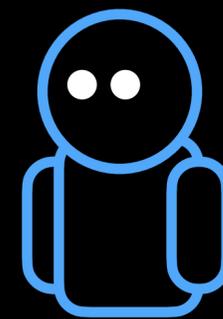


Weaponizing Middleboxes for TCP Reflected Amplification

Kevin Bock Abdulrahman Alaraj Yair Fax
Kyle Hurley Eric Wustrow Dave Levin



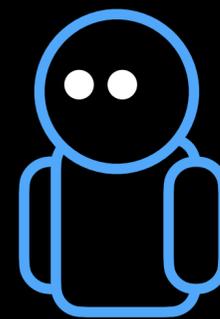
Denial of Service attacks



Denial of Service attacks



Attacker



Denial of Service attacks



Attacker

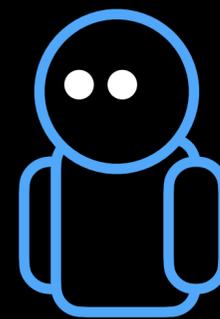


Victim

Denial of Service attacks



Attacker



Victim

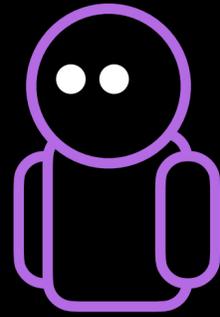
Reflected amplification attacks



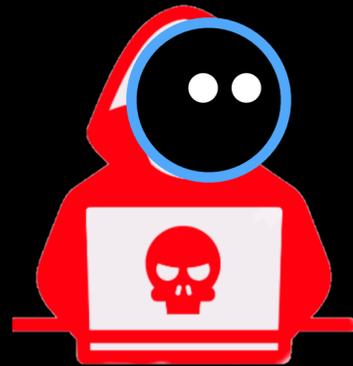
Open Server



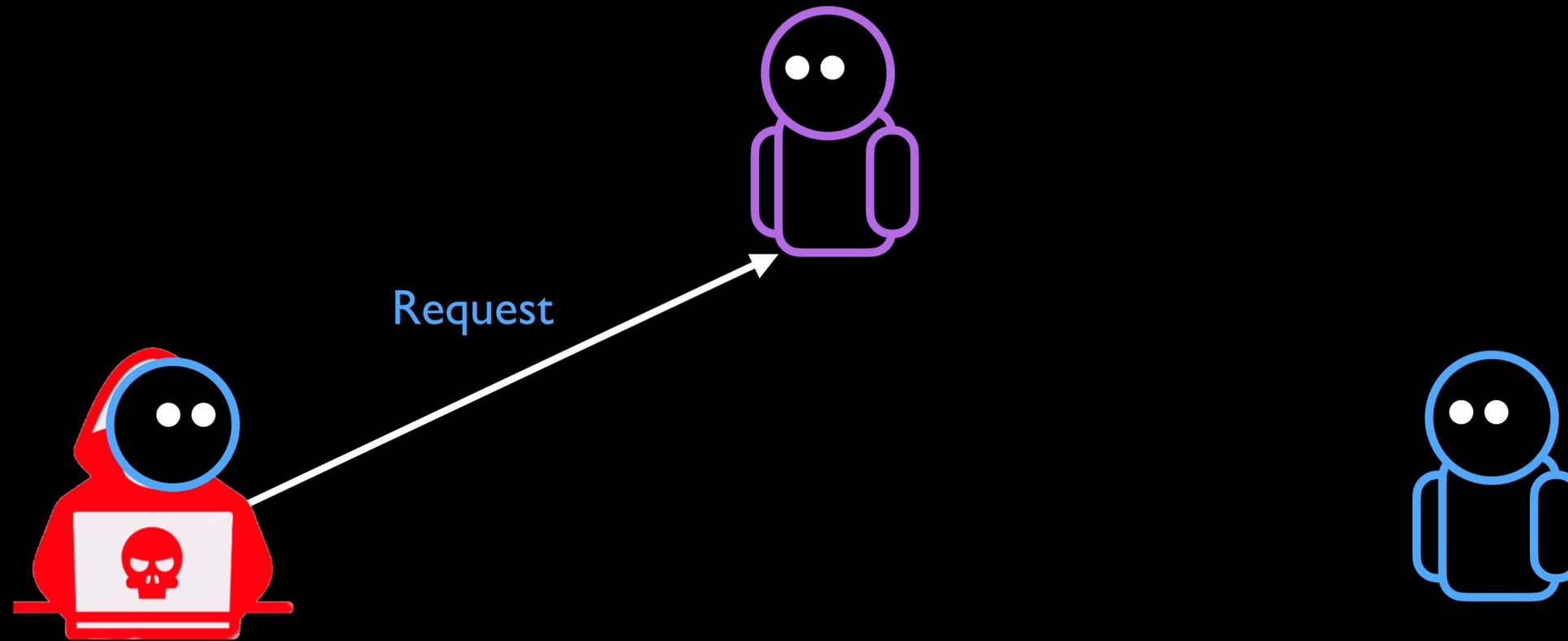
Reflected amplification attacks



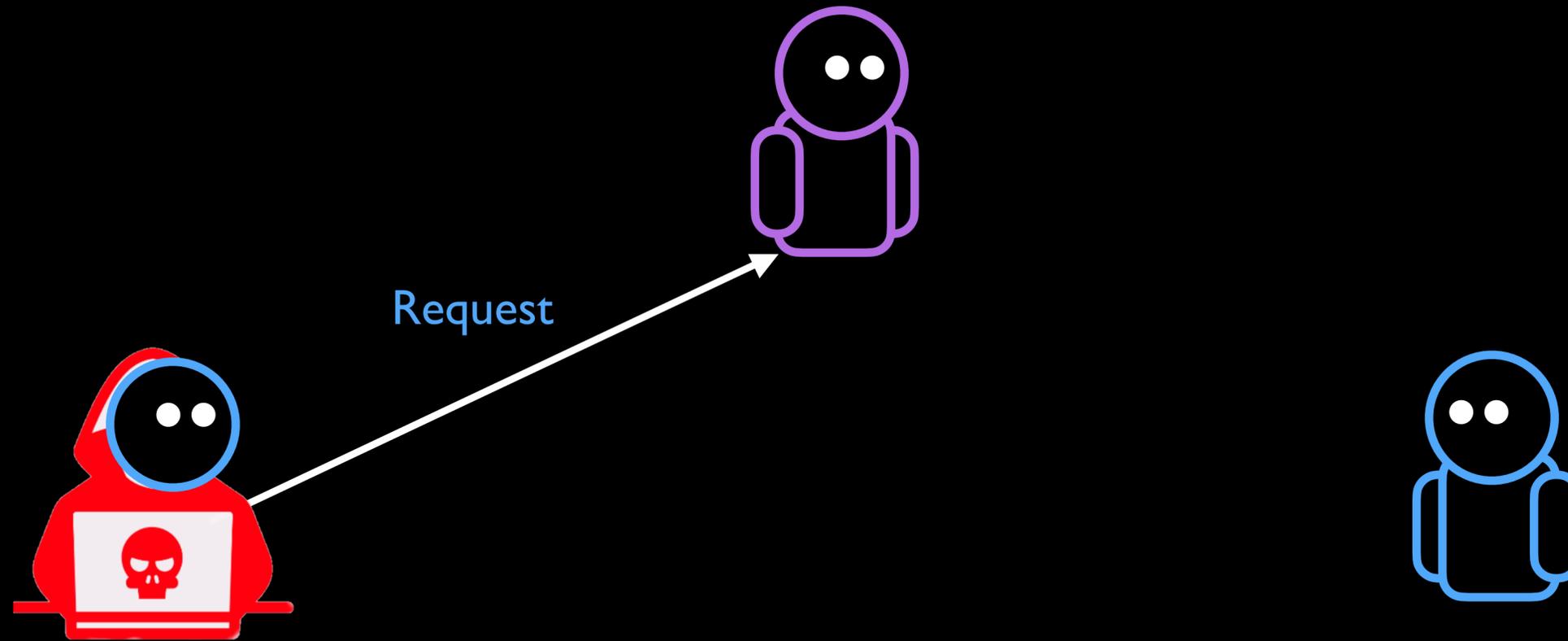
Open Server



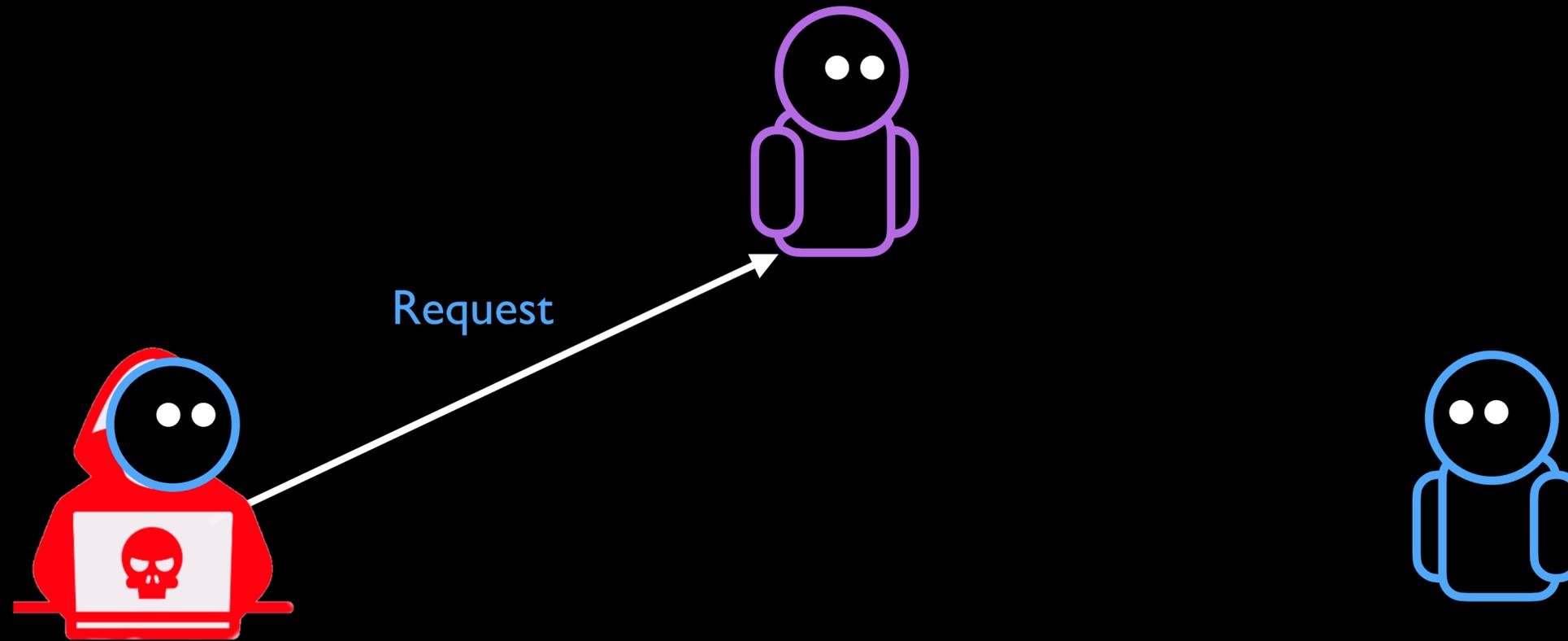
Reflected amplification attacks



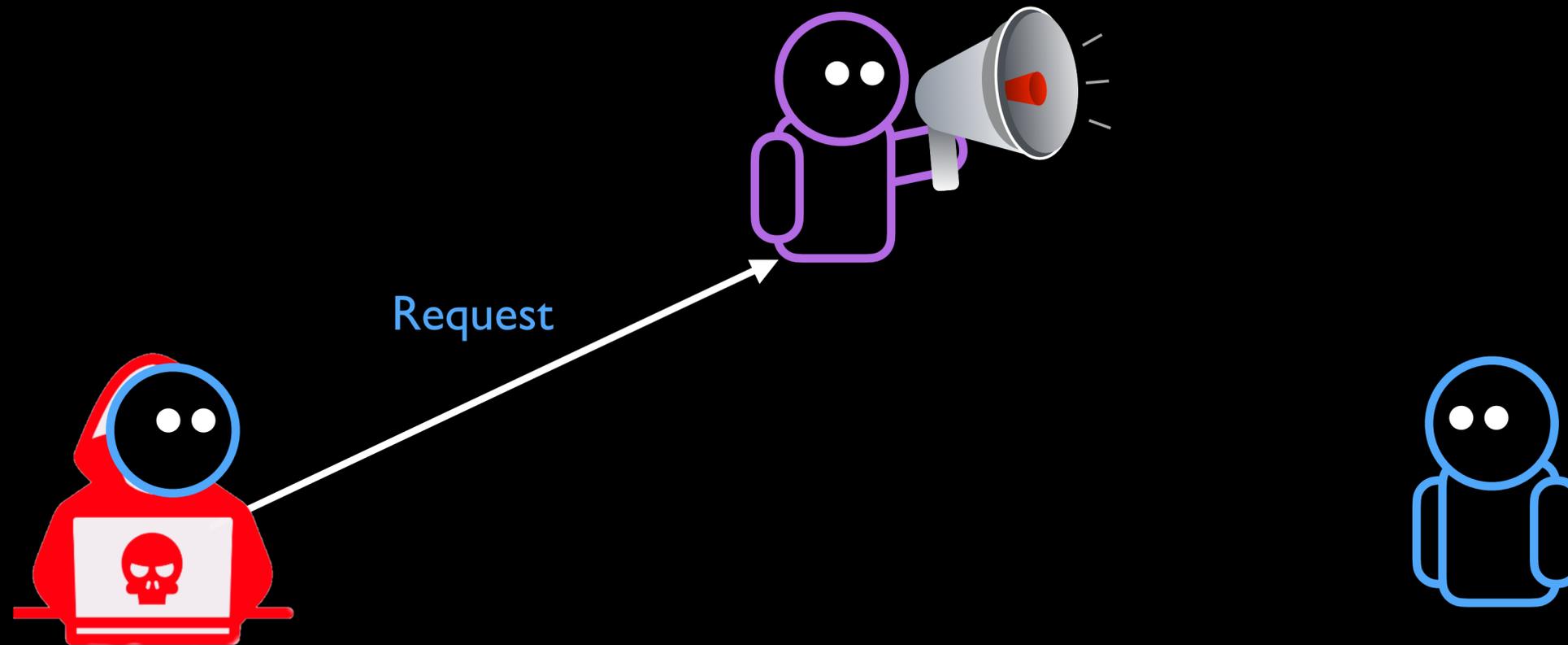
Reflected amplification attacks



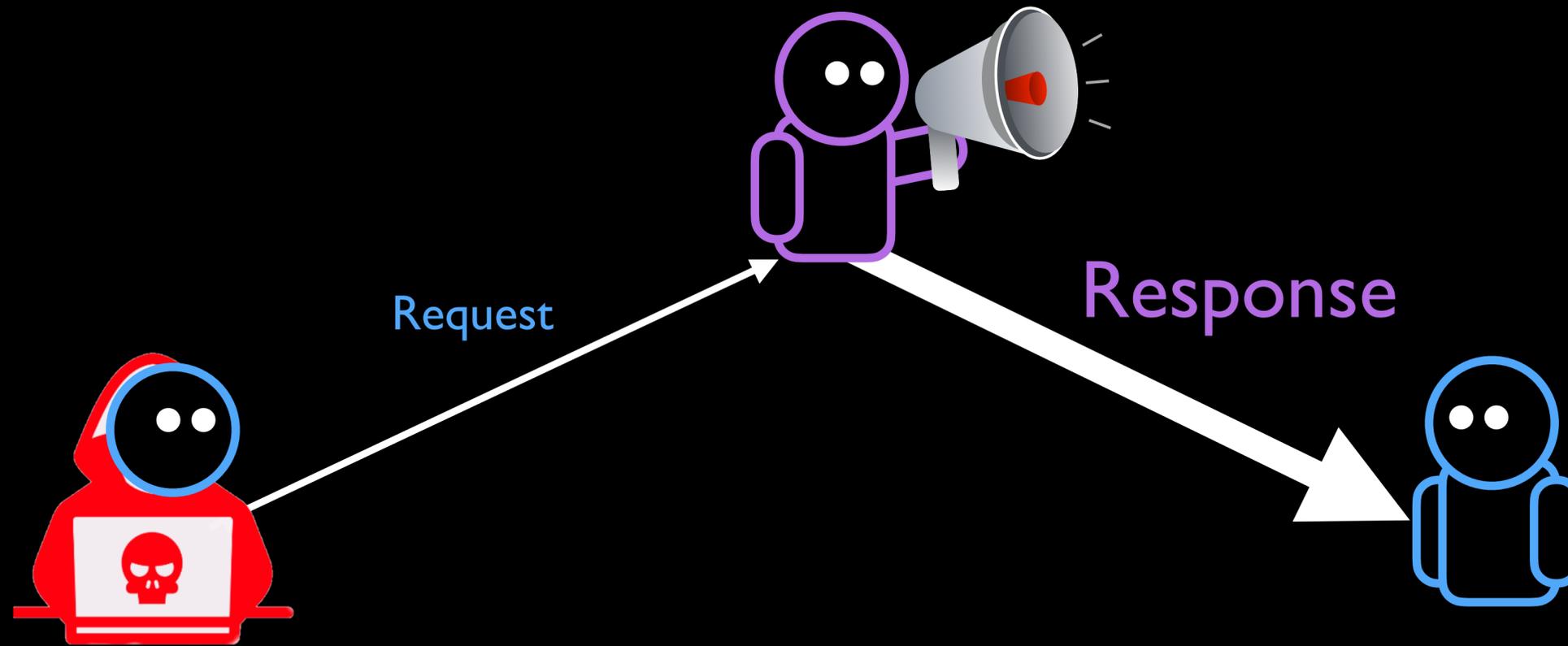
Reflected amplification attacks



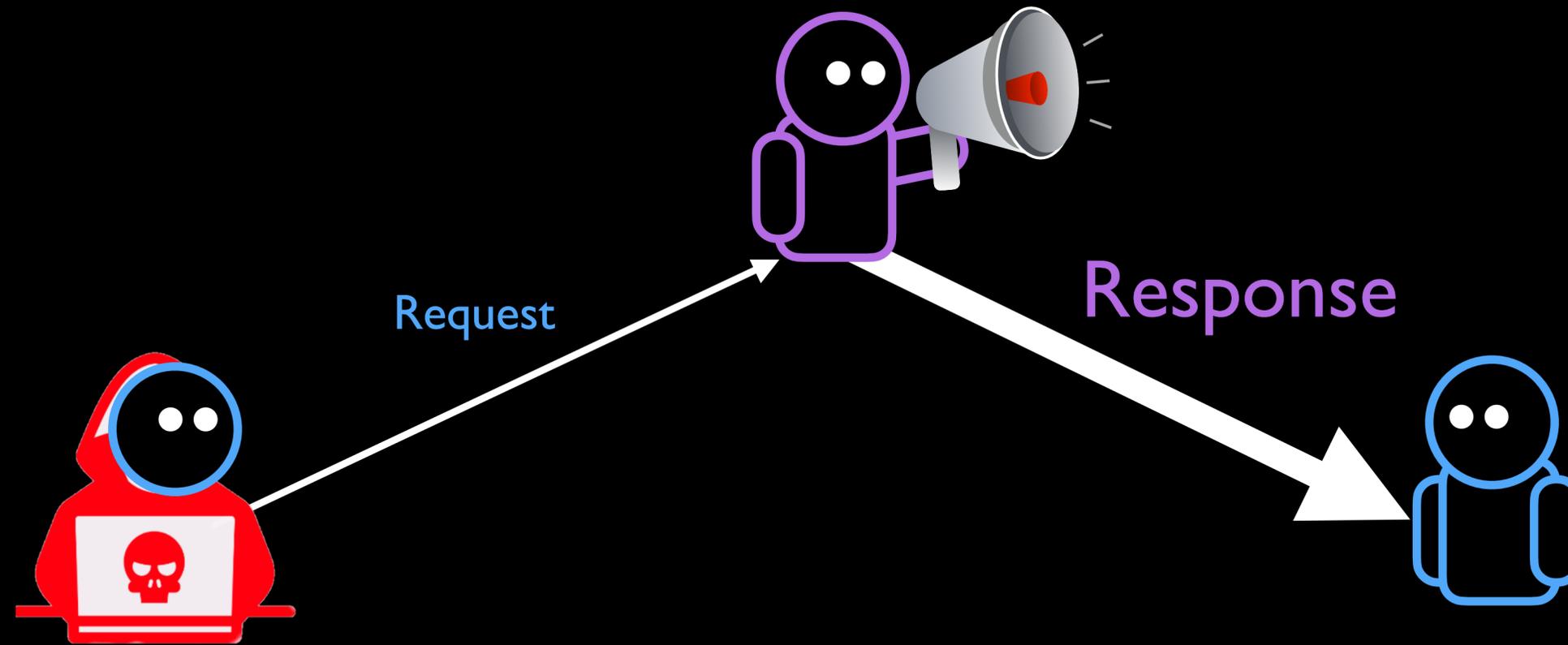
Reflected amplification attacks



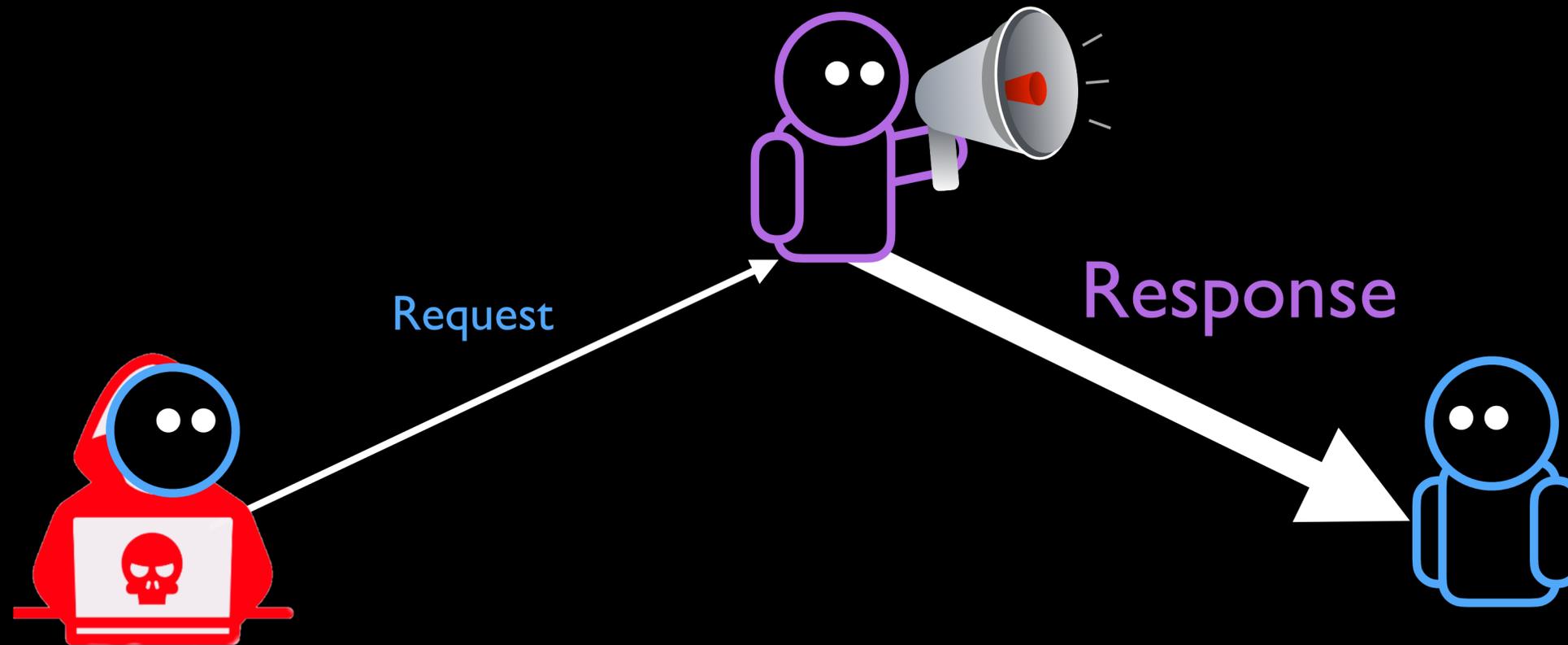
Reflected amplification attacks



Reflected amplification attacks

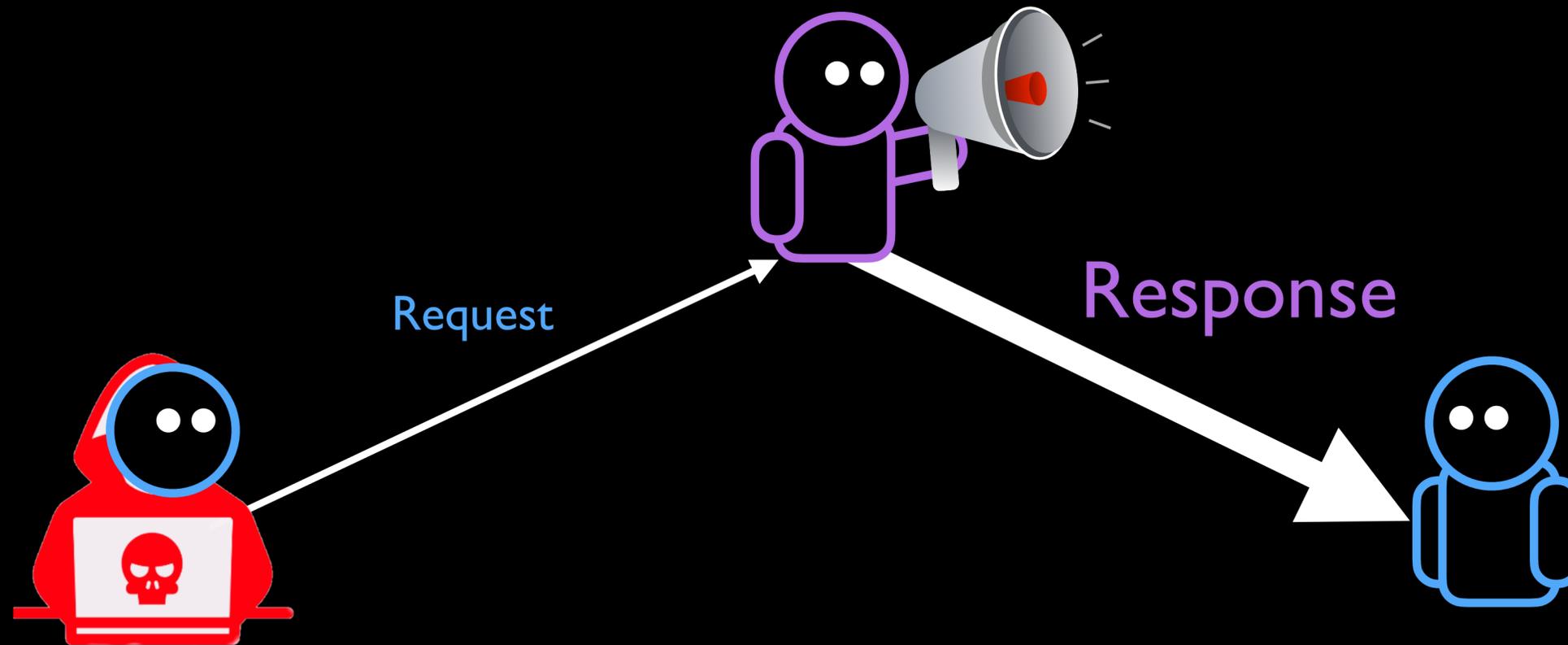


Reflected amplification attacks



$$\text{Amplification factor} = \frac{|\text{Response}|}{|\text{Request}|}$$

Reflected amplification attacks



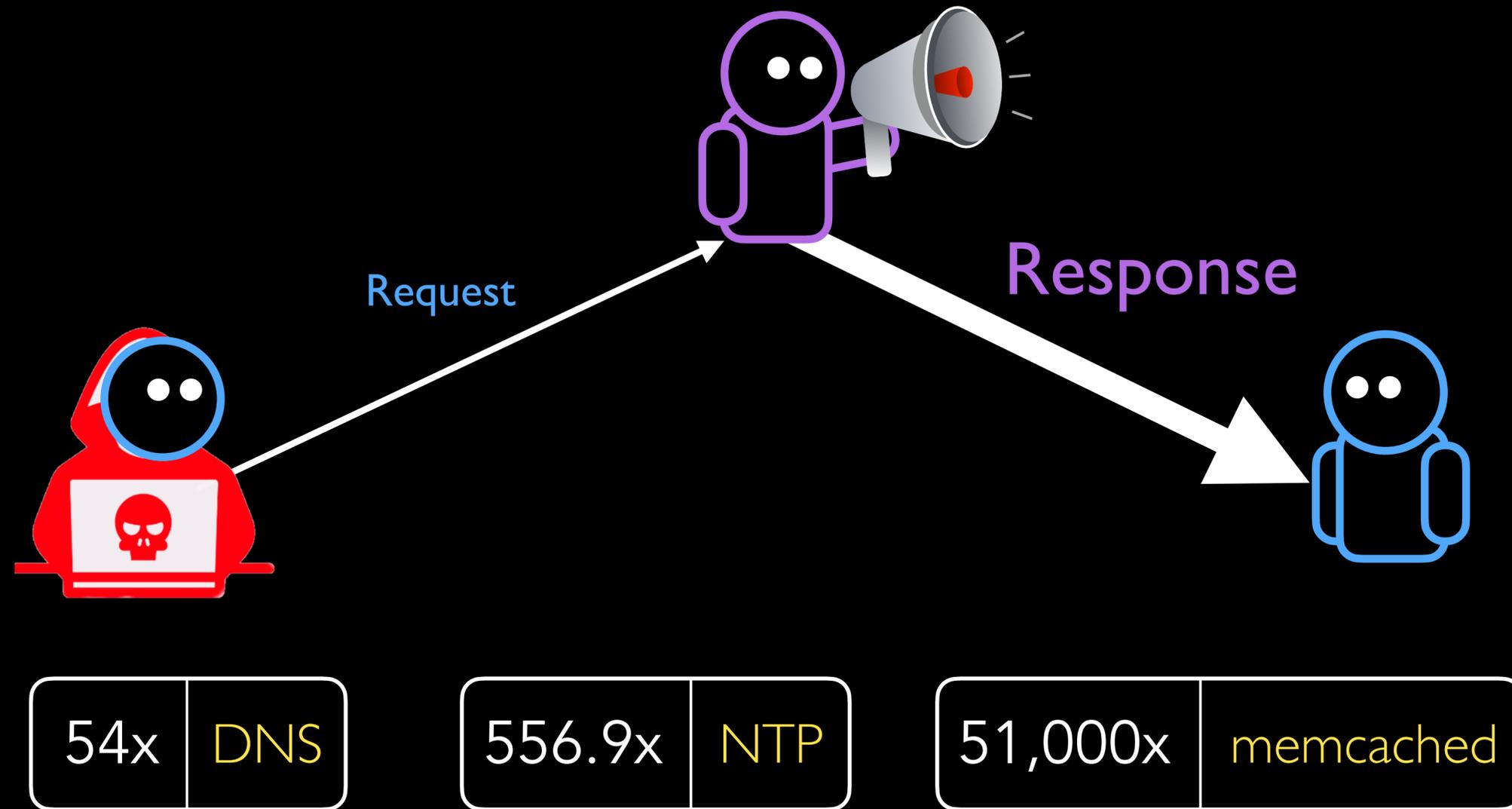
$$\text{Amplification factor} = \frac{|\text{Response}|}{|\text{Request}|}$$

54x DNS

556.9x NTP

51,000x memcached

Reflected amplification attacks



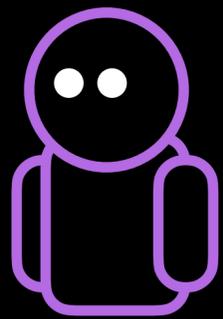
Almost all prior reflected amplification attacks use UDP

Reflected amplification attacks

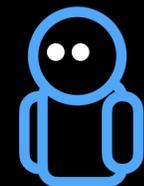
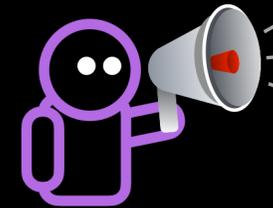
UDP is connection-less



Client

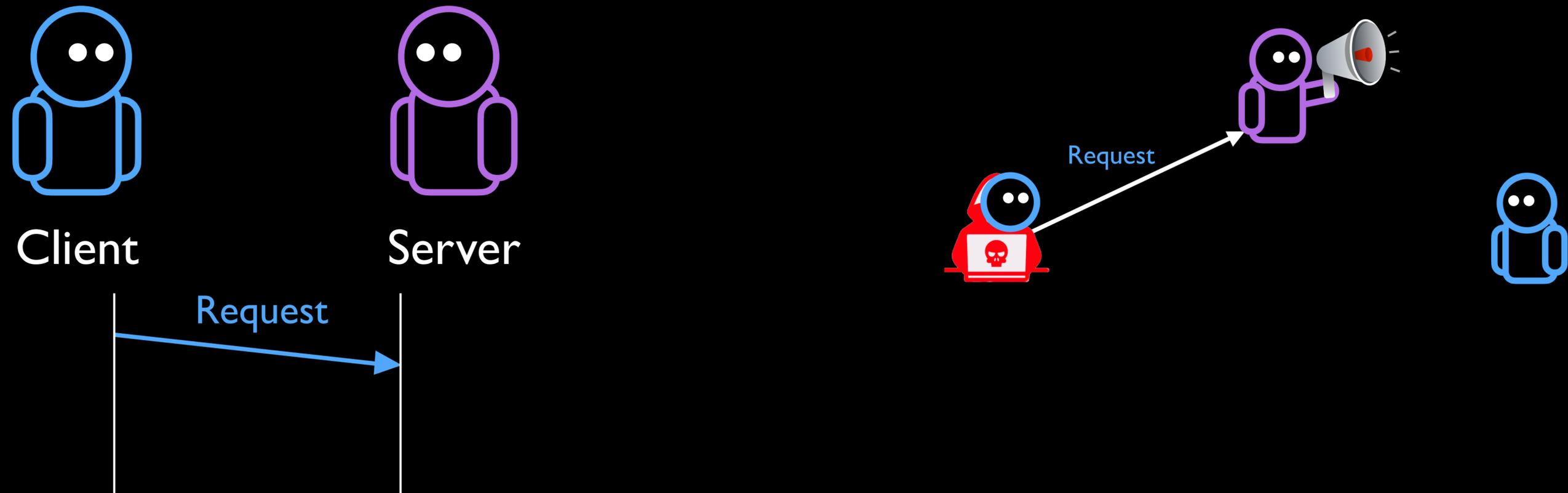


Server



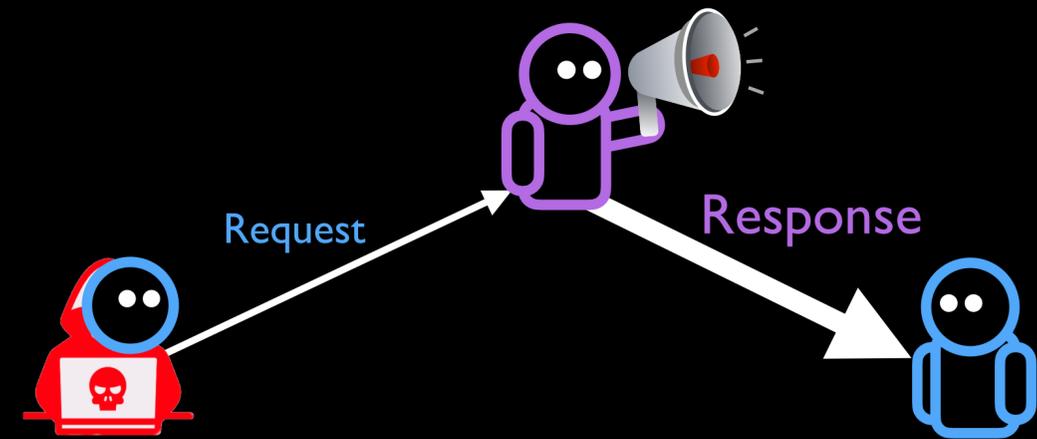
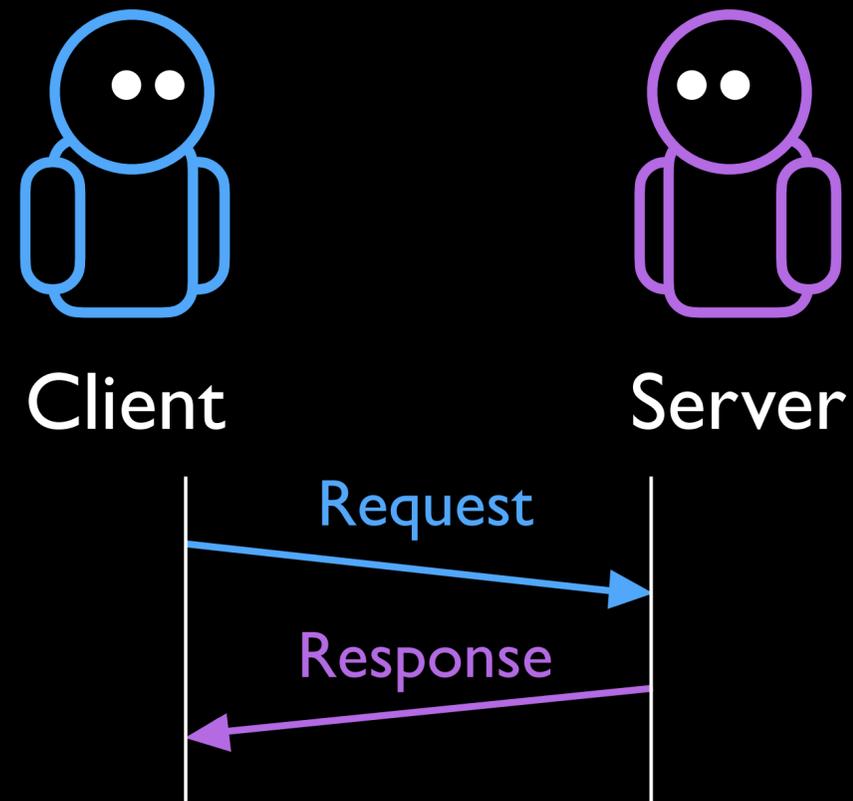
Reflected amplification attacks

UDP is connection-less



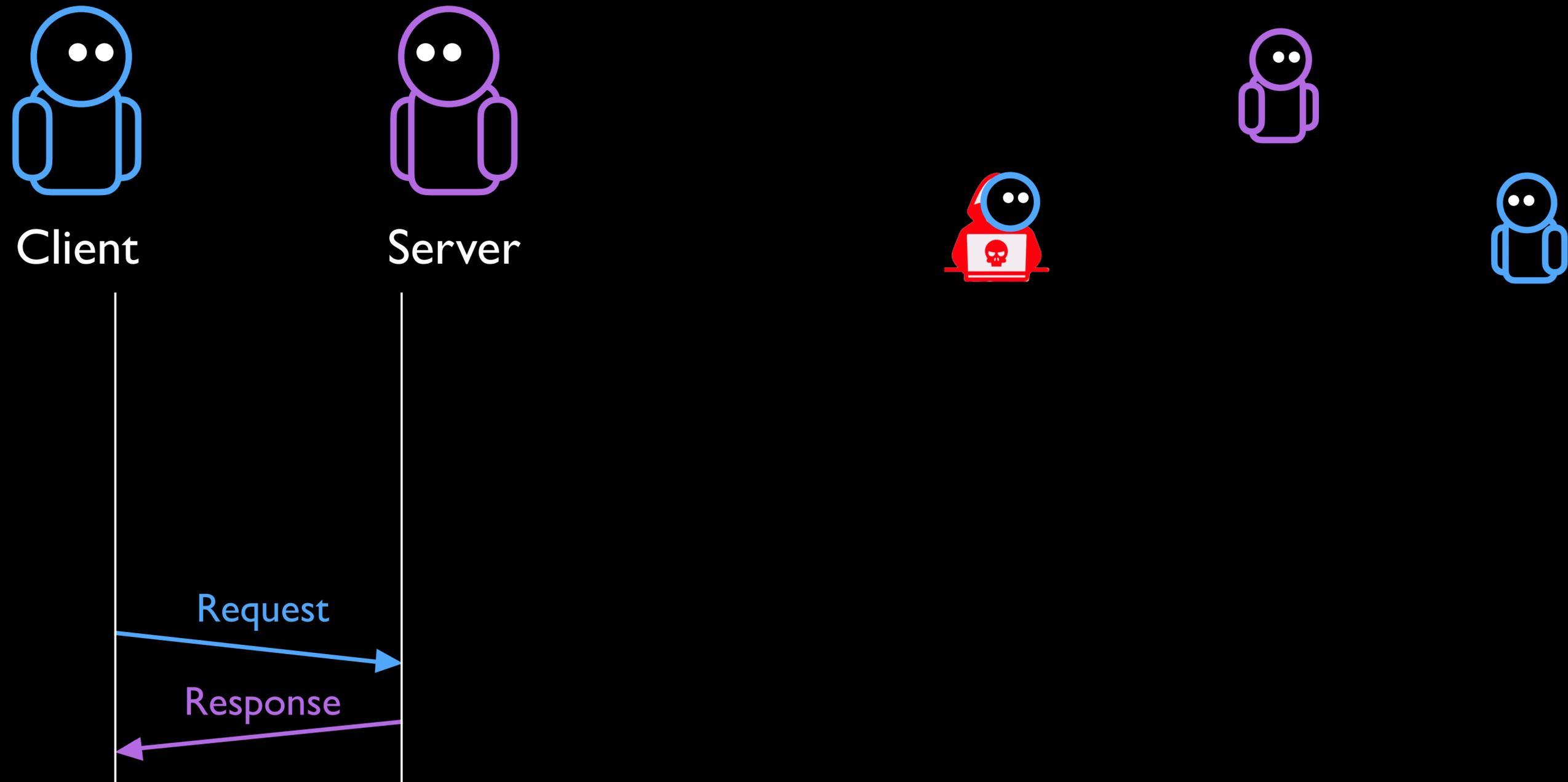
Reflected amplification attacks

UDP is connection-less



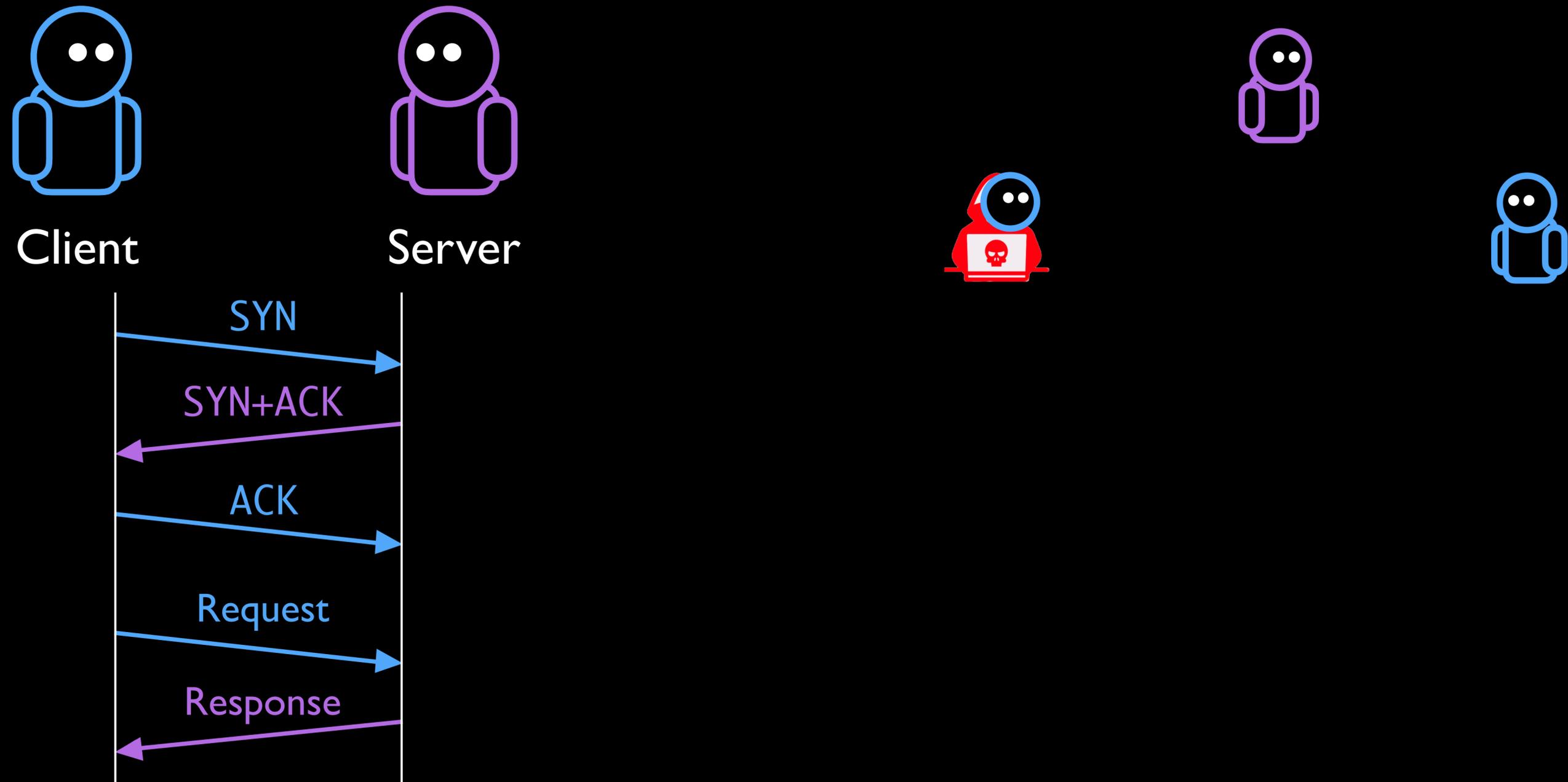
Reflected amplification attacks

TCP requires a threeway handshake



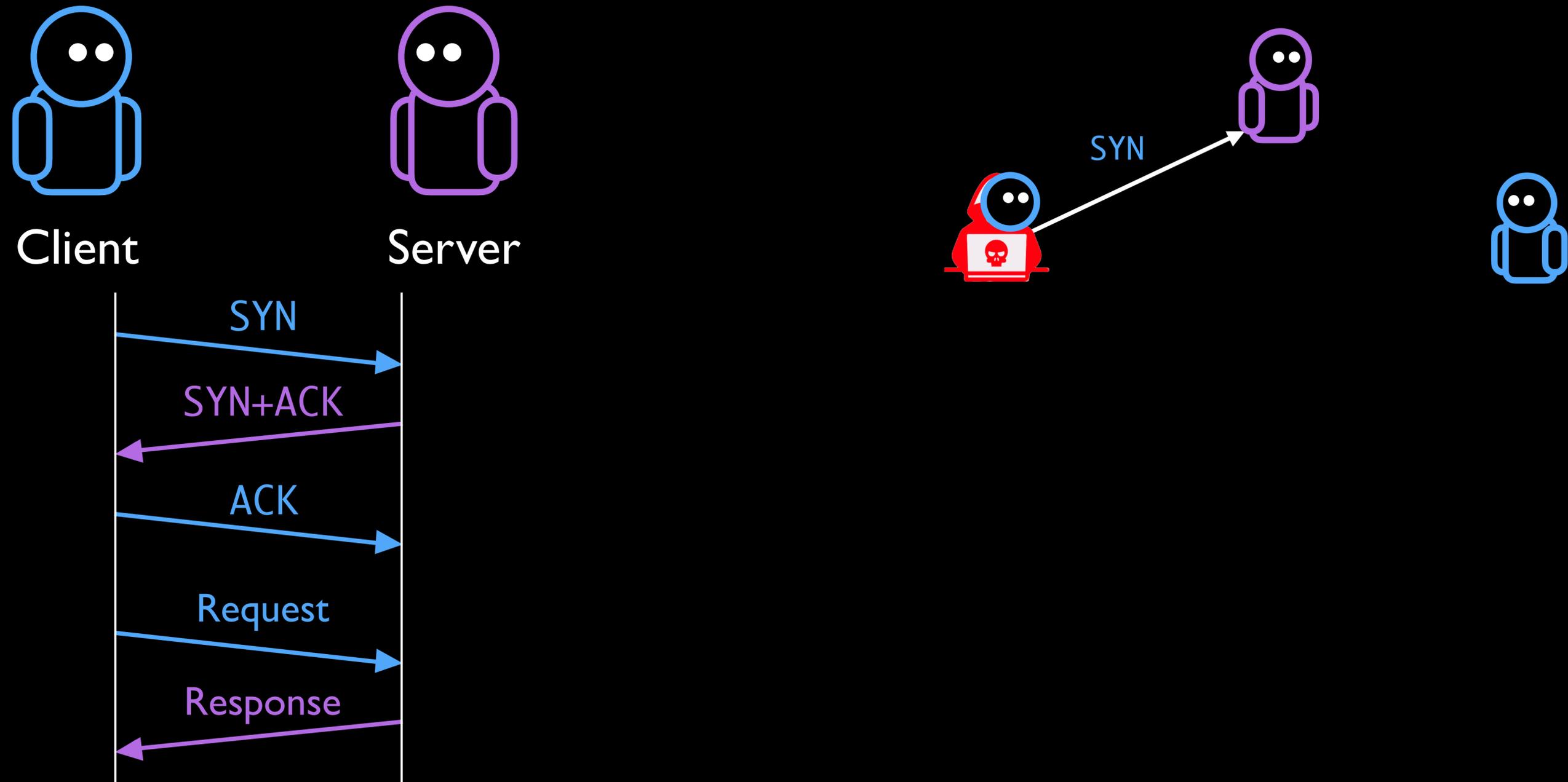
Reflected amplification attacks

TCP requires a threeway handshake



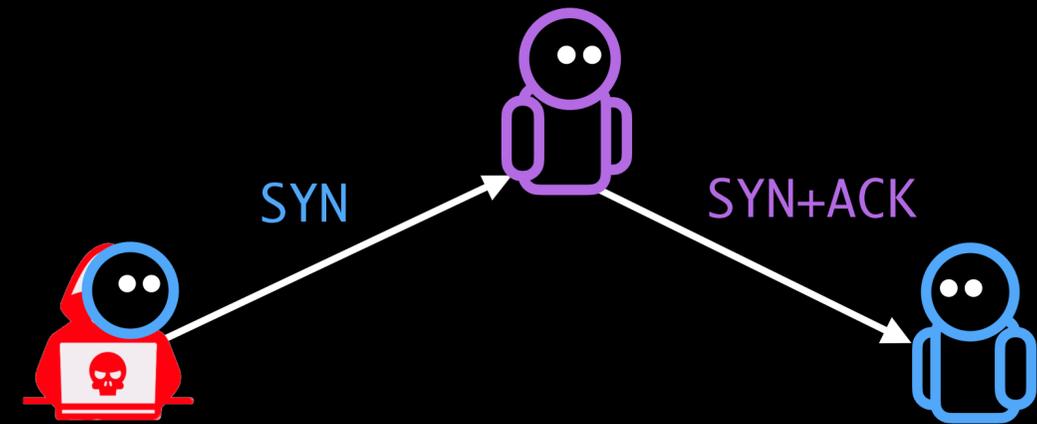
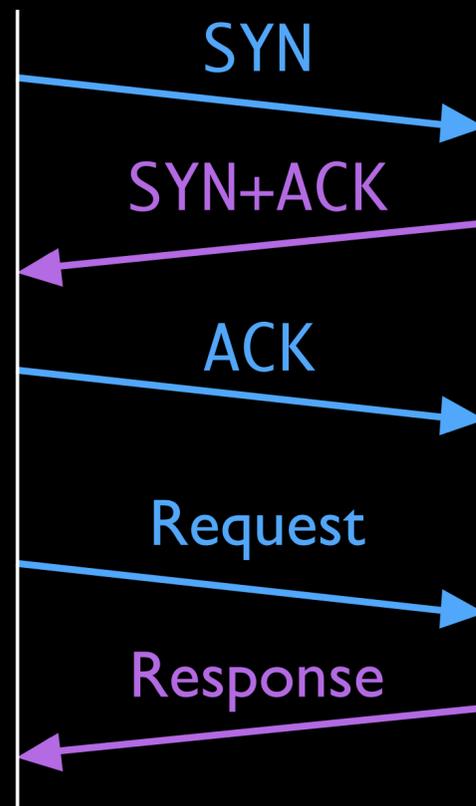
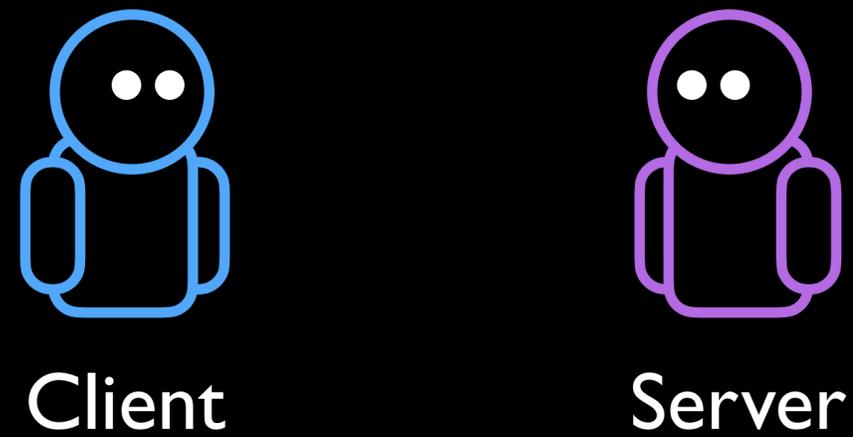
Reflected amplification attacks

TCP requires a threeway handshake



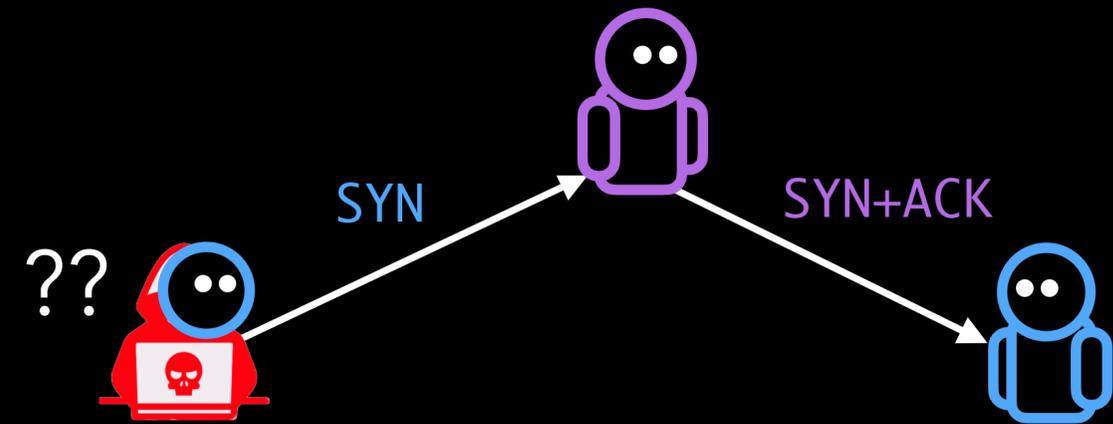
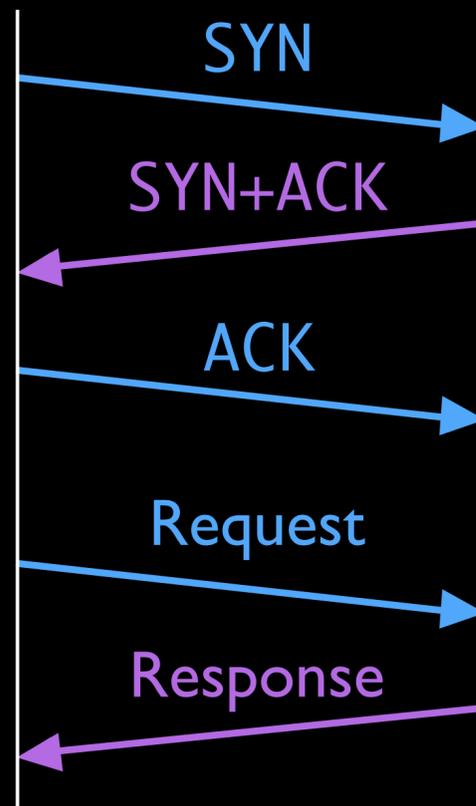
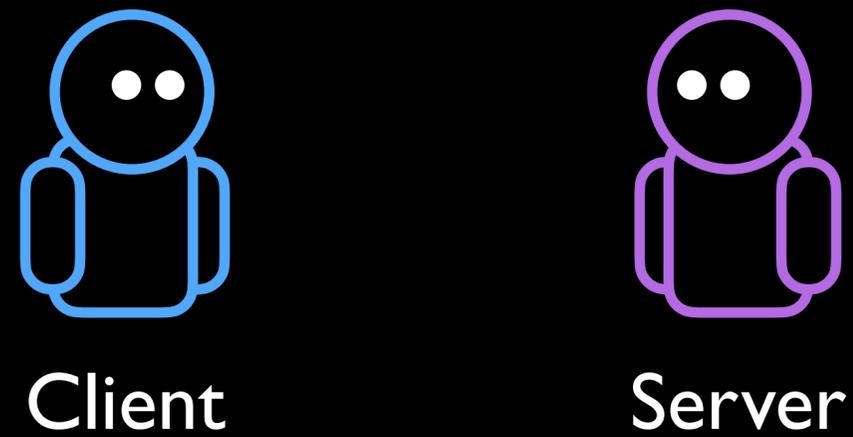
Reflected amplification attacks

TCP requires a threeway handshake



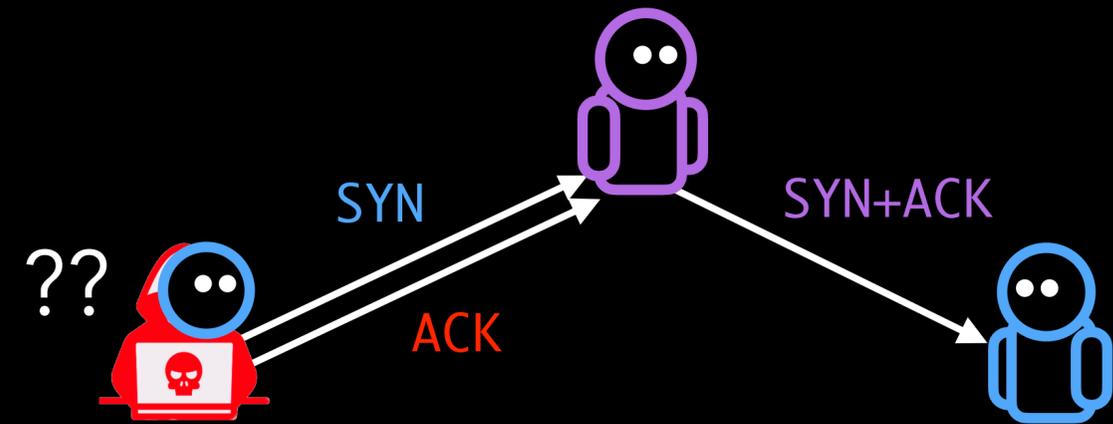
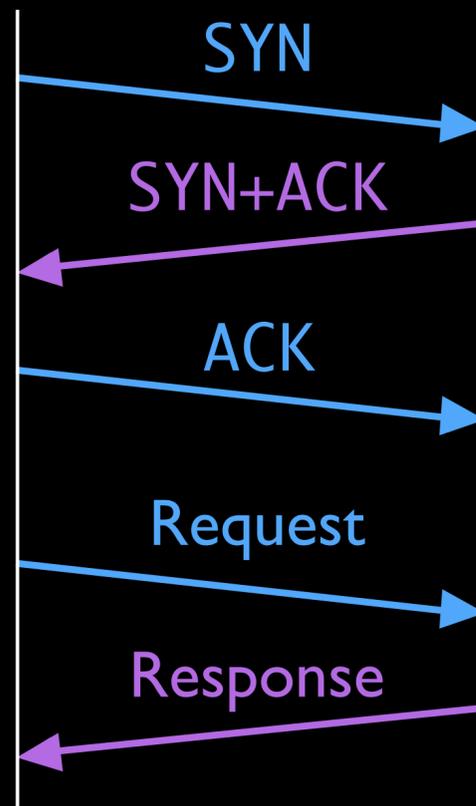
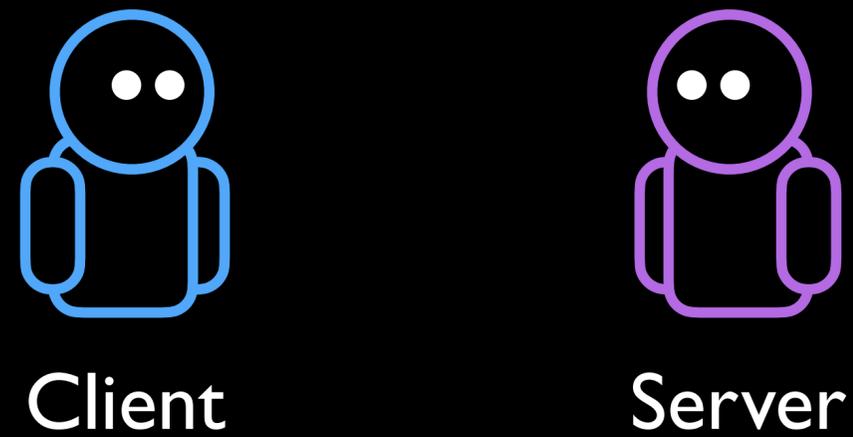
Reflected amplification attacks

TCP requires a threeway handshake



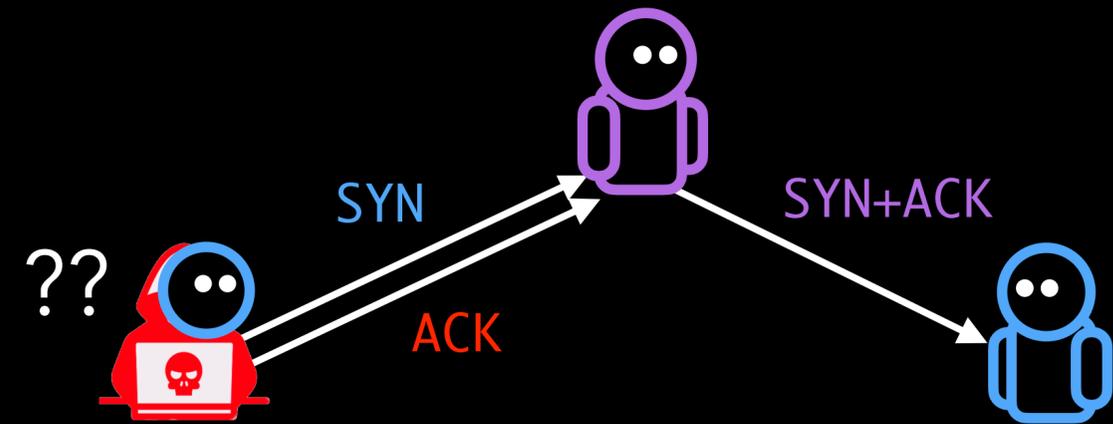
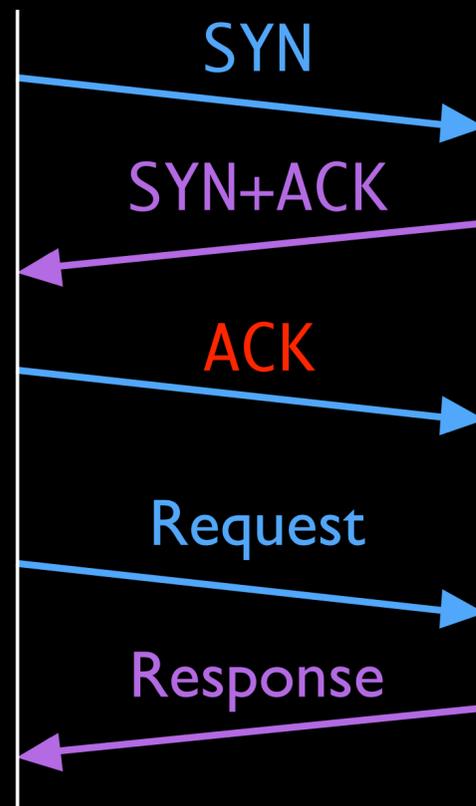
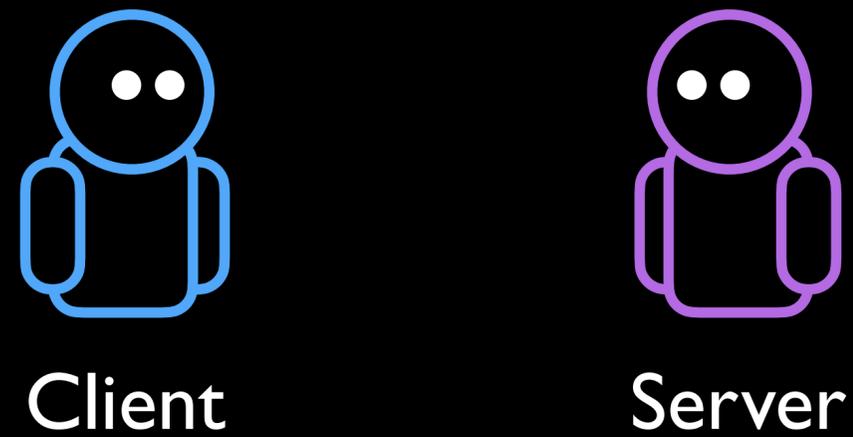
Reflected amplification attacks

TCP requires a threeway handshake



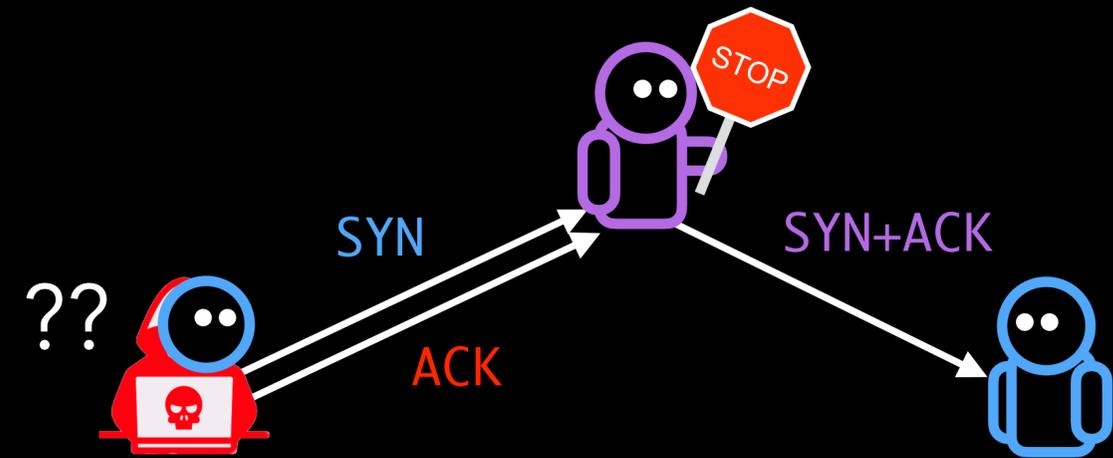
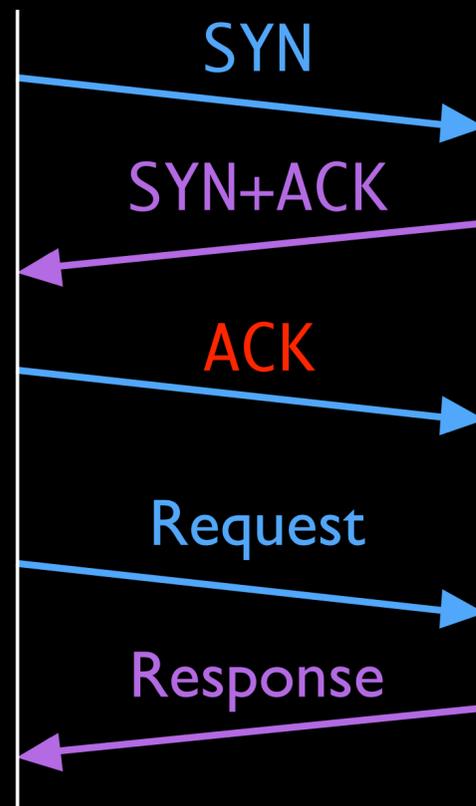
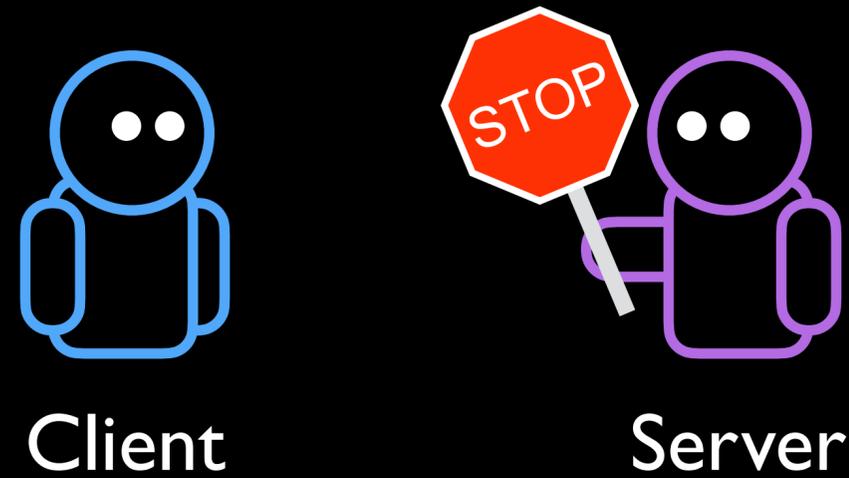
Reflected amplification attacks

TCP requires a threeway handshake



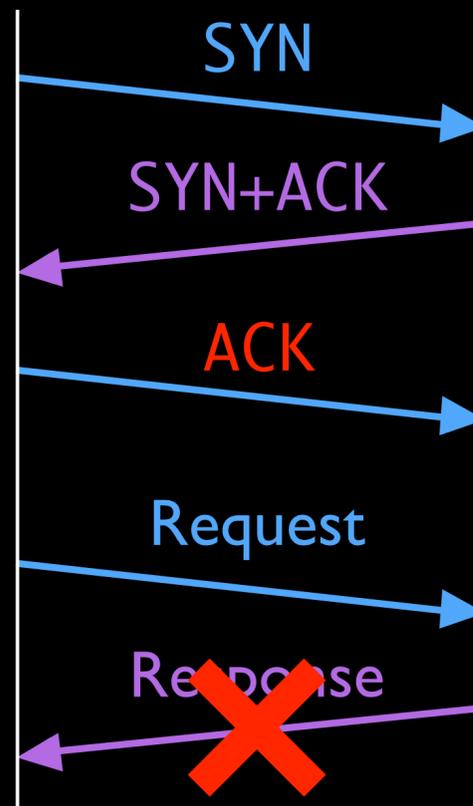
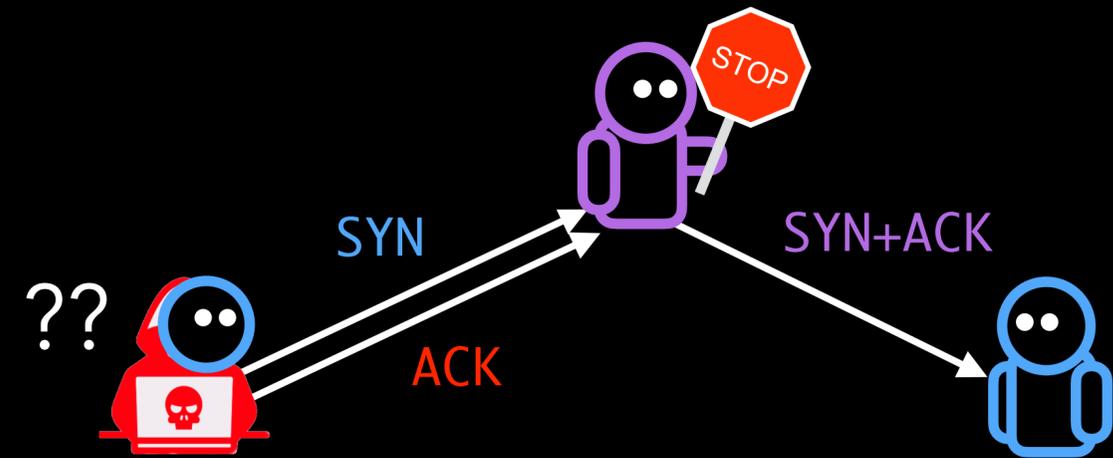
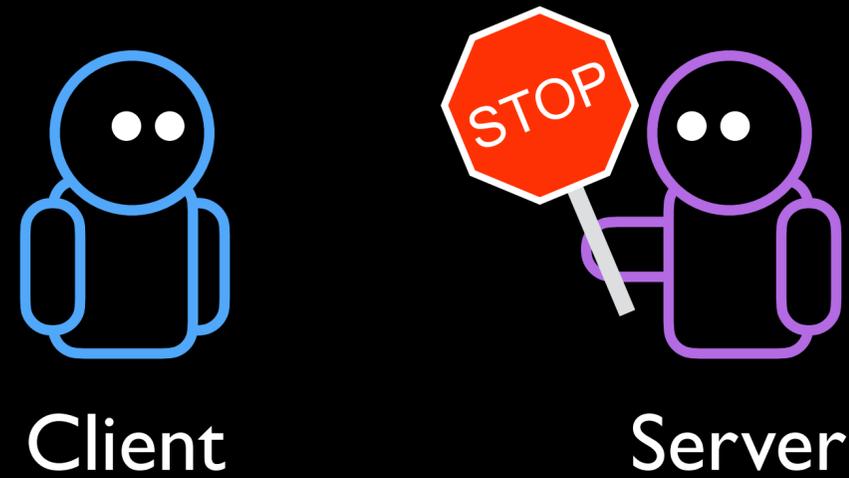
Reflected amplification attacks

TCP requires a threeway handshake



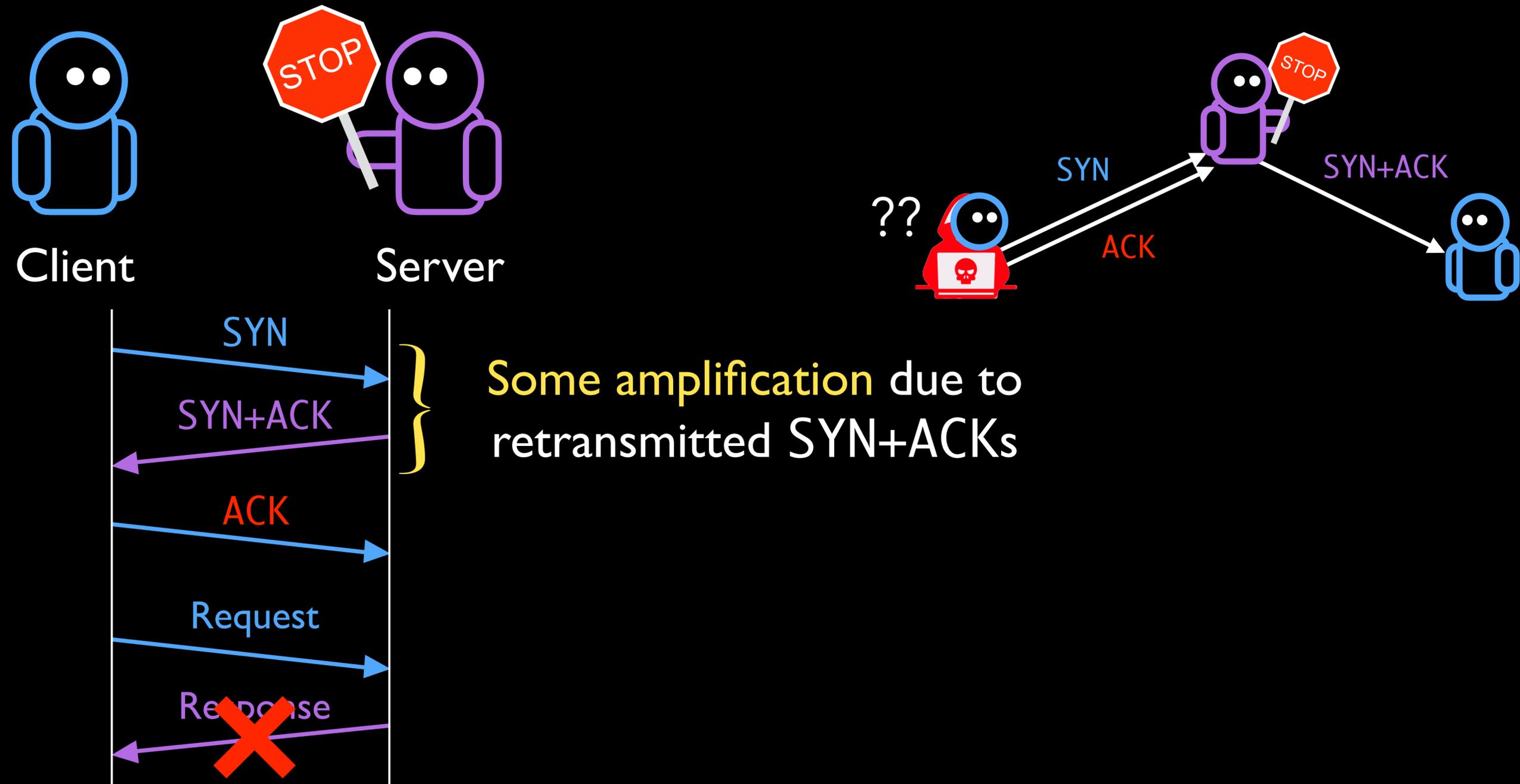
Reflected amplification attacks

TCP requires a threeway handshake



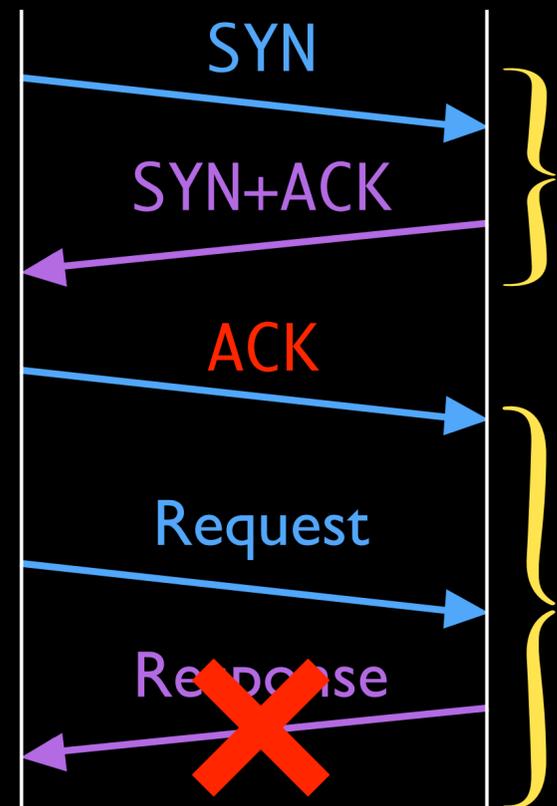
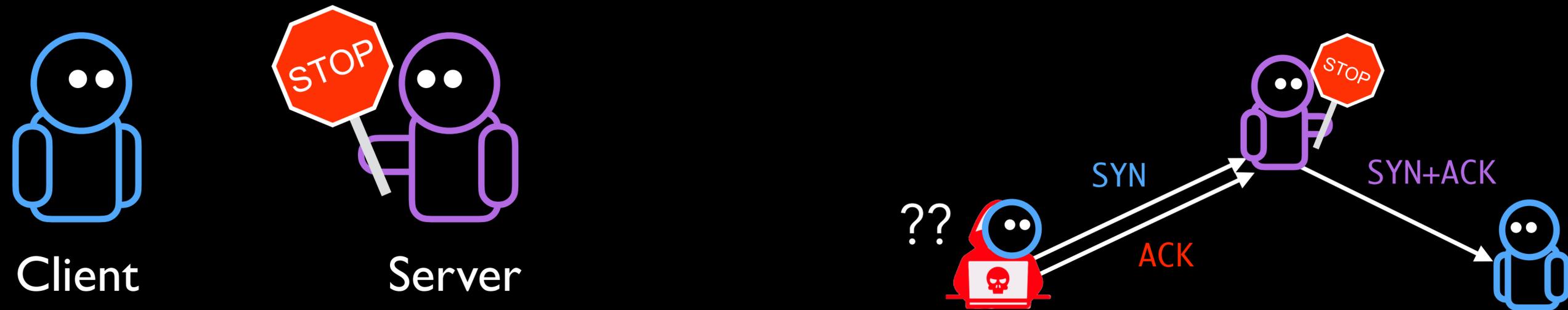
Reflected amplification attacks

TCP requires a threeway handshake



Reflected amplification attacks

TCP requires a threeway handshake



Some amplification due to retransmitted SYN+ACKs

This was believed to be off-limits to attackers

Our findings

TCP-based reflected amplification is *possible* and *effective*

- ▶ Five distinct attacks
- ▶ Millions of amplifiers
- ▶ Amplification factors in the millions

Found *infinite amplification* and identified *root causes*

Our findings

TCP-based reflected amplification is *possible* and *effective*

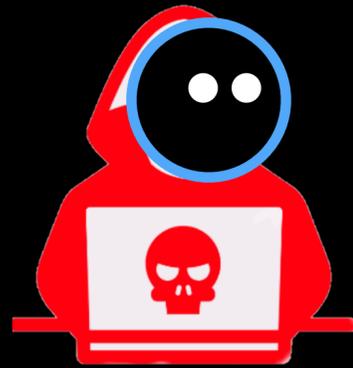
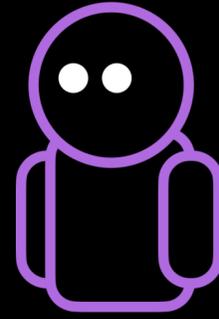
- ▶ Five distinct attacks
- ▶ Millions of amplifiers
- ▶ Amplification factors in the millions

Found *infinite amplification* and identified *root causes*

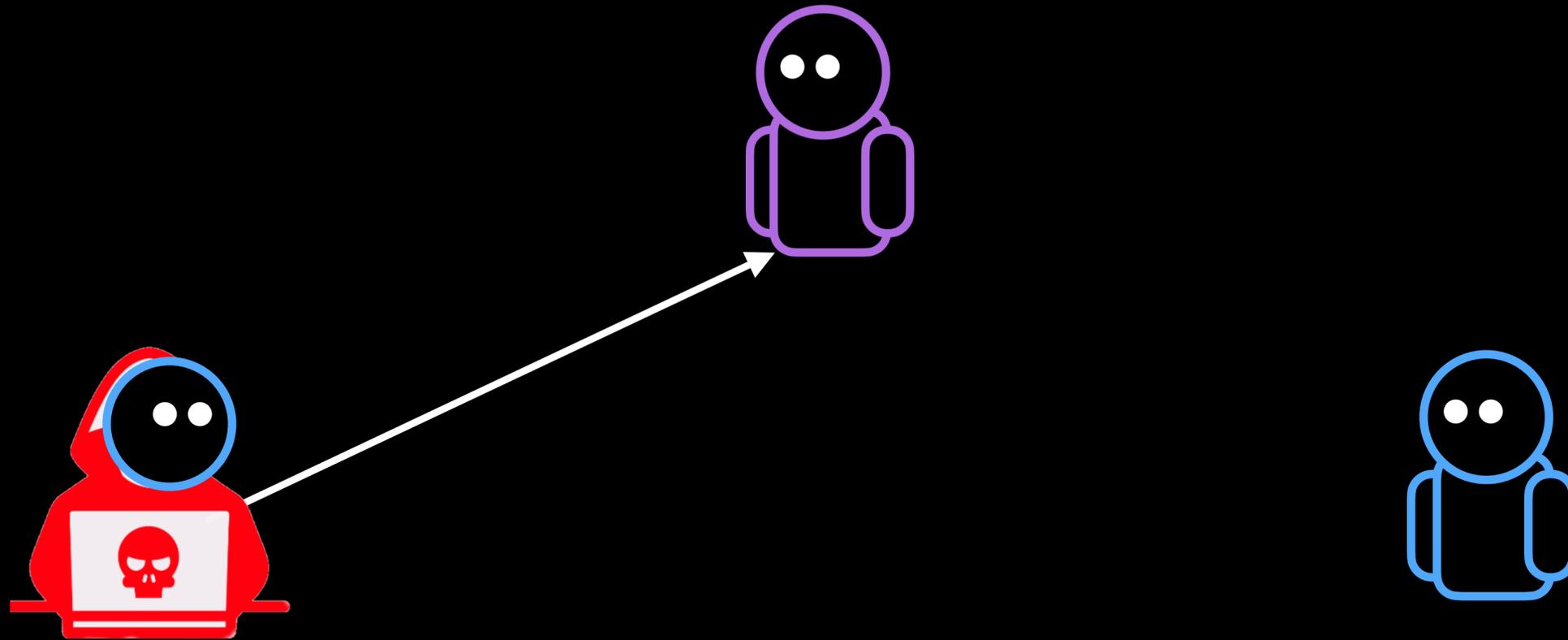
Use middleboxes as amplifiers!

Weaponizing middleboxes

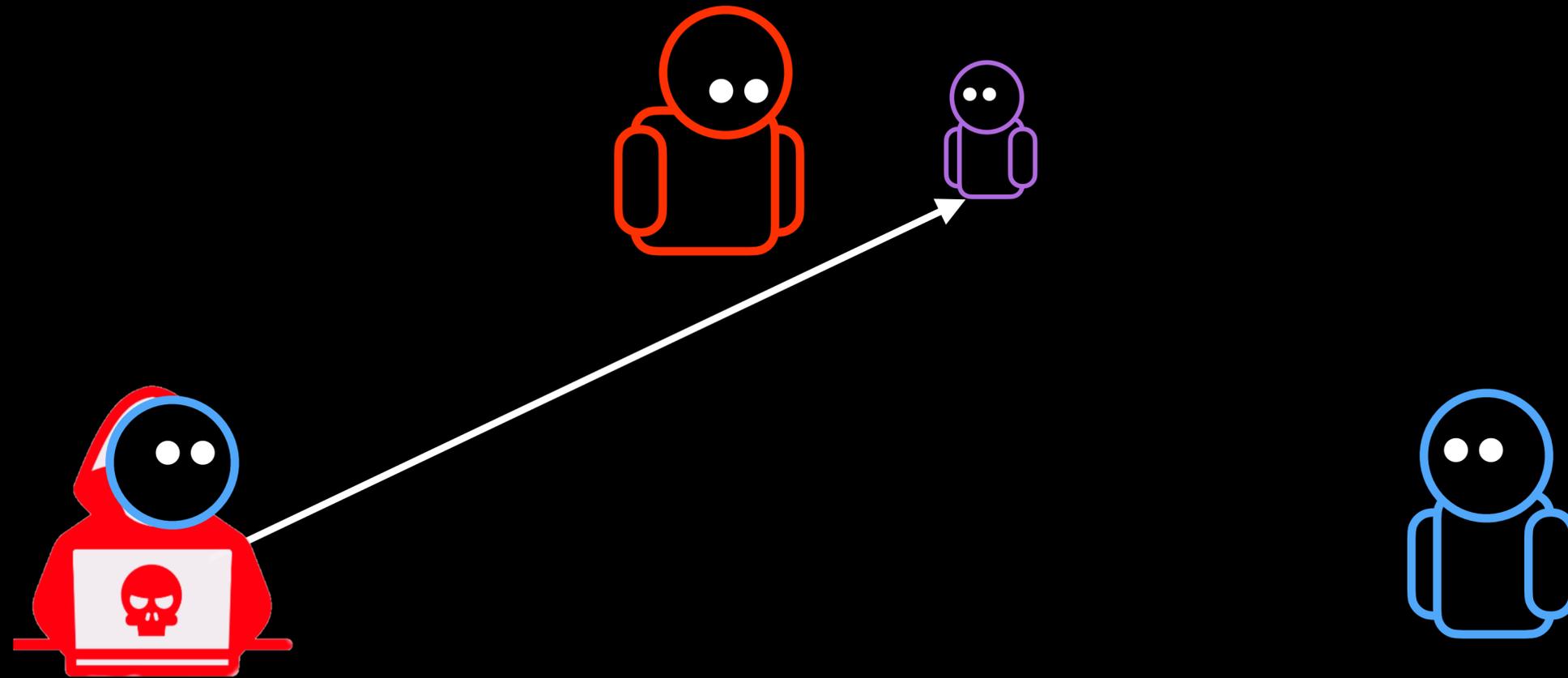
Weaponizing middleboxes



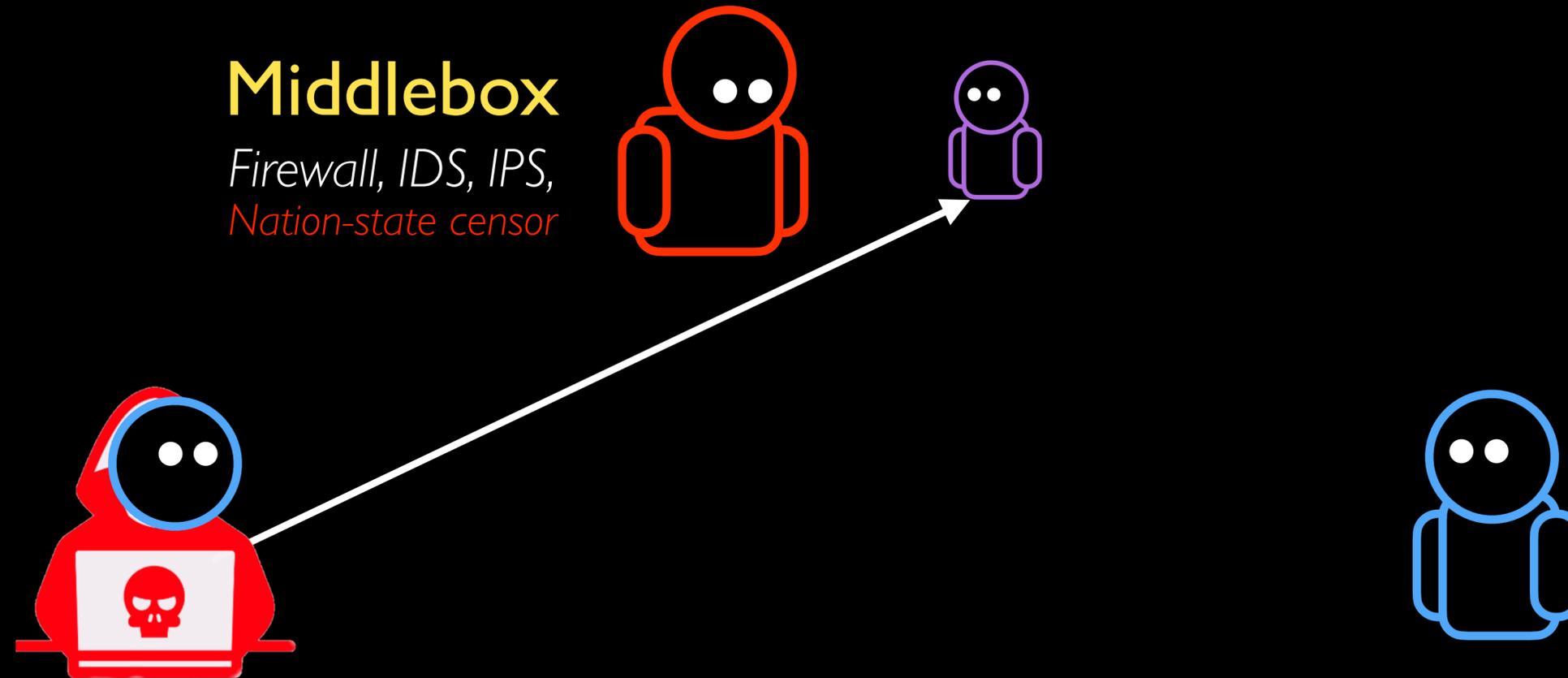
Weaponizing middleboxes



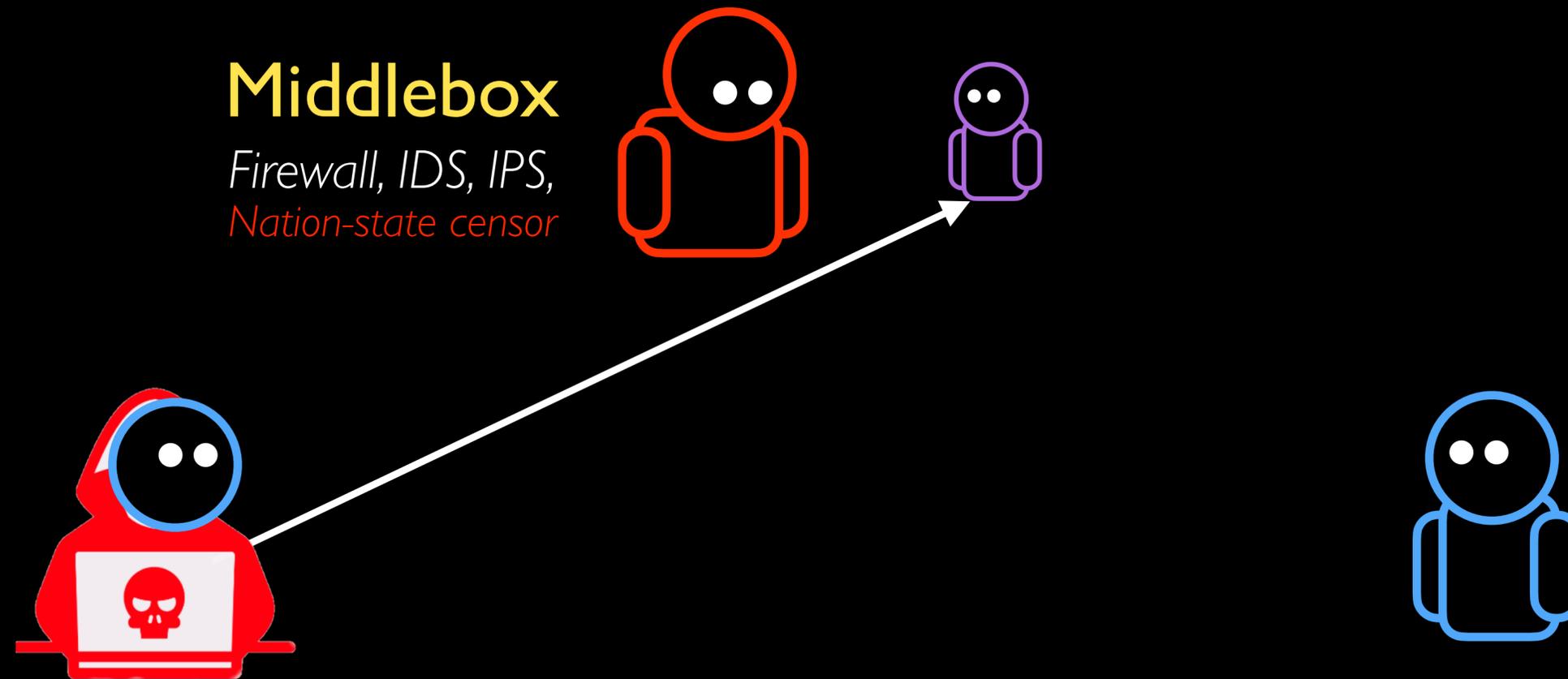
Weaponizing middleboxes



Weaponizing middleboxes

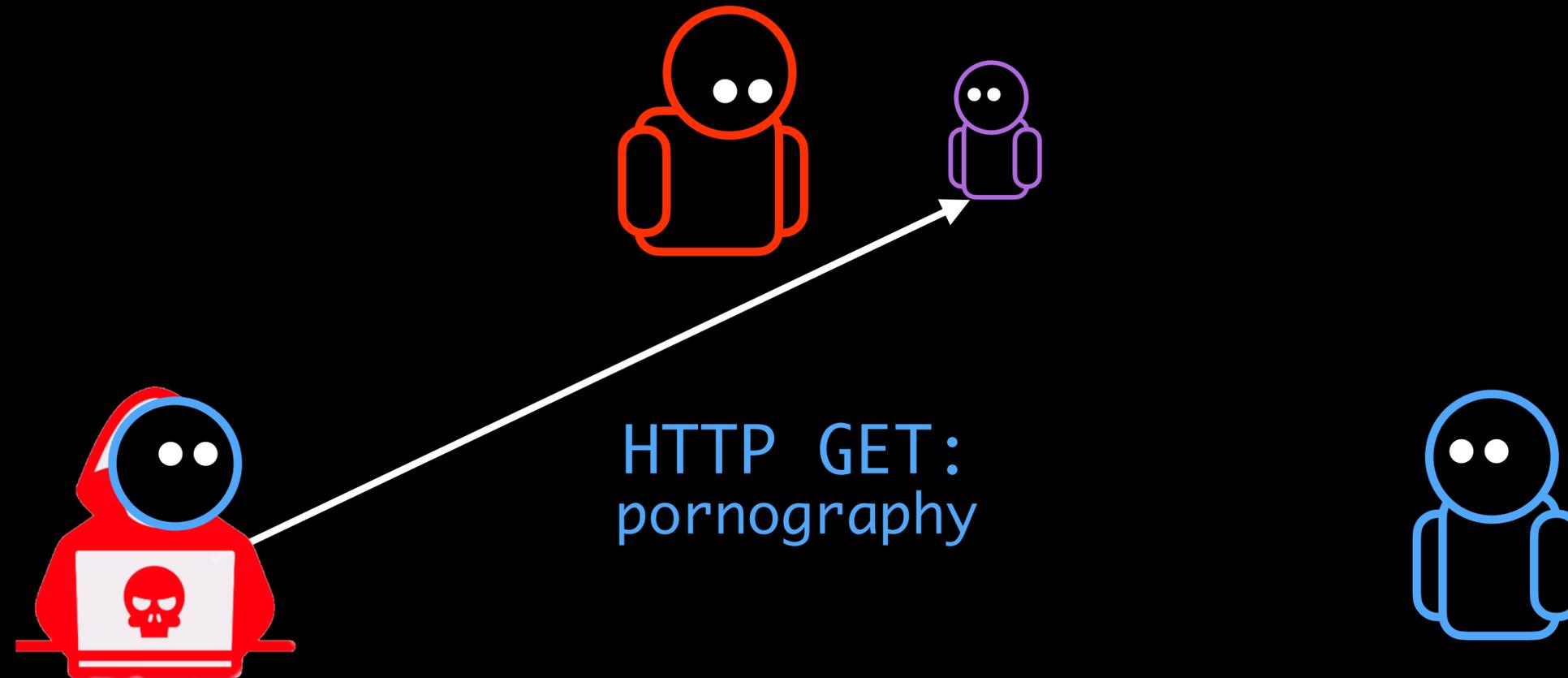


Weaponizing middleboxes



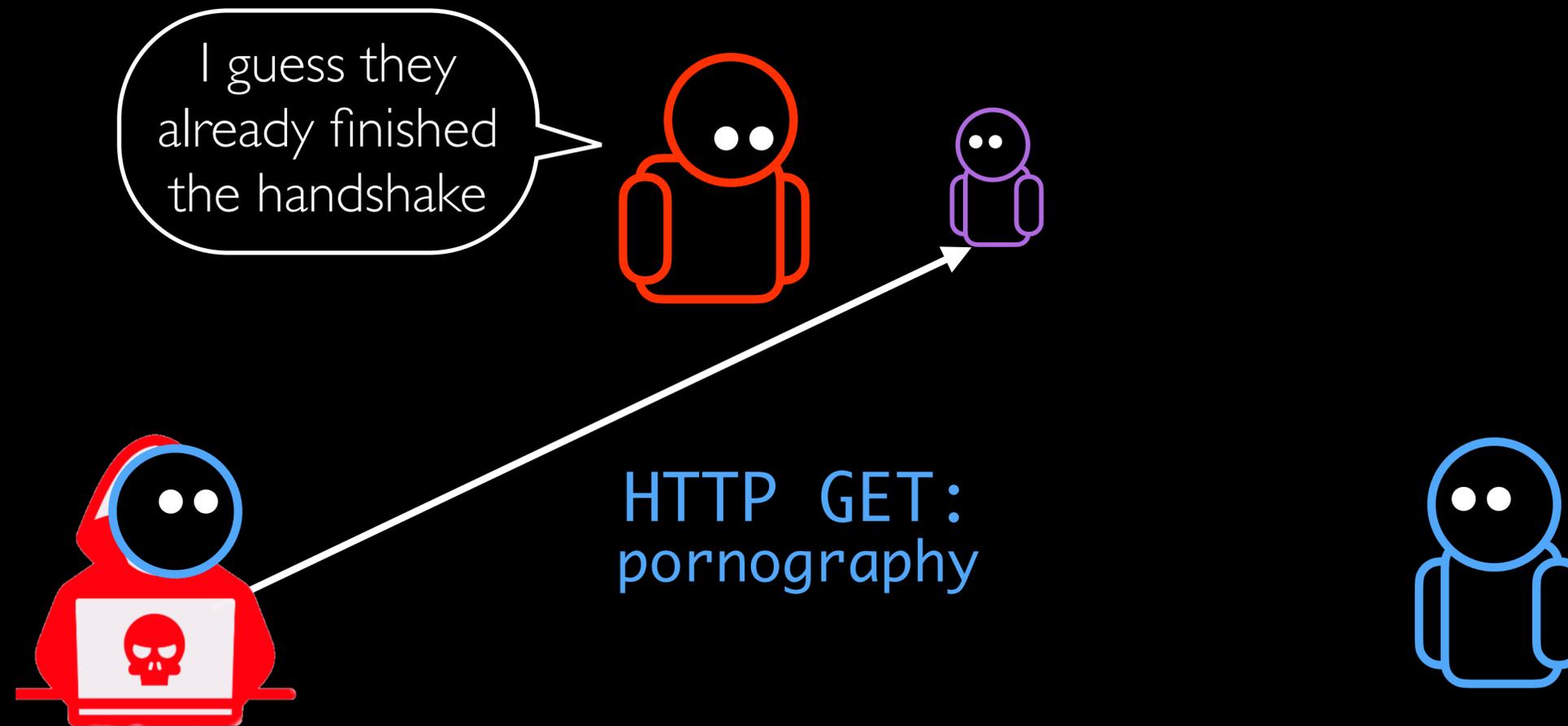
① Middleboxes expect to miss some packets

Weaponizing middleboxes



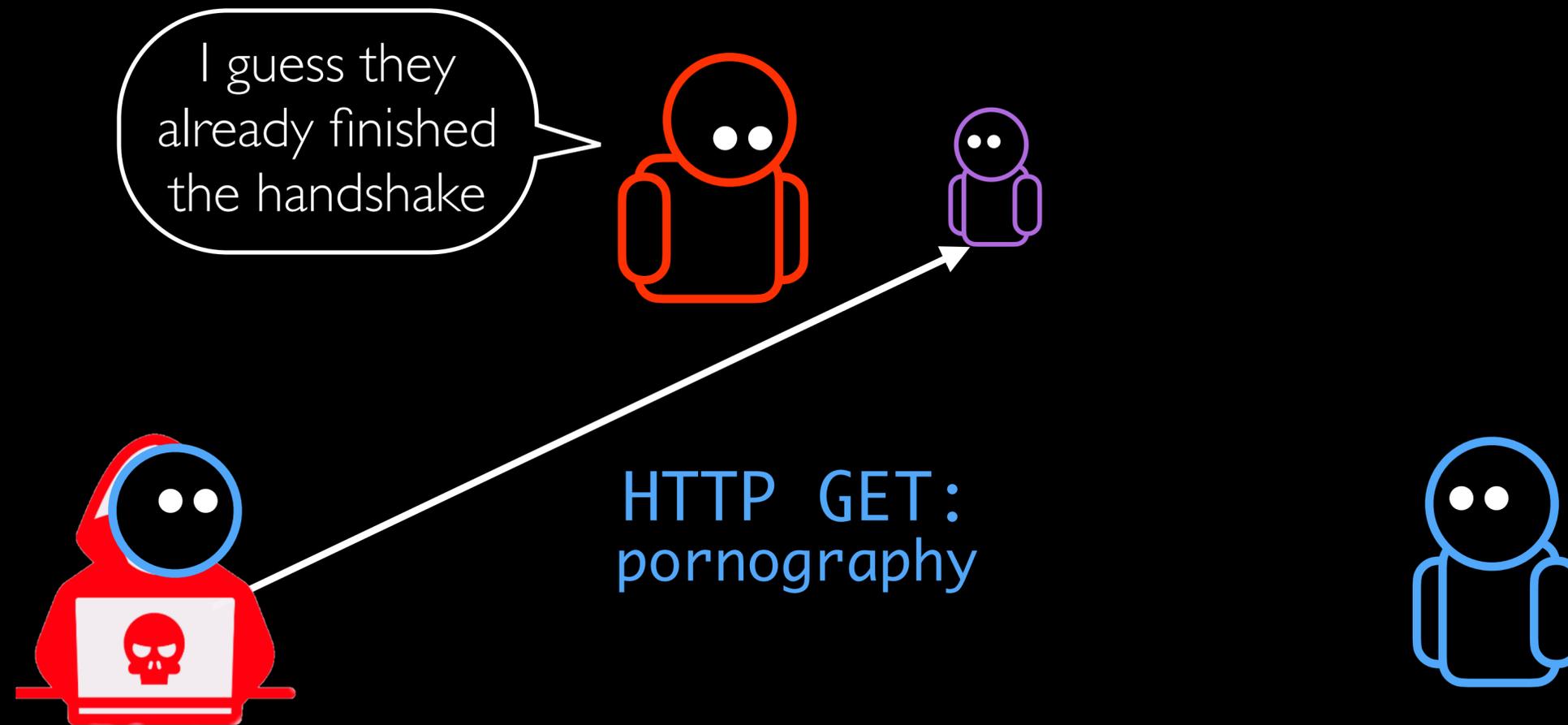
① Middleboxes expect to miss some packets

Weaponizing middleboxes



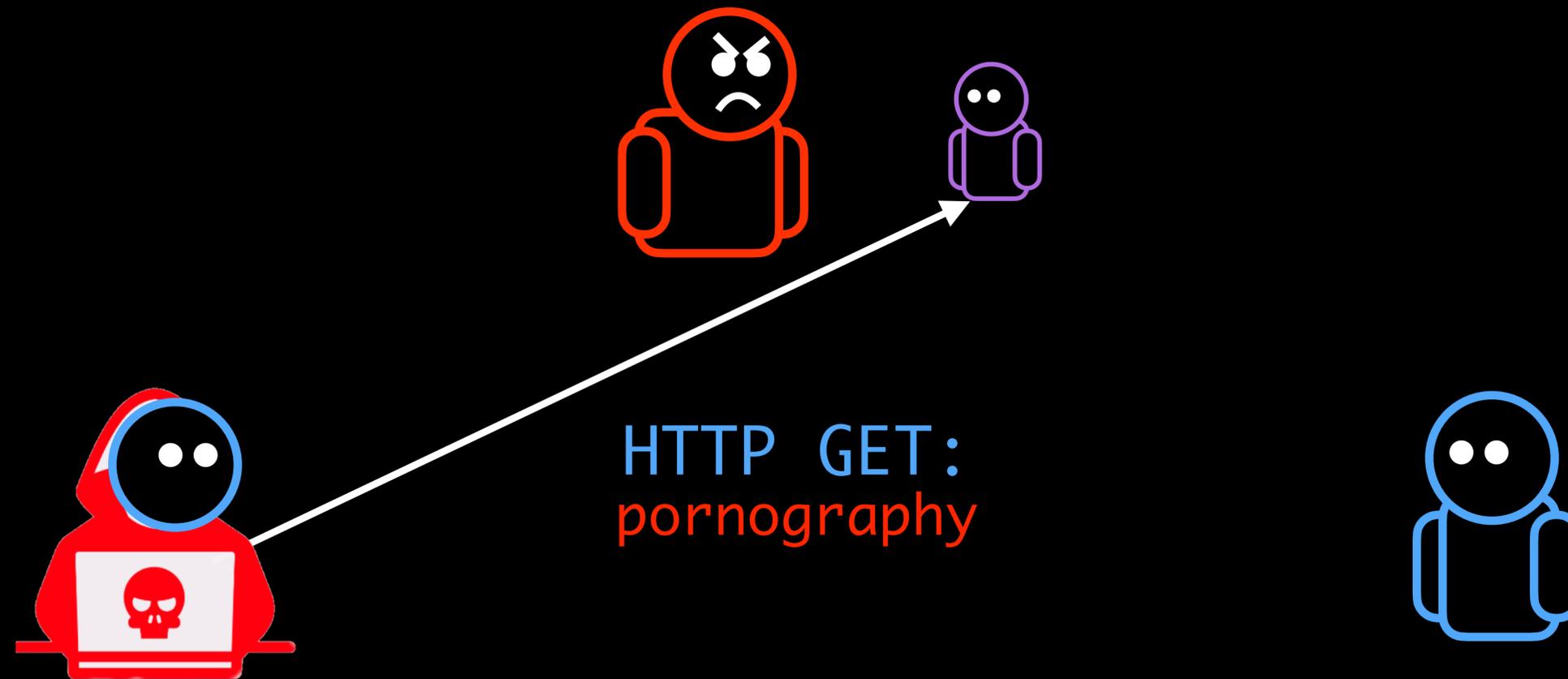
① Middleboxes expect to miss some packets

Weaponizing middleboxes



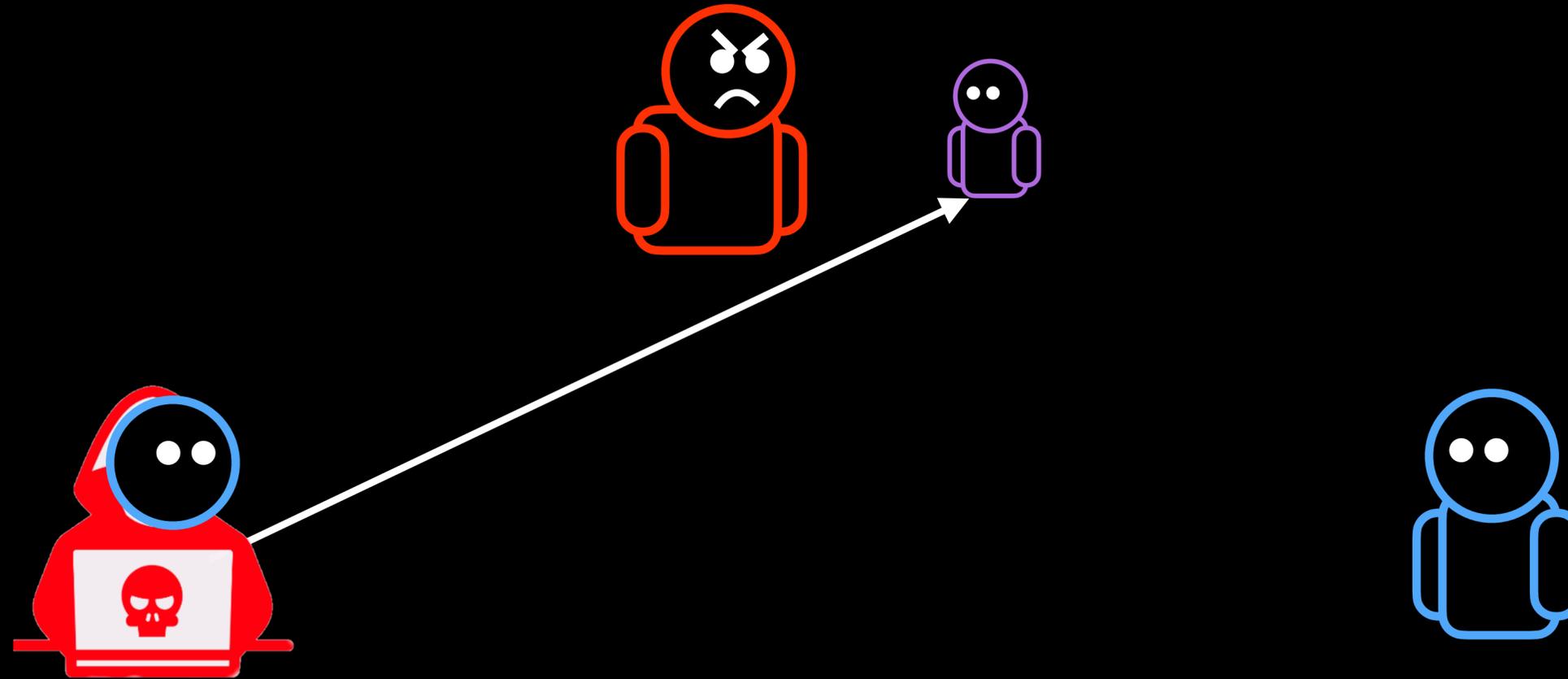
- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes



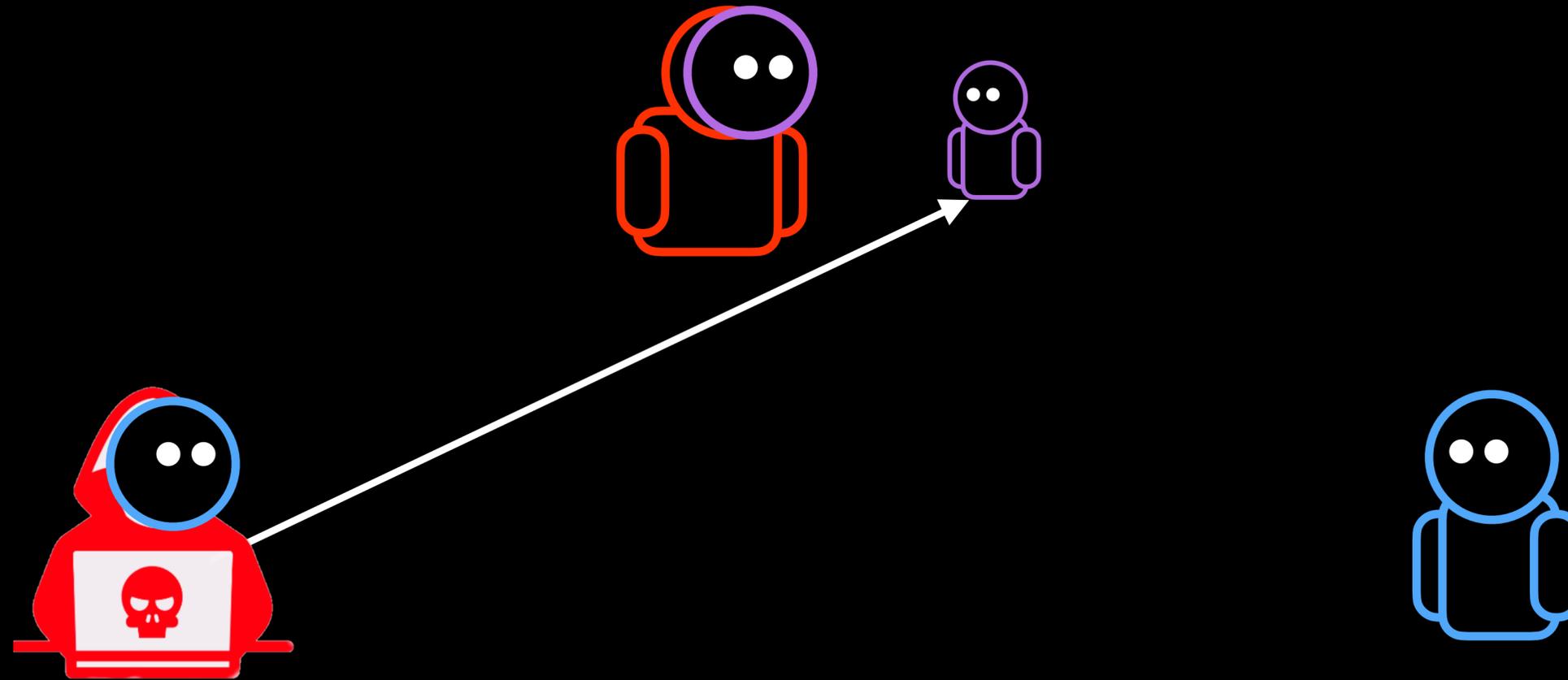
- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes



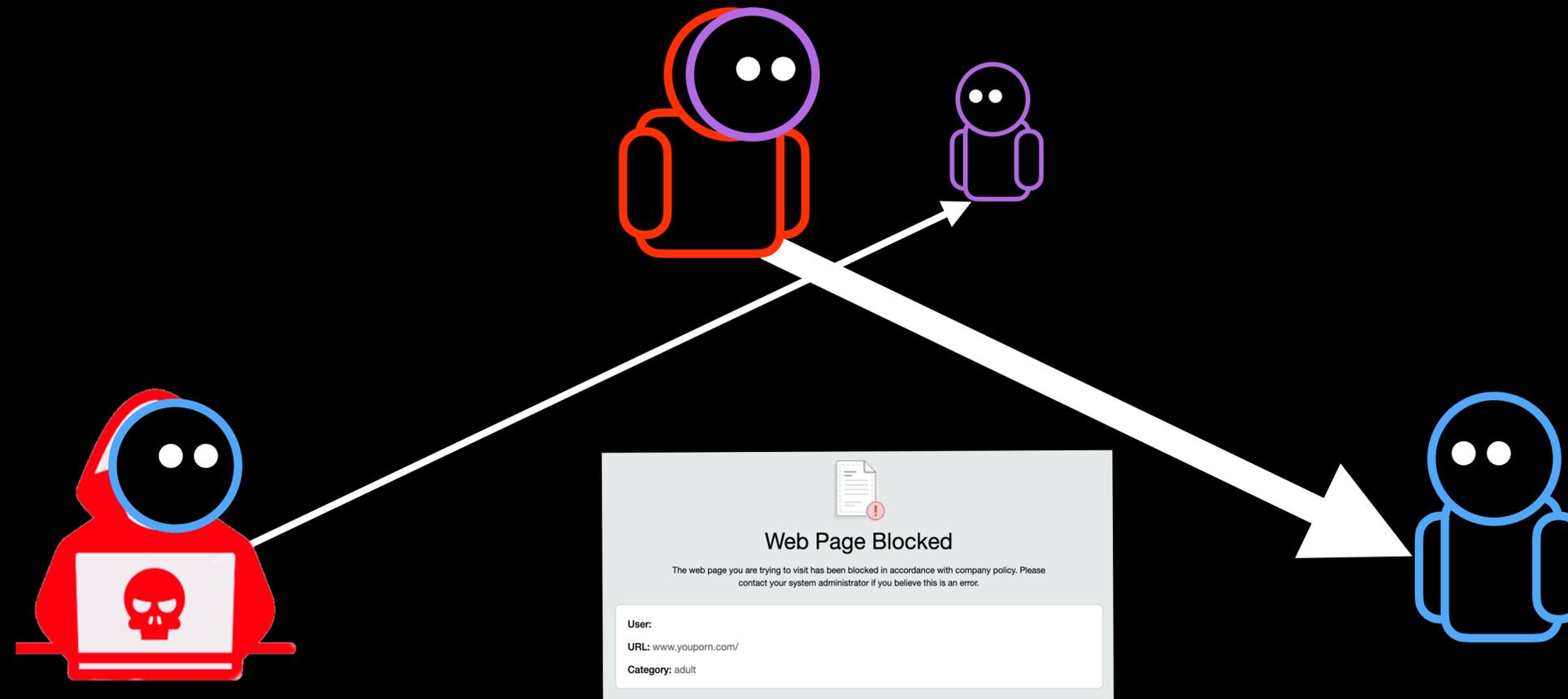
- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes



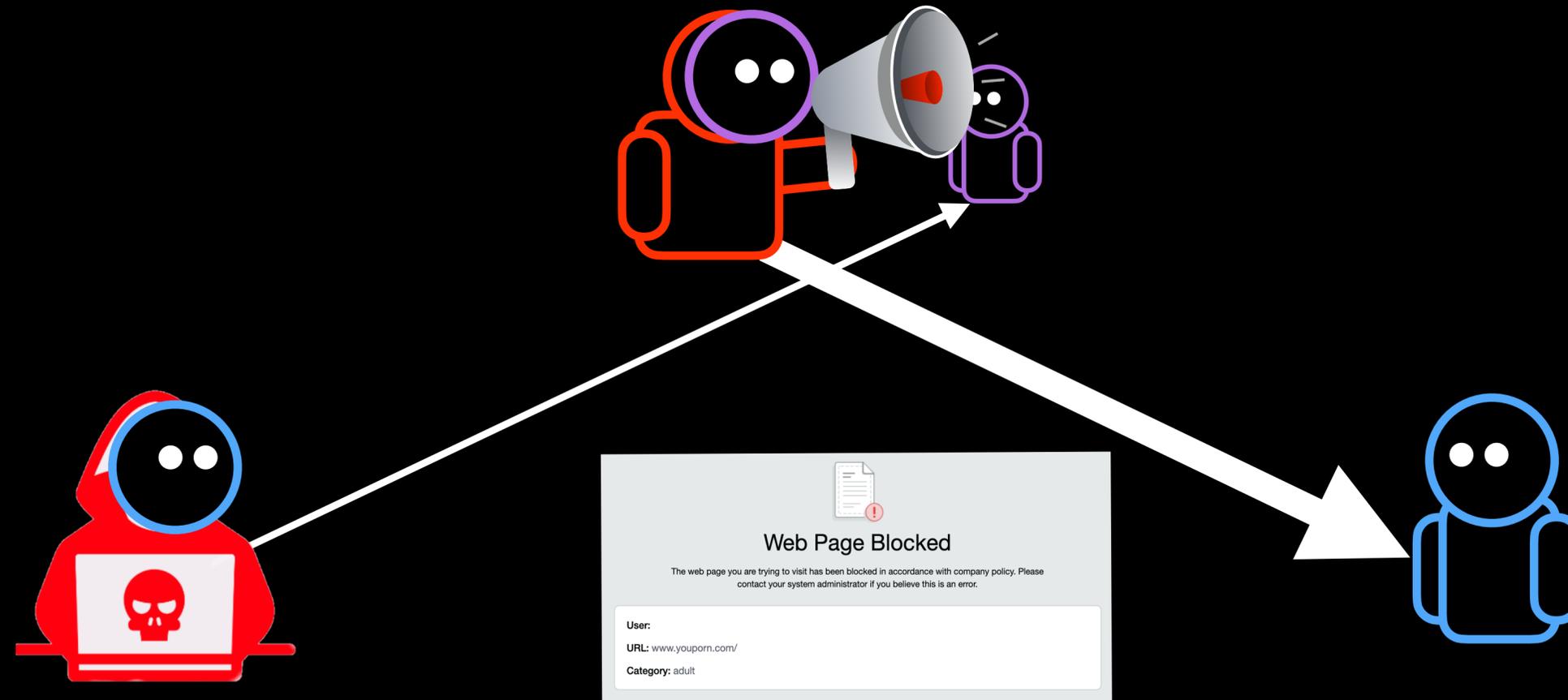
- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes



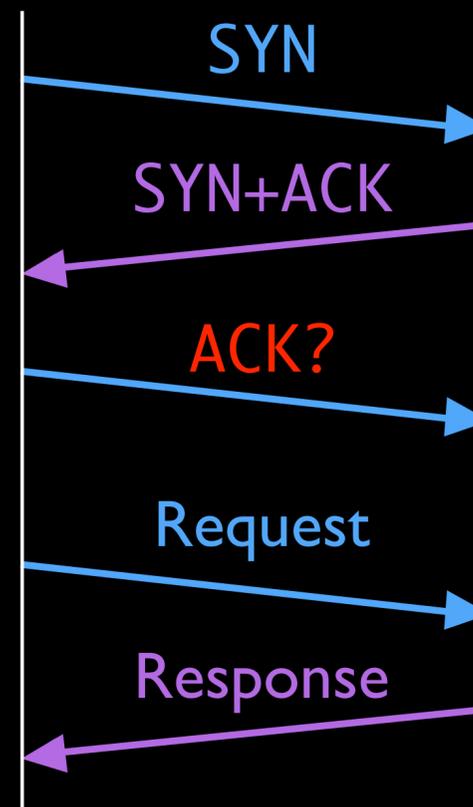
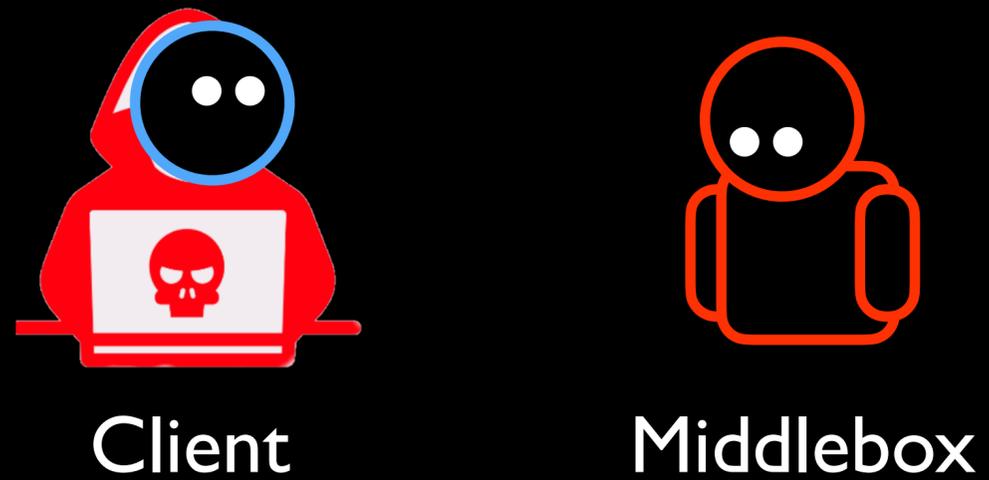
- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes

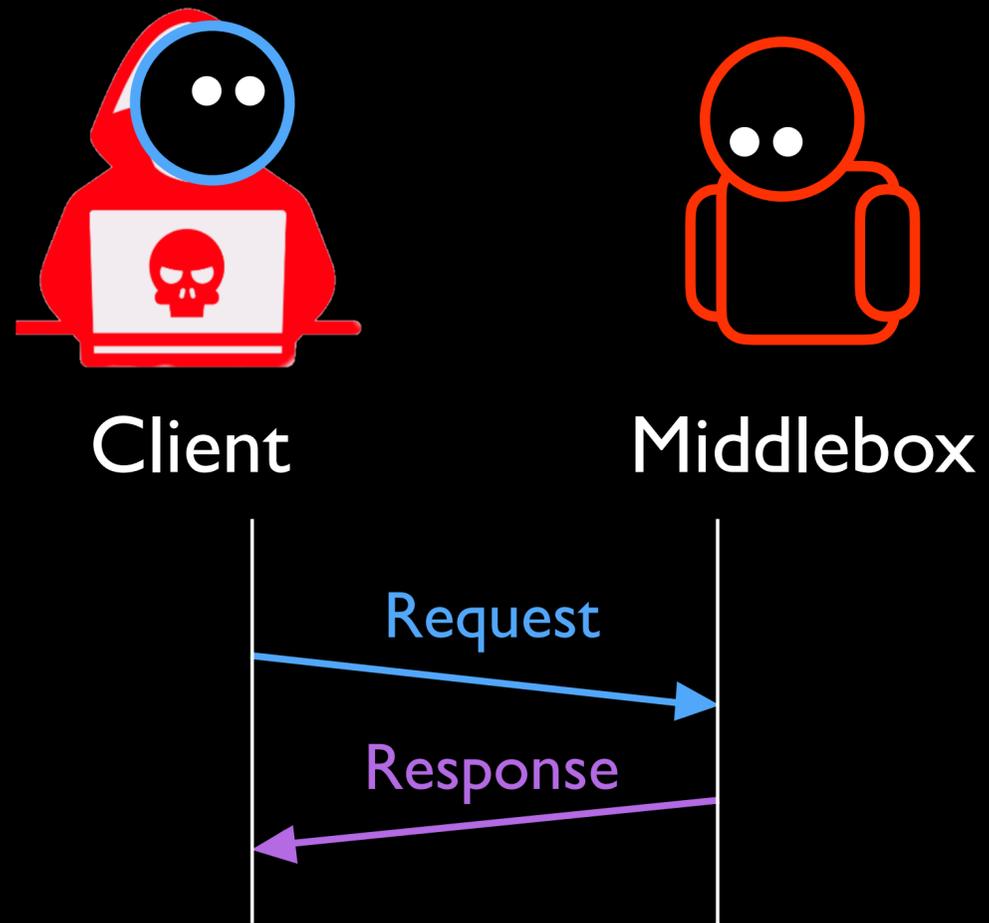


- ① Middleboxes expect to miss some packets
- ② Middleboxes *inject traffic* to block connections

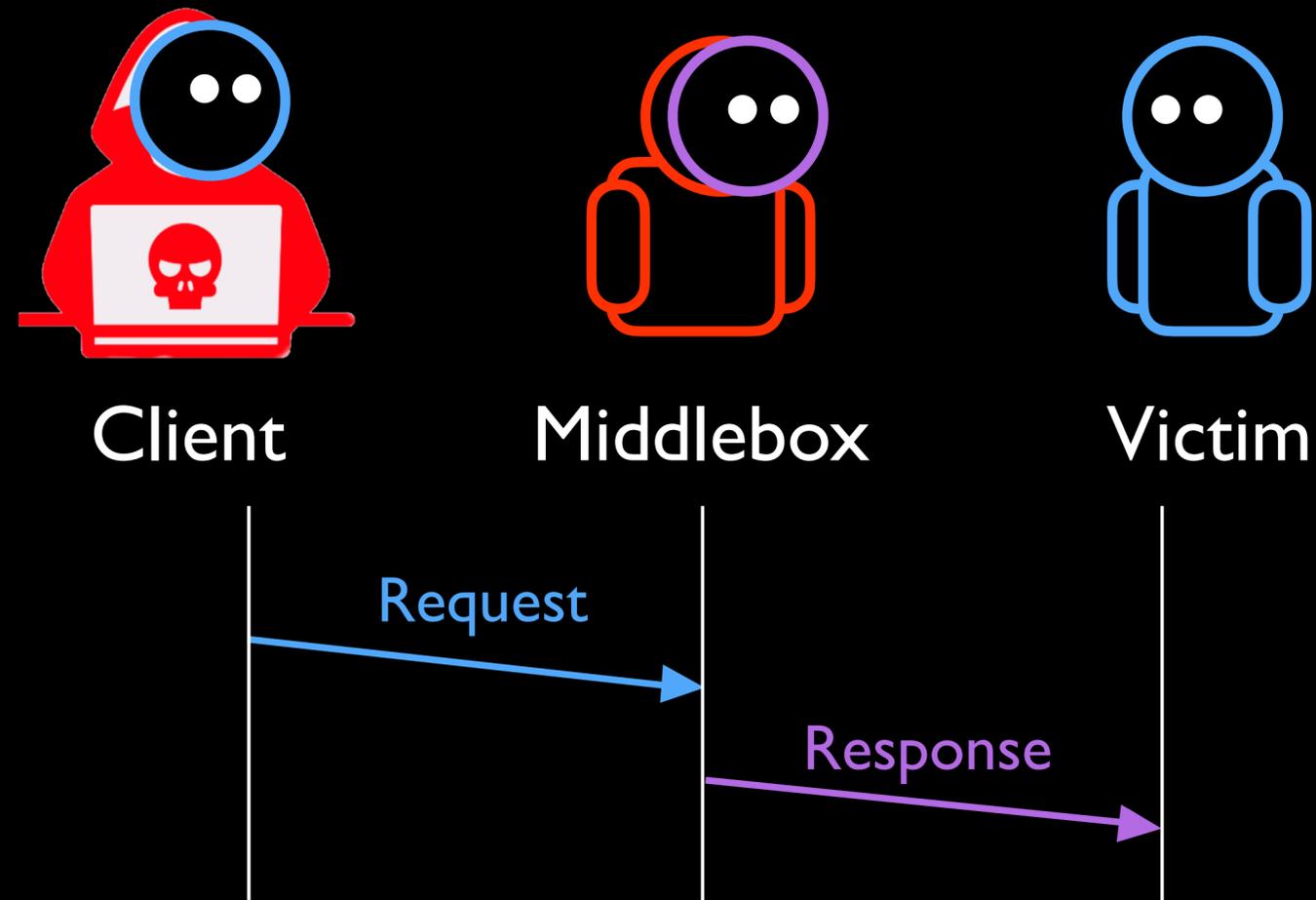
Middleboxes make TCP-based amplification possible



Middleboxes make TCP-based amplification possible



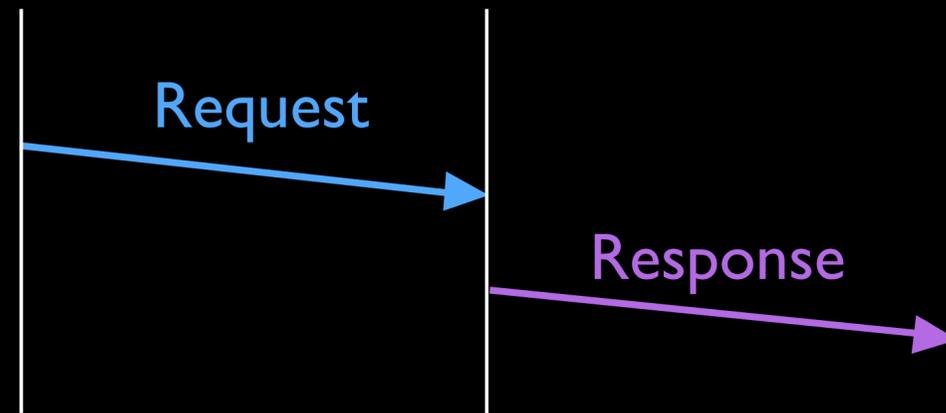
Middleboxes make TCP-based amplification possible



Middleboxes make TCP-based amplification possible



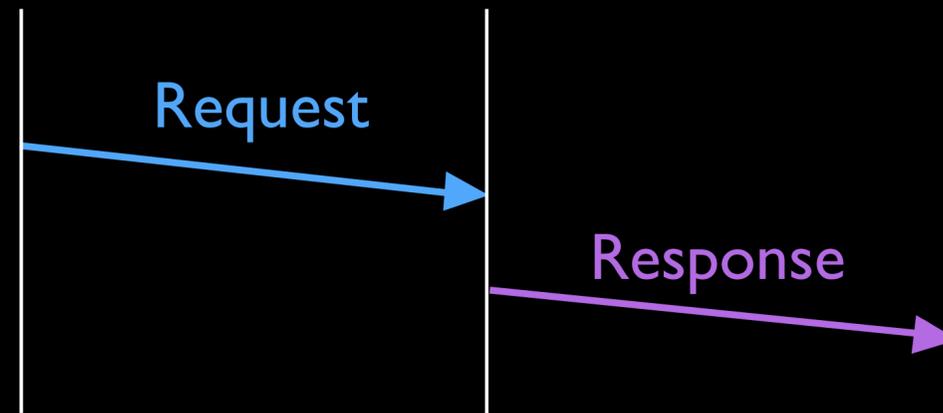
What packets best trigger middleboxes?



Middleboxes make TCP-based amplification possible



What packets best trigger middleboxes?



What amplifications are attainable?

Methodology

① Automated Discovery

Geneva
Genetic Evasion



Train

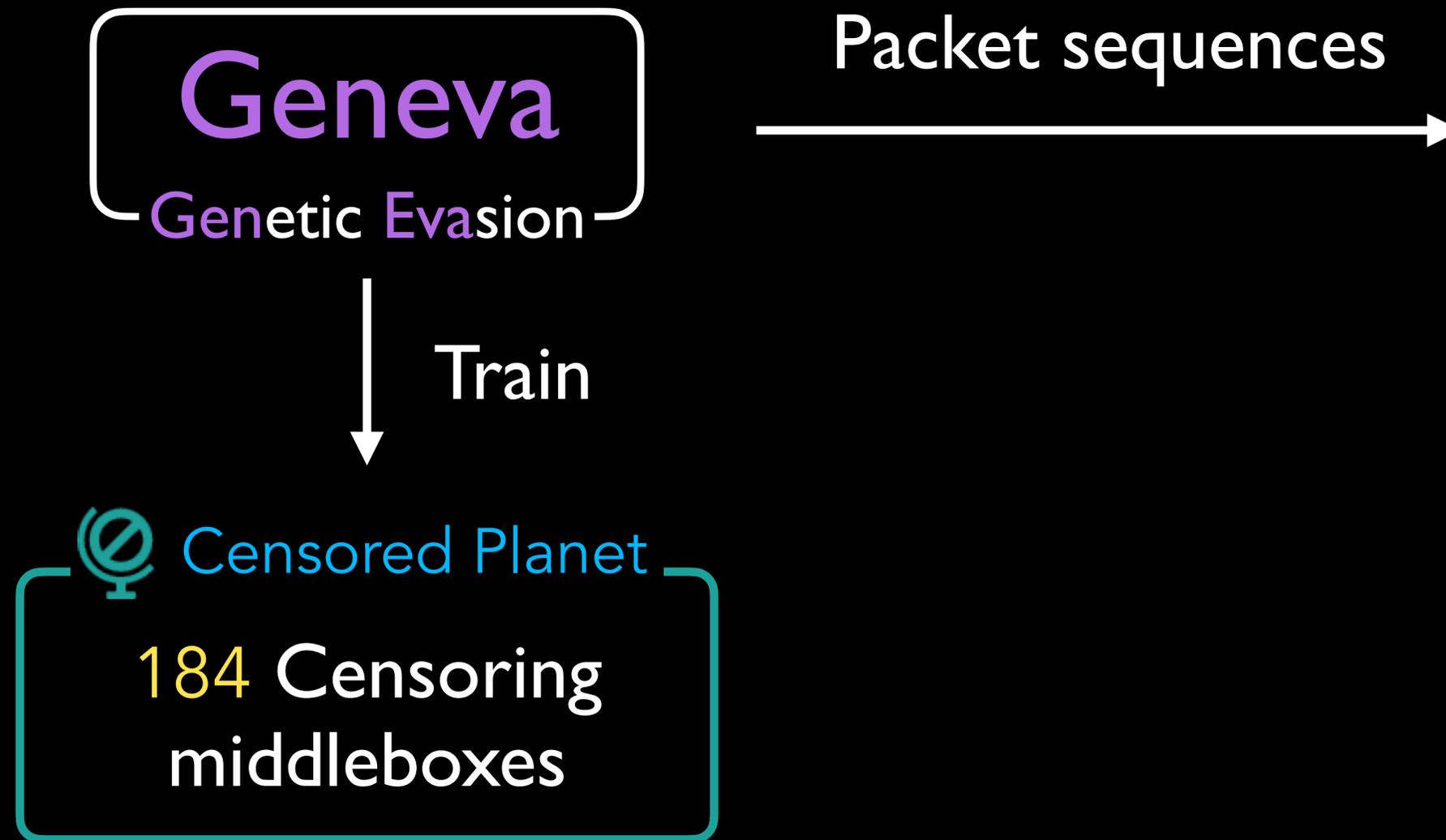


Censored Planet

184 Censoring
middleboxes

Methodology

① Automated Discovery



Methodology

① Automated Discovery

Geneva
Genetic Evasion

Train

 Censored Planet

184 Censoring
middleboxes

Packet sequences

② Internet-wide Evaluation

 **zmap**

IPv4-wide scans
(~3.7 billion)

- 35 Internet-wide scans
- Only “attacked” ourselves
- Responsibly disclosed our findings

TCP-based amplification attacks

Issue an HTTP request for **forbidden content**

Packet sequences

SYN with Request

Request

SYN ; Request

TCP-based amplification attacks

Issue an HTTP request for **forbidden content**

Packet sequences

SYN *with Request*

HTTP request
in the SYN payload

Request

SYN ; Request

TCP-based amplification attacks

Issue an HTTP request for **forbidden content**

Packet sequences

SYN with Request

HTTP request
in the SYN payload

Request

SYN ; Request

Request can be either
PSH or PSH+ACK

TCP-based amplification attacks

Issue an HTTP request for **forbidden content**

Packet sequences

SYN *with Request*

PSH

PSH+ACK

SYN ; PSH

SYN ; PSH+ACK

Middleboxes can be triggered without any ACK whatsoever

TCP-based amplification attacks

Packet sequences

SYN *with Request*

PSH

PSH+ACK

SYN ; PSH

SYN ; PSH+ACK

Variants

Details in the paper

Increased TTL

Increased wscale

TCP Segmentation

FIN+CWR

HTTP without \r\n

Increase amplification for
small fractions of middleboxes

TCP-based amplification attacks

Packet sequences

SYN *with Request*

PSH

PSH+ACK

SYN ; PSH

SYN ; PSH+ACK

Triggering domains

www.youporn.com porn

www.roxypalace.com gambling

plus.google.com social

www.bittorent.com file sharing

www.survive.org.uk sex health

TCP-based amplification attacks

Packet sequences

SYN *with Request*

PSH

PSH+ACK

SYN ; PSH

SYN ; PSH+ACK

Triggering domains

www.youporn.com **porn**

www.roxypalace.com **gambling**

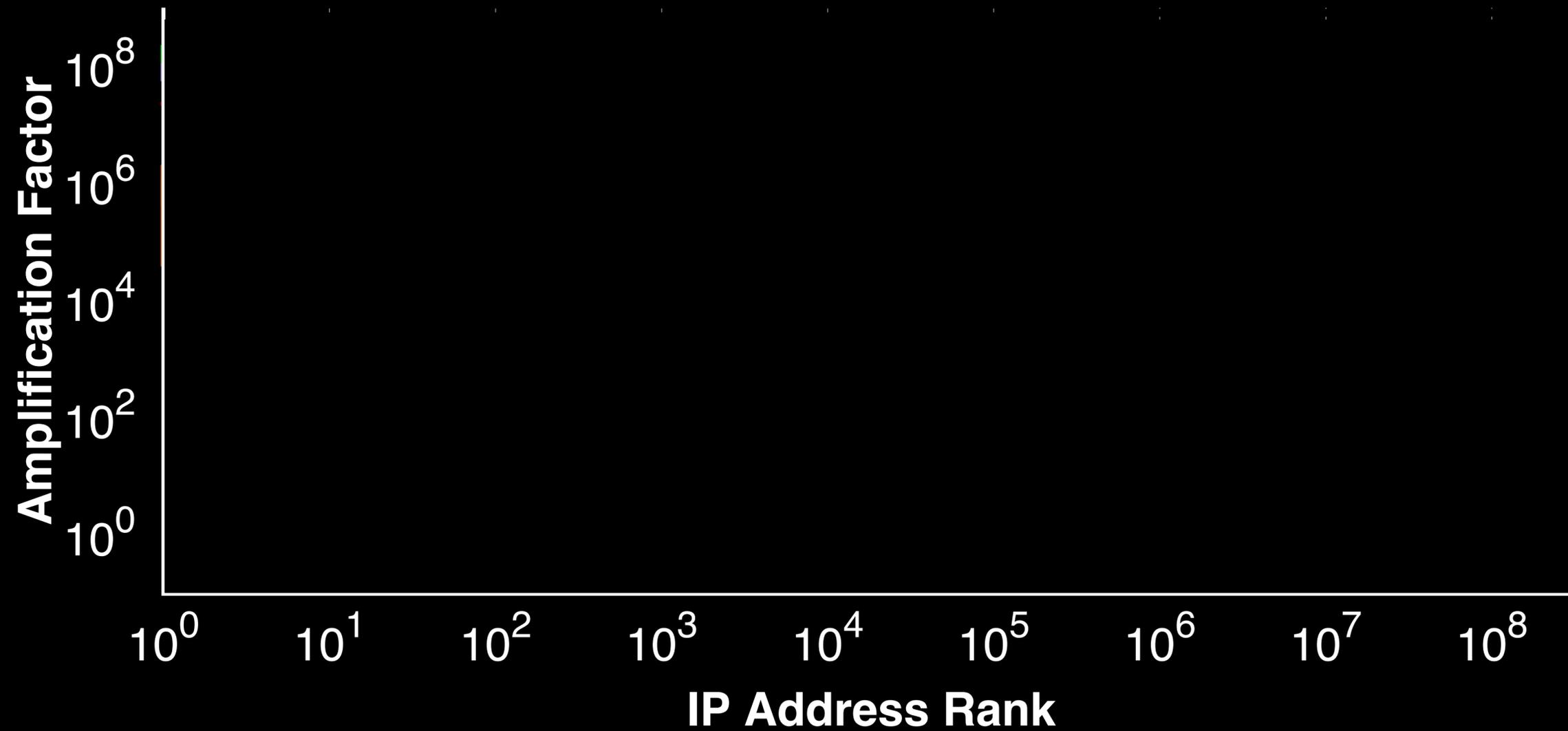
plus.google.com **social**

www.bittorent.com **file sharing**

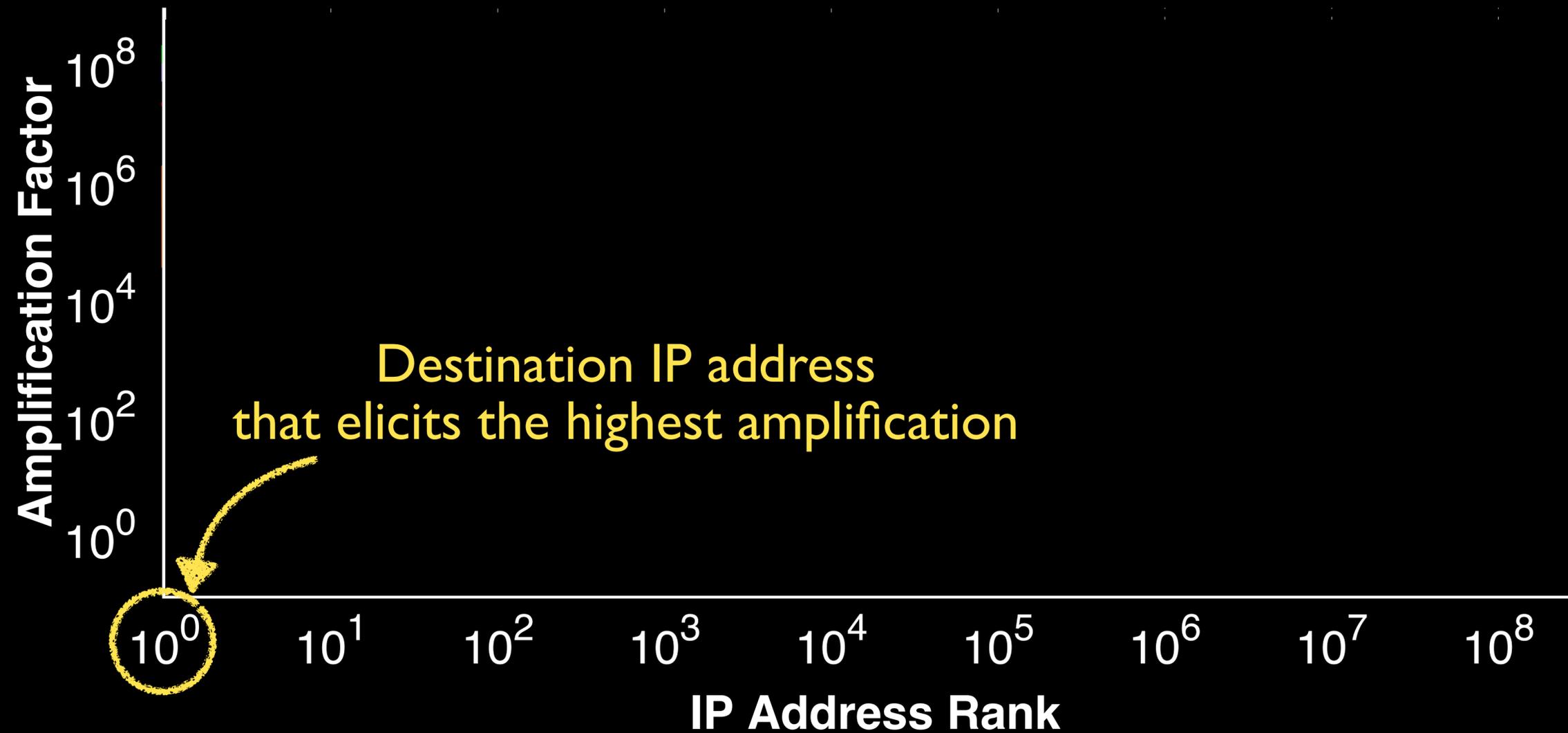
www.survive.org.uk **sex health**

Middleboxes differ in their bugs and their configurations

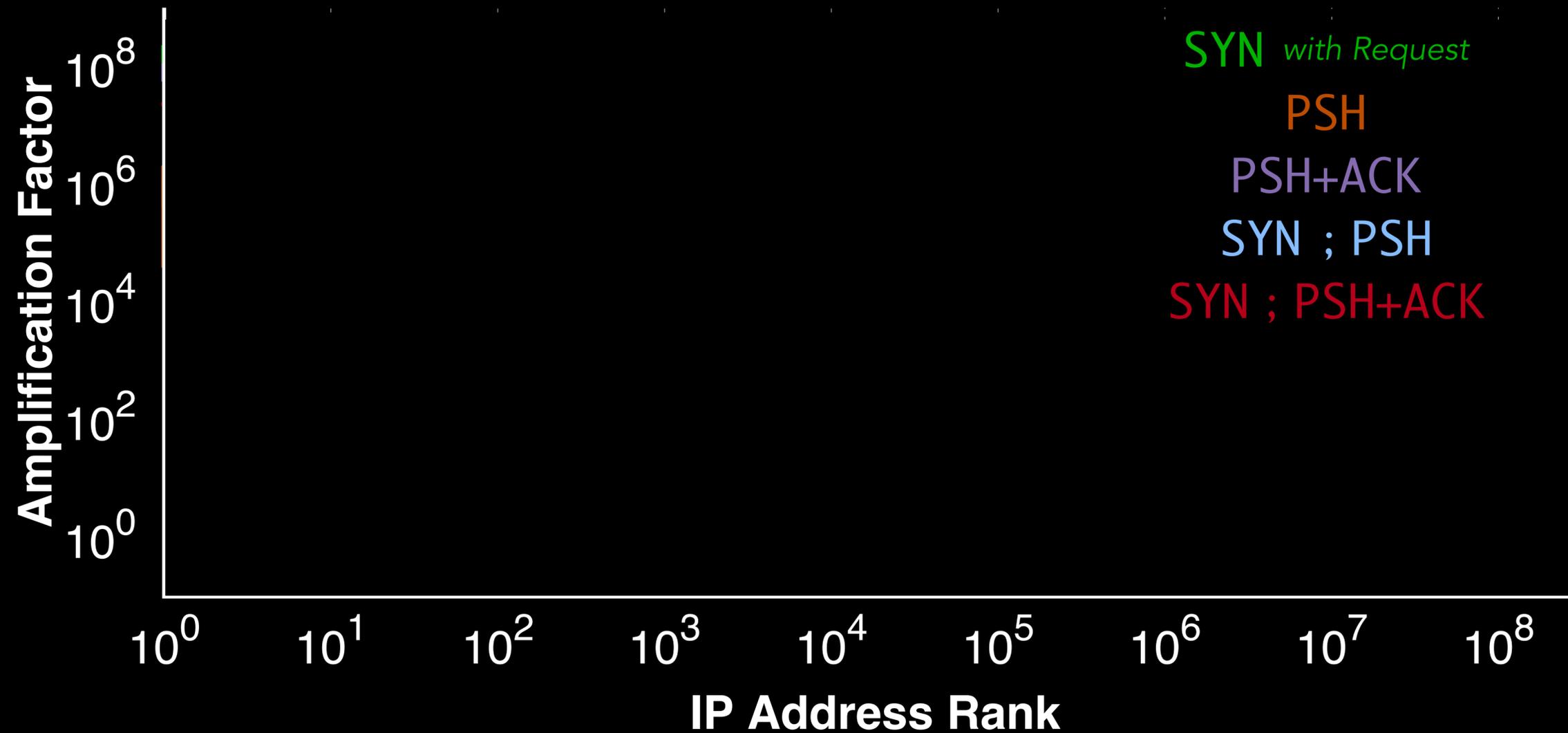
Amplification by packet sequence



Amplification by packet sequence

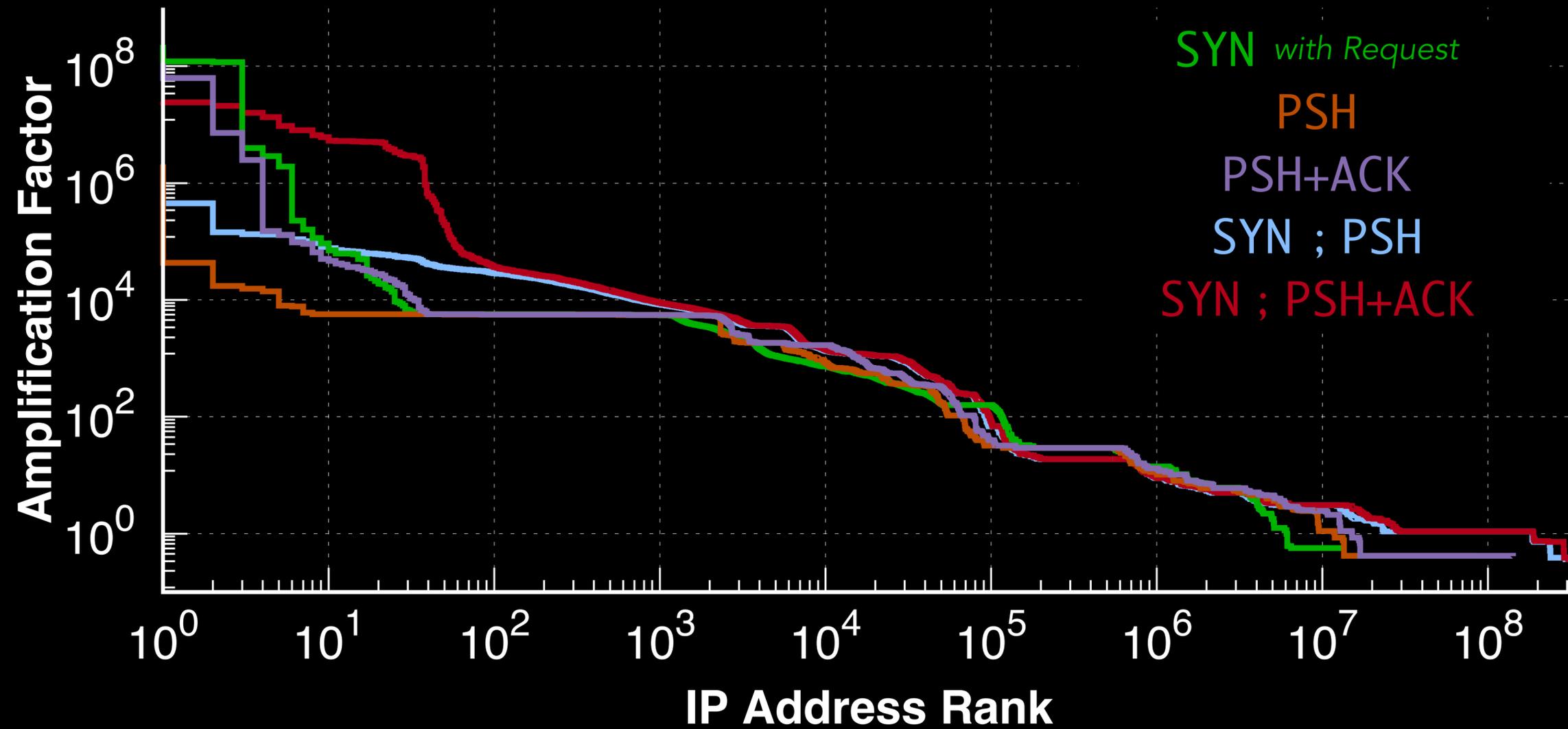


Amplification by packet sequence



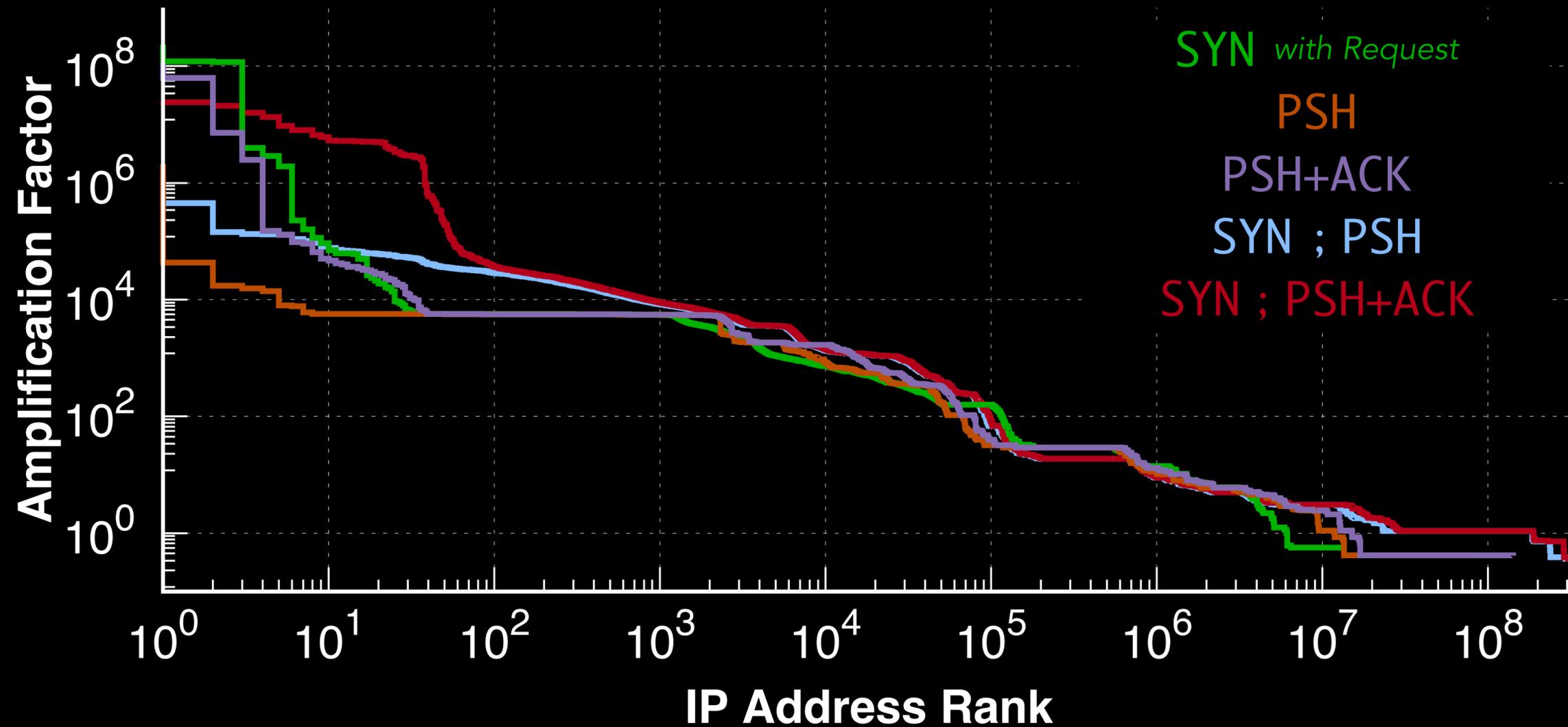
Amplification by packet sequence

Triggered with www.youporn.com



Amplification by packet sequence

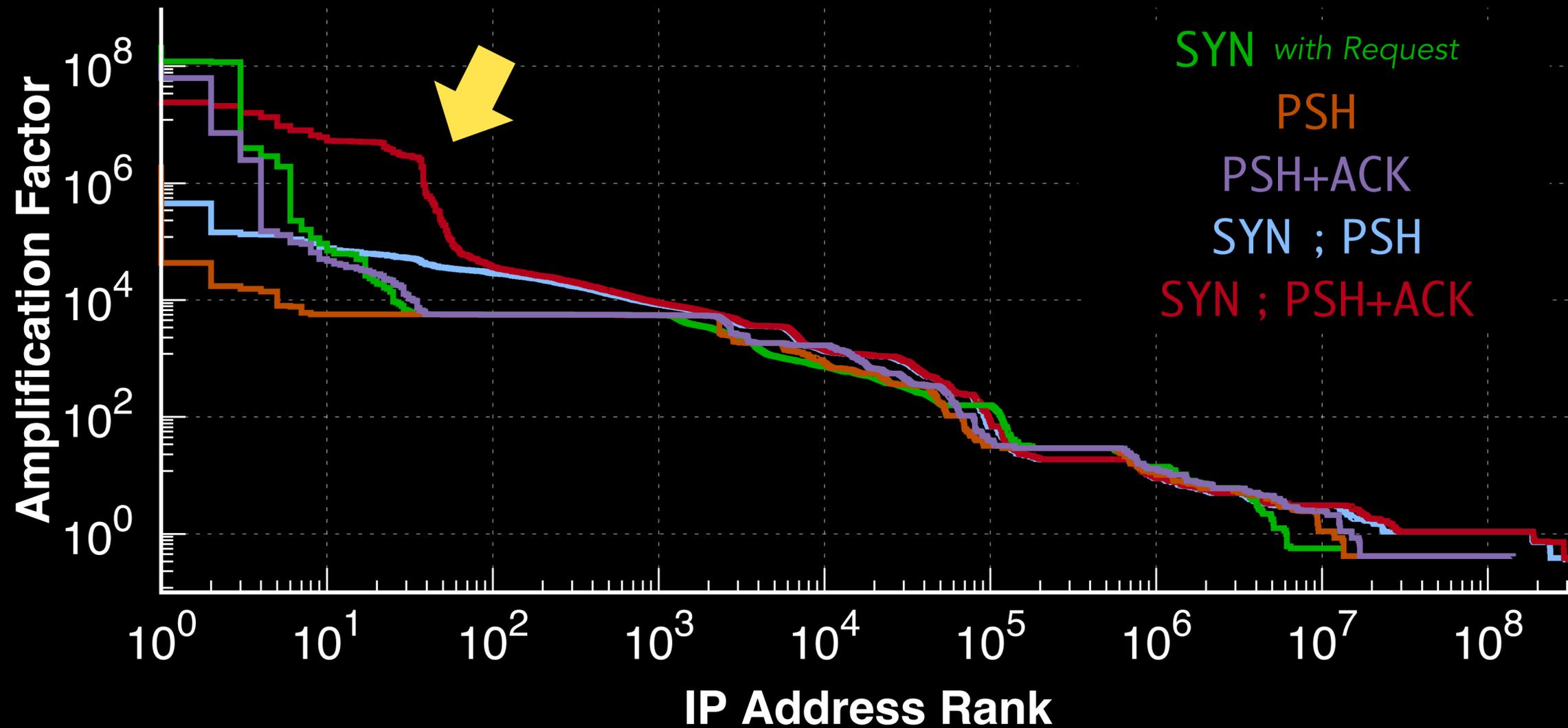
Triggered with www.youporn.com



Packet sequences differ in amplification and number of amplifiers

Amplification by packet sequence

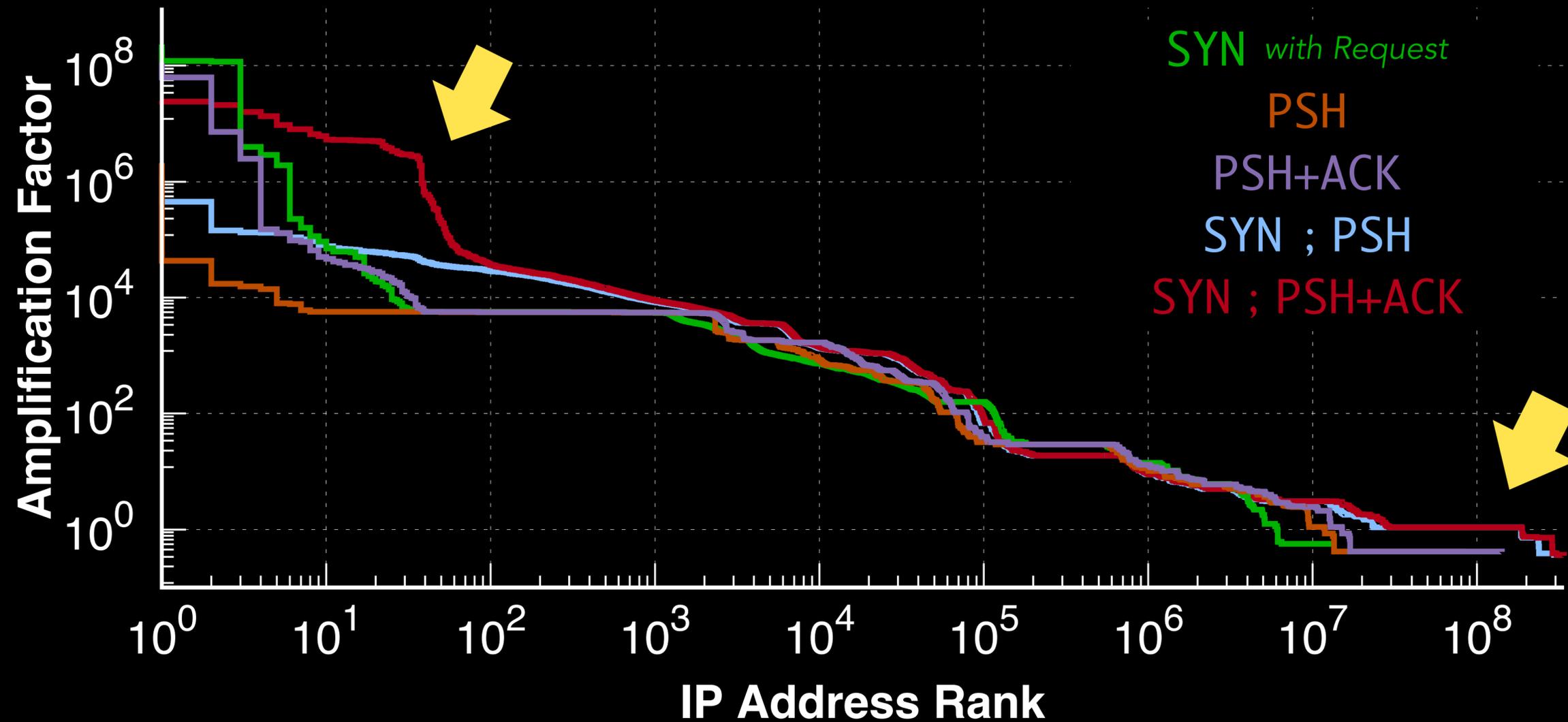
Triggered with www.youporn.com



Packet sequences differ in amplification and number of amplifiers

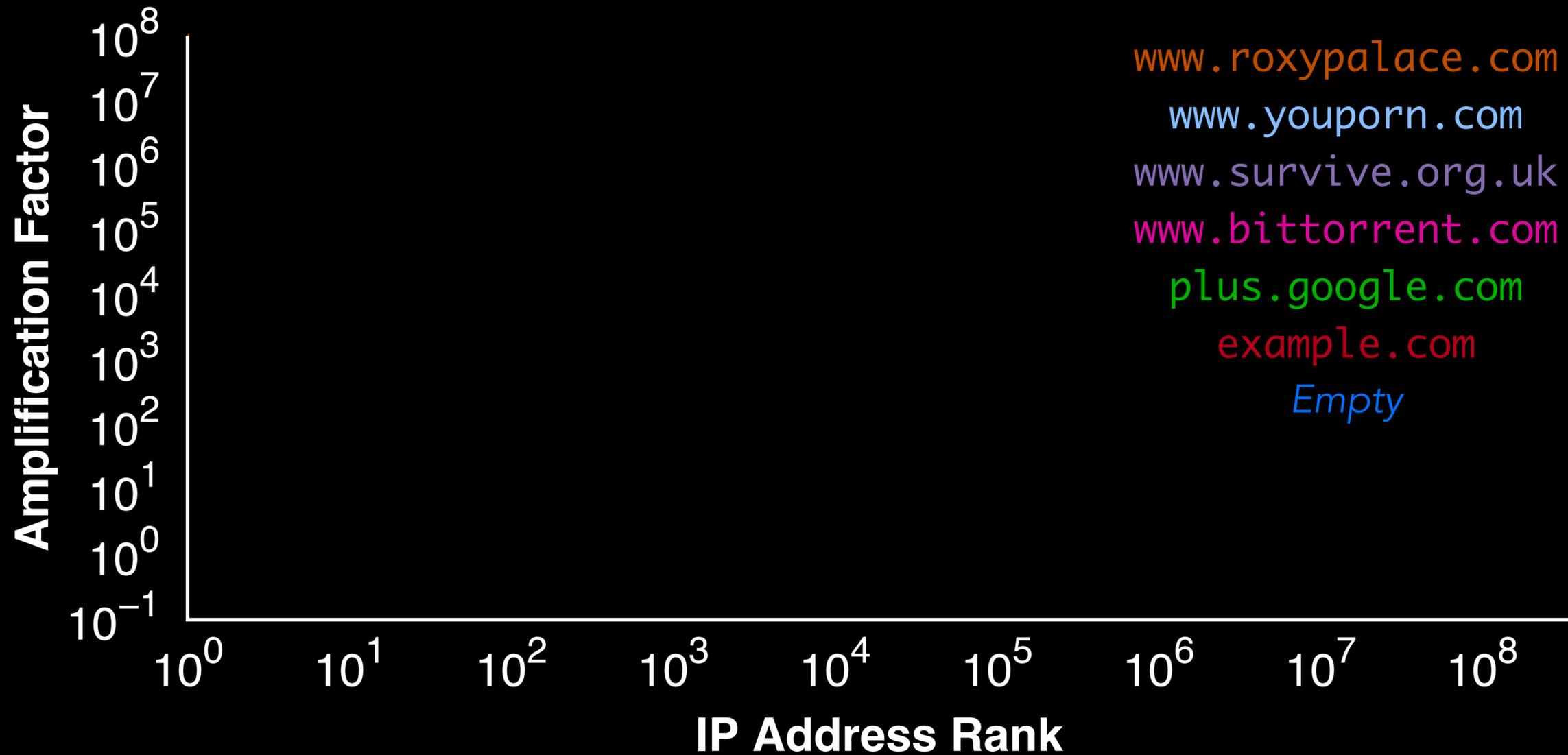
Amplification by packet sequence

Triggered with `www.youporn.com`

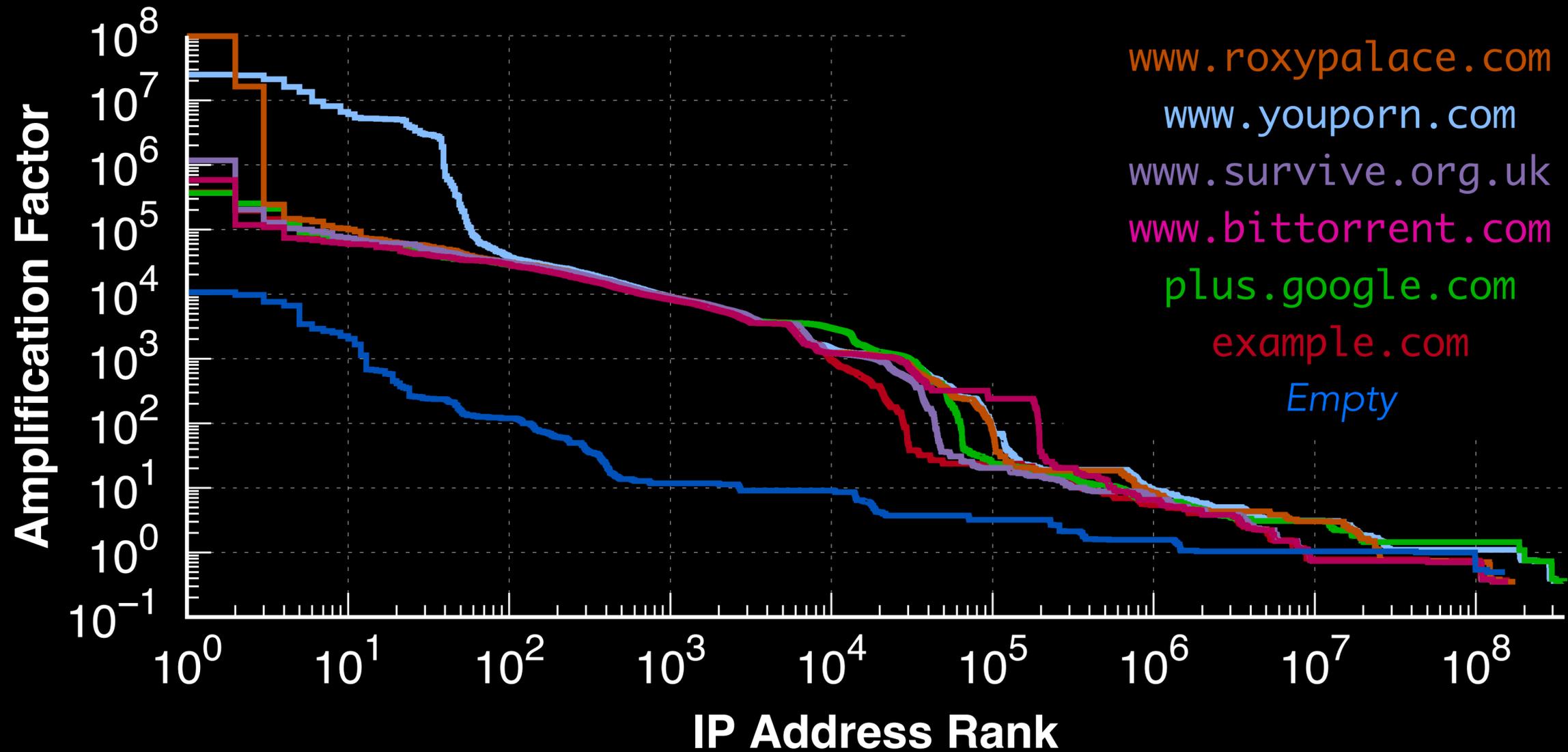


Packet sequences differ in amplification and number of amplifiers

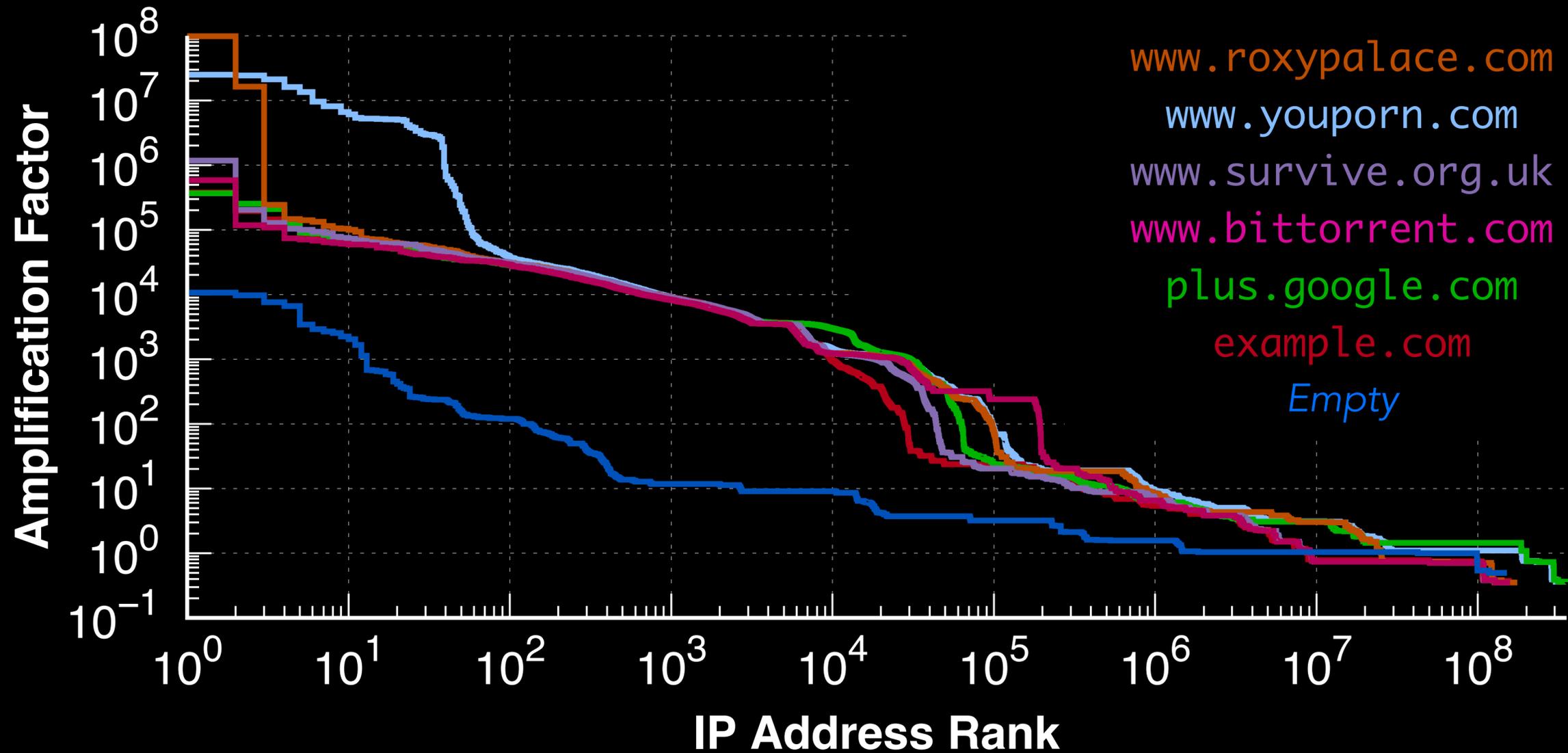
Amplification by triggering domain



Amplification by triggering domain



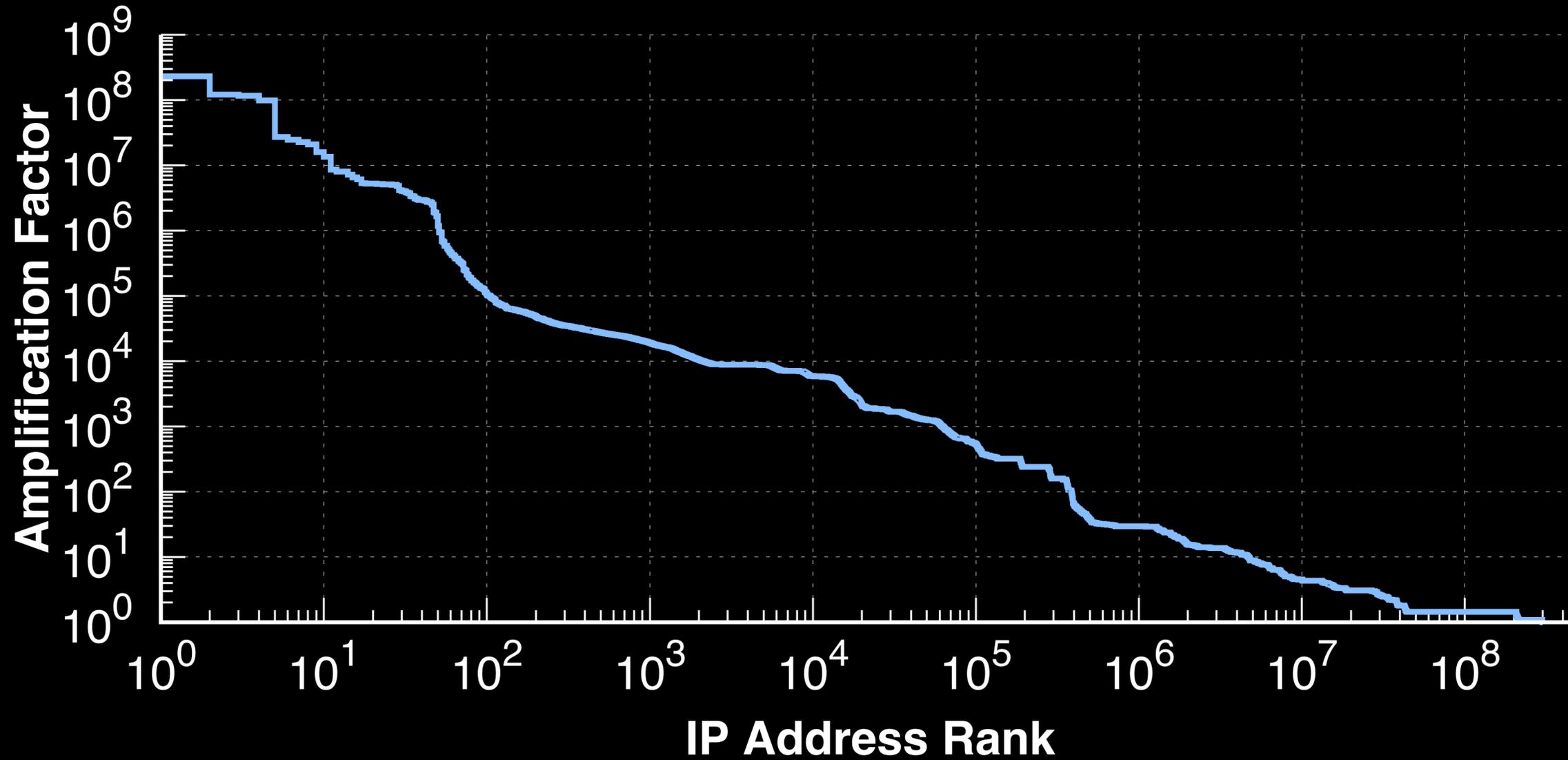
Amplification by triggering domain



Different triggering domains can yield drastically different amplification

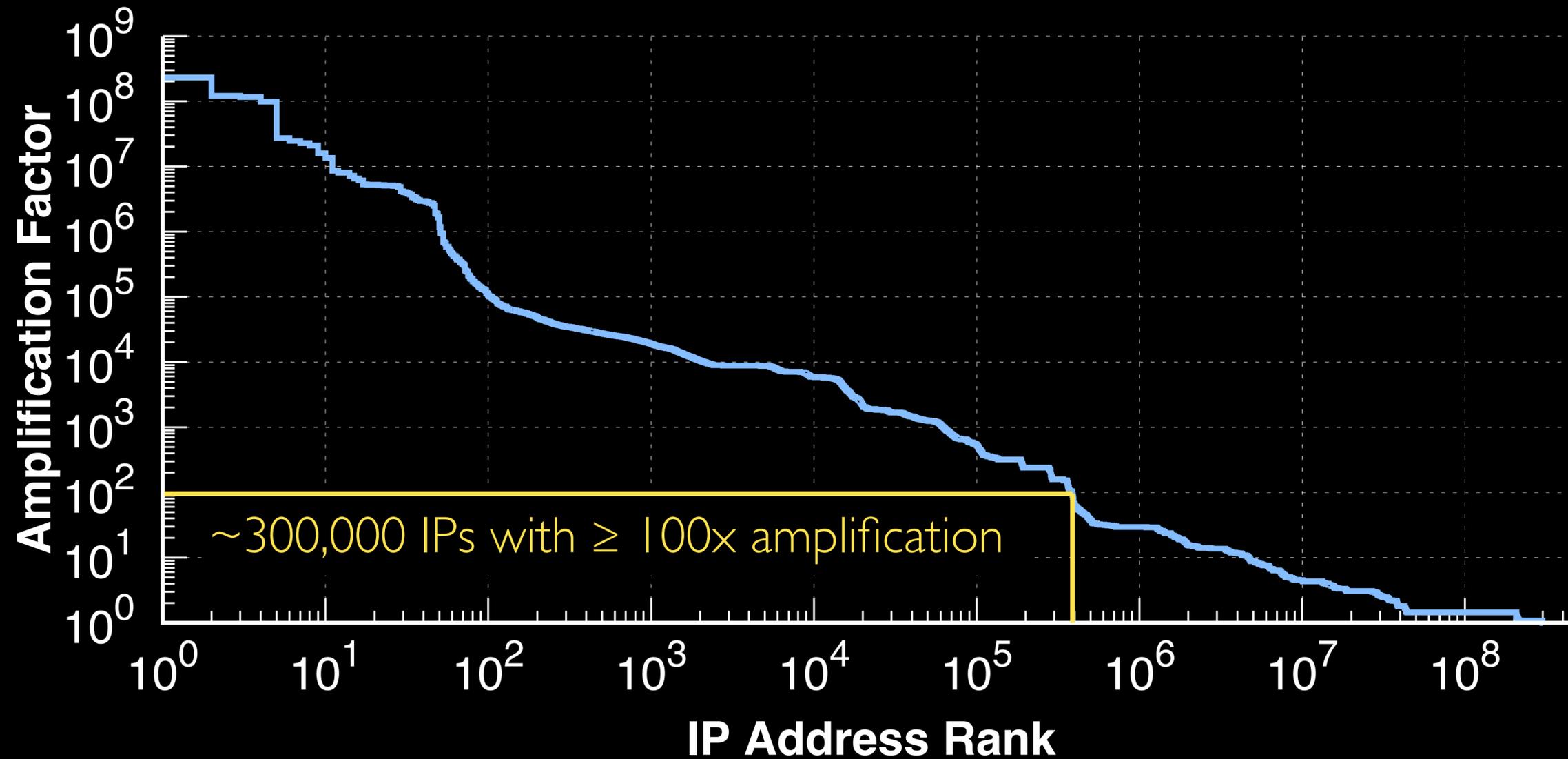
Maximum amplification

Assuming a perfectly-informed attacker



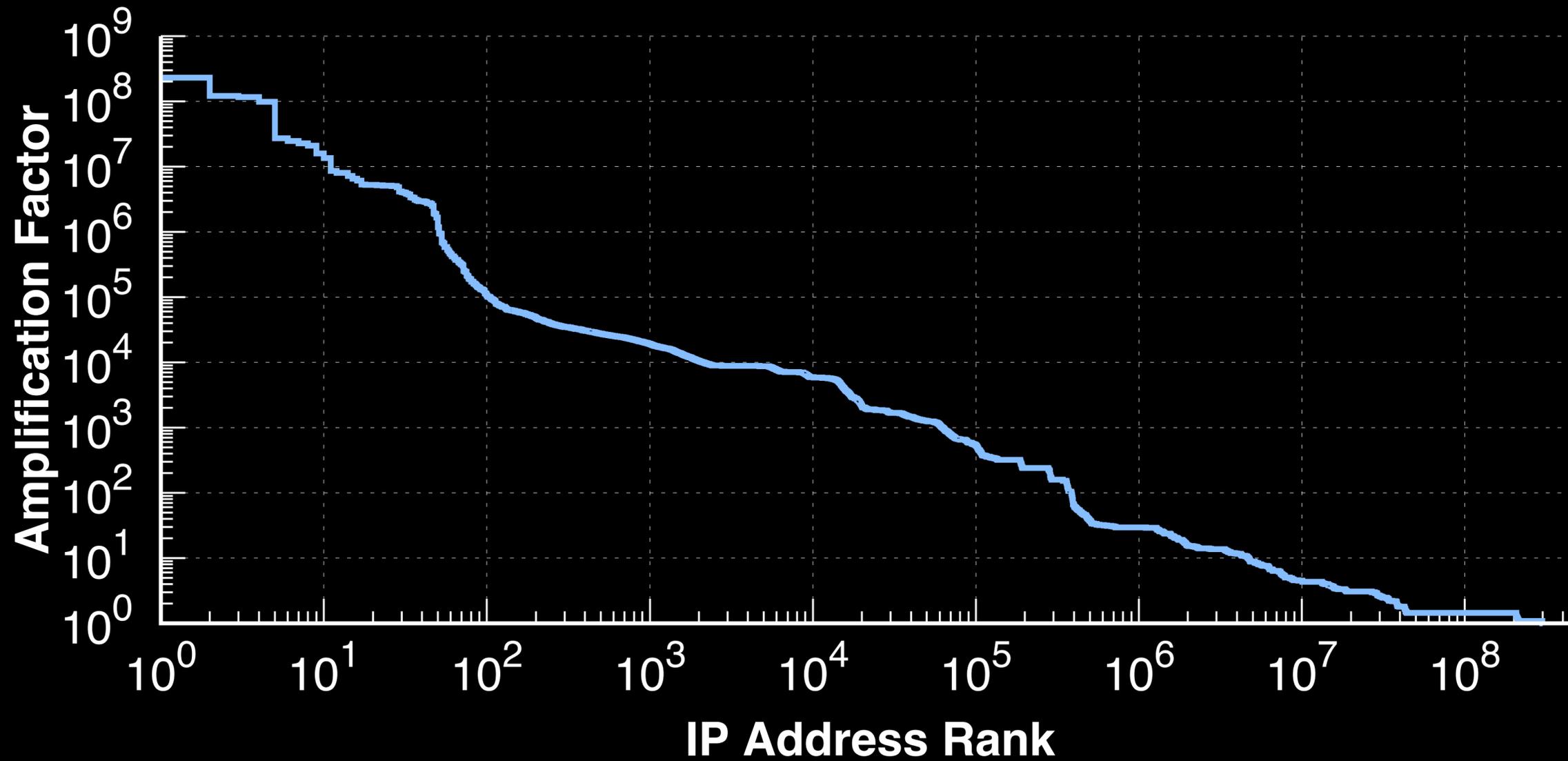
Maximum amplification

Assuming a perfectly-informed attacker



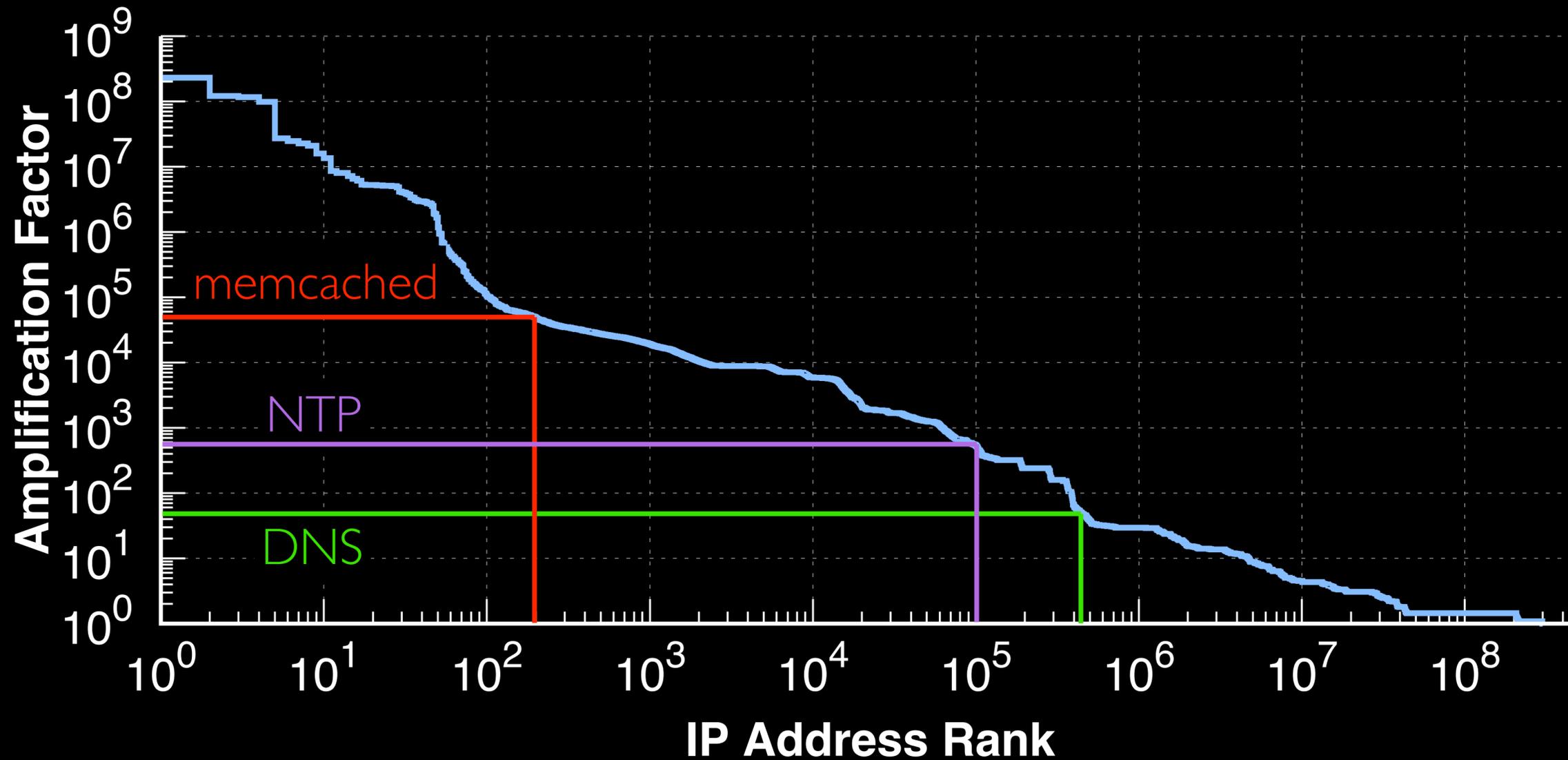
Maximum amplification

Assuming a perfectly-informed attacker



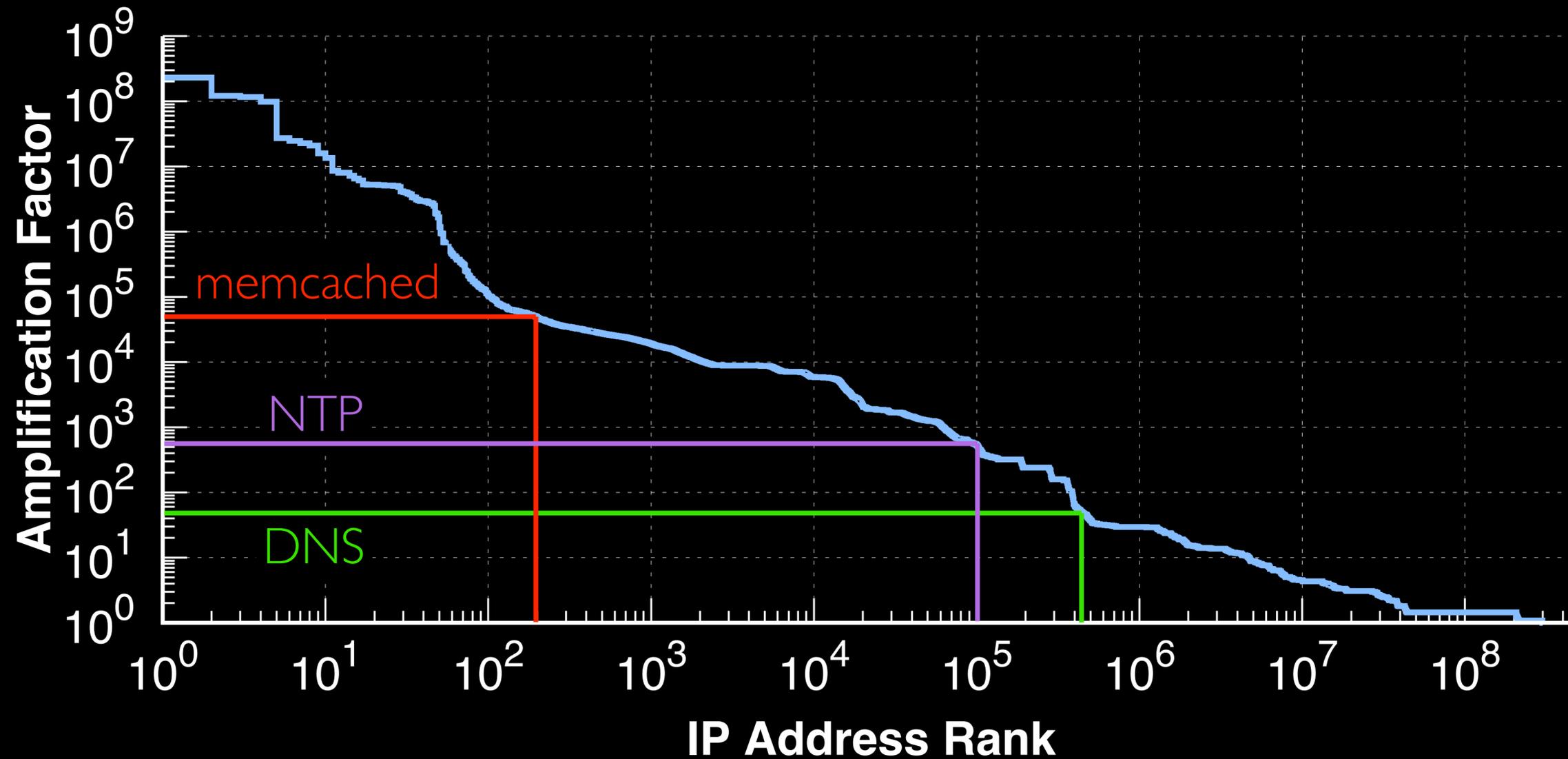
Maximum amplification

Assuming a perfectly-informed attacker



Maximum amplification

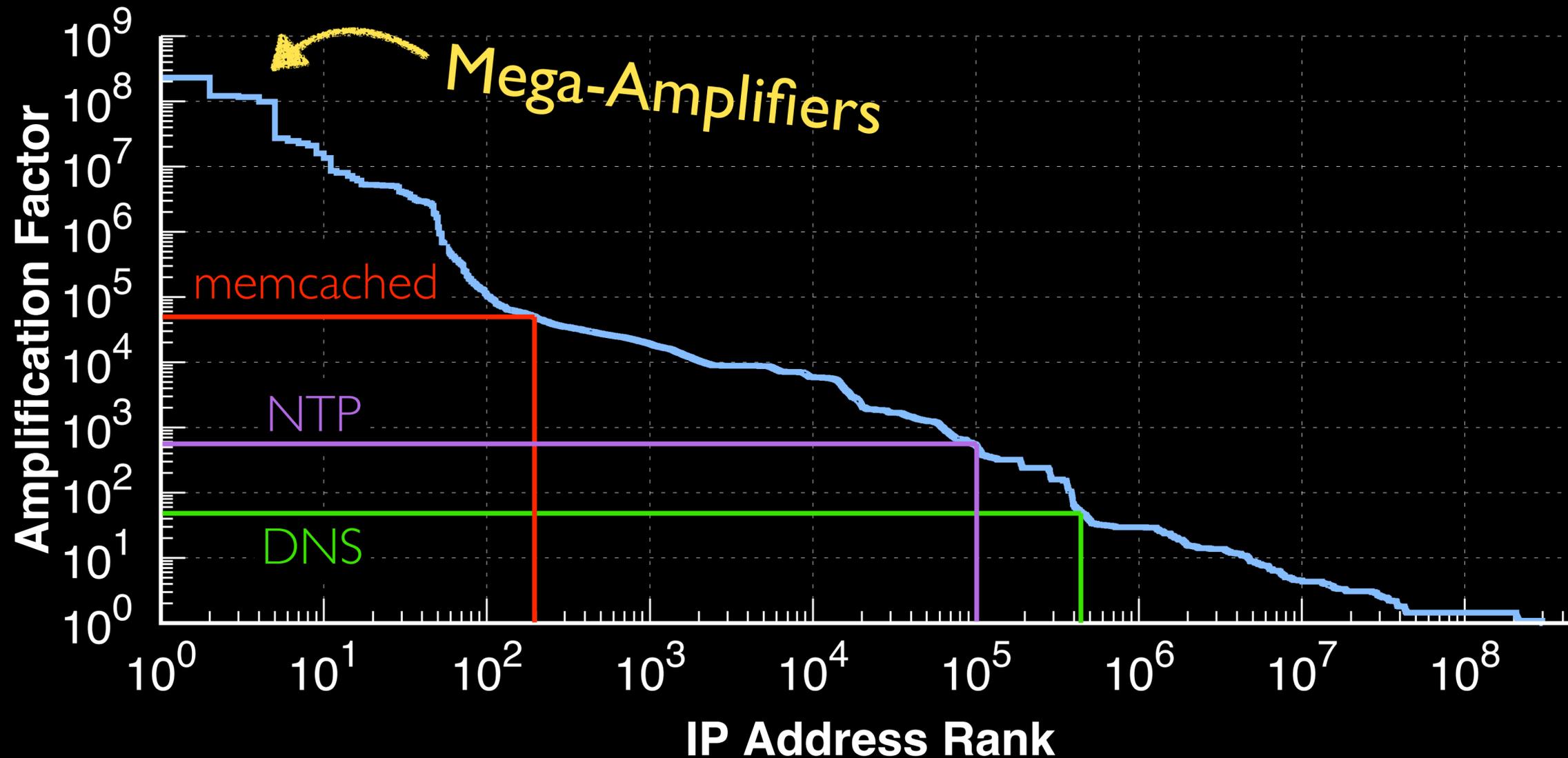
Assuming a perfectly-informed attacker



TCP-based amplification is at least as powerful
as UDP-based alternatives

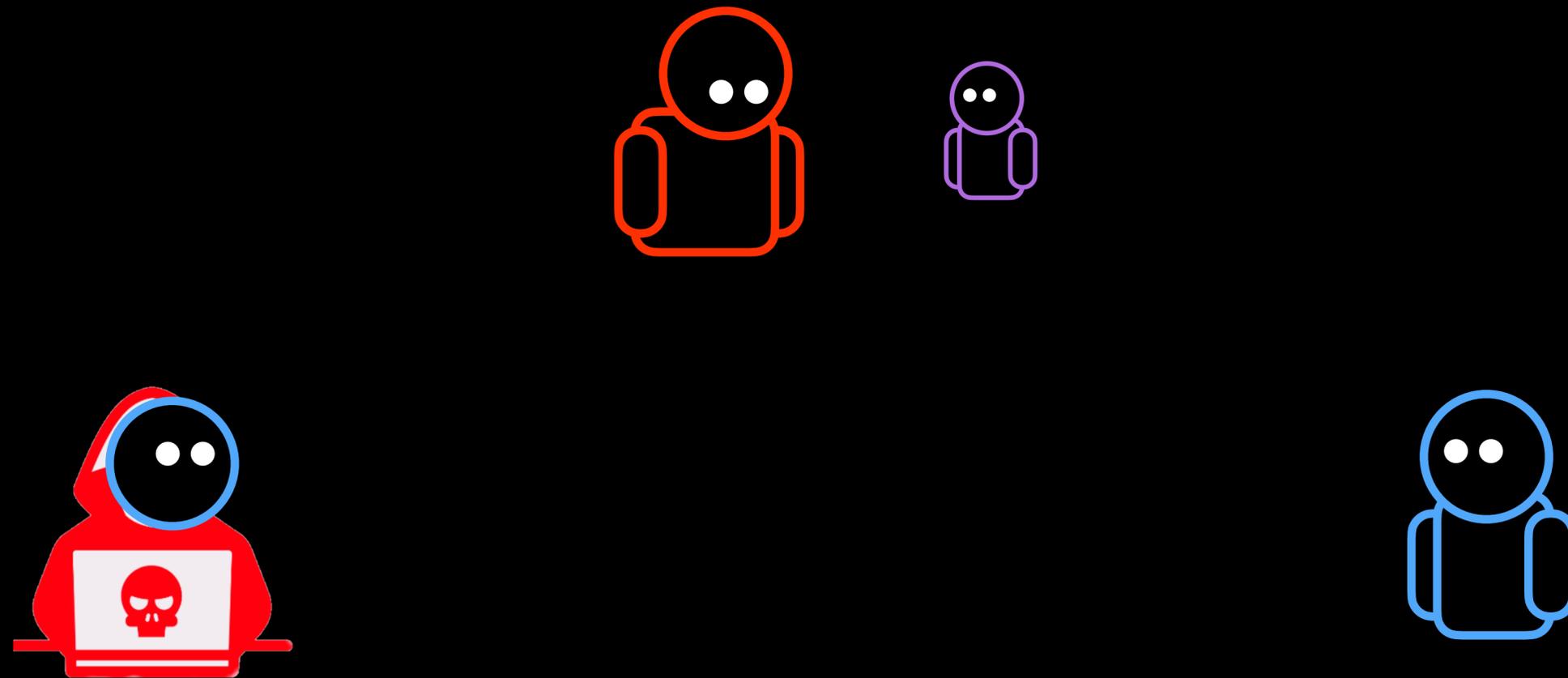
Maximum amplification

Assuming a perfectly-informed attacker

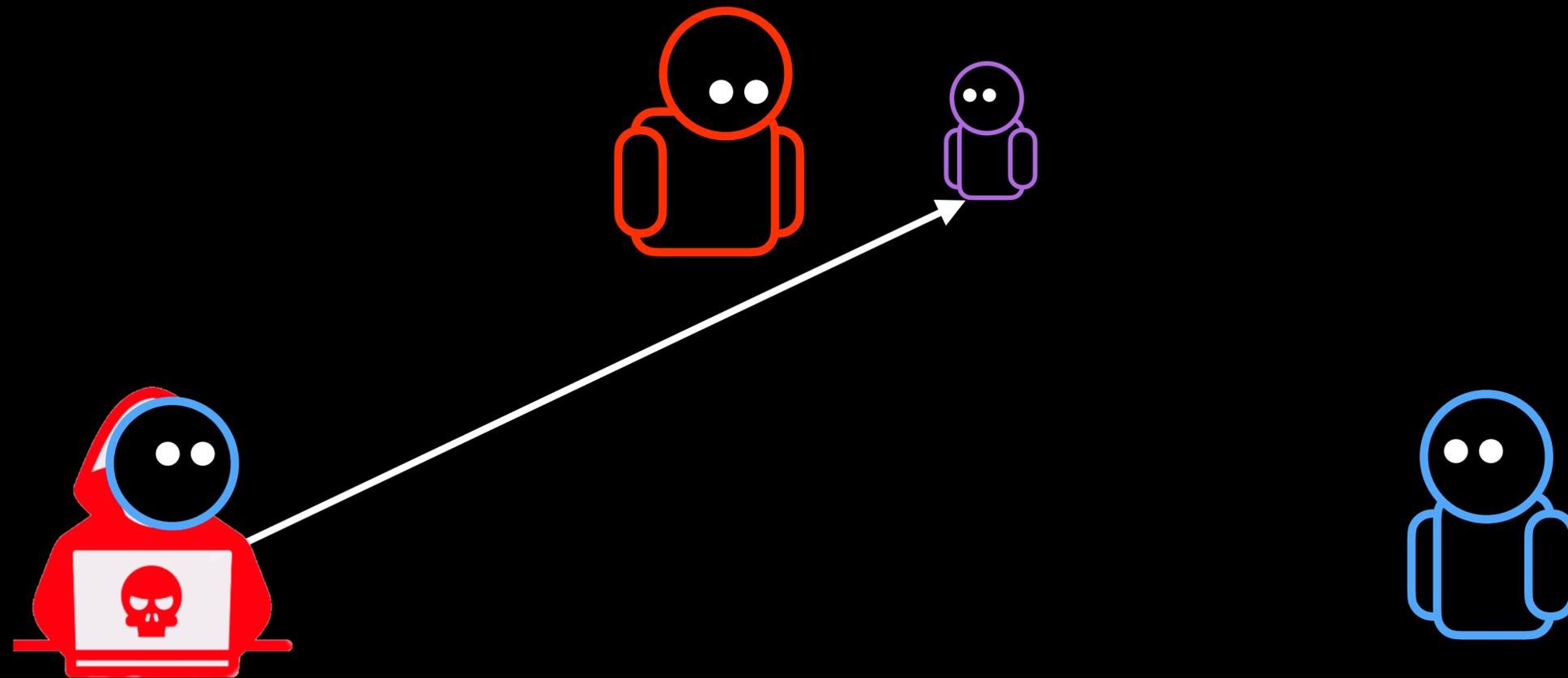


TCP-based amplification is at least as powerful
as UDP-based alternatives

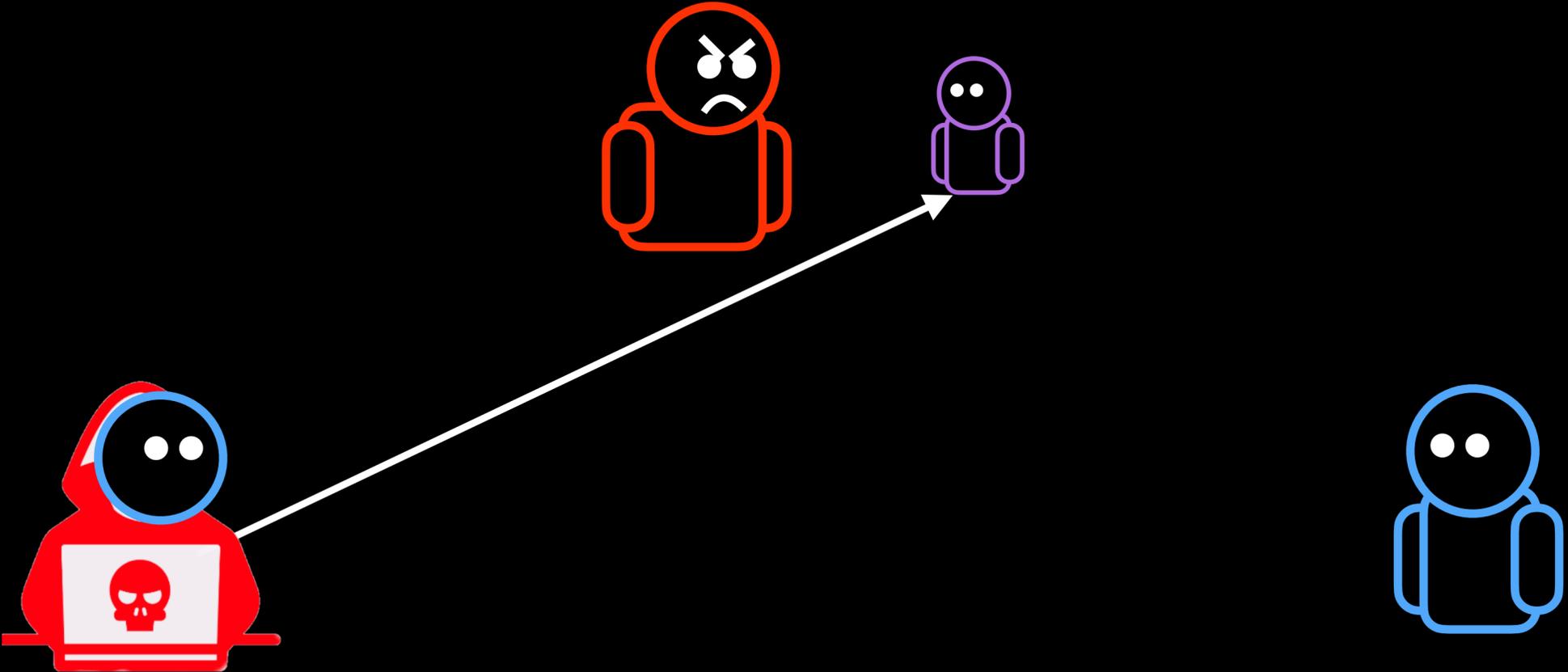
Mega-amplifier cause #1: Victim-sustained loops



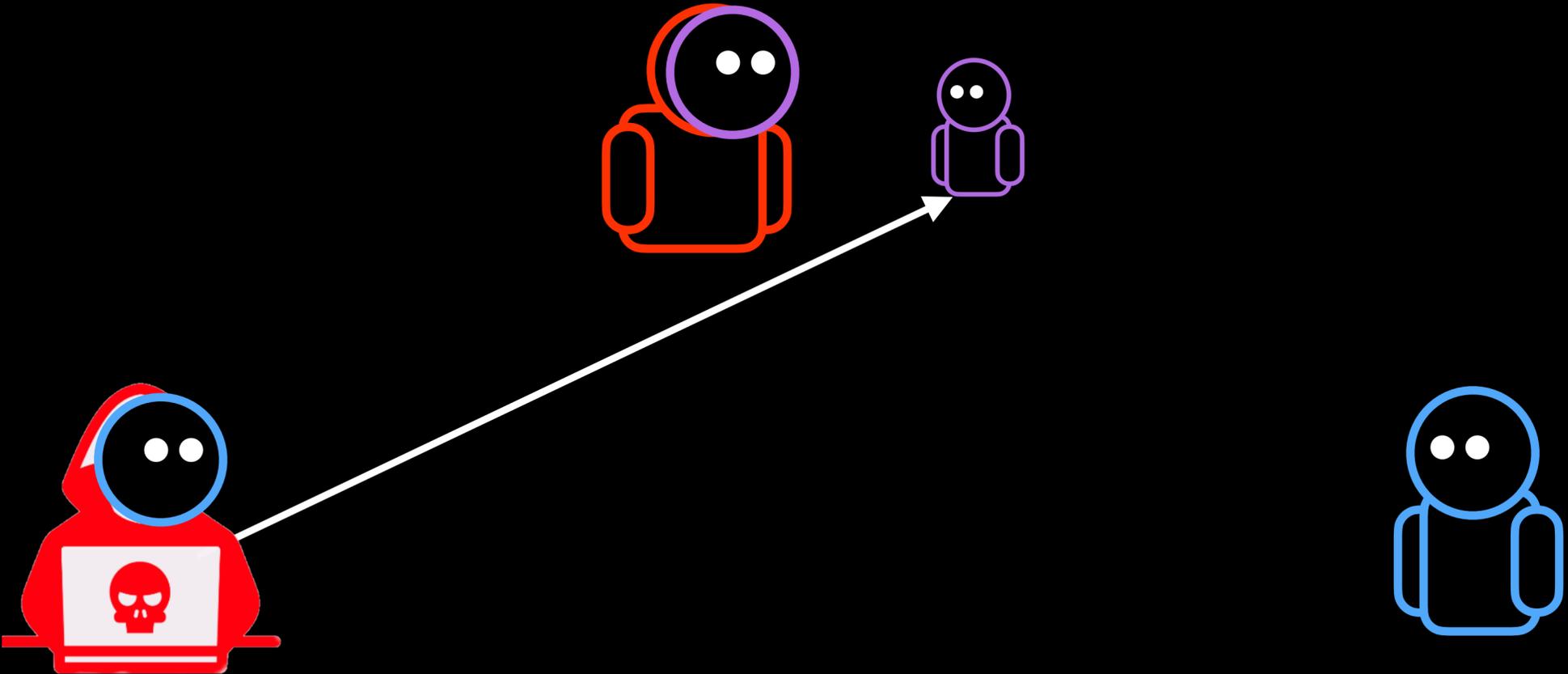
Mega-amplifier cause #1: Victim-sustained loops



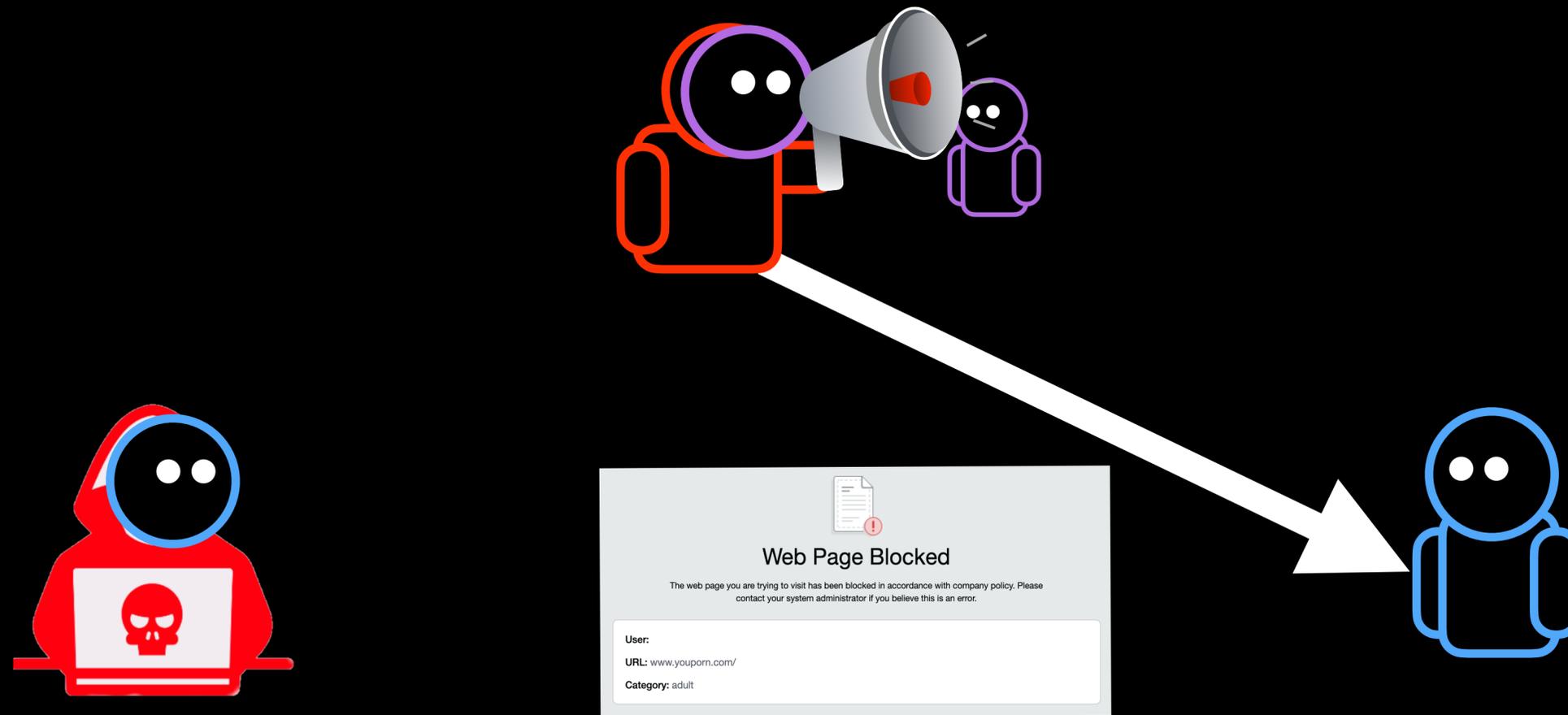
Mega-amplifier cause #1: Victim-sustained loops



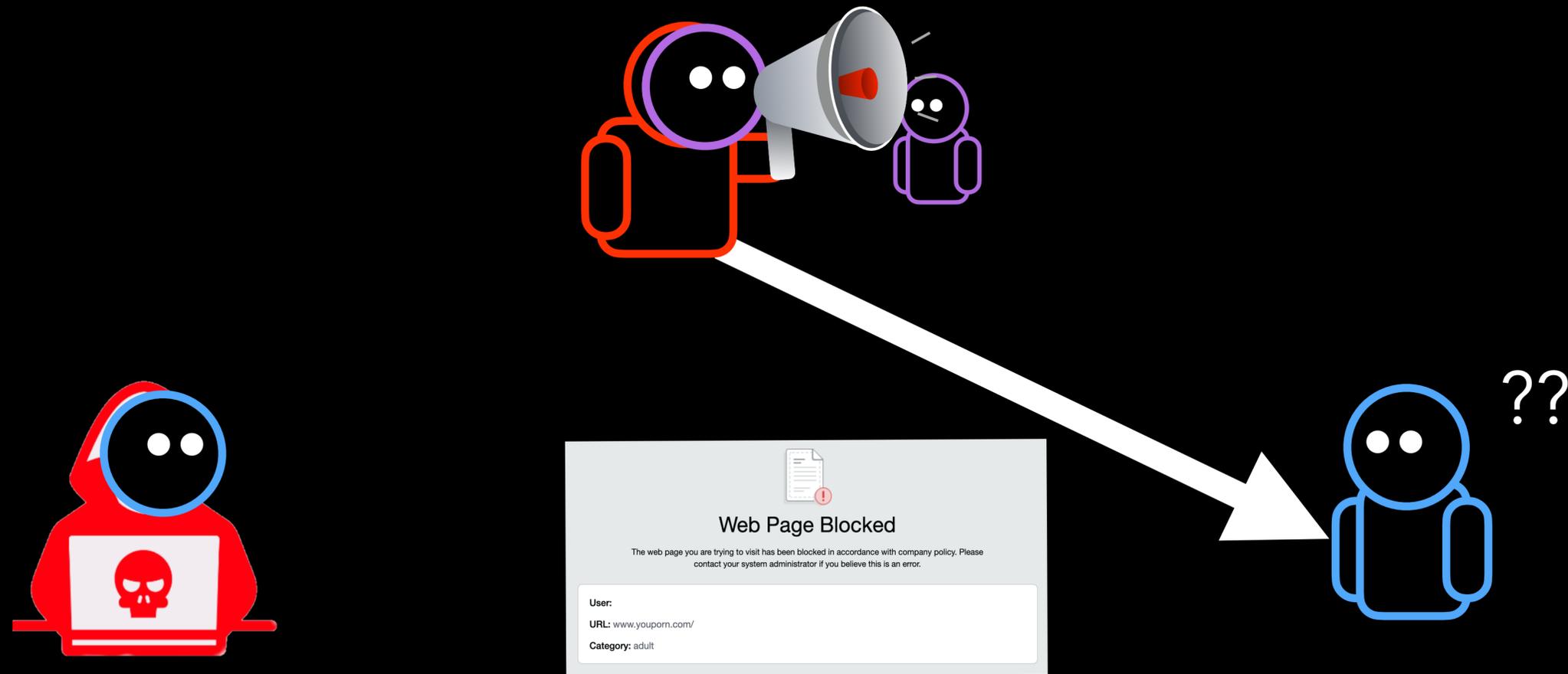
Mega-amplifier cause #1: Victim-sustained loops



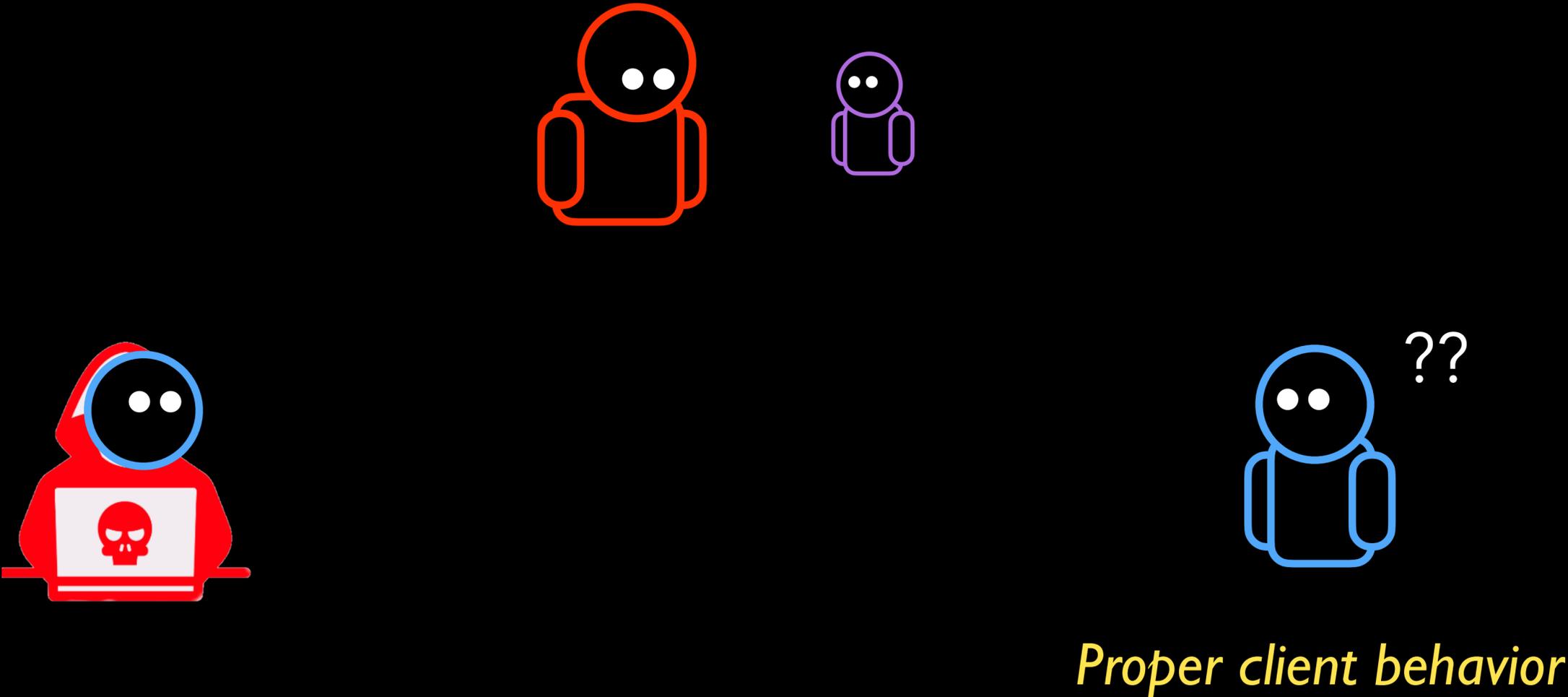
Mega-amplifier cause #1: Victim-sustained loops



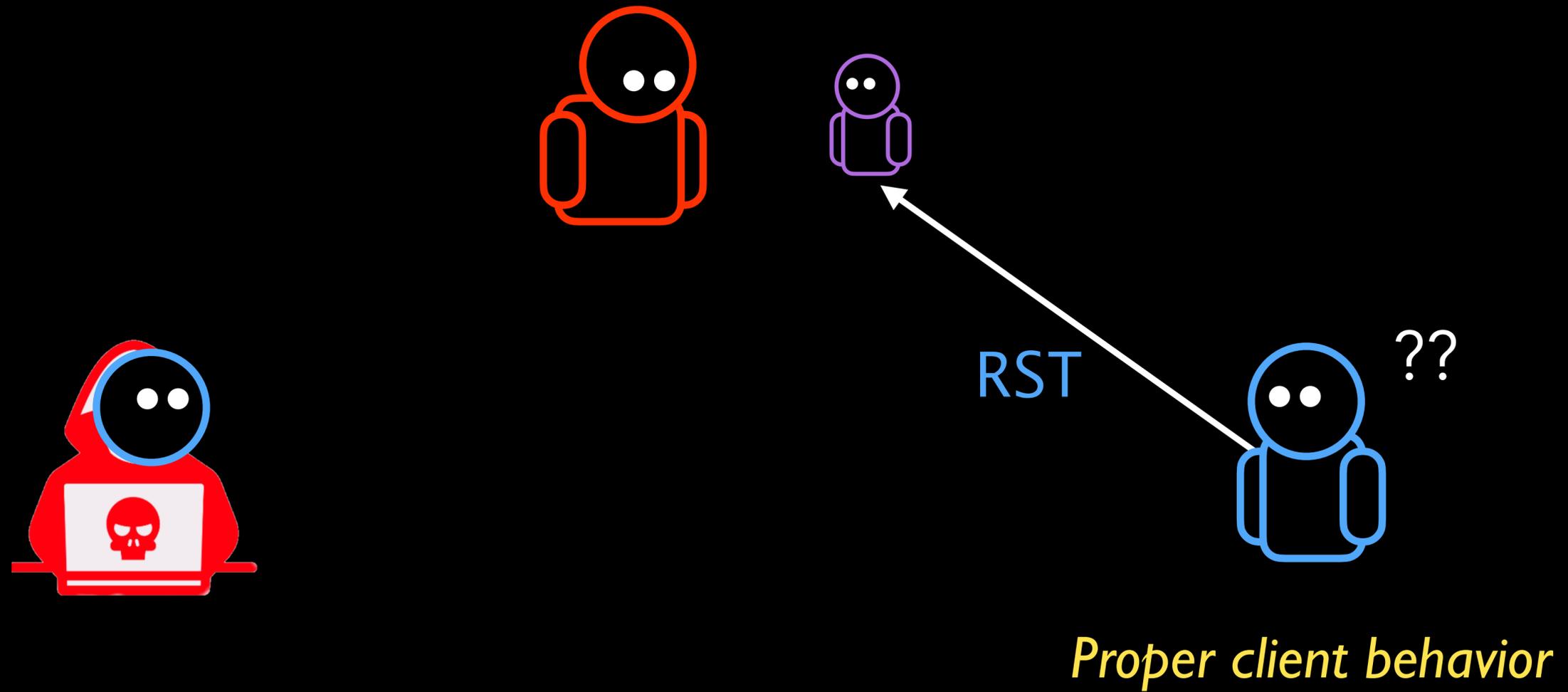
Mega-amplifier cause #1: Victim-sustained loops



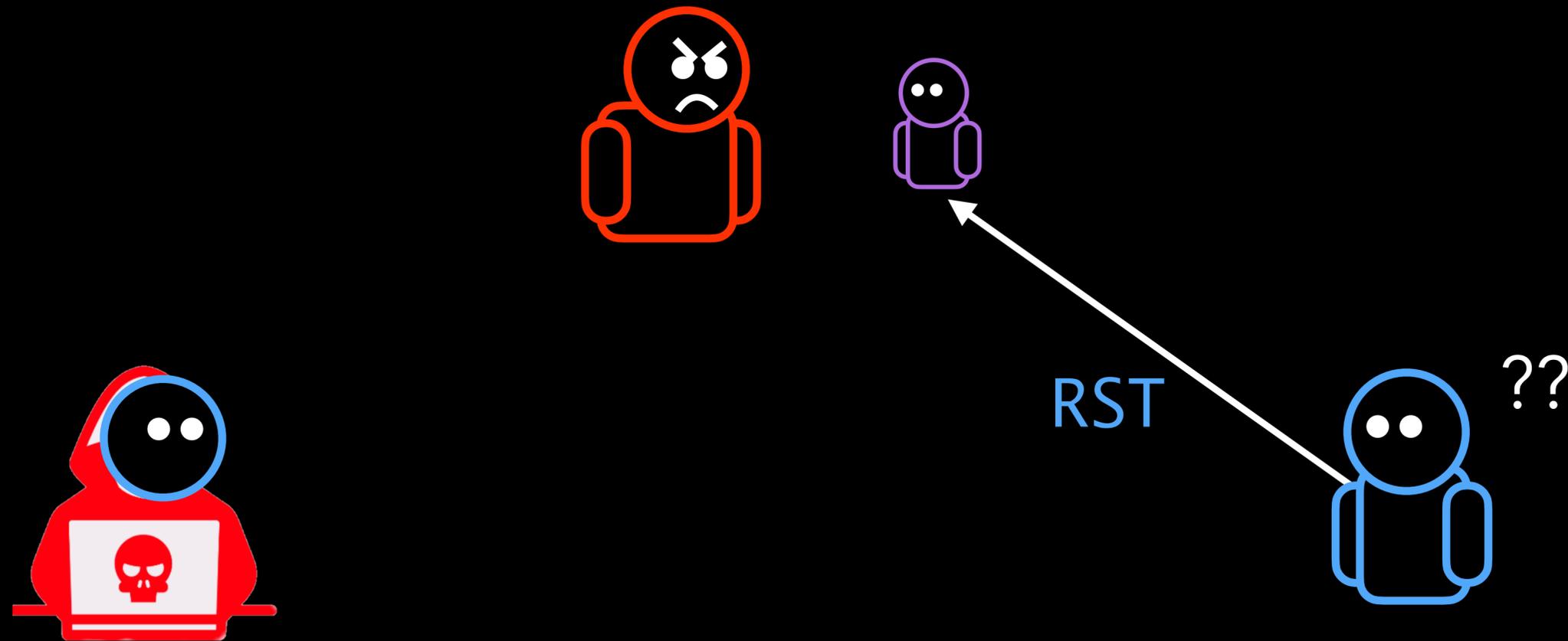
Mega-amplifier cause #1: Victim-sustained loops



Mega-amplifier cause #1: Victim-sustained loops

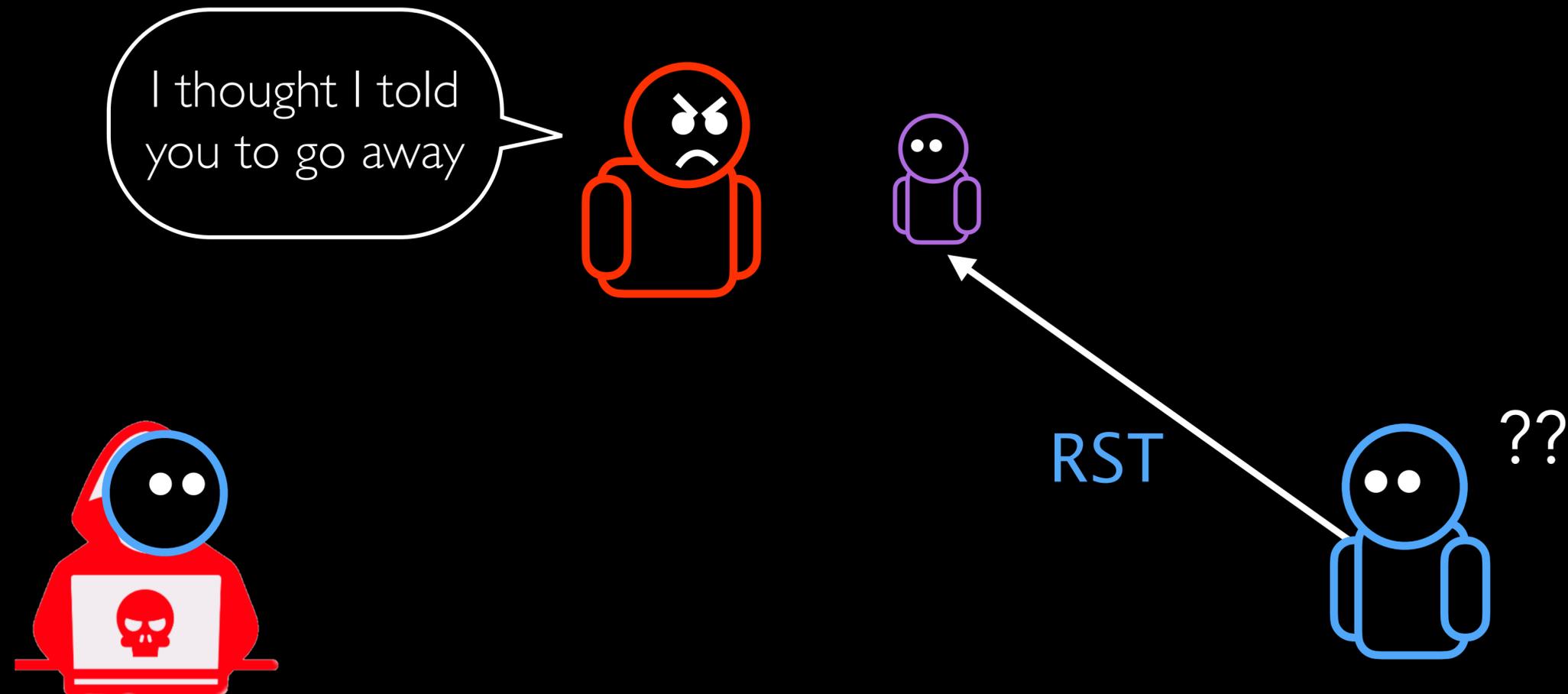


Mega-amplifier cause #1: Victim-sustained loops



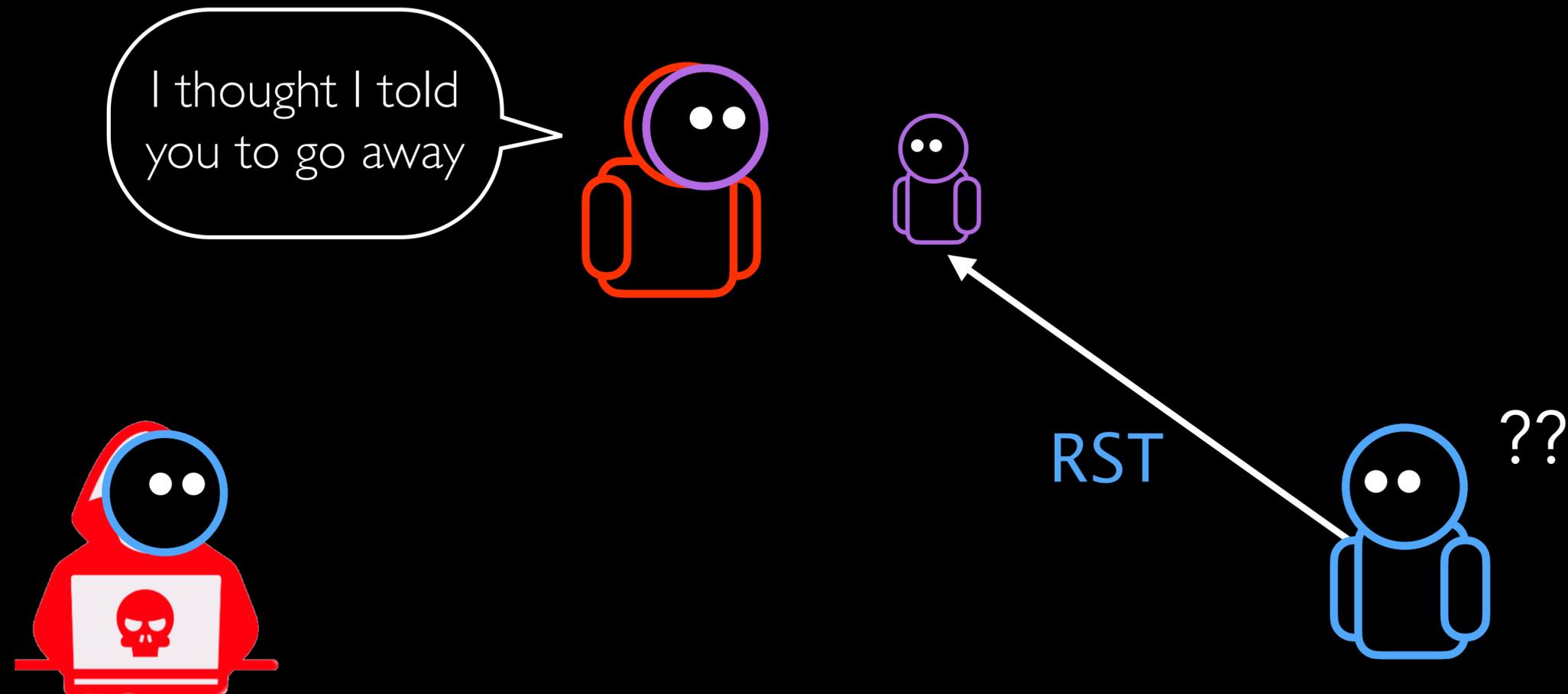
Sometimes, *any* packet re-triggers censorship

Mega-amplifier cause #1: Victim-sustained loops



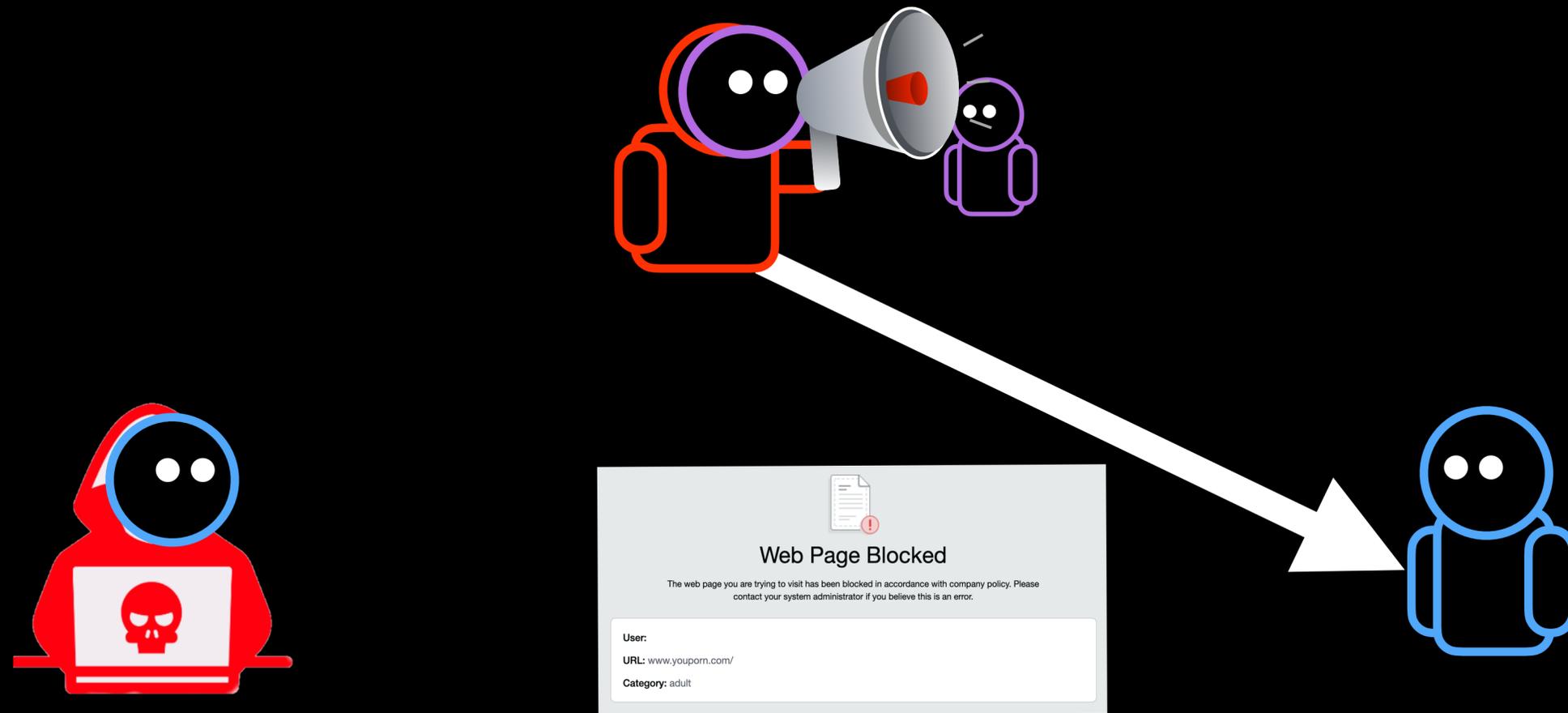
Sometimes, *any* packet re-triggers censorship

Mega-amplifier cause #1: Victim-sustained loops

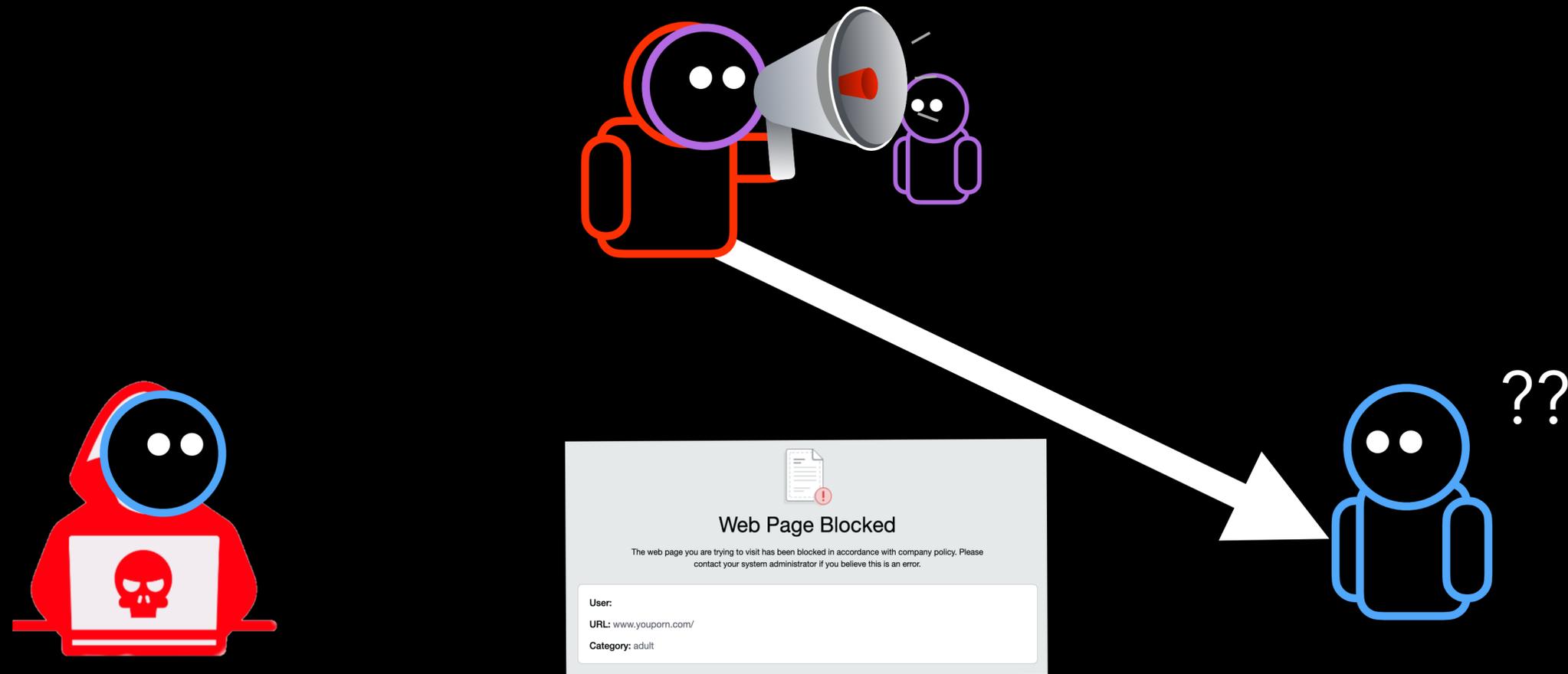


Sometimes, *any* packet re-triggers censorship

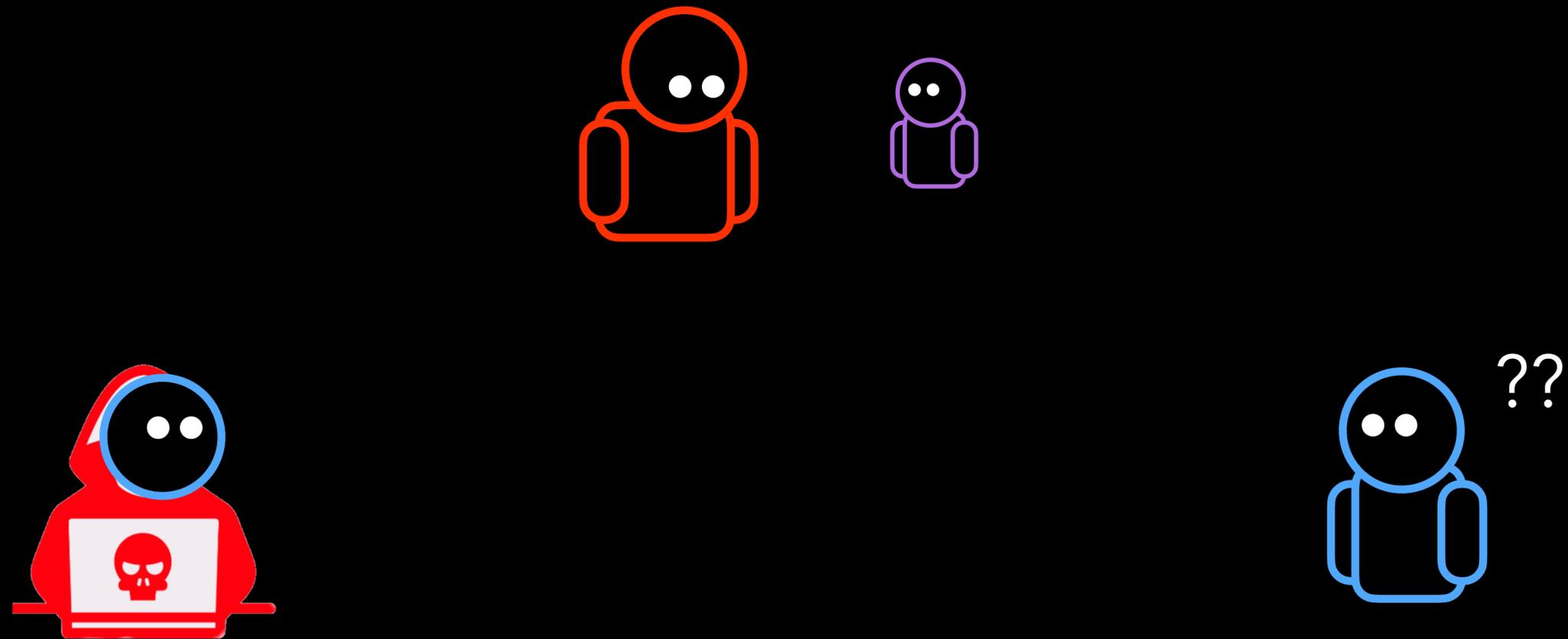
Mega-amplifier cause #1: Victim-sustained loops



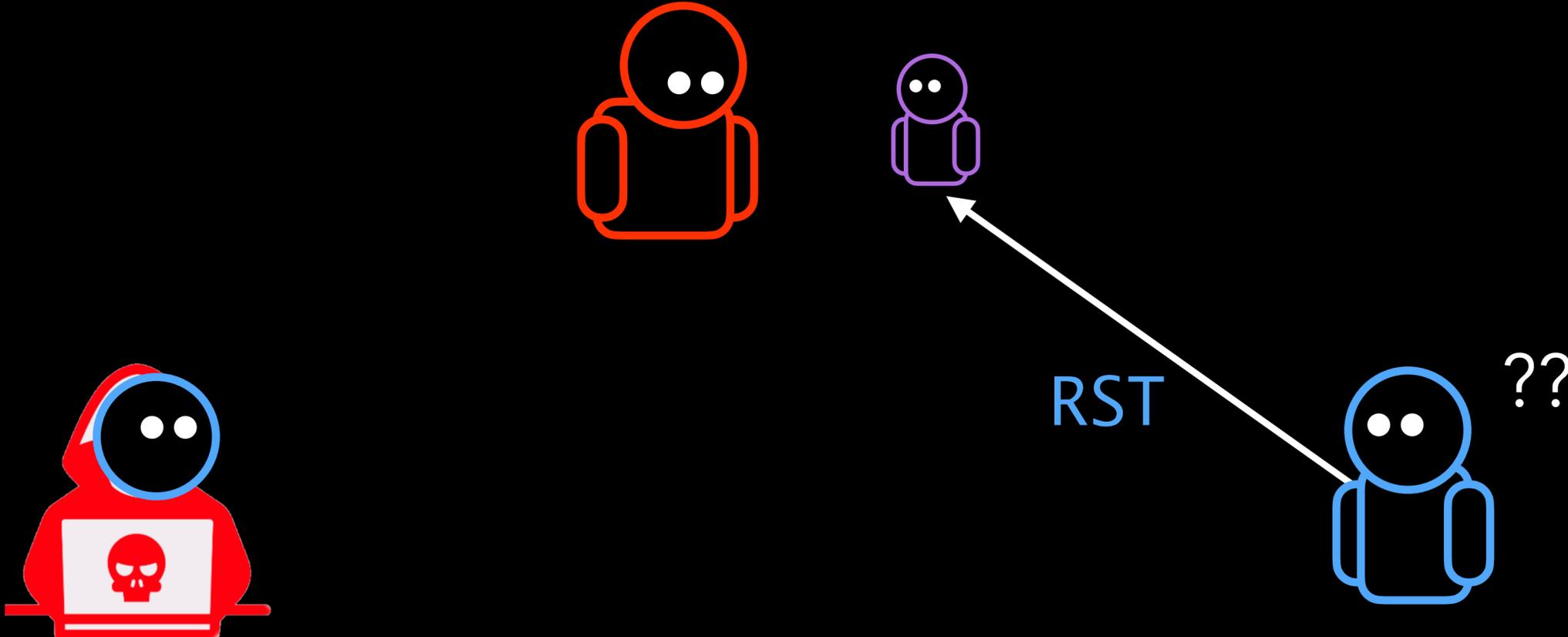
Mega-amplifier cause #1: Victim-sustained loops



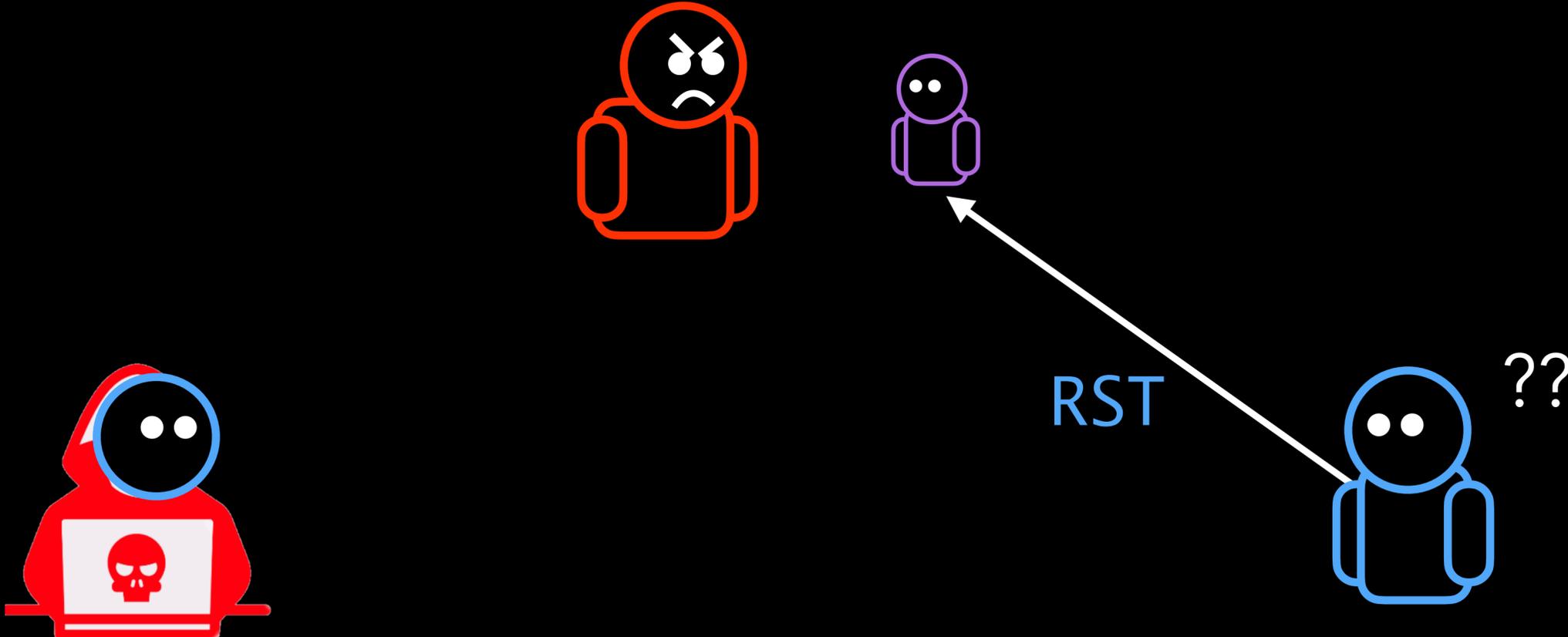
Mega-amplifier cause #1: Victim-sustained loops



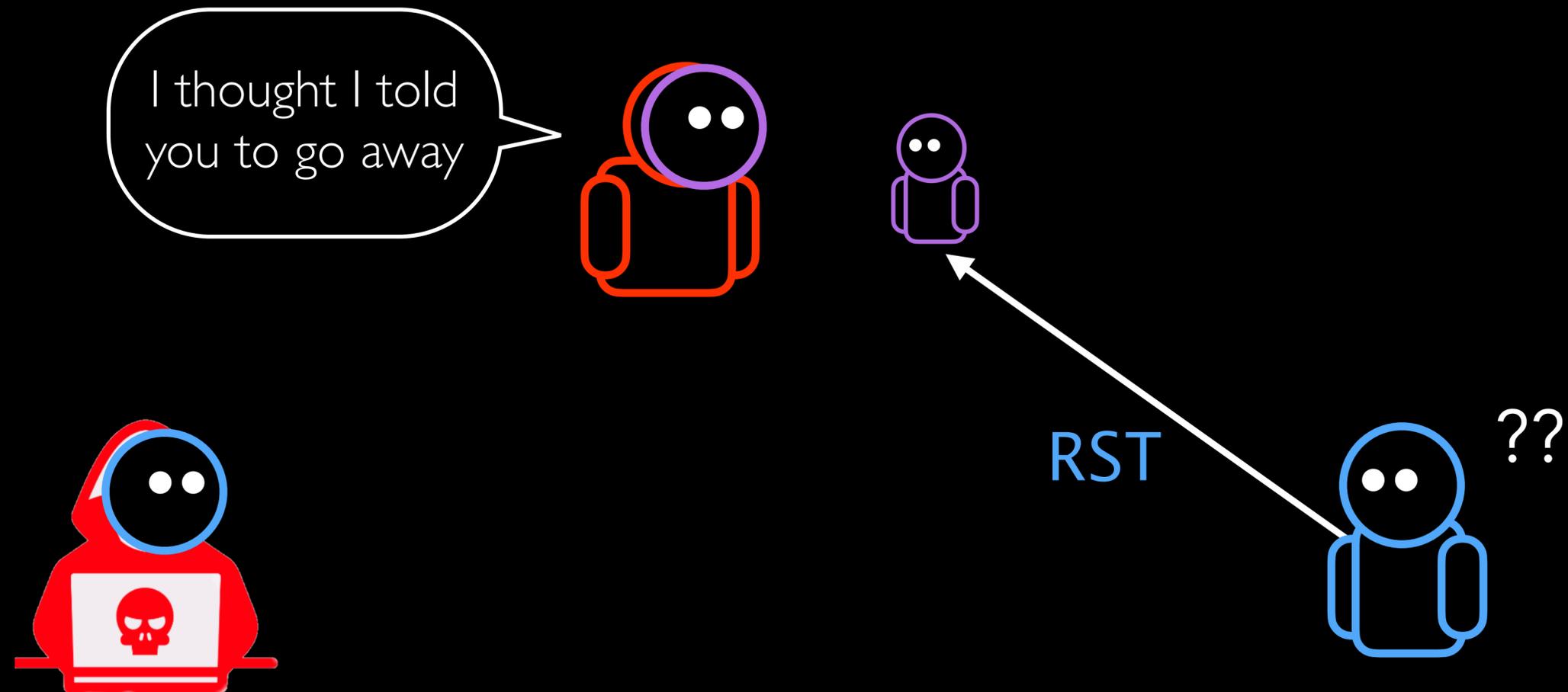
Mega-amplifier cause #1: Victim-sustained loops



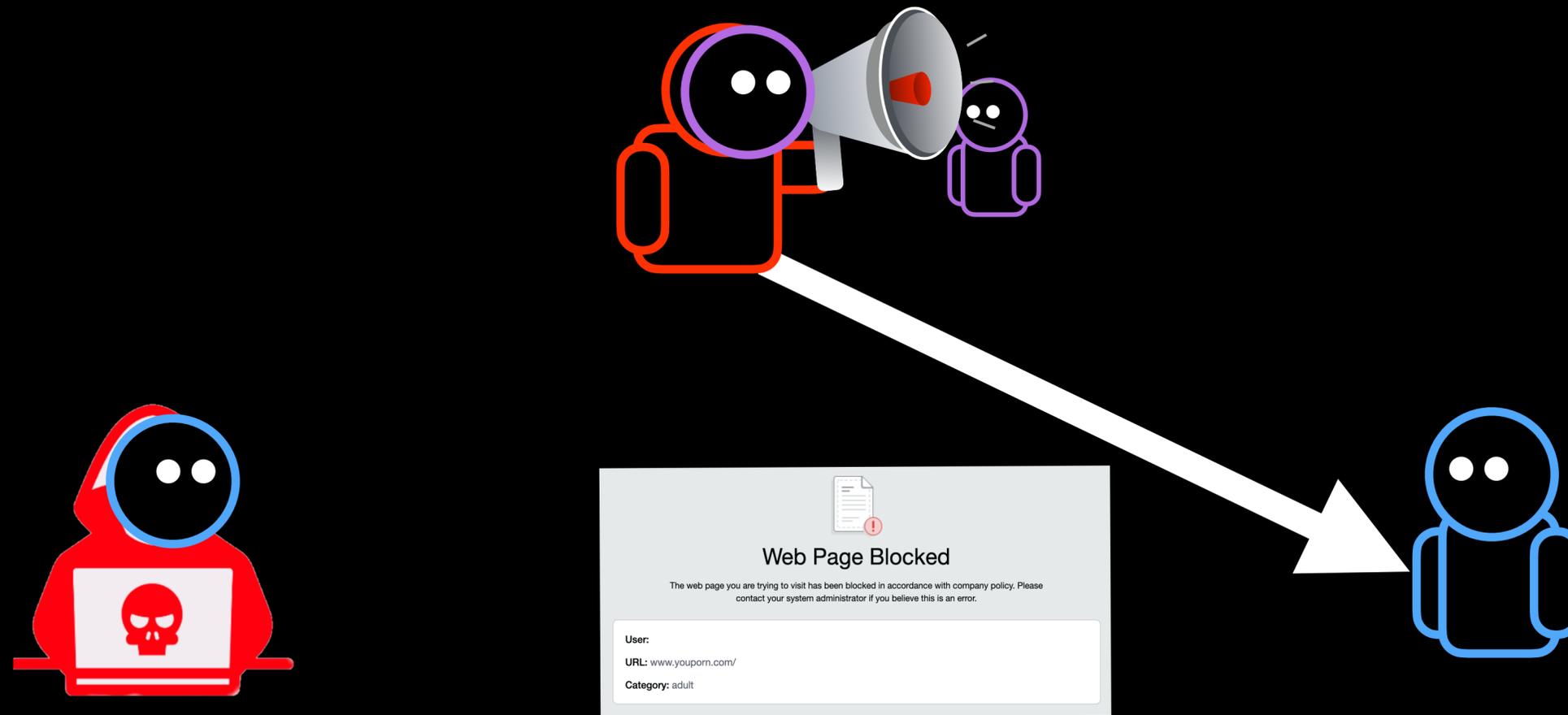
Mega-amplifier cause #1: Victim-sustained loops



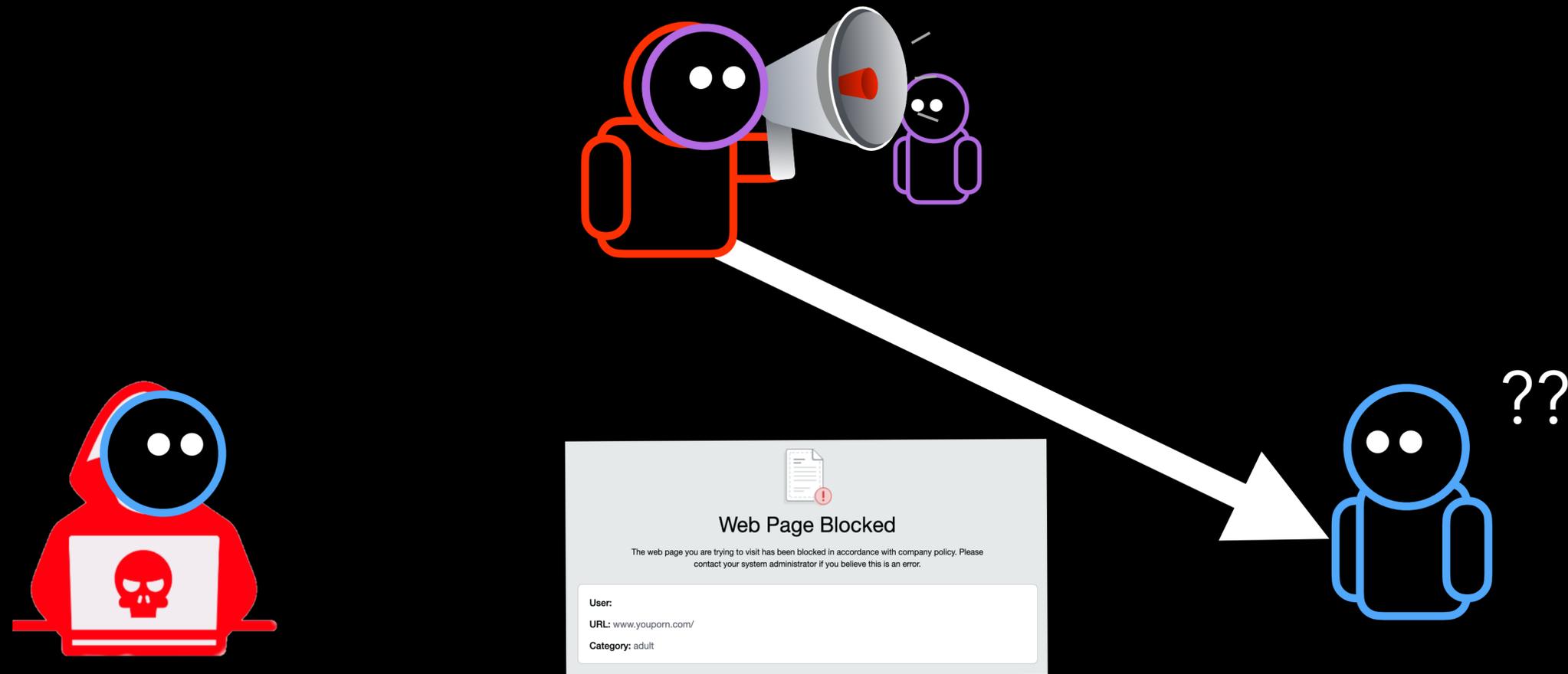
Mega-amplifier cause #1: Victim-sustained loops



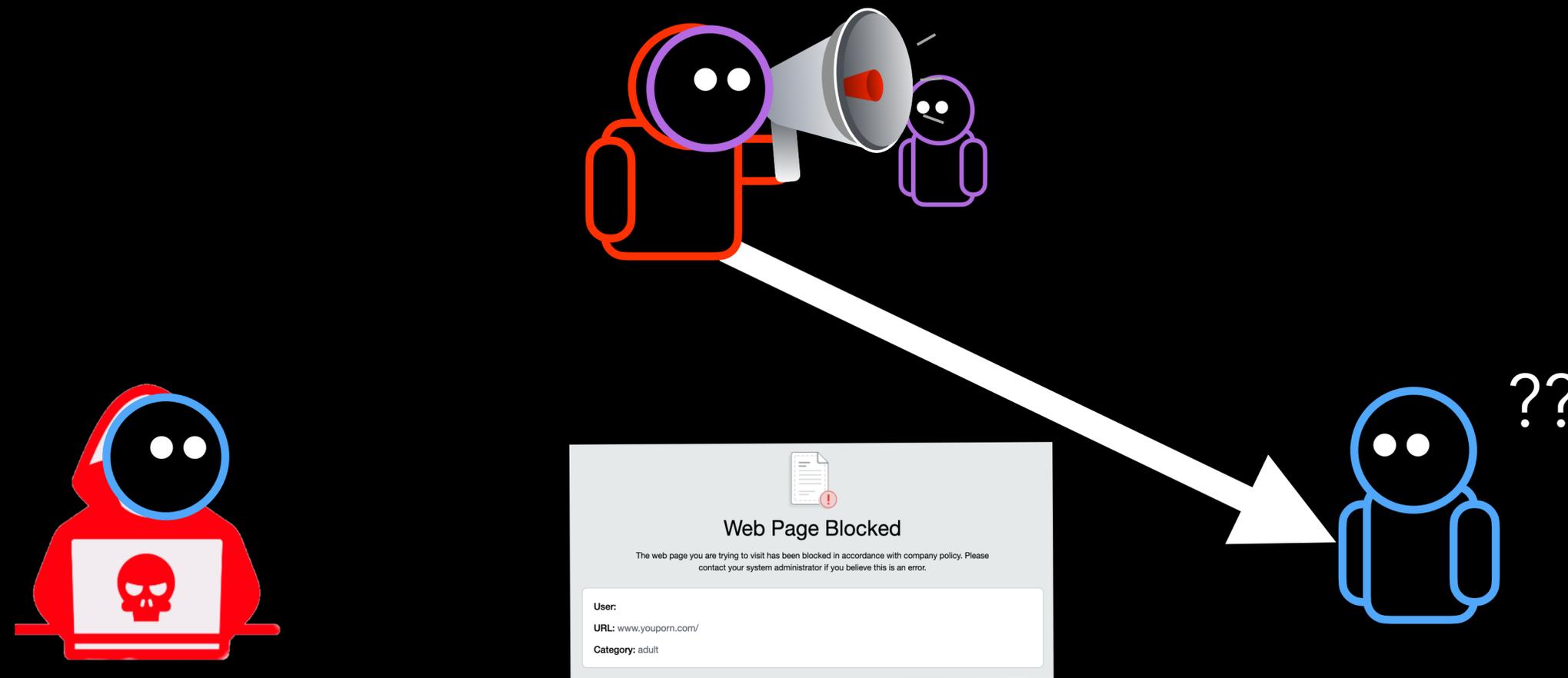
Mega-amplifier cause #1: Victim-sustained loops



Mega-amplifier cause #1: Victim-sustained loops



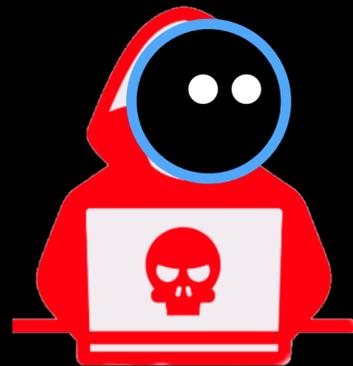
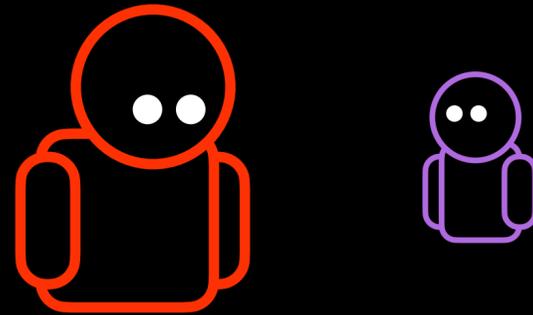
Mega-amplifier cause #1: Victim-sustained loops



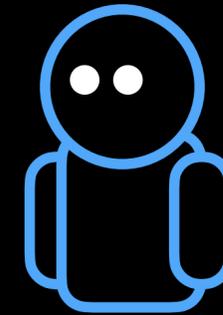
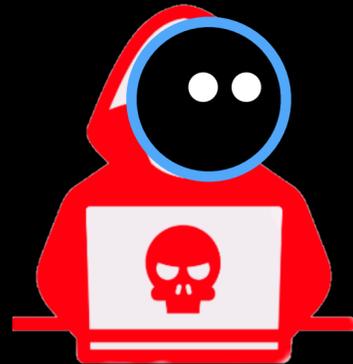
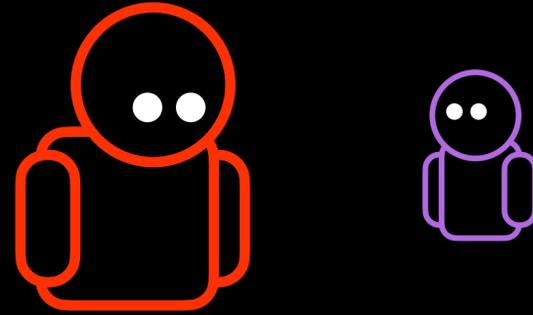
Victim-sustained amplification can be effectively *infinite*

Attacks the victim's downlink *and* uplink

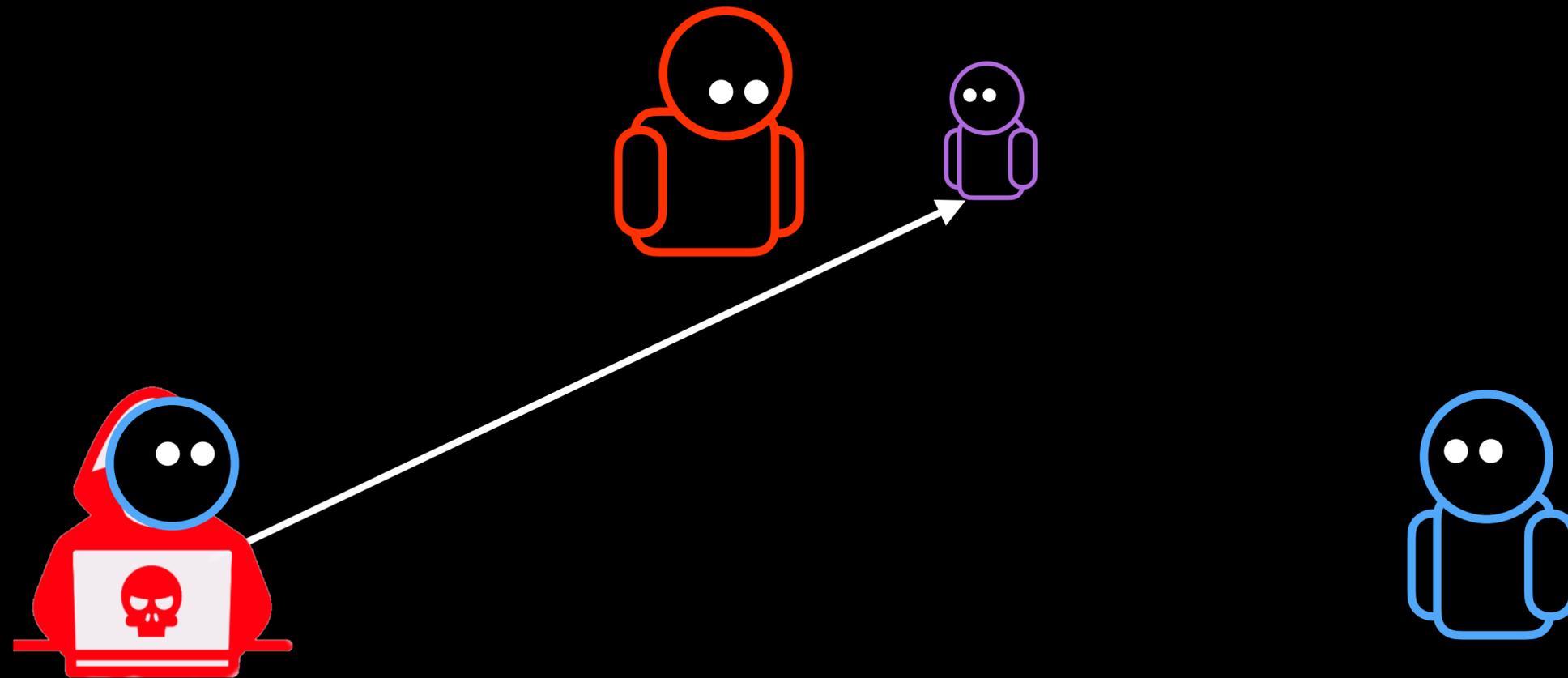
Mega-amplifier cause #2



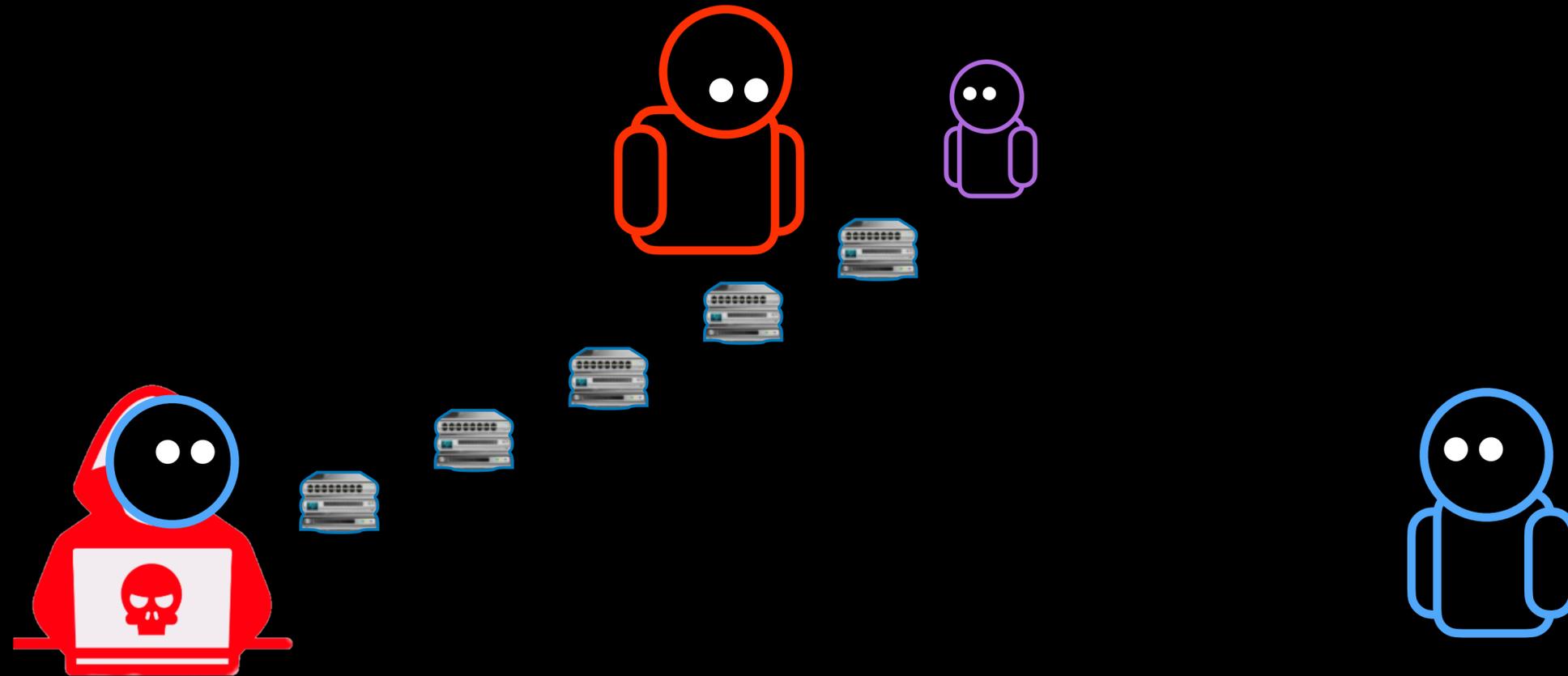
Mega-amplifier cause #2



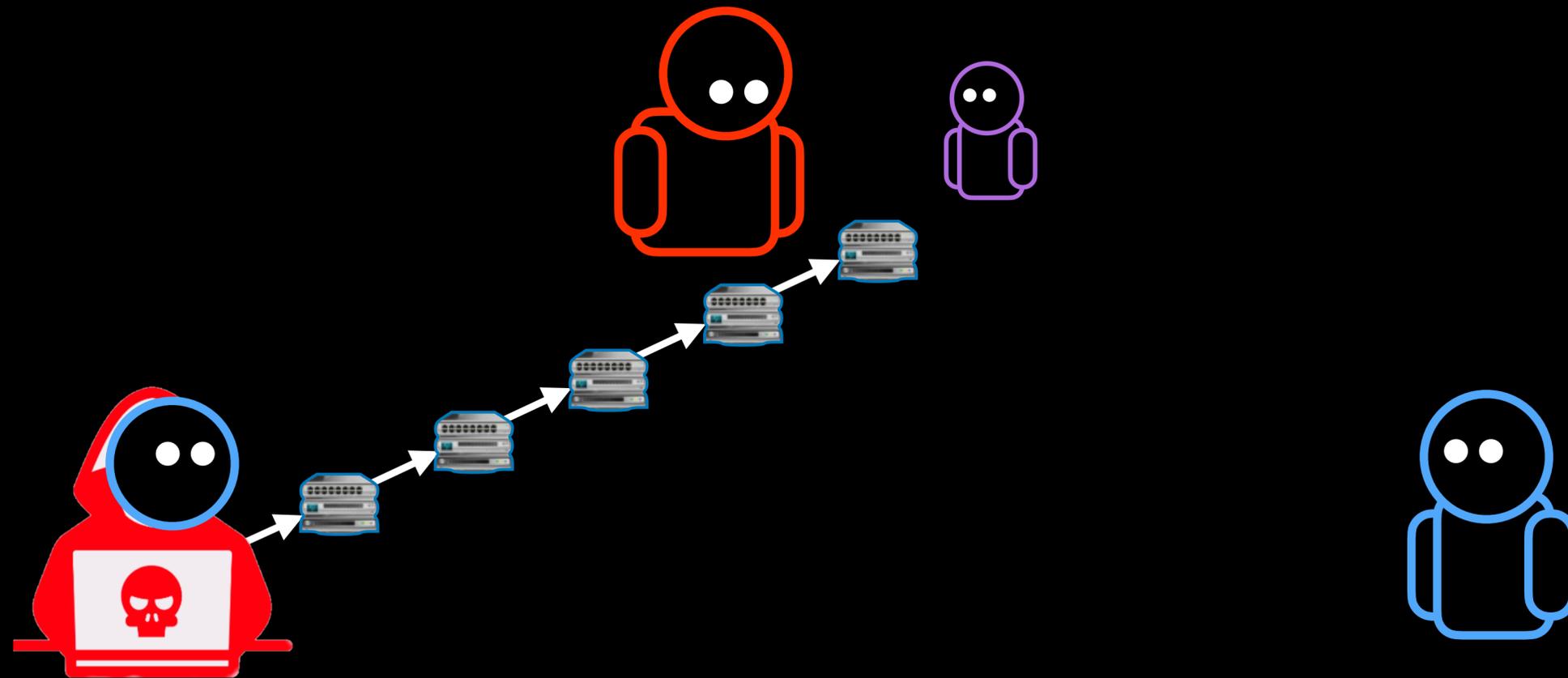
Mega-amplifier cause #2



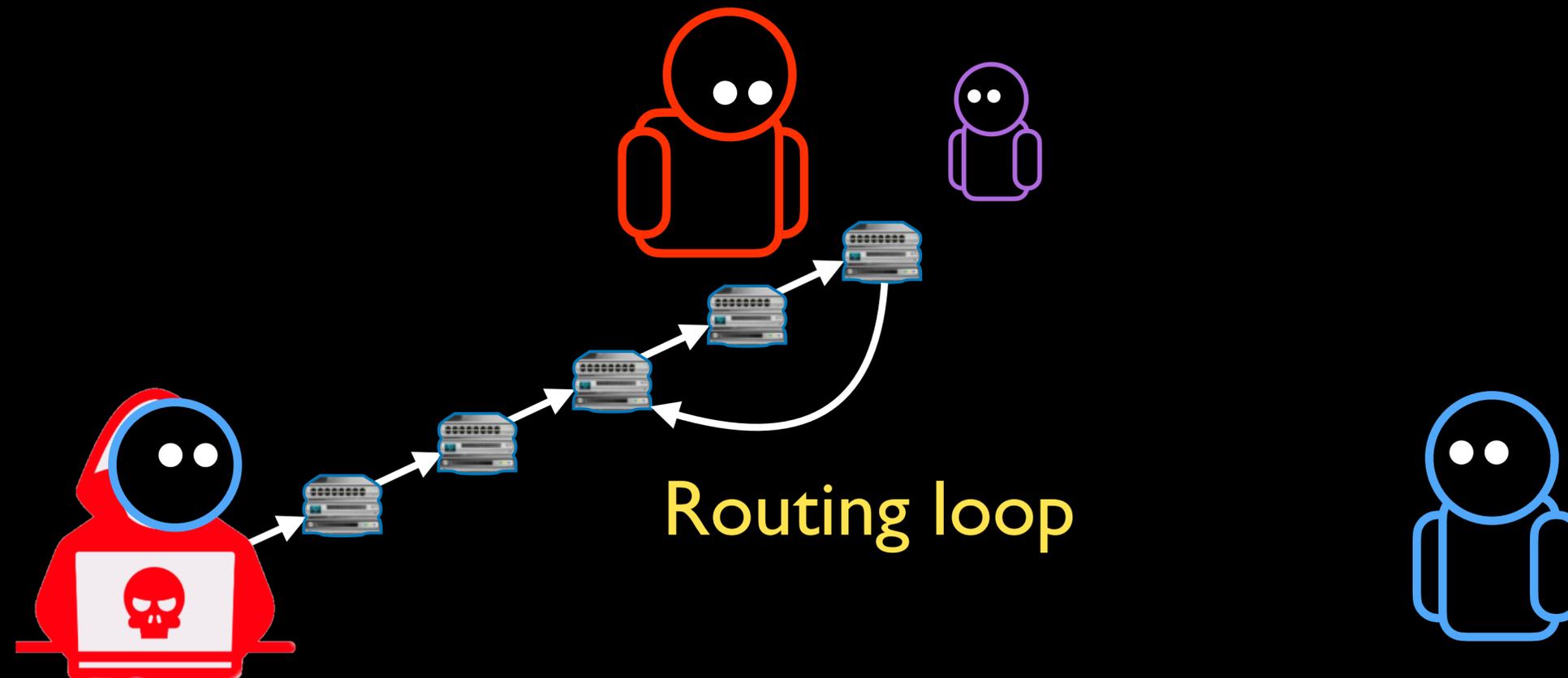
Mega-amplifier cause #2



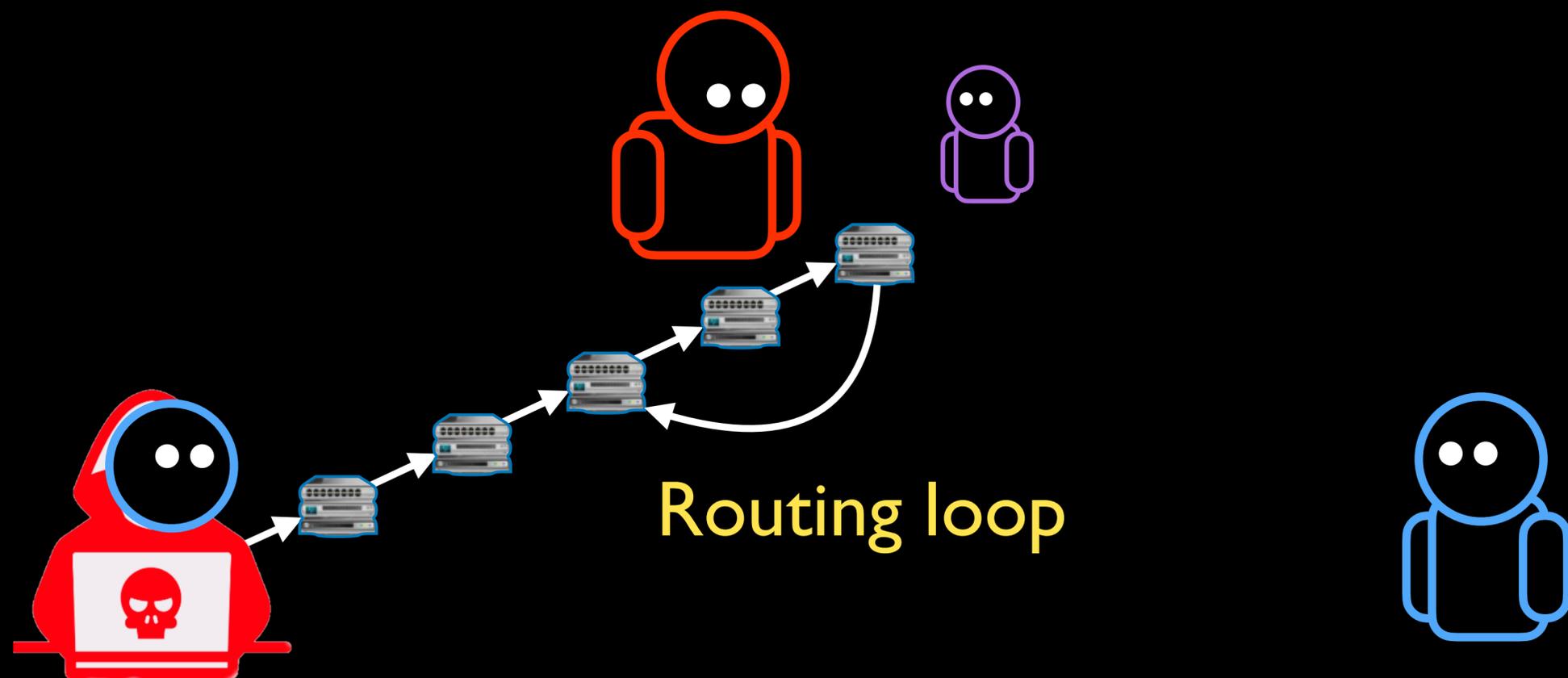
Mega-amplifier cause #2



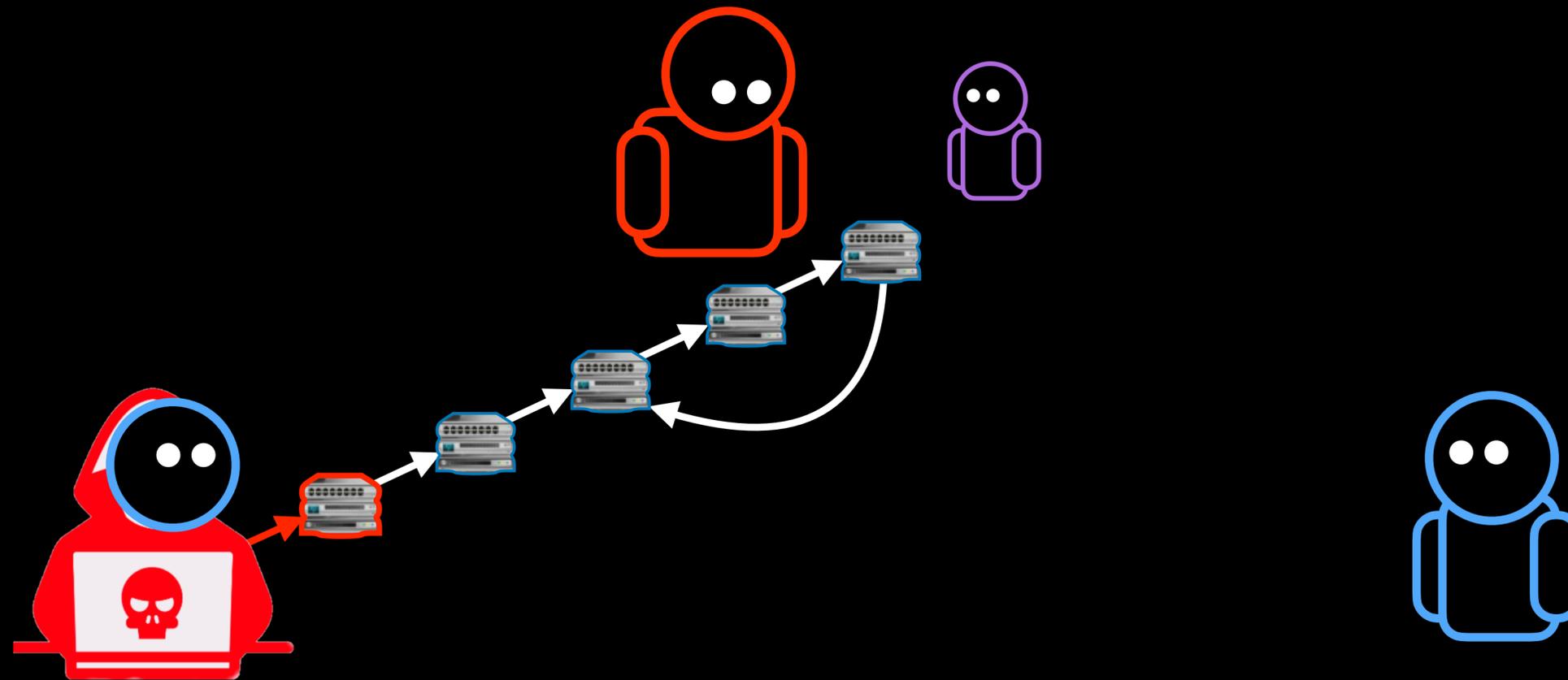
Mega-amplifier cause #2



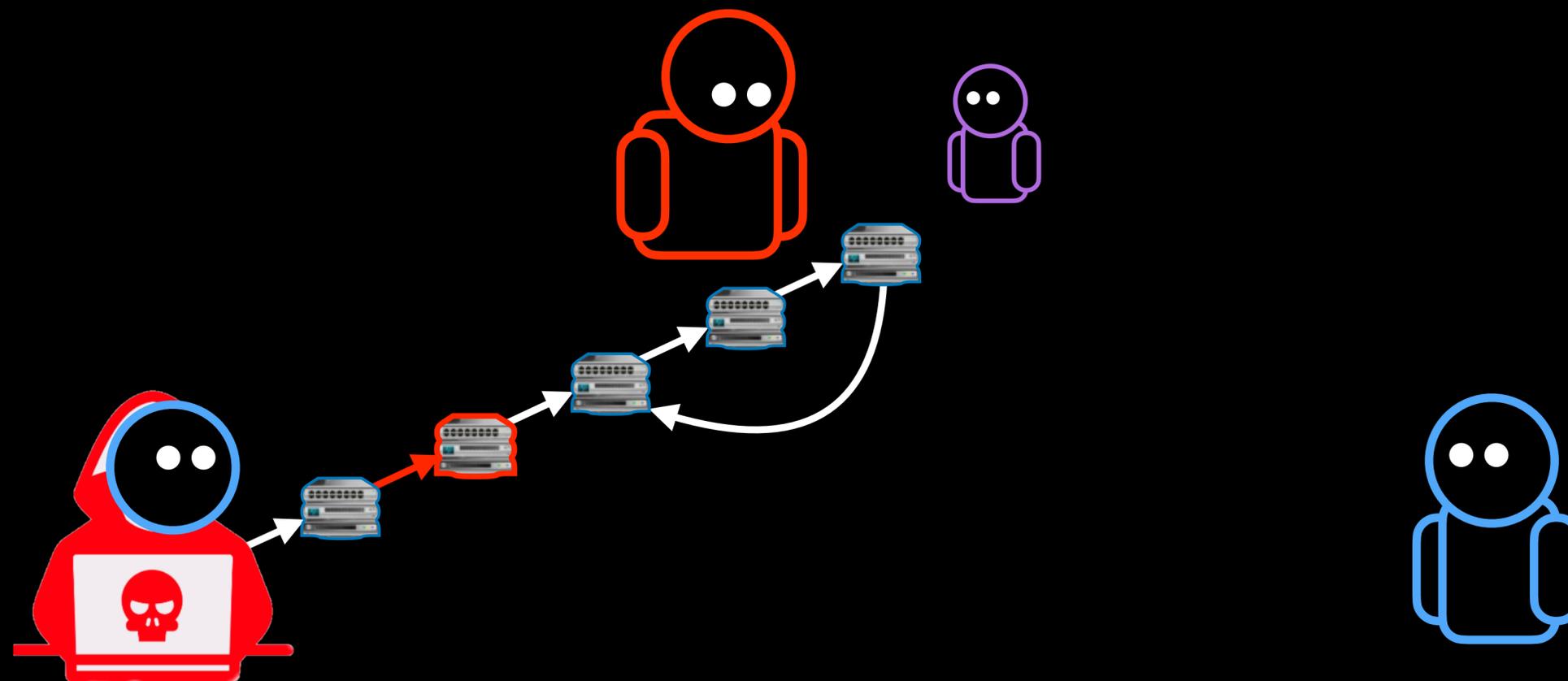
Mega-amplifier cause #2: Routing loops



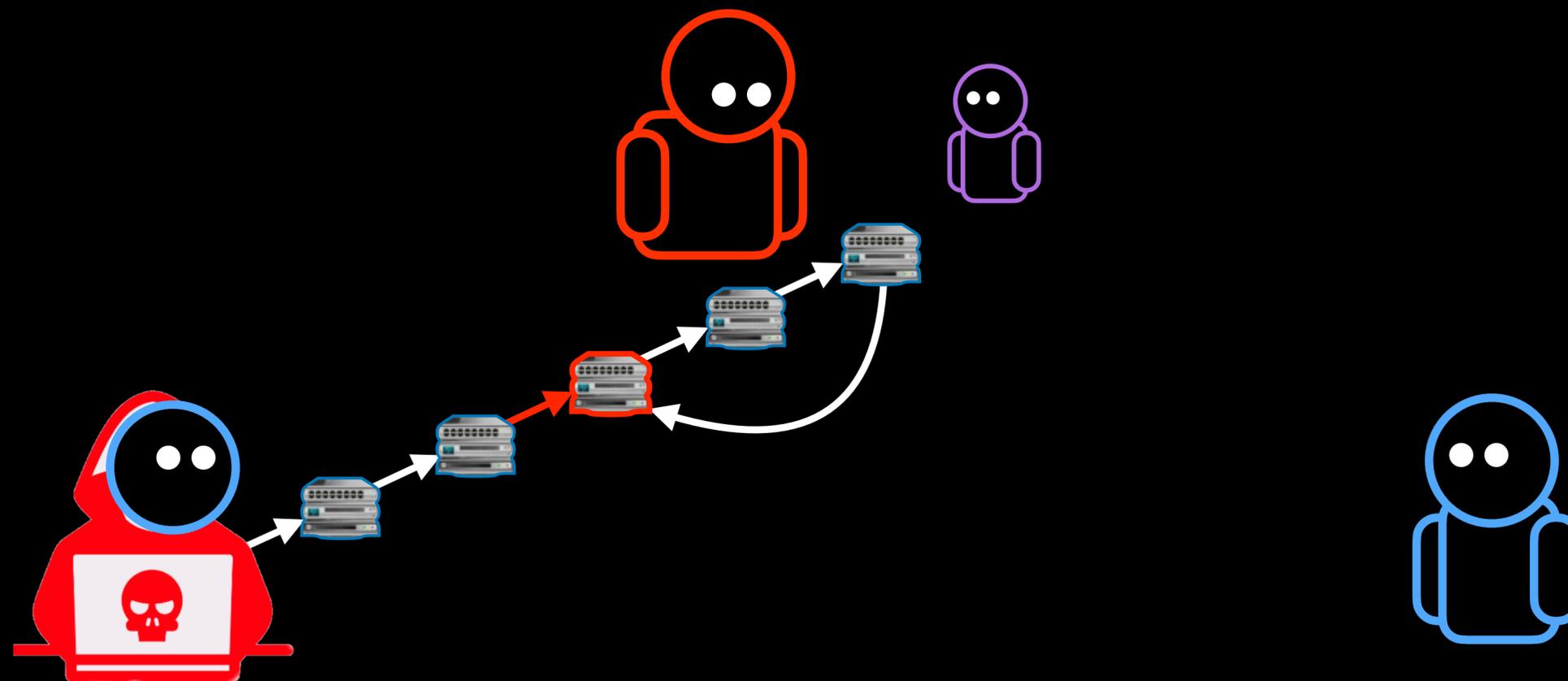
Mega-amplifier cause #2: Routing loops



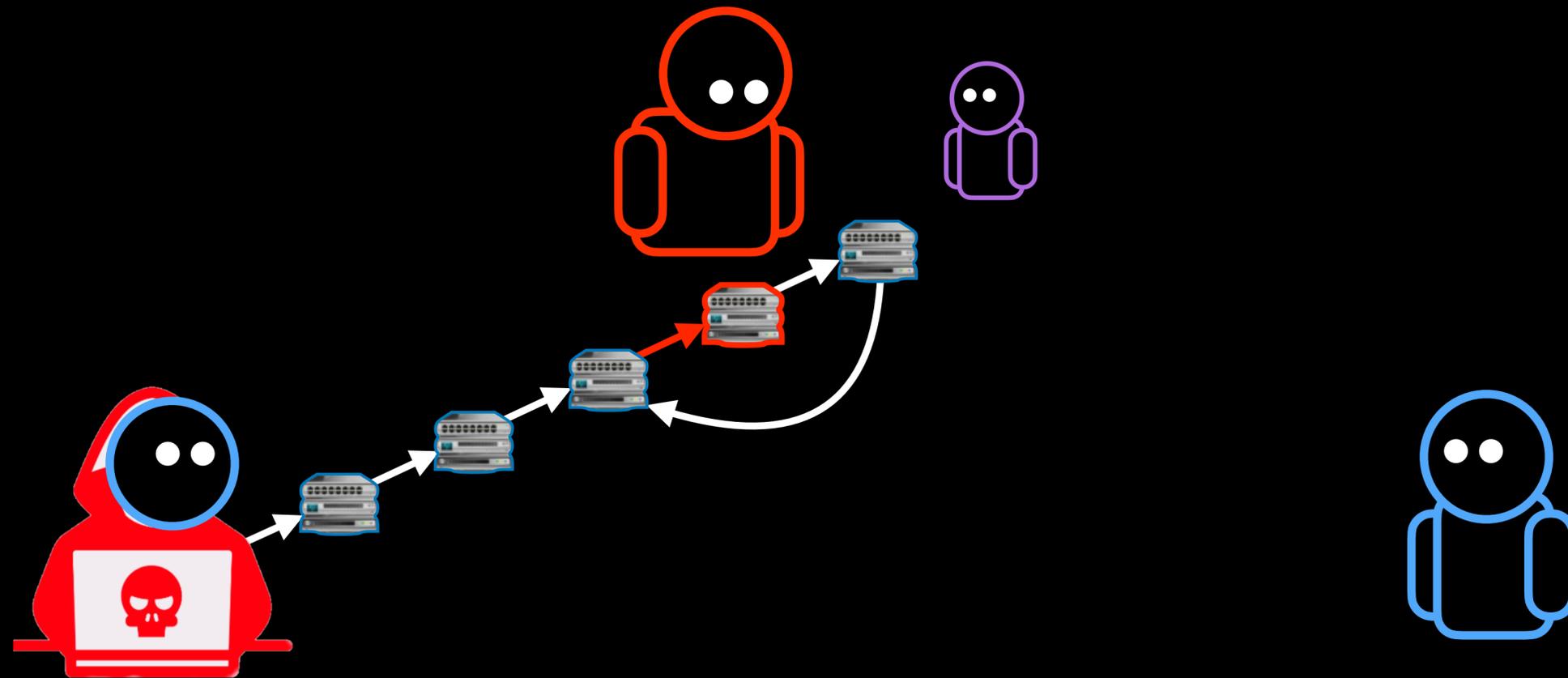
Mega-amplifier cause #2: Routing loops



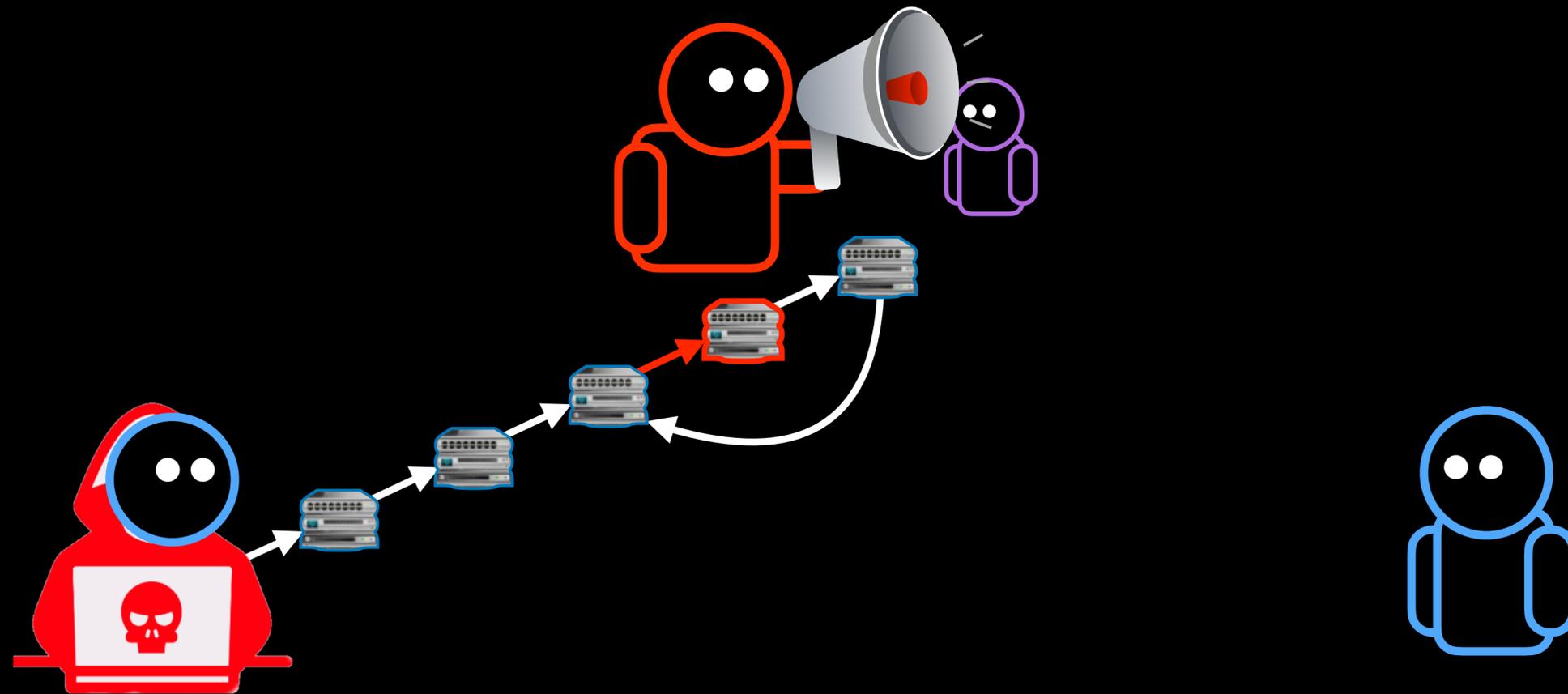
Mega-amplifier cause #2: Routing loops



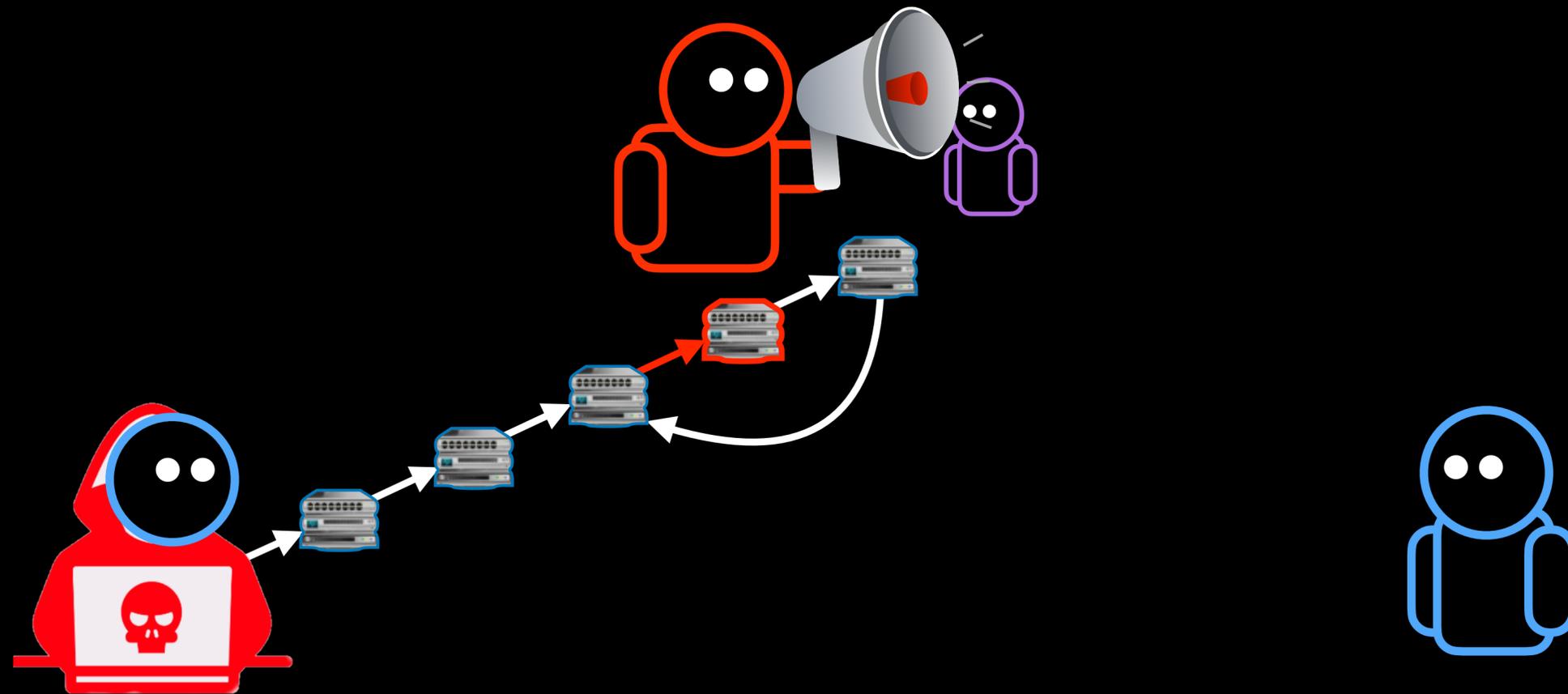
Mega-amplifier cause #2: Routing loops



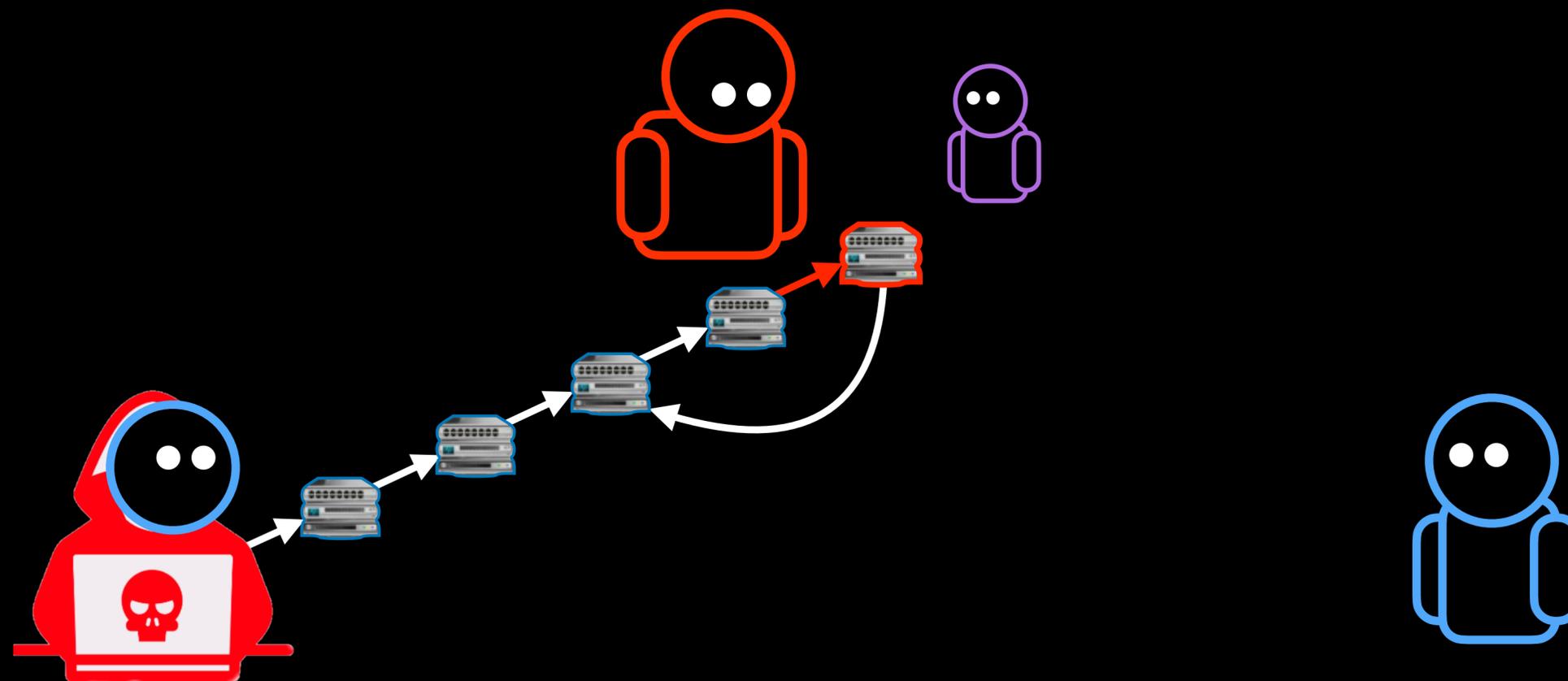
Mega-amplifier cause #2: Routing loops



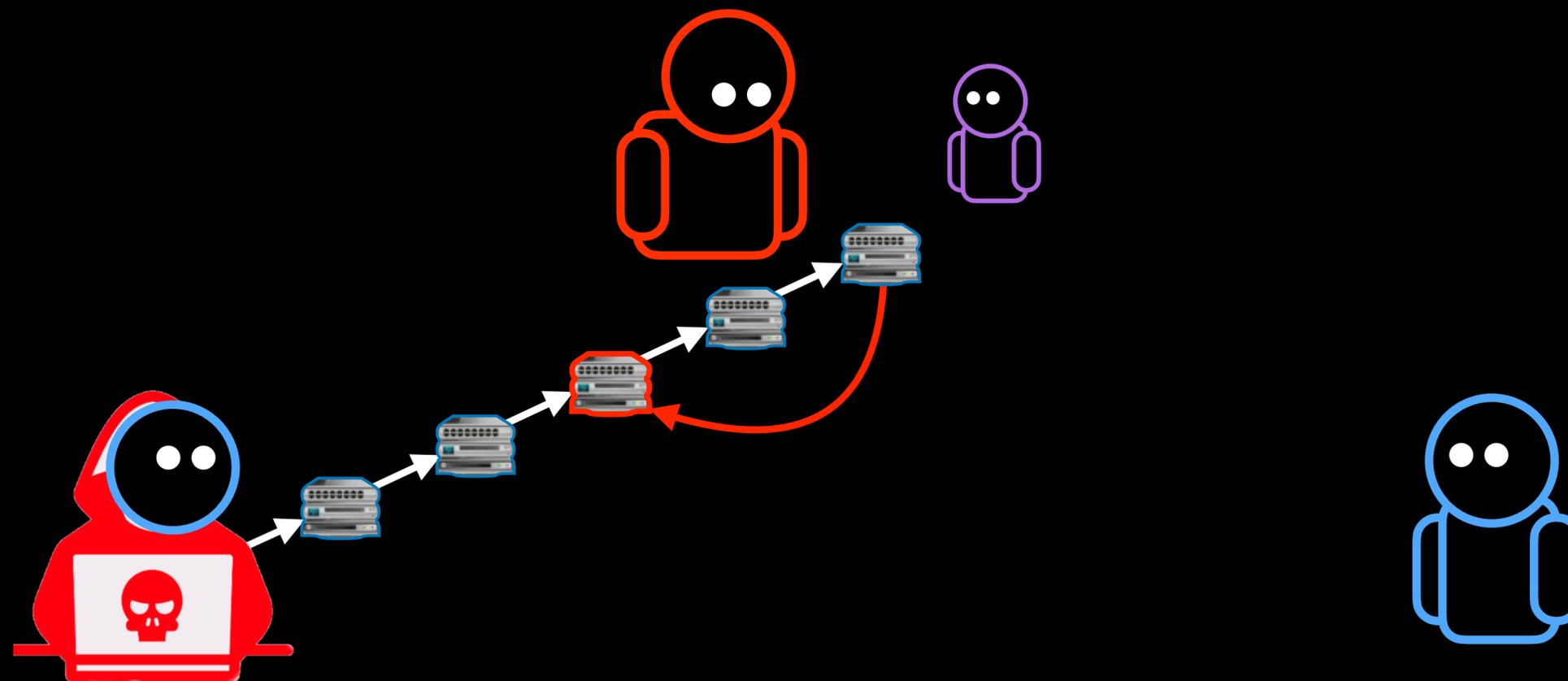
Mega-amplifier cause #2: Routing loops



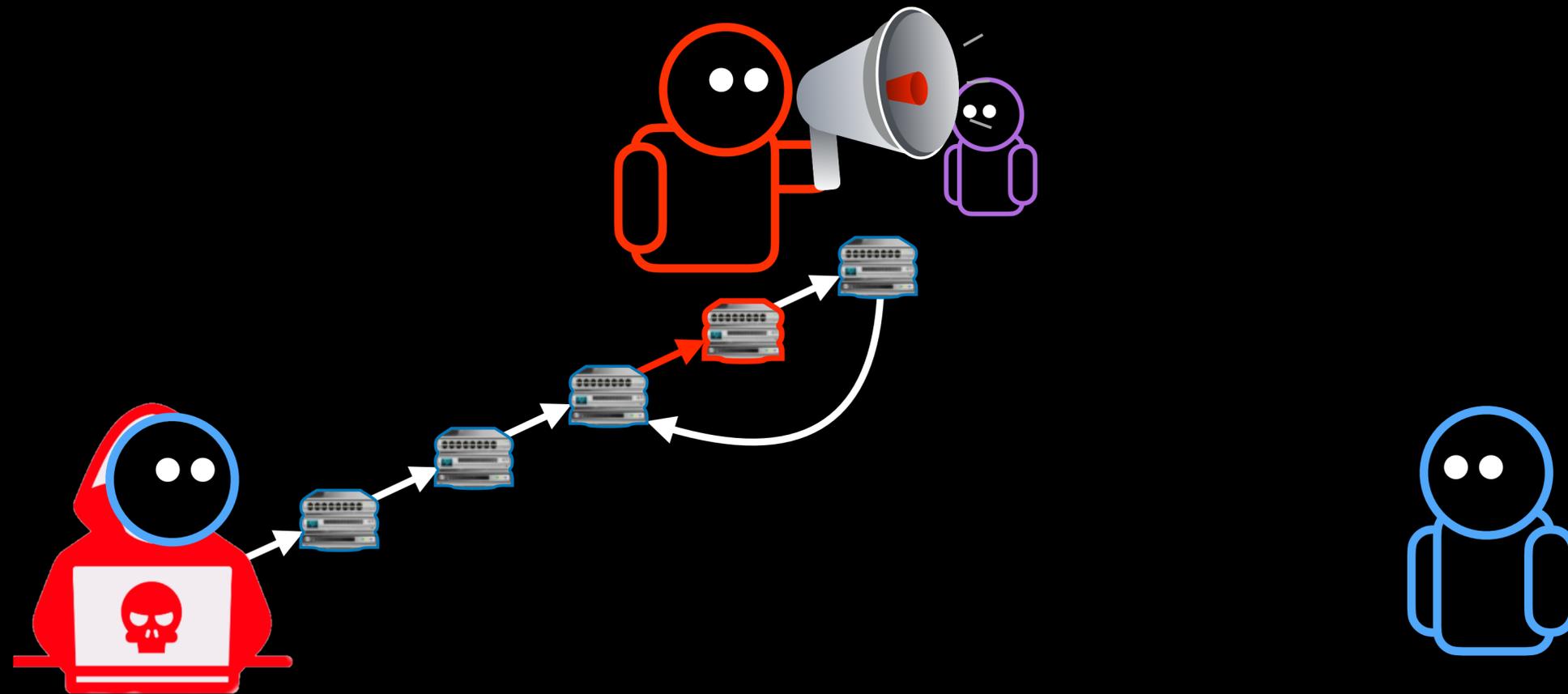
Mega-amplifier cause #2: Routing loops



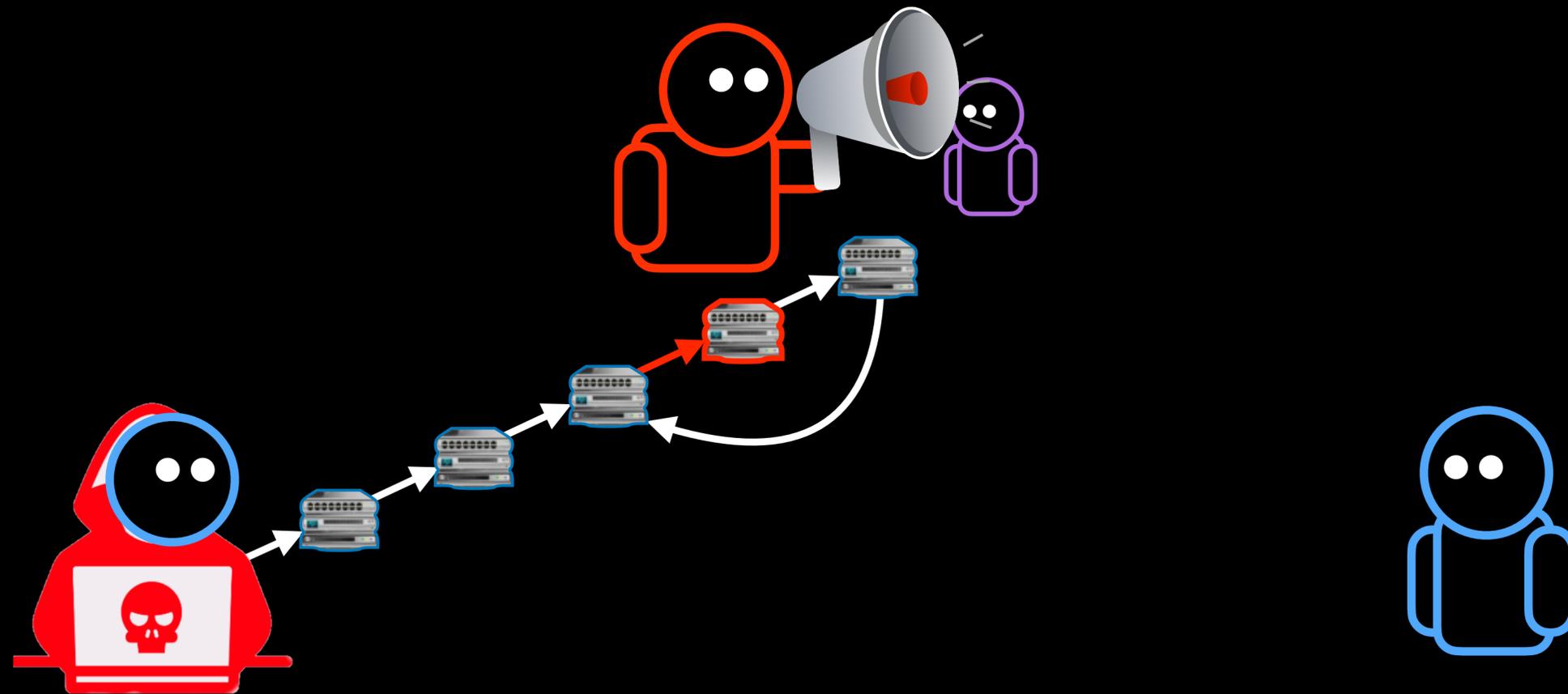
Mega-amplifier cause #2: Routing loops



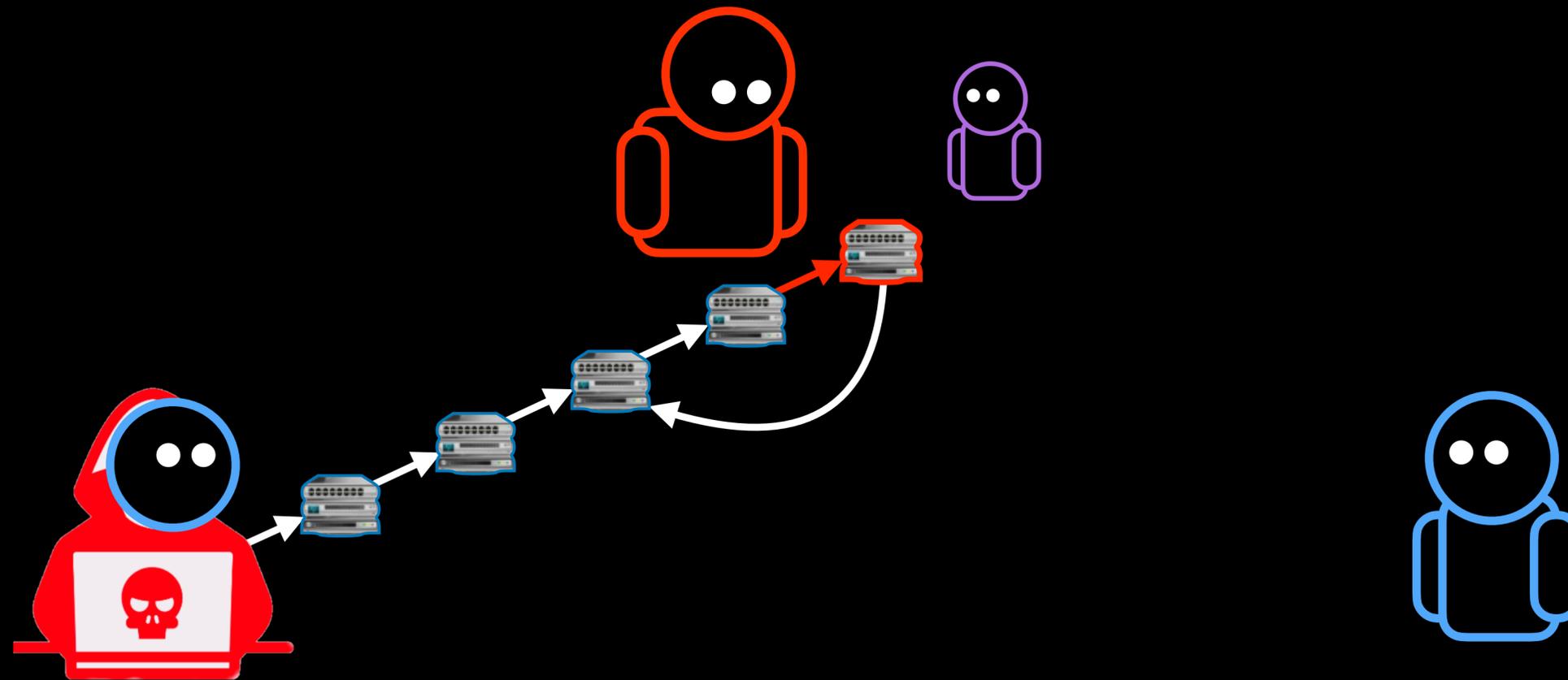
Mega-amplifier cause #2: Routing loops



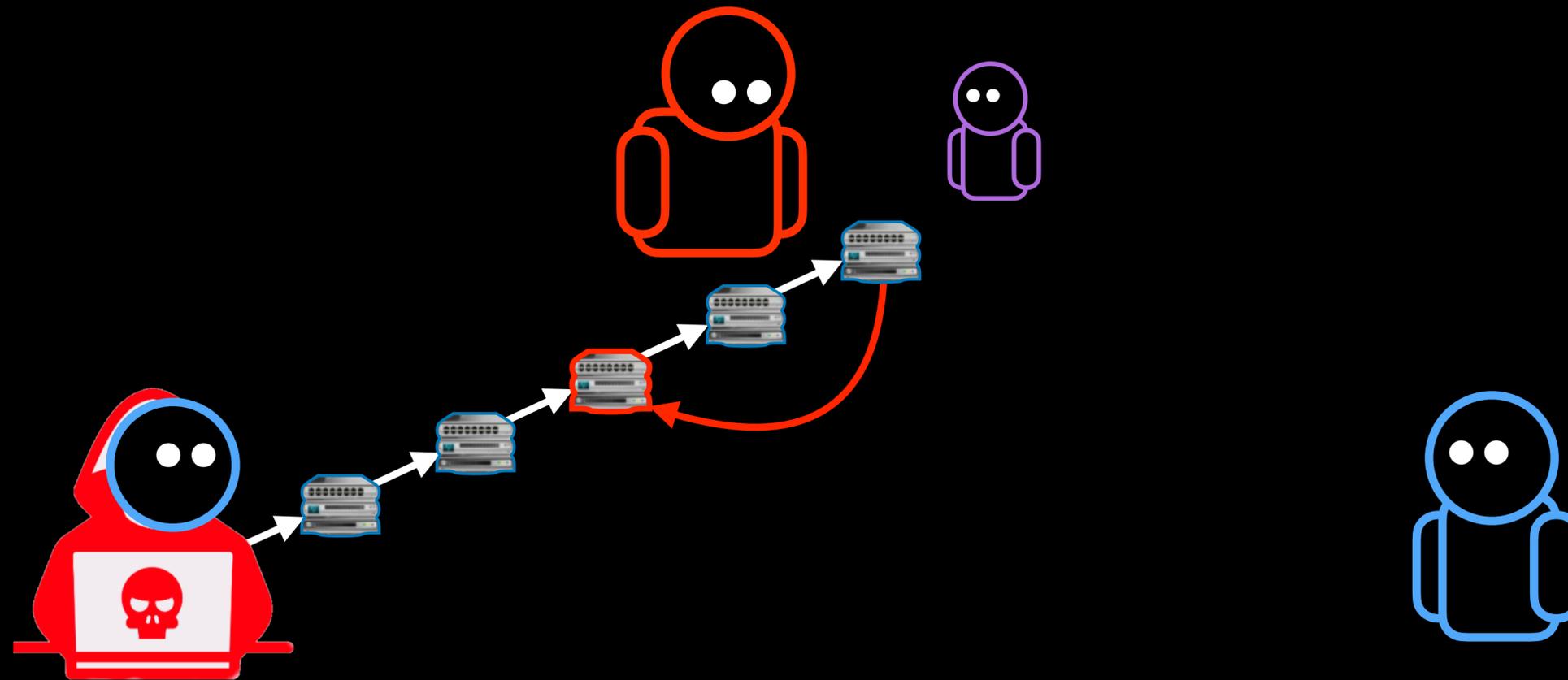
Mega-amplifier cause #2: Routing loops



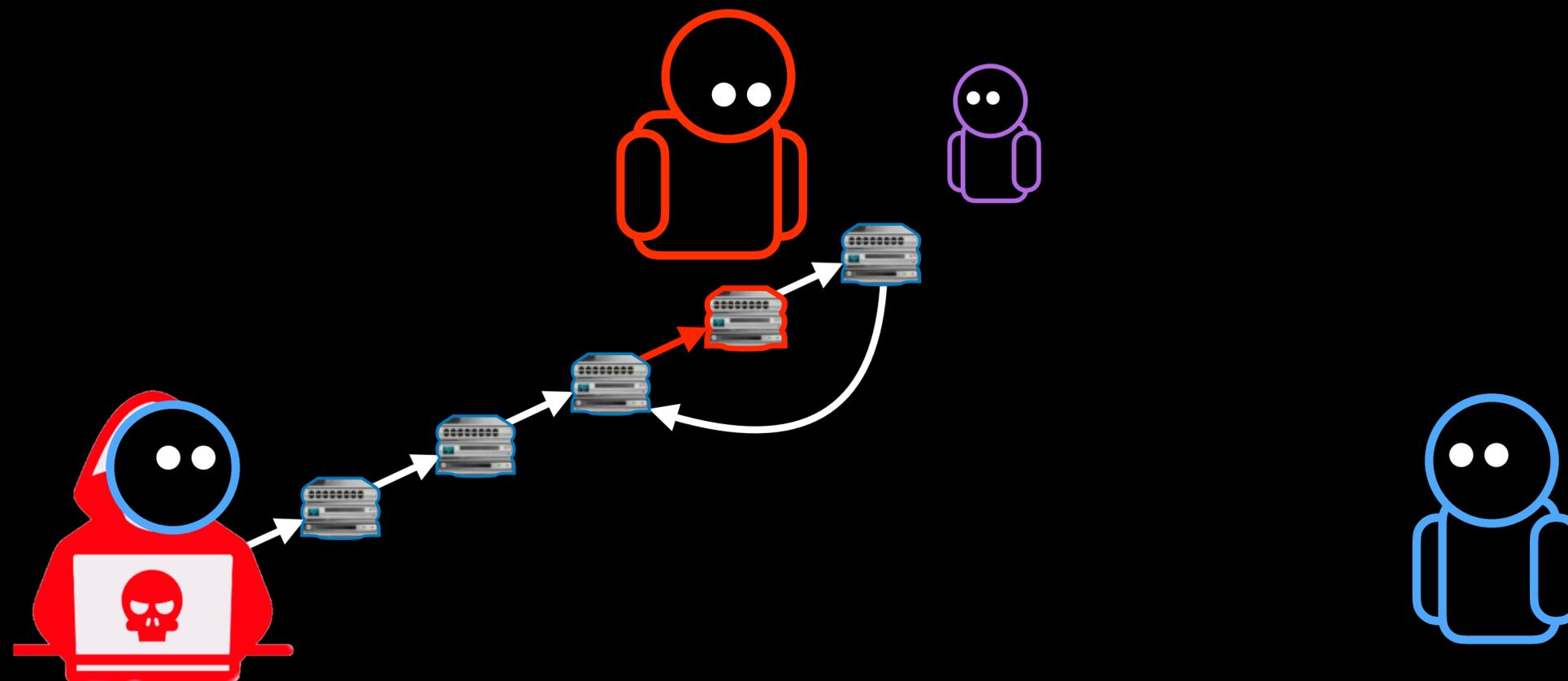
Mega-amplifier cause #2: Routing loops



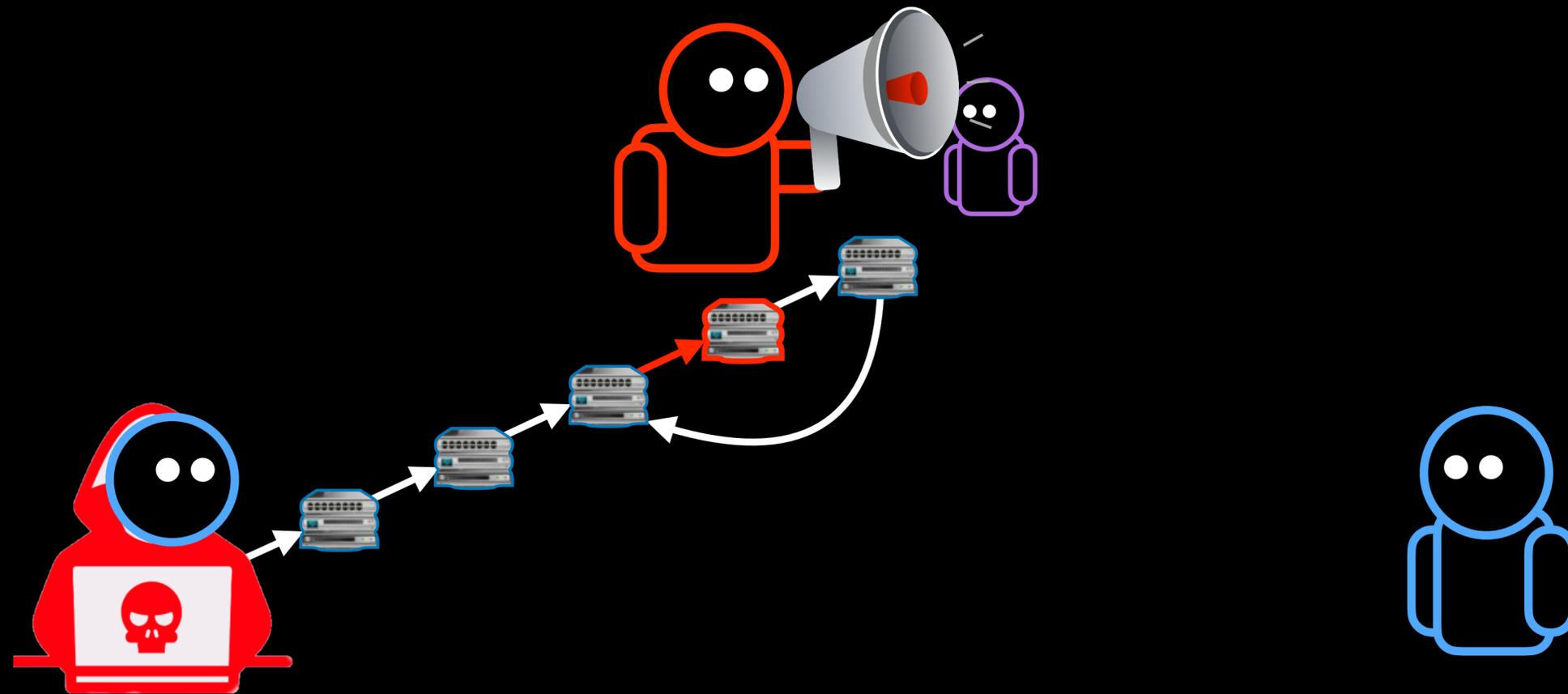
Mega-amplifier cause #2: Routing loops



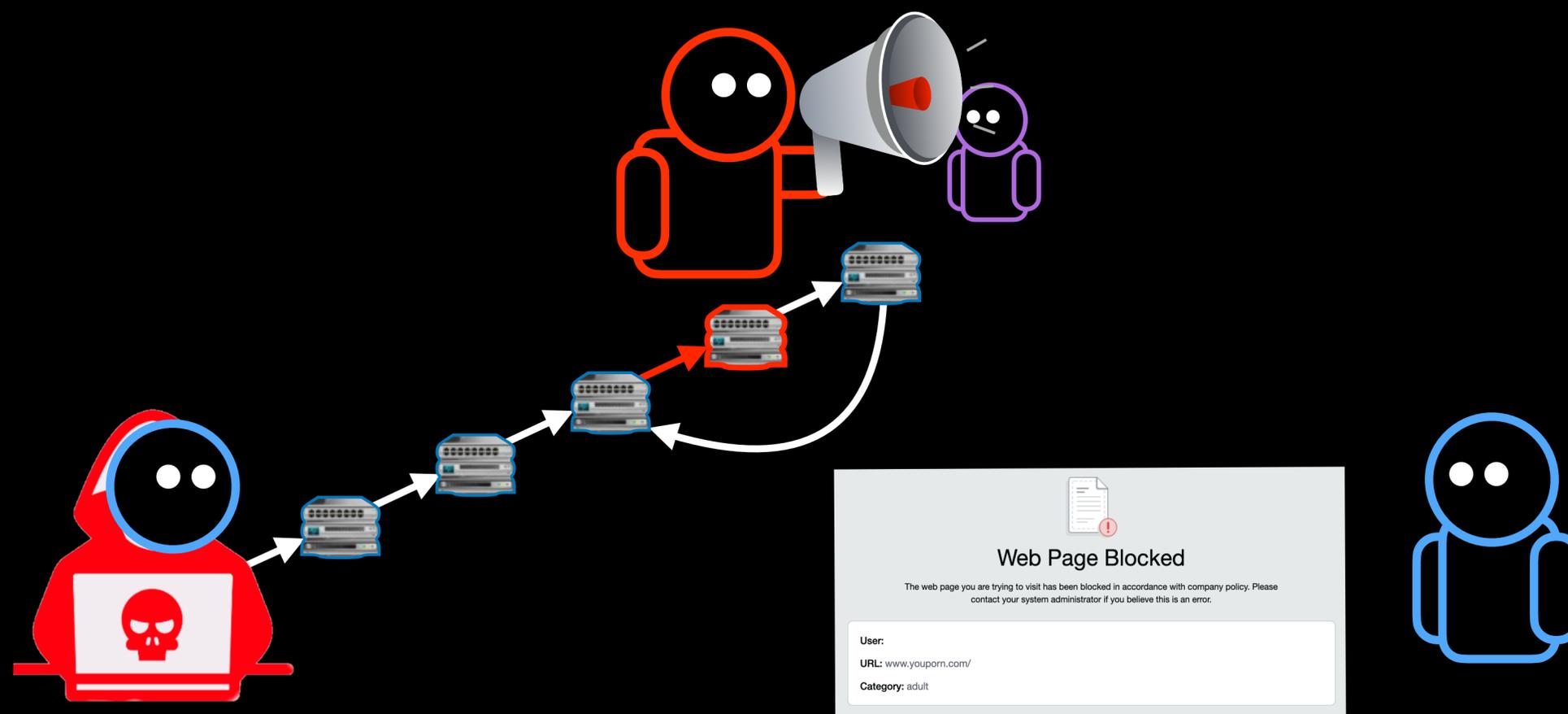
Mega-amplifier cause #2: Routing loops



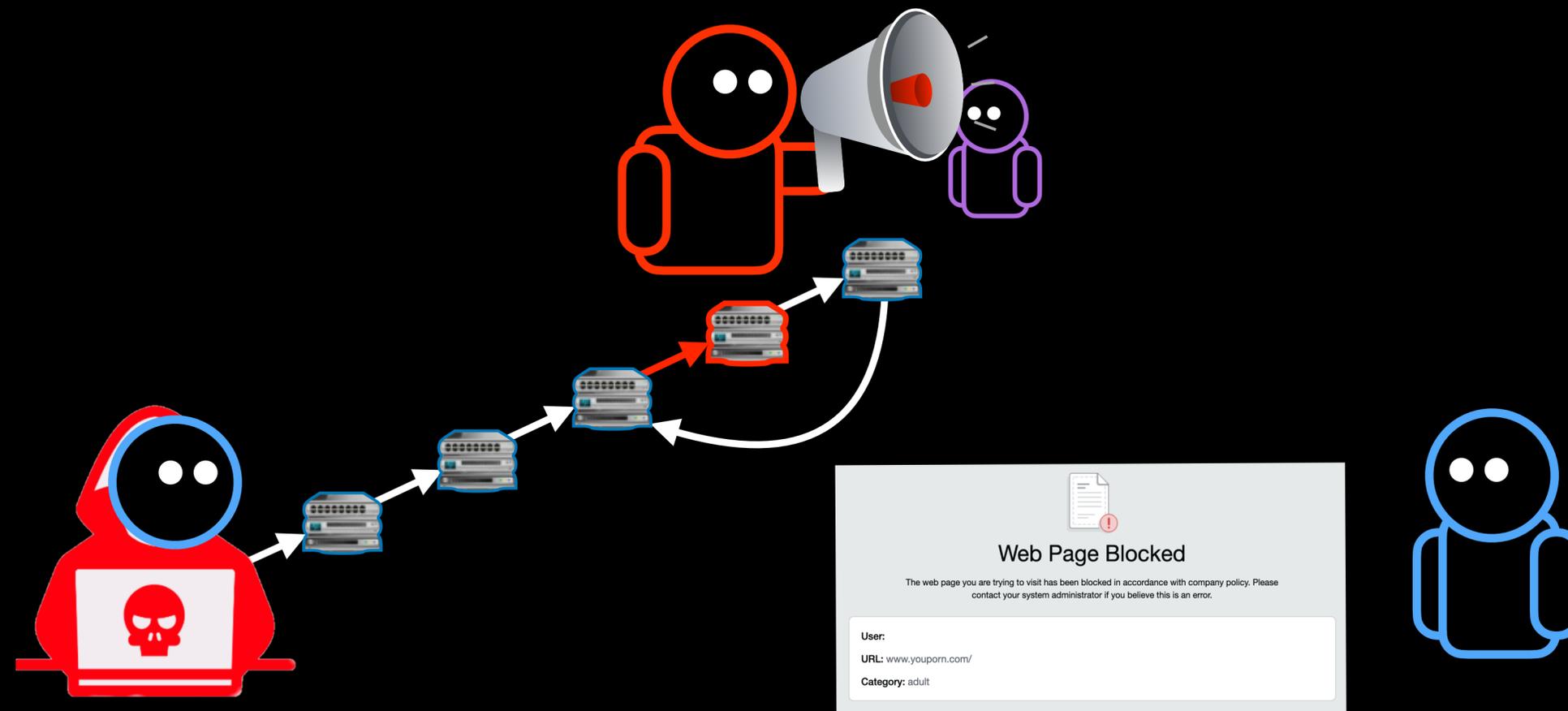
Mega-amplifier cause #2: Routing loops



Mega-amplifier cause #2: Routing loops

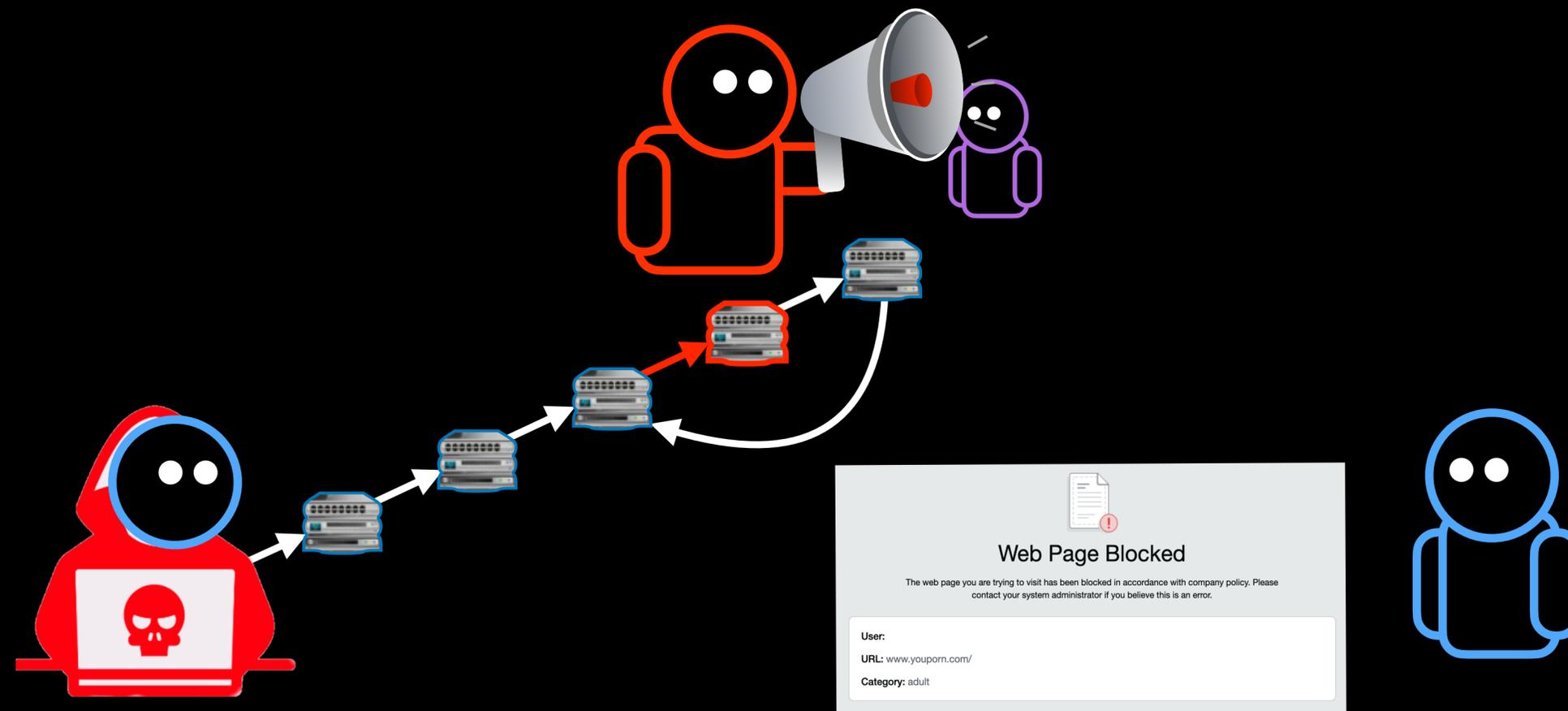


Mega-amplifier cause #2: Routing loops



Finite routing loops \Rightarrow Greater amplification with higher TTL

Mega-amplifier cause #2: Routing loops



Finite routing loops \Rightarrow Greater amplification with higher TTL

Infinite routing loops \Rightarrow *Infinite amplification*

Other details in the paper

Middlebox fingerprints

Fingerprints of packets from middleboxes

Confirmed middleboxes

TTL limited experiments to confirm most reflectors are middleboxes

Routing loop analysis

Details on prefixes that have abusable routing loops

National firewalls

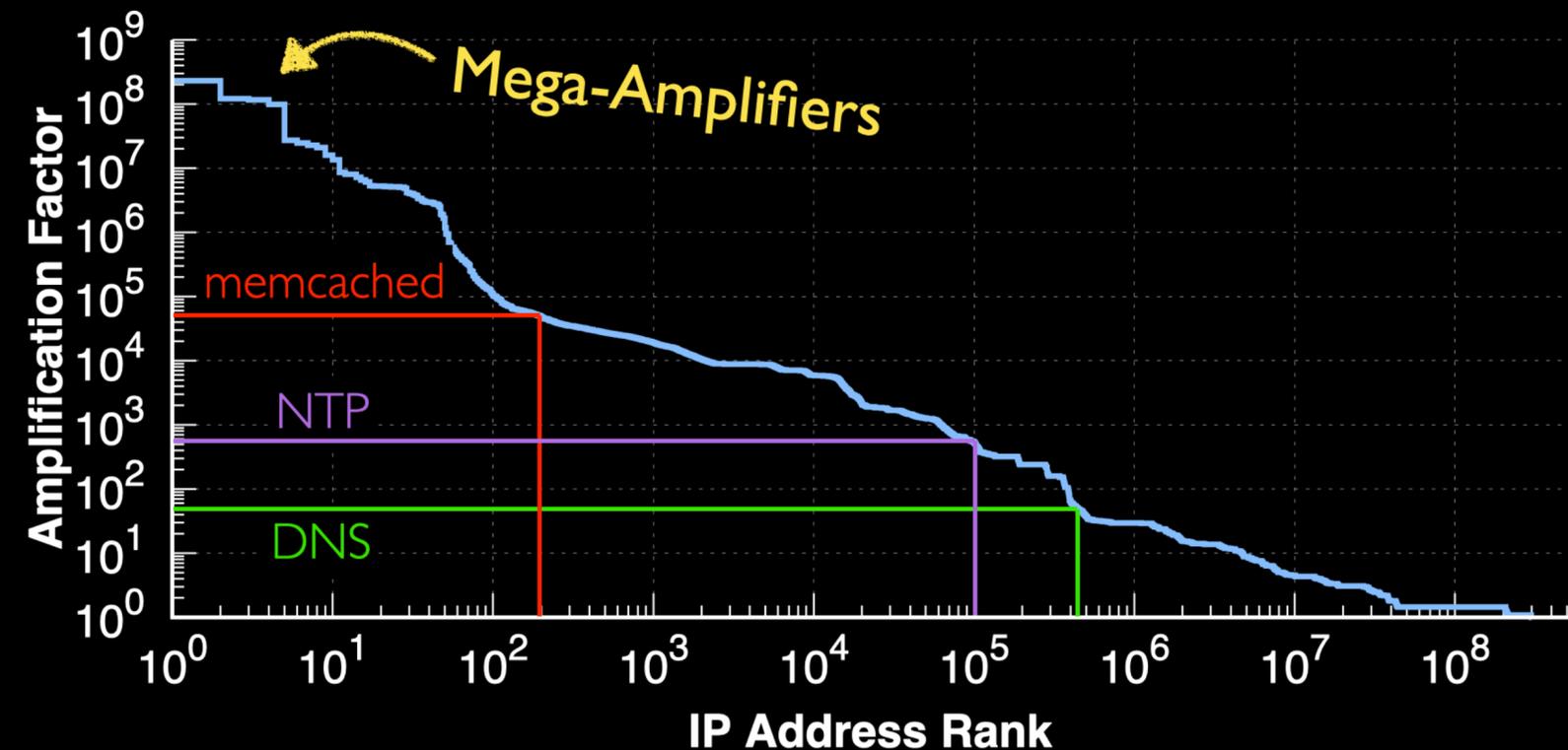
Analysis of impact of national firewalls

Weaponizing Middleboxes

Middleboxes make
TCP-based reflected amplification
possible and effective

Automated discovery of
new amplification attacks

Root causes of ∞ -amplification:
Victim-sustained & Routing-loops



Code and website

censorship.ai