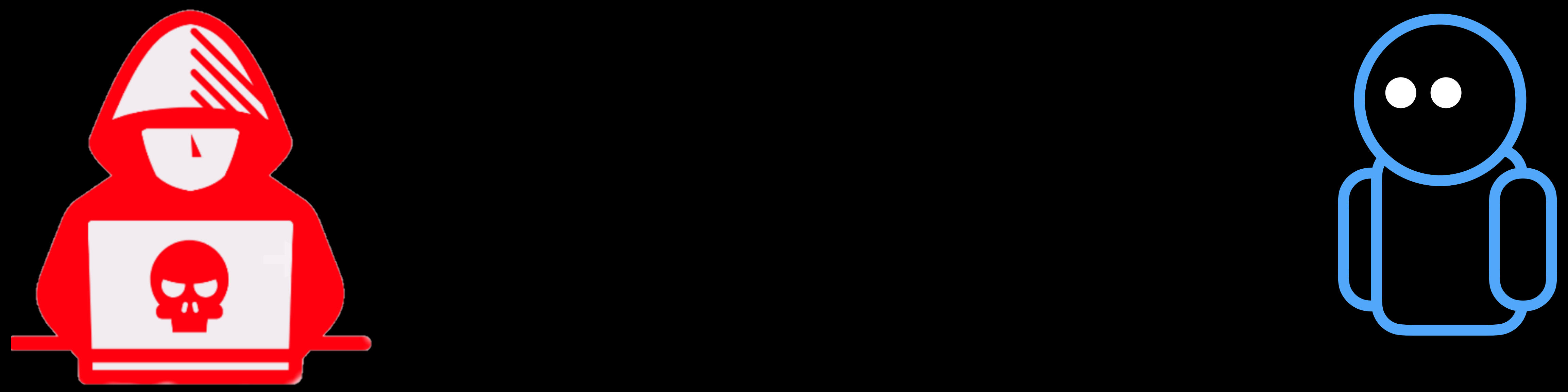
Weaponizing Middleboxes for TCP Reflected Amplification

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

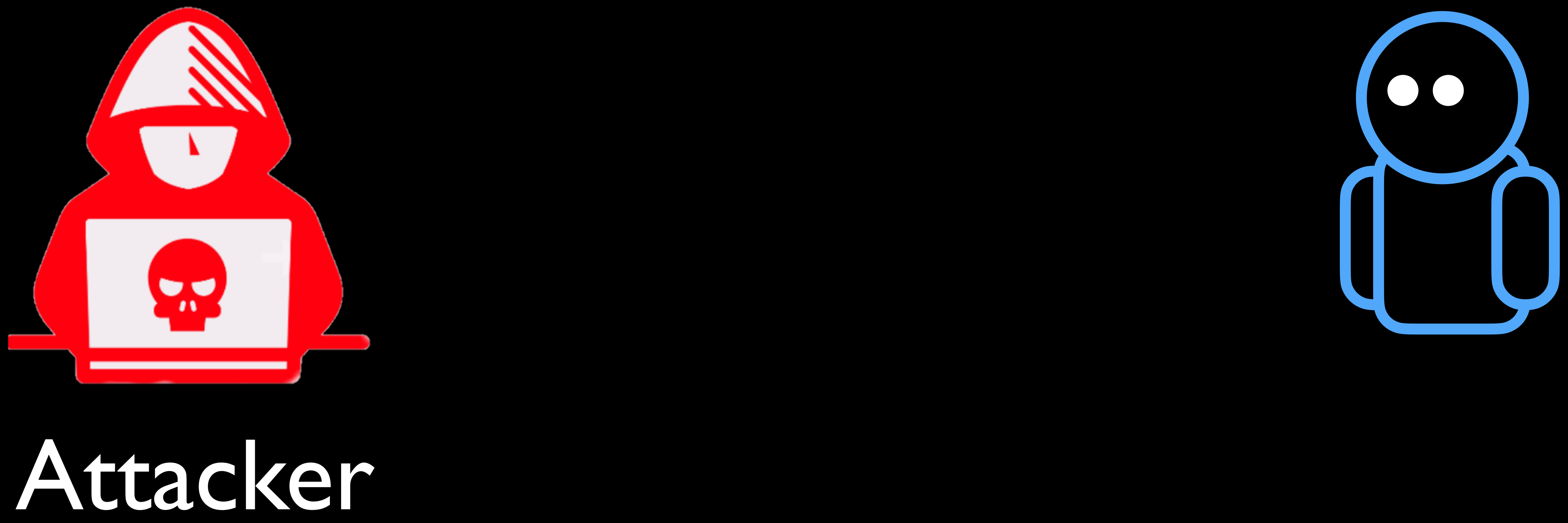
UNIVERSITY OF MARYLAND

University of Colorado Boulder

Denial of Service attacks

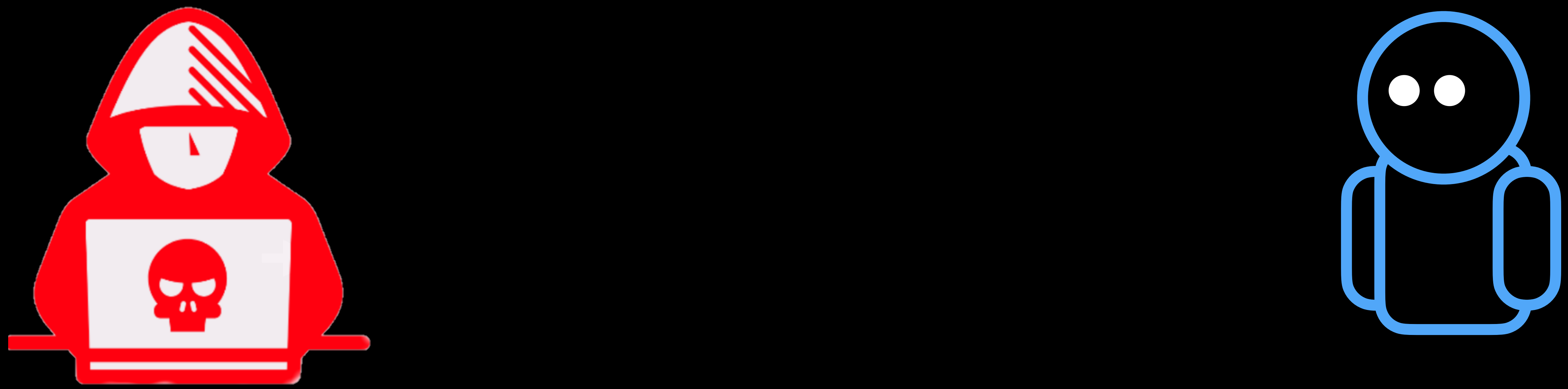


Denial of Service attacks



Attacker

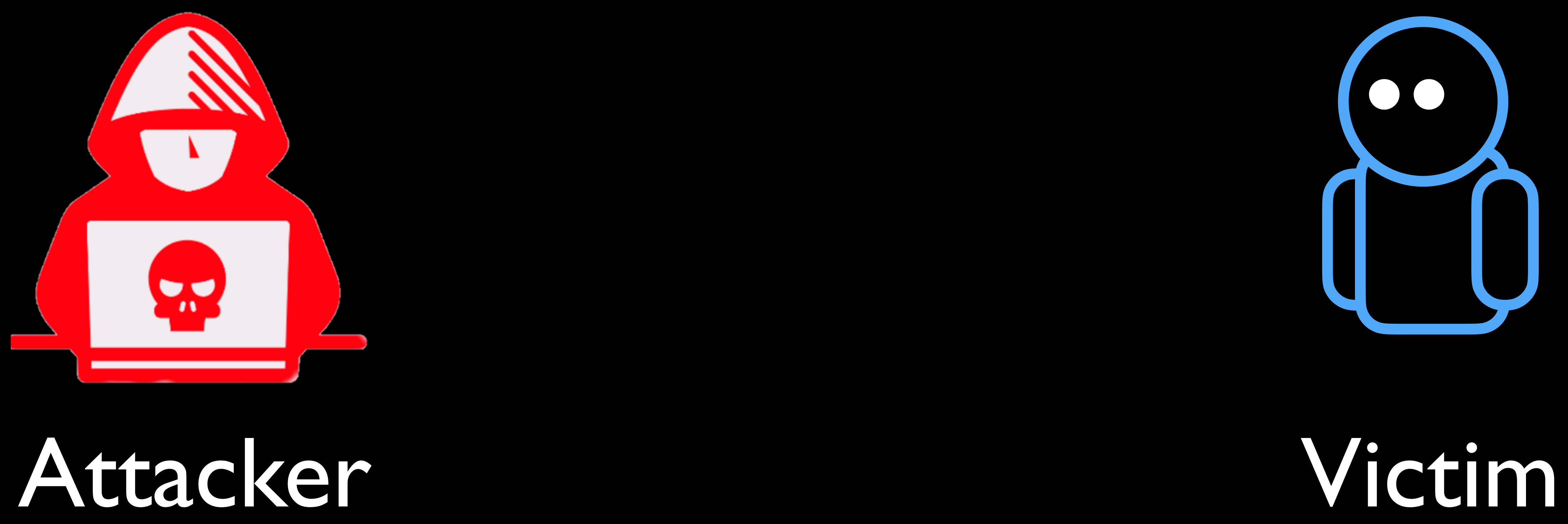
Denial of Service attacks



Attacker

Victim

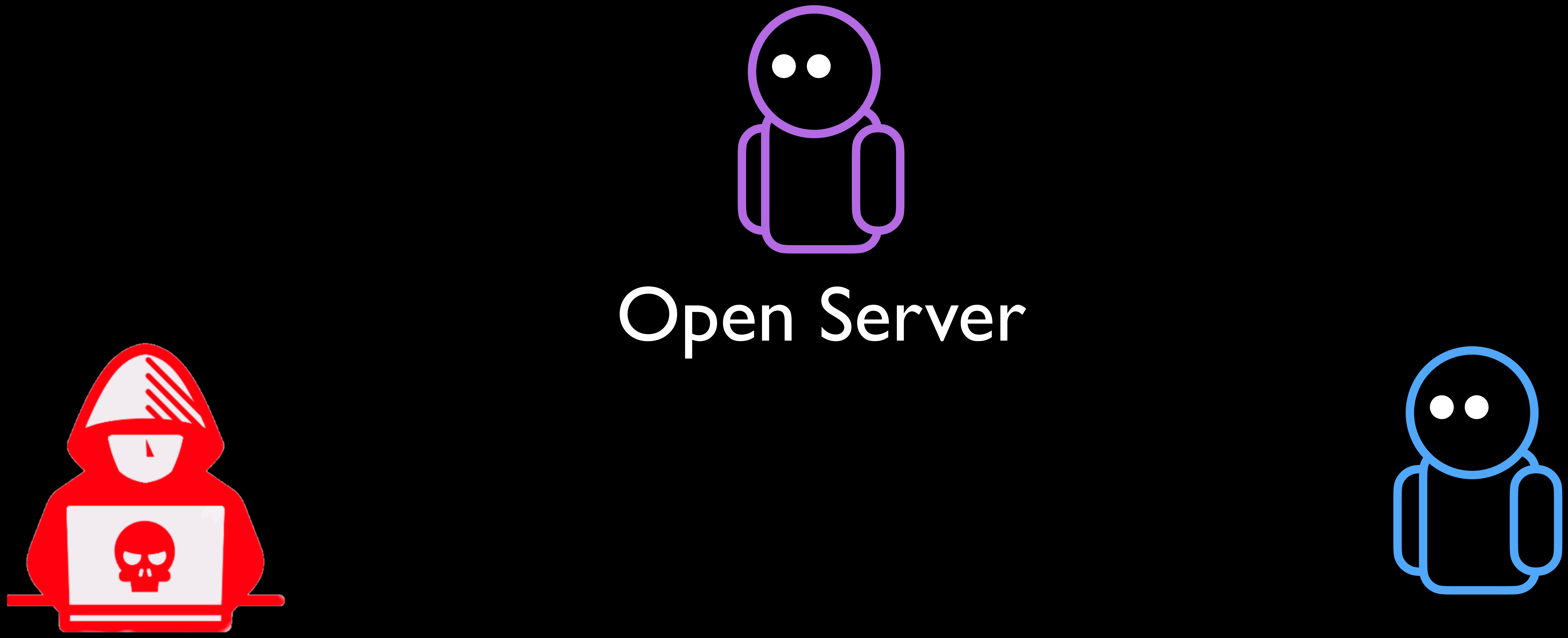
Denial of Service attacks



Attacker

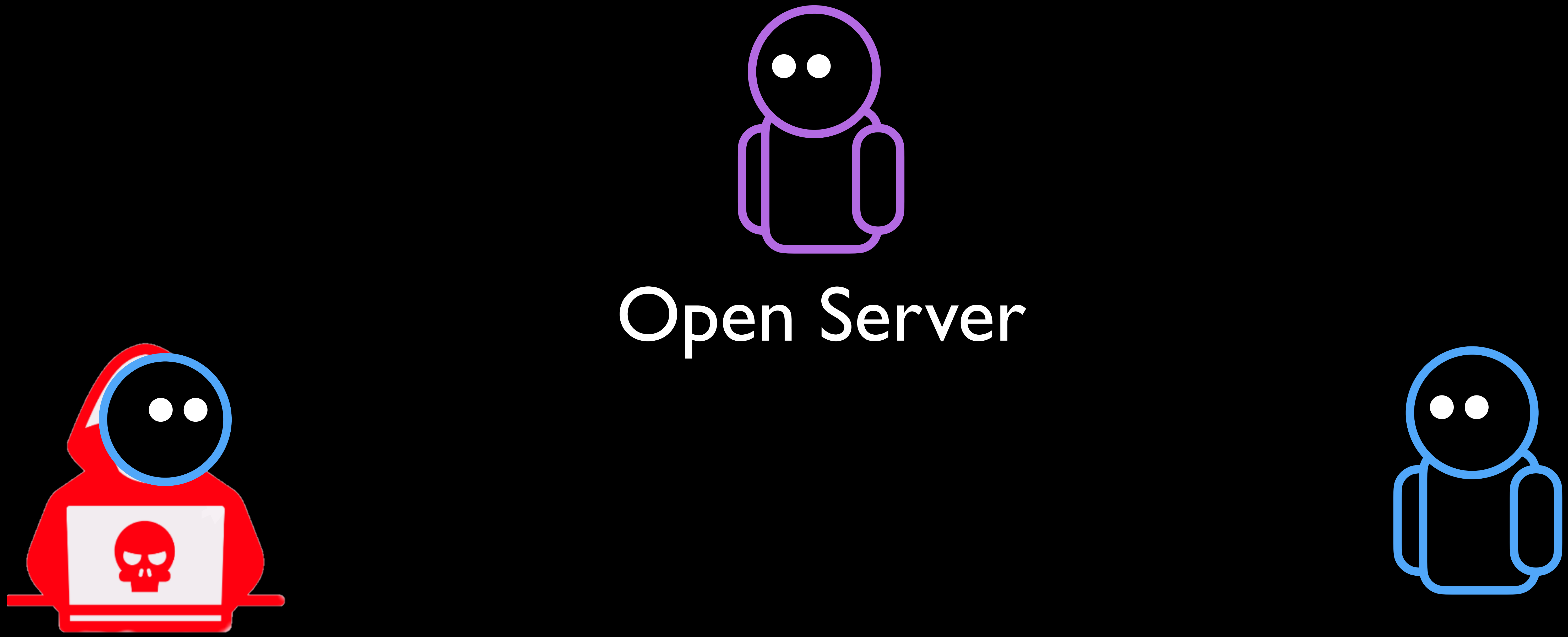
Victim

Reflected amplification attacks



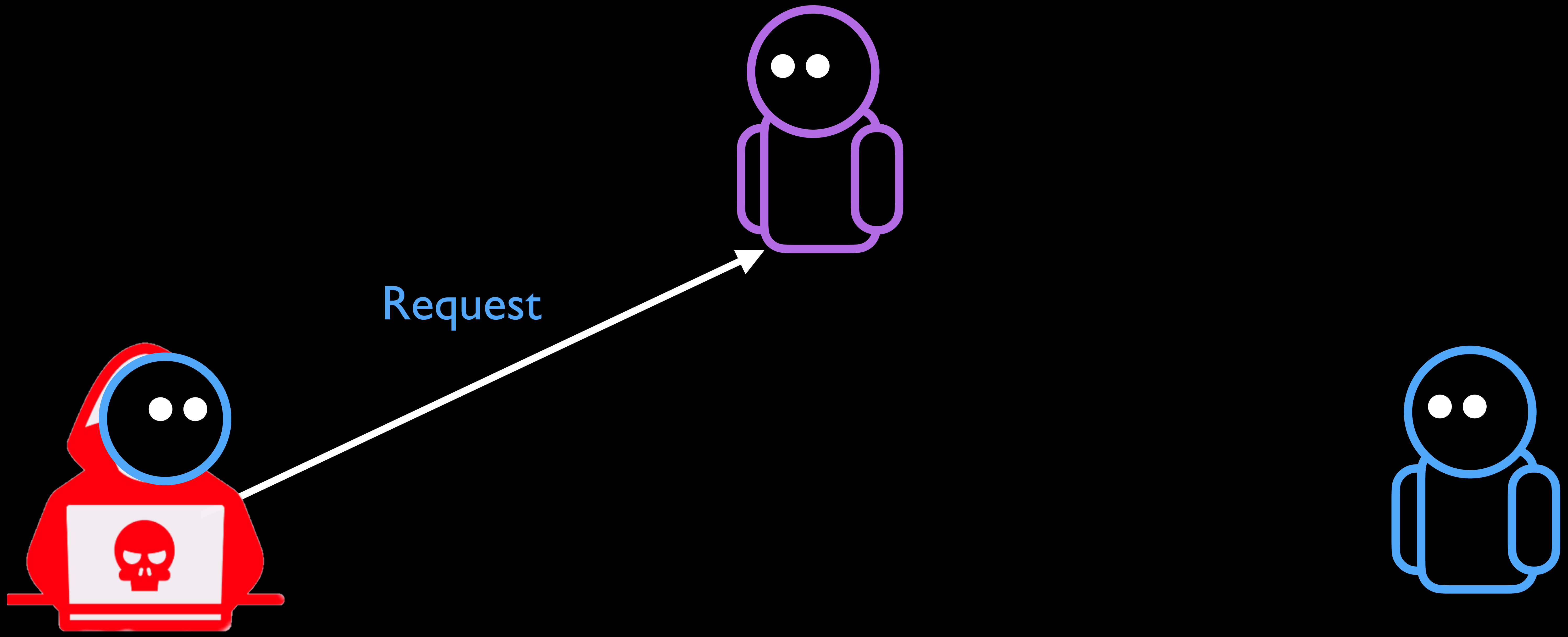
Open Server

Reflected amplification attacks

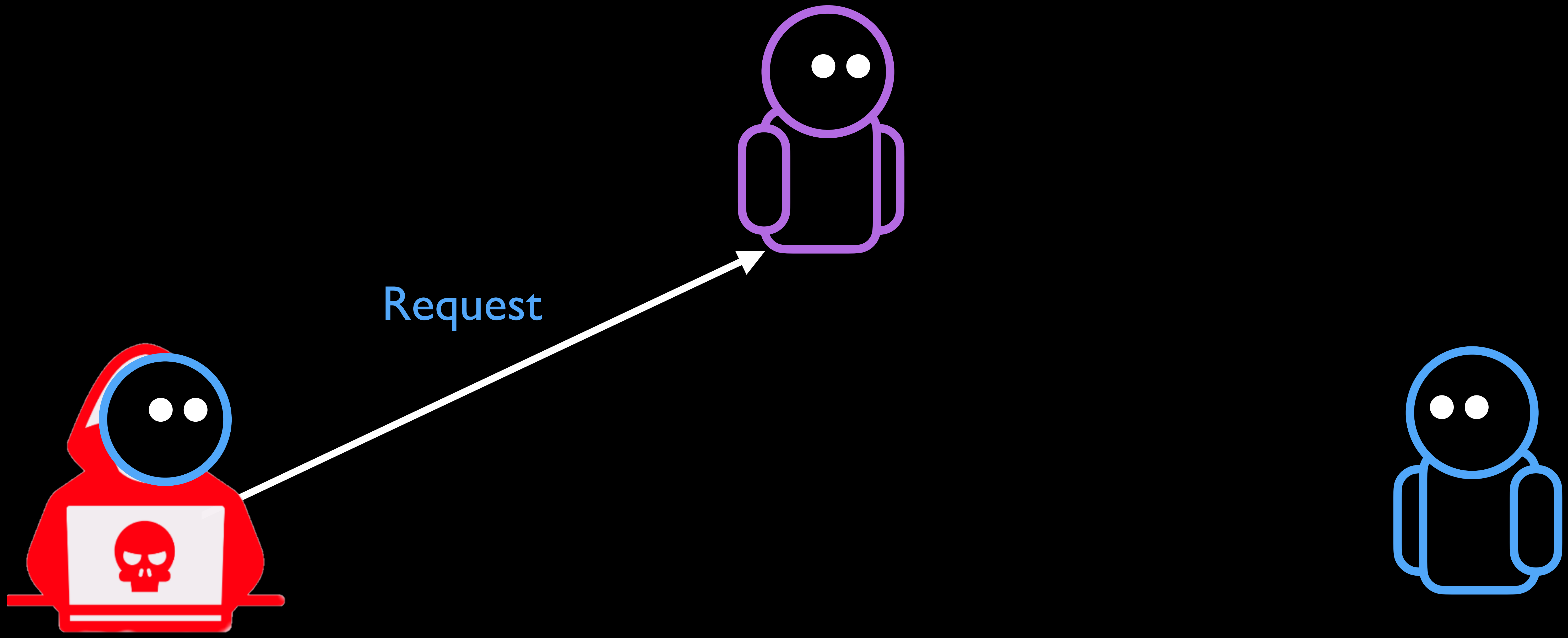


Open Server

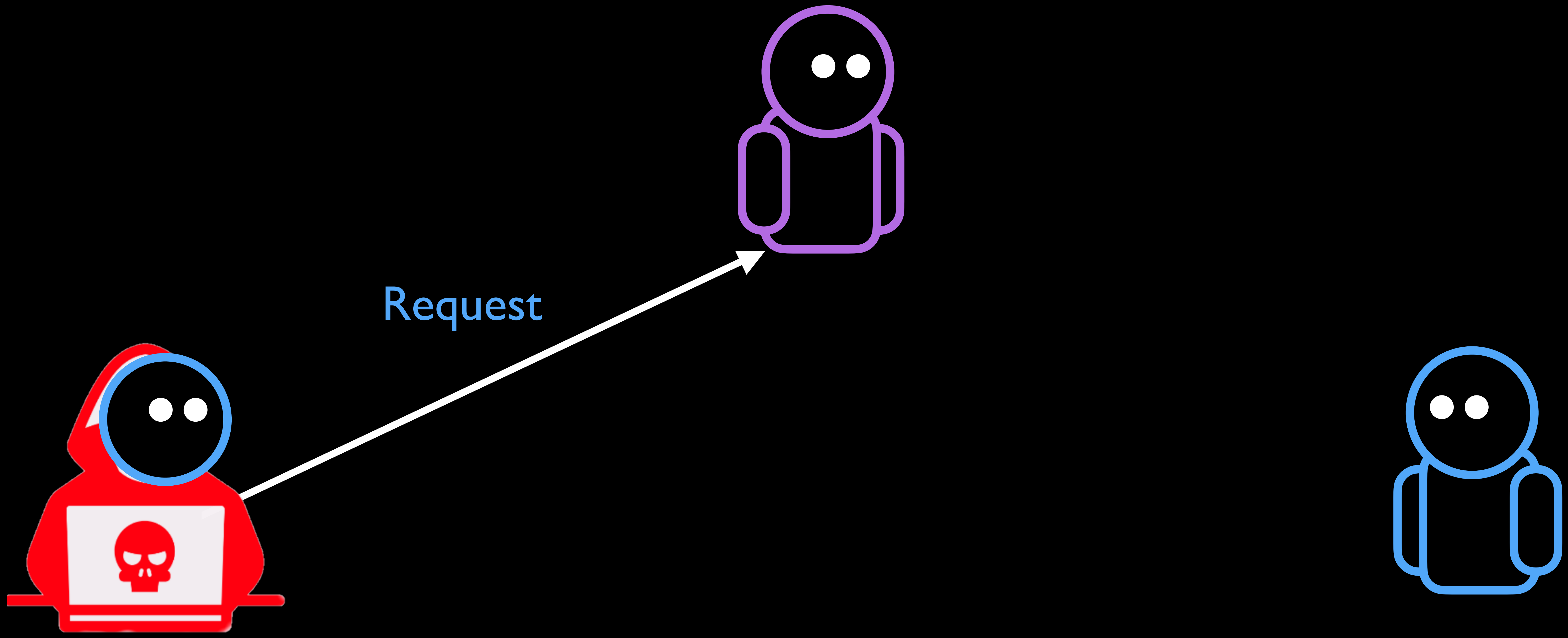
Reflected amplification attacks



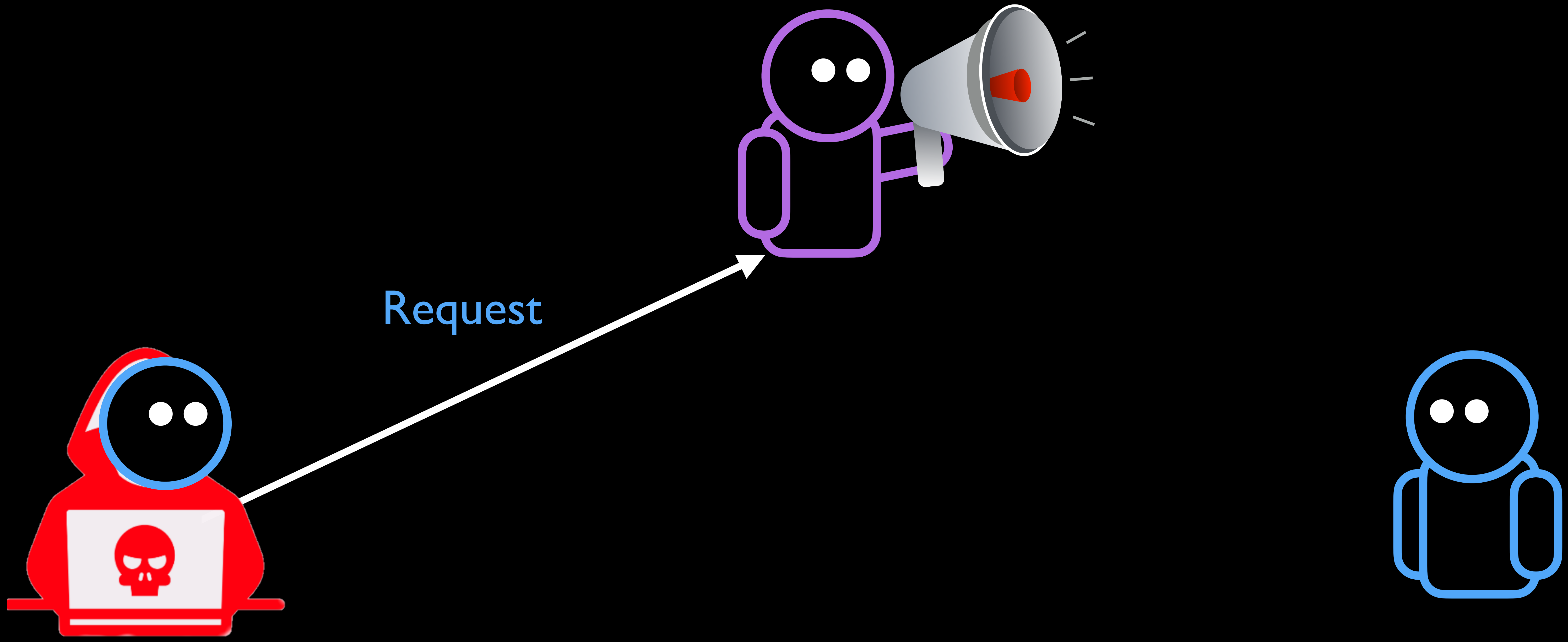
Reflected amplification attacks



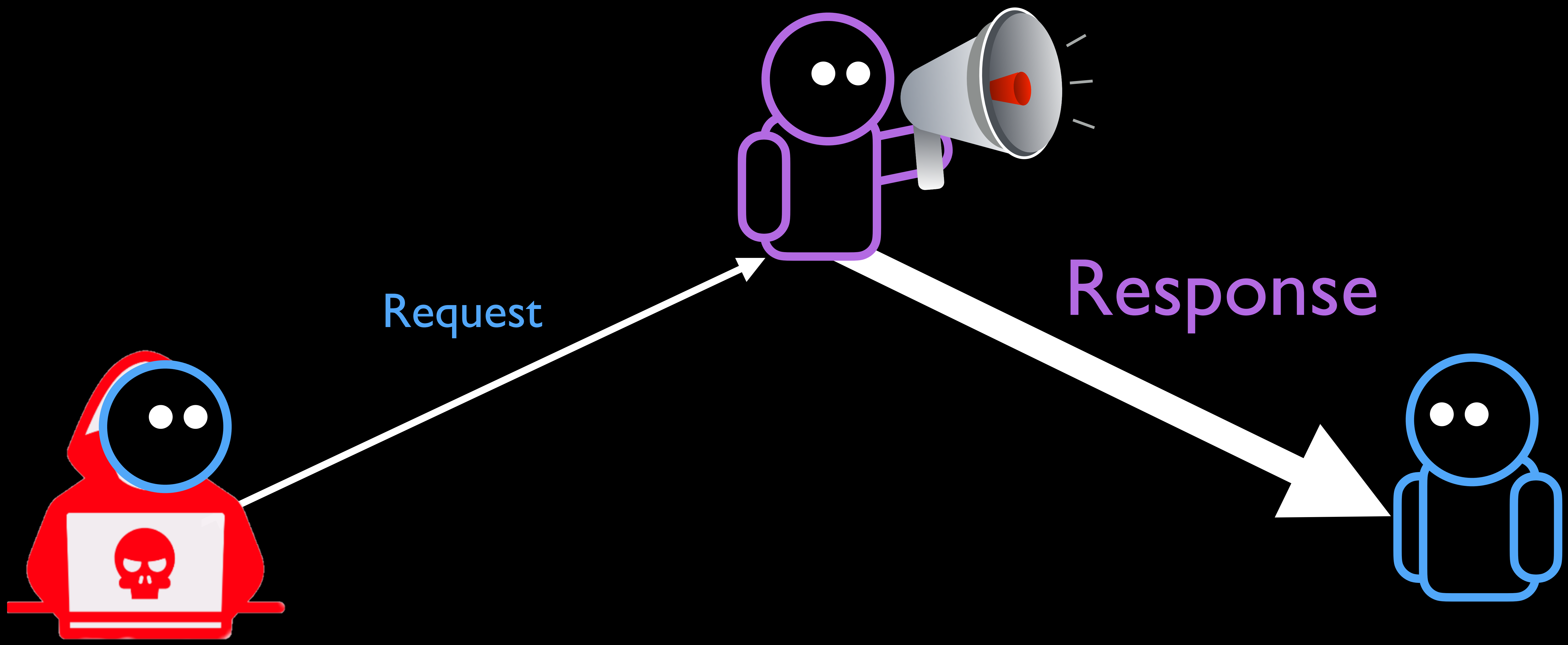
Reflected amplification attacks



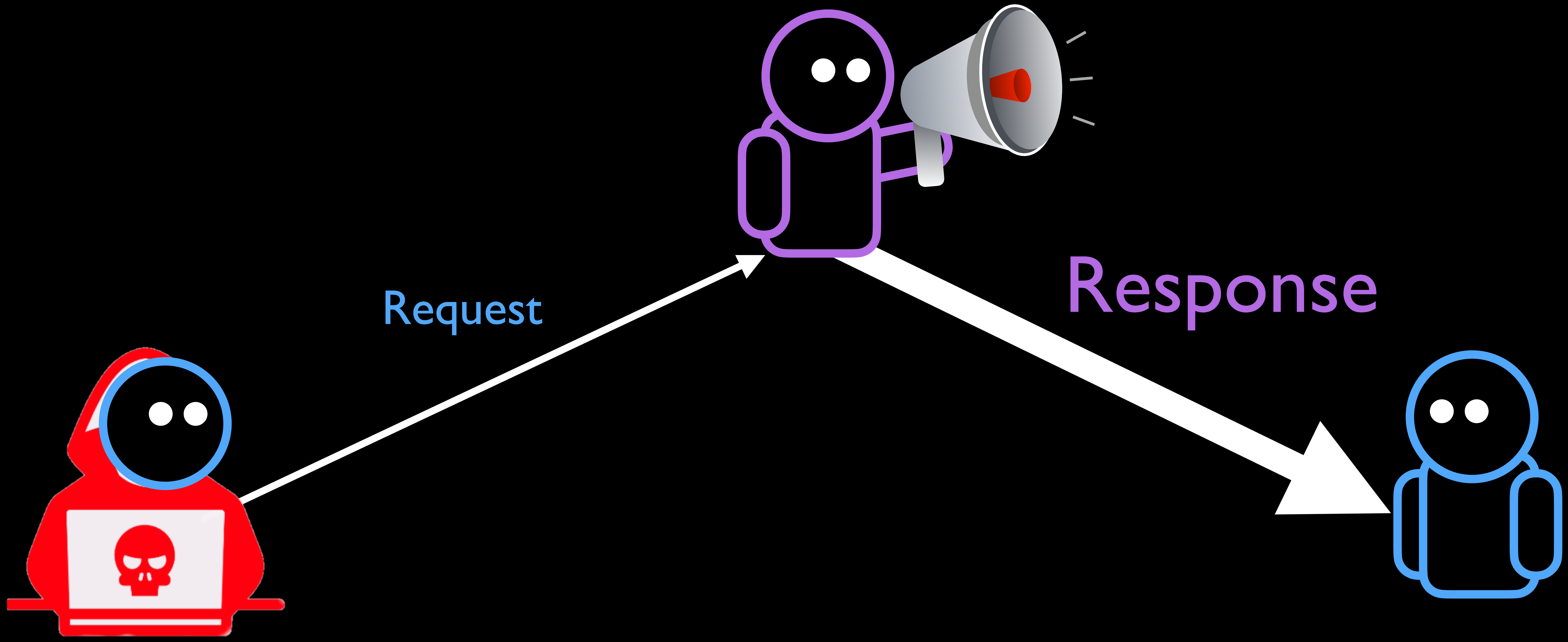
Reflected amplification attacks



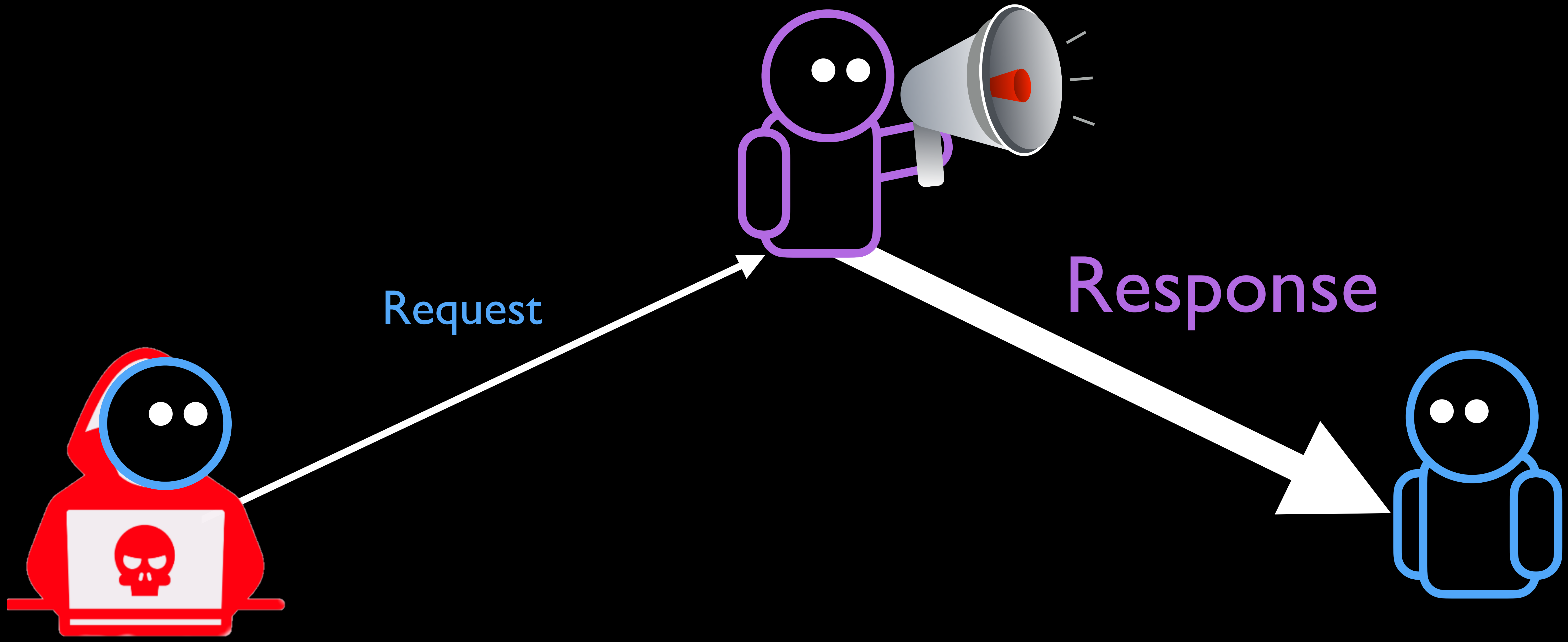
Reflected amplification attacks



Reflected amplification attacks

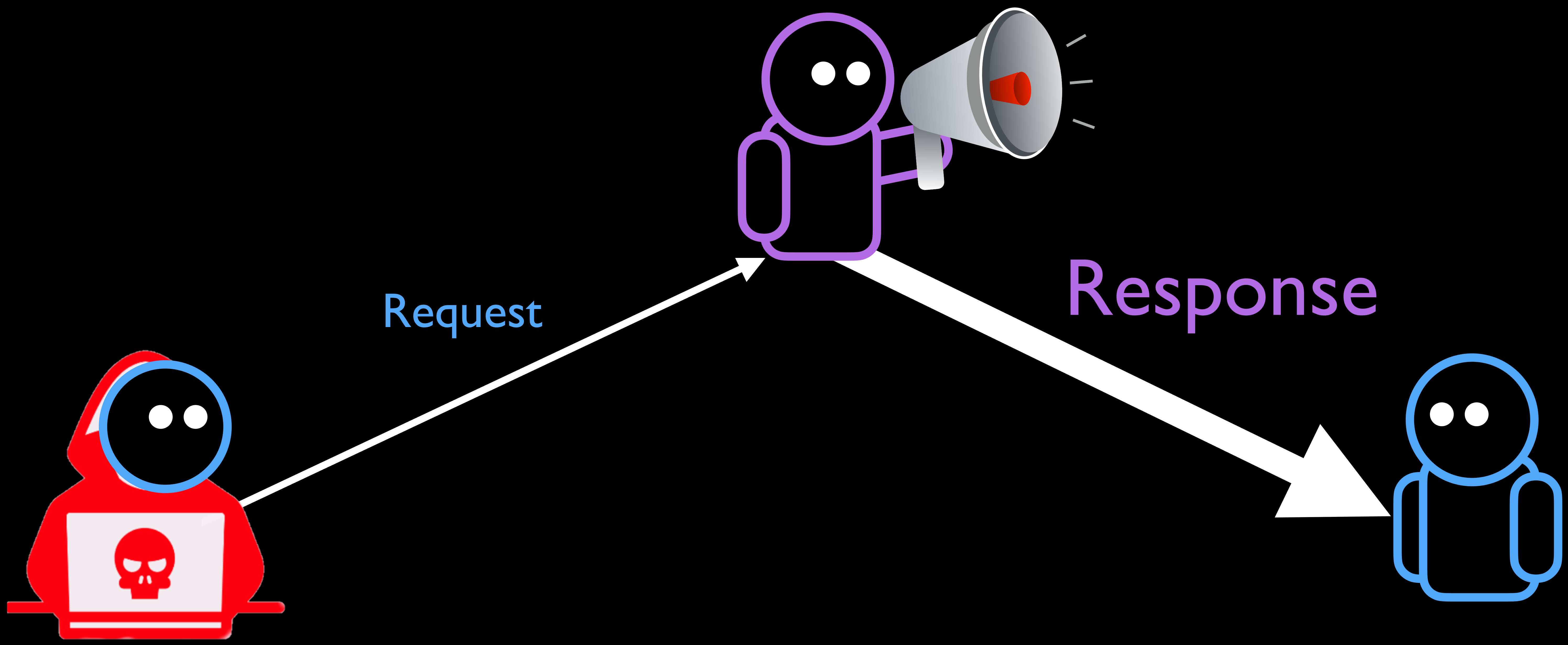


Reflected amplification attacks



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

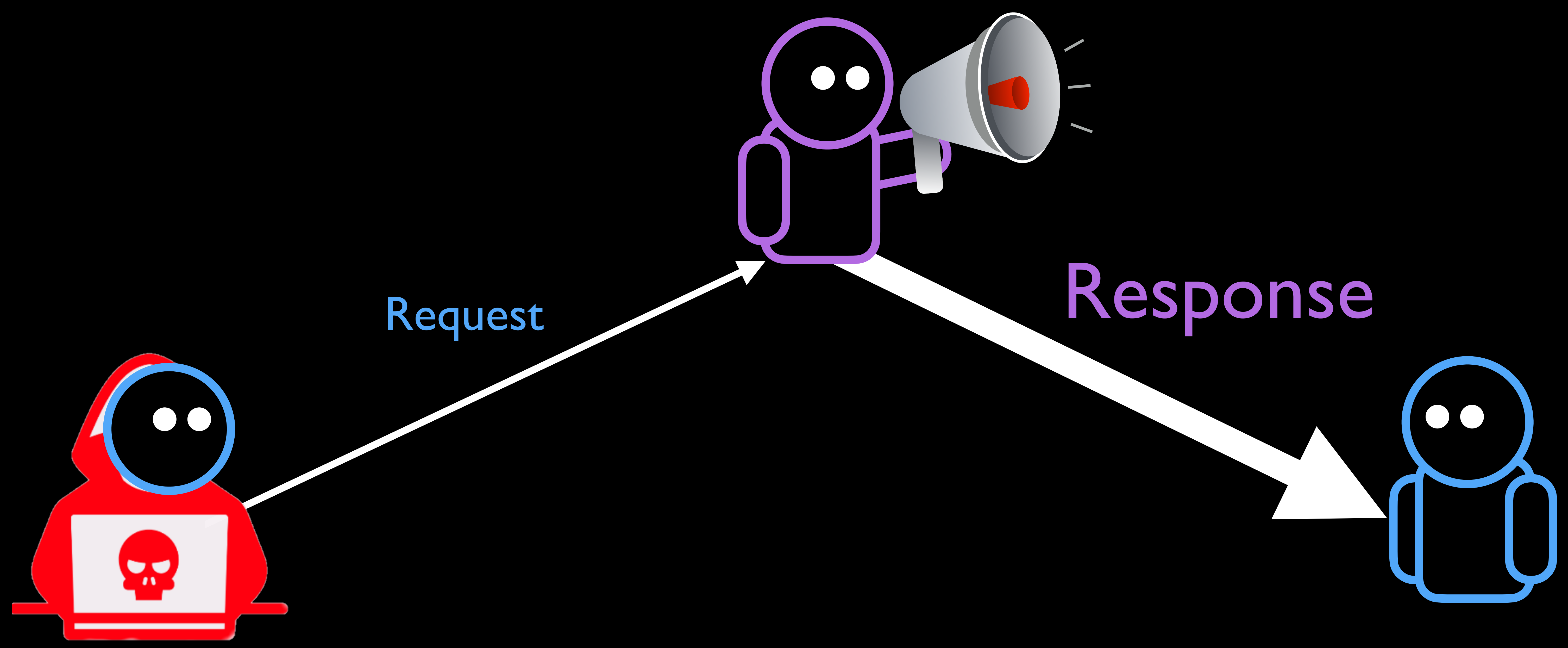
Reflected amplification attacks



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

54x	DNS
556.9x	NTP
51,000x	memcached

Reflected amplification attacks

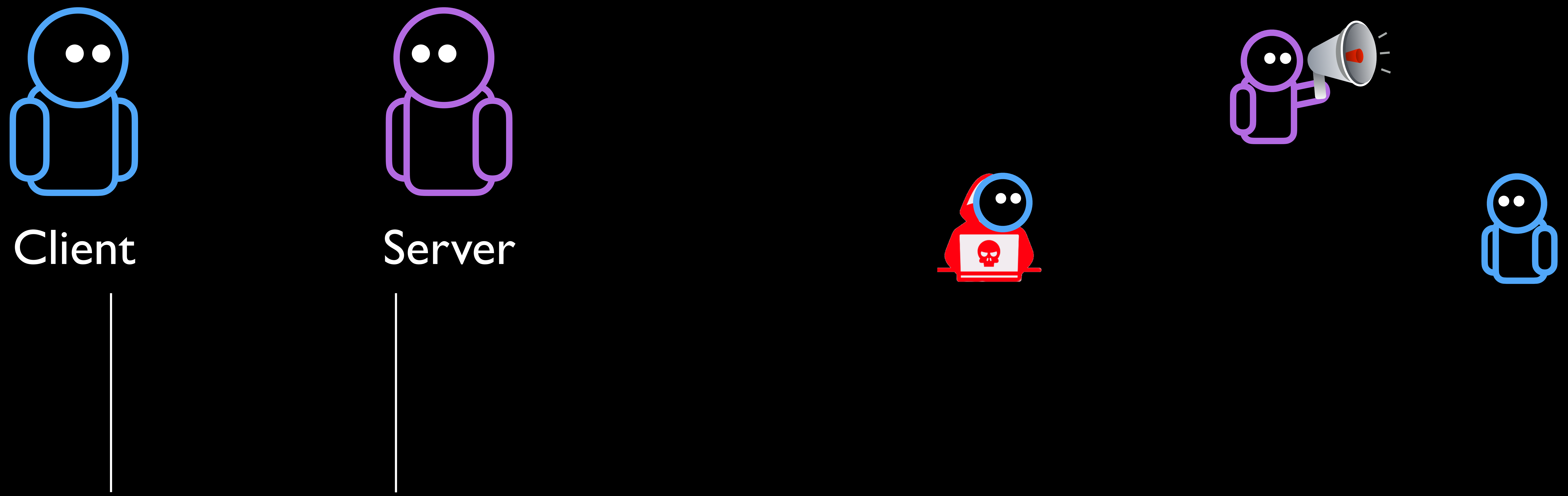


54x	DNS
556.9x	NTP
51,000x	memcached

Almost all prior reflected amplification attacks use UDP

Reflected amplification attacks

UDP is connection-less

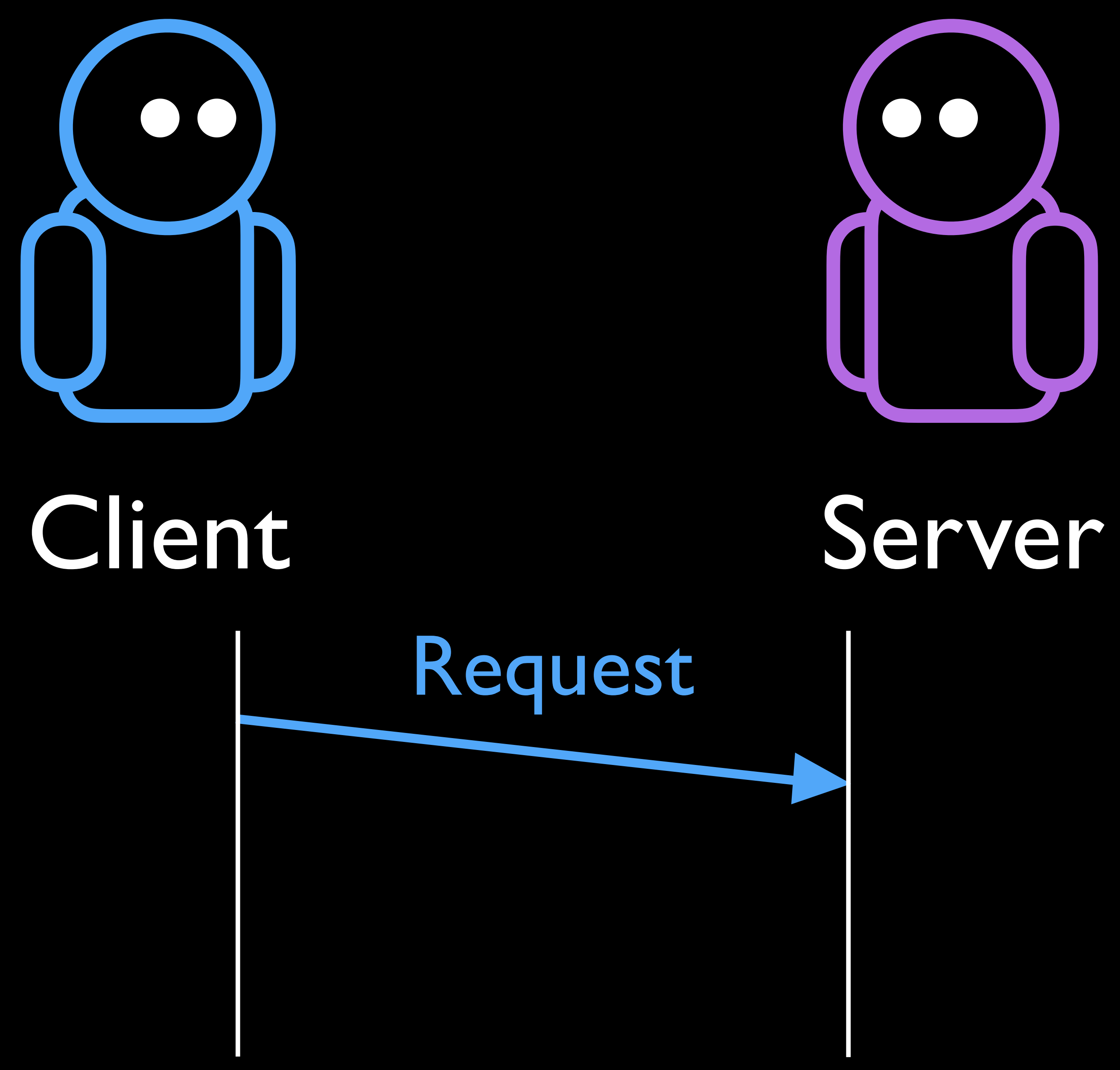


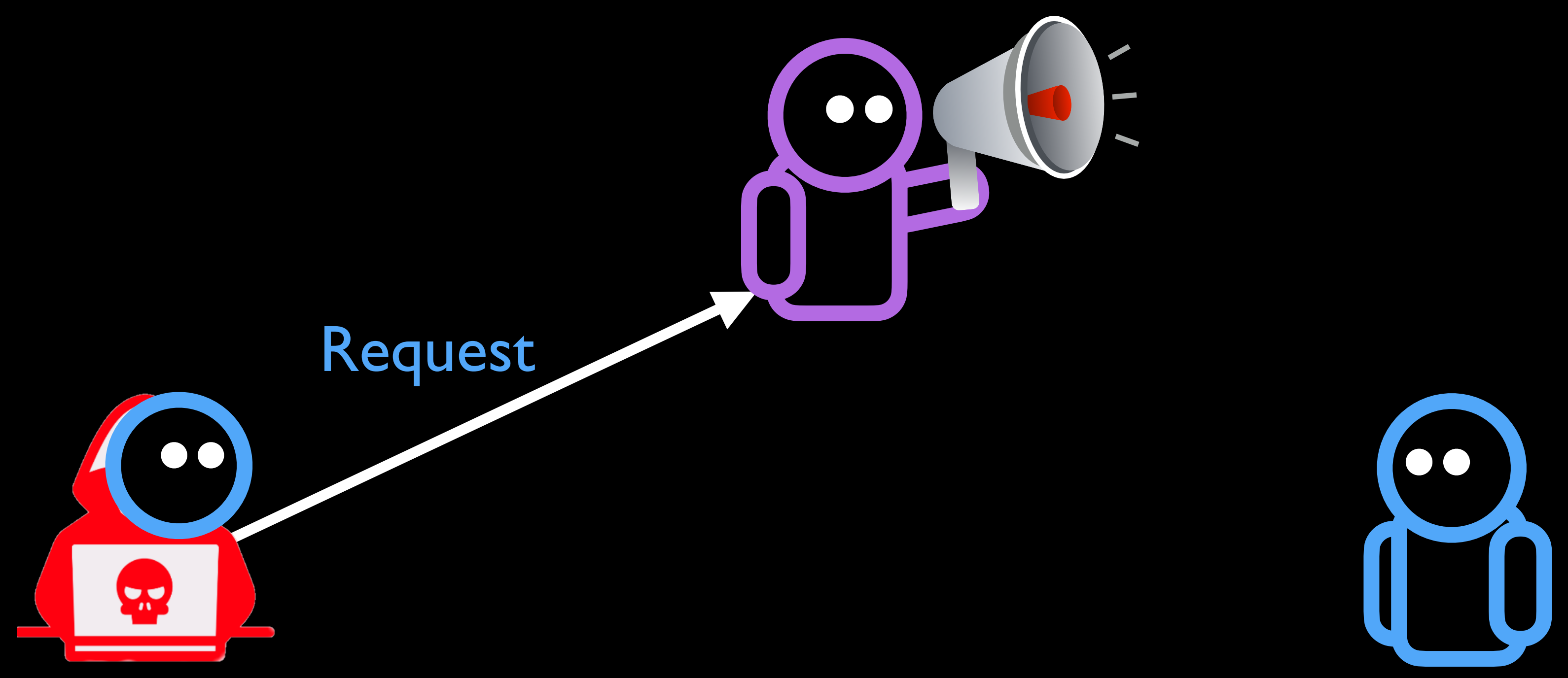
Client

Server

Reflected amplification attacks

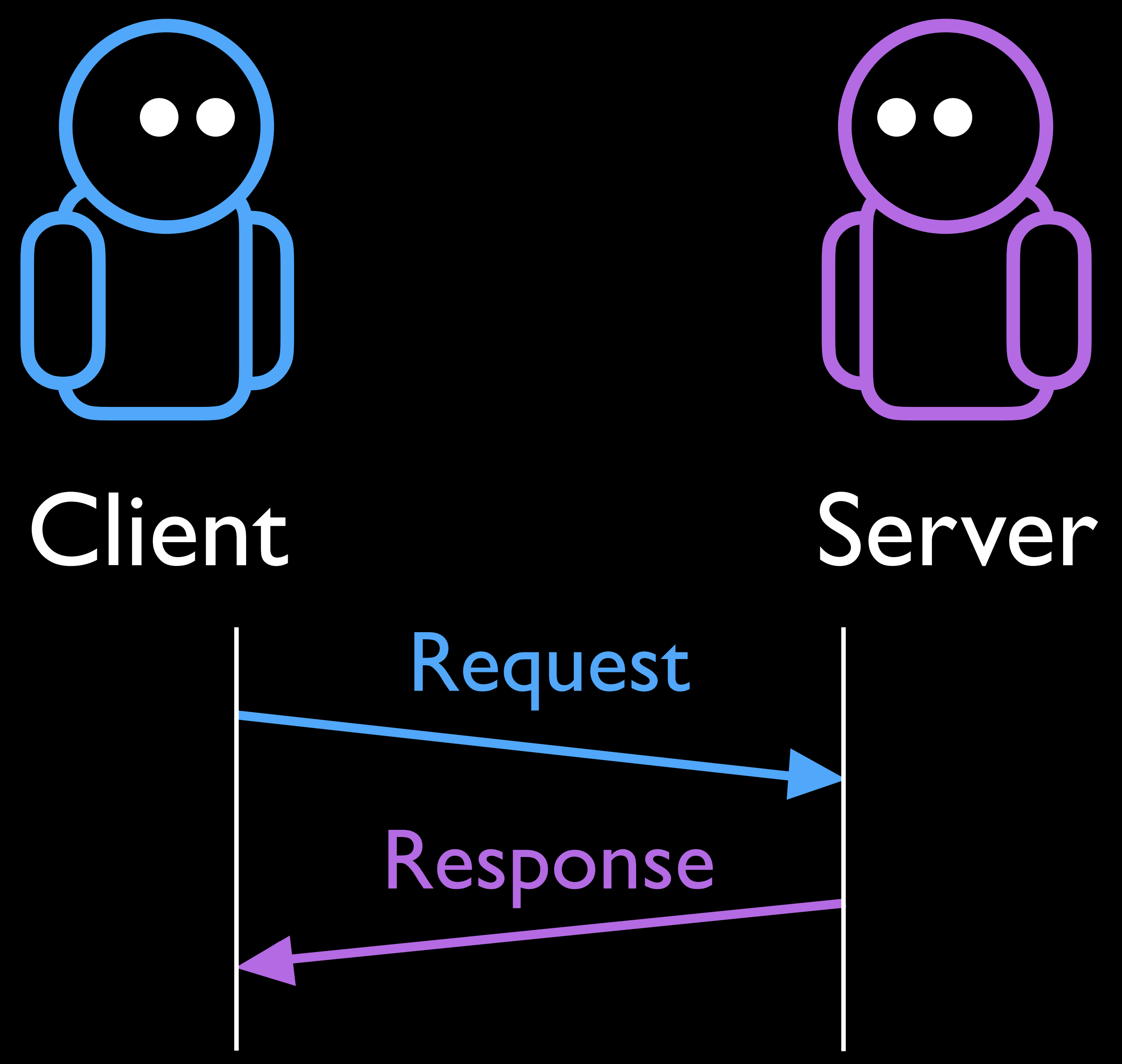
UDP is connection-less

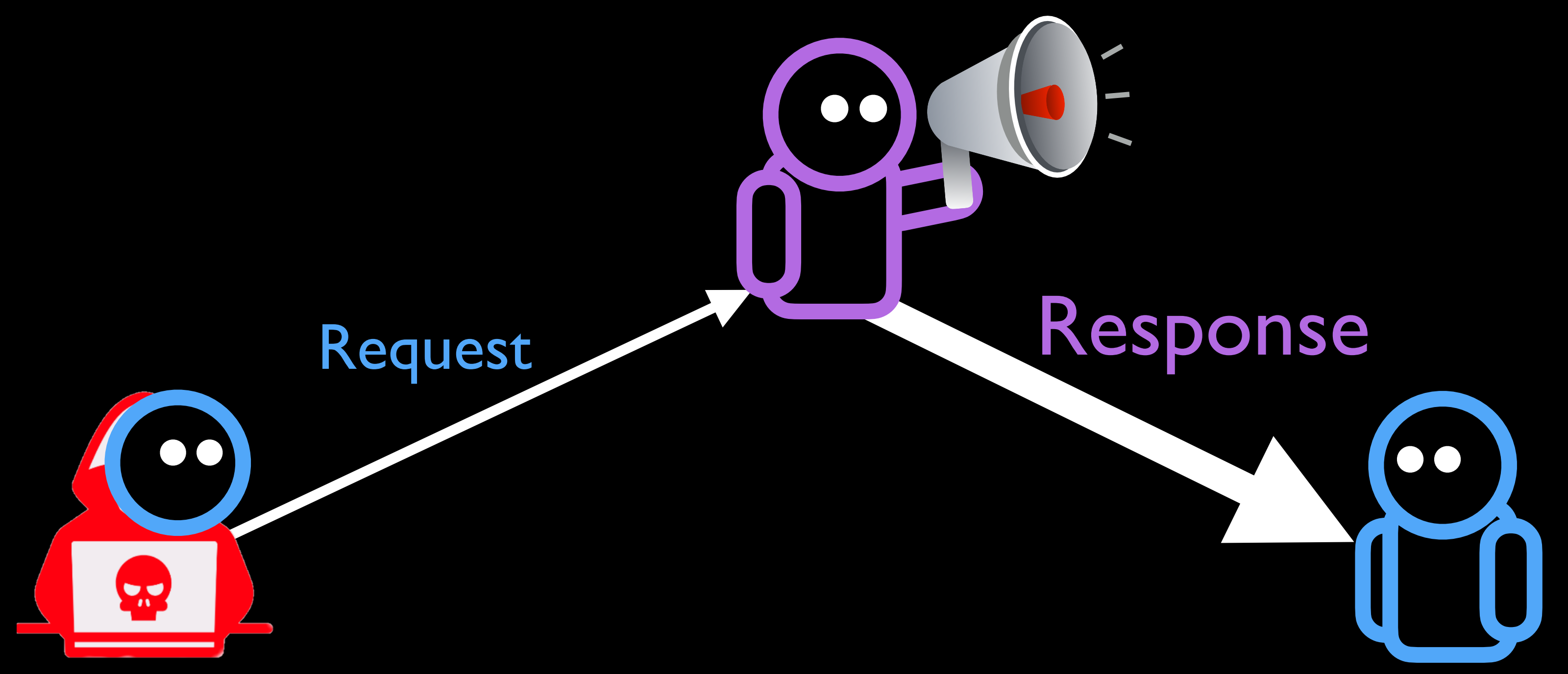




Reflected amplification attacks

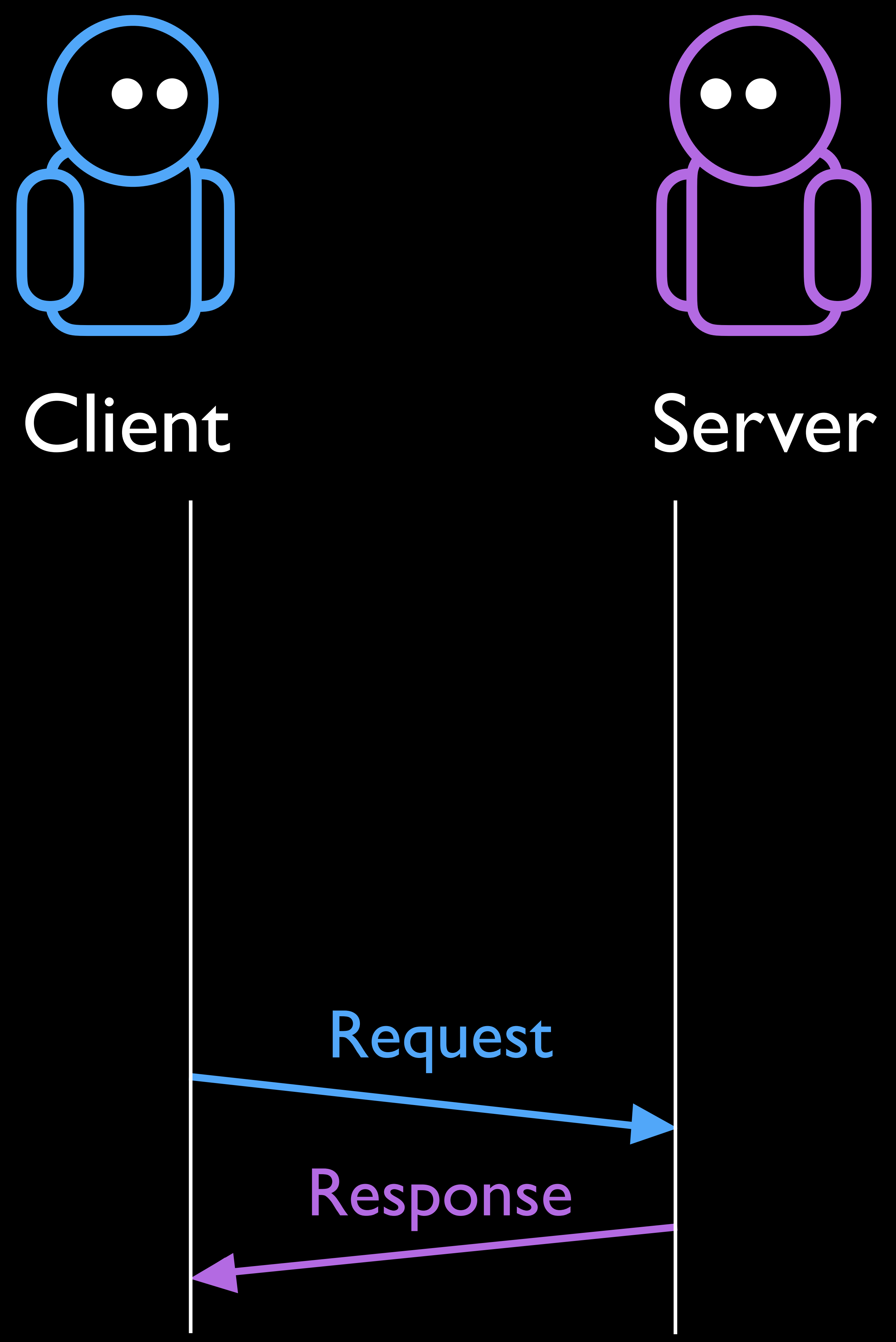
UDP is connection-less

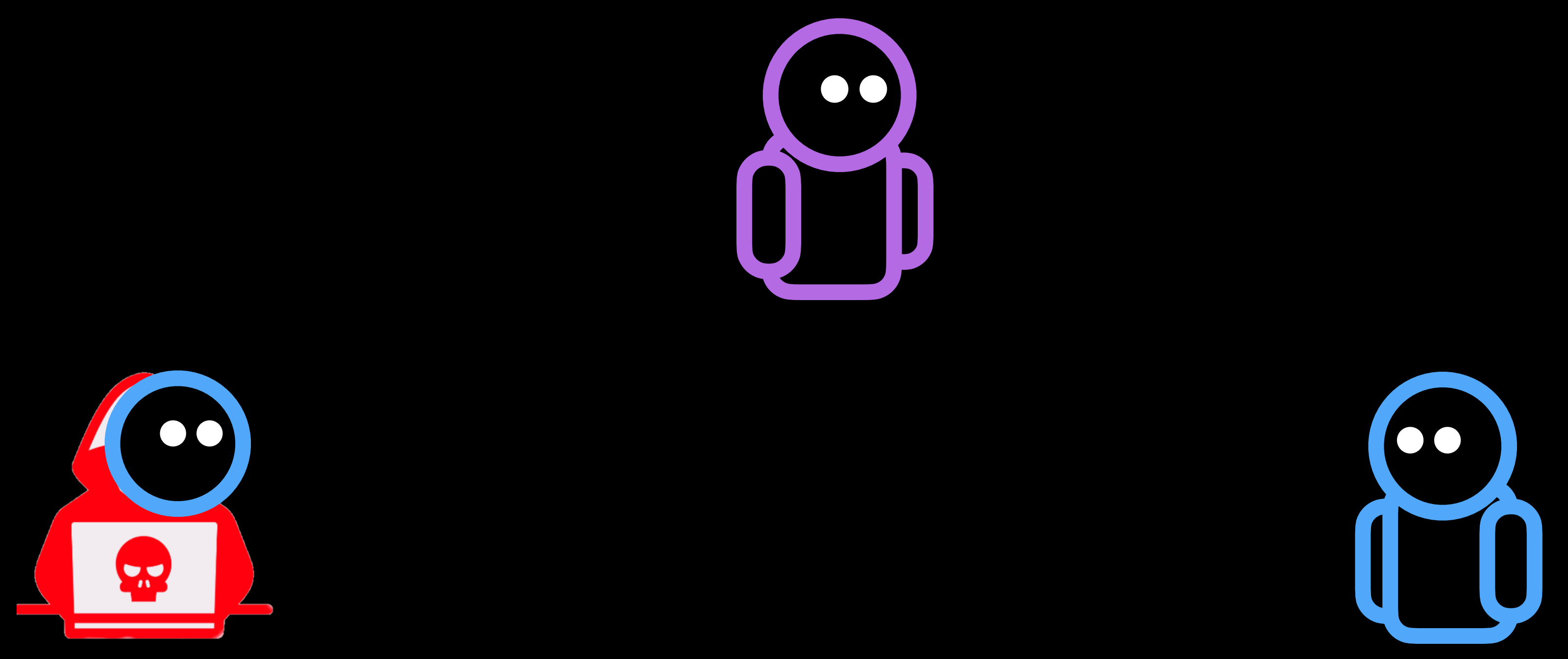




Reflected amplification attacks

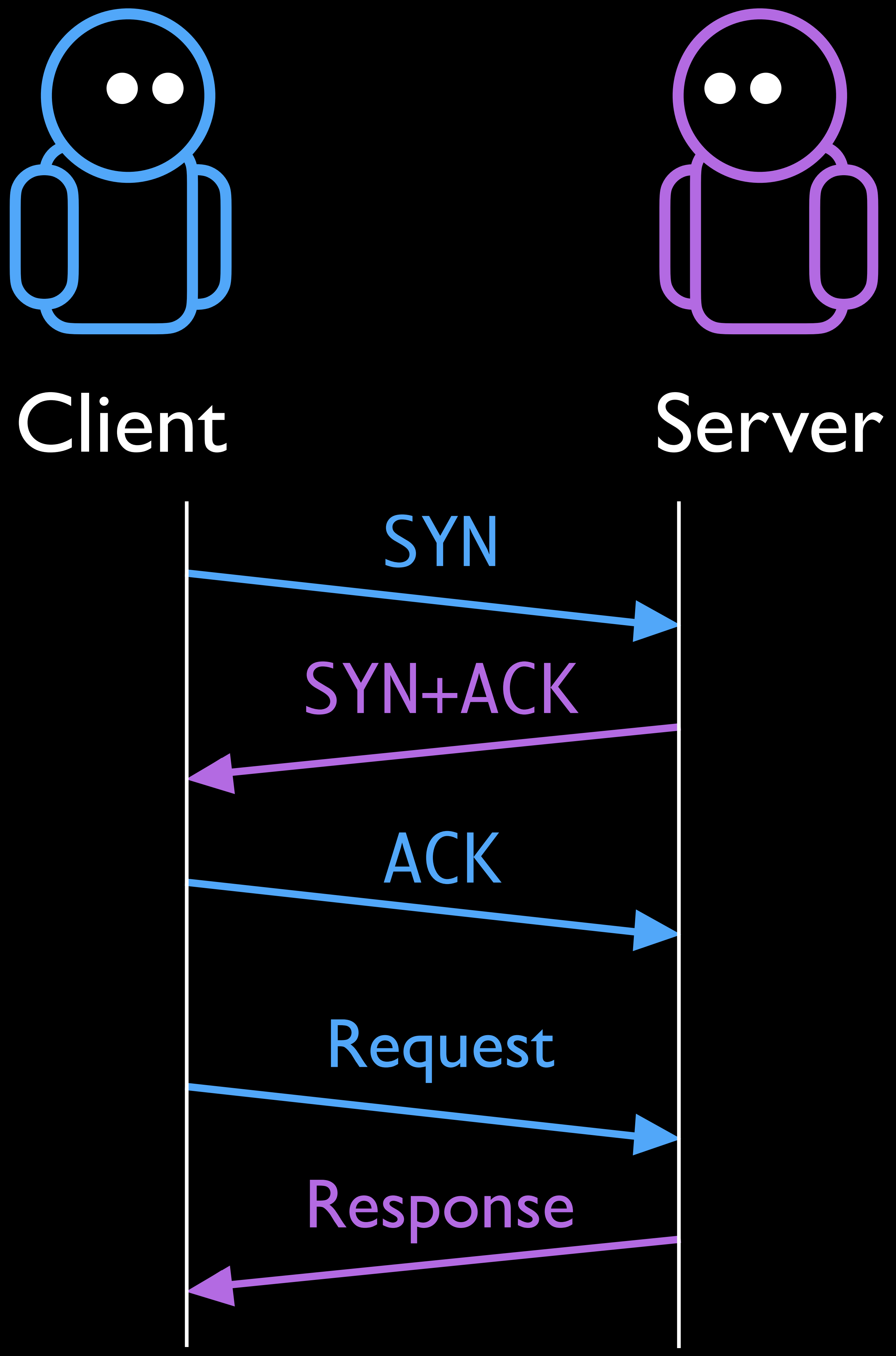
TCP requires a threeway handshake

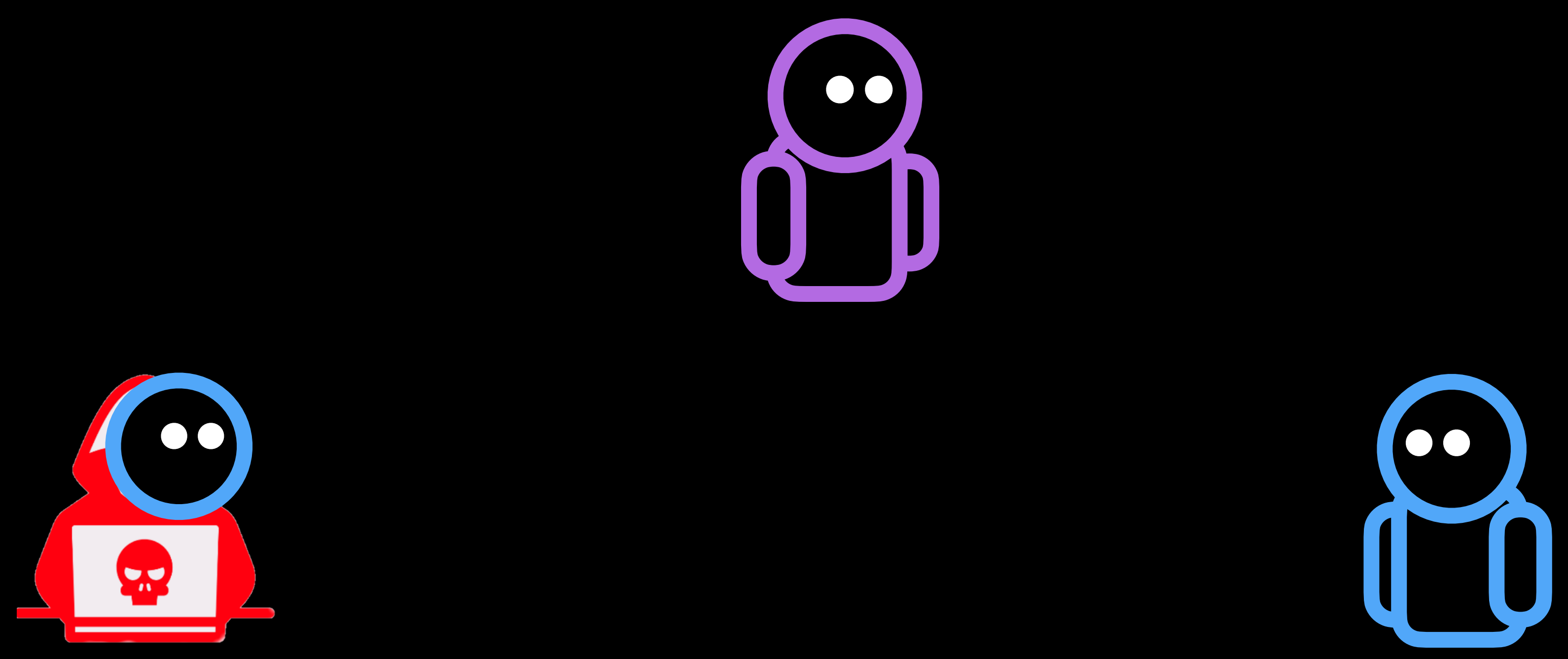




Reflected amplification attacks

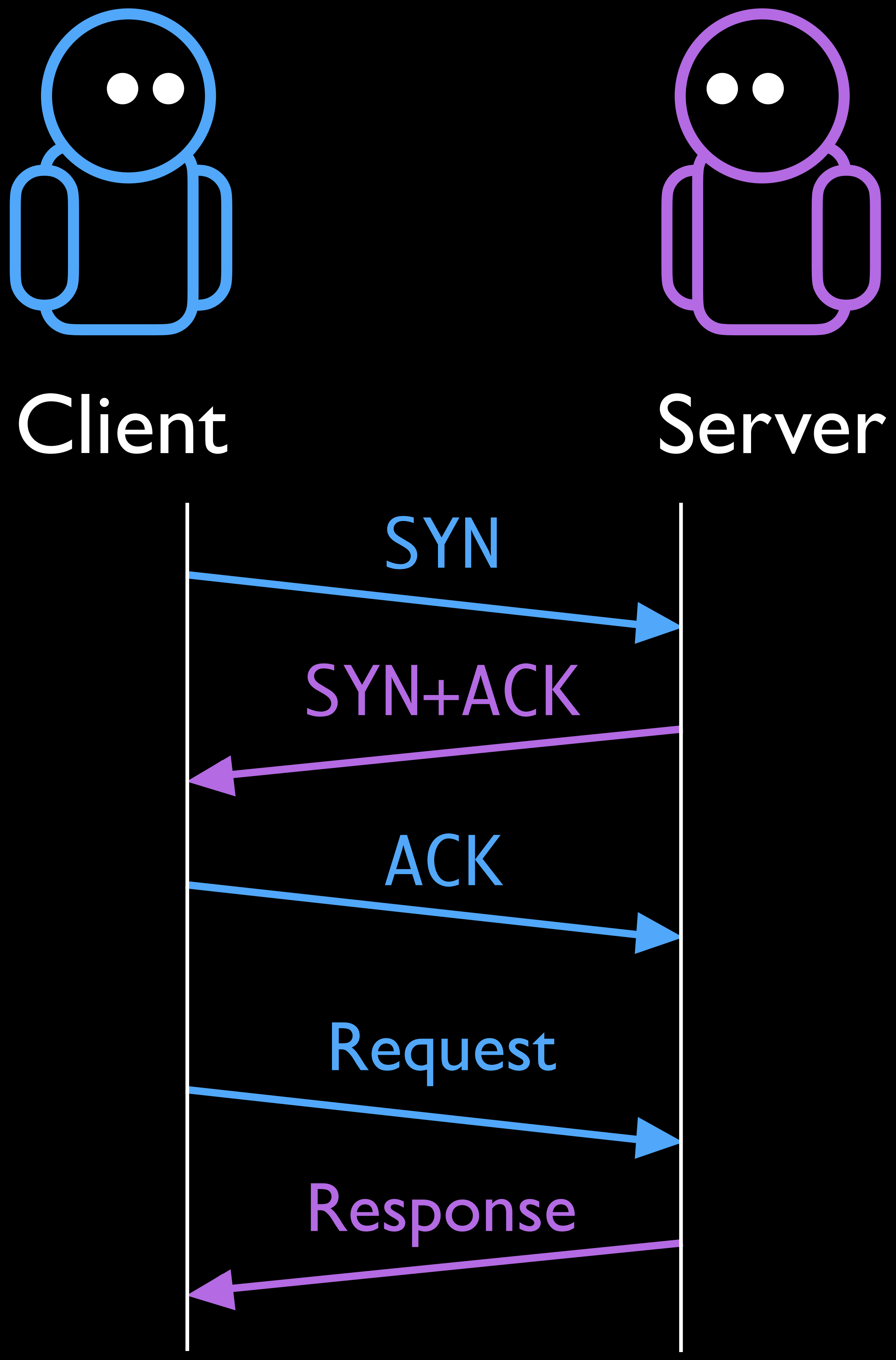
TCP requires a threeway handshake

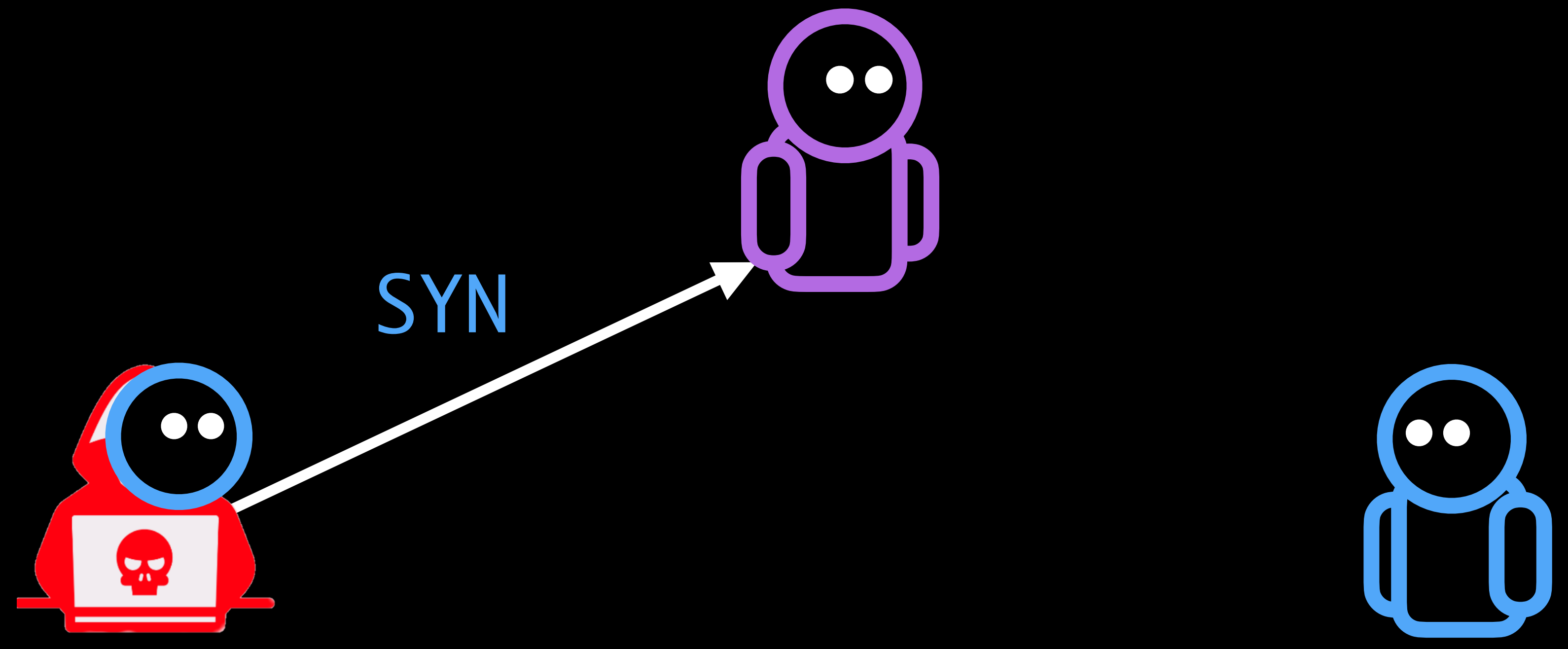




Reflected amplification attacks

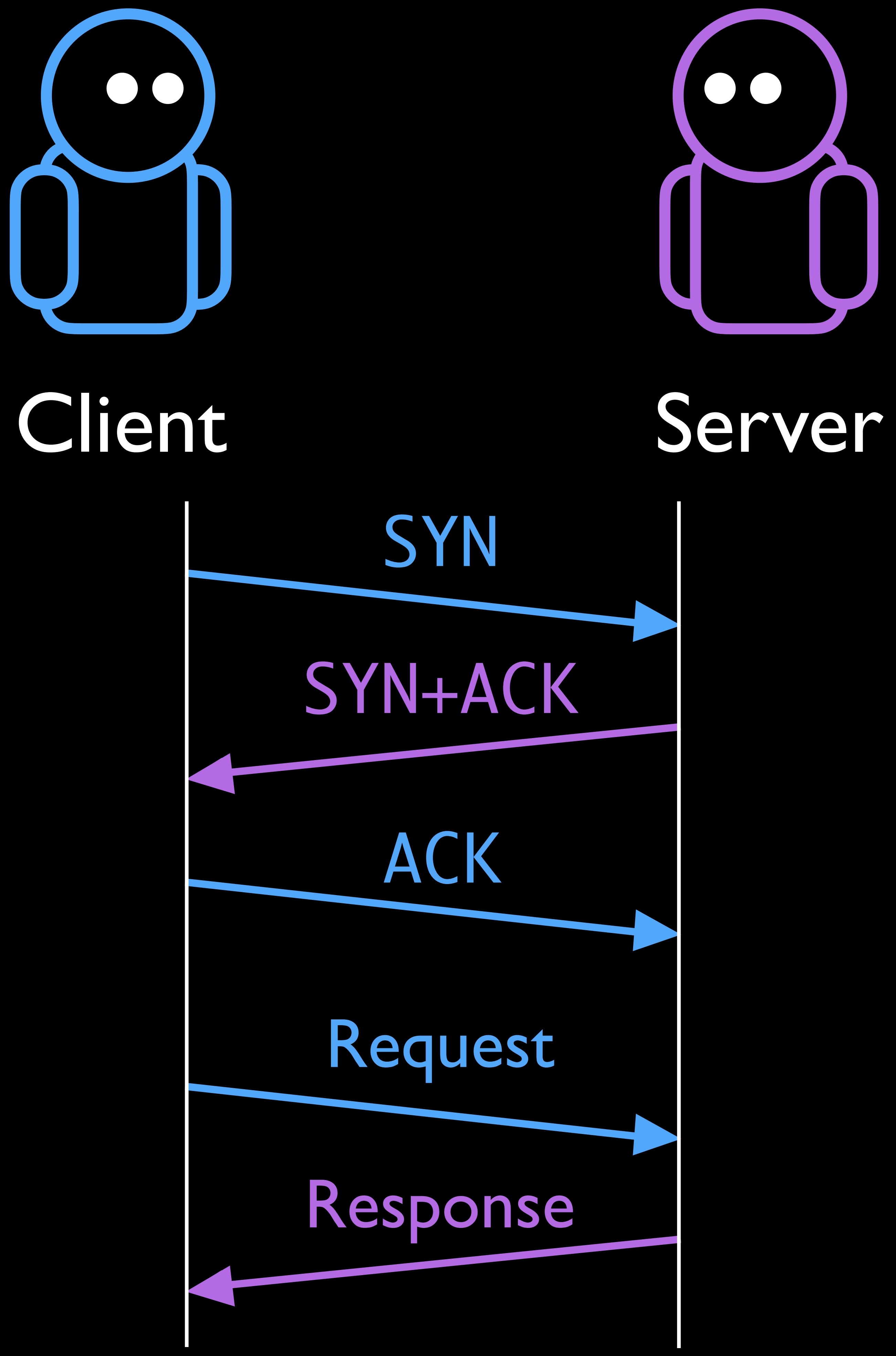
TCP requires a threeway handshake

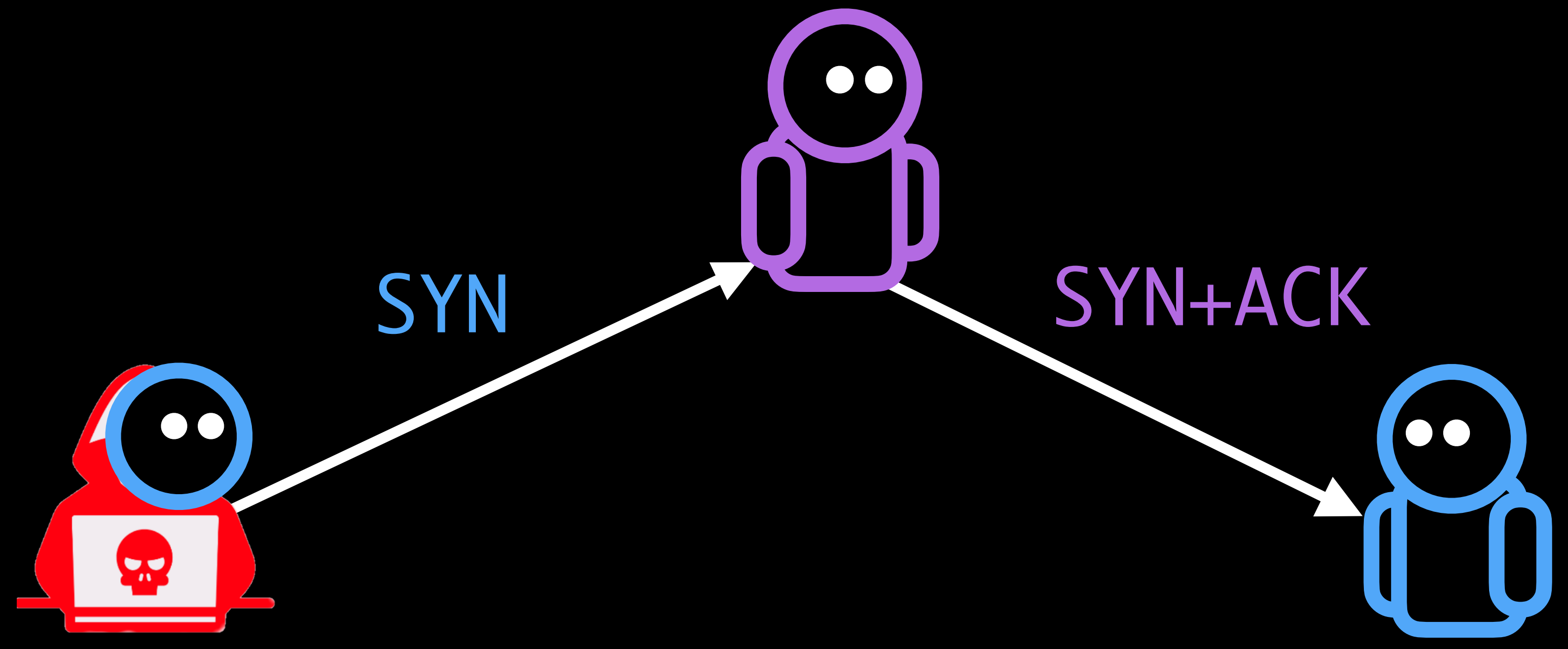




Reflected amplification attacks

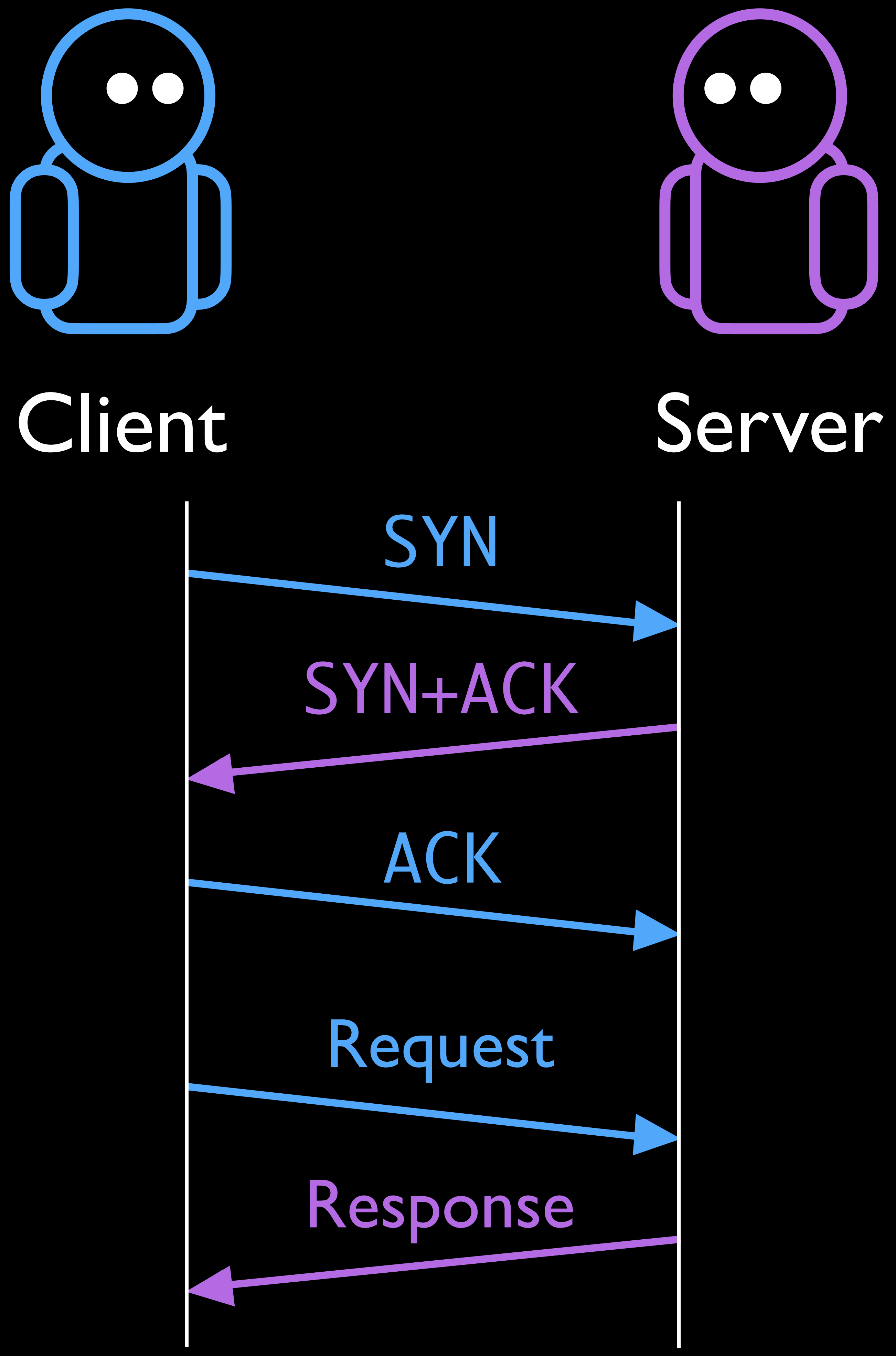
TCP requires a threeway handshake

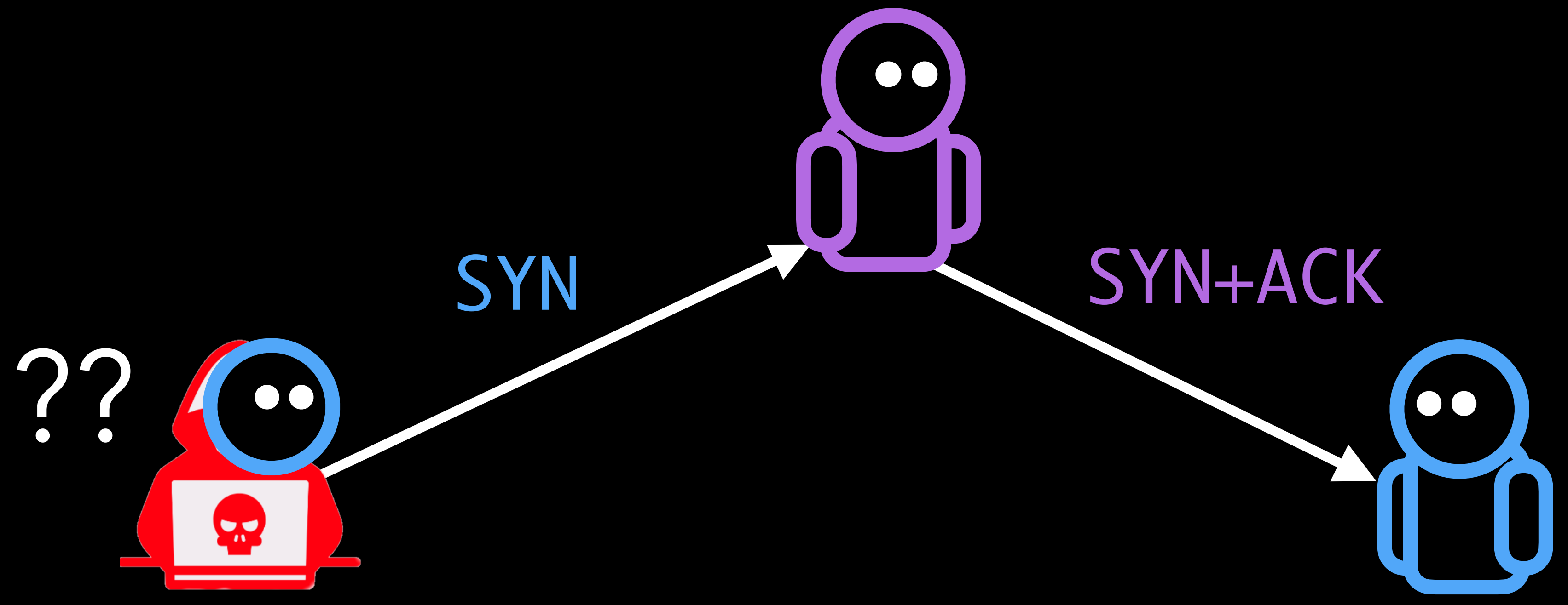




Reflected amplification attacks

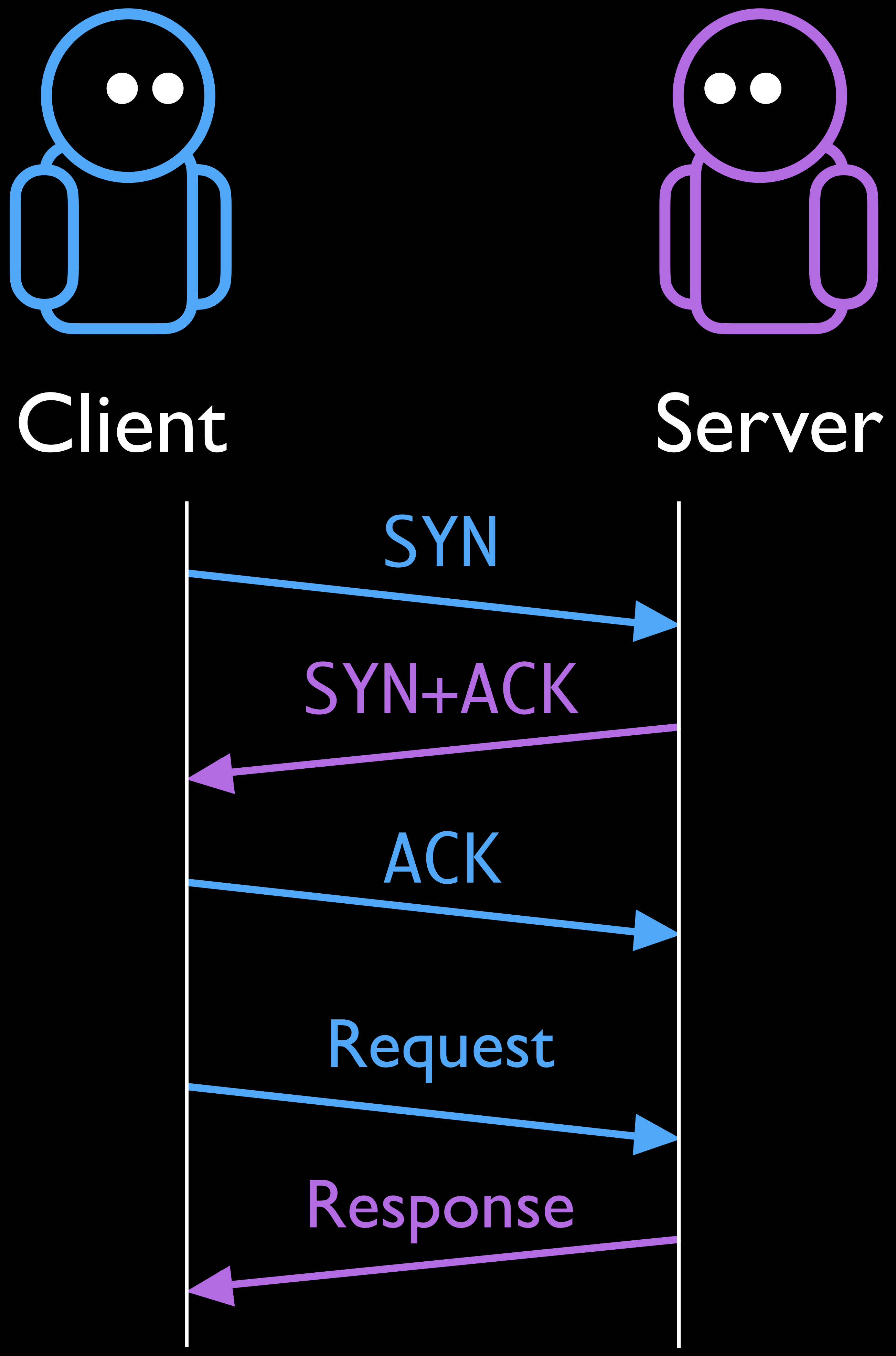
TCP requires a threeway handshake

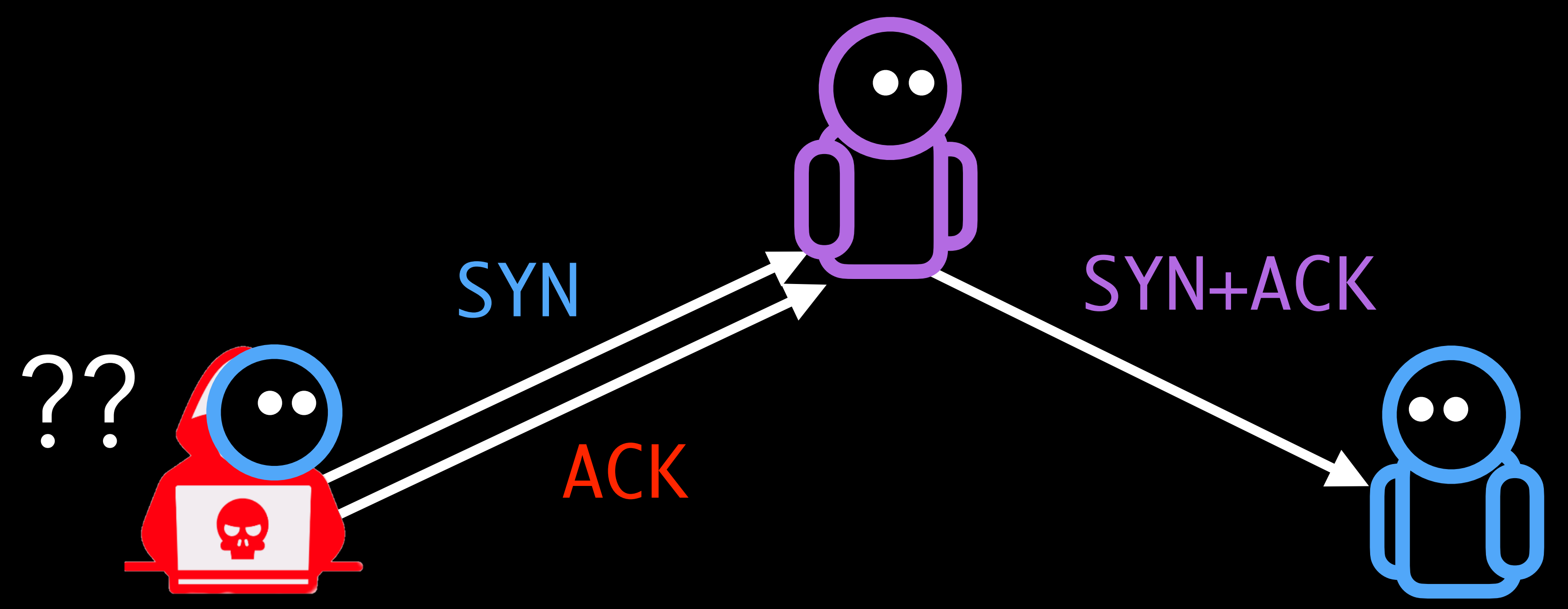




Reflected amplification attacks

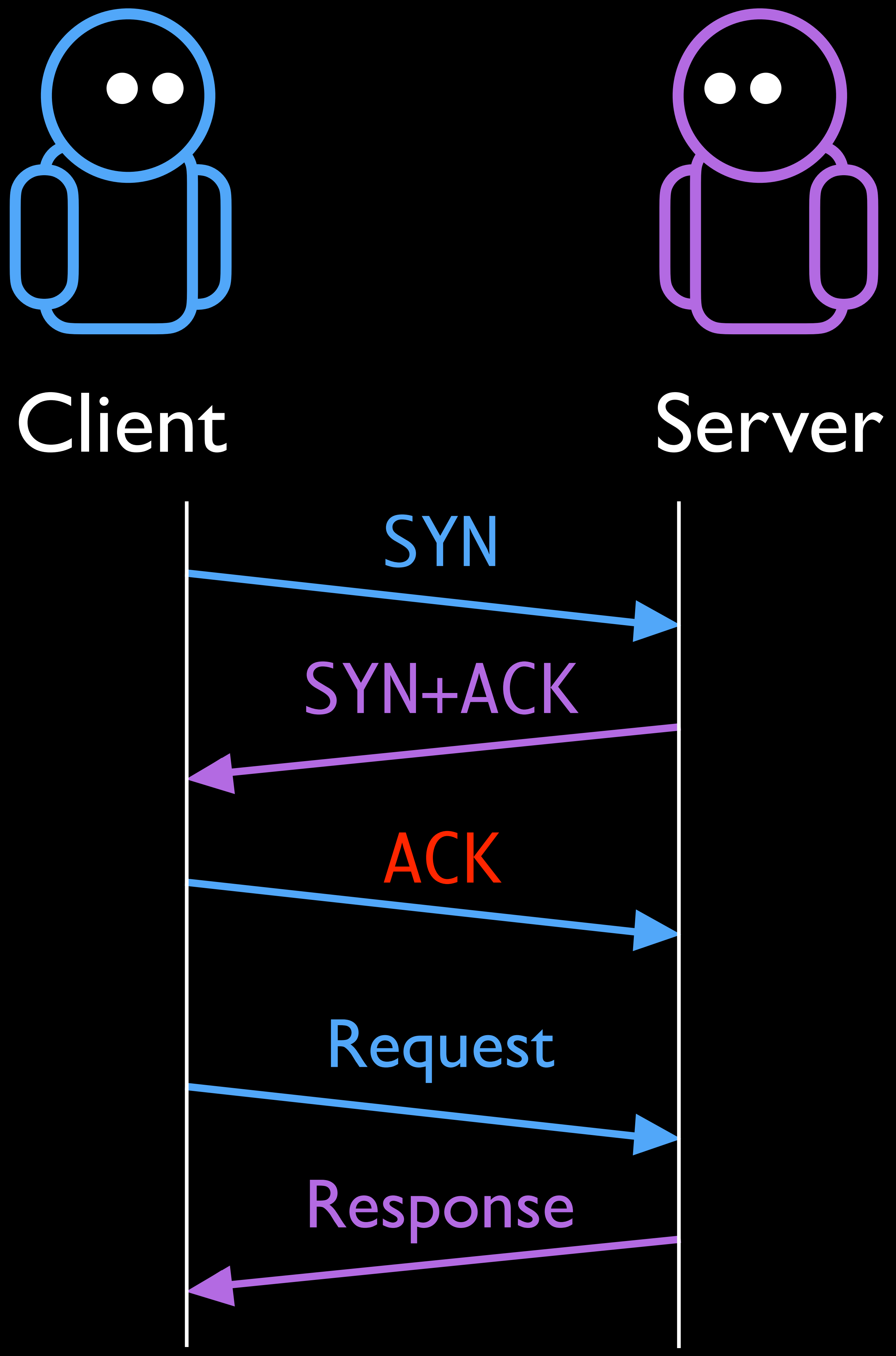
TCP requires a threeway handshake

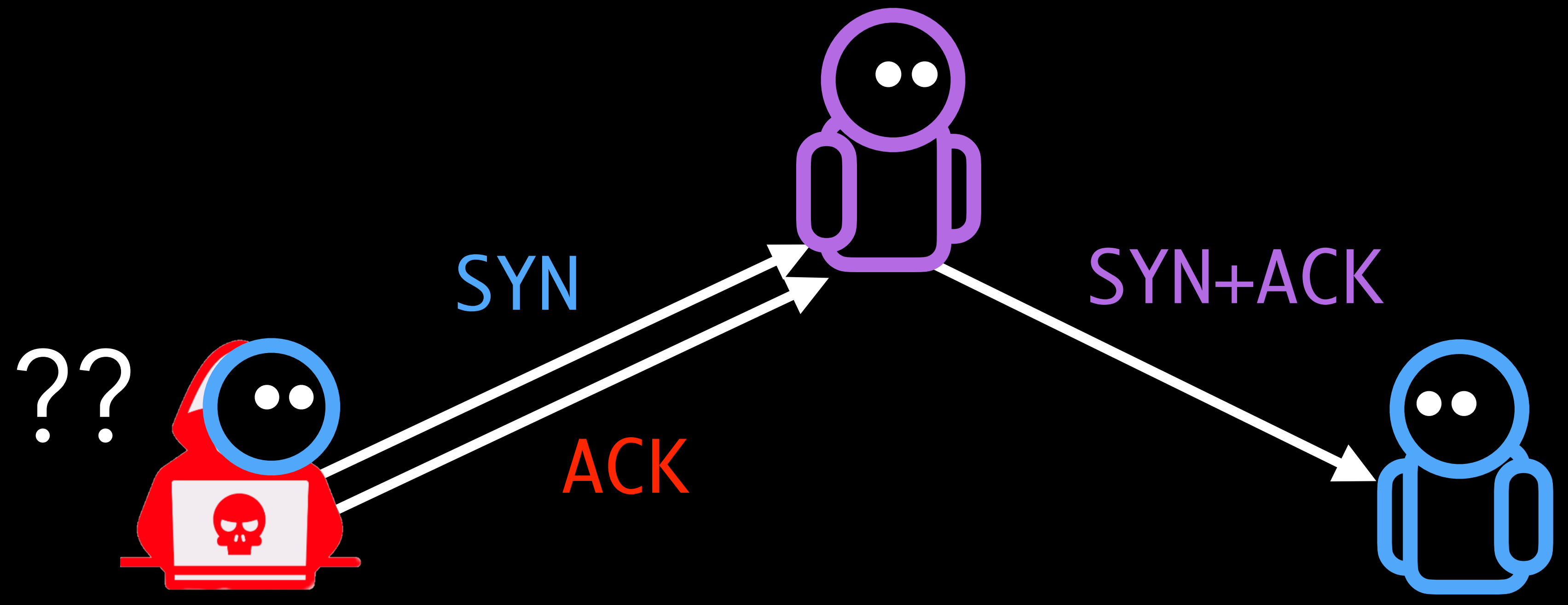




Reflected amplification attacks

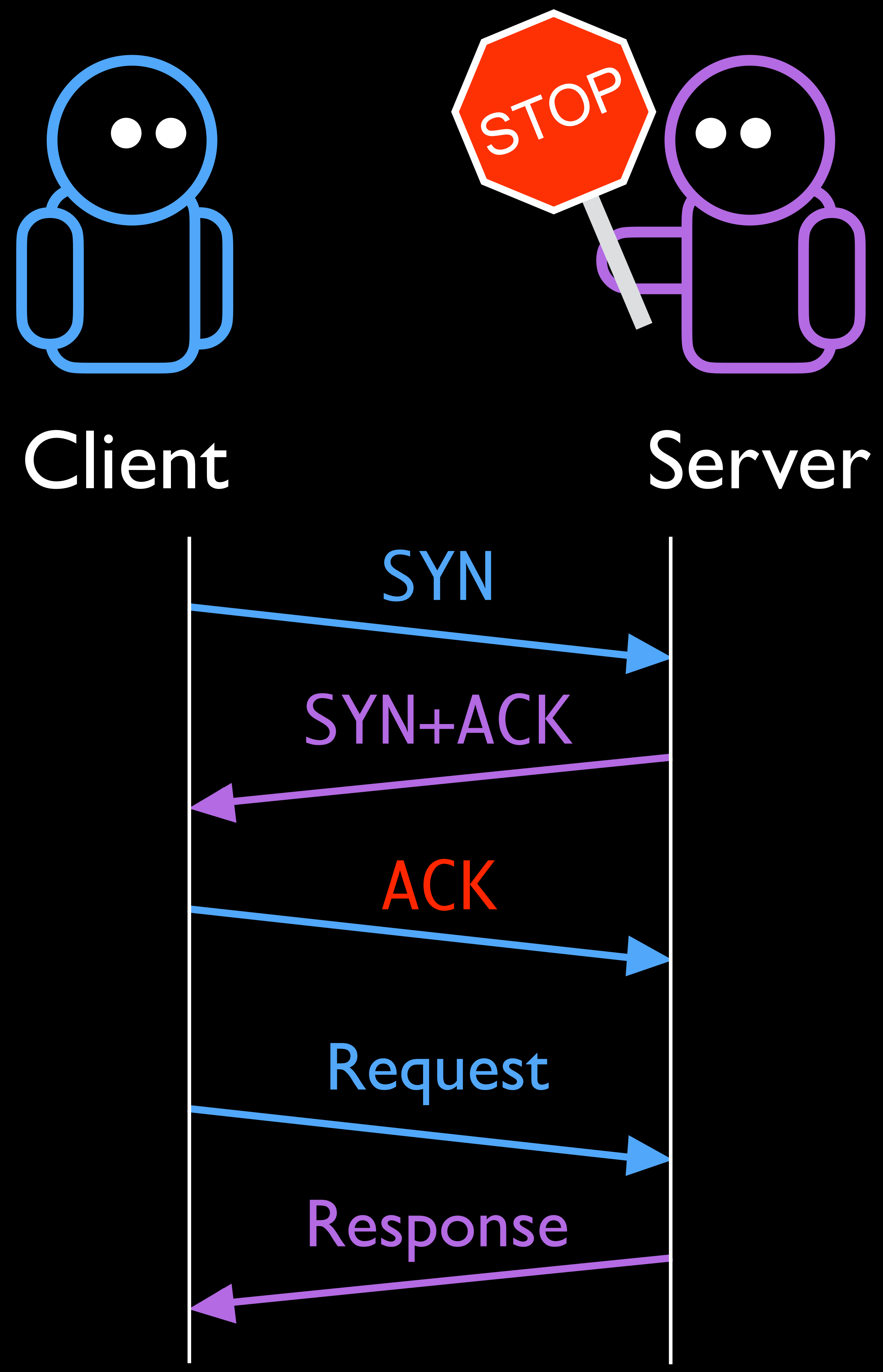
TCP requires a threeway handshake

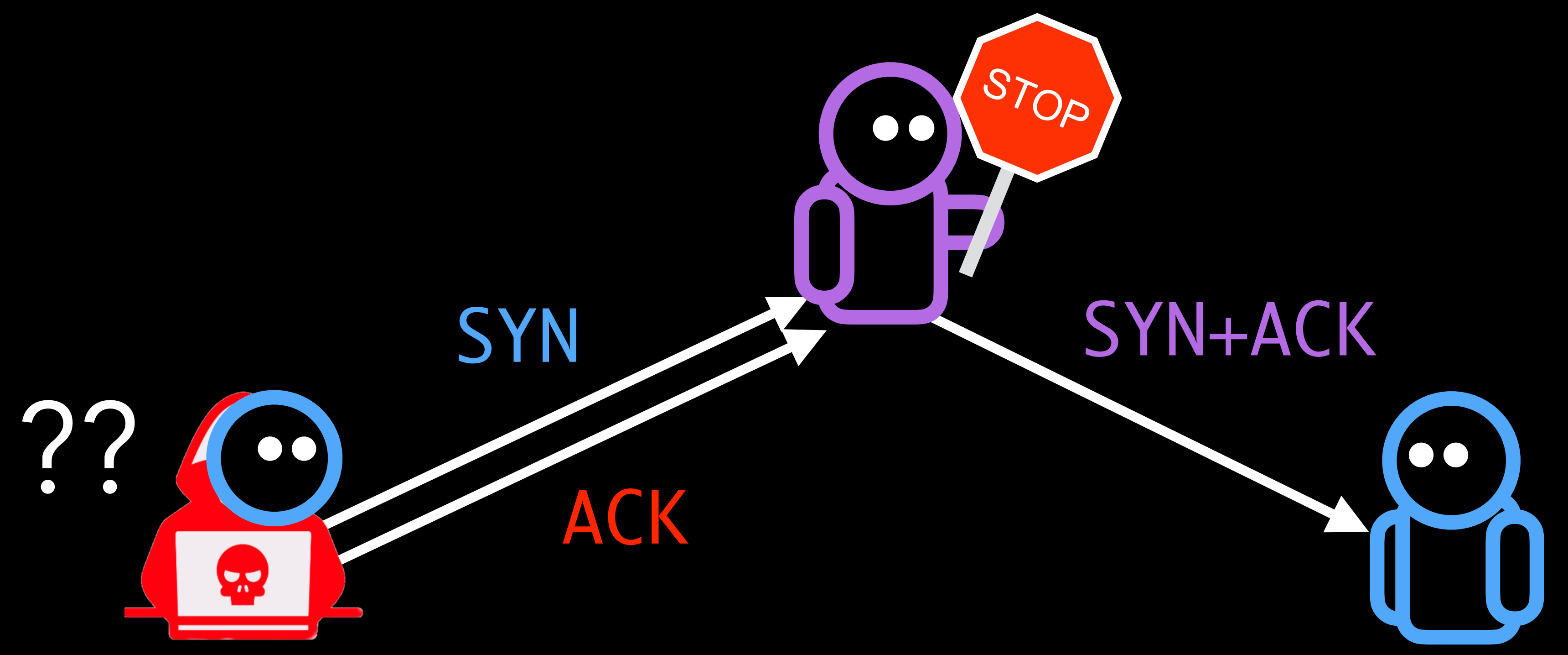




Reflected amplification attacks

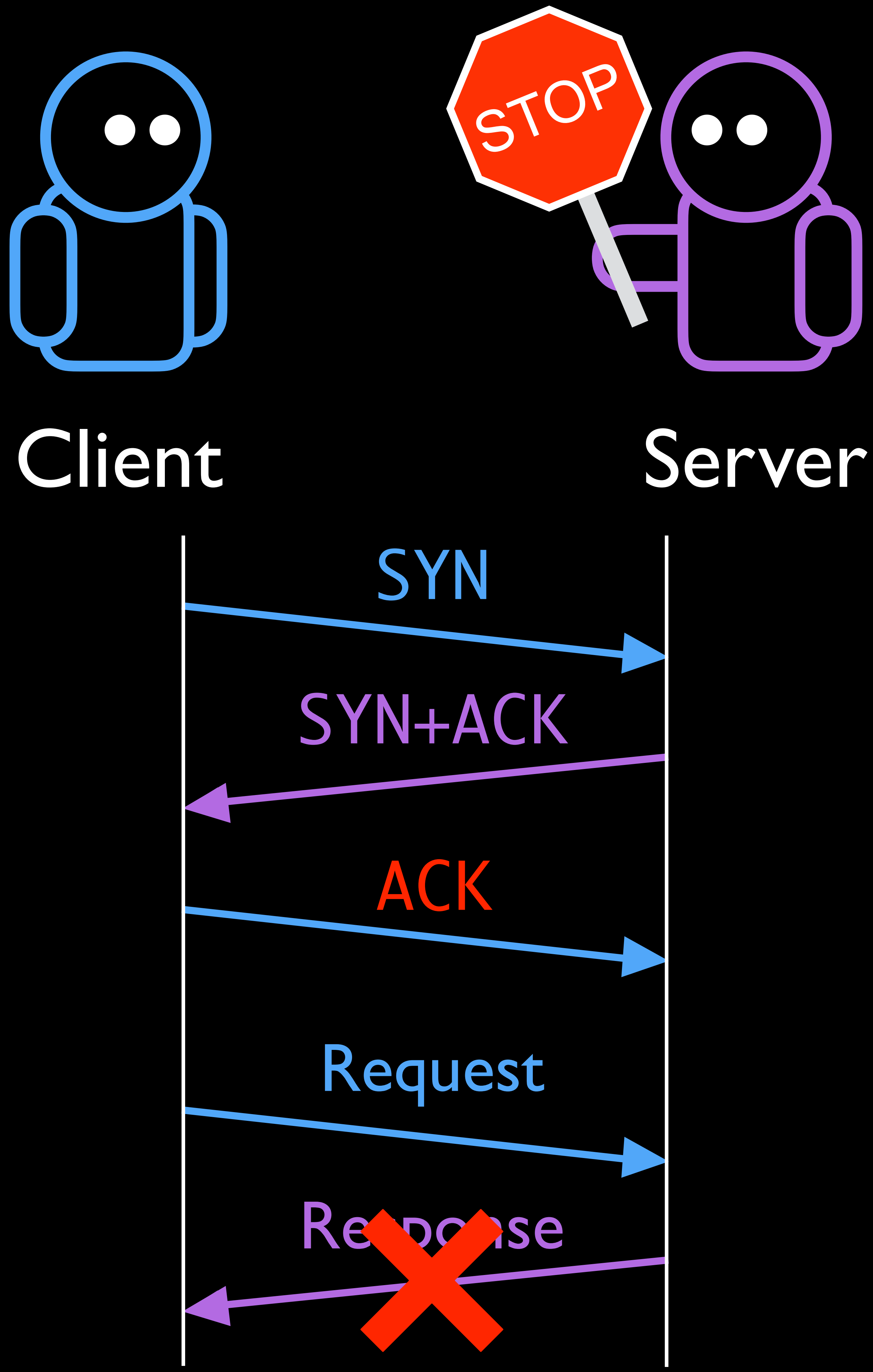
TCP requires a threeway handshake

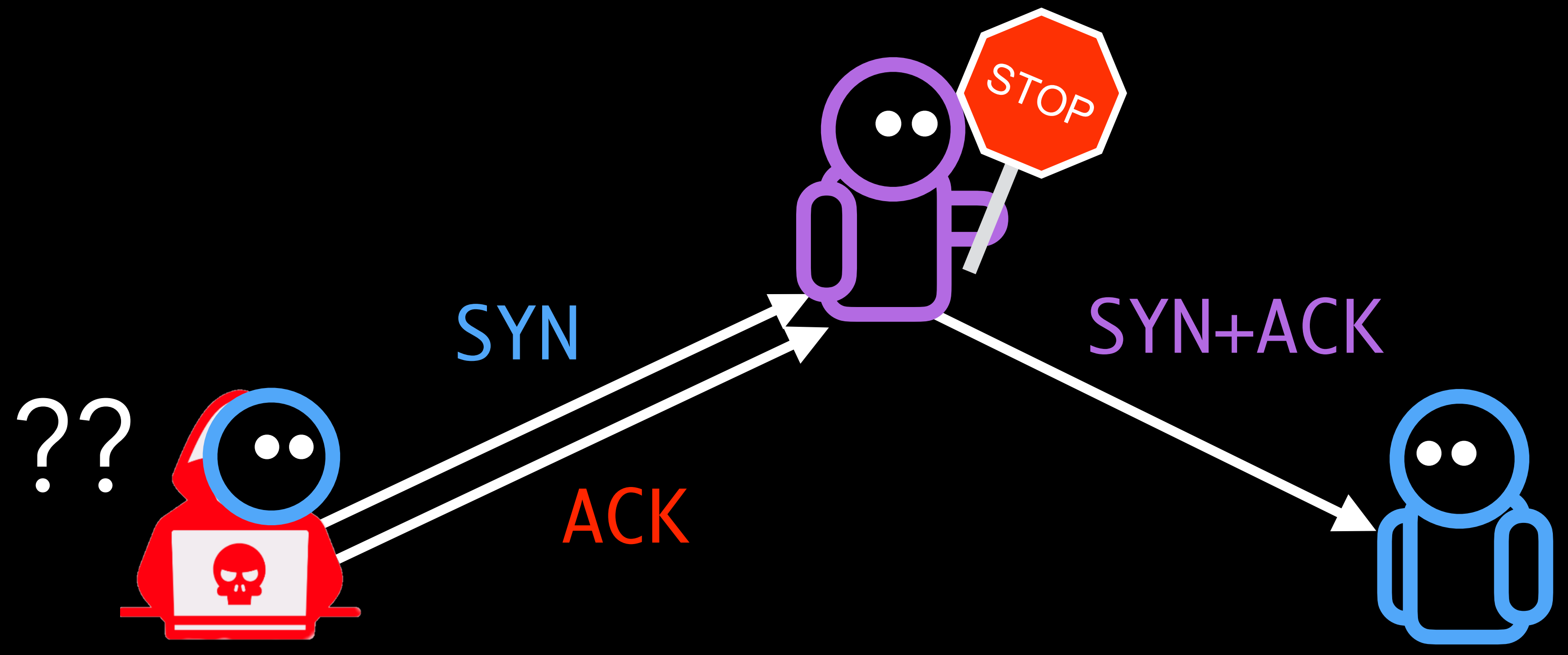




Reflected amplification attacks

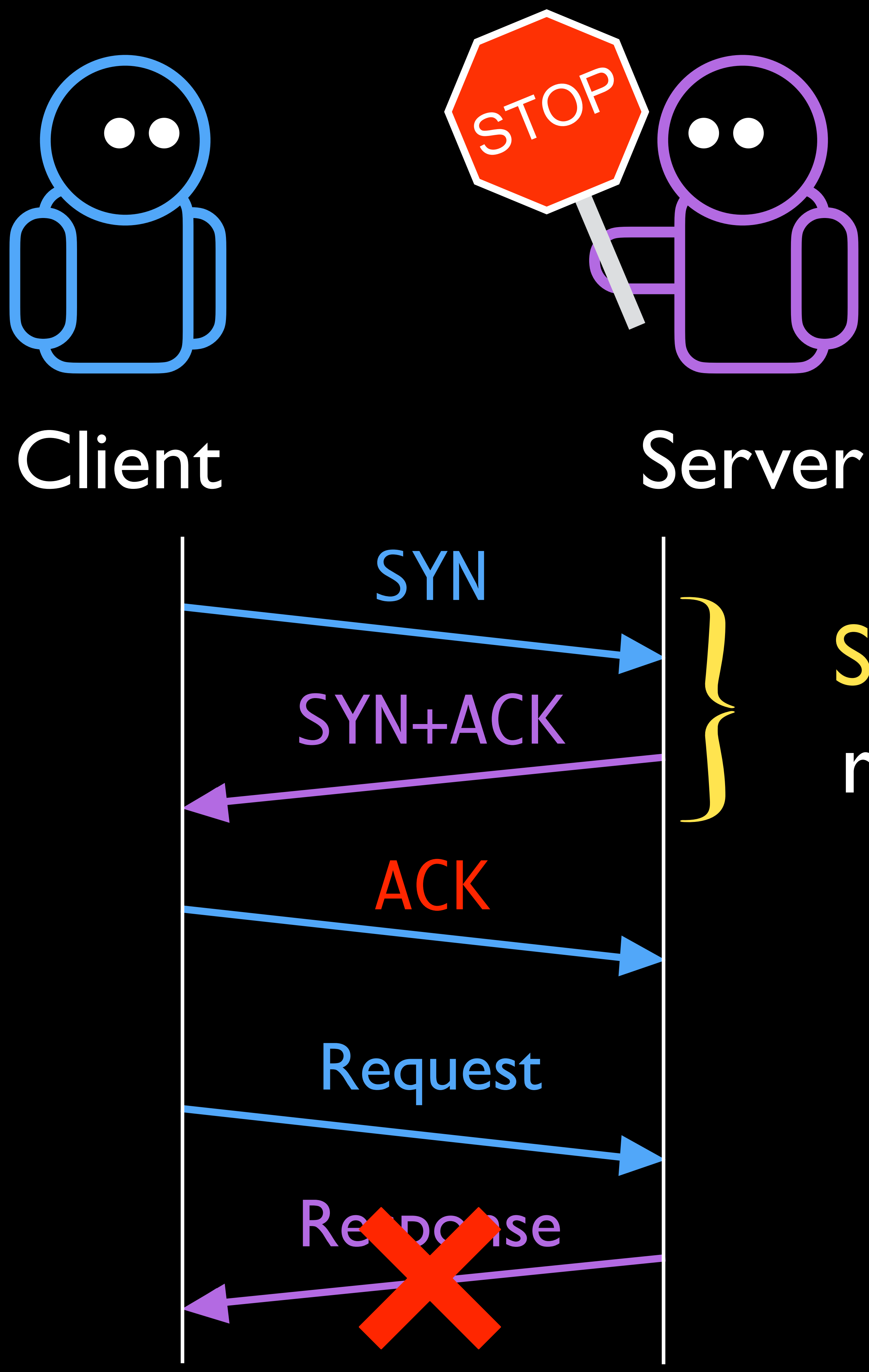
TCP requires a threeway handshake

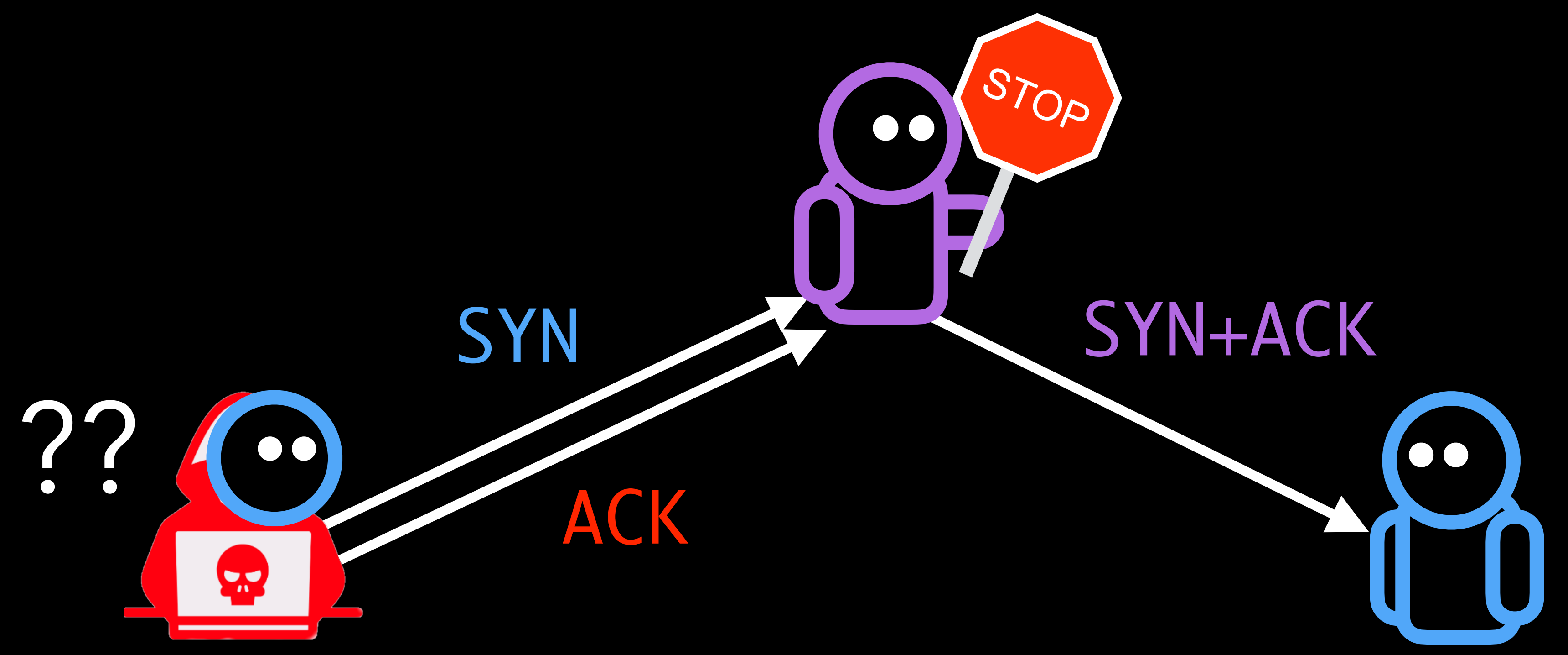




Reflected amplification attacks

TCP requires a threeway handshake

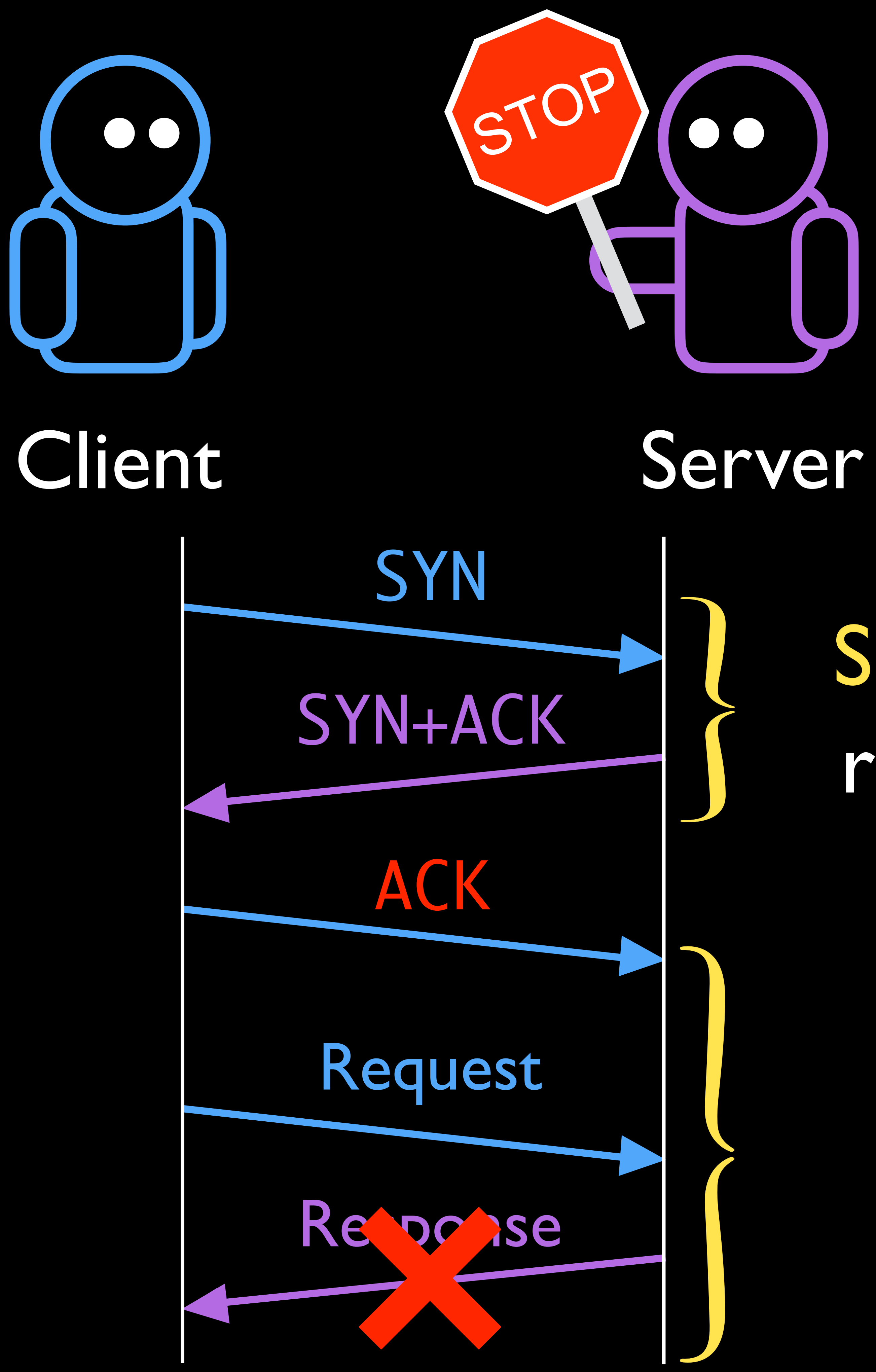




Some amplification due to retransmitted SYN+ACKs

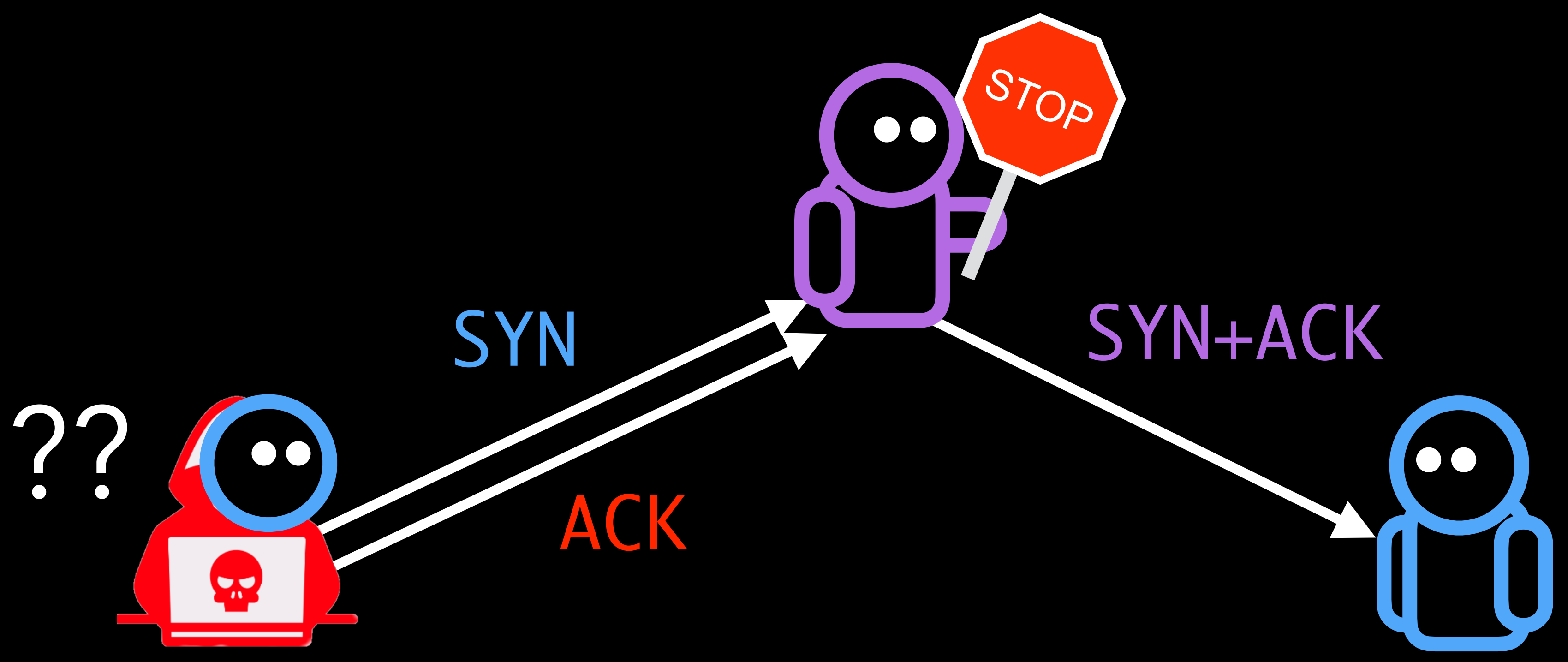
Reflected amplification attacks

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*

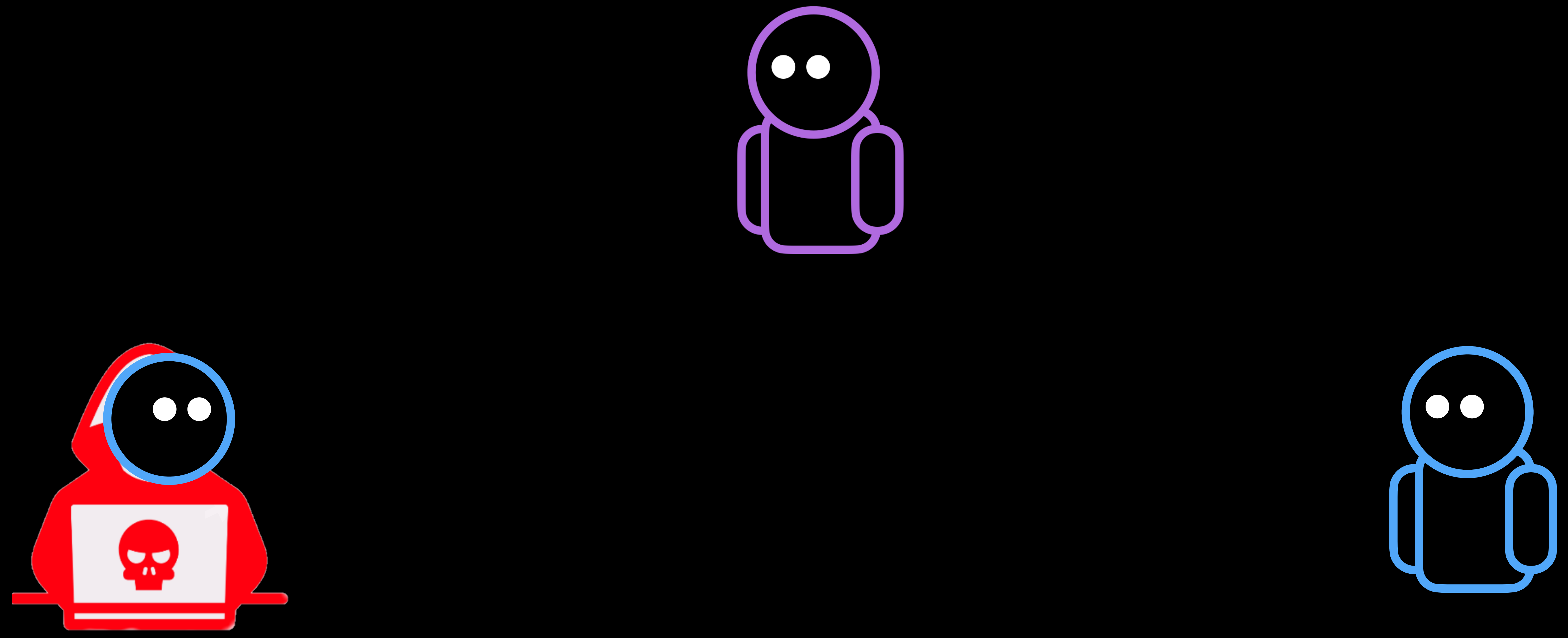
- Five distinct attacks
- Millions of amplifiers
- Amplification factors in the millions

Found *infinite amplification* and identified *root causes*

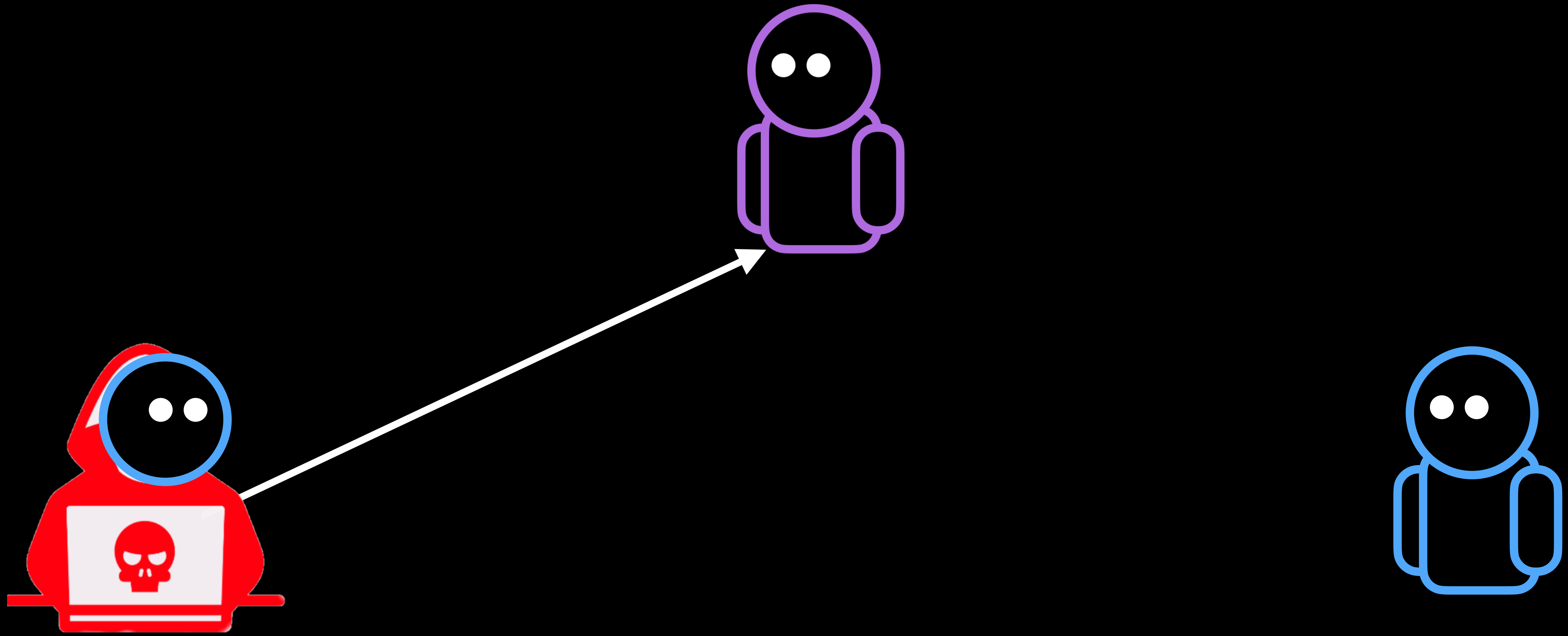
Use middleboxes as amplifiers!

Weaponizing middleboxes

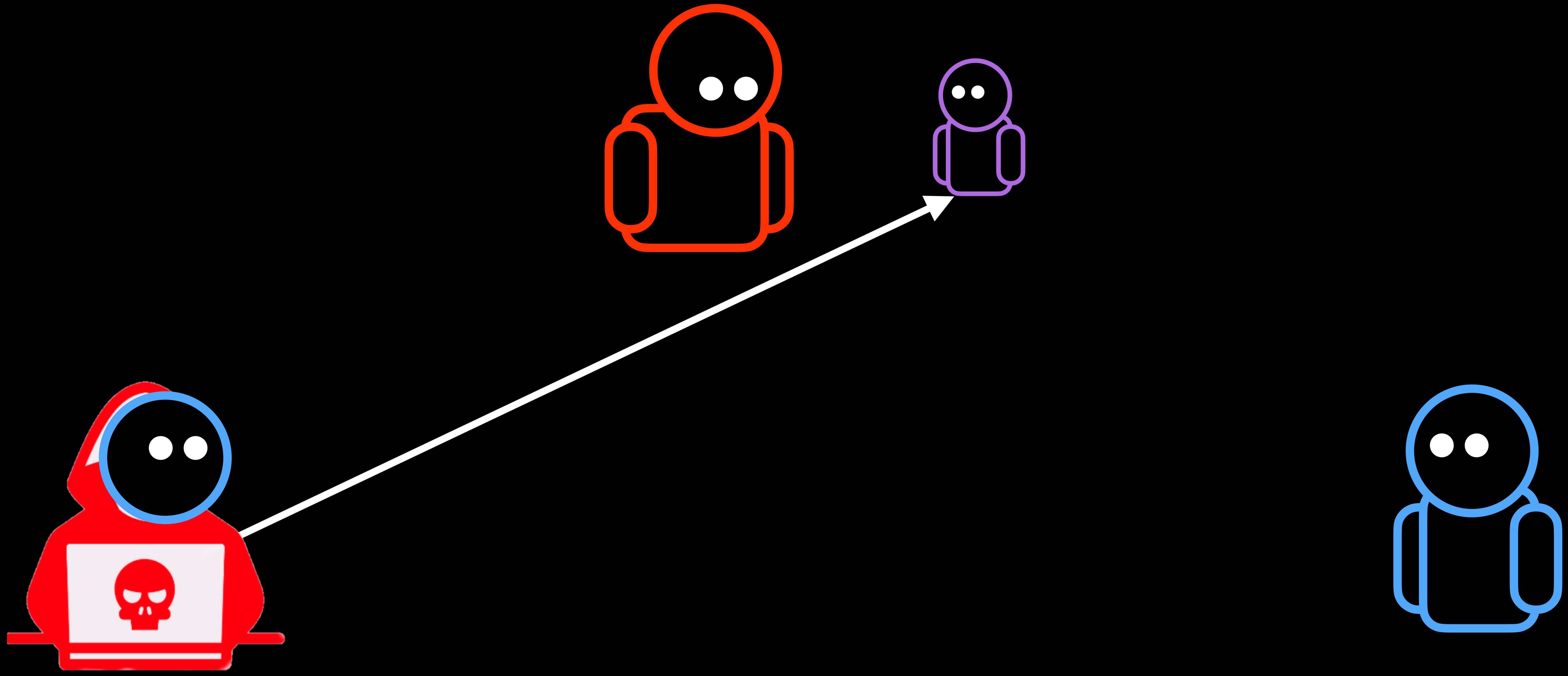
Weaponizing middleboxes



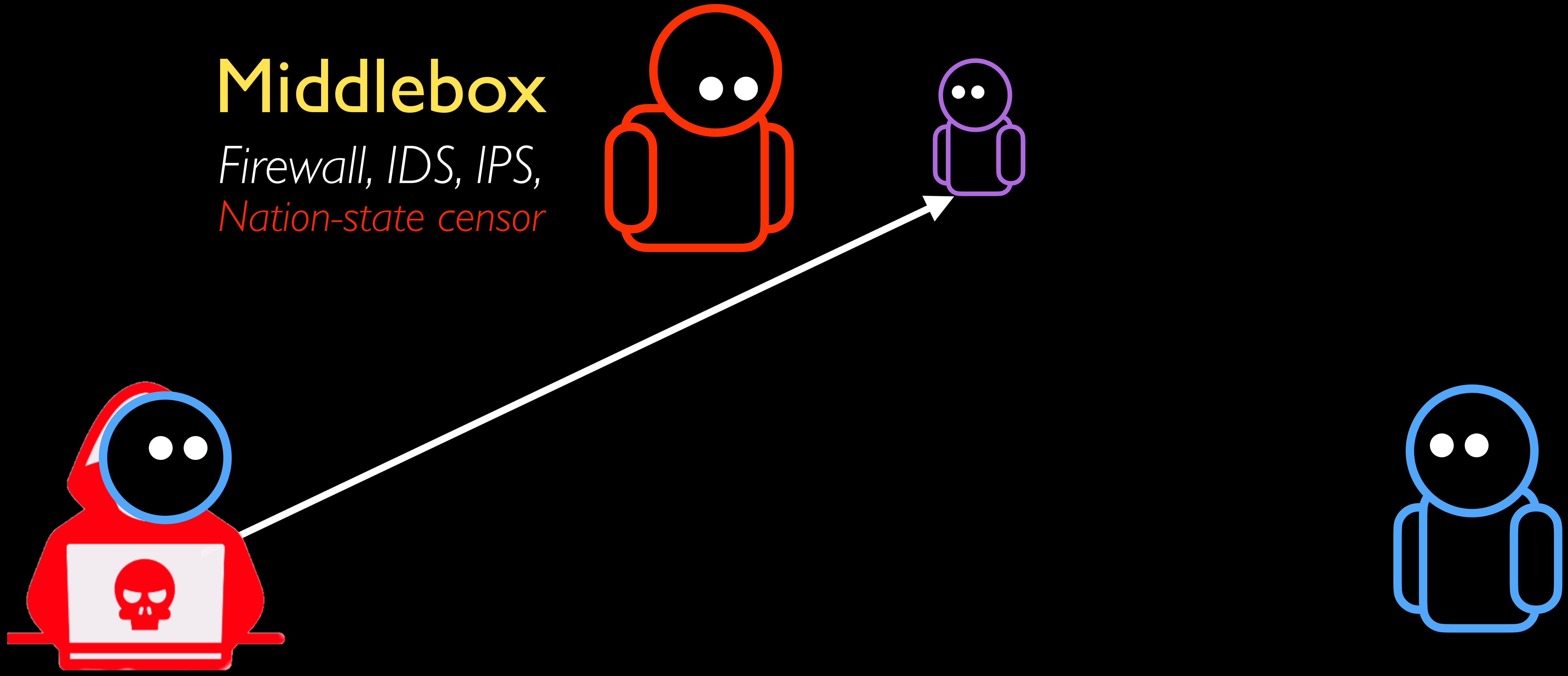
Weaponizing middleboxes



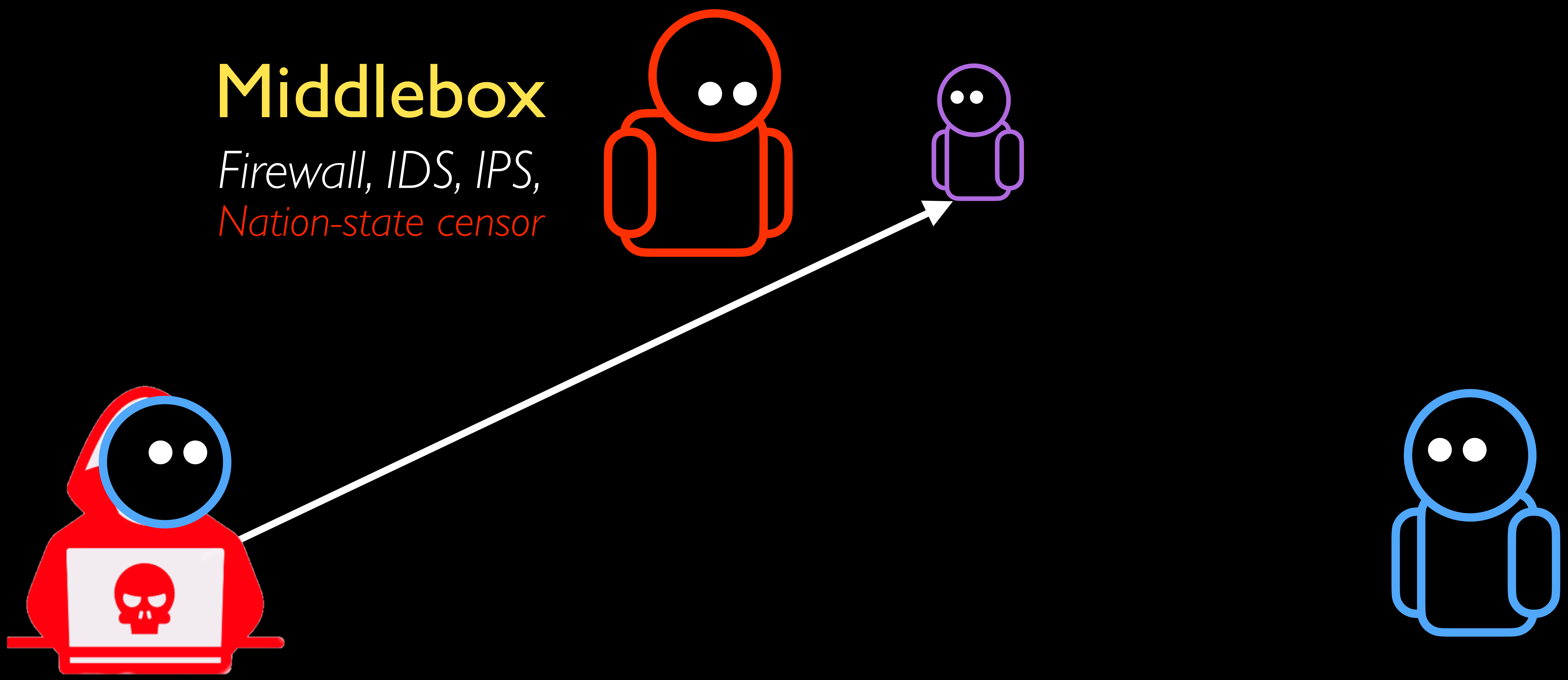
Weaponizing middleboxes



Weaponizing middleboxes

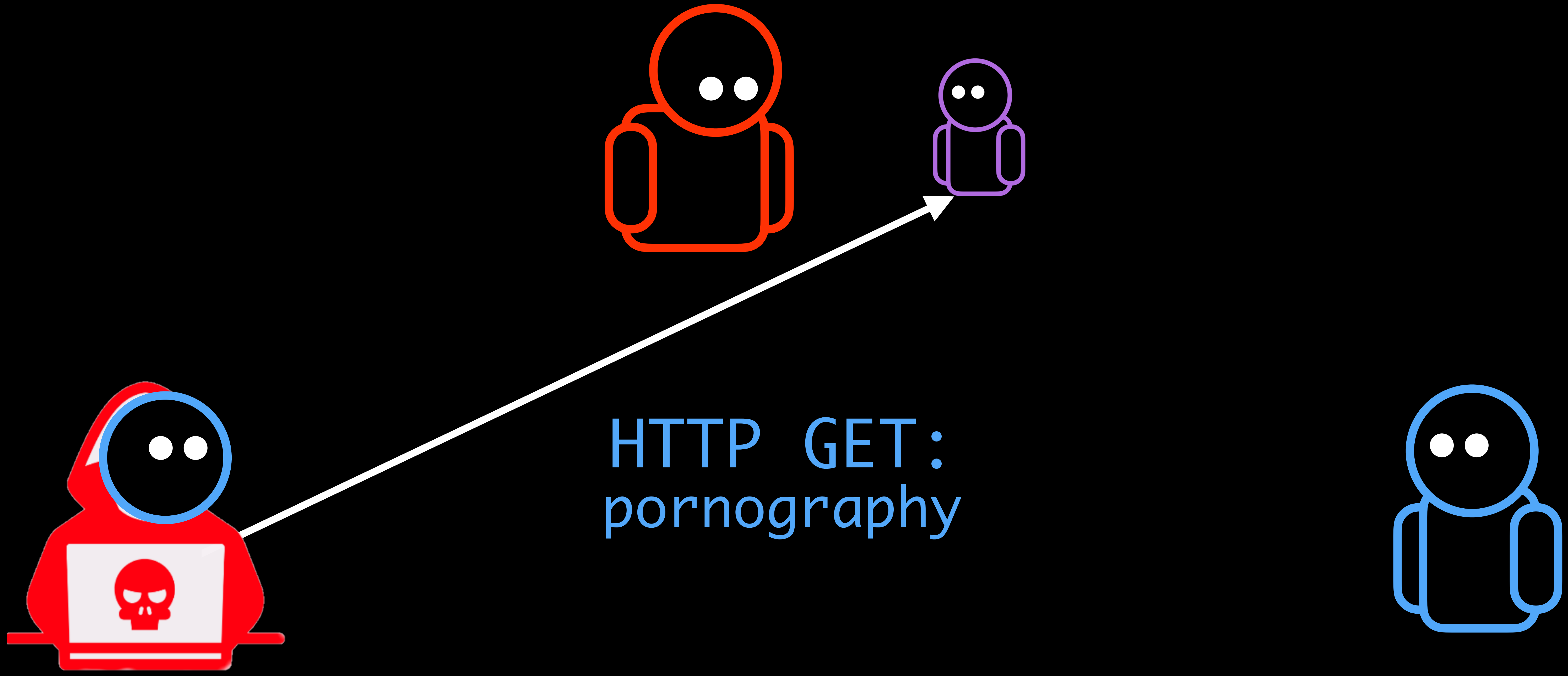


Weaponizing middleboxes



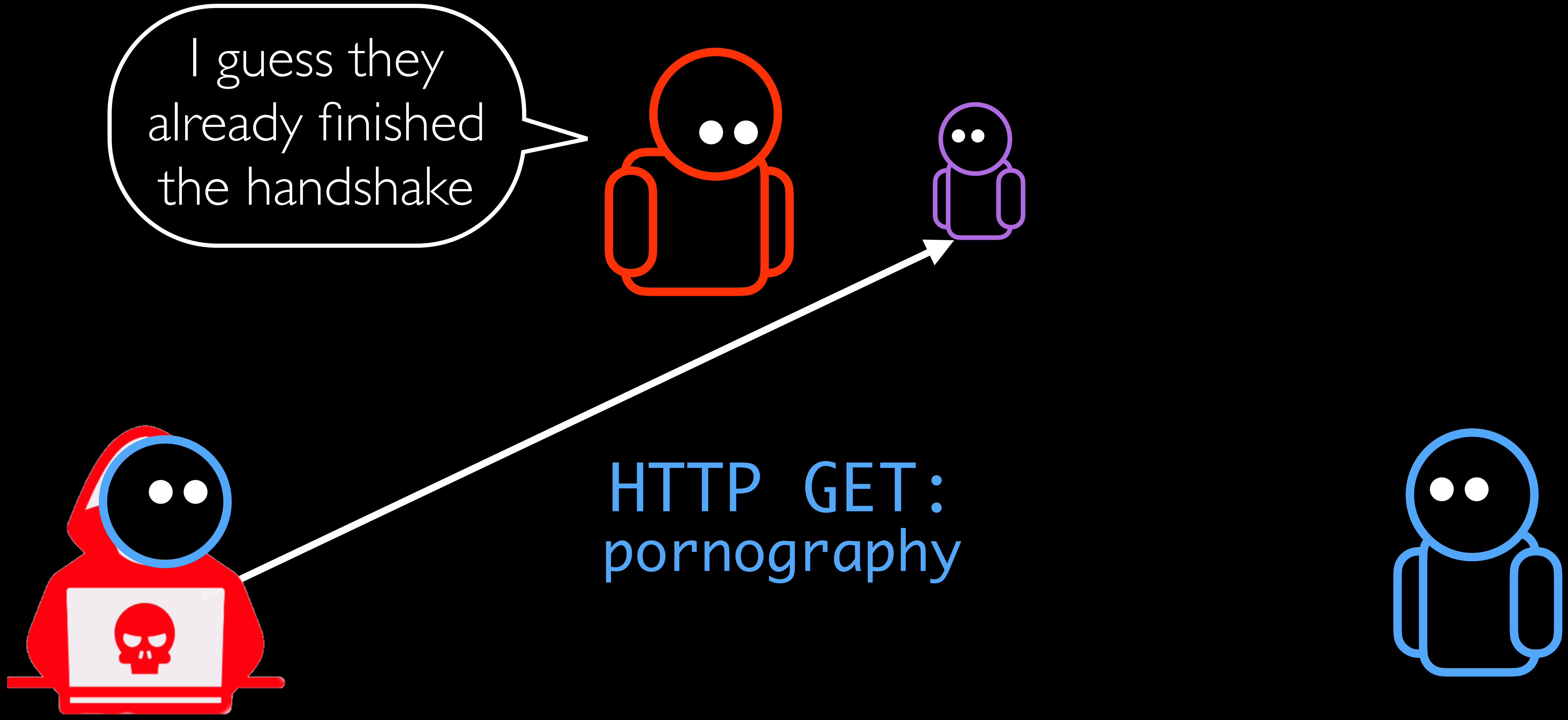
① Middleboxes expect to miss some packets

Weaponizing middleboxes



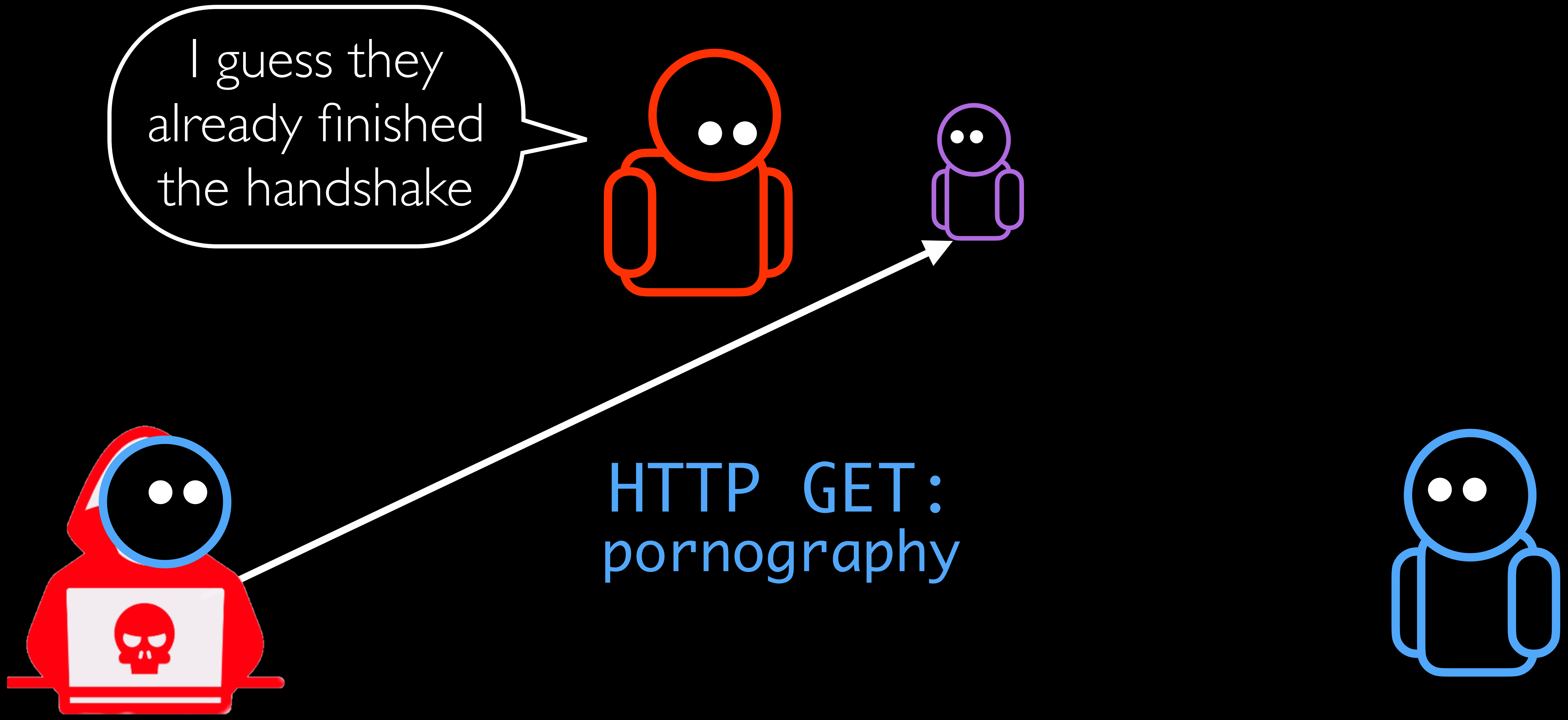
① Middleboxes expect to miss some packets

Weaponizing middleboxes



① Middleboxes expect to miss some packets

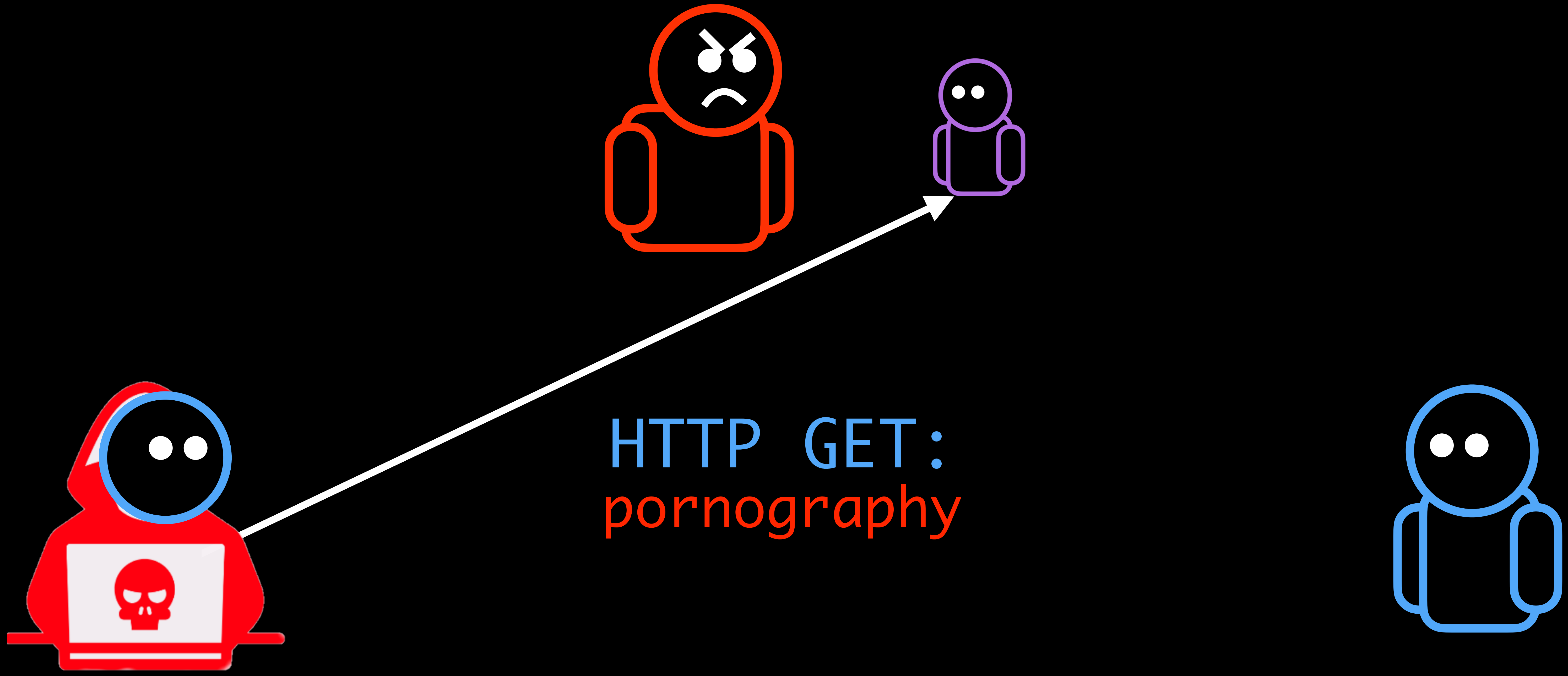
Weaponizing middleboxes



① Middleboxes expect to miss some packets

② Middleboxes *inject traffic* to block connections

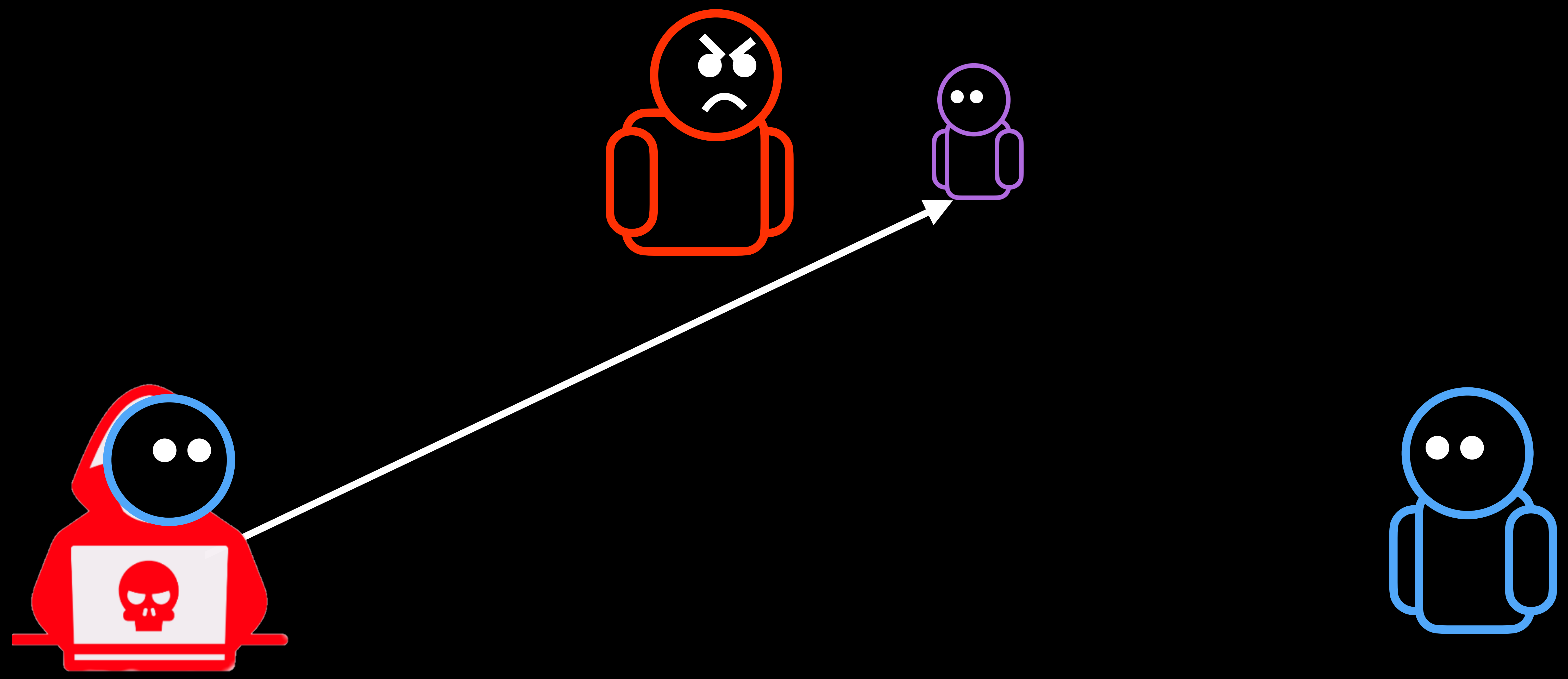
Weaponizing middleboxes



① Middleboxes expect to miss some packets

② Middleboxes *inject traffic* to block connections

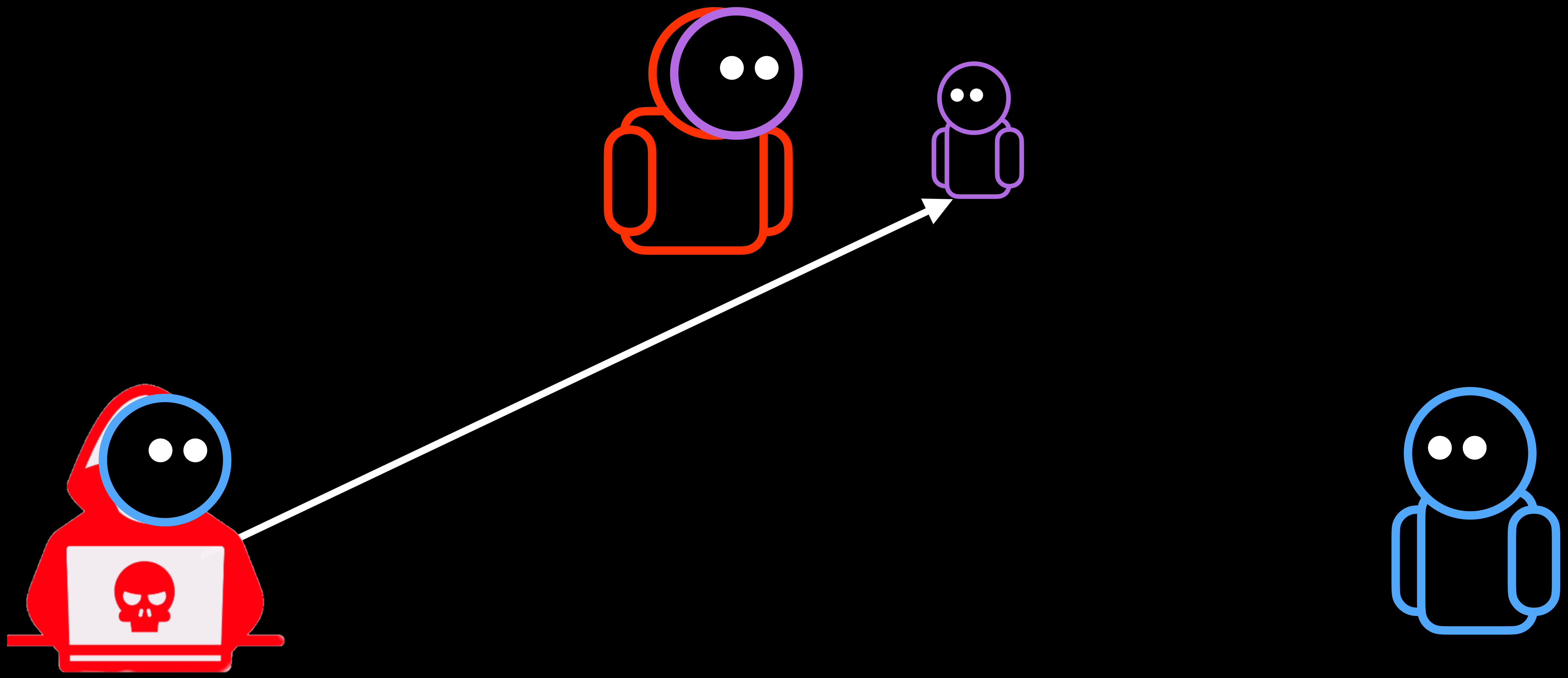
Weaponizing middleboxes



① Middleboxes expect to miss some packets

② Middleboxes *inject traffic* to block connections

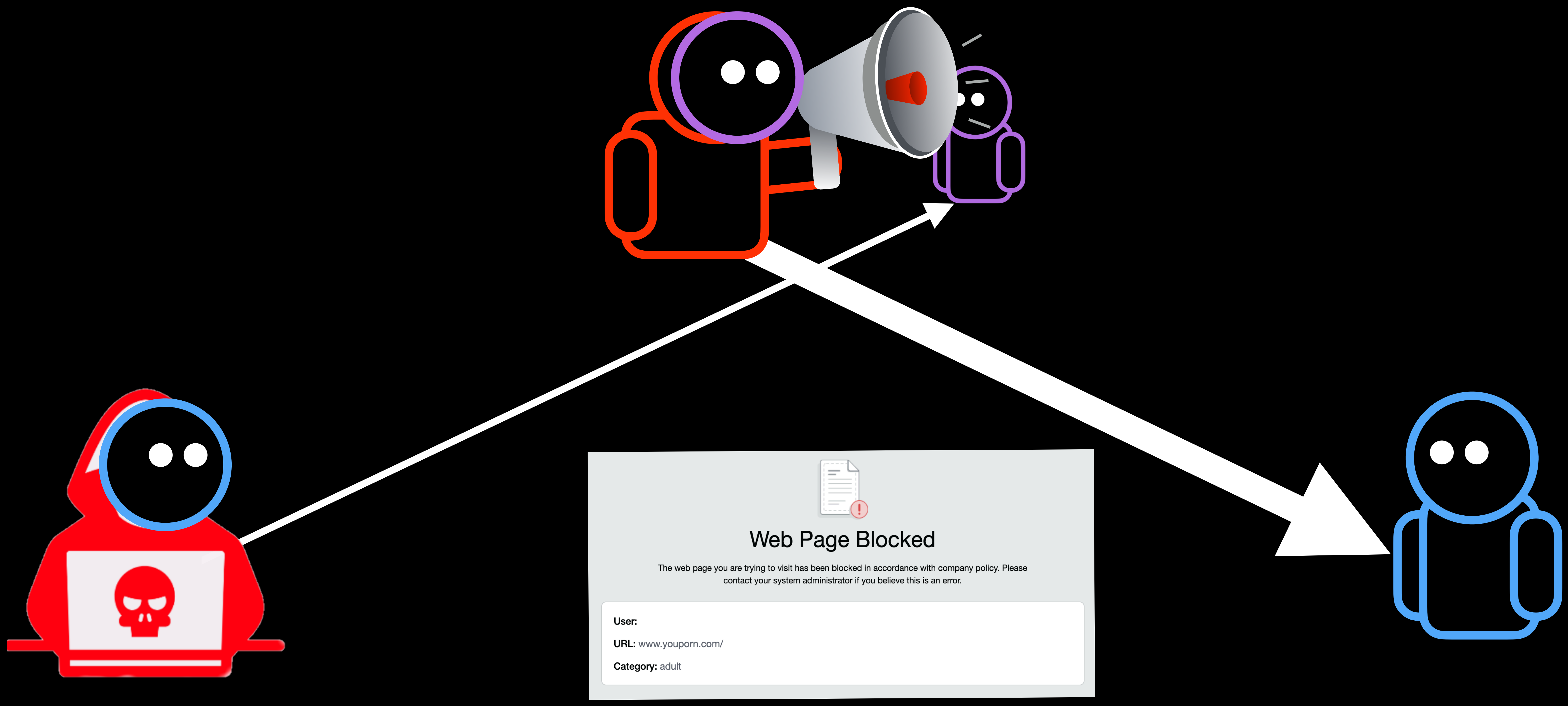
Weaponizing middleboxes



① Middleboxes expect to miss some packets

② Middleboxes *inject traffic* to block connections

Weaponizing middleboxes



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

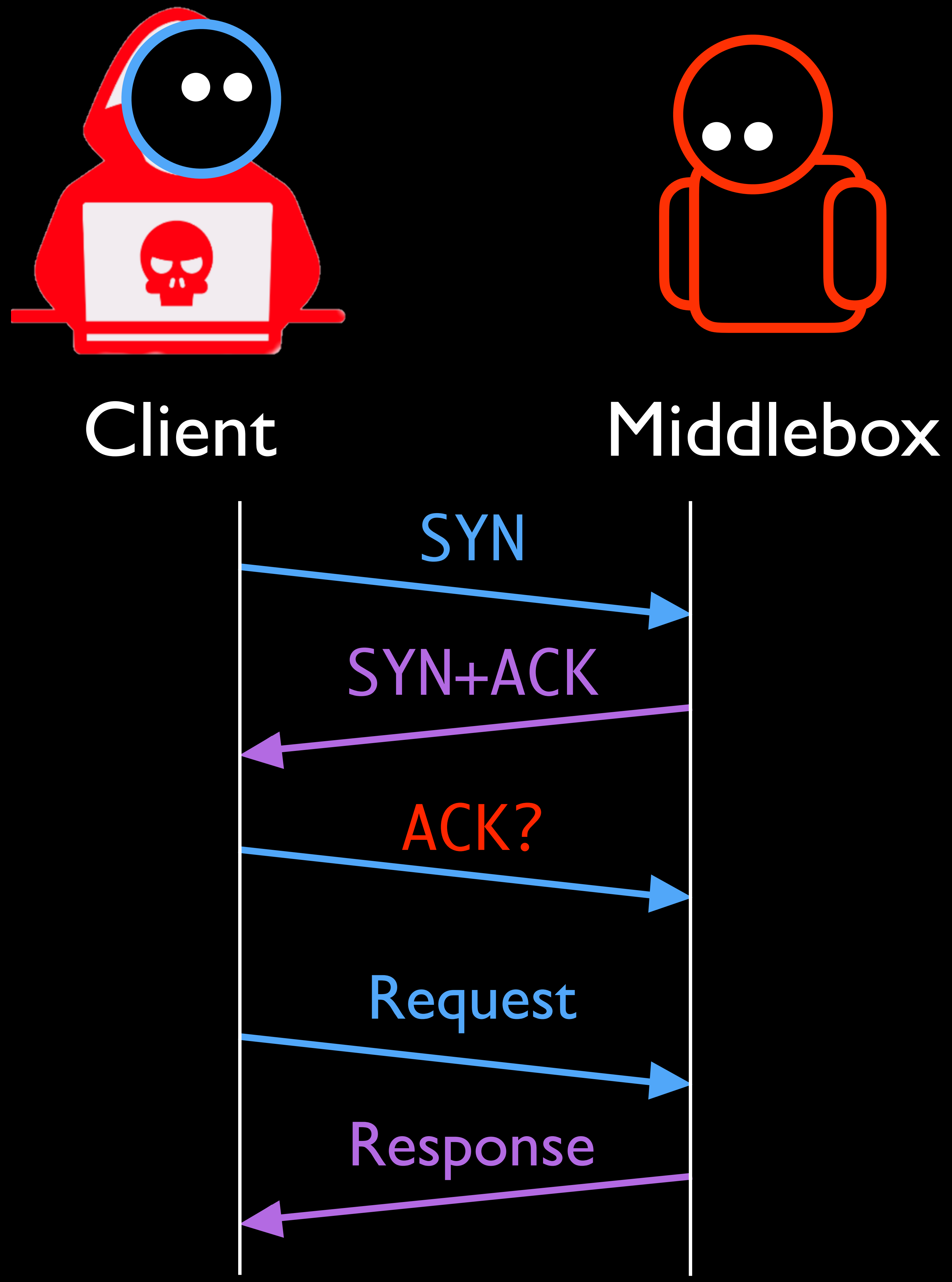
URL: www.youporn.com/

Category: adult

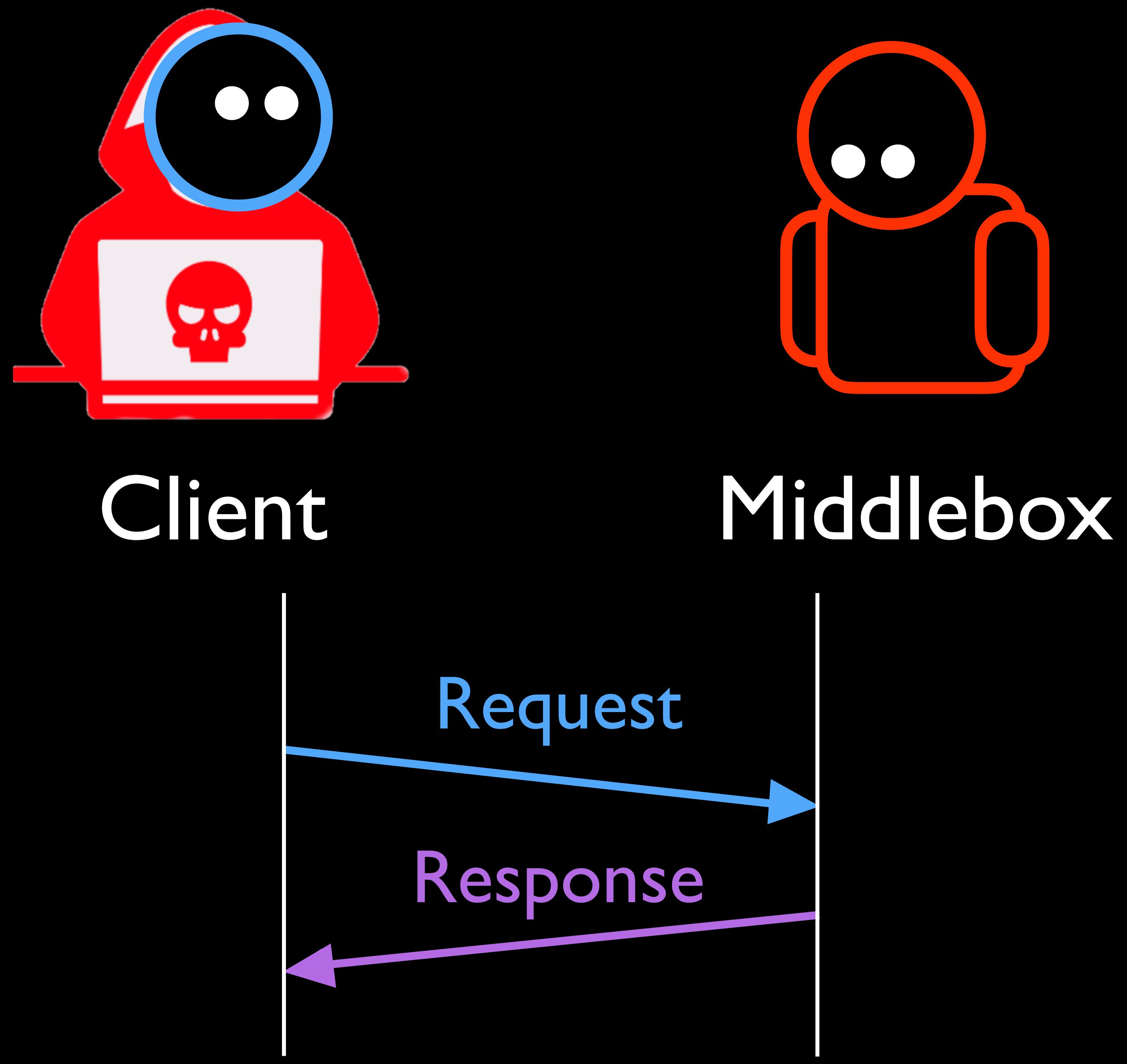
① Middleboxes expect to miss some packets

② Middleboxes *inject traffic* to block connections

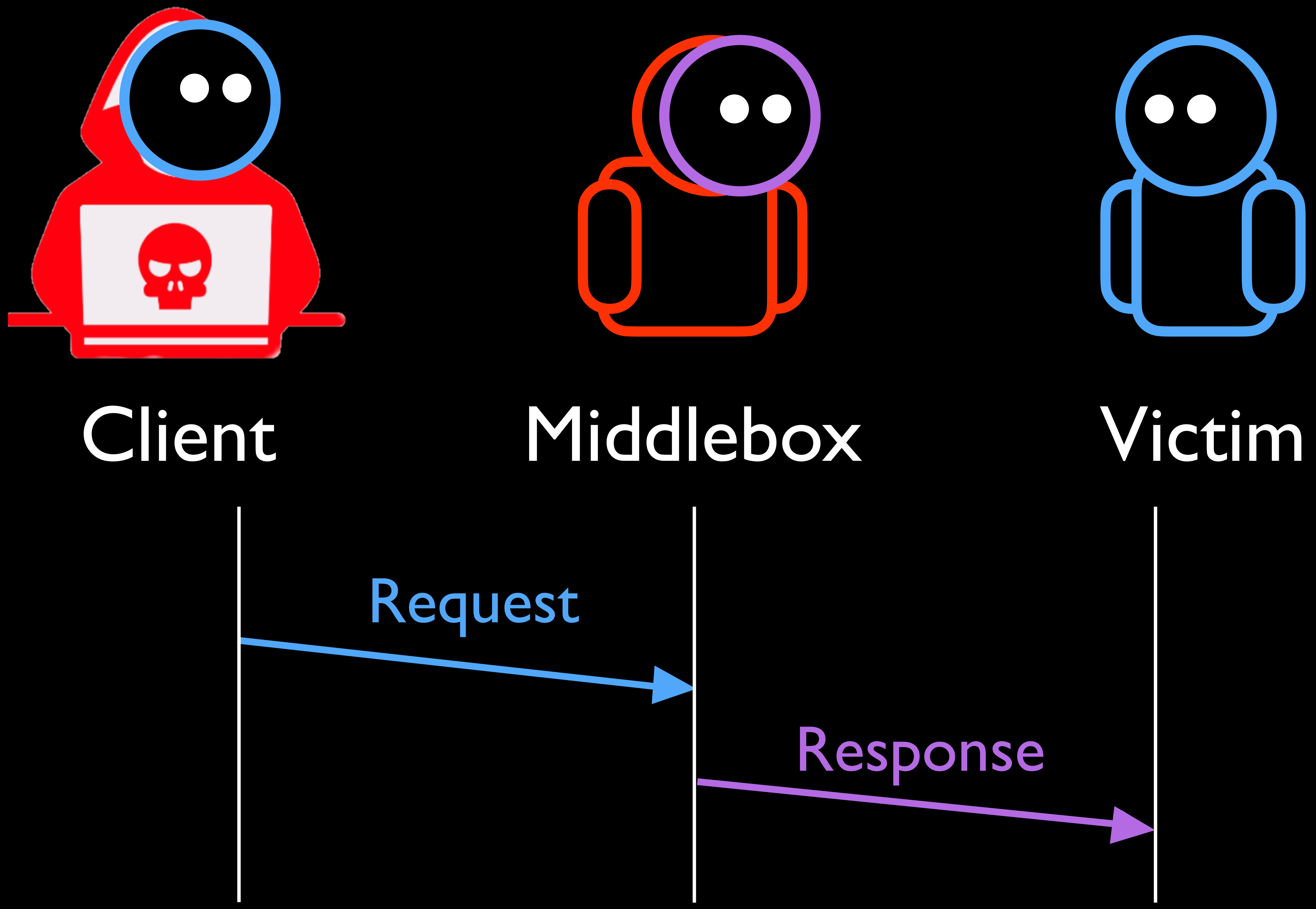
Middleboxes make TCP-based amplification possible



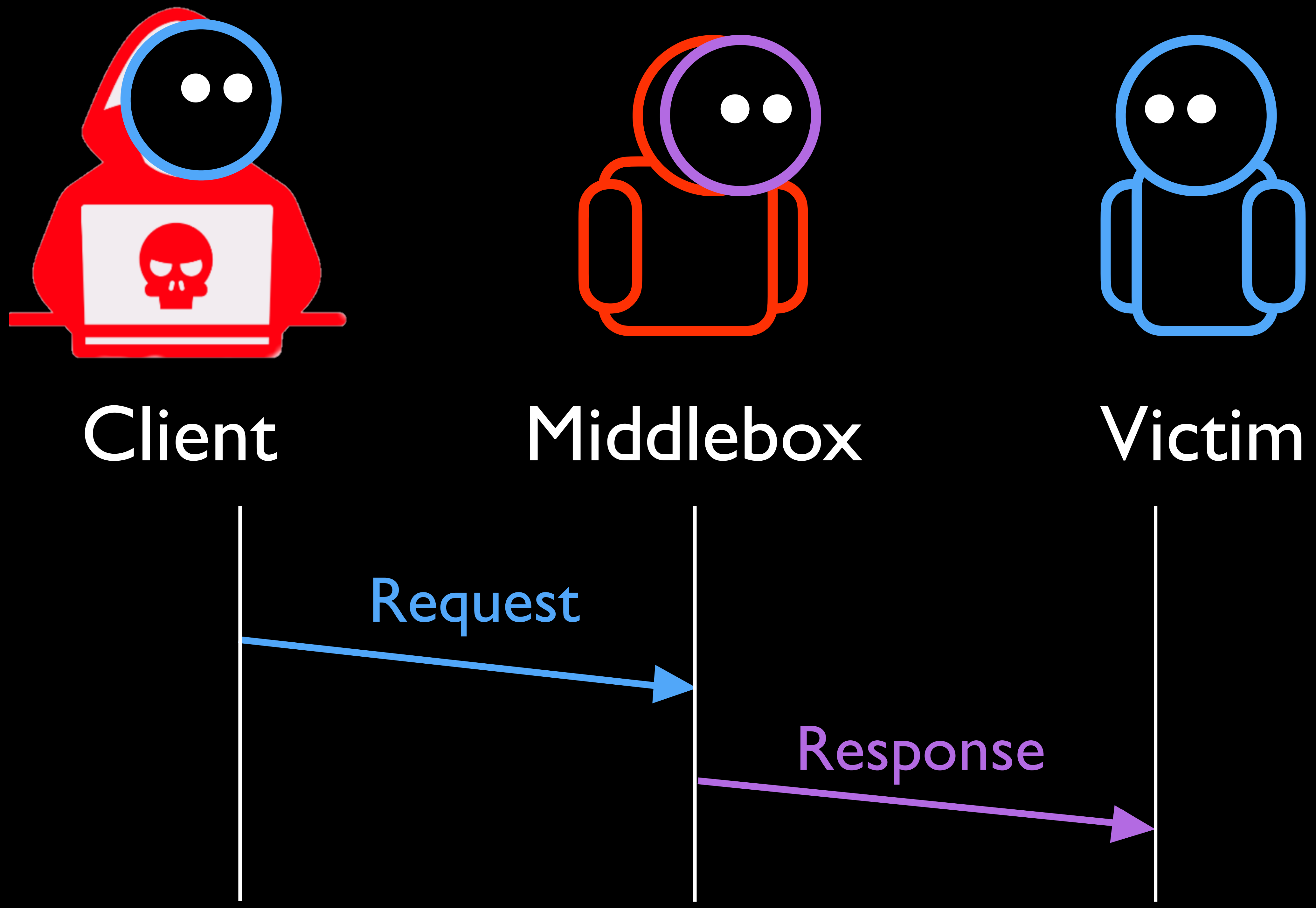
Middleboxes make TCP-based amplification possible



Middleboxes make TCP-based amplification possible

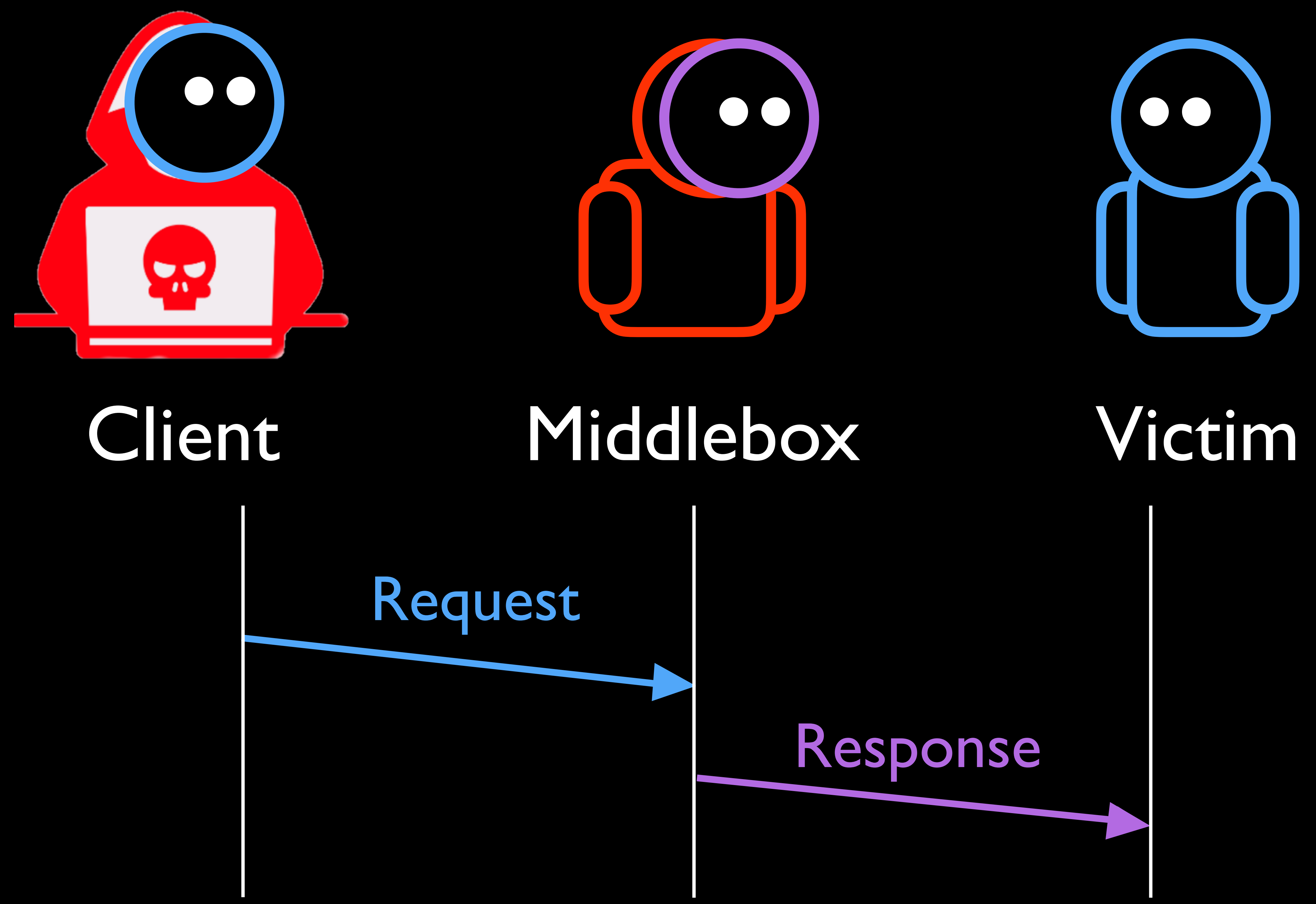


Middleboxes make TCP-based amplification possible



What packets best trigger middleboxes?

Middleboxes make TCP-based amplification possible

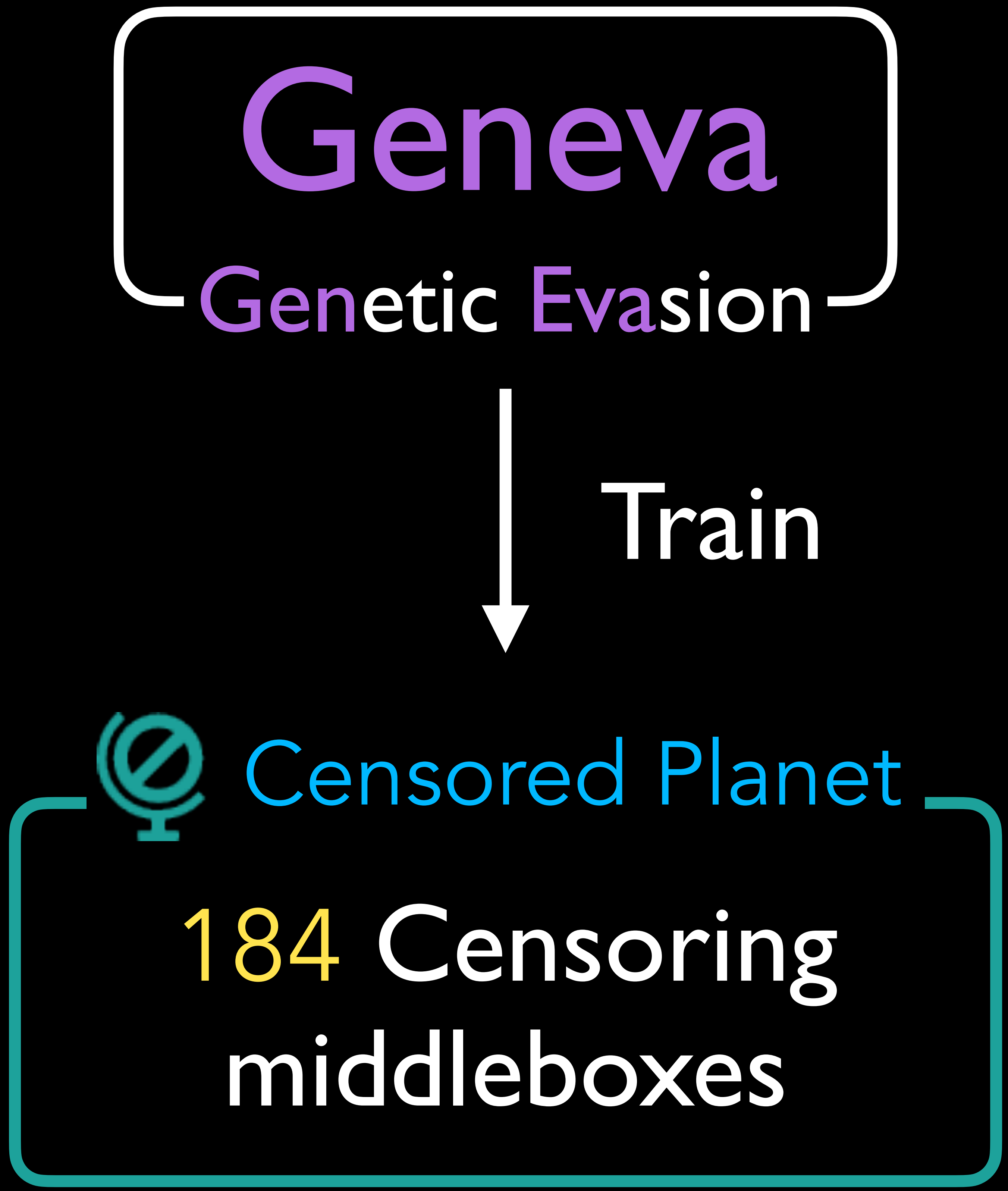


What packets best trigger middleboxes?

What amplifications are attainable?

Methodology

① Automated Discovery



Geneva

Genetic Evasion

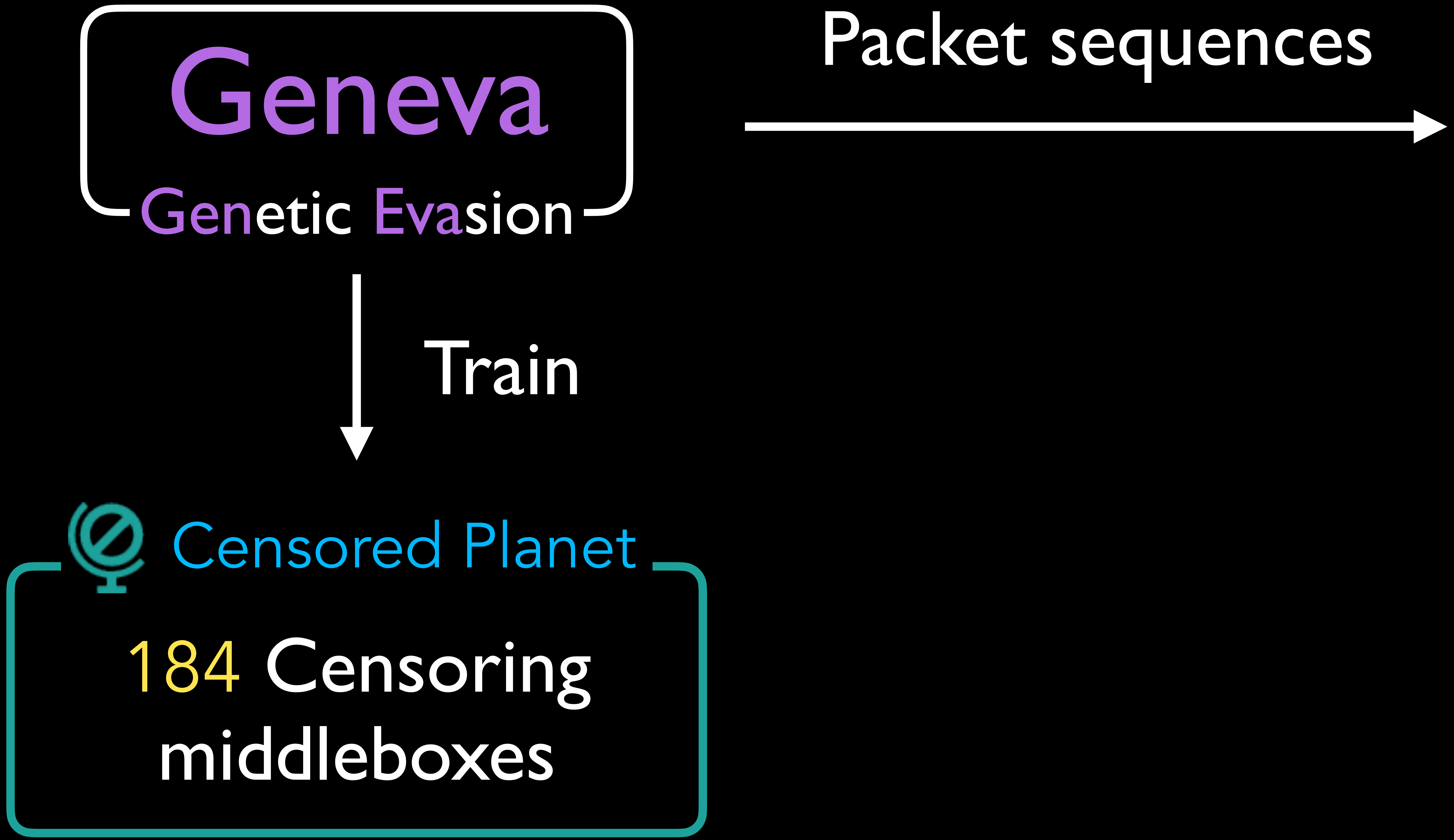
Train

Censored Planet

184 Censoring middleboxes

Methodology

① Automated Discovery



Geneva

Genetic Evasion

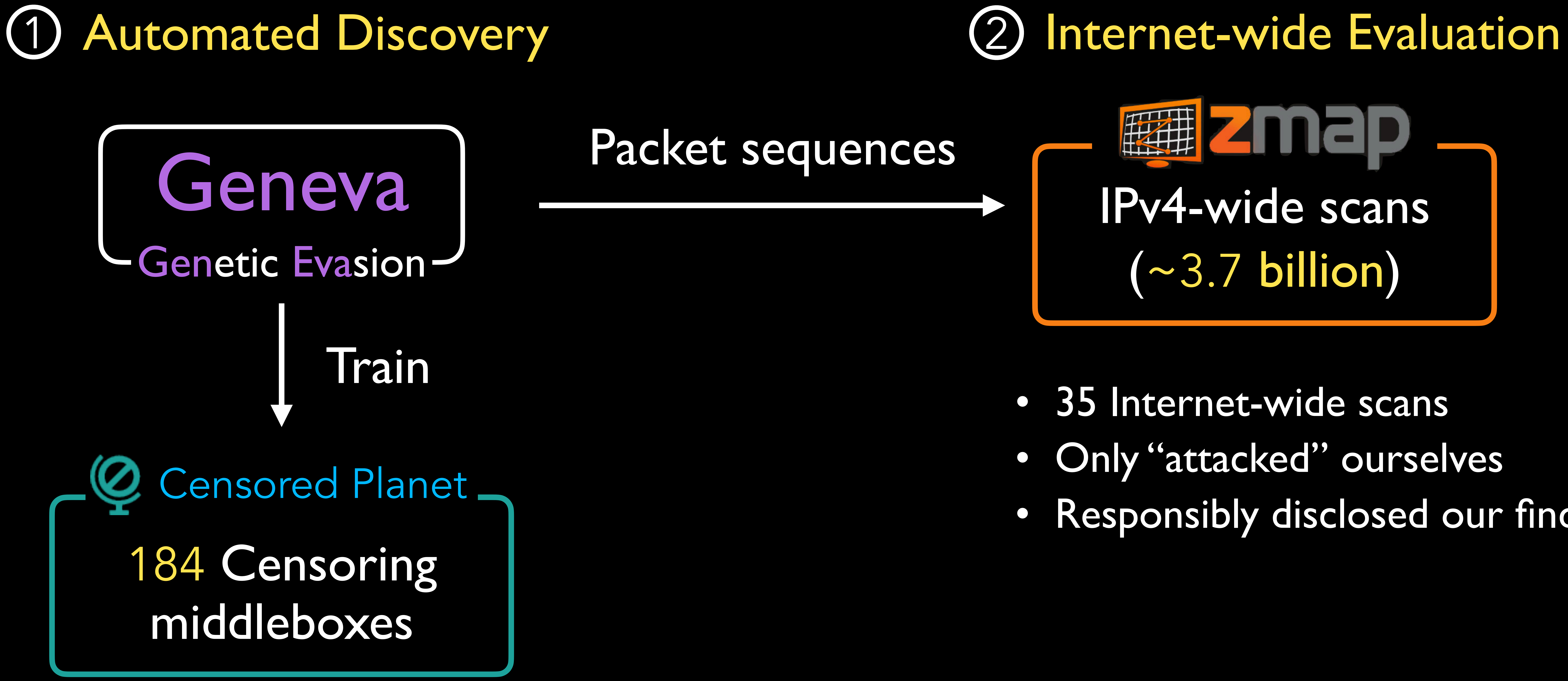
Packet sequences

Train

Censored Planet

184 Censoring middleboxes

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*

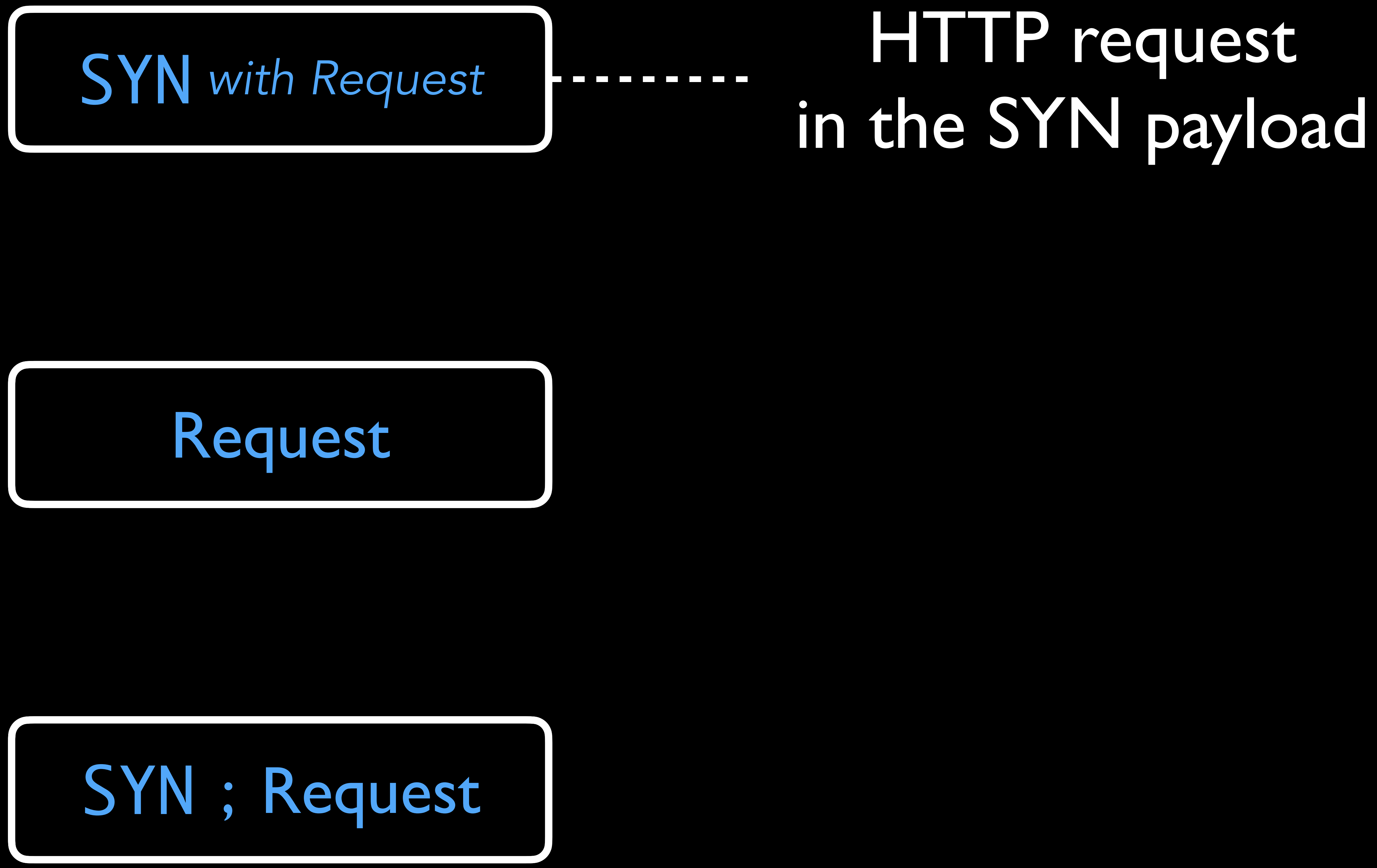
Request

SYN ; Request

TCP-based amplification attacks

Issue an HTTP request for forbidden content

Packet sequences



SYN *with Request*

HTTP request in the SYN payload

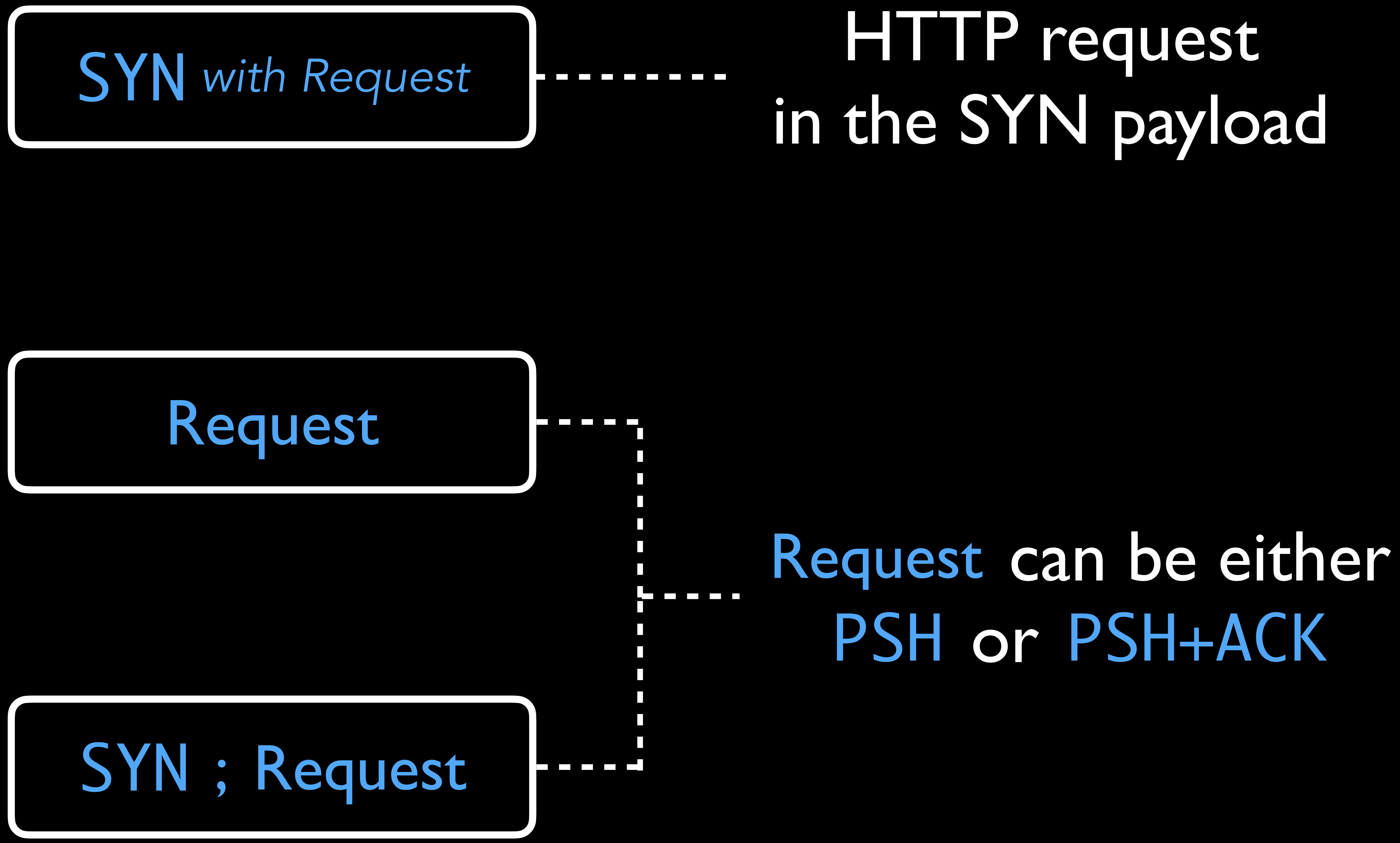
Request

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

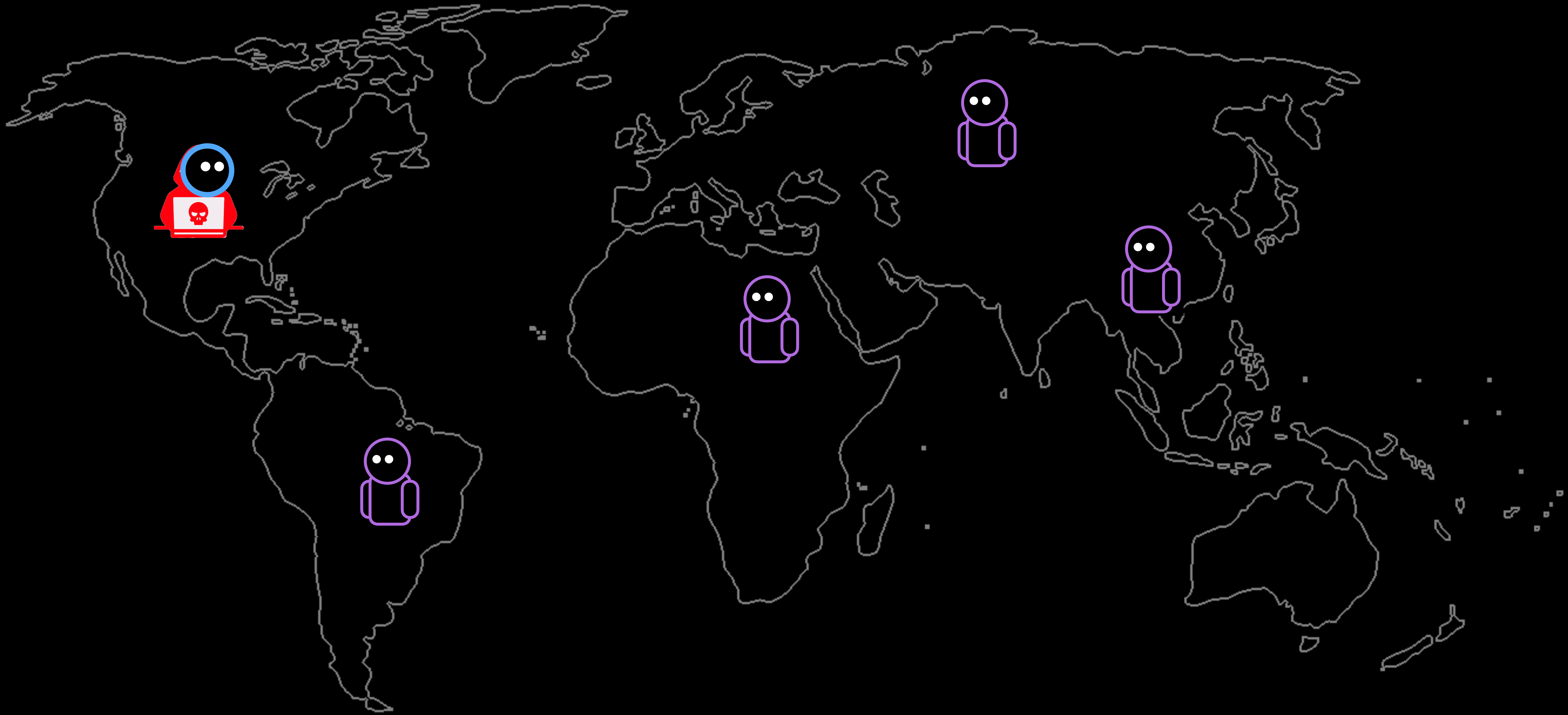
www.youporn.com	porn
www.roxypalace.com	gambling
plus.google.com	social
www.bittorent.com	file sharing
www.survive.org.uk	sex health

Middleboxes differ in their bugs and their configurations

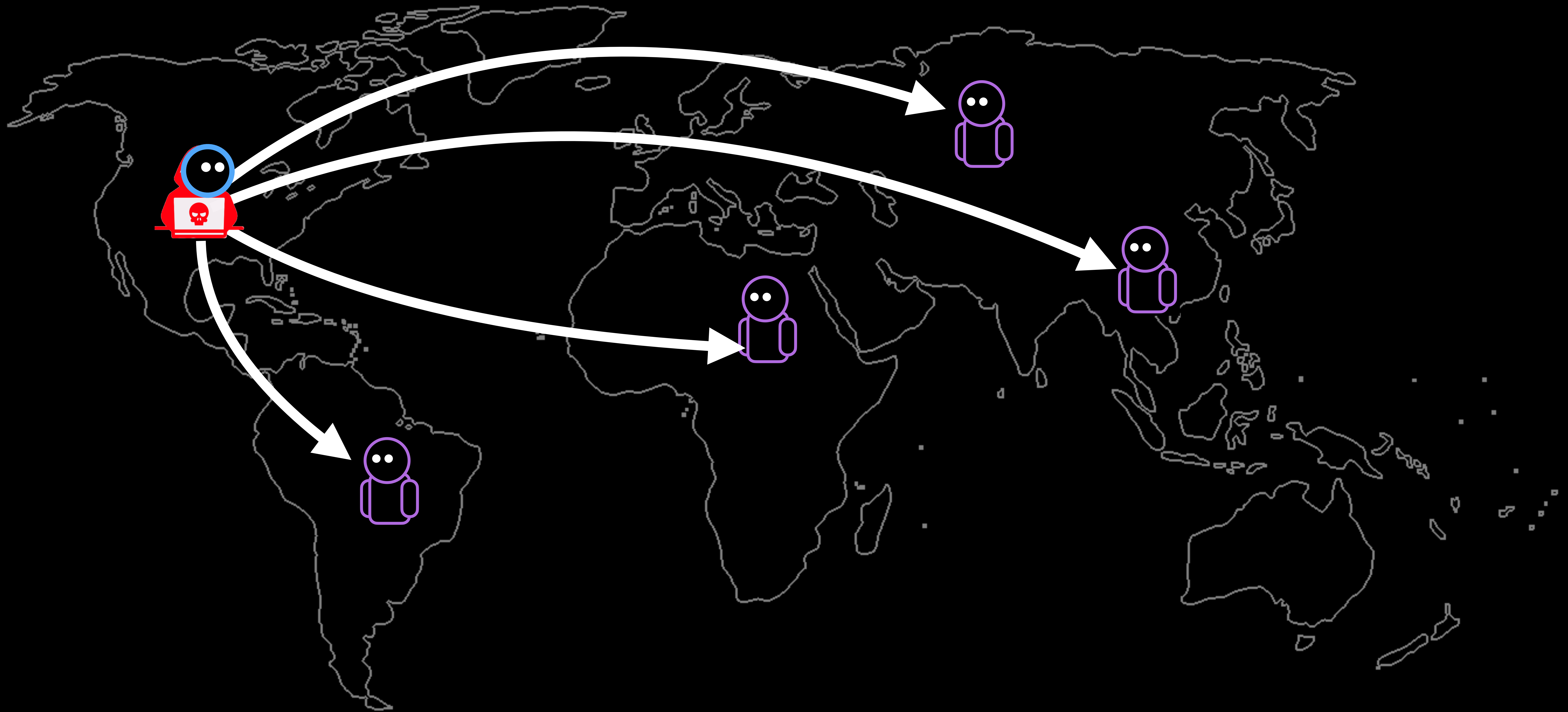
How can we evaluate this attack?

How can we evaluate this attack?

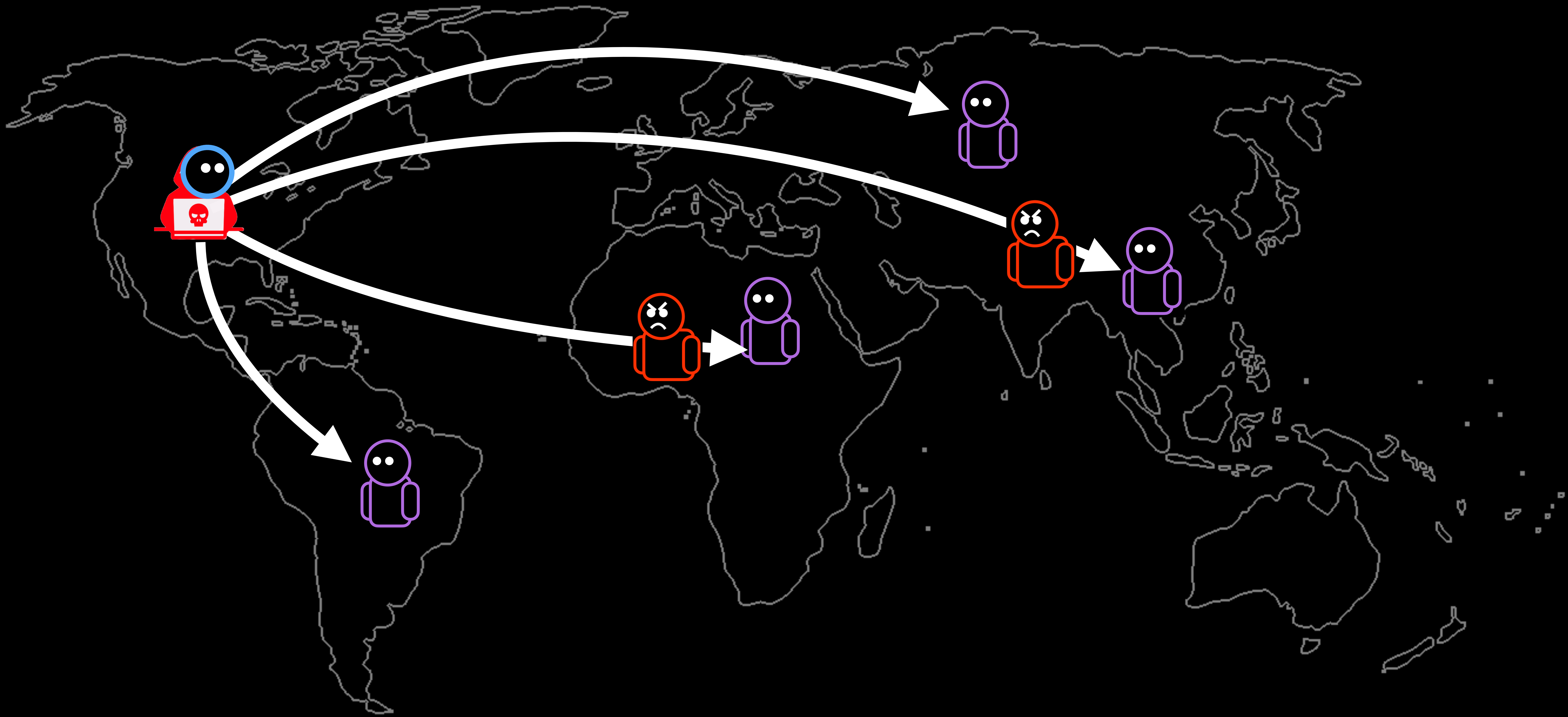
How can we evaluate this attack?



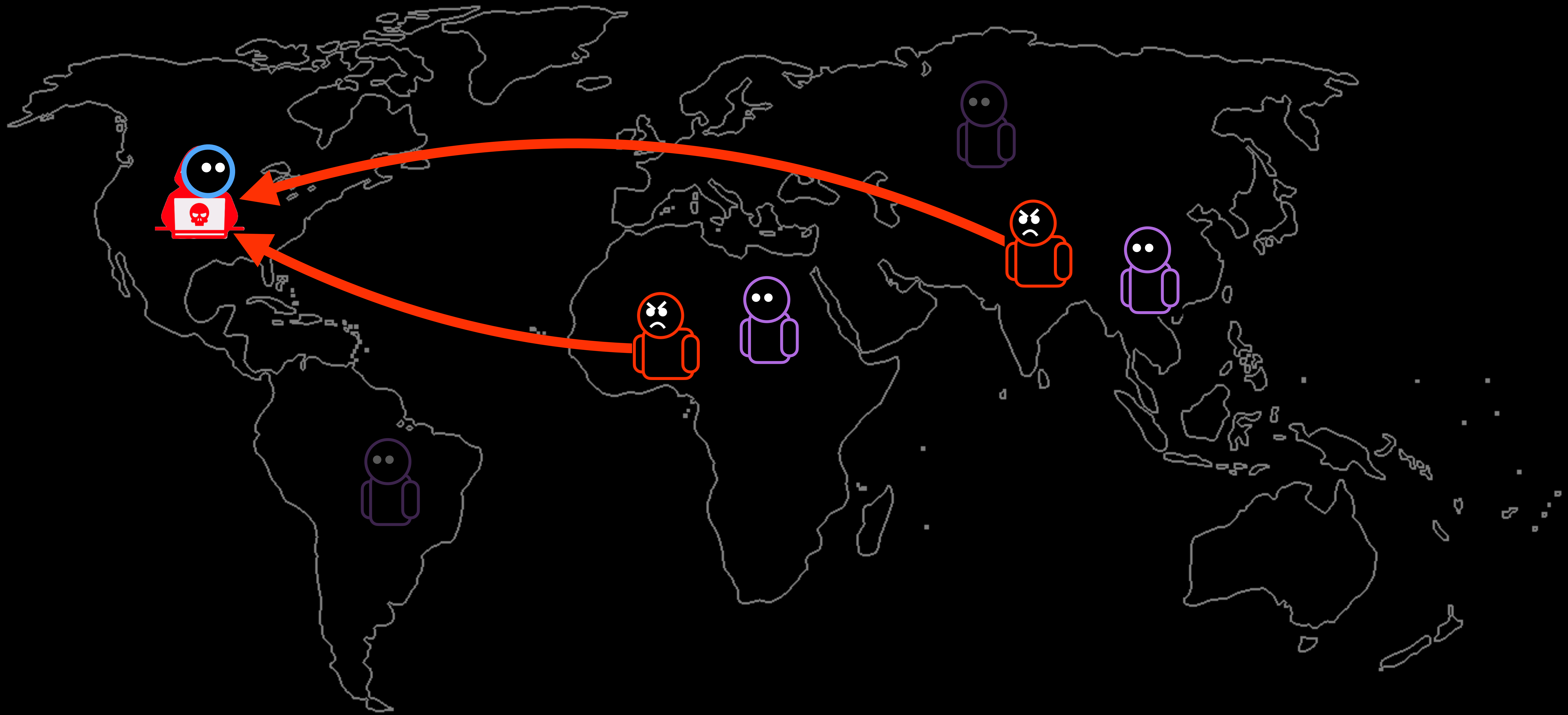
How can we evaluate this attack?



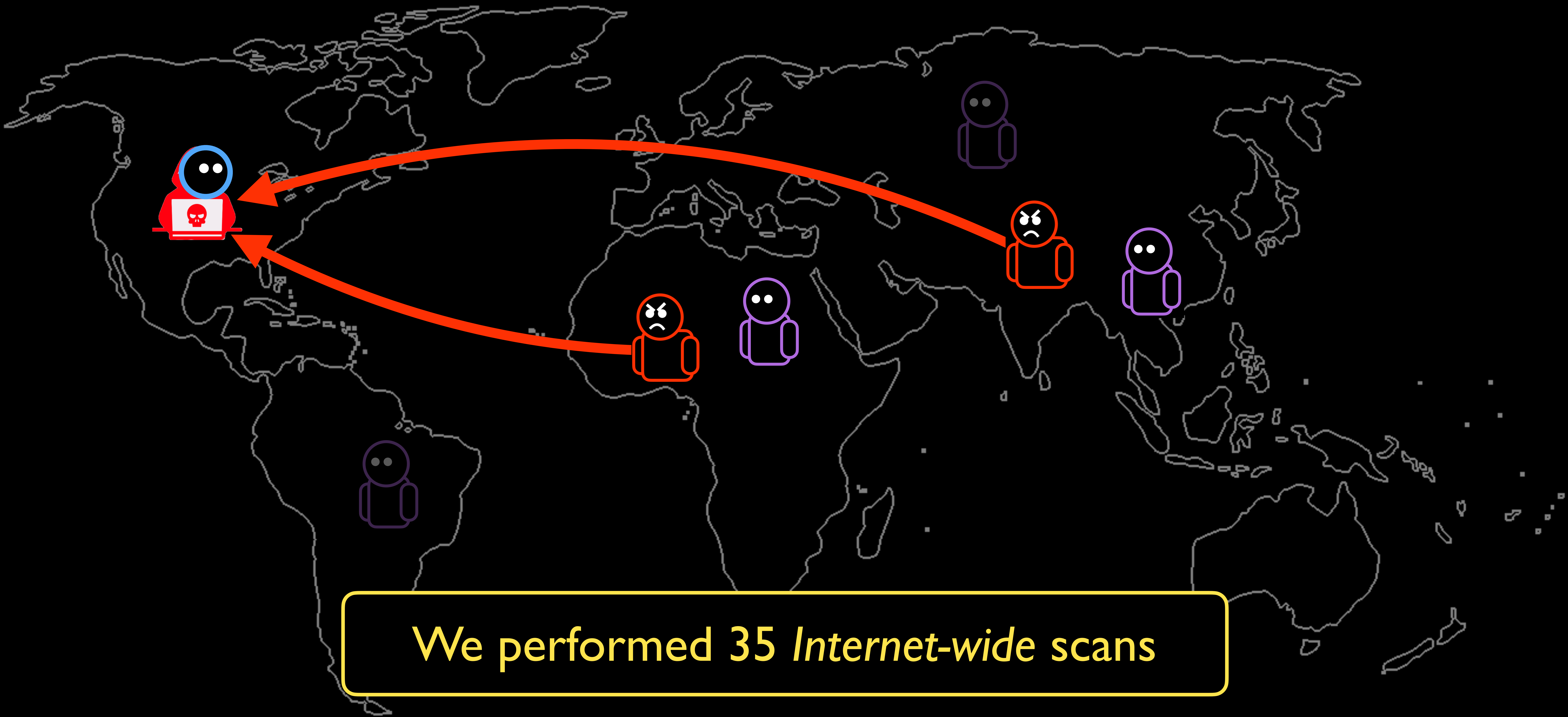
How can we evaluate this attack?



How can we evaluate this attack?

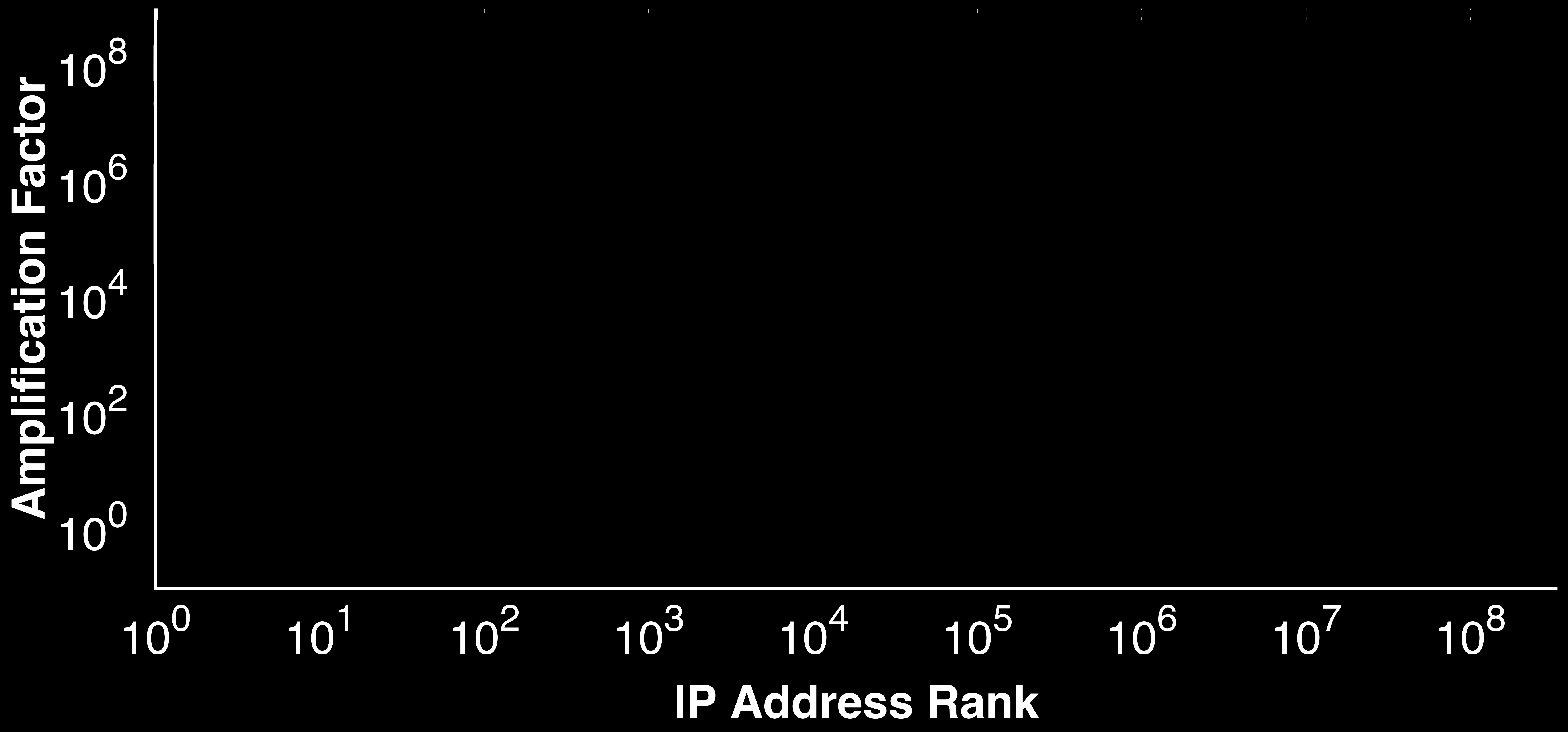


How can we evaluate this attack?

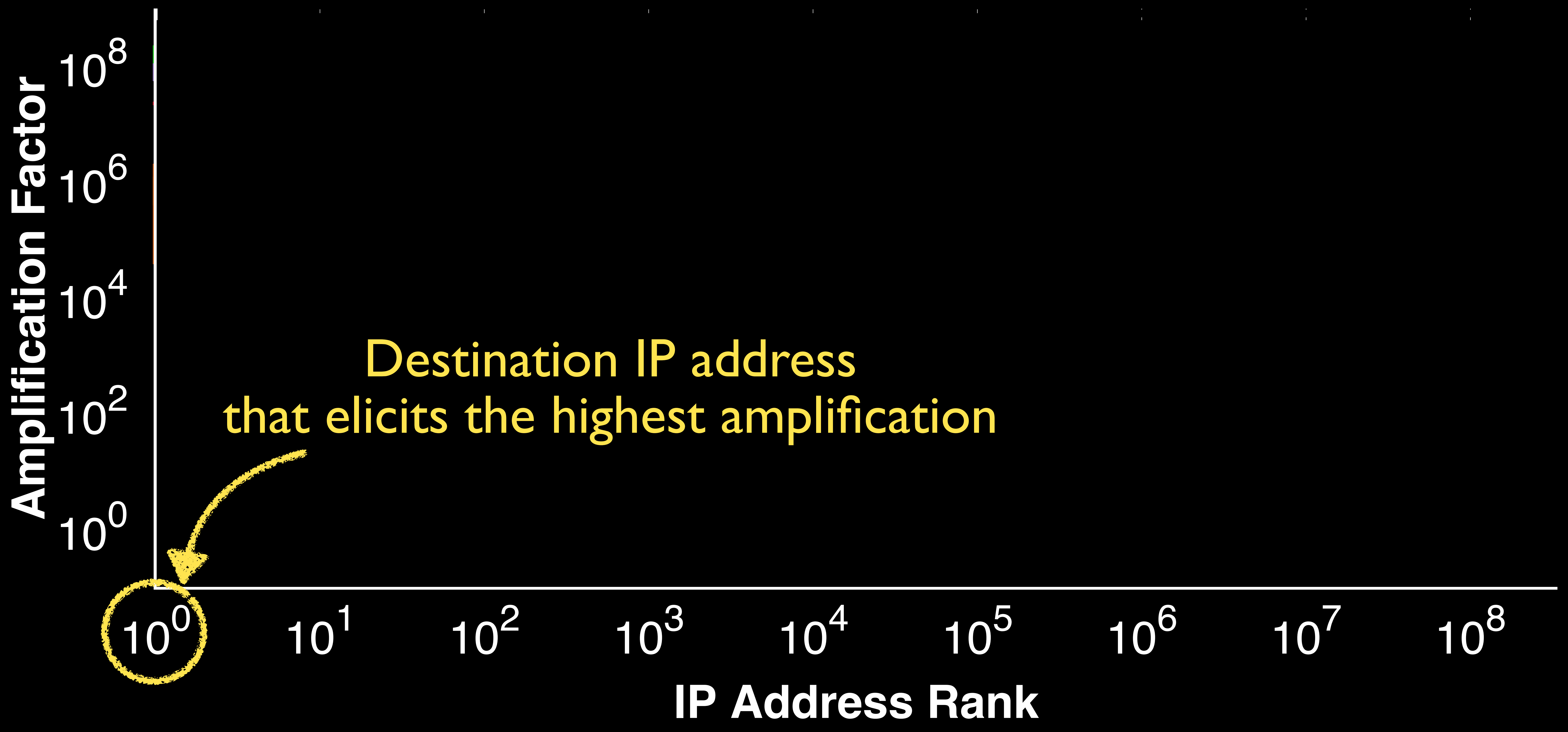


We performed 35 *Internet-wide* scans

Amplification by packet sequence

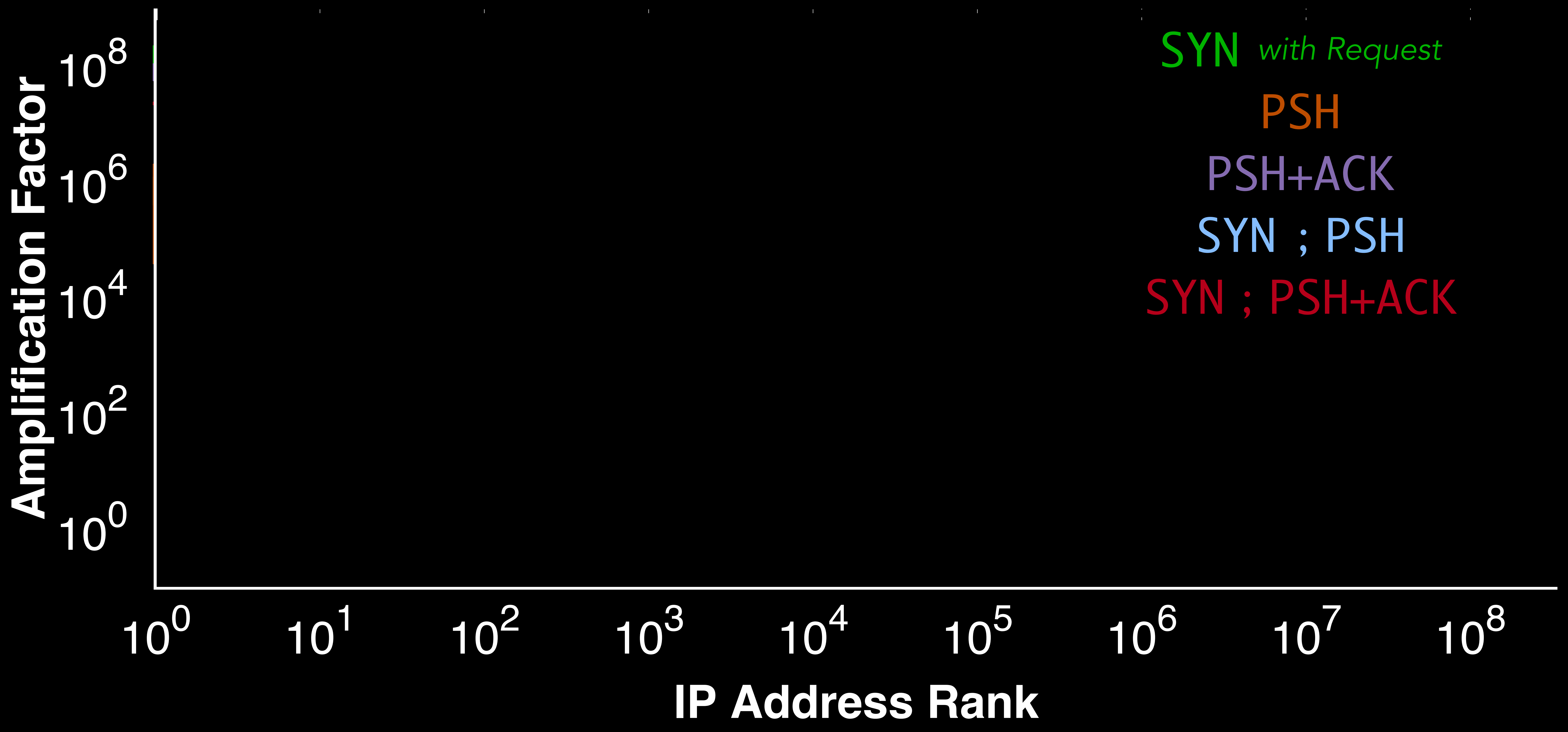


Amplification by packet sequence



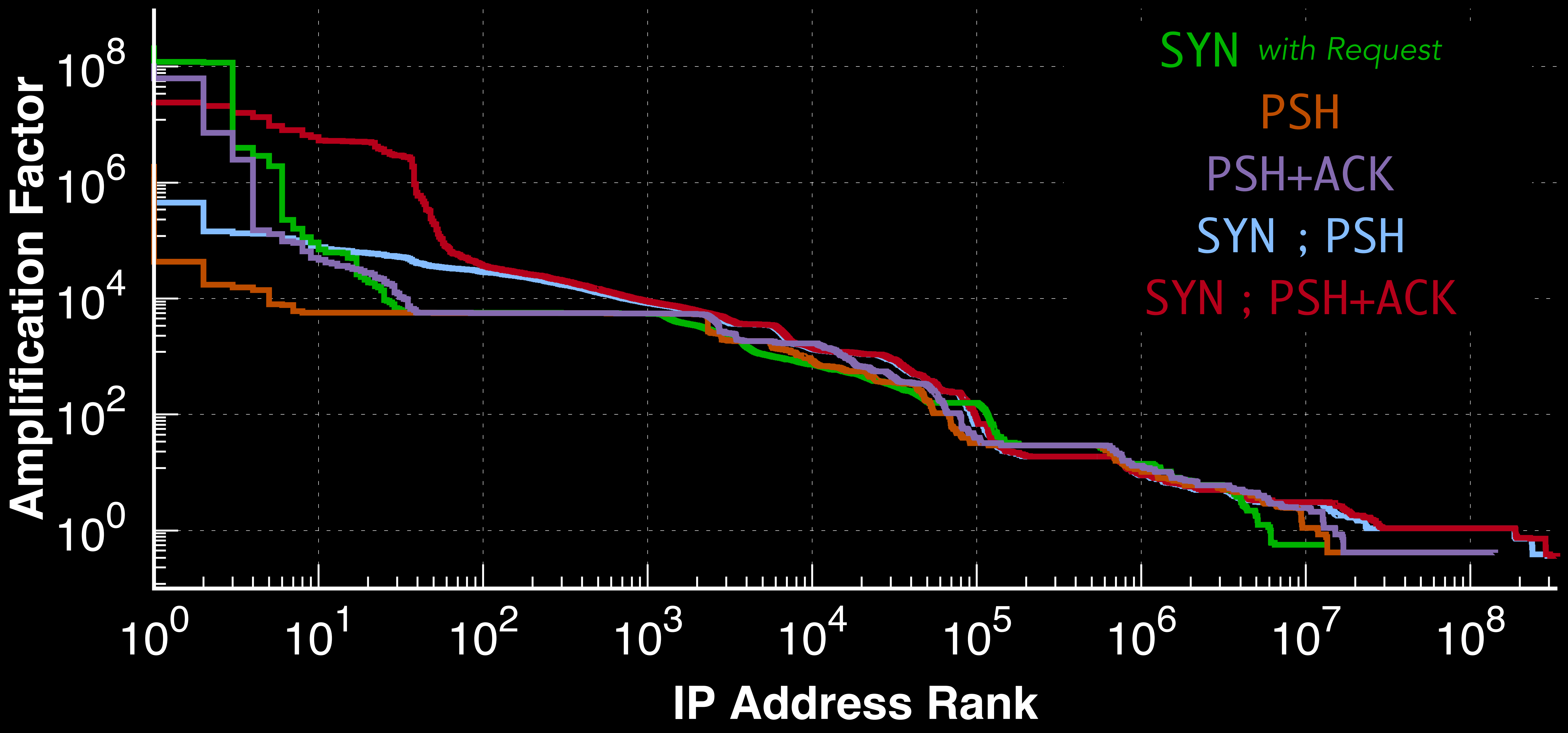
Destination IP address
that elicits the highest amplification

Amplification by packet sequence



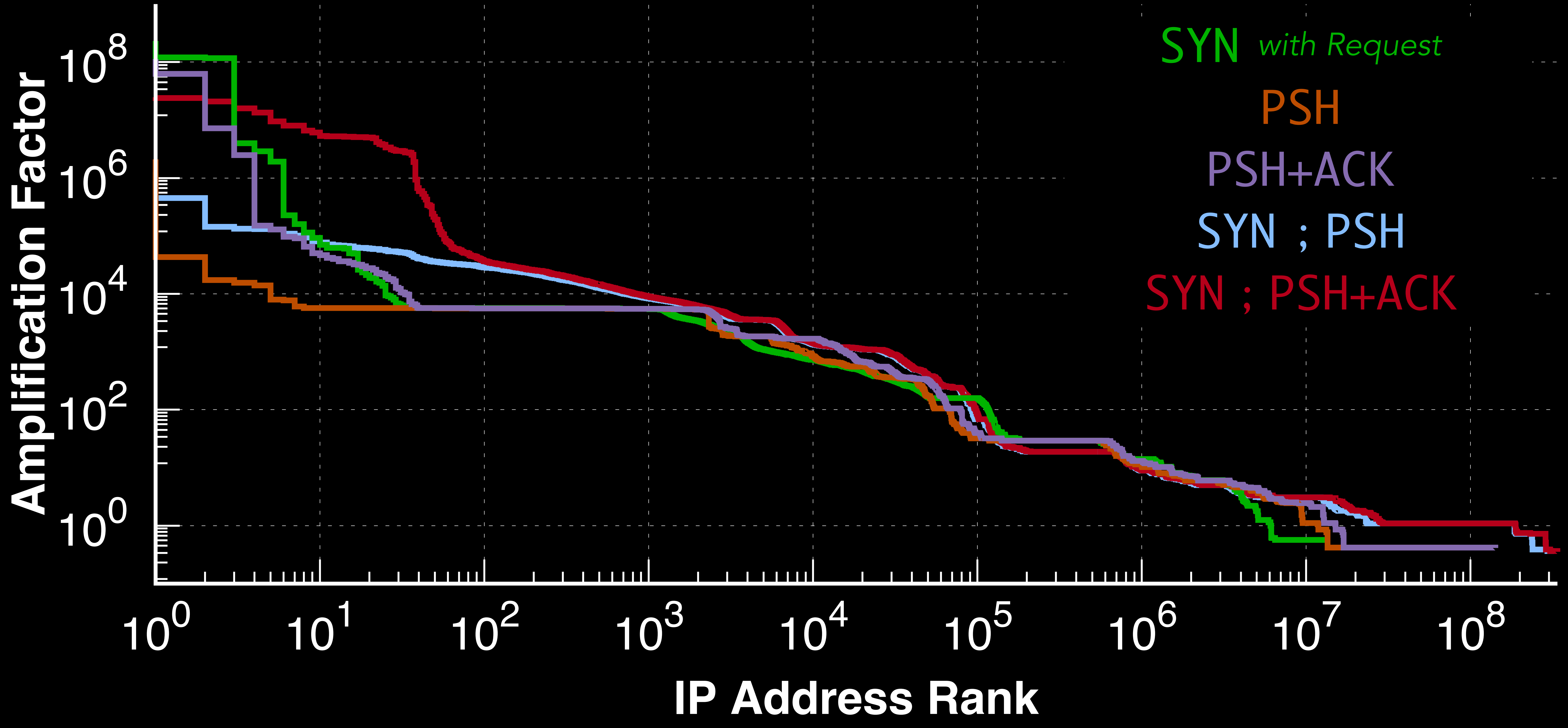
Amplification by packet sequence

Triggered with `www.youporn.com`



Amplification by packet sequence

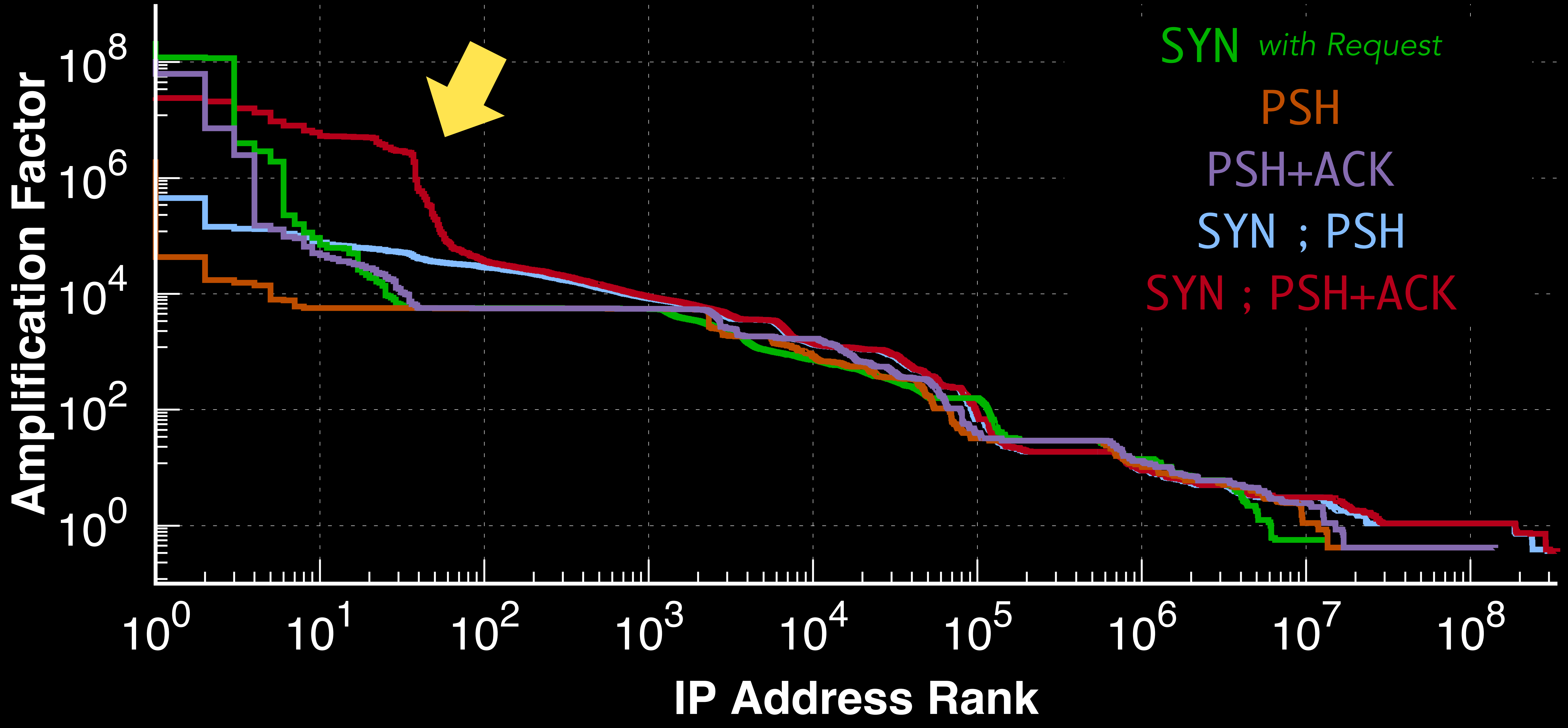
Triggered with `www.youporn.com`



Packet sequences differ in amplification and number of amplifiers

Amplification by packet sequence

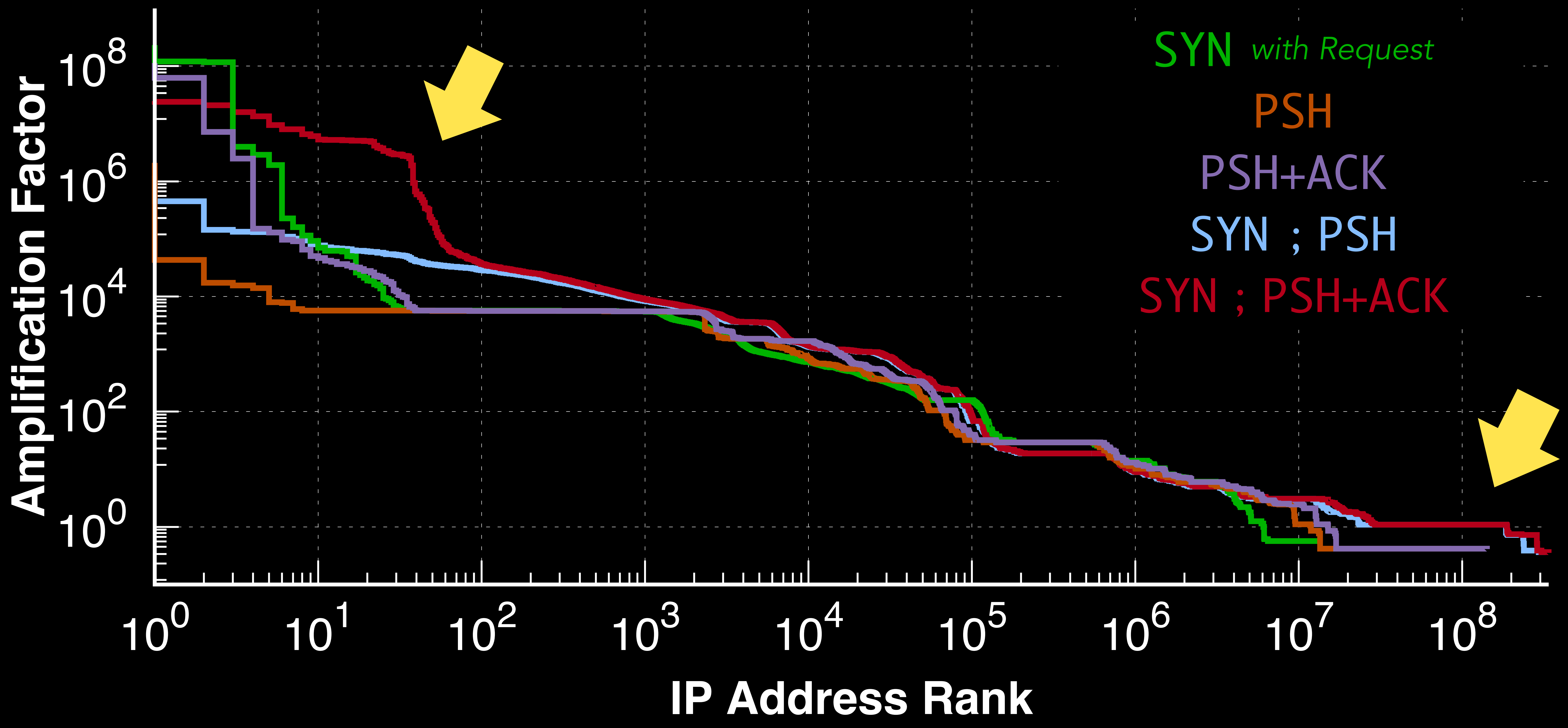
Triggered with `www.youporn.com`



Packet sequences differ in amplification and number of amplifiers

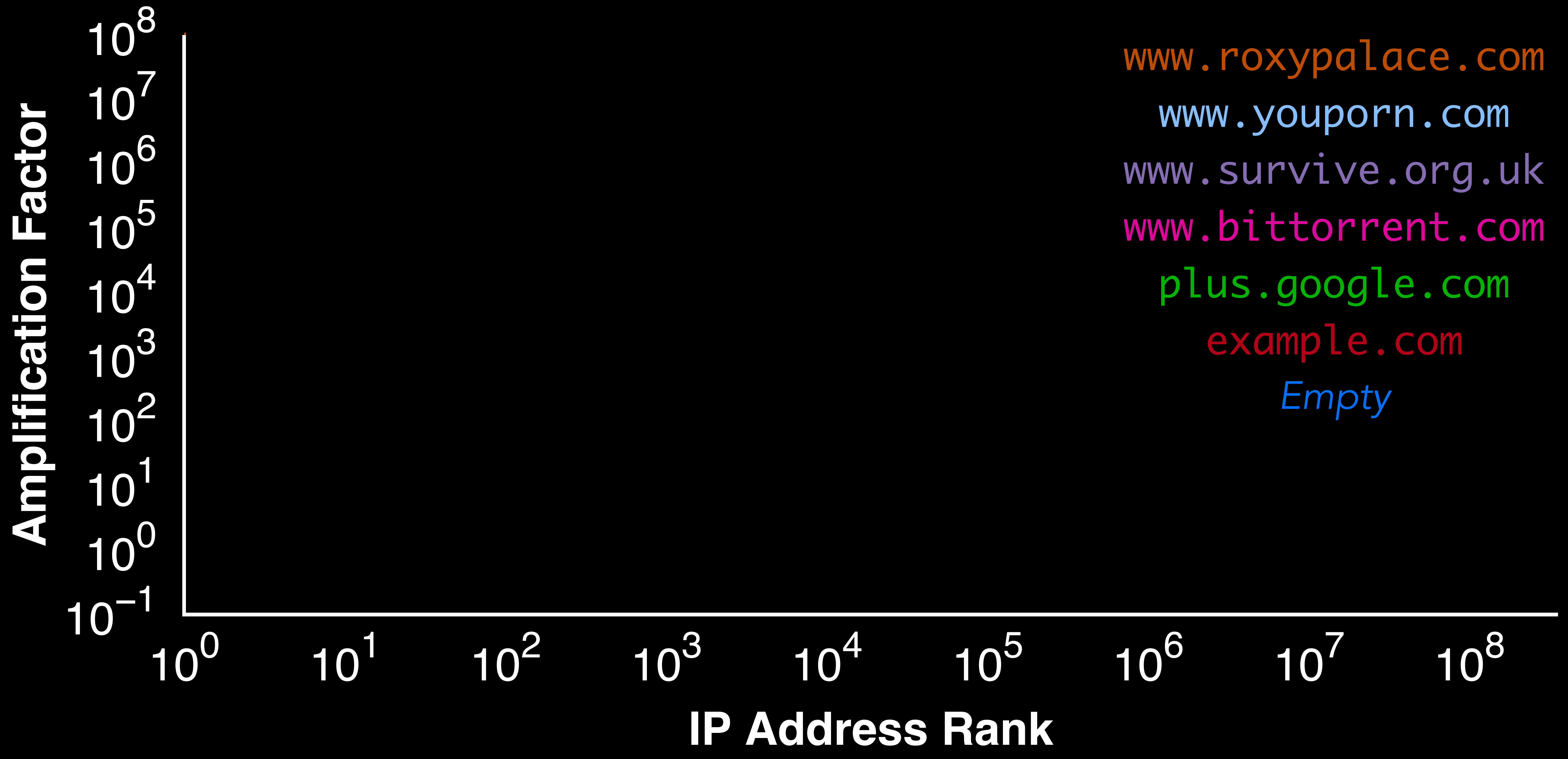
Amplification by packet sequence

Triggered with `www.youporn.com`

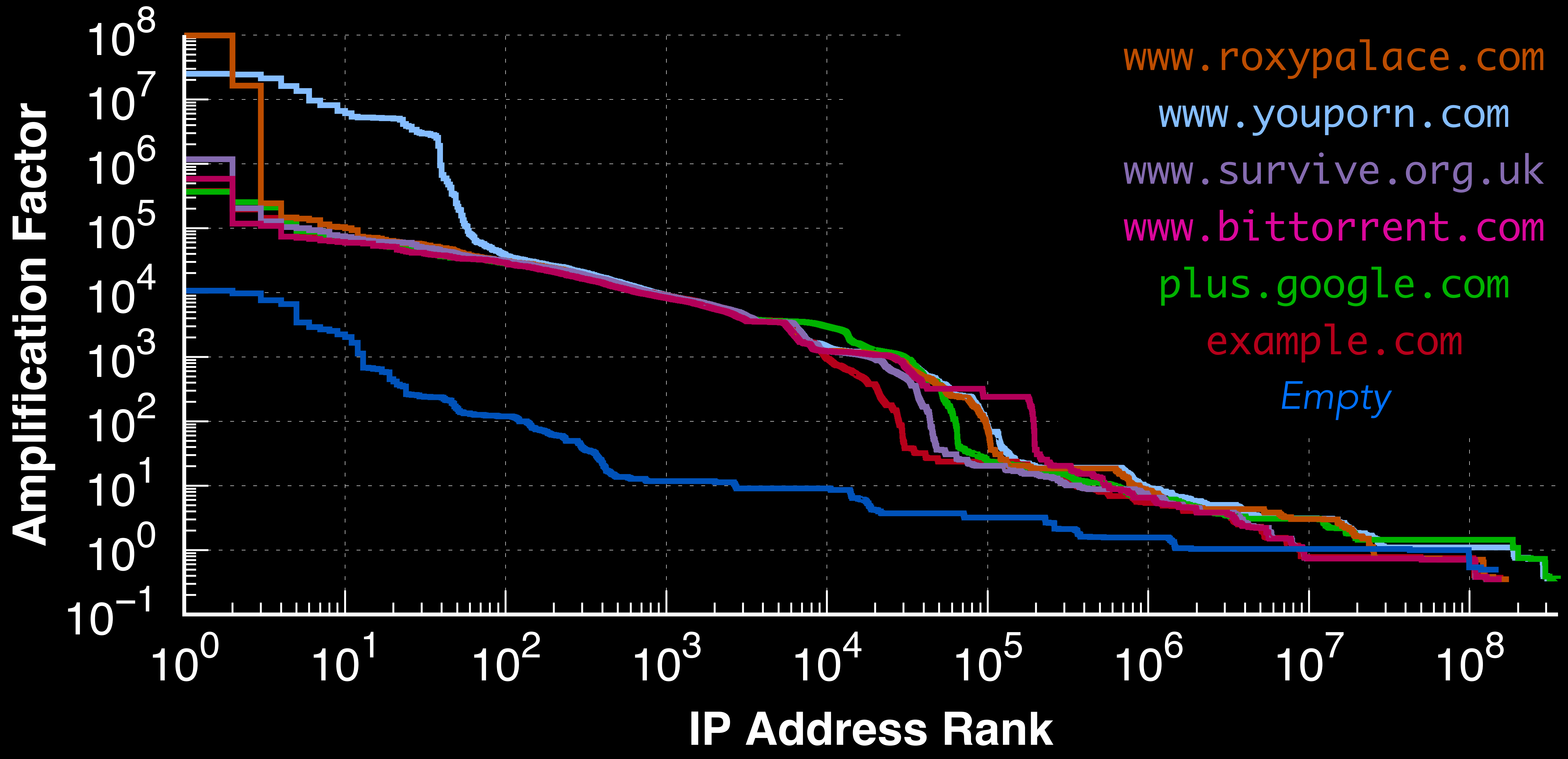


Packet sequences differ in amplification and number of amplifiers

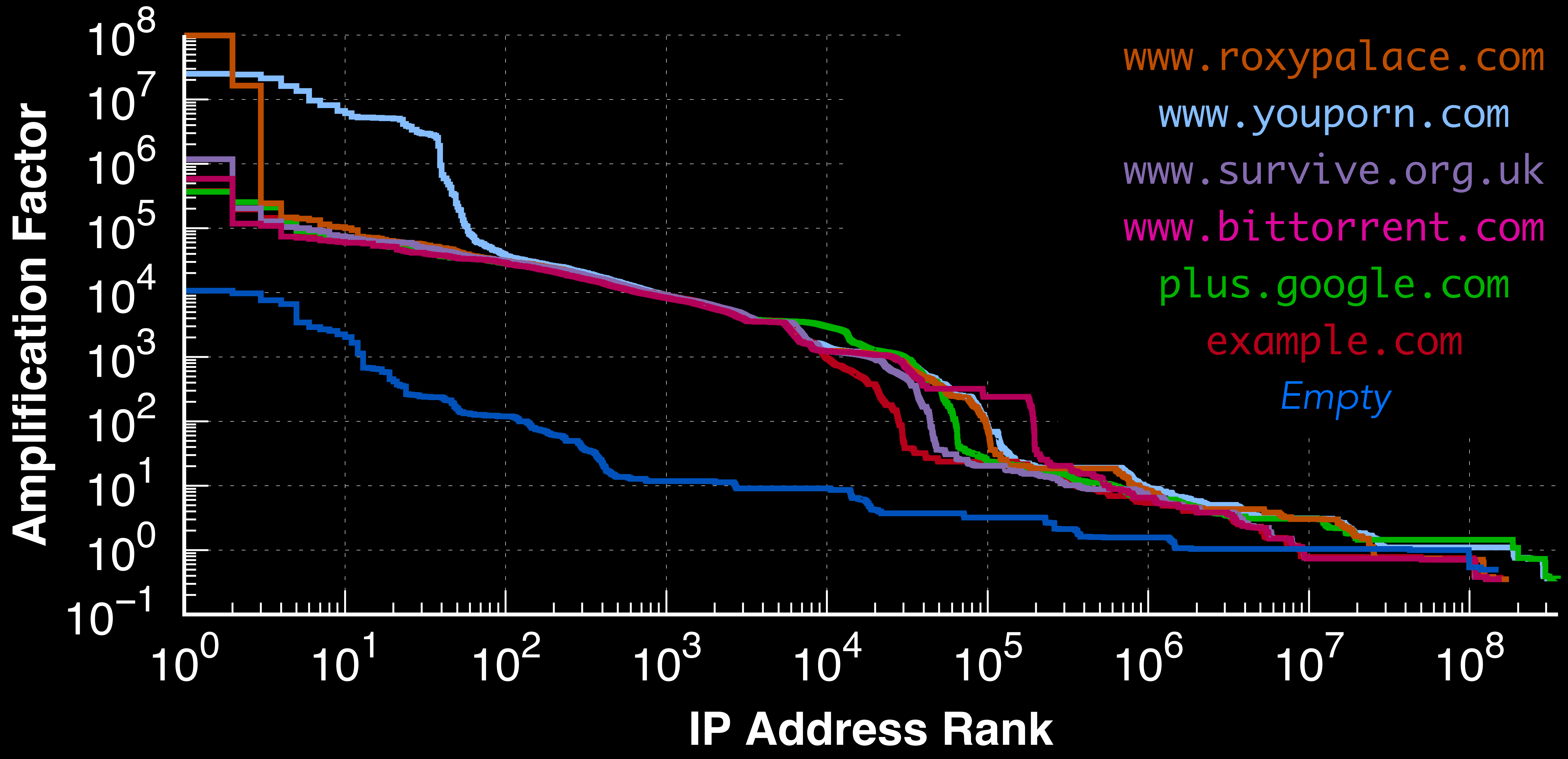
Amplification by triggering domain



Amplification by triggering domain



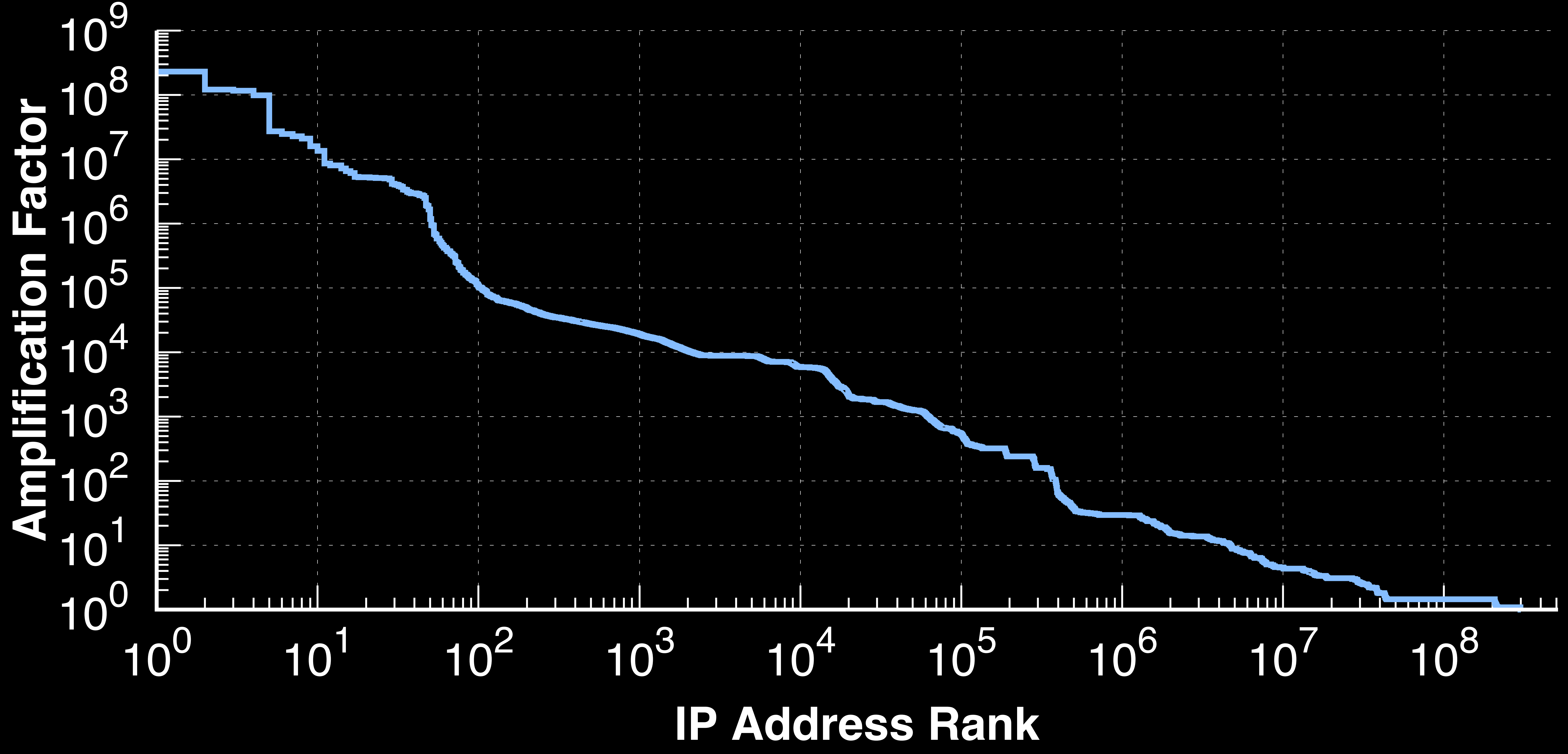
Amplification by triggering domain



Different triggering domains can yield drastically different amplification

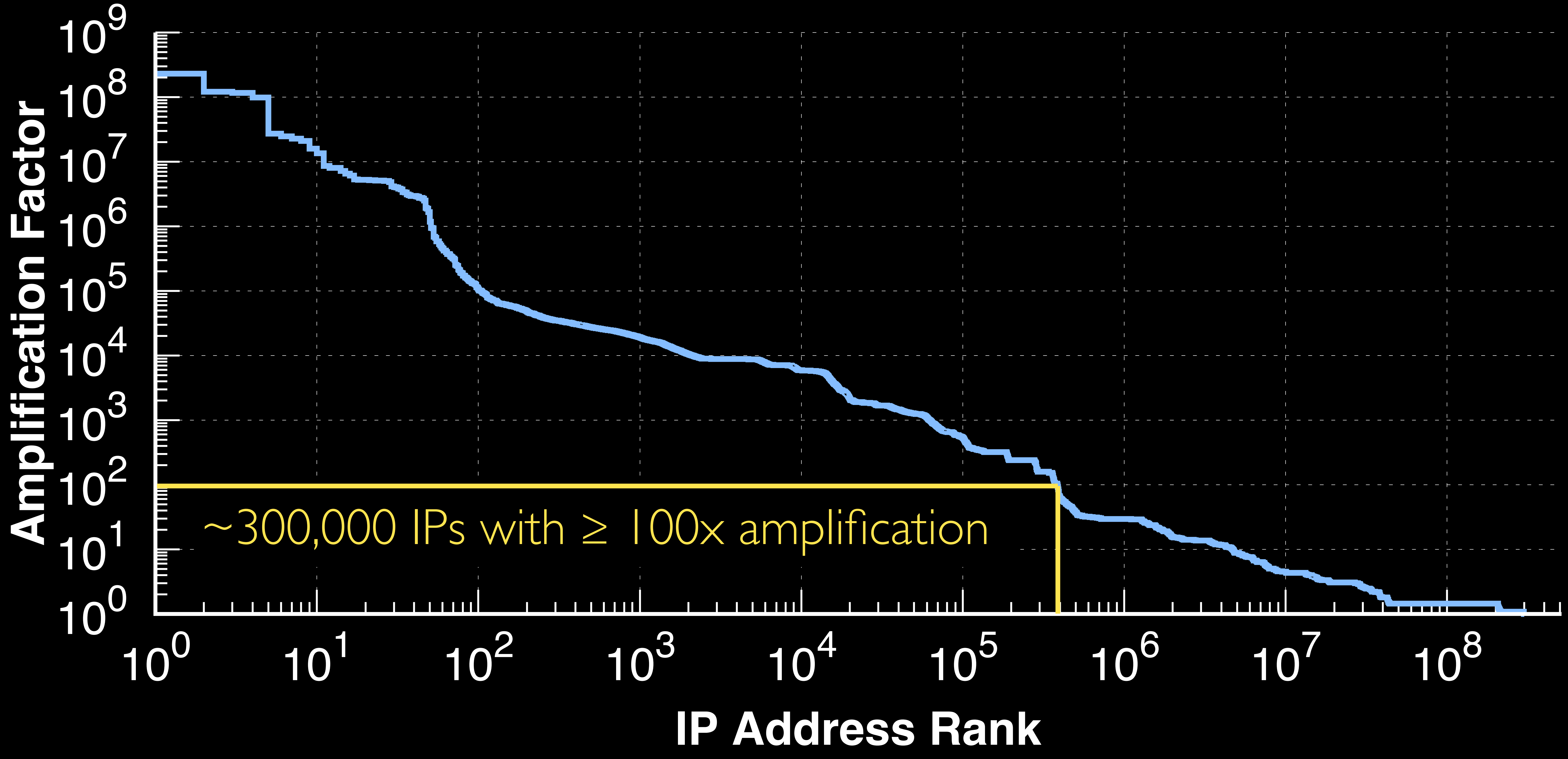
Maximum amplification

Assuming a perfectly-informed attacker



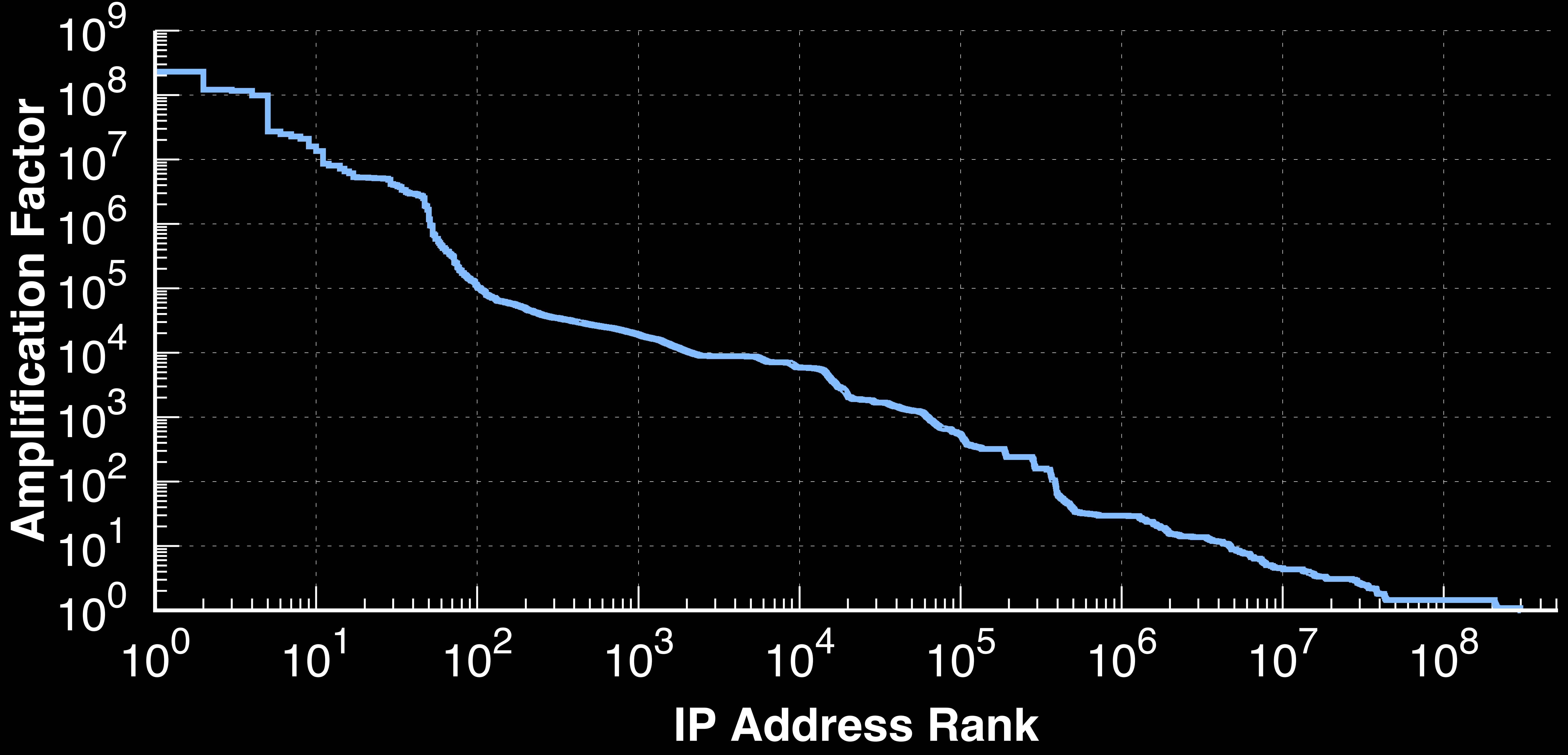
Maximum amplification

Assuming a perfectly-informed attacker



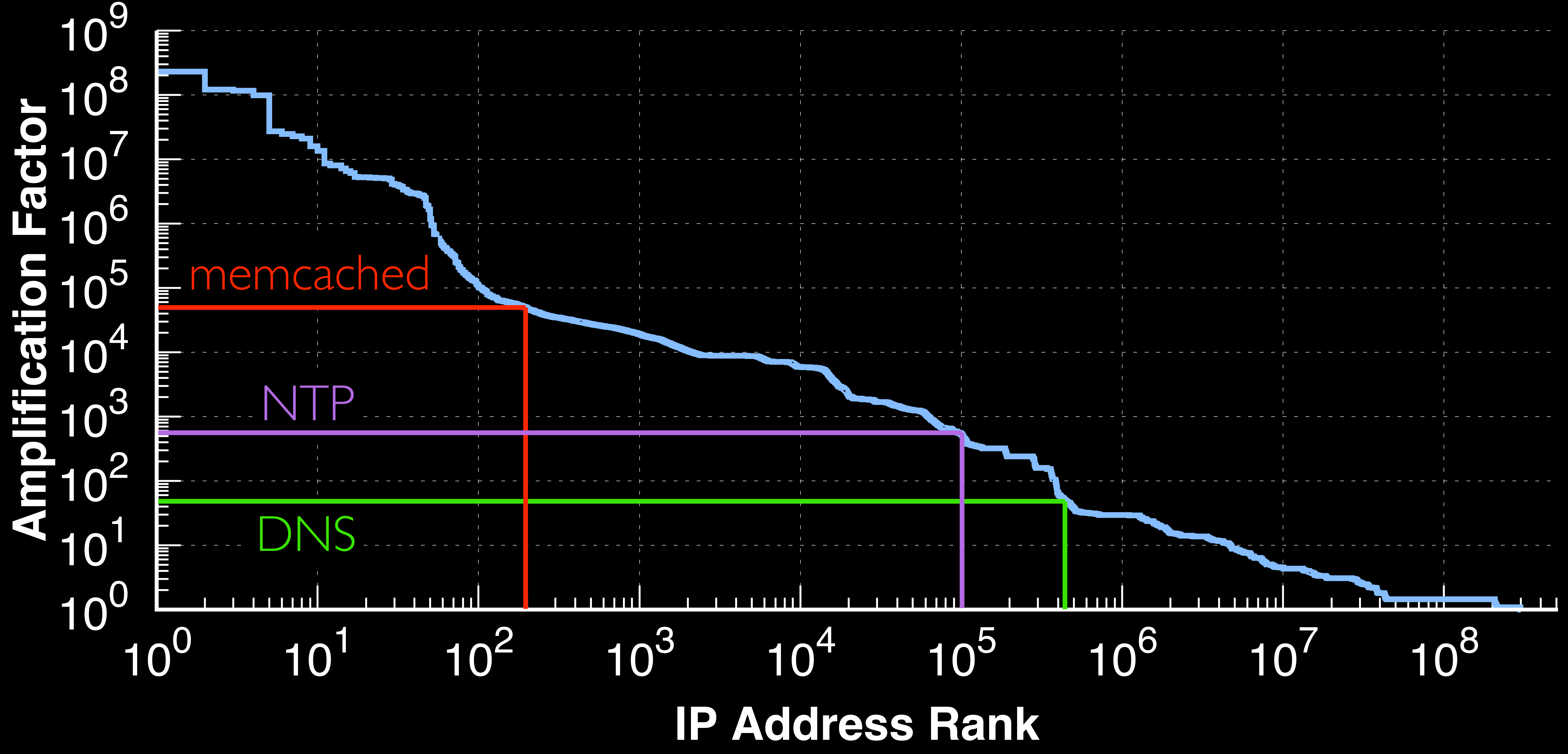
Maximum amplification

Assuming a perfectly-informed attacker



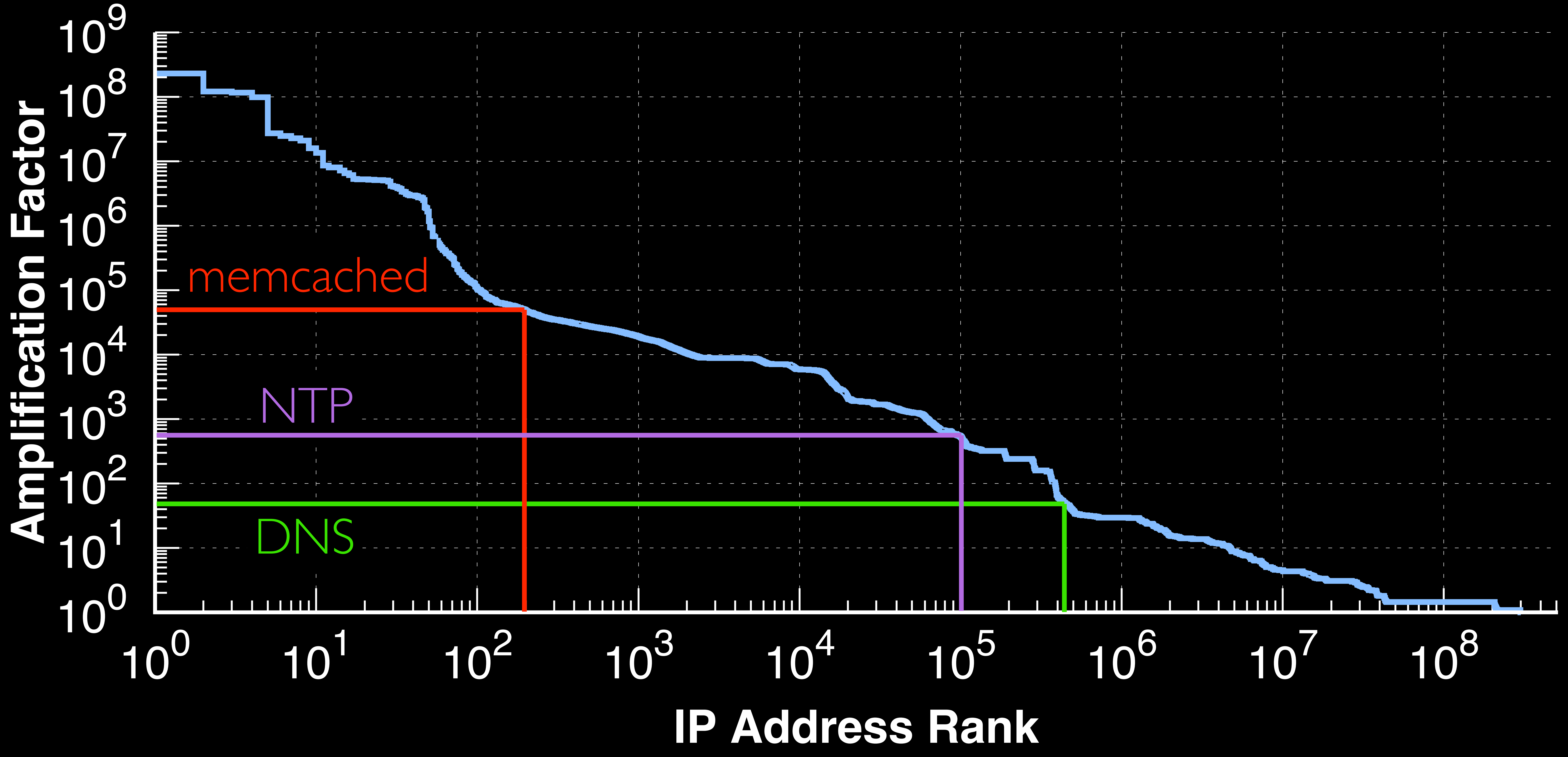
Maximum amplification

Assuming a perfectly-informed attacker



Maximum amplification

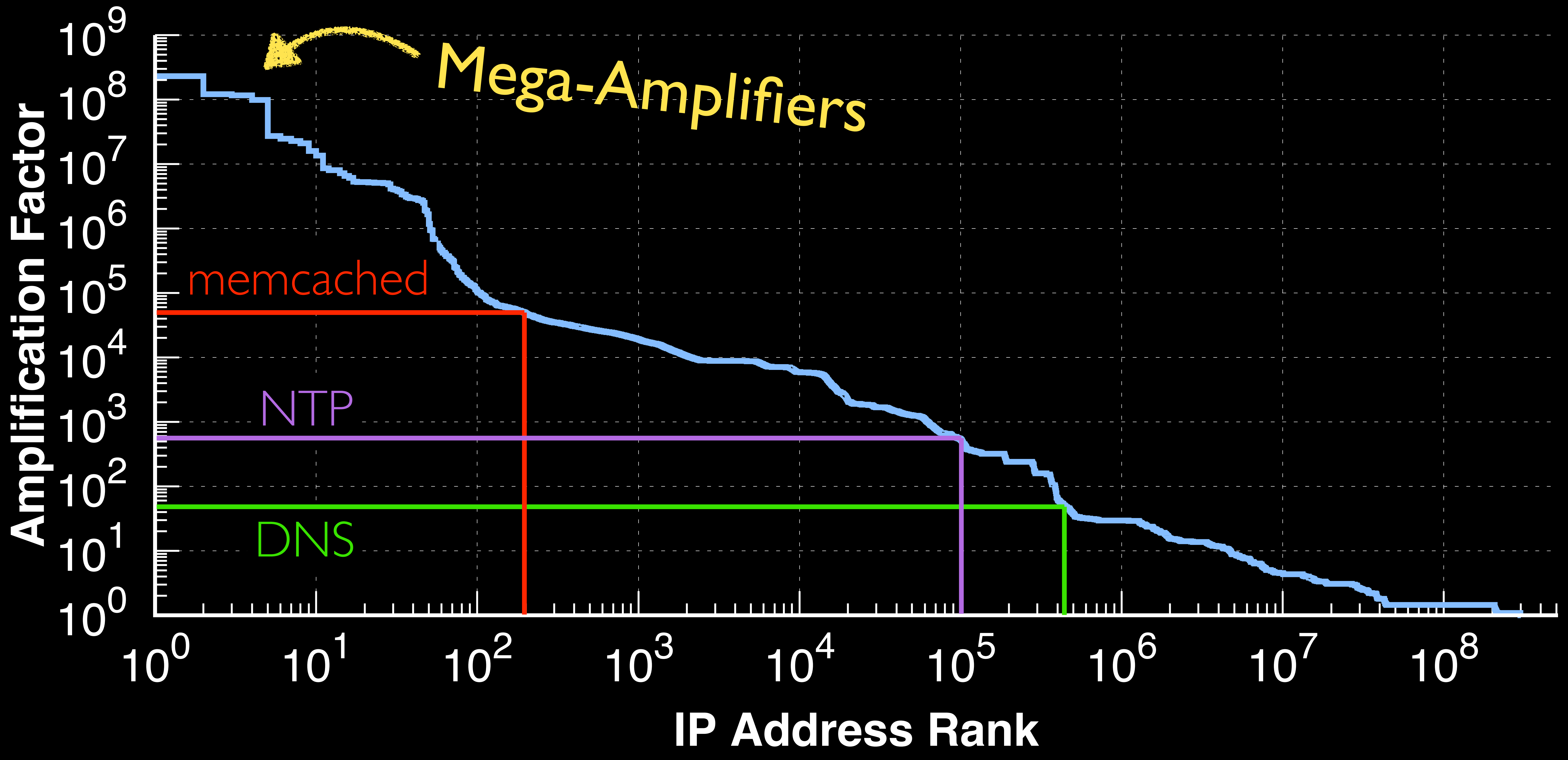
Assuming a perfectly-informed attacker



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

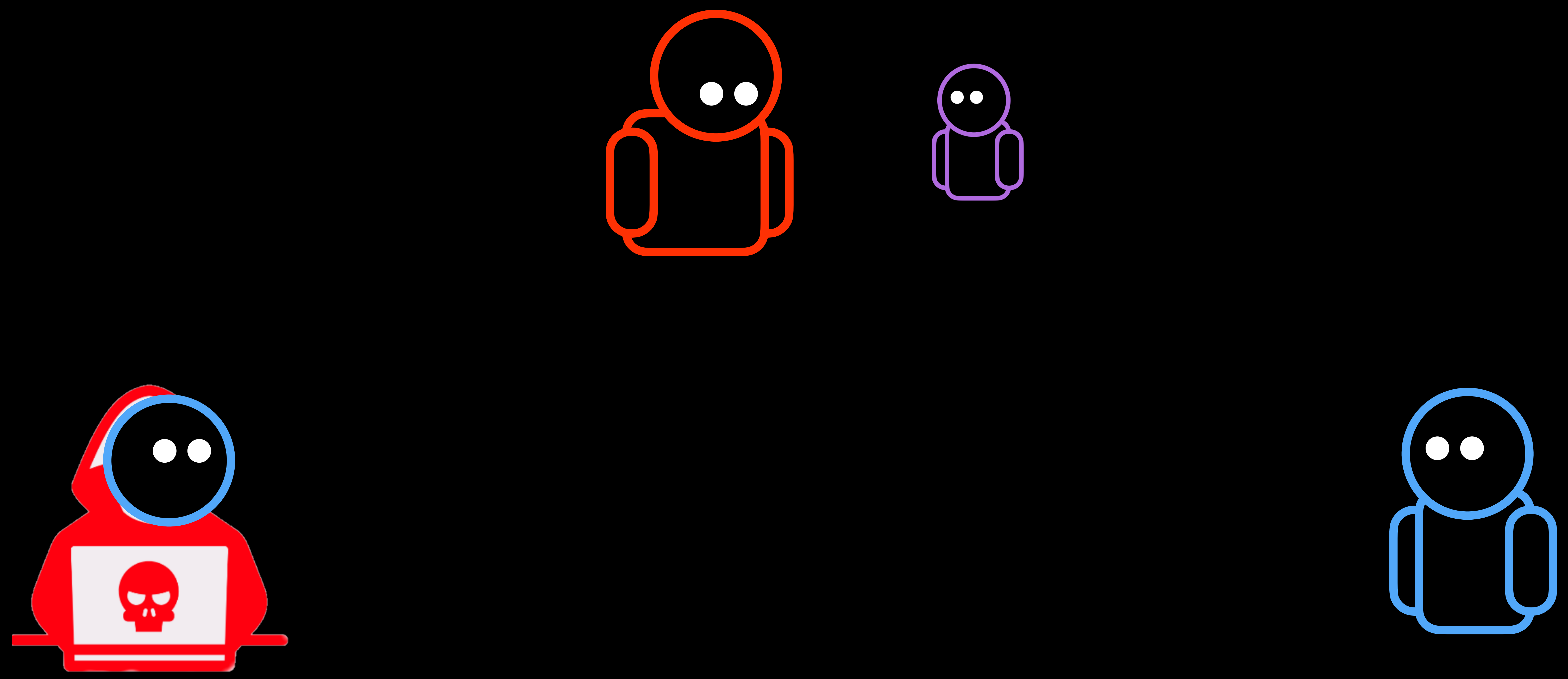
Maximum amplification

Assuming a perfectly-informed attacker

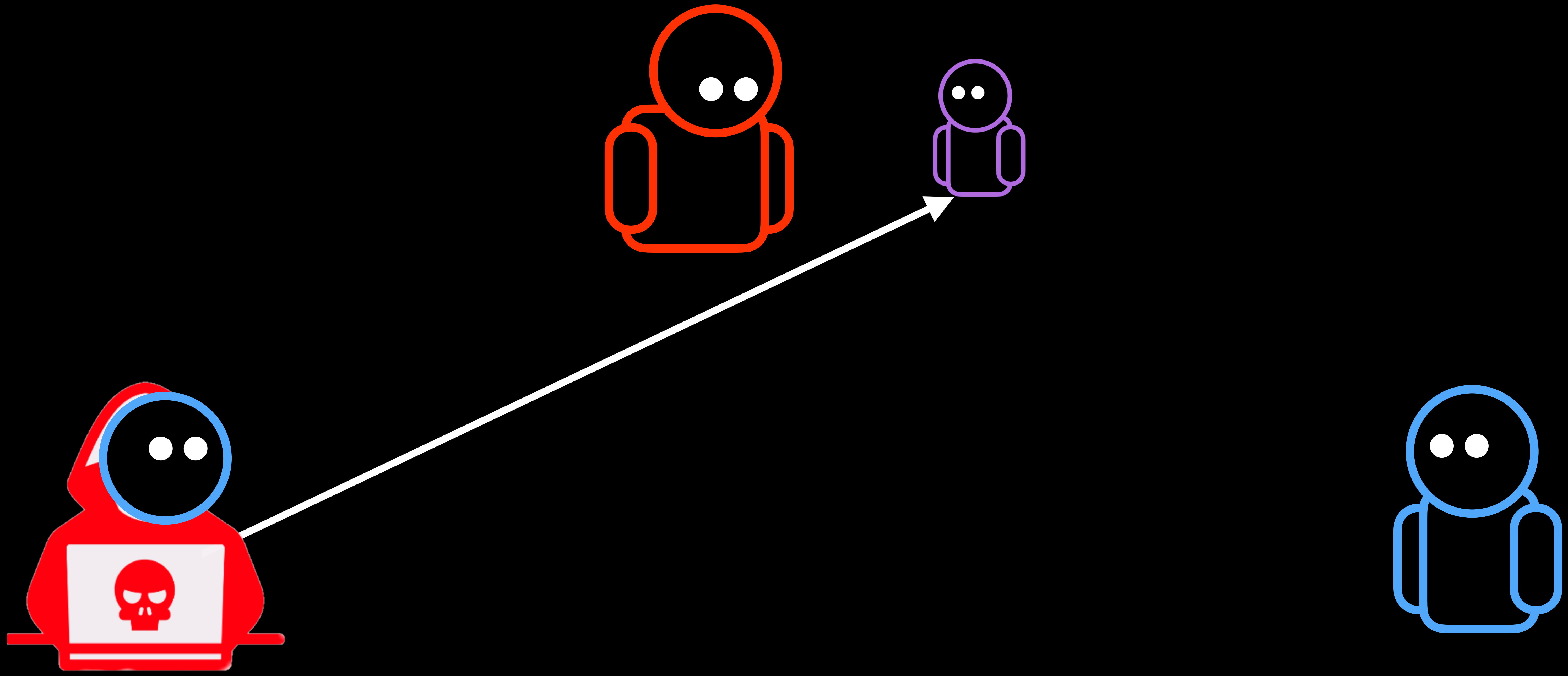


TCP-based amplification is at least as powerful as UDP-based alternatives

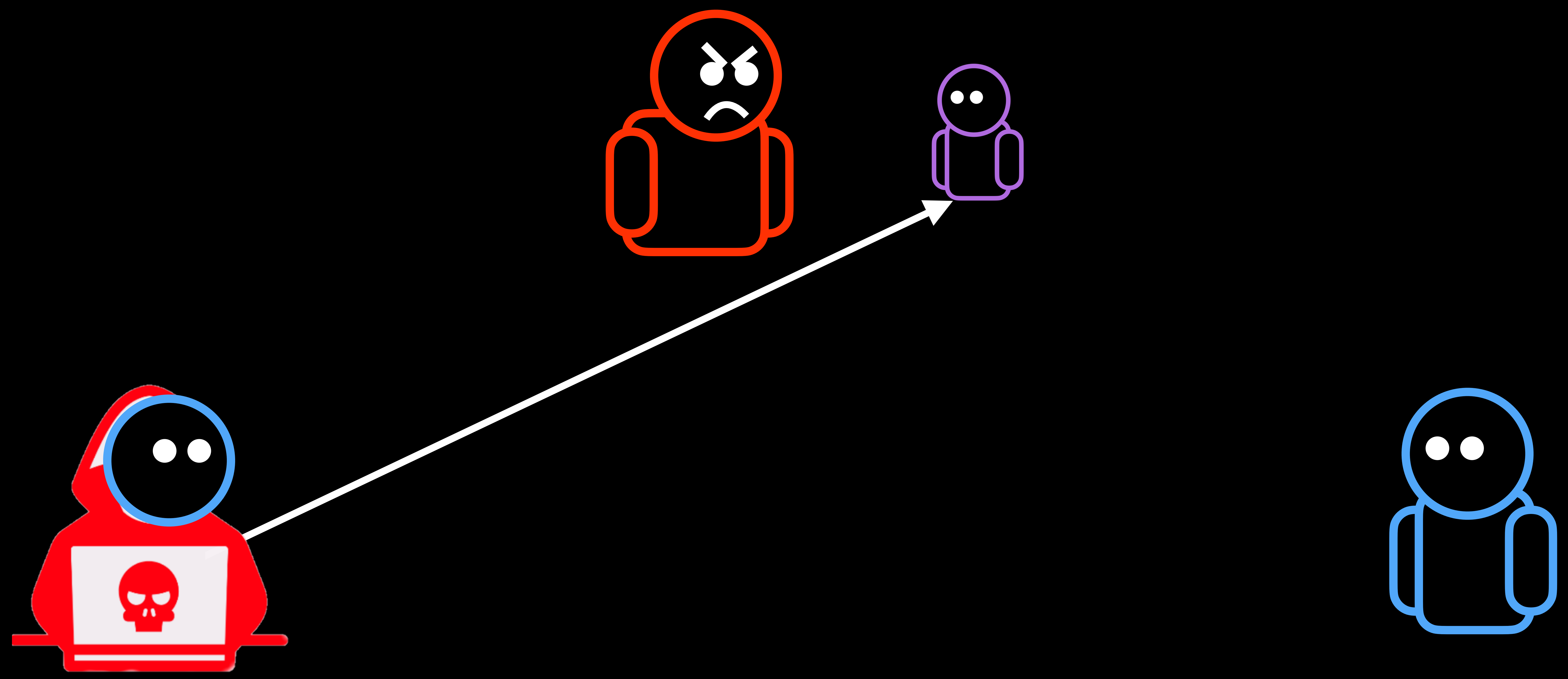
Mega-amplifier cause #1: Victim-sustained loops



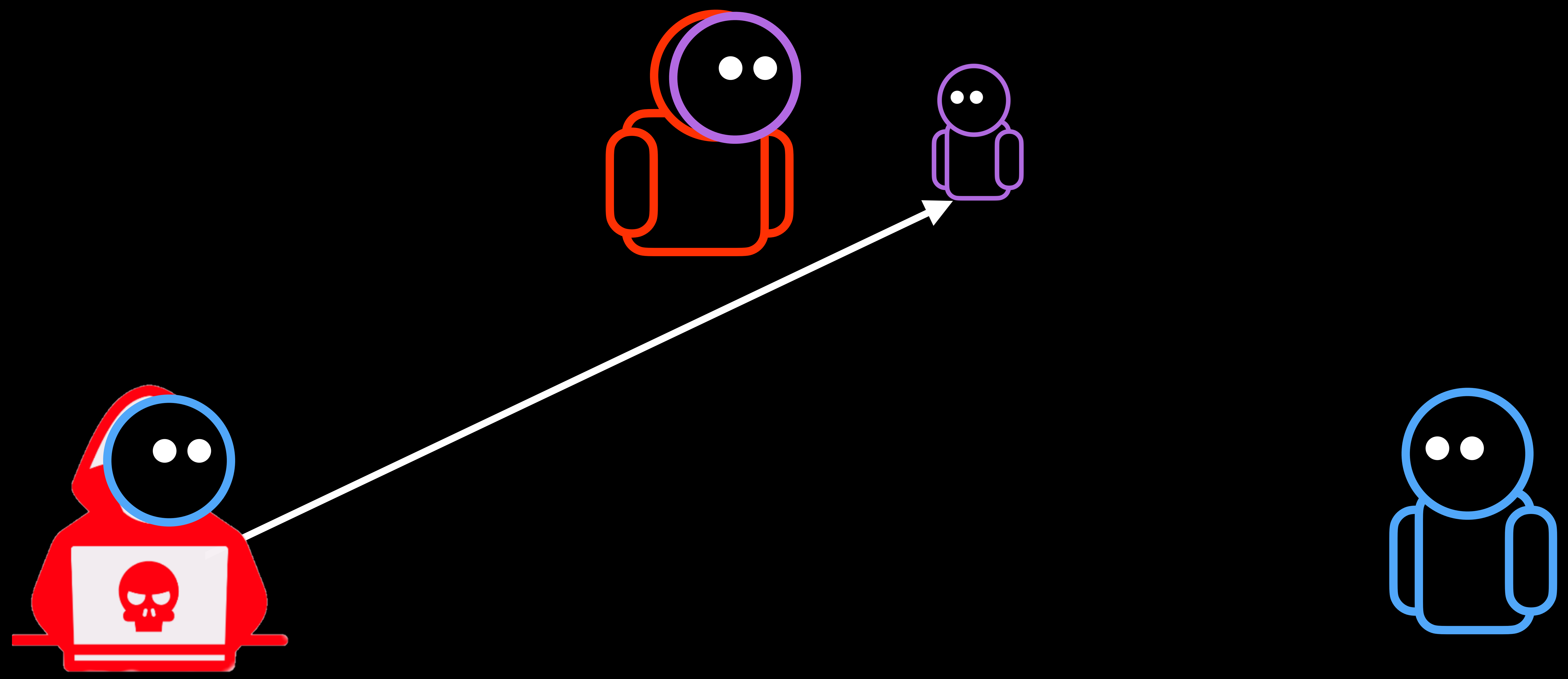
Mega-amplifier cause #1: Victim-sustained loops



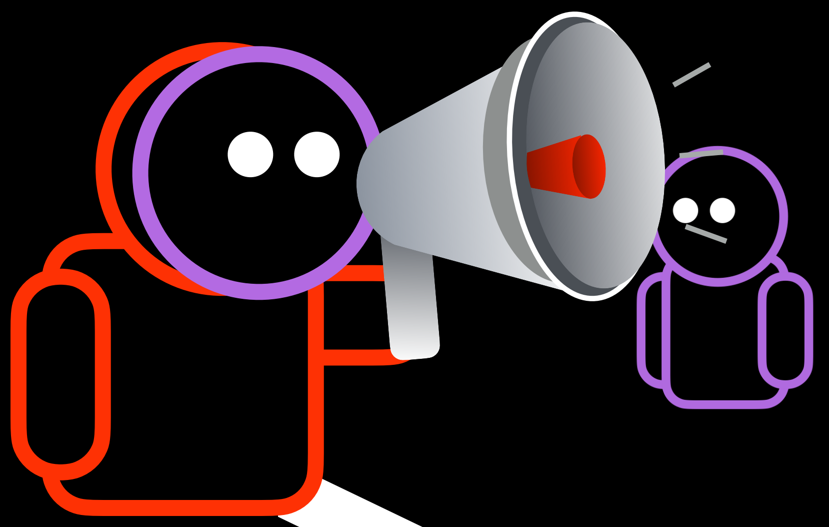
Mega-amplifier cause #1: Victim-sustained loops

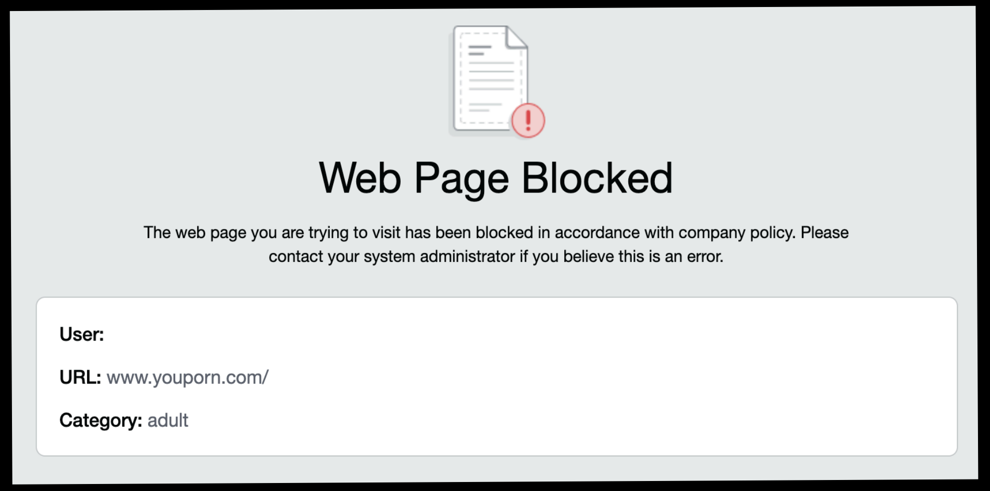


Mega-amplifier cause #1: Victim-sustained loops



Mega-amplifier cause #1: Victim-sustained loops





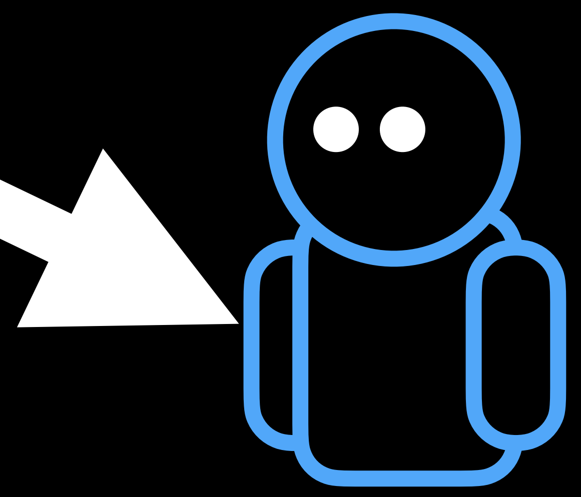
Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

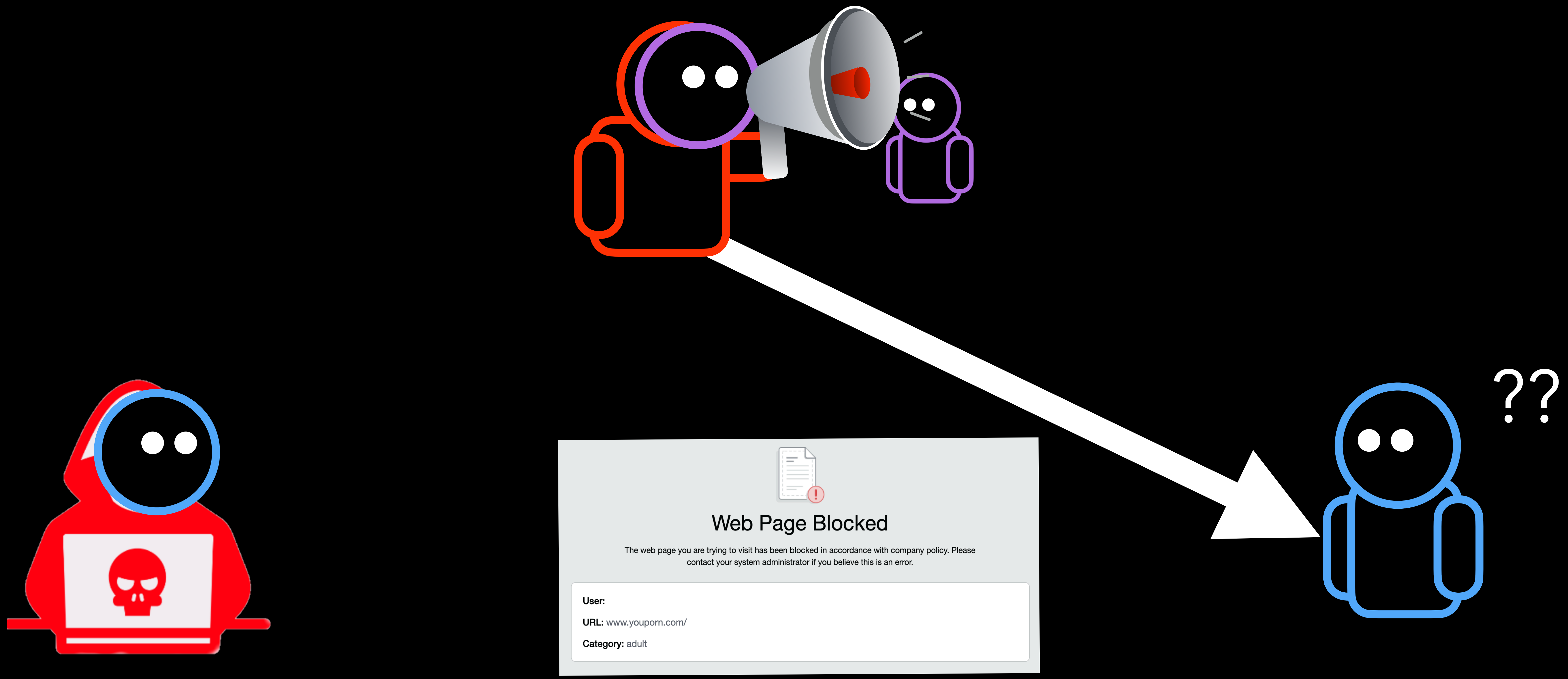
User:

URL: www.youporn.com/

Category: adult



Mega-amplifier cause #1: Victim-sustained loops



Web Page Blocked

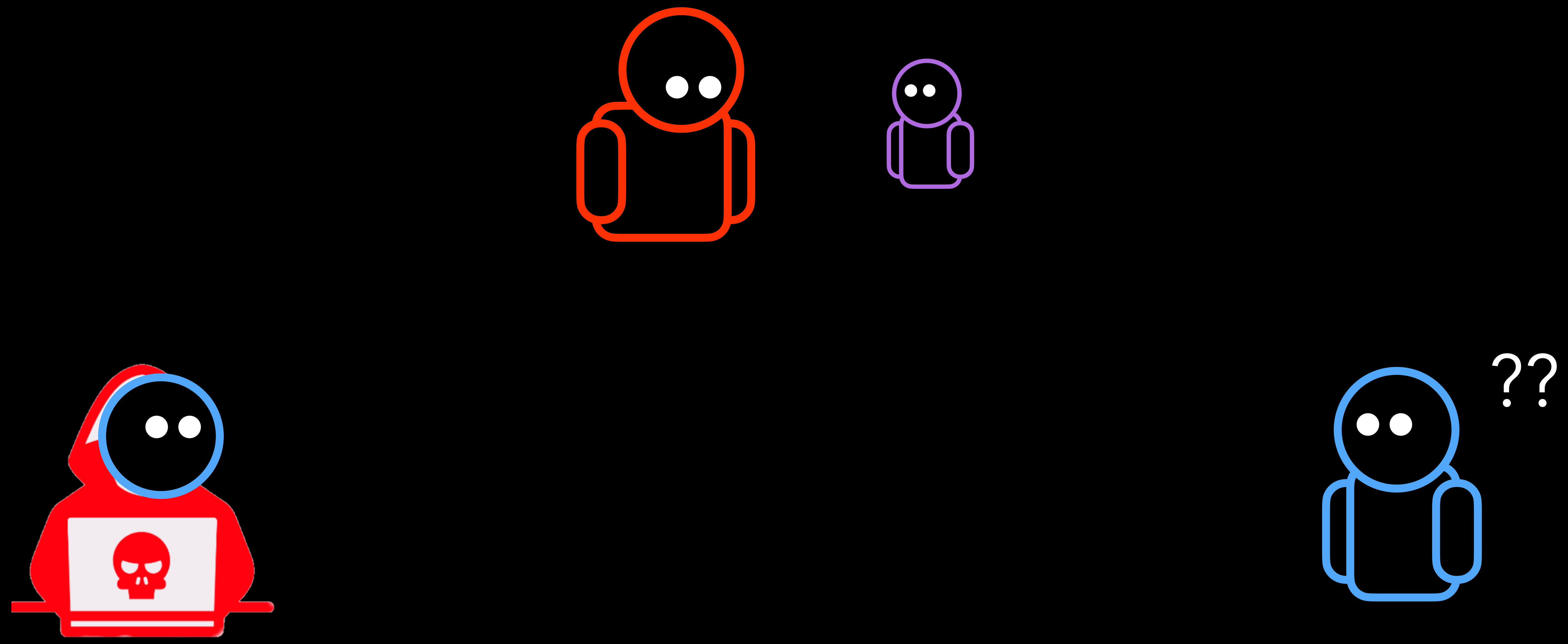
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

URL: www.youporn.com/

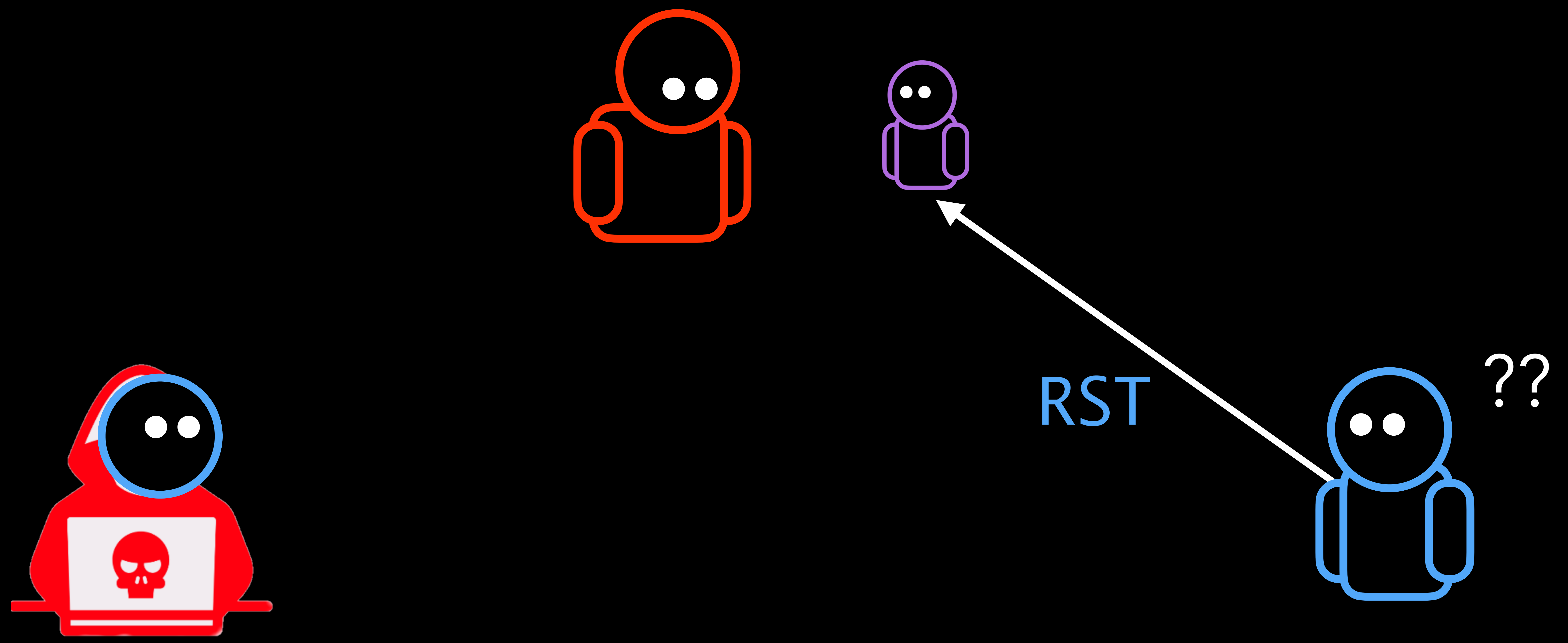
Category: adult

Mega-amplifier cause #1: Victim-sustained loops



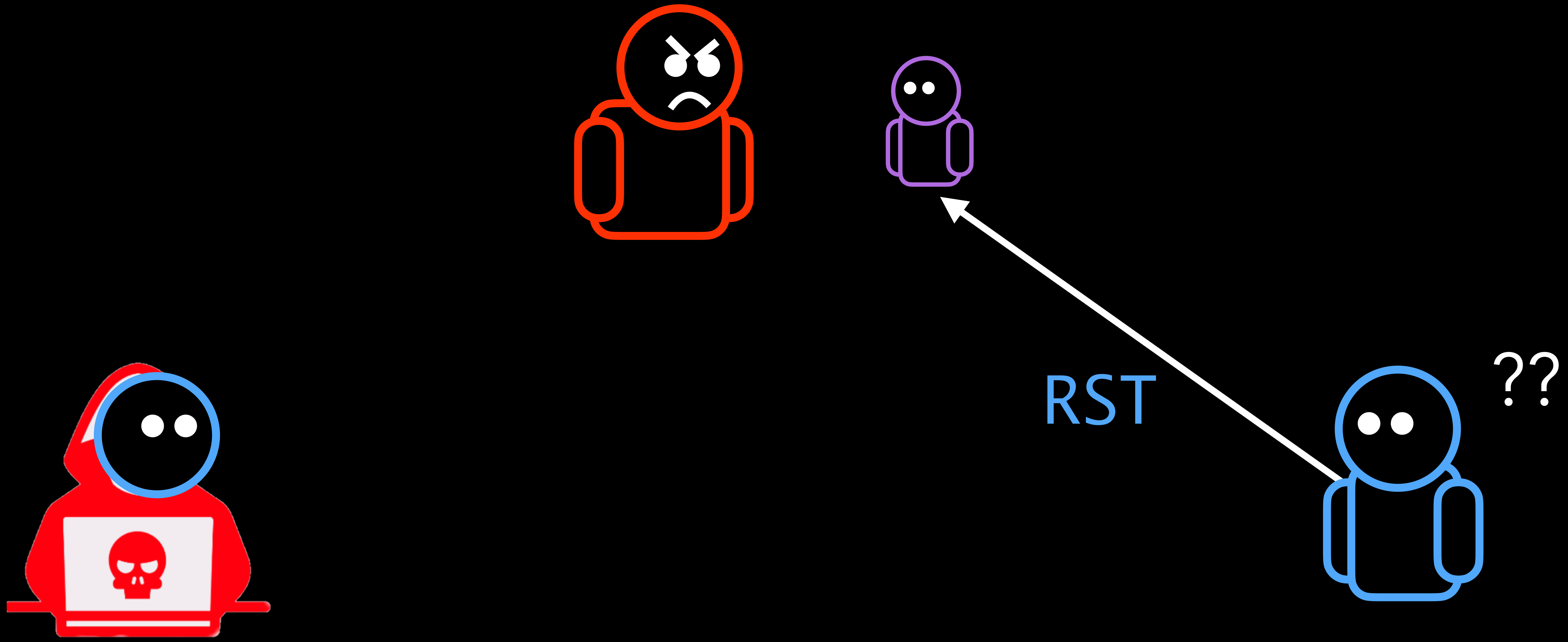
Proper client behavior

Mega-amplifier cause #1: Victim-sustained loops



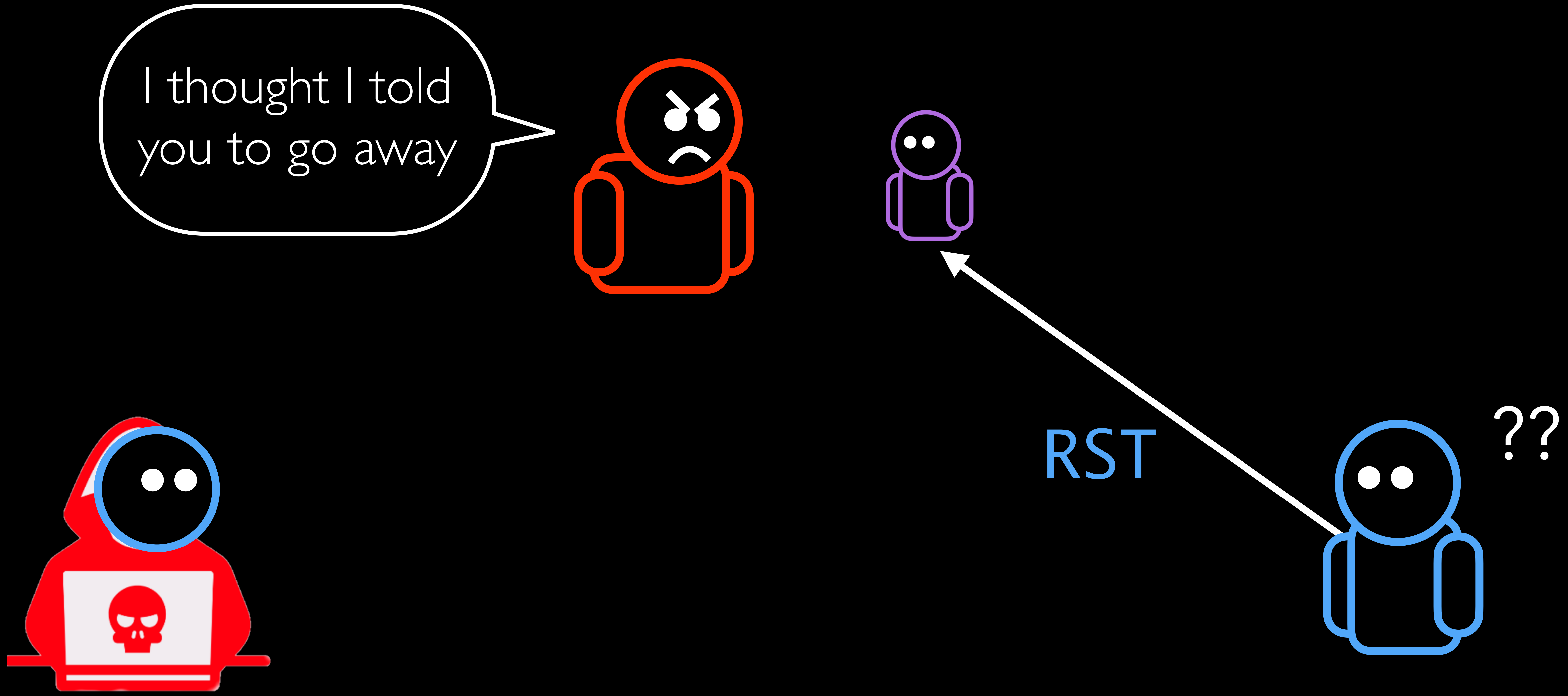
Proper client behavior

Mega-amplifier cause #1: Victim-sustained loops



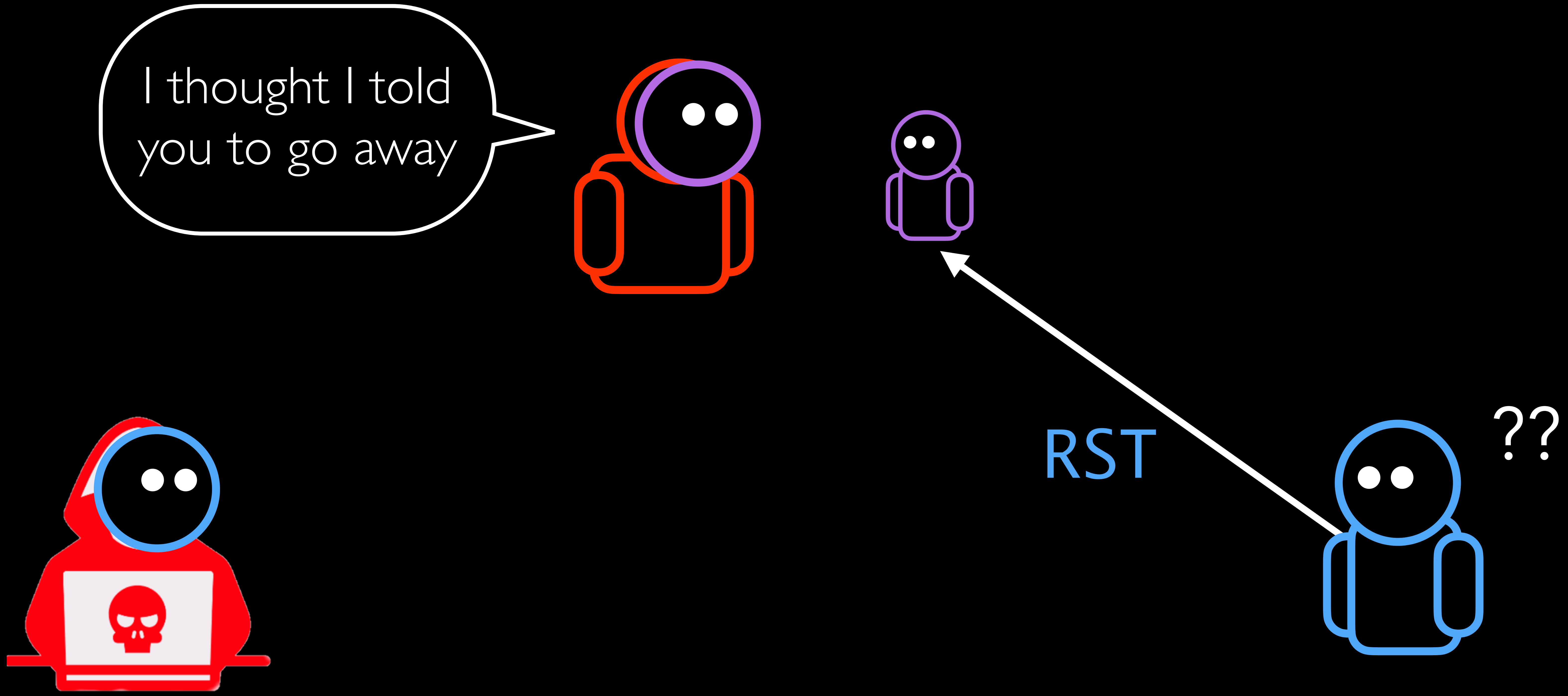
Sometimes, *any* packet re-triggers censorship

Mega-amplifier cause #1: Victim-sustained loops



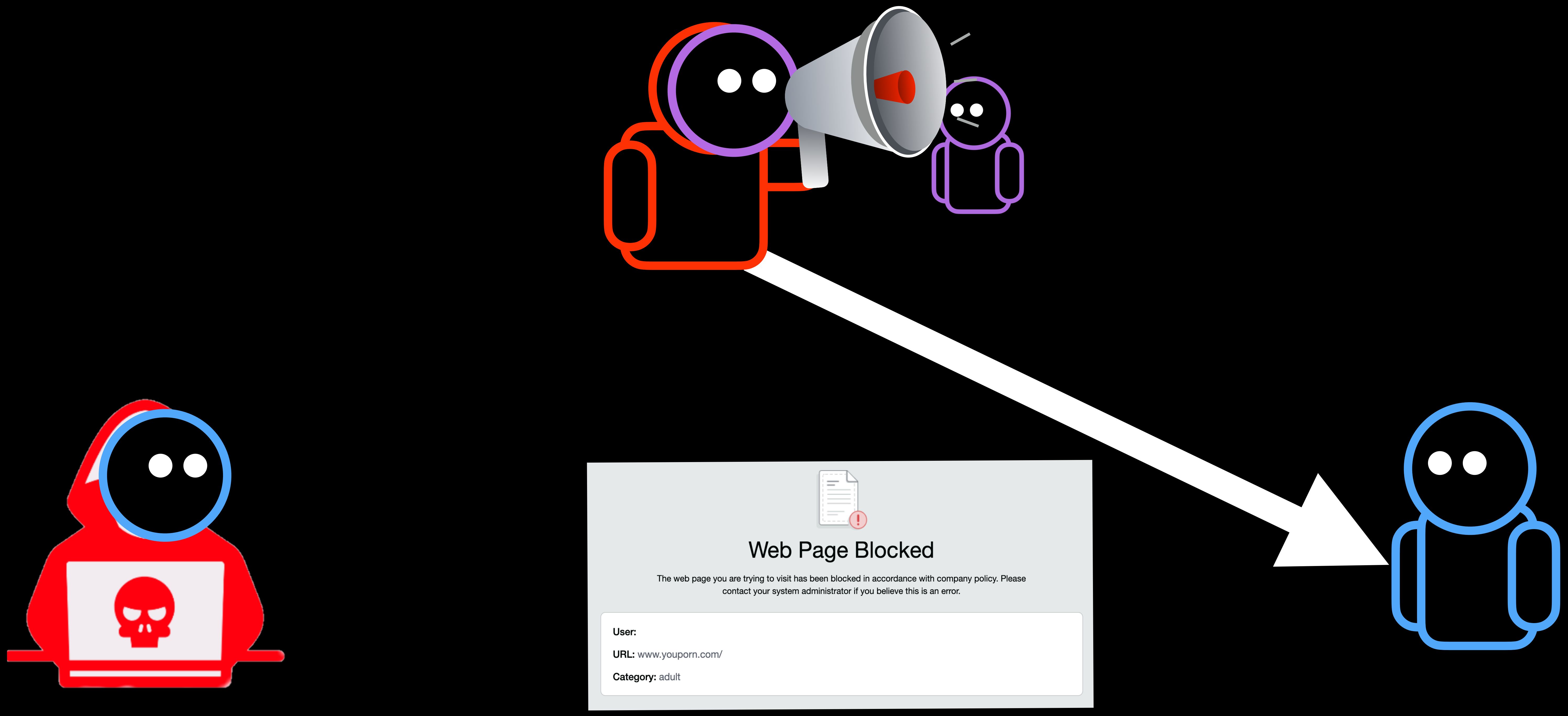
Sometimes, *any* packet re-triggers censorship

Mega-amplifier cause #1: Victim-sustained loops



Sometimes, *any* packet re-triggers censorship

Mega-amplifier cause #1: Victim-sustained loops



Web Page Blocked

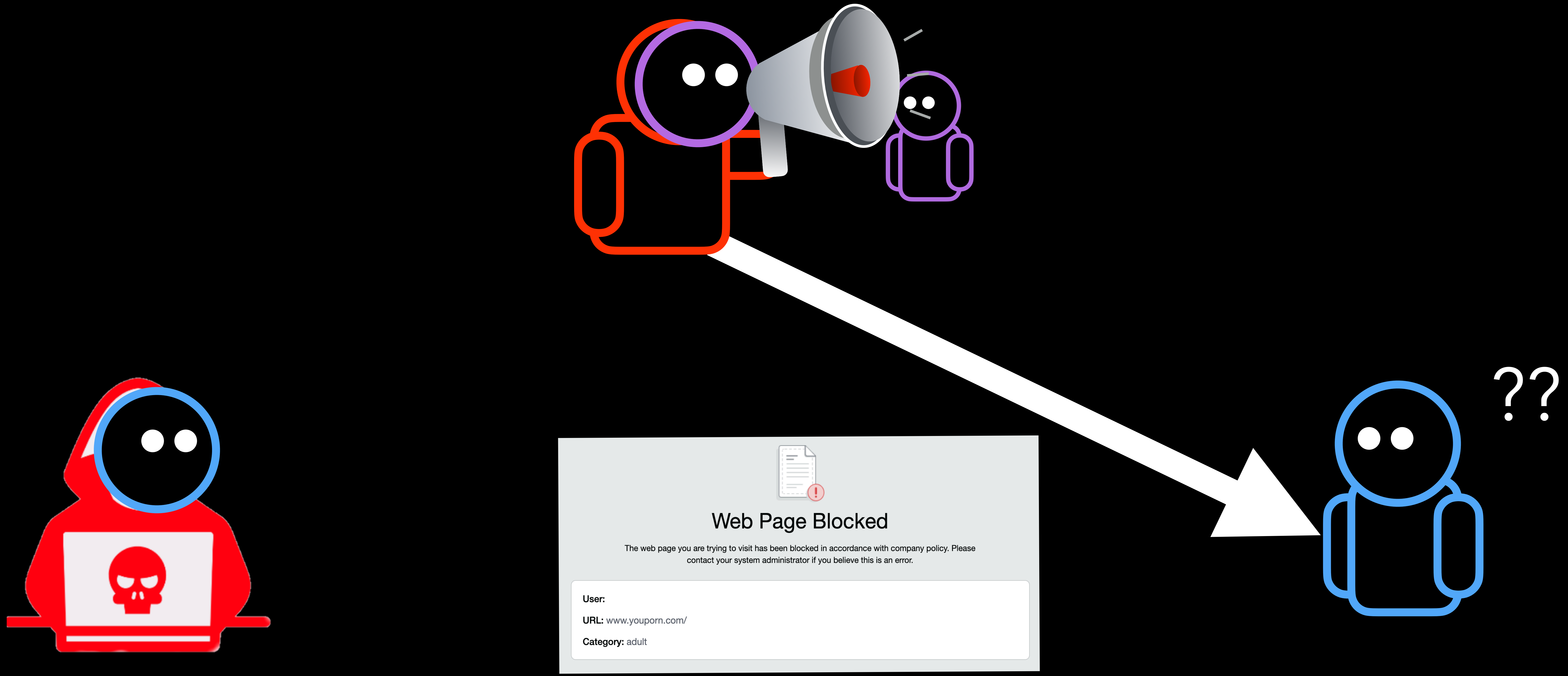
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

URL: www.youporn.com/

Category: adult

Mega-amplifier cause #1: Victim-sustained loops



Web Page Blocked

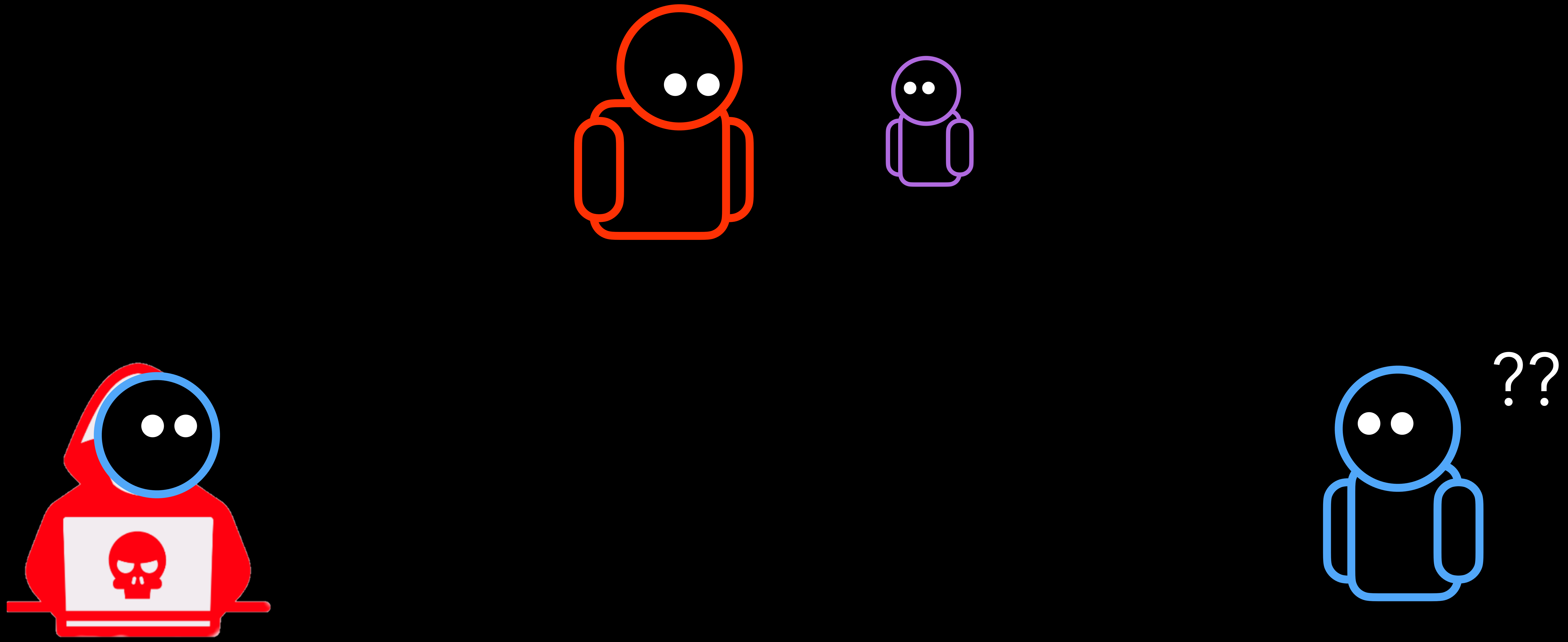
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

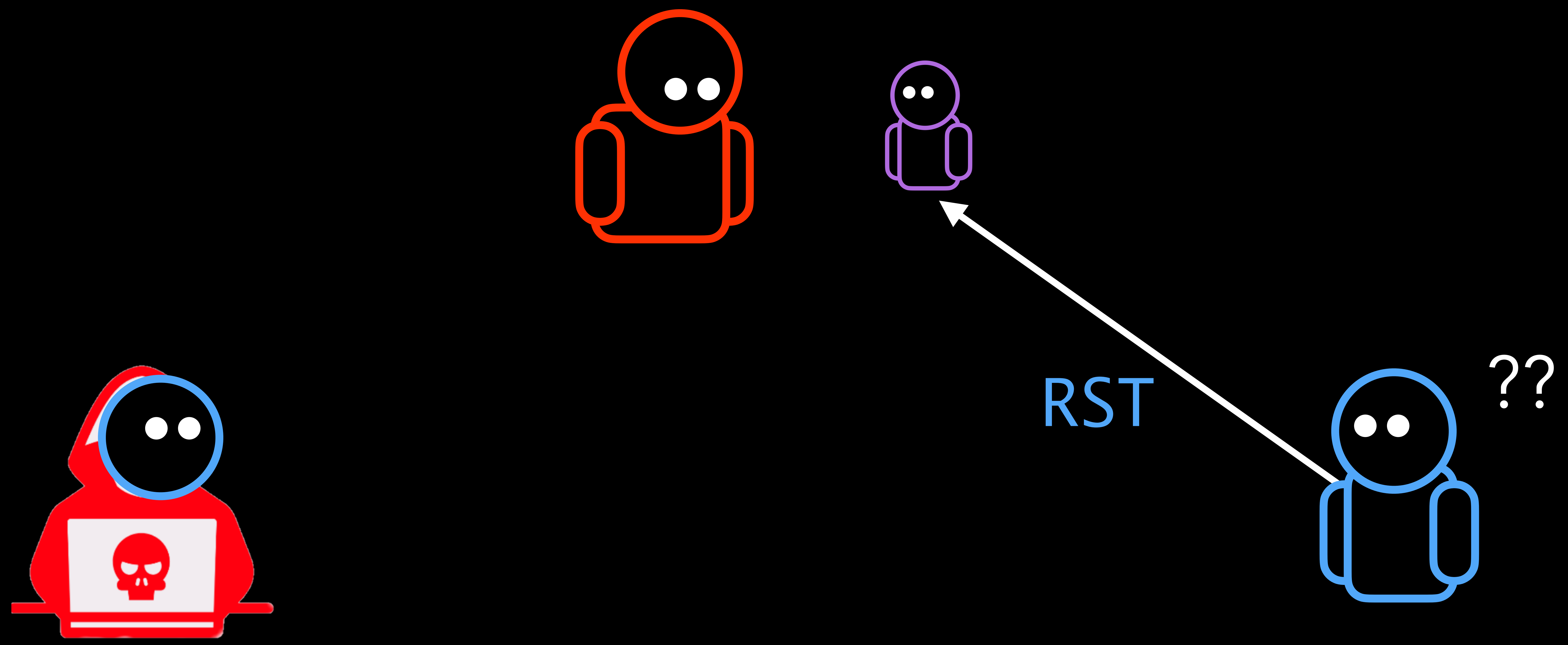
URL: www.youporn.com/

Category: adult

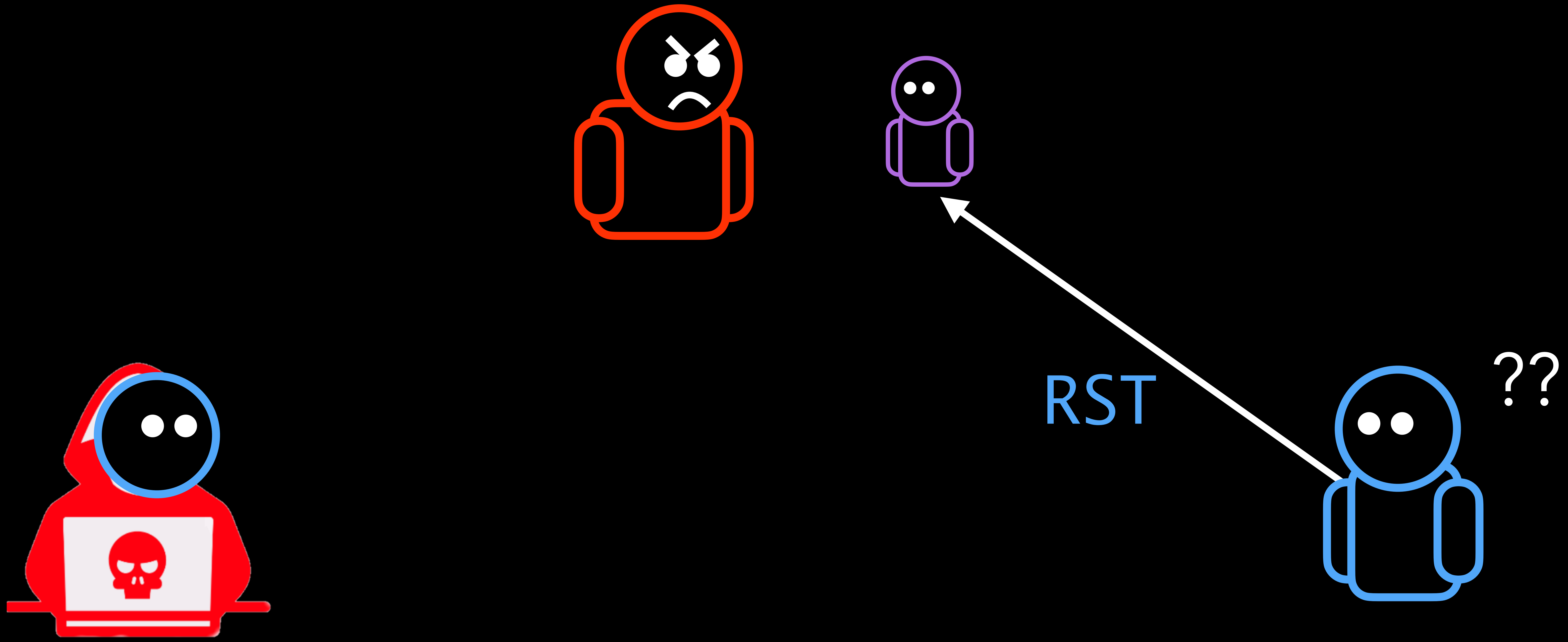
Mega-amplifier cause #1: Victim-sustained loops



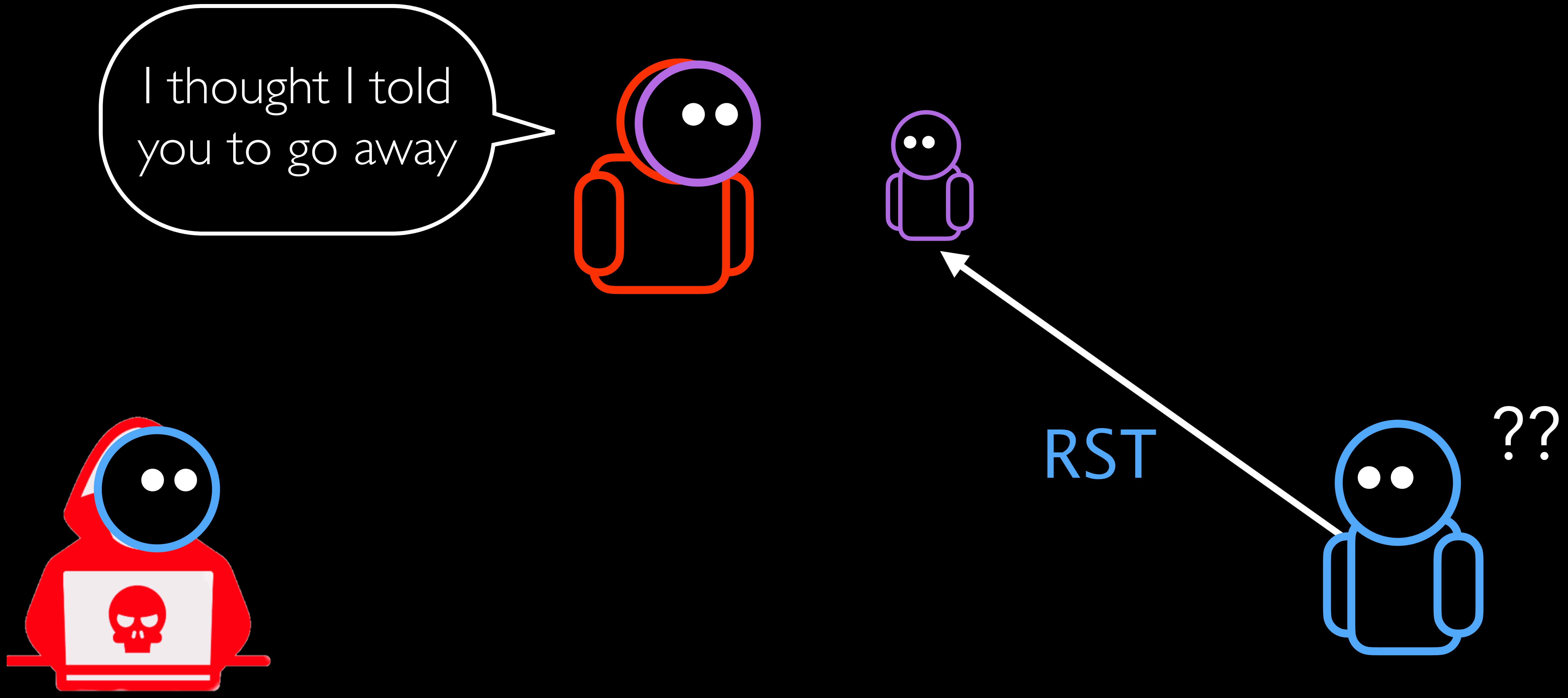
Mega-amplifier cause #1: Victim-sustained loops



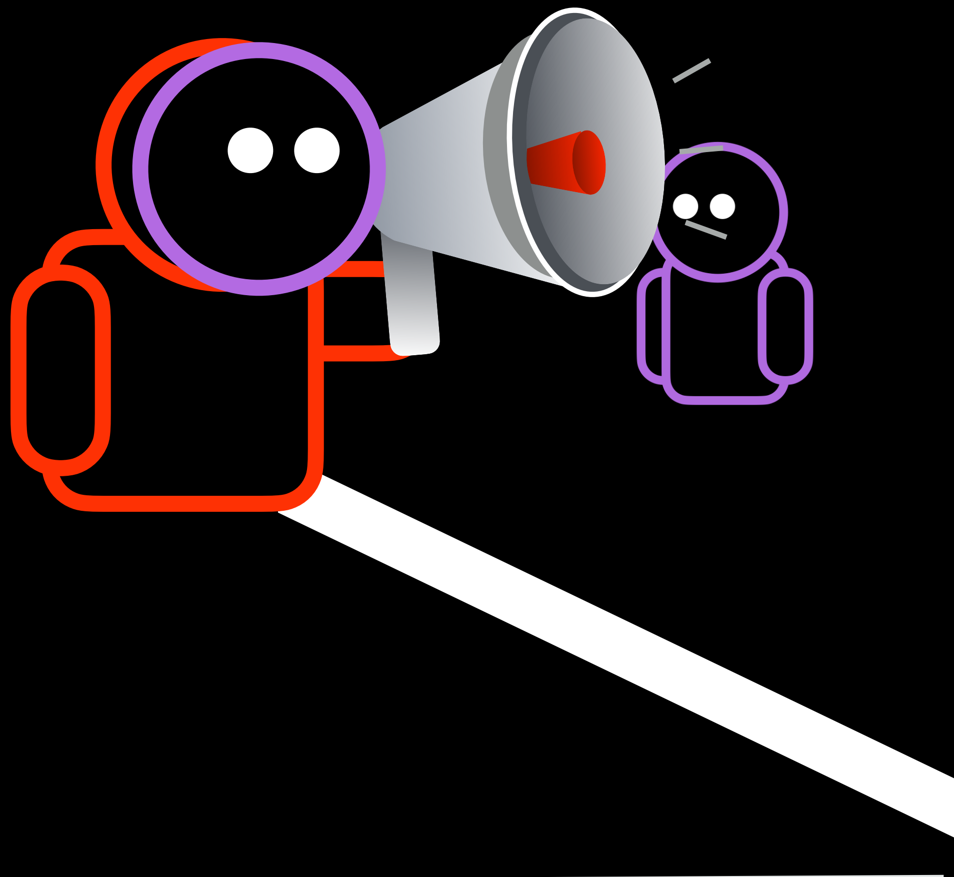
Mega-amplifier cause #1: Victim-sustained loops

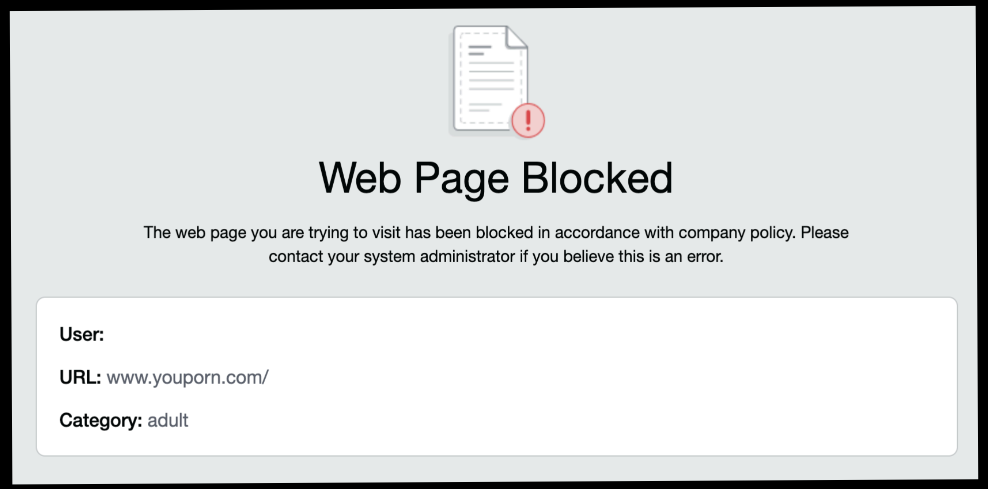


Mega-amplifier cause #1: Victim-sustained loops



Mega-amplifier cause #1: Victim-sustained loops





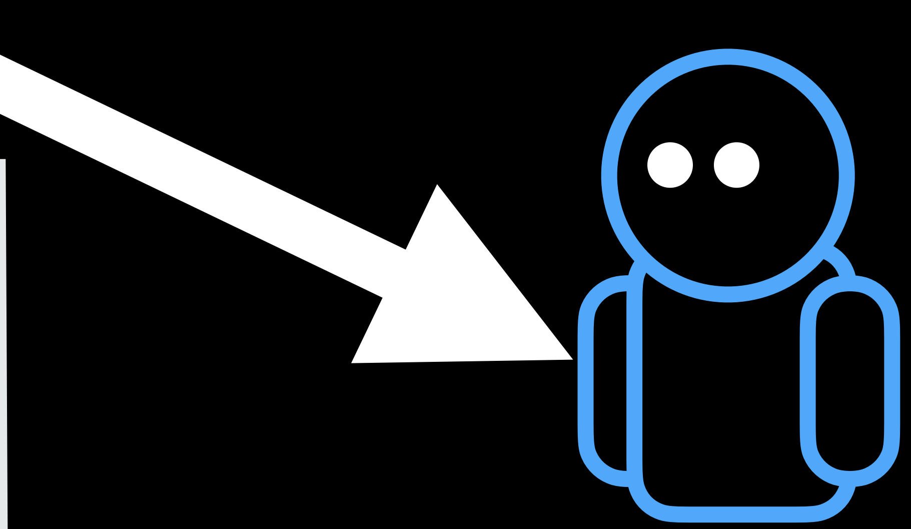
Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

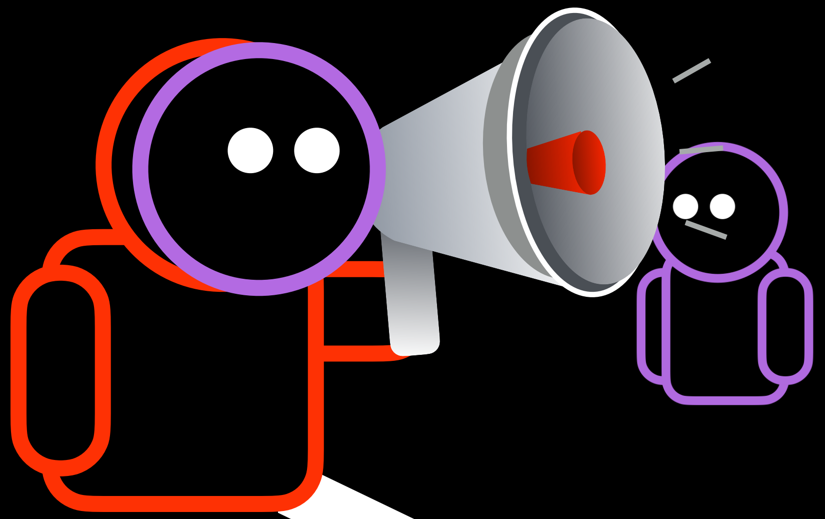
User:

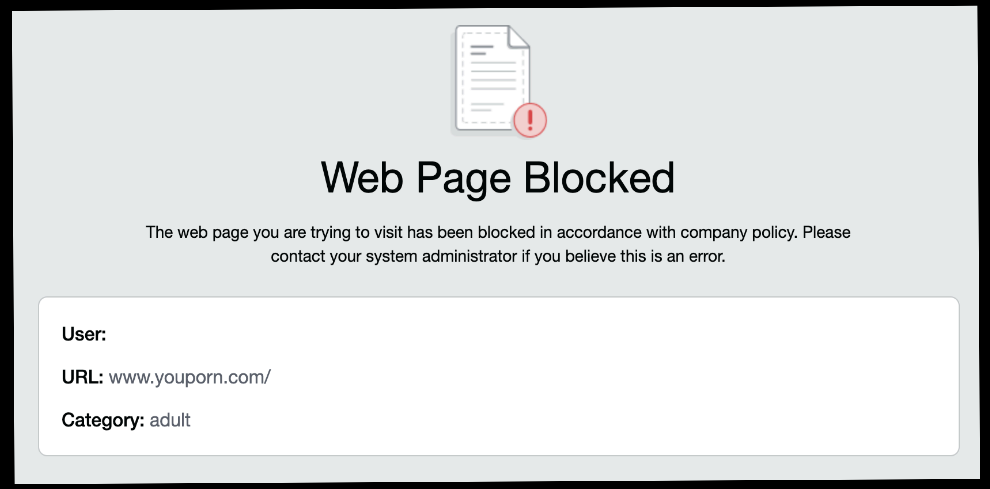
URL: www.youporn.com/

Category: adult



Mega-amplifier cause #1: Victim-sustained loops





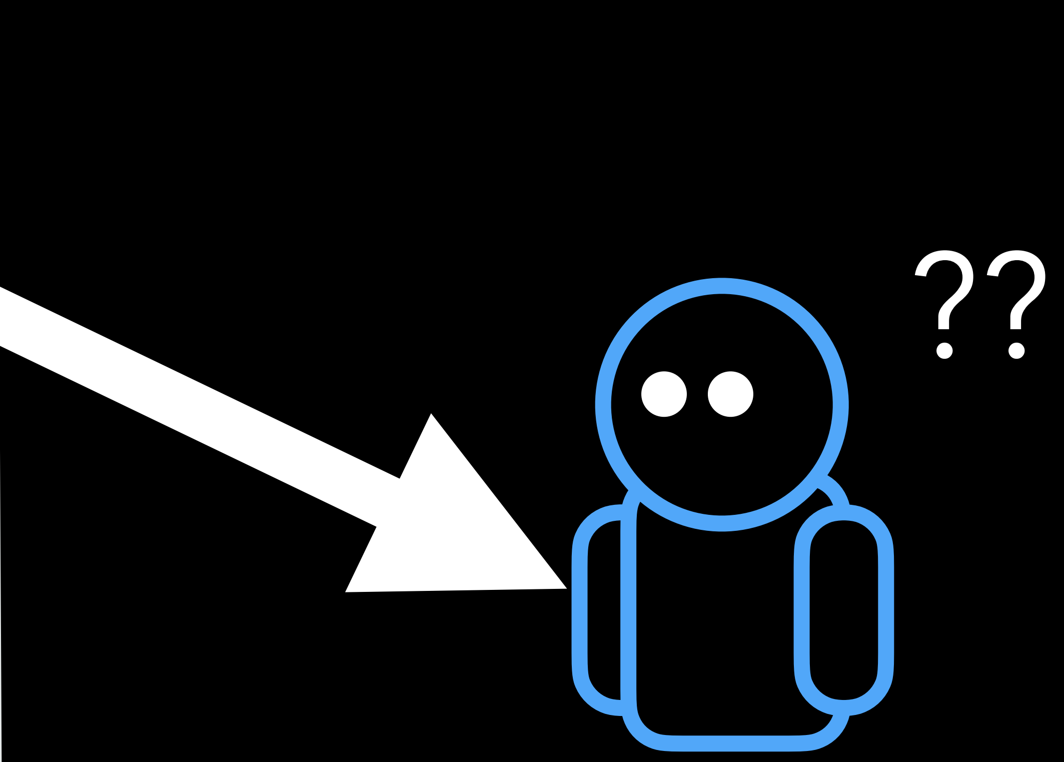
Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

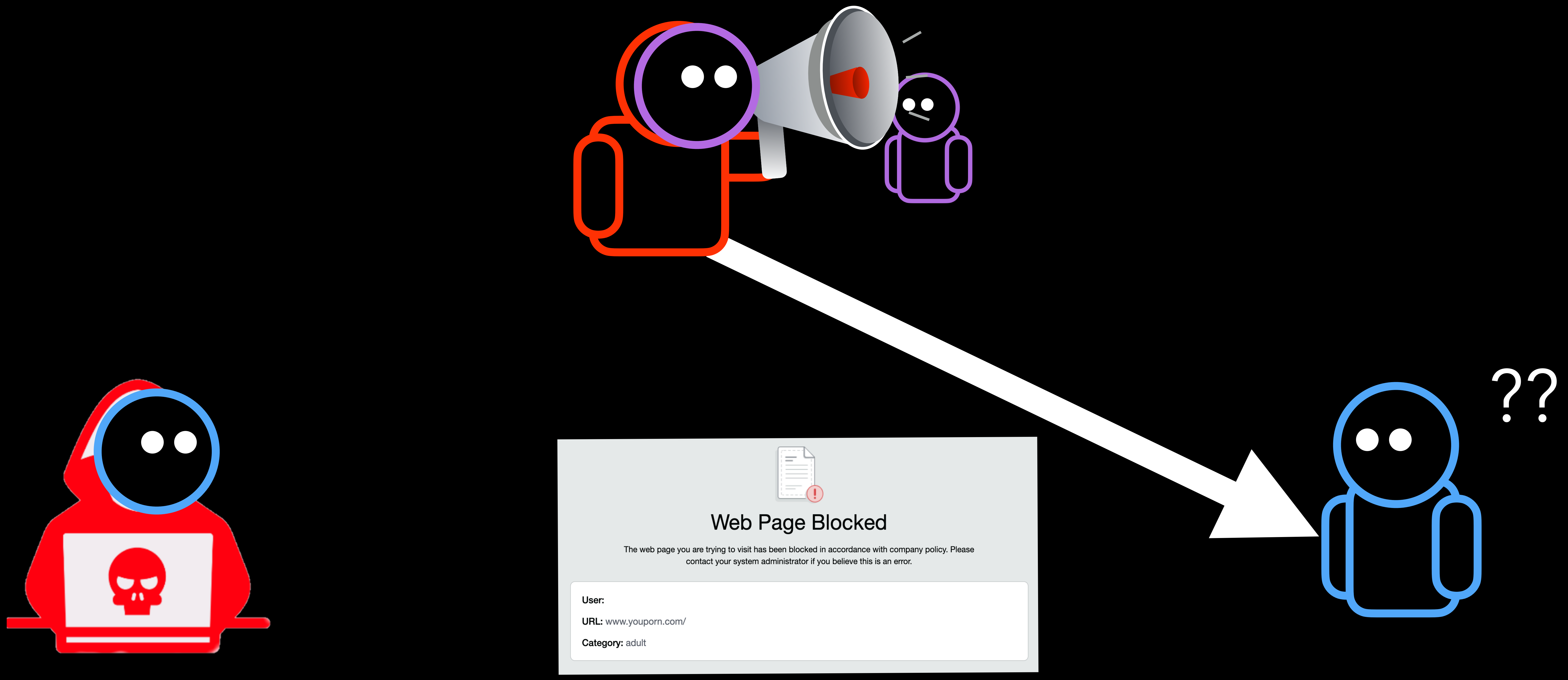
User:

URL: www.youporn.com/

Category: adult



Mega-amplifier cause #1: Victim-sustained loops



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

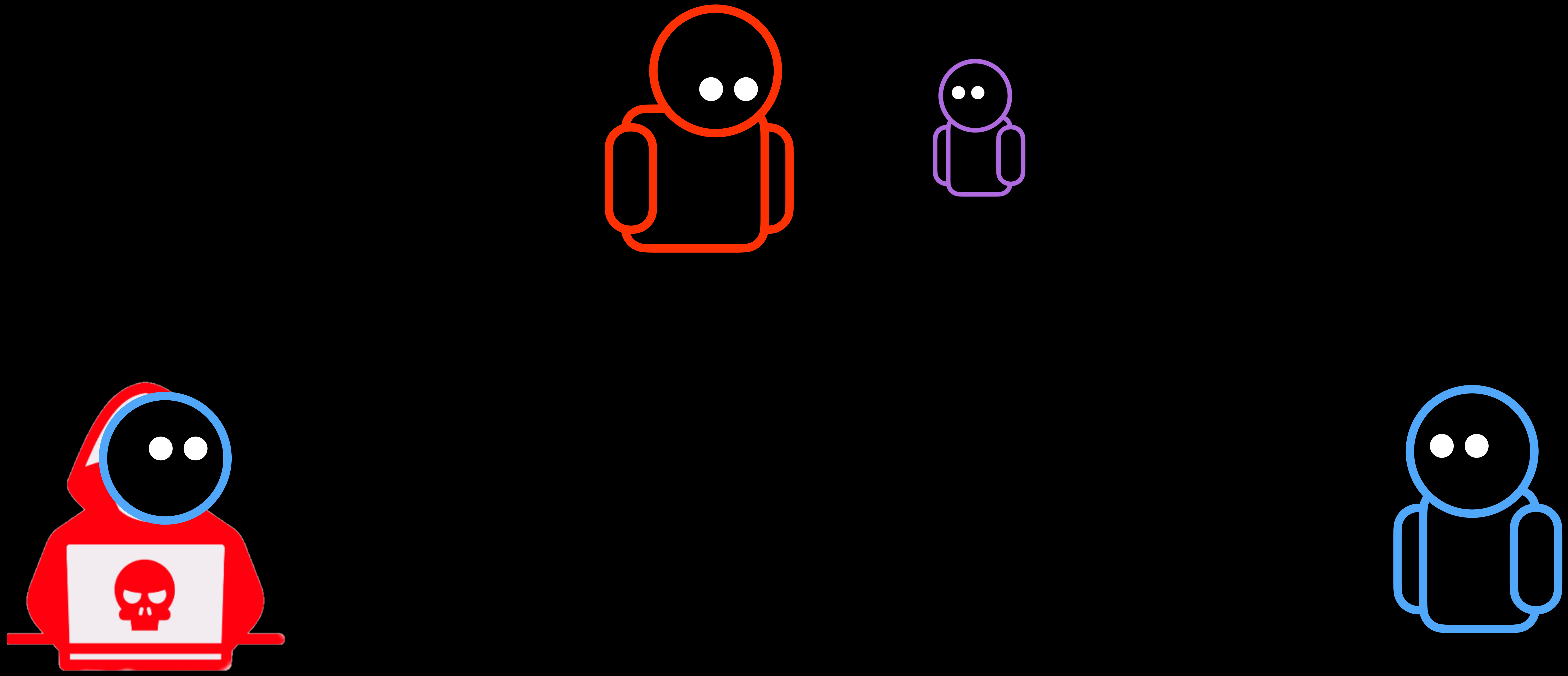
URL: www.youporn.com/

Category: adult

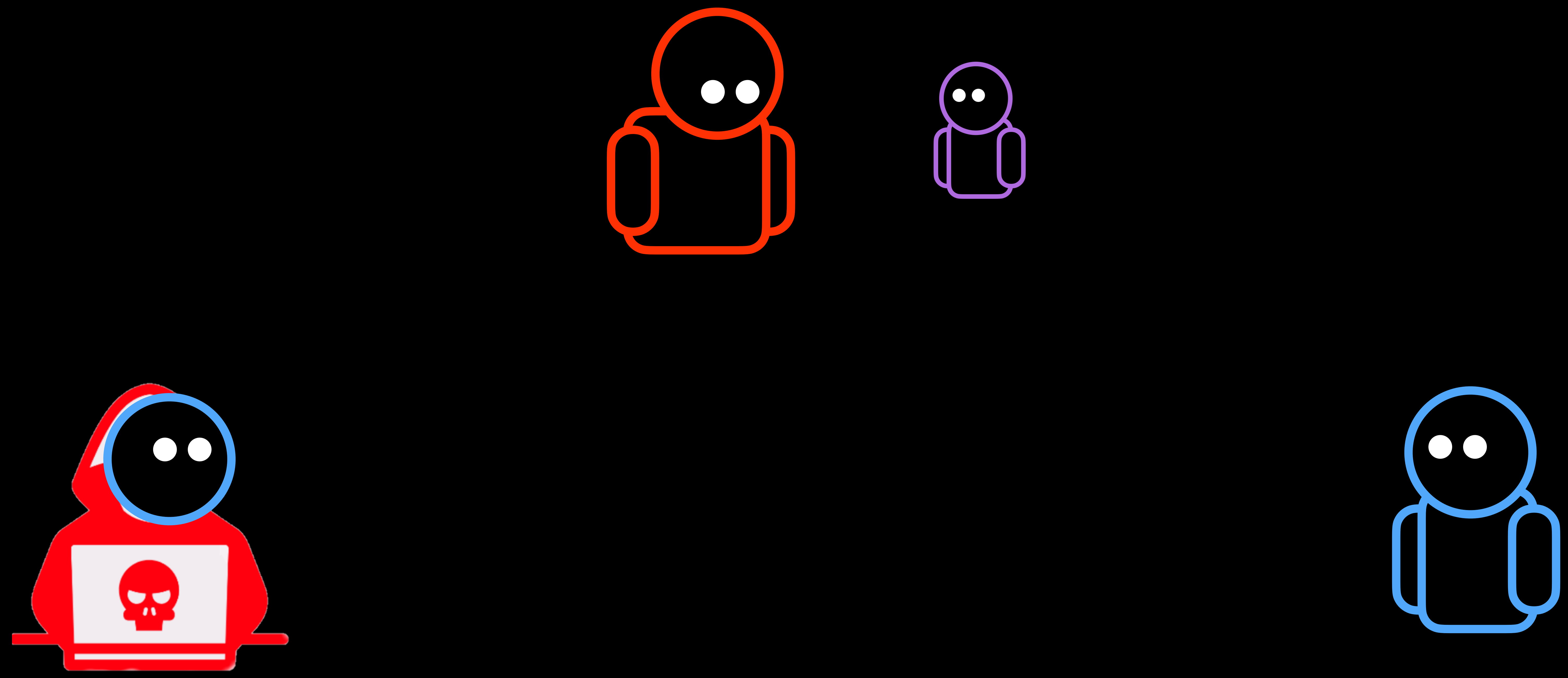
Victim-sustained amplification can be effectively *infinite*

Attacks the victim’s downlink *and* uplink

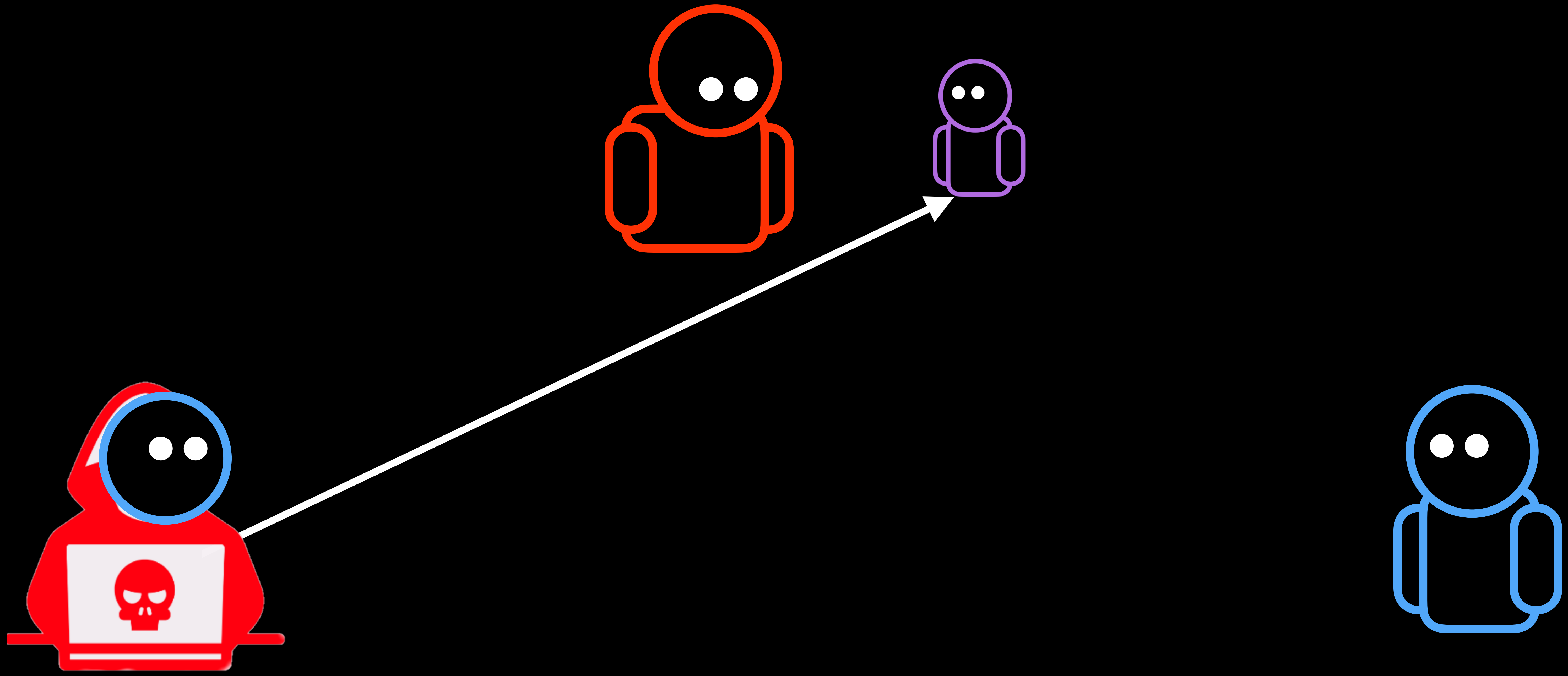
Mega-amplifier cause #2



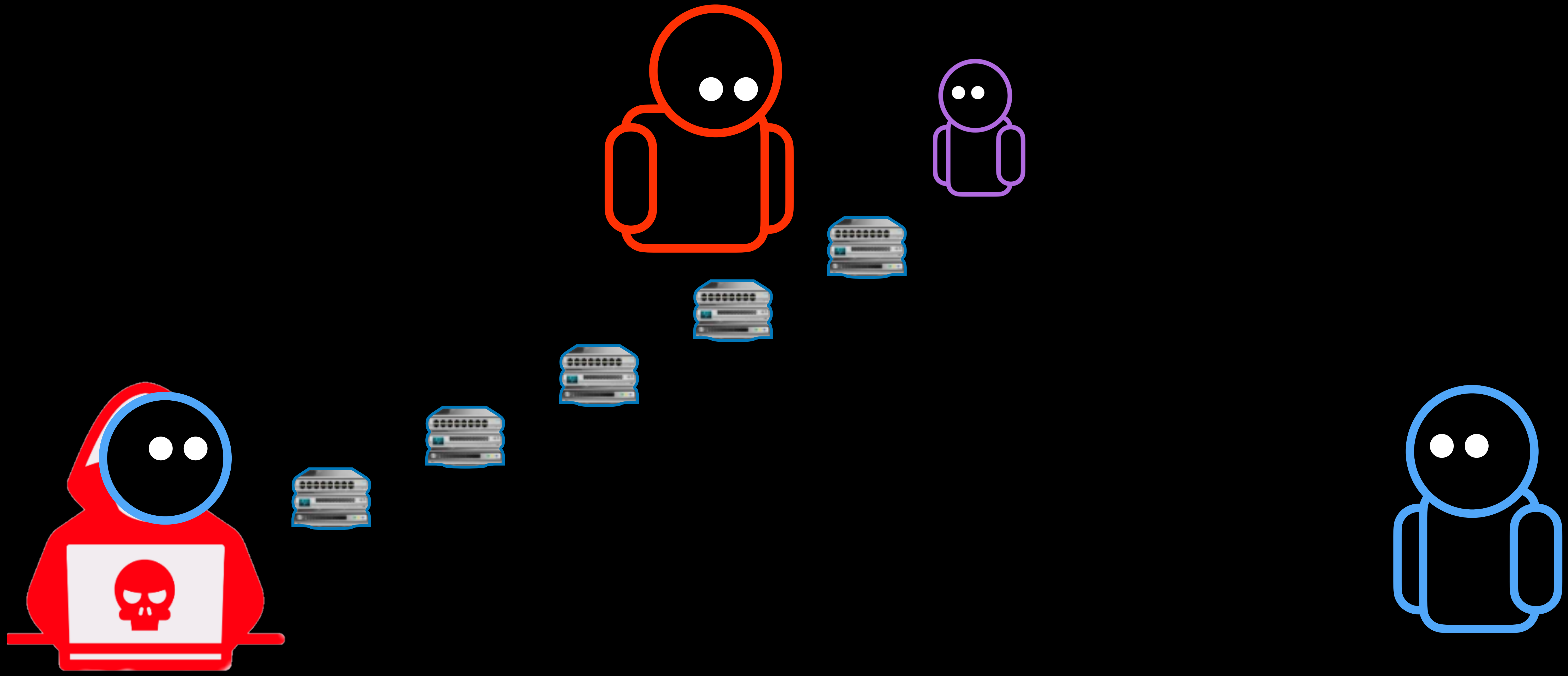
Mega-amplifier cause #2



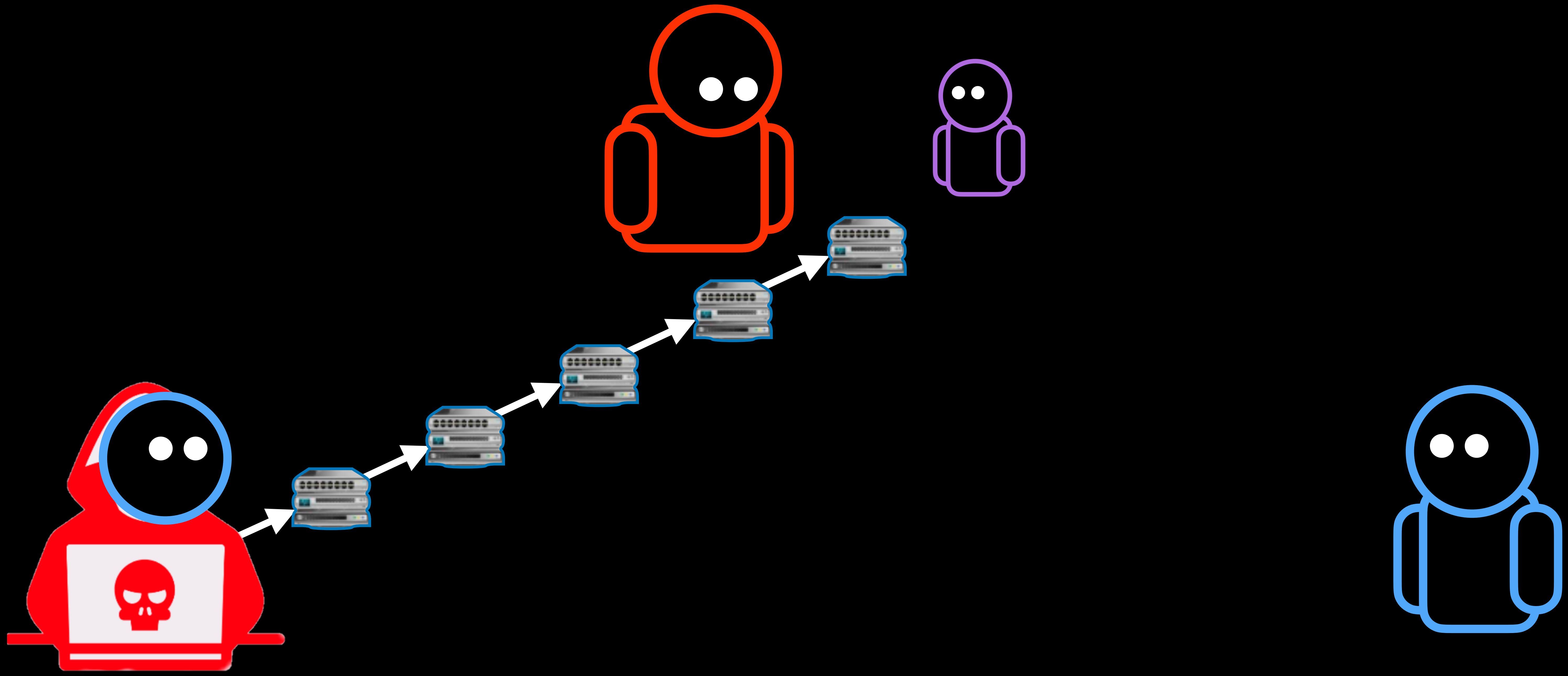
Mega-amplifier cause #2



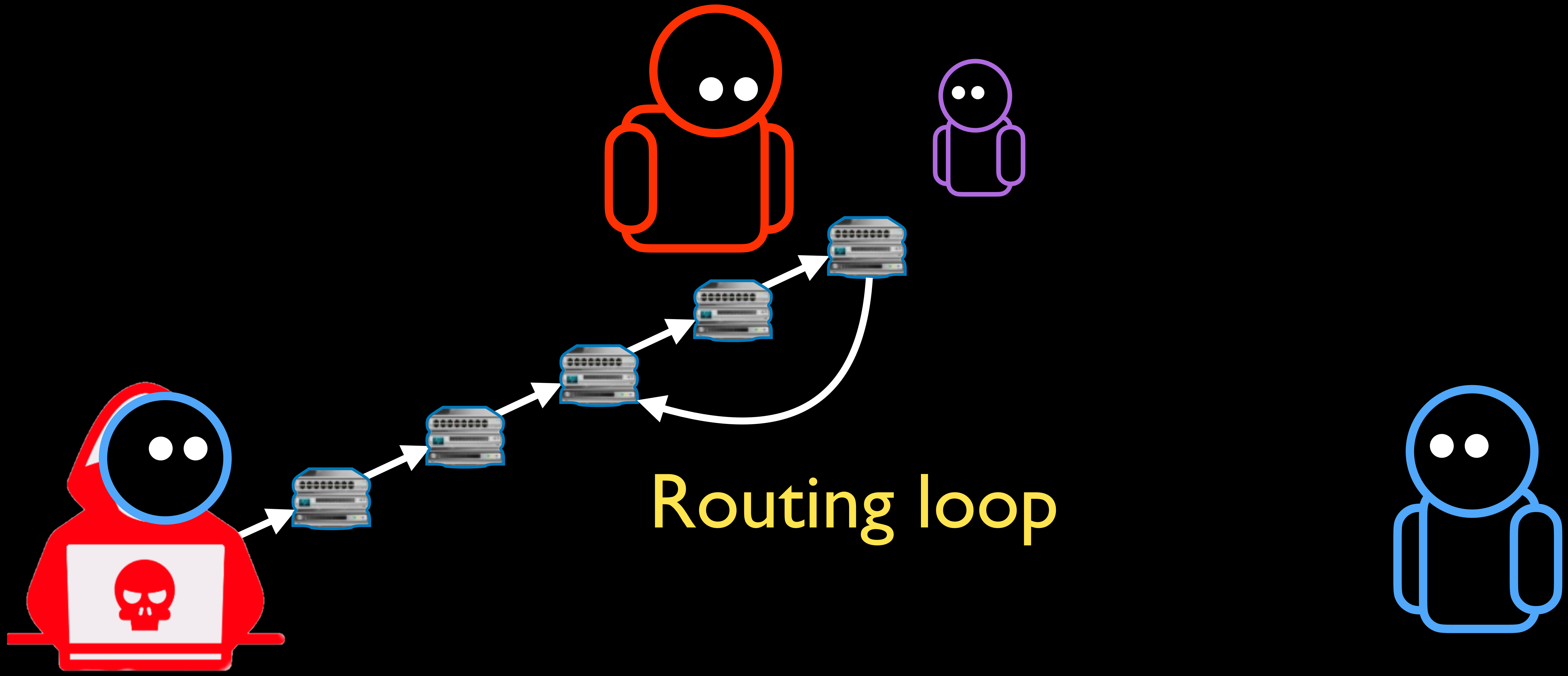
Mega-amplifier cause #2



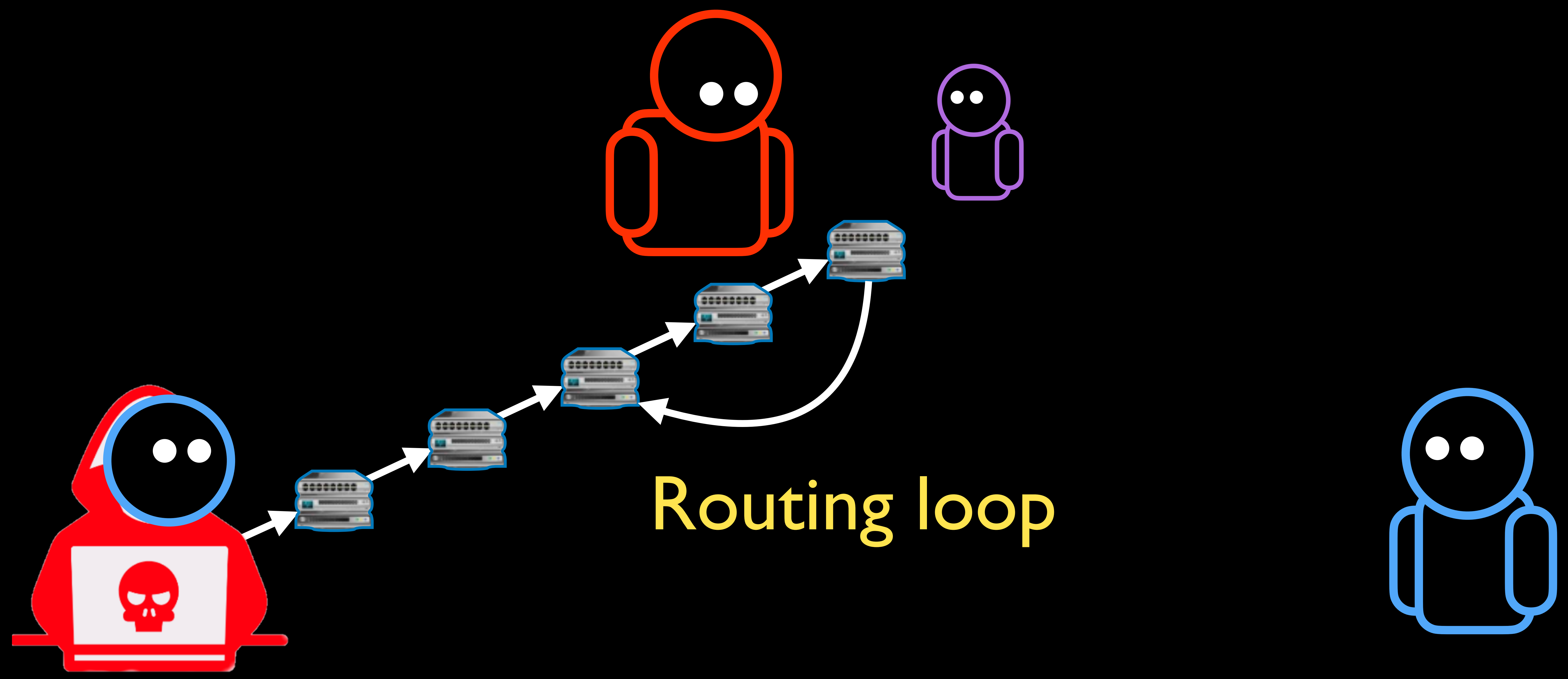
Mega-amplifier cause #2



Mega-amplifier cause #2

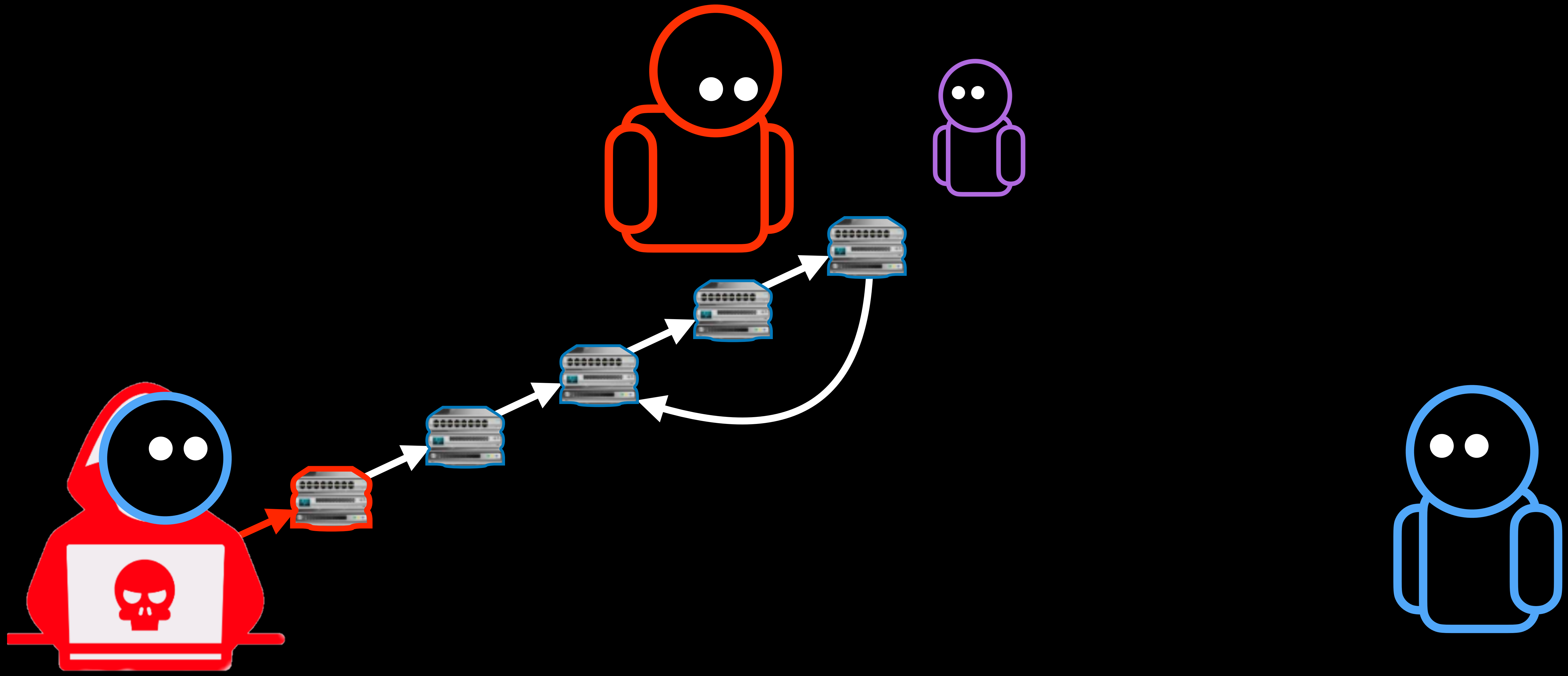


Mega-amplifier cause #2: Routing loops

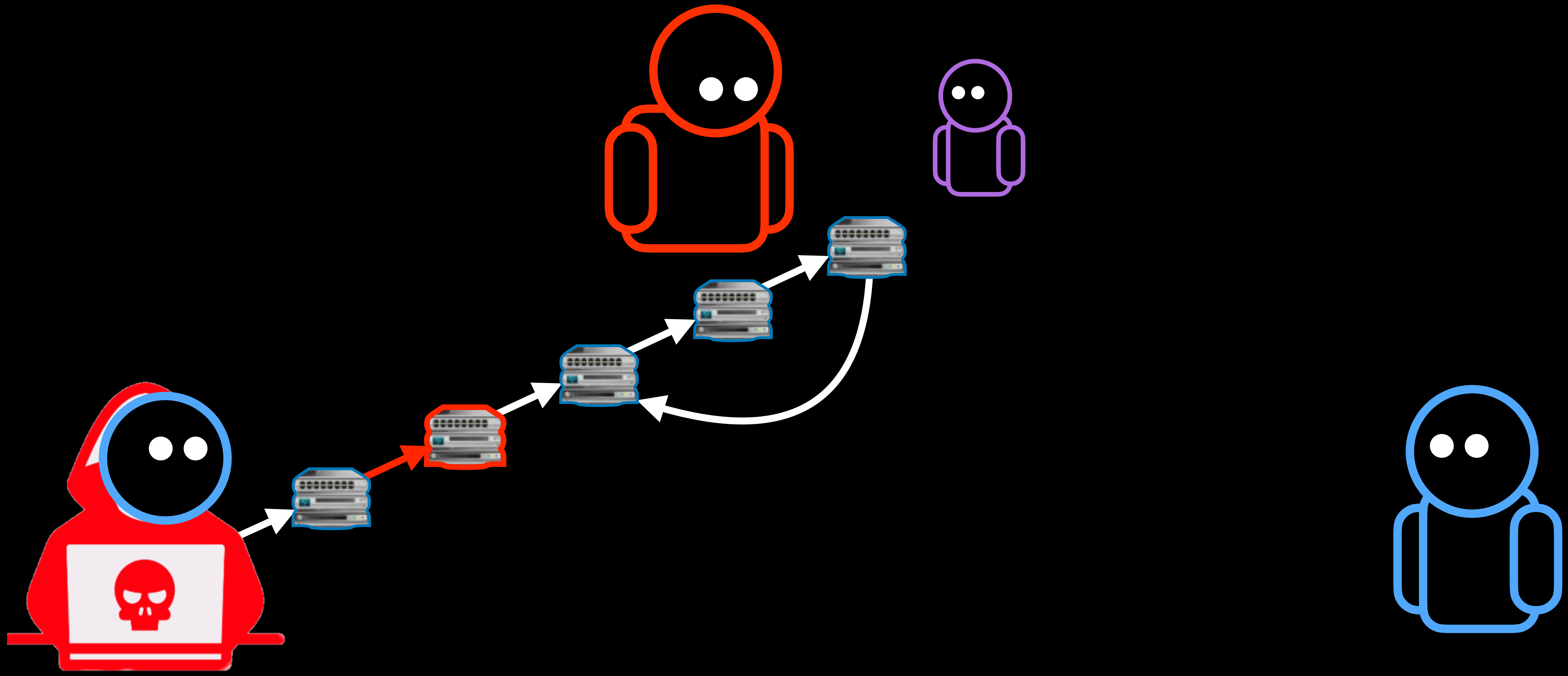


Routing loop

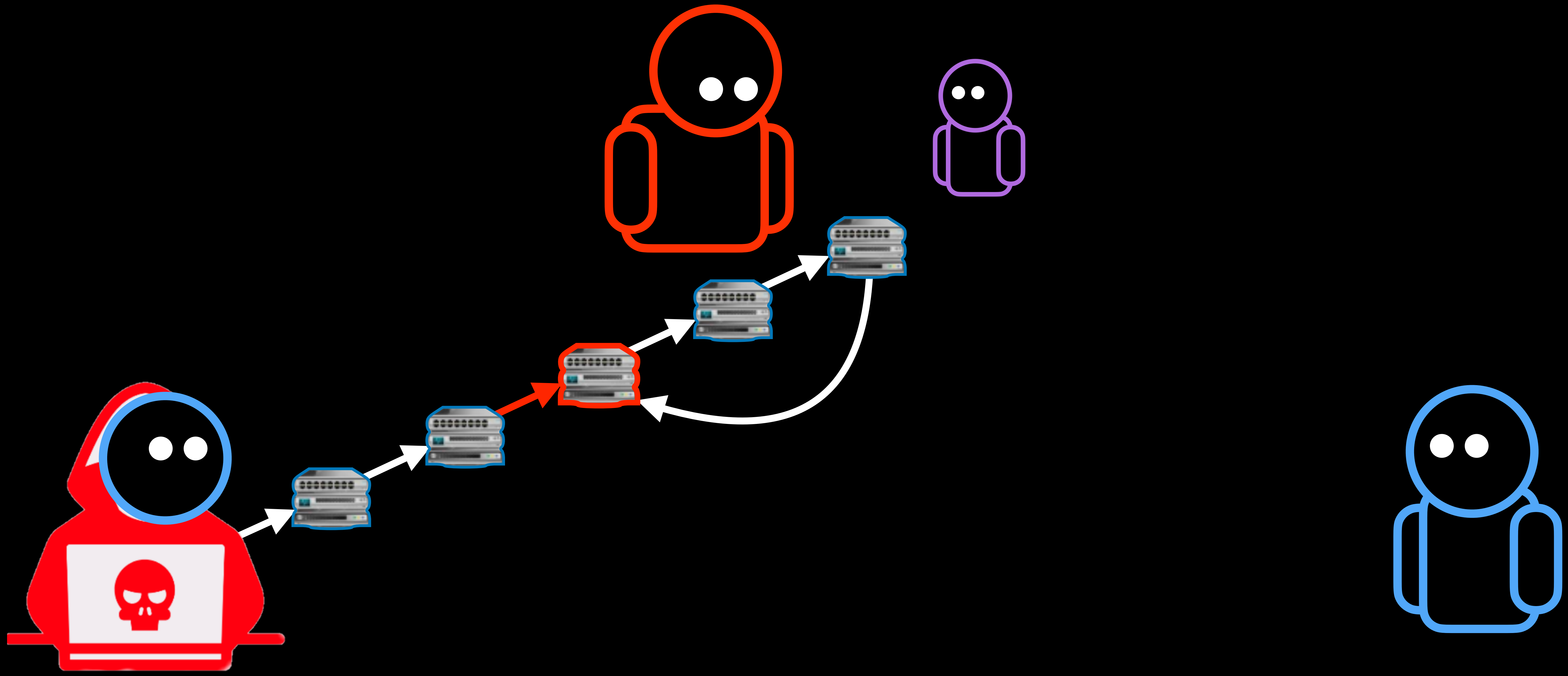
Mega-amplifier cause #2: Routing loops



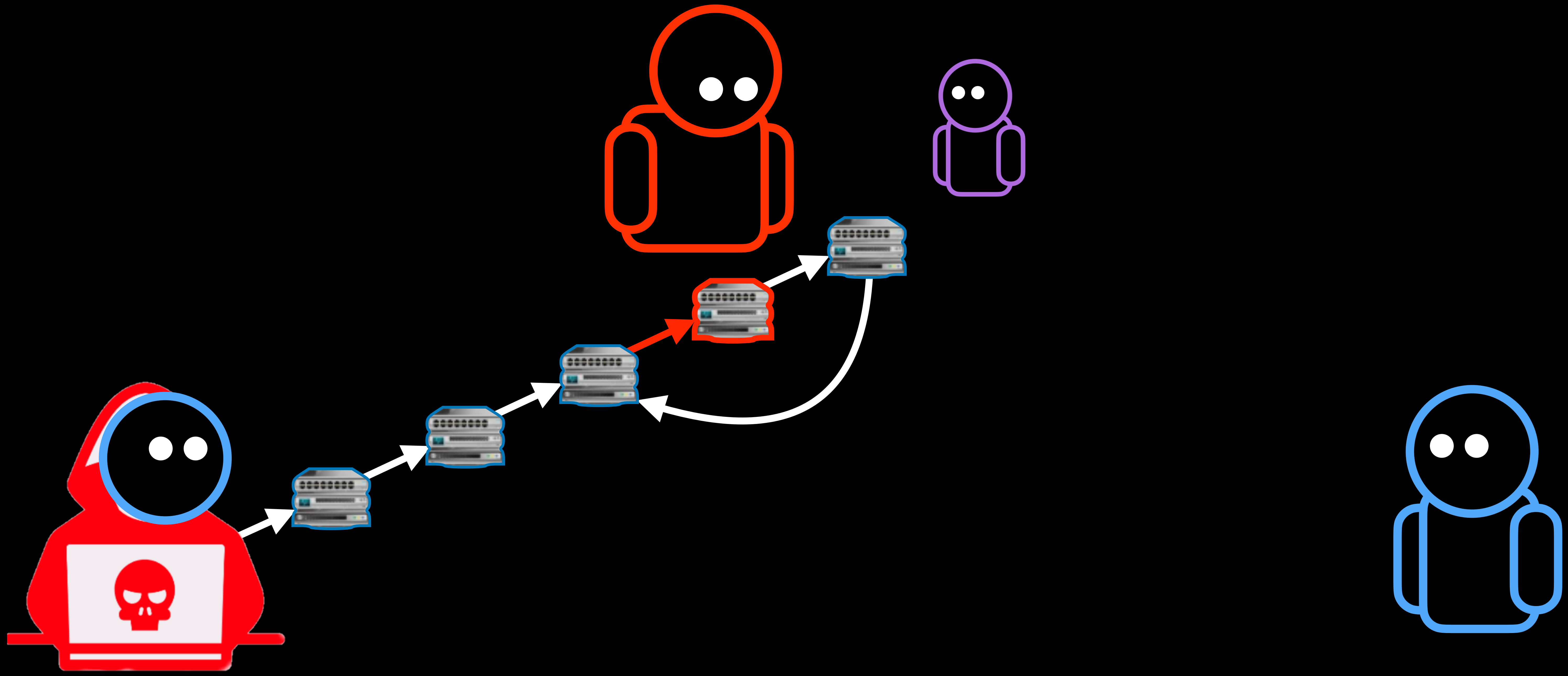
Mega-amplifier cause #2: Routing loops



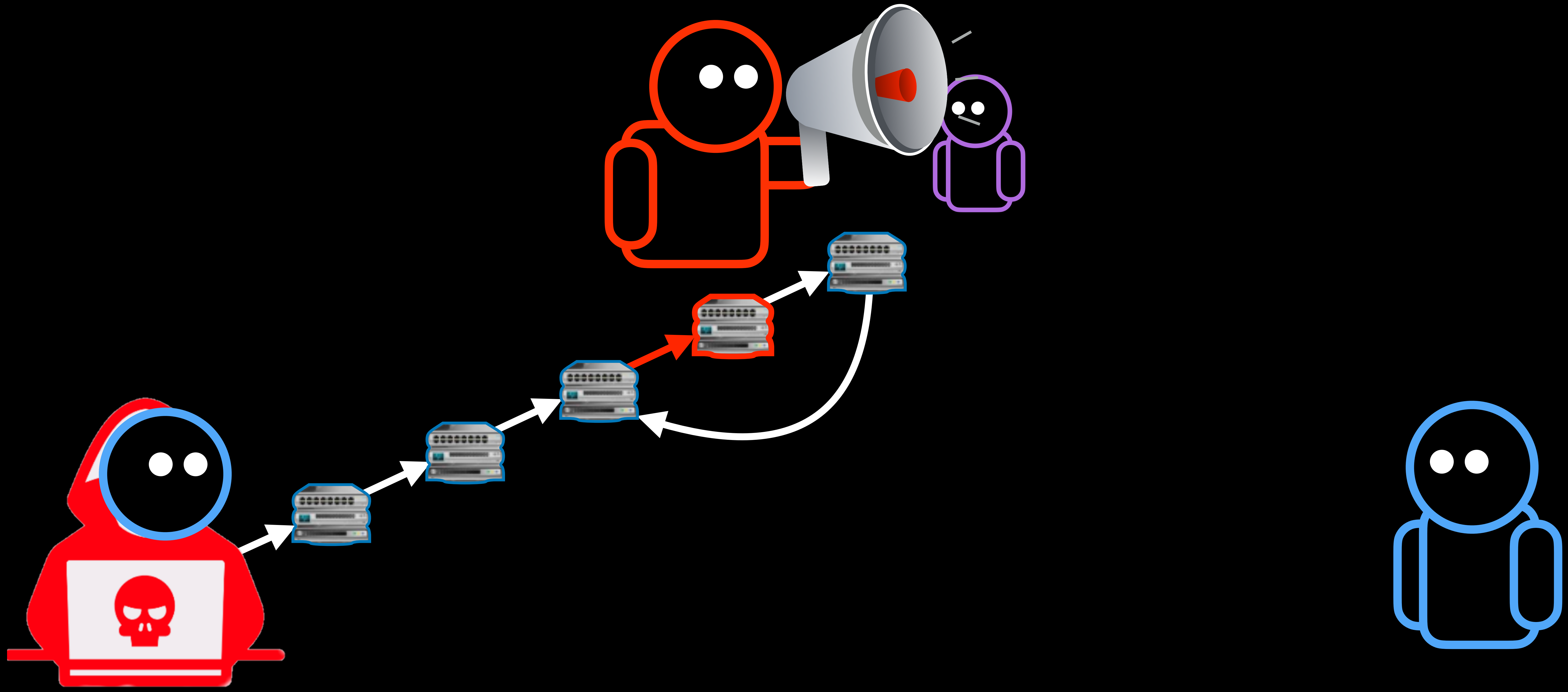
Mega-amplifier cause #2: Routing loops



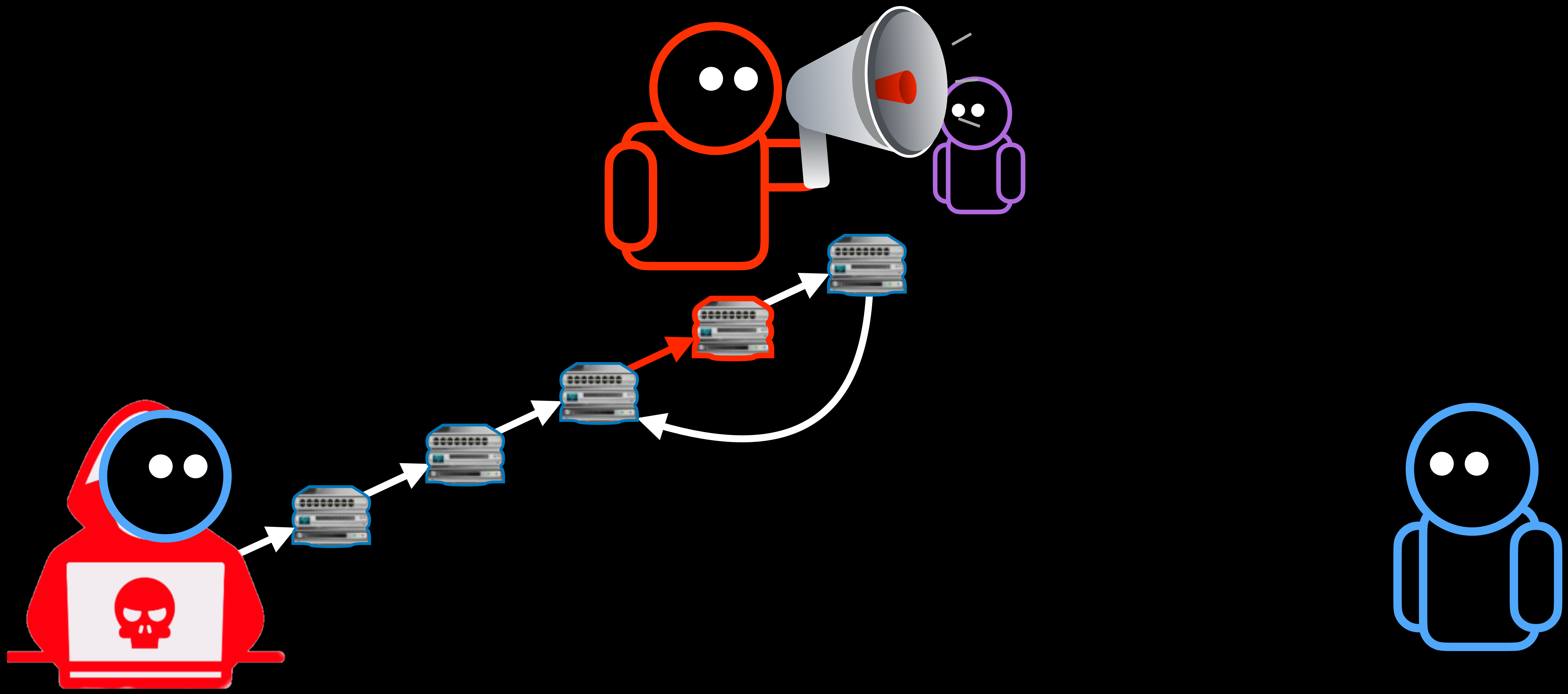
Mega-amplifier cause #2: Routing loops



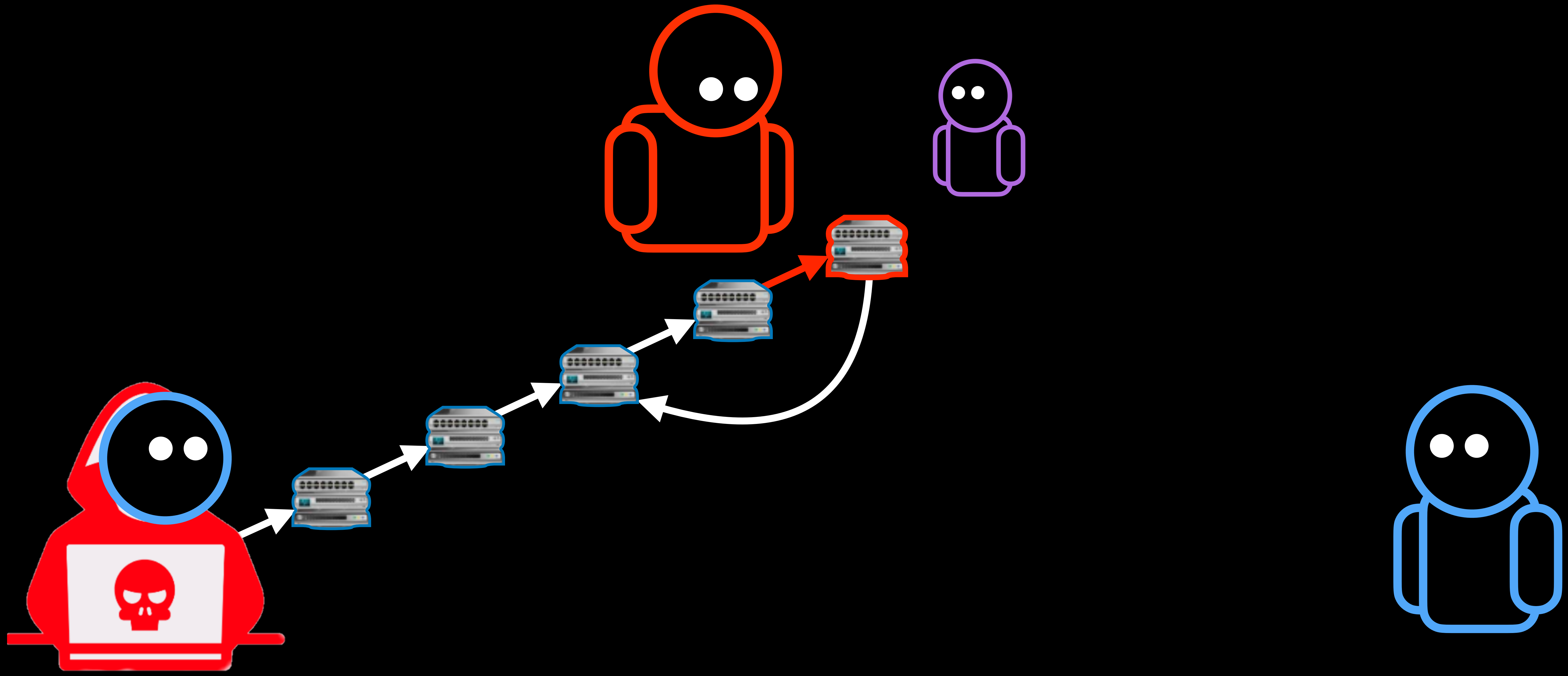
Mega-amplifier cause #2: Routing loops



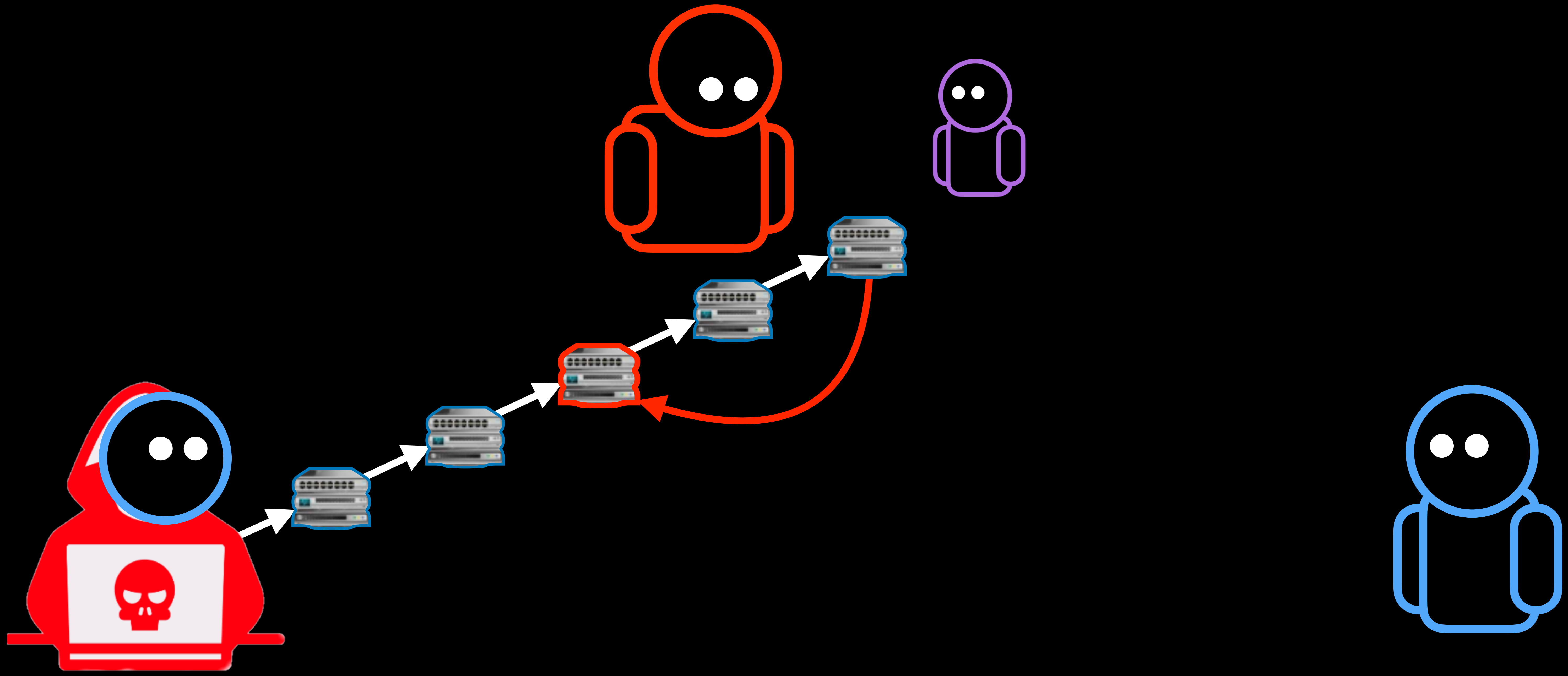
Mega-amplifier cause #2: Routing loops



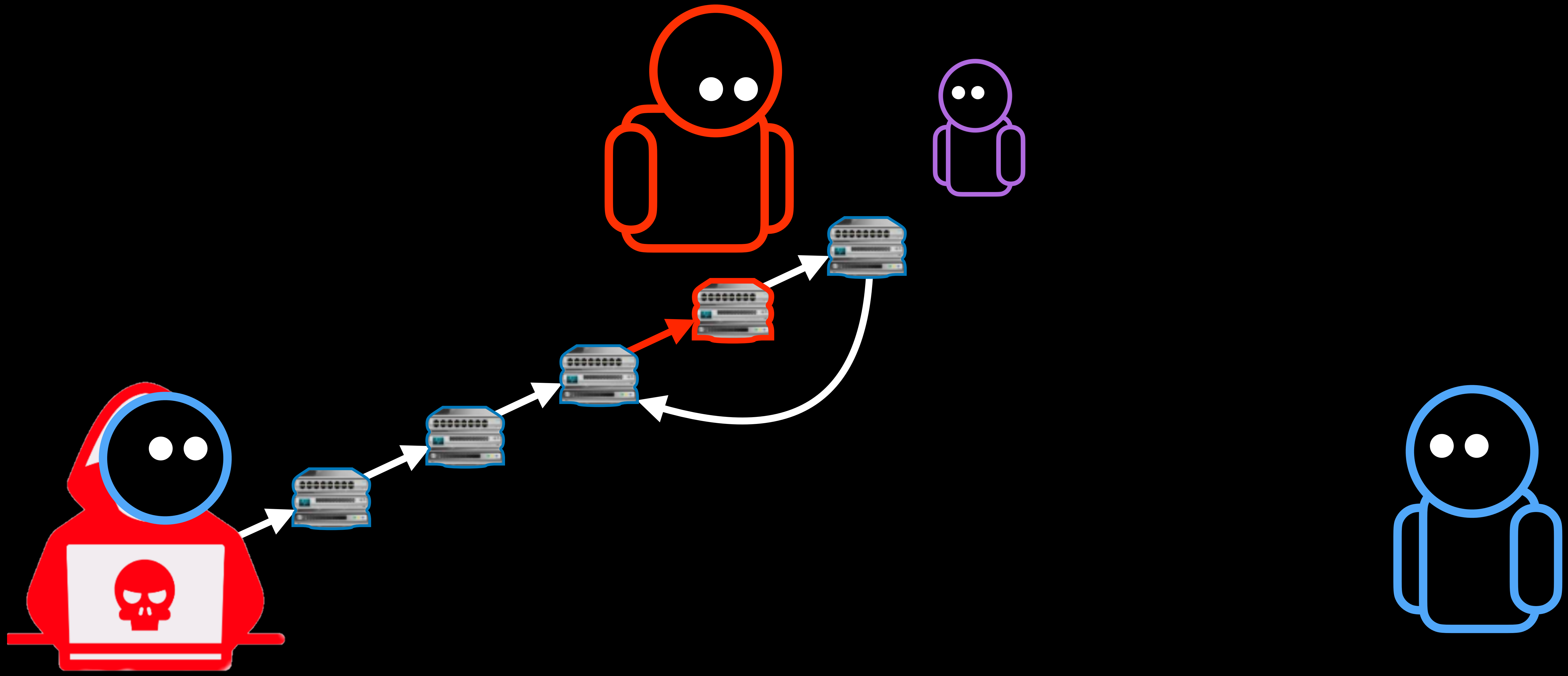
Mega-amplifier cause #2: Routing loops



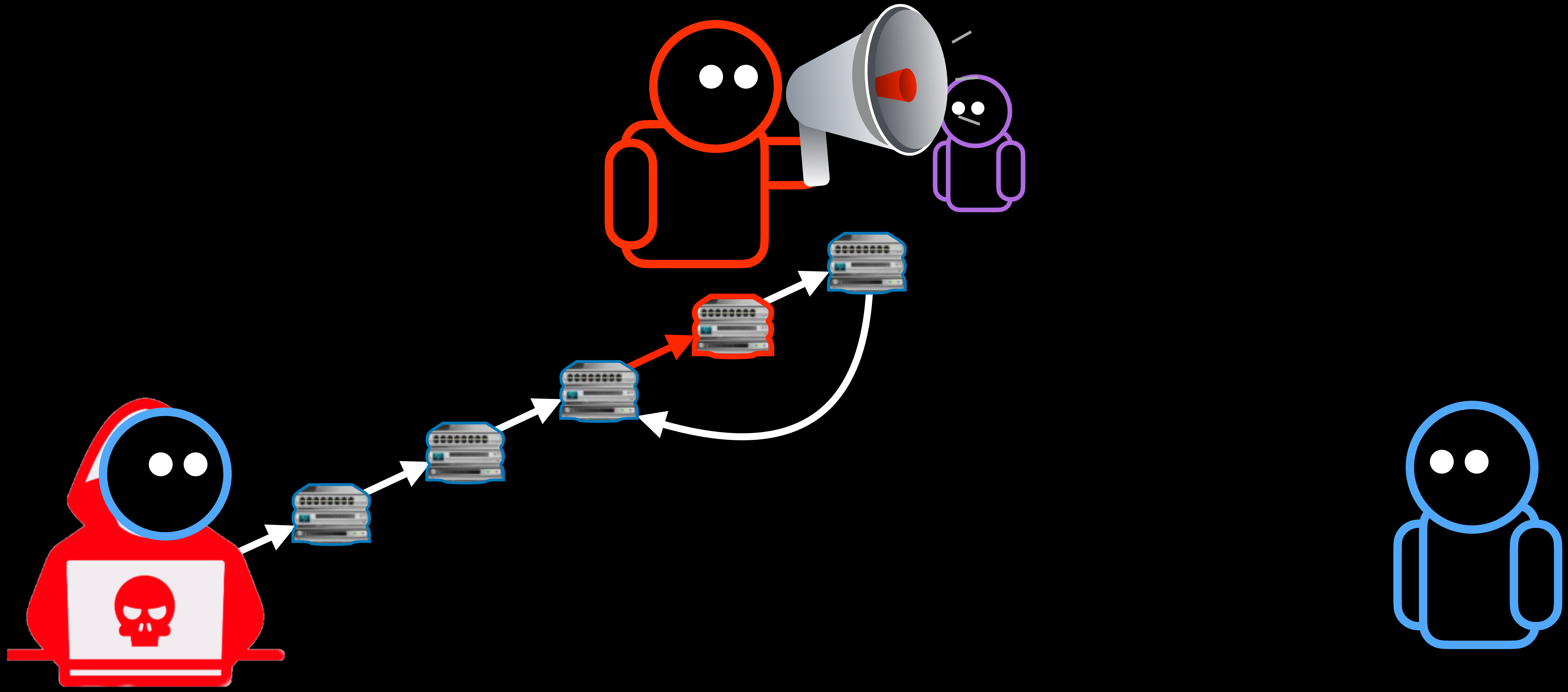
Mega-amplifier cause #2: Routing loops



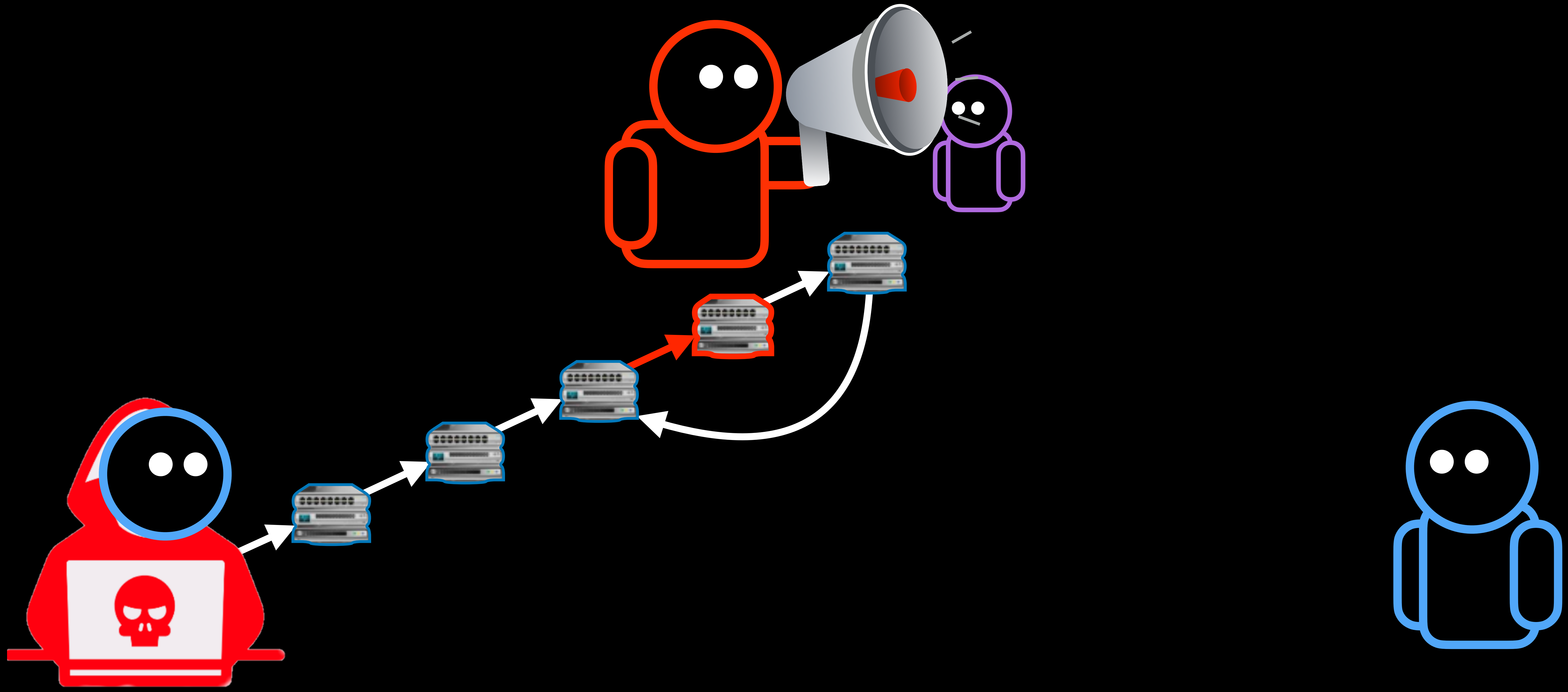
Mega-amplifier cause #2: Routing loops



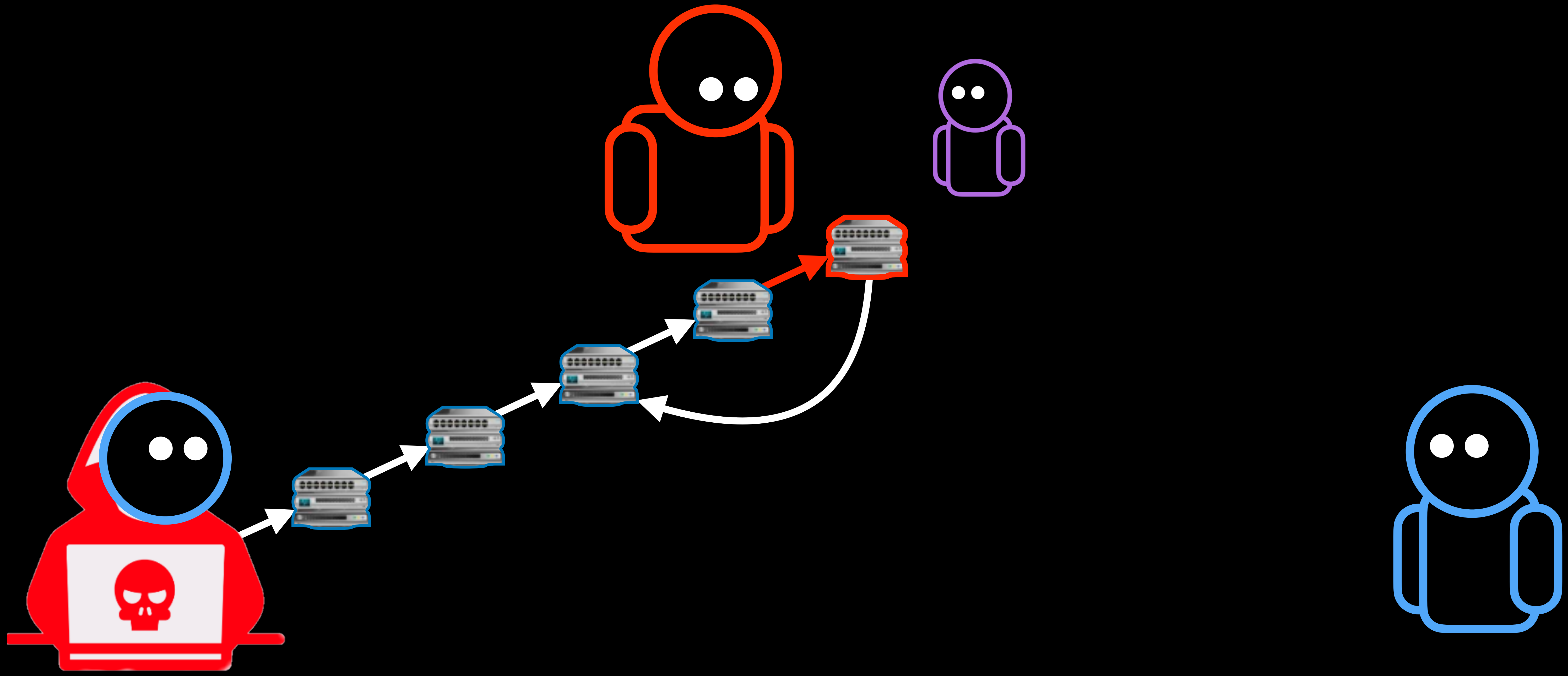
Mega-amplifier cause #2: Routing loops



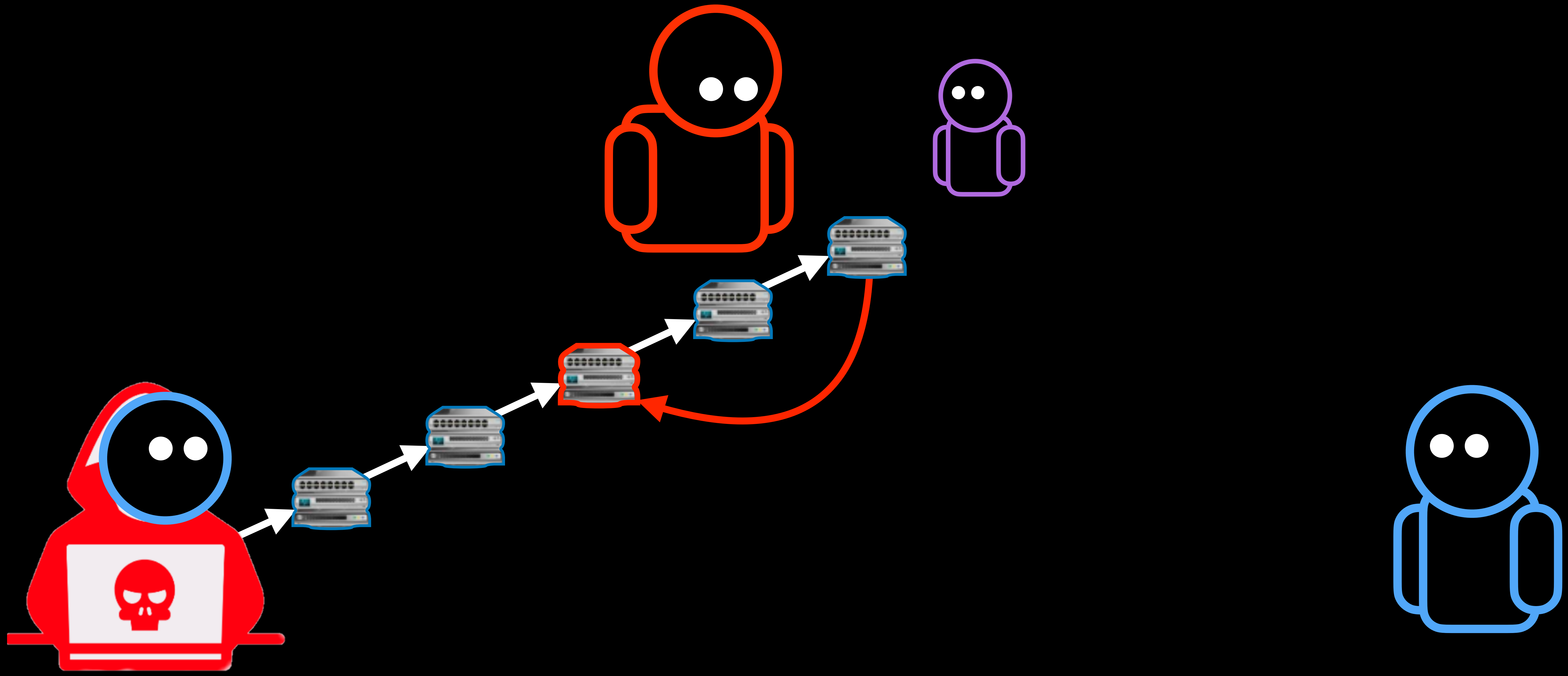
Mega-amplifier cause #2: Routing loops



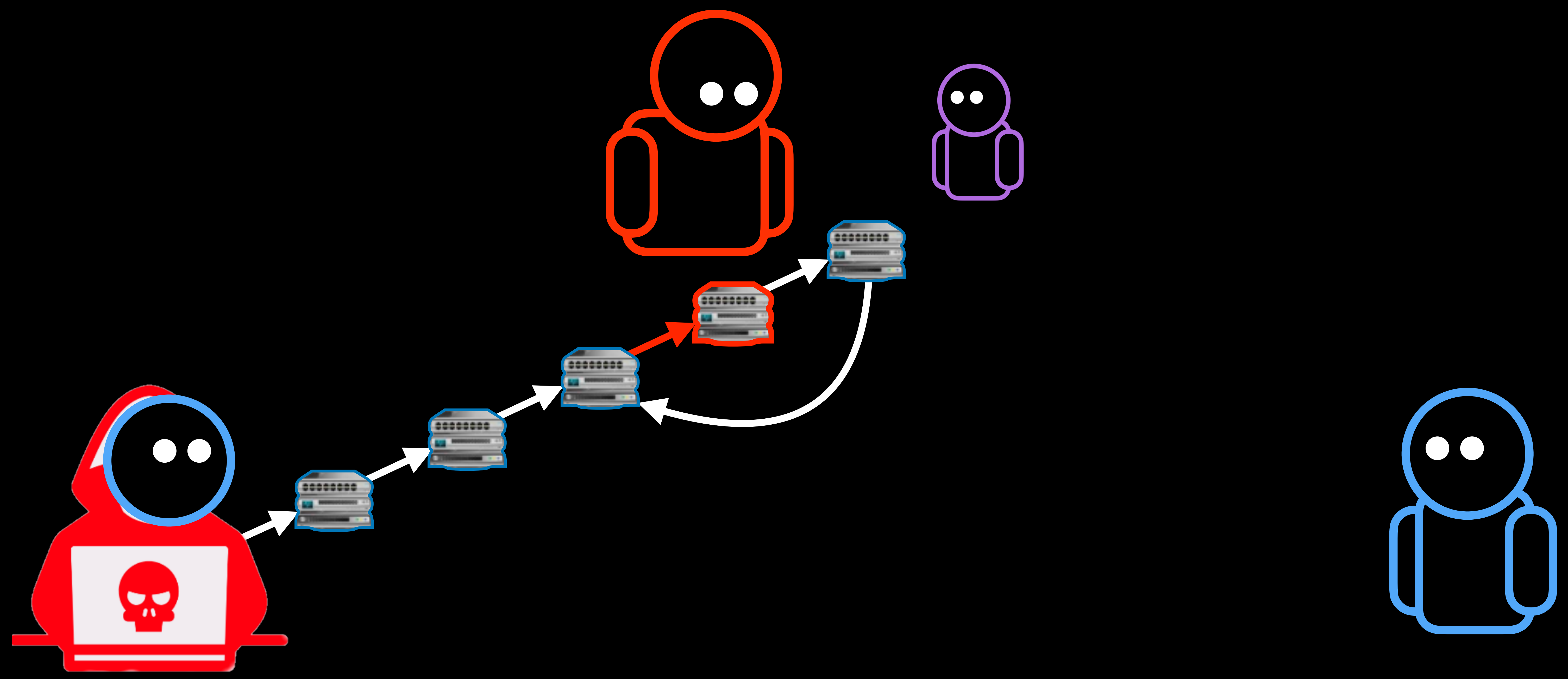
Mega-amplifier cause #2: Routing loops



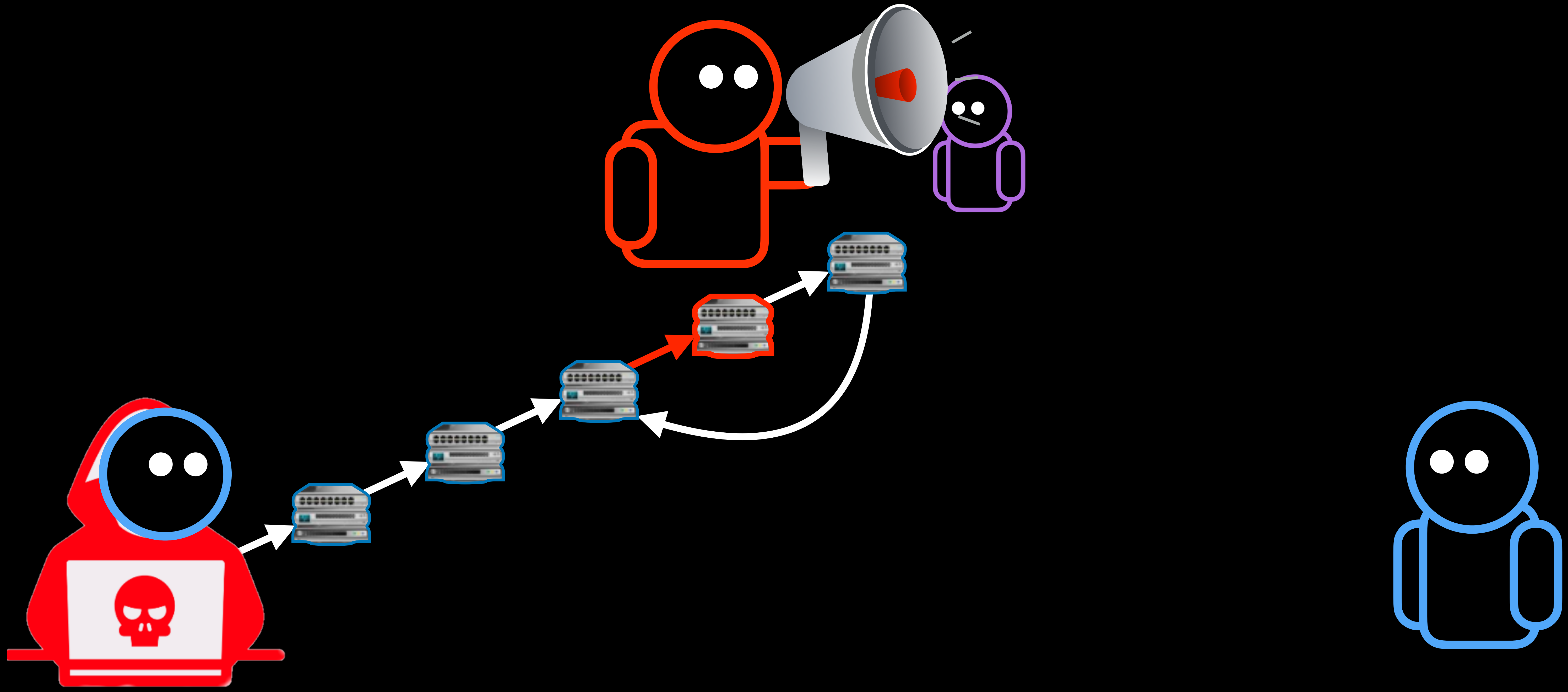
Mega-amplifier cause #2: Routing loops



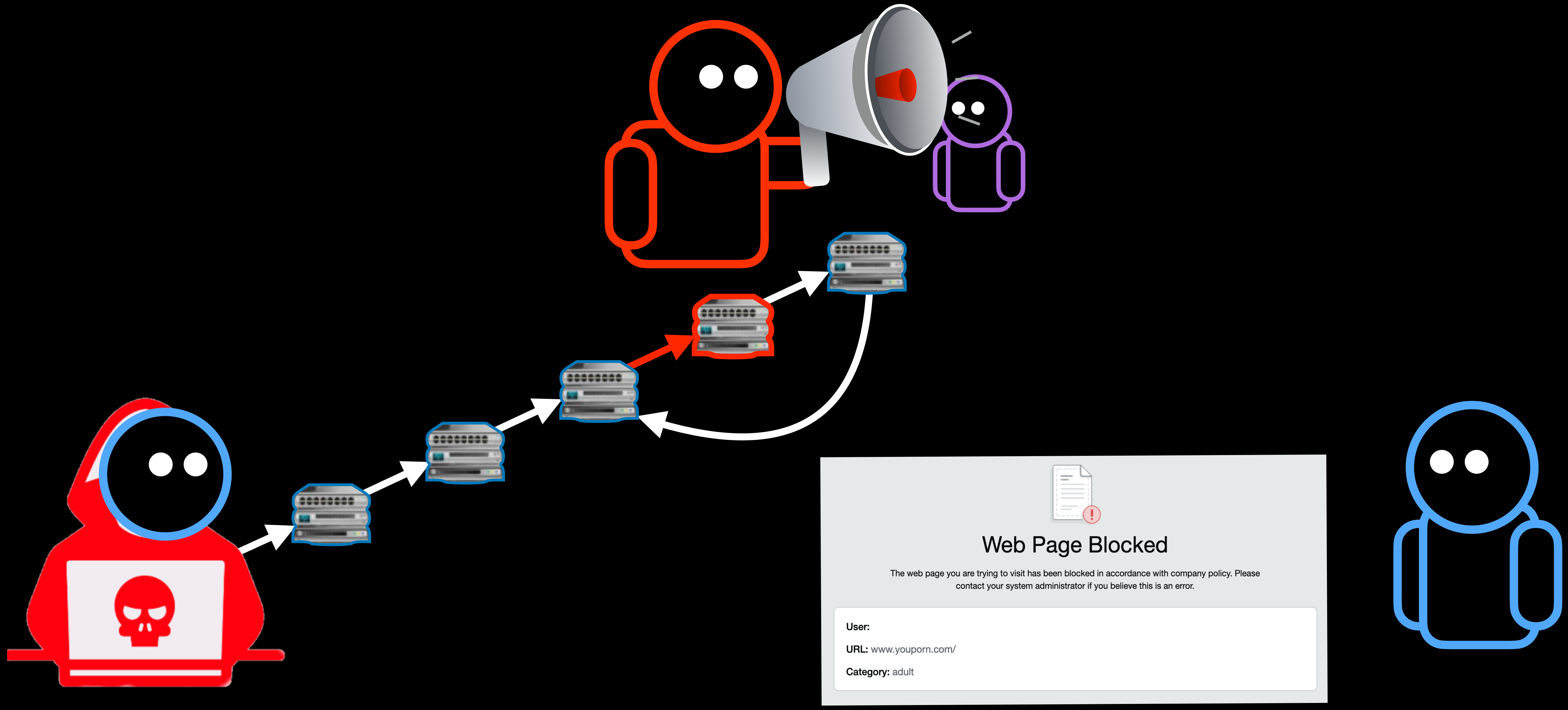
Mega-amplifier cause #2: Routing loops



Mega-amplifier cause #2: Routing loops



Mega-amplifier cause #2: Routing loops



Web Page Blocked

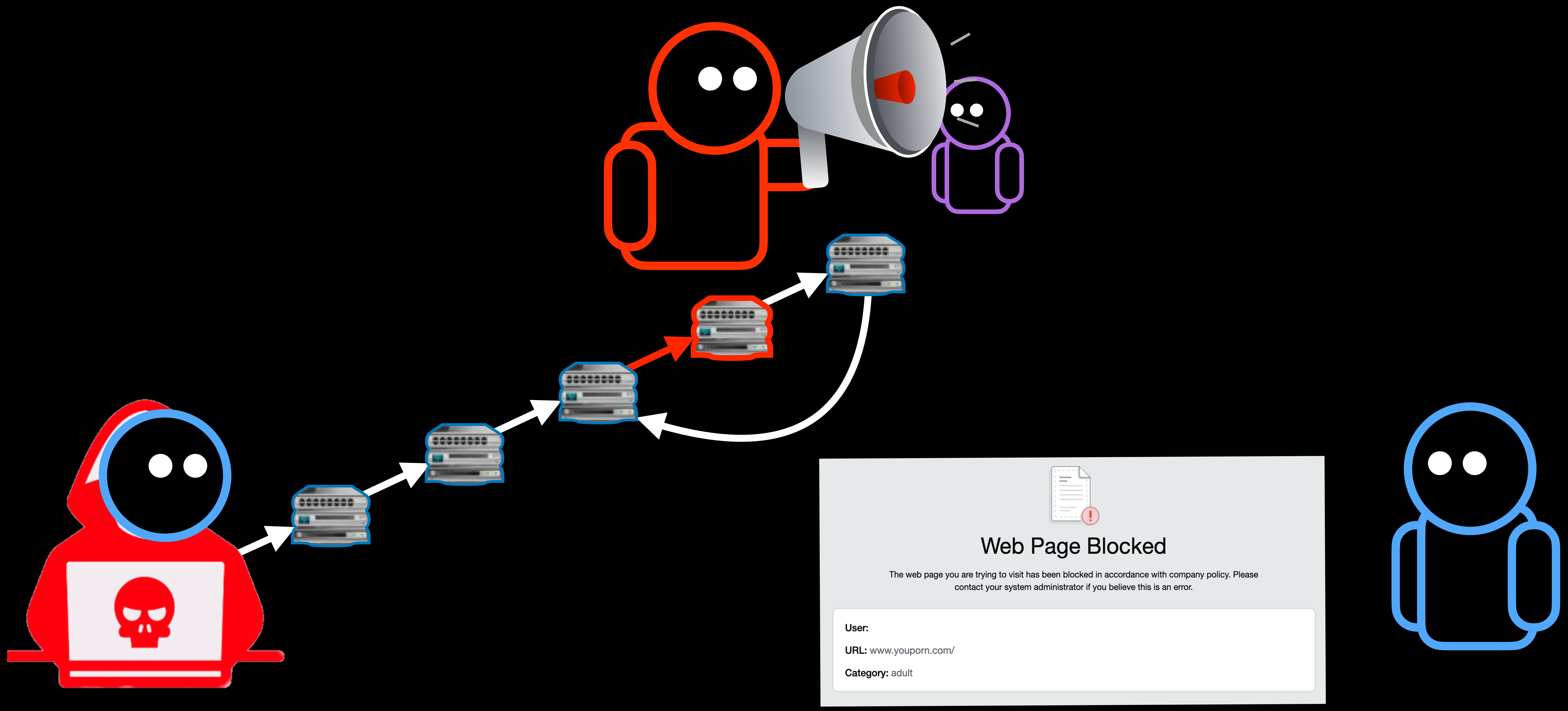
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

URL: www.youporn.com/

Category: adult

Mega-amplifier cause #2: Routing loops



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

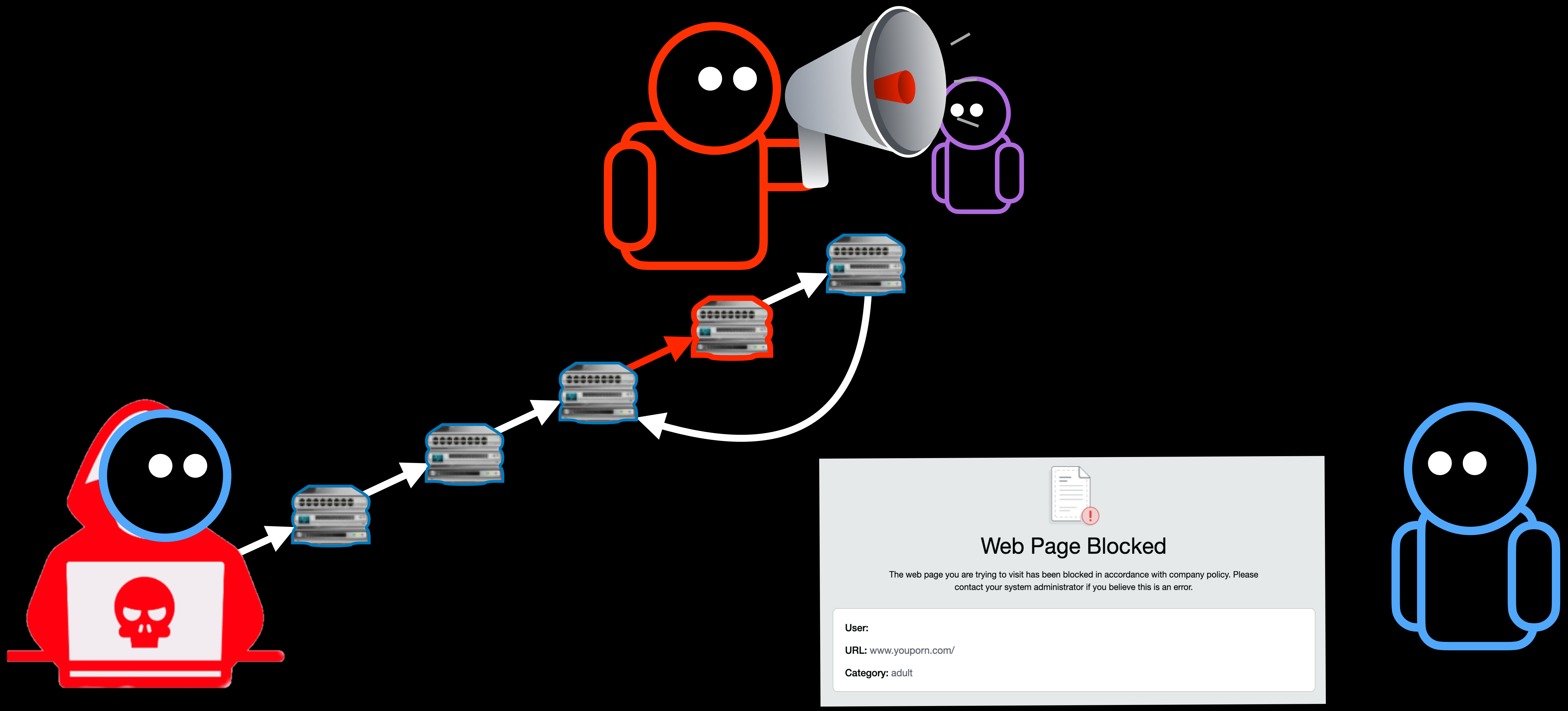
User:

URL: www.youporn.com/

Category: adult

Finite routing loops ⇒ Greater amplification with higher TTL

Mega-amplifier cause #2: Routing loops



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User:

URL: www.youporn.com/

Category: adult

Finite routing loops ⇒ Greater amplification with higher TTL

Infinite routing loops ⇒ *Infinite amplification*

Notable Amplifiers

∞	🇷🇺	ISP in Russia
949,387x	🇺🇸	Holiday Inn & Suites, Salt Lake City, USA
93,352x	🇧🇭	National Bank of Bahrain
9,084x	🇺🇸	Private Residence in Richardson Texas, USA
4,471x	🇺🇾	LACNIC Regional IP address Registry
1,265x	🇨🇳	International Bank Center, GuangZhou
312x	🇧🇪	University of Ghent, Belgium
239x	🇺🇸	City of Jacksonville, Florida
20x	🇸🇦	Entire Country of Saudi Arabia

Even defensive middleboxes pose a threat to the Internet

Responsible Disclosure

6 months prior to publication

CERTs

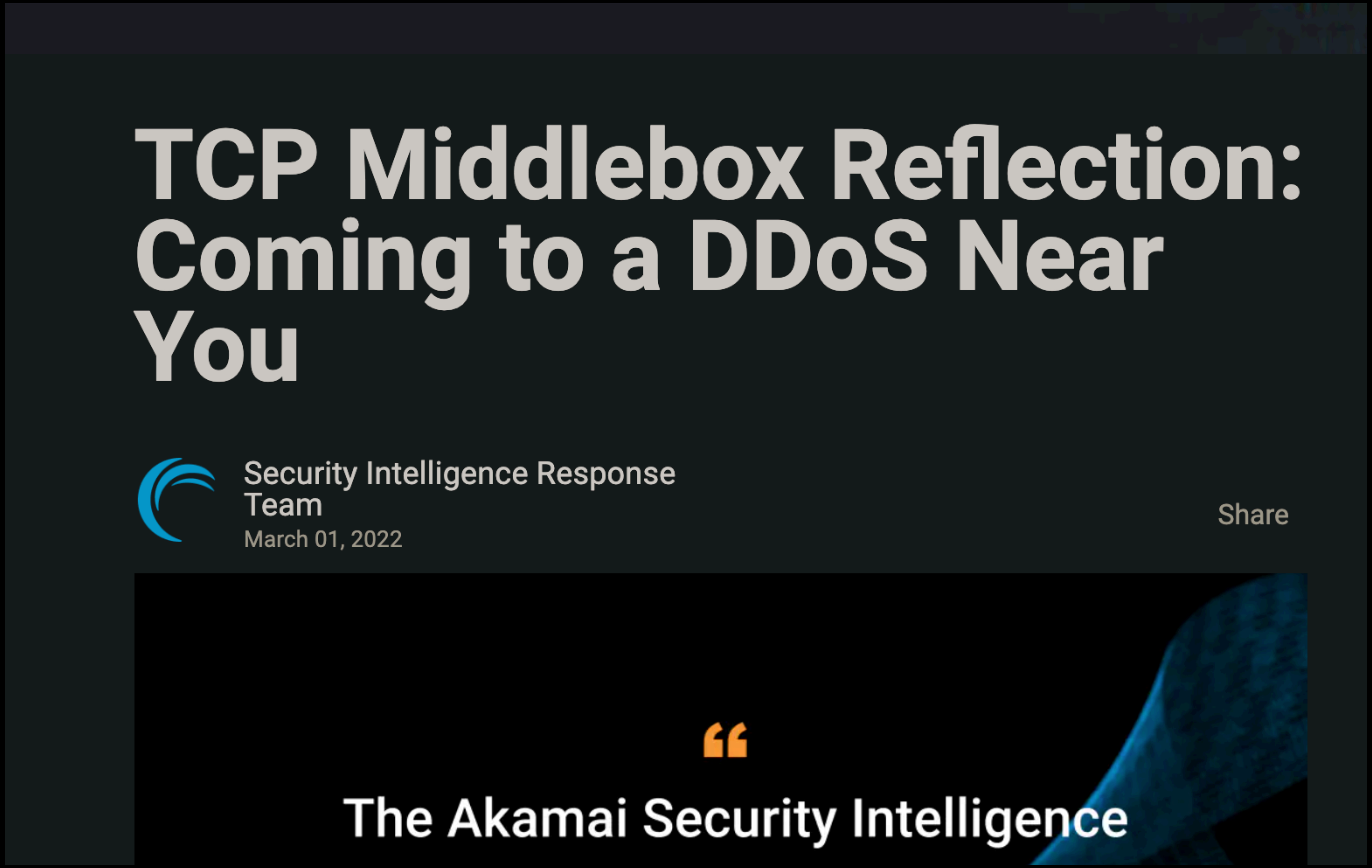
Firewall Manufacturers

DDoS Protection

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

In the Wild



TCP Middlebox Reflection: Coming to a DDoS Near You

Security Intelligence Response Team
March 01, 2022

“The Akamai Security Intelligence

…peaking at 11 Gbps at 1.5 Mpps…

Middleboxes complicate defenses

Respond with larger amounts of data

With unexpected TCP flags

While ignoring protocol signals to stop

```
17:54:20.399947 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [S], seq 0:33, win 8192, length 33
17:54:20.685491 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 1300:2156, win 8760, options [mss 1360], length 856
17:54:20.685521 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 2157, win 0, length 0
17:54:20.685563 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 0:1300, win 8760, options [mss 1360], length 1300
17:54:20.685568 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 4294966441, win 0, length 0
```

Middleboxes complicate defenses

Respond with larger amounts of data

With unexpected TCP flags

While ignoring protocol signals to stop

```
17:54:20.399947 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [S], seq 0:33, win 8192, length 33
17:54:20.685491 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 1300:2156, win 8760, options [mss 1360], length 856
17:54:20.685521 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 2157, win 0, length 0
17:54:20.685563 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 0:1300, win 8760, options [mss 1360], length 1300
17:54:20.685568 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 4294966441, win 0, length 0
```

Middleboxes complicate defenses

Respond with larger amounts of data

With unexpected TCP flags

While ignoring protocol signals to stop

```
17:54:20.399947 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [S], seq 0:33, win 8192, length 33
17:54:20.685491 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 1300:2156, win 8760, options [mss 1360], length 856
17:54:20.685521 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 2157, win 0, length 0
17:54:20.685563 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 0:1300, win 8760, options [mss 1360], length 1300
17:54:20.685568 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 4294966441, win 0, length 0
```

Middleboxes complicate defenses

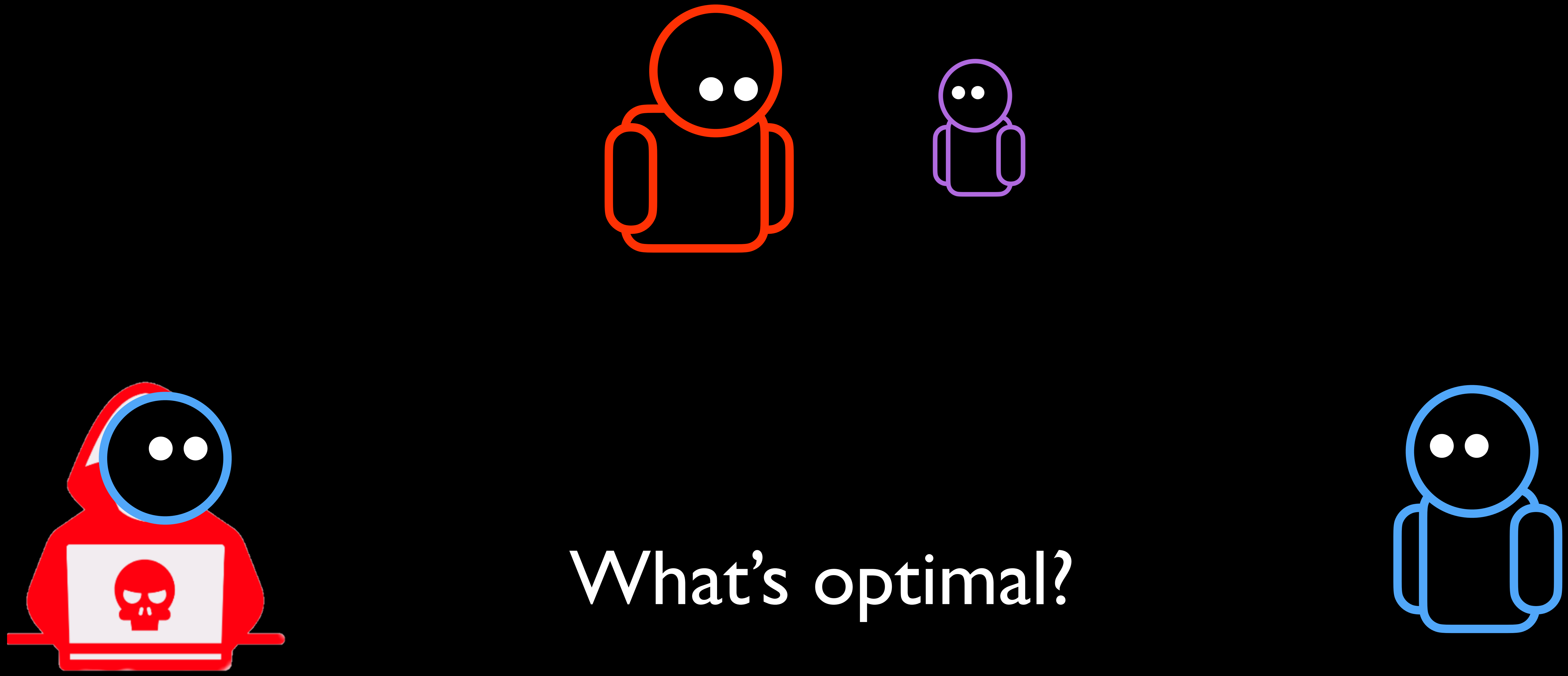
Respond with larger amounts of data

With unexpected TCP flags

While ignoring protocol signals to stop

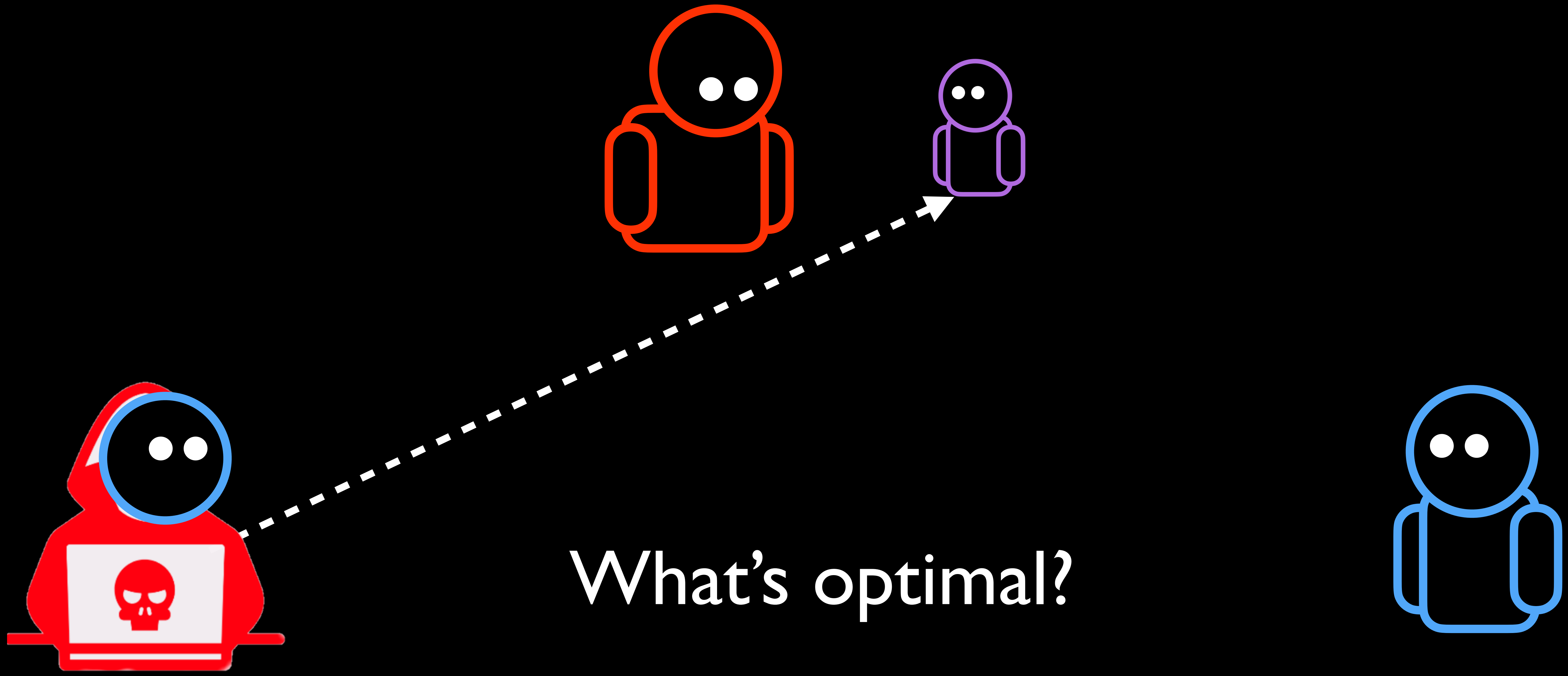
```
17:54:20.399947 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [S], seq 0:33, win 8192, length 33
17:54:20.685491 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 1300:2156, win 8760, options [mss 1360], length 856
17:54:20.685521 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 2157, win 0, length 0
17:54:20.685563 IP Z.Z.Z.Z.443 > X.X.X.X.45678: Flags [S], seq 0:1300, win 8760, options [mss 1360], length 1300
17:54:20.685568 IP X.X.X.X.45678 > Z.Z.Z.Z.443: Flags [R.], seq 0, ack 4294966441, win 0, length 0
```

Attackers are still optimizing



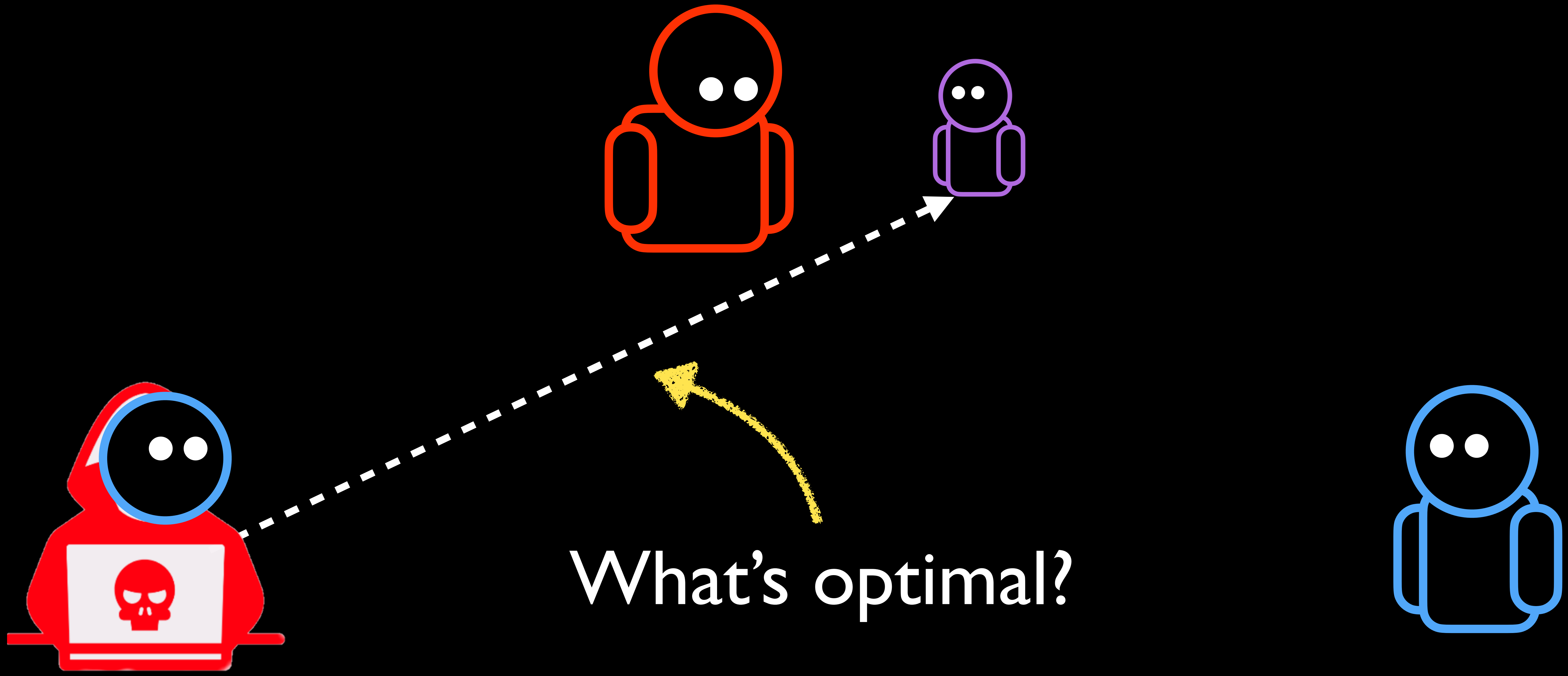
What's optimal?

Attackers are still optimizing



What's optimal?

Attackers are still optimizing



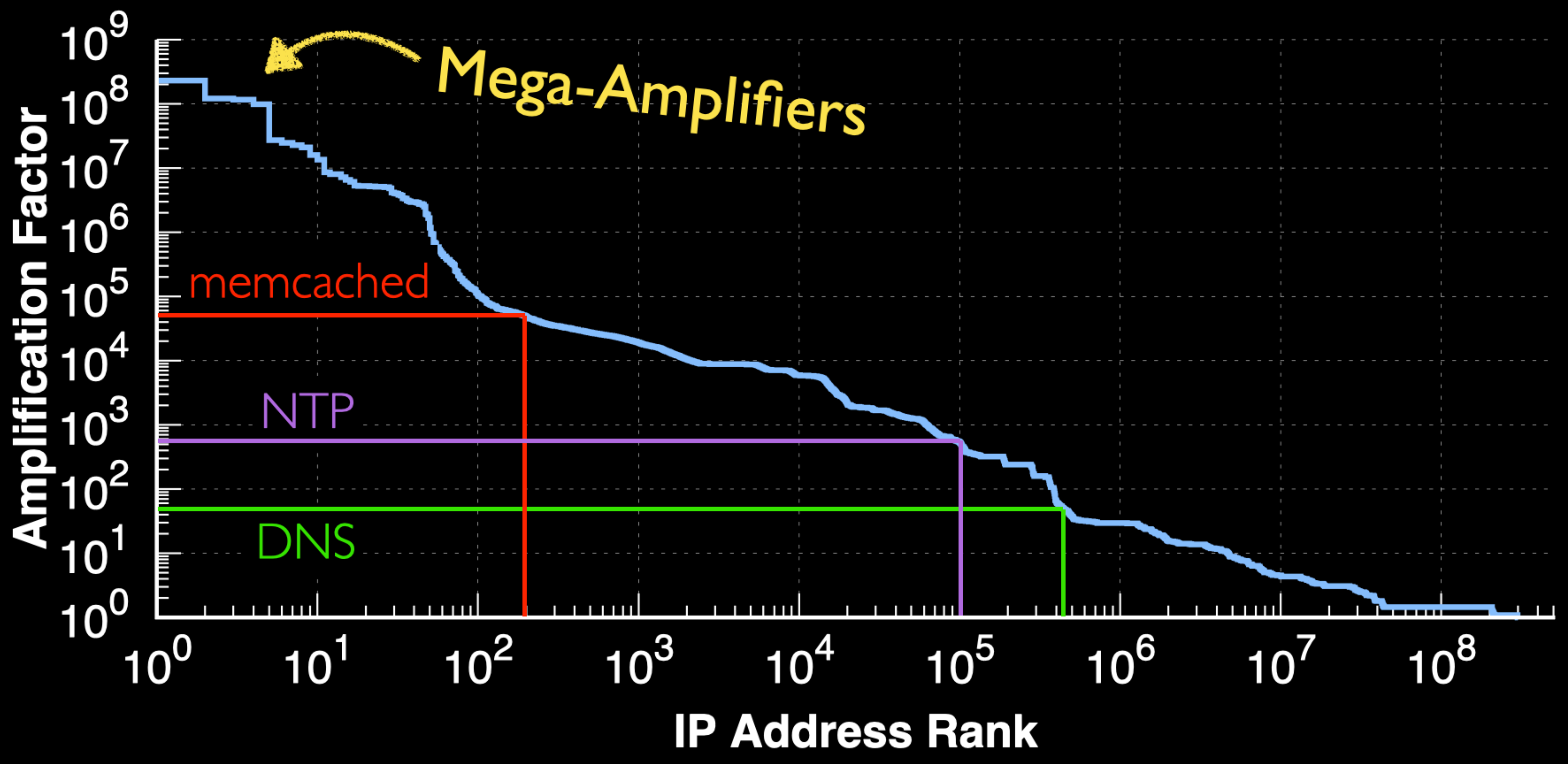
What's optimal?

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