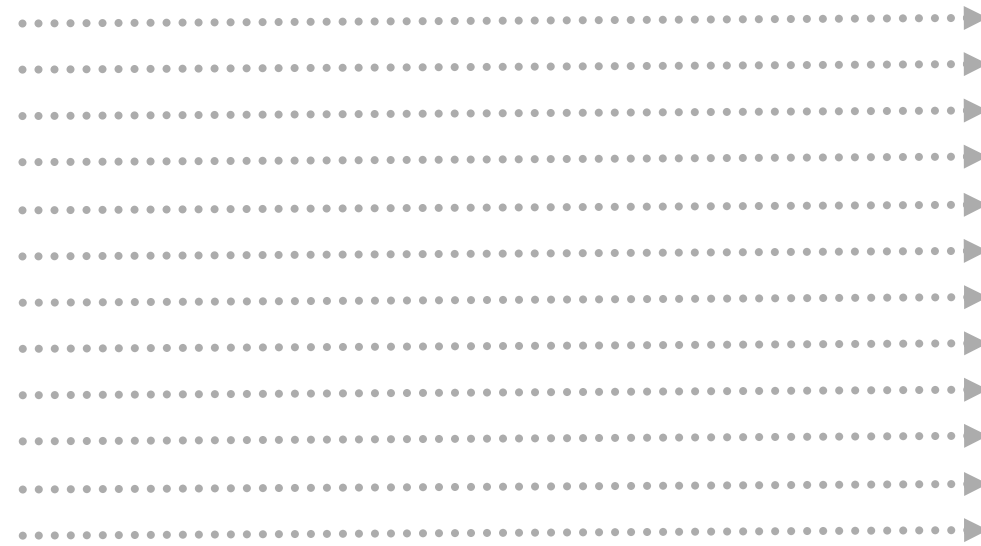




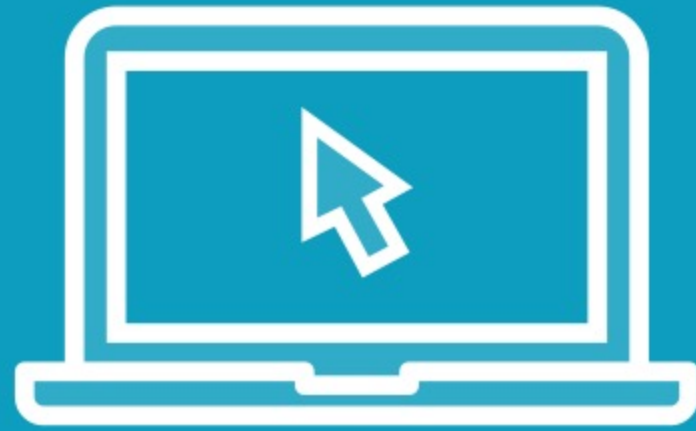


Slowloris

150 HTTP Headers



Demo



Impact with Slowloris

- Installation
- Default options
- Advanced options

