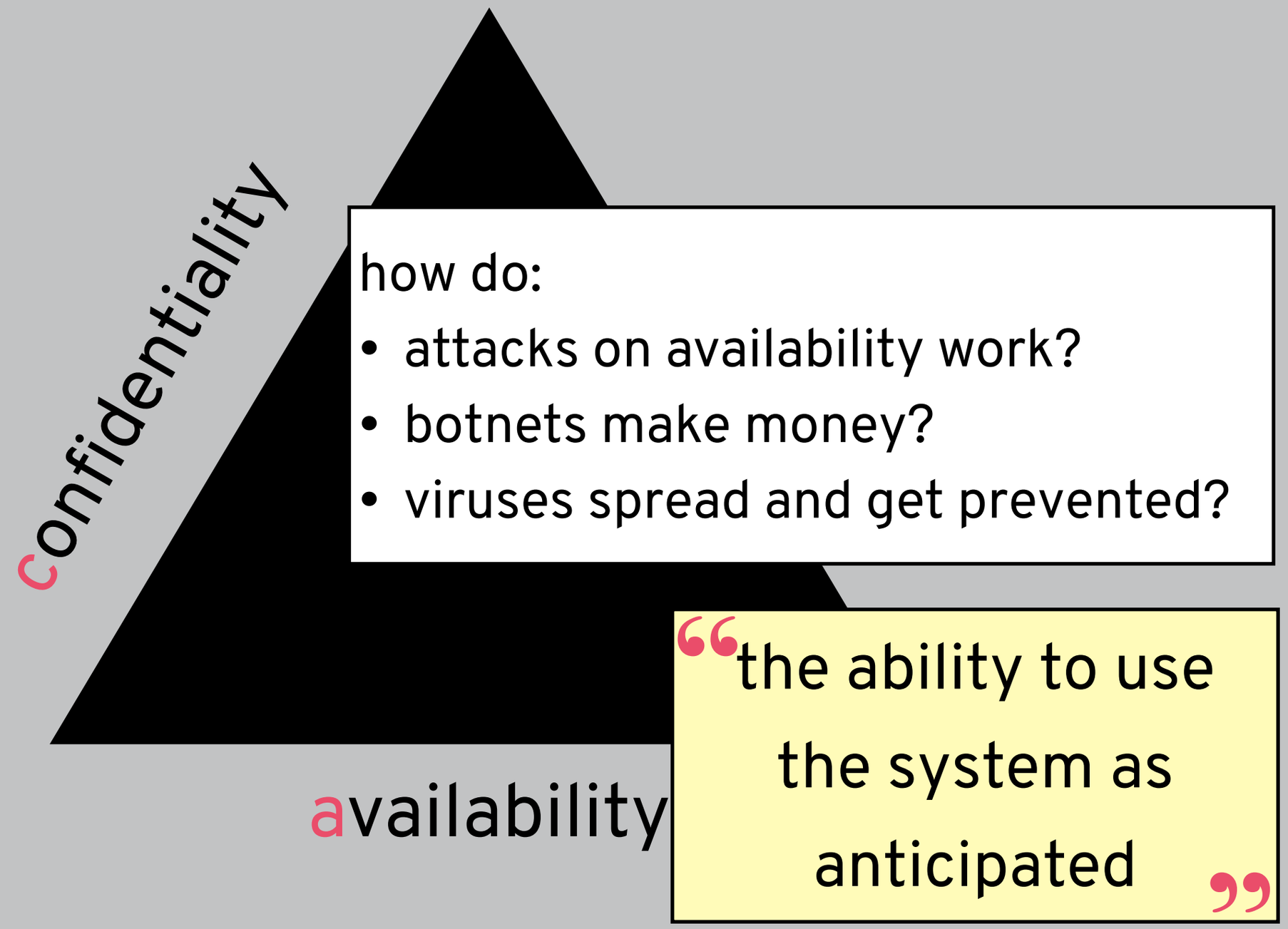
SECURITY (COMP0141): AVAILABILITY

UCL

AVAILABILITY



WHY IS AVAILABILITY IMPORTANT?

goal: prevent Alice from getting to that website

`http://me.bob.com/hi.html`

can’t get stuff done

can’t run business (make $)

THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

Malware

THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

Malware

THREAT MODEL FOR DOS

goal: take down a service

simple: have one machine

distributed: have many machines

$: small amount of computational power

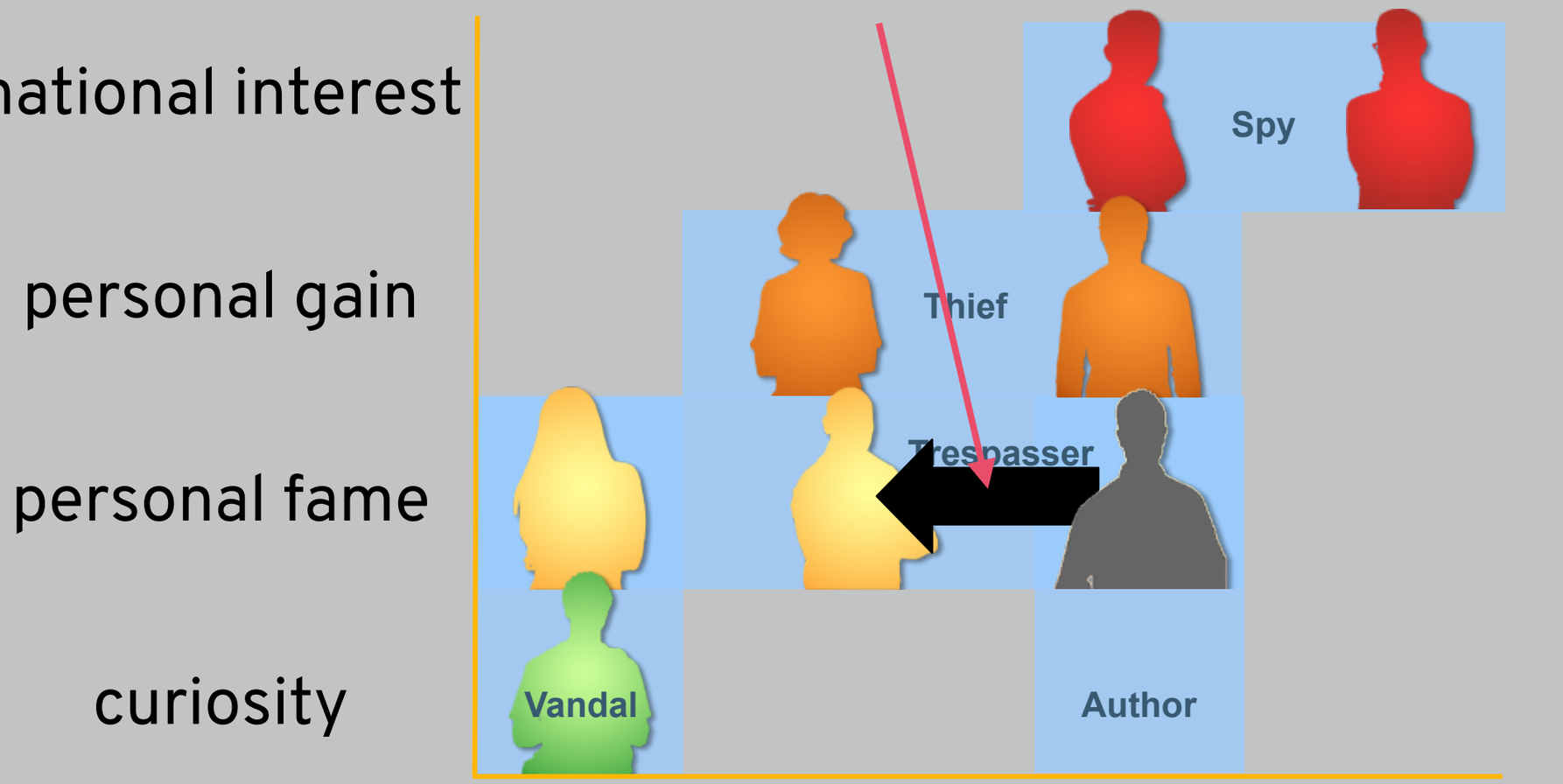
$$$: large amount of computational power

clueless: little technical ability

savvy: strong technical ability

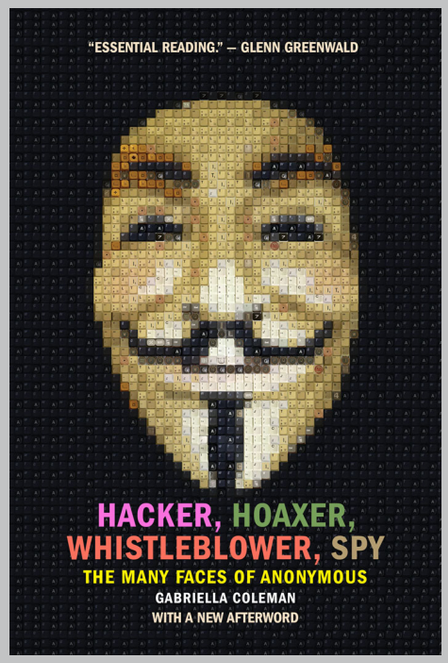
THREAT LANDSCAPE

tools created by experts now used by less-skilled attackers and criminals



(David Aucsmith, Microsoft)

ANONYMOUS



politically motivated attacks

targets advertised on social media

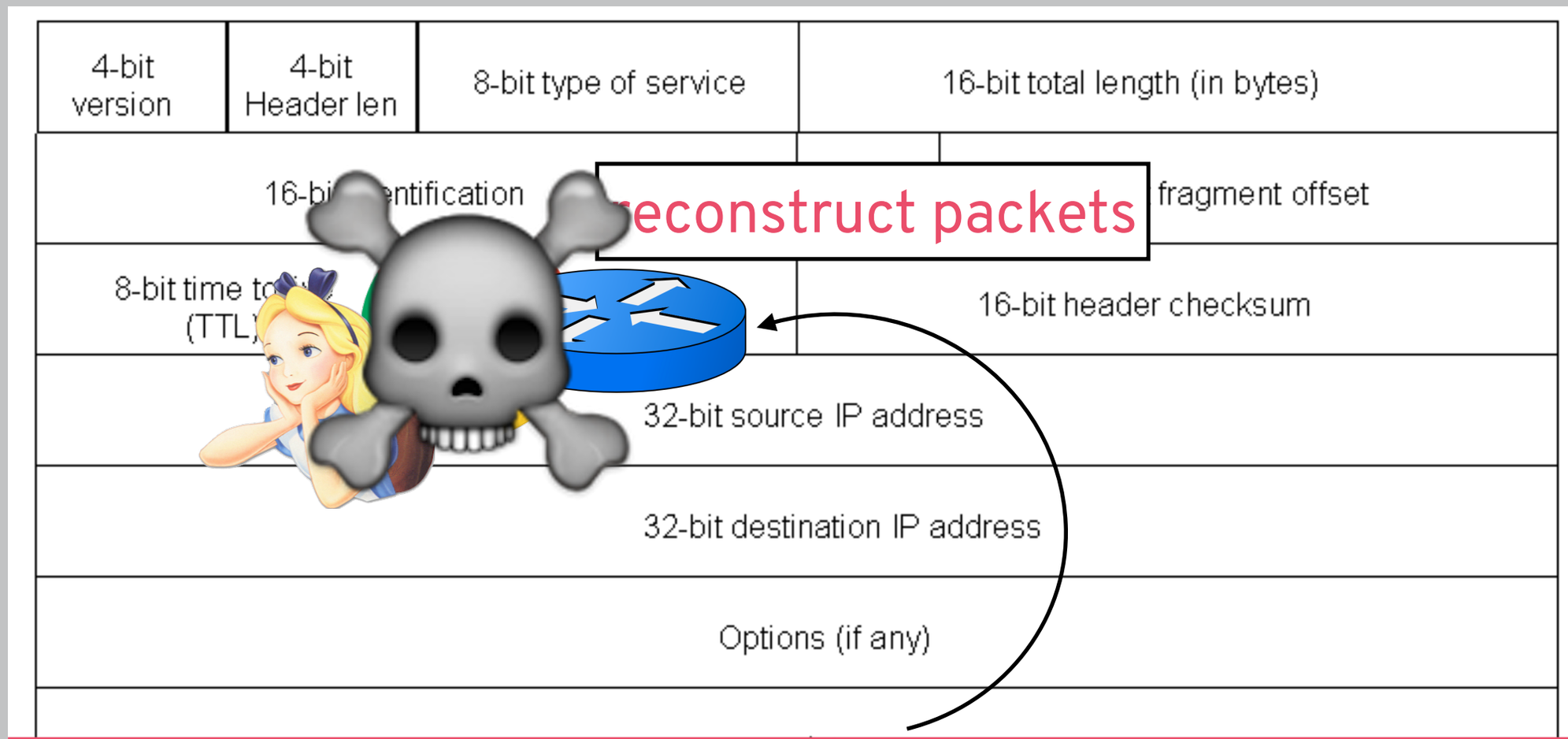
join by downloading Loic program

famous targets: PayPal, Scientology, Sony, Visa

HOW DOES DOS WORK?

“Ping of death” 

PING OF DEATH



20 Bytes	8 Bytes	65.510 Bytes
IP Header	ICMP header	ICMP data

The size of this packet is 65.538 bytes. It exceedes the size limit prescribed by RFC 791, *Internet Protocol*, which is 65.535 bytes. As the packet is transmitted, it becomes broken into numberous fragments. The reassembly process might cause the receiving system to crash

PING OF DEATH

vulnerability?

reconstruction fails on packets that are too big

threat?

simple: have one machine

$: small amount of computational power

clueless(-ish): little technical ability

protection?

easy: filter out these packets before reconstruction

HOW DOES DOS WORK?

“Ping of death” 

Unintentional 

UNINTENTIONAL

UNINTENTIONAL

vulnerability?

inability to predict spikes in popularity

threat?

distributed: have many machines

$$$: large amount of computational power

clueless: little technical ability (not even an attack!)

protection?

hard: no real way to know

HOW DOES DOS WORK?

“Ping of death”

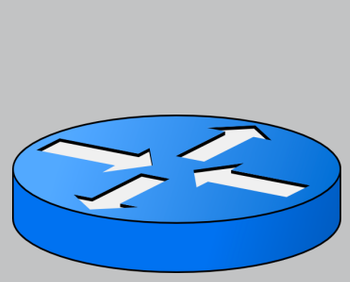
Unintentional

Smurf attack

BROADCAST ADDRESSES

192.168.1.119

192.168.1.5



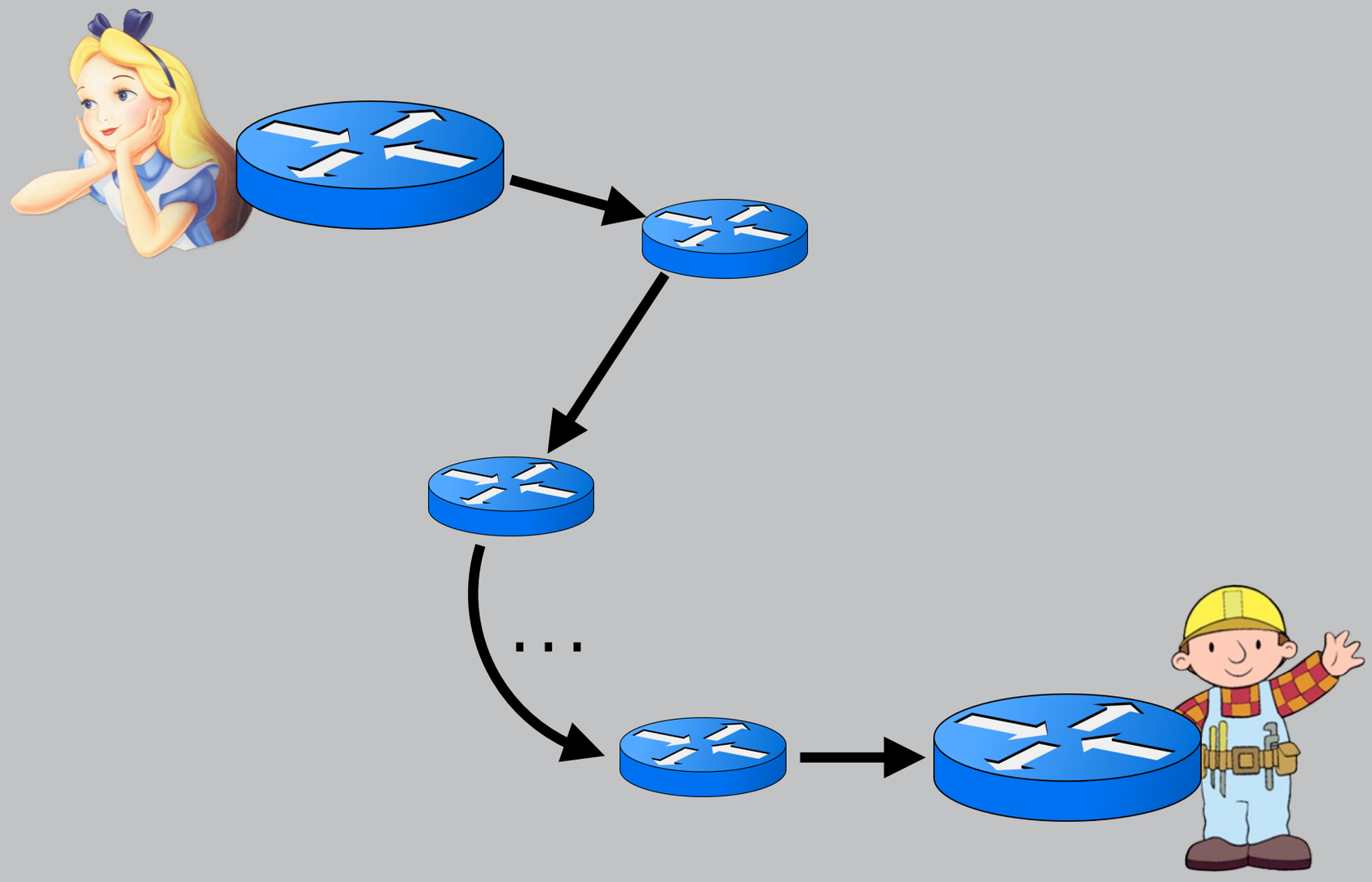
192.168.1.1

represents
192.168.1.2 –
192.168.1.255

192.168.1.23

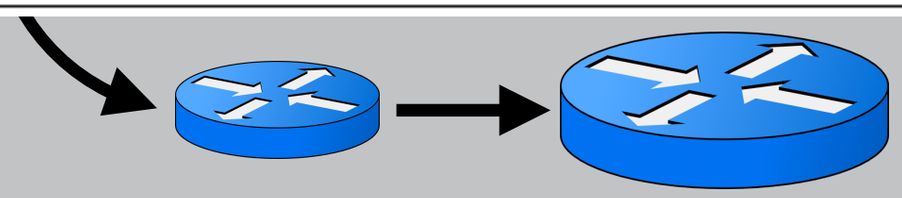
192.168.1.58

IP SPOOFING



IP SPOOFING

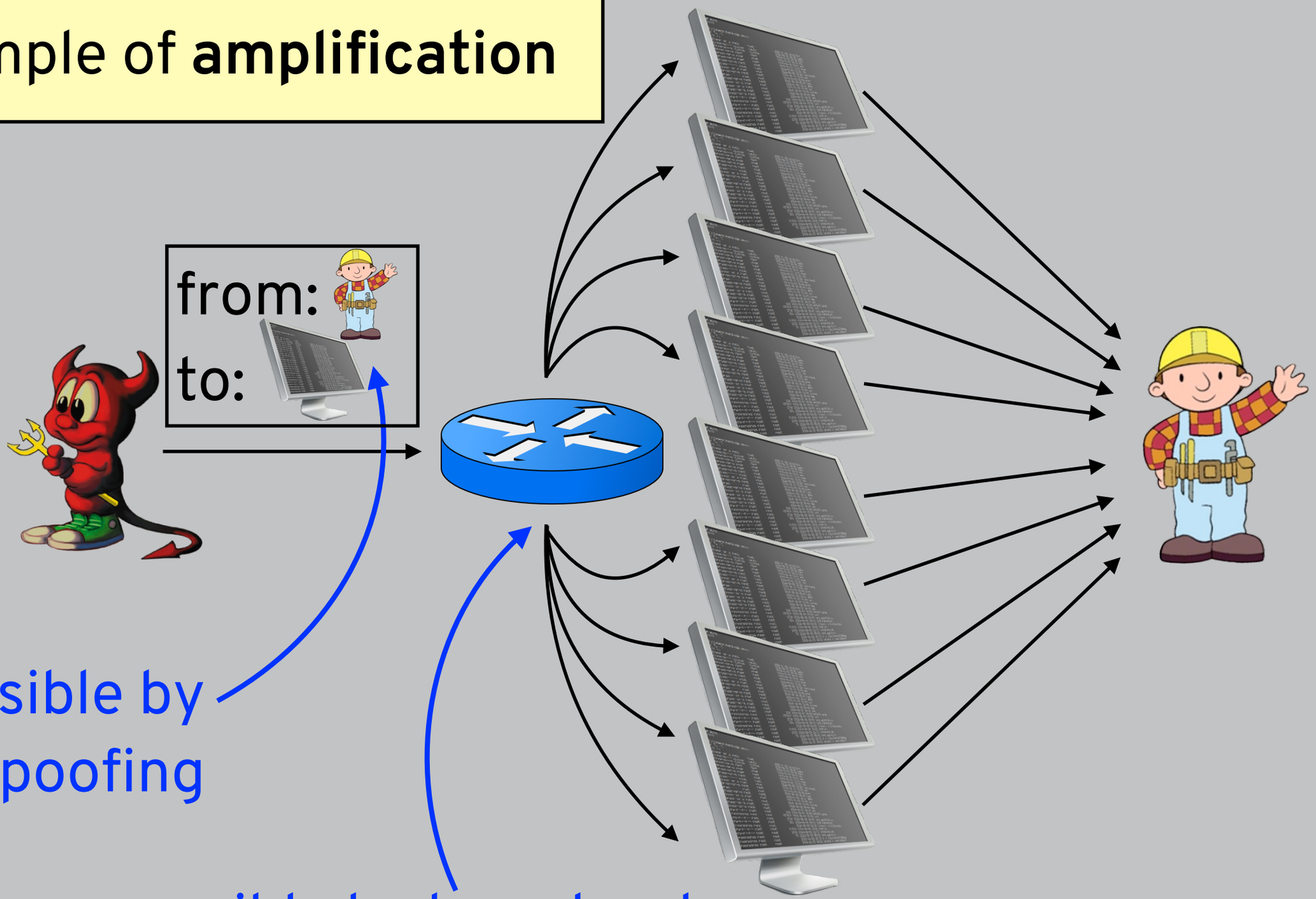
4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)		8-bit protocol	16-bit header checksum	
Professor Evil's ~~Alice's~~ IP address				
Bob's IP address				
Options (if any)				
"I want the content at `hi.html`"				



the Internet was not designed for security!

SMURF ATTACK

example of **amplification**



SMURF ATTACK

vulnerability?

ability to fake source IP address + use broadcast

threat?

simple: have one machine

$: small amount of computational power

savvy(-ish): strong technical ability

protection?

pretty easy: don't allow this usage of broadcast

HOW DOES DOS WORK?

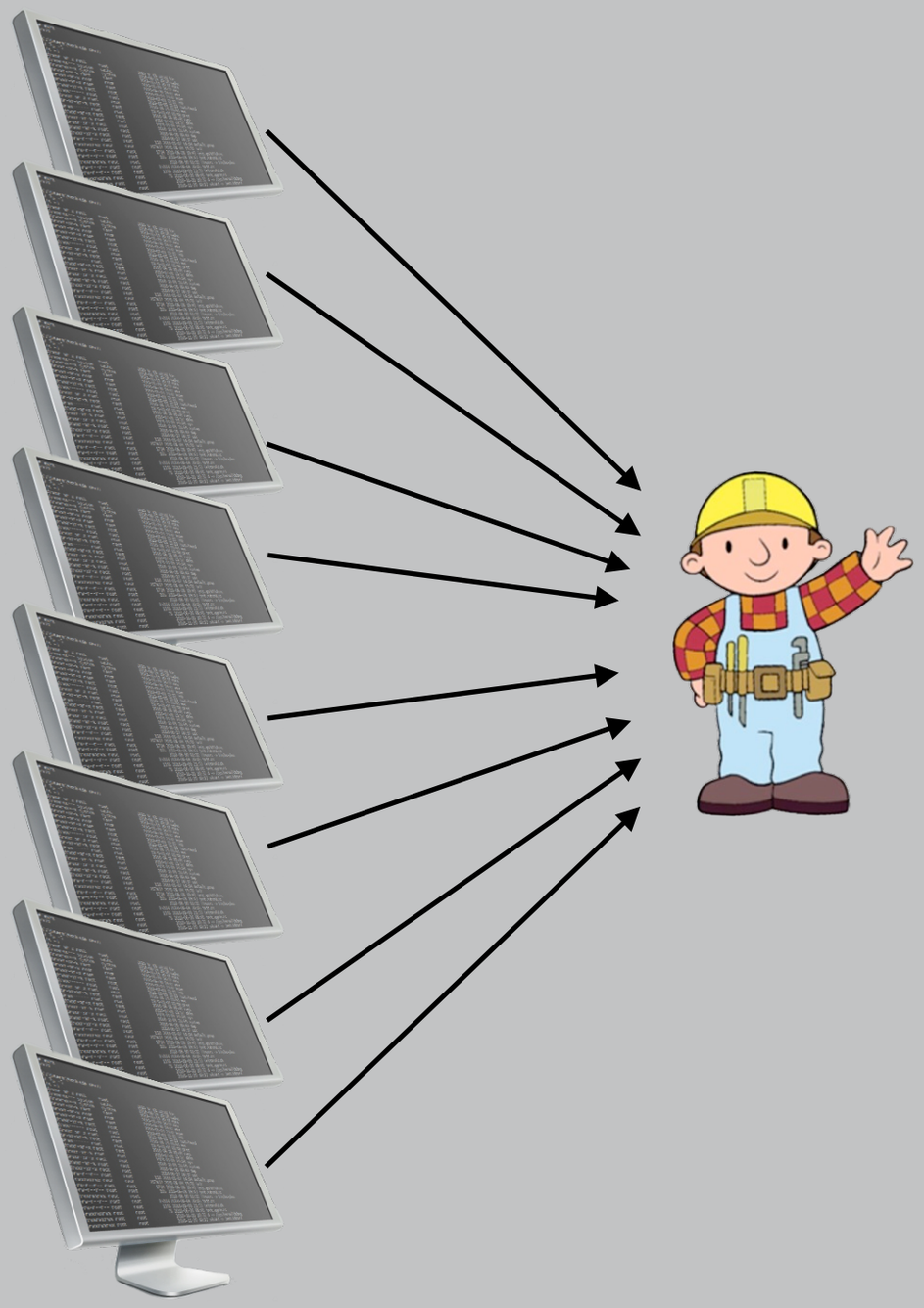
“Ping of death”

Unintentional

Smurf attack

DDoS

DISTRIBUTED DOS (DDOS)



DDOS

vulnerability?

none, really!

threat?

distributed: have many machines

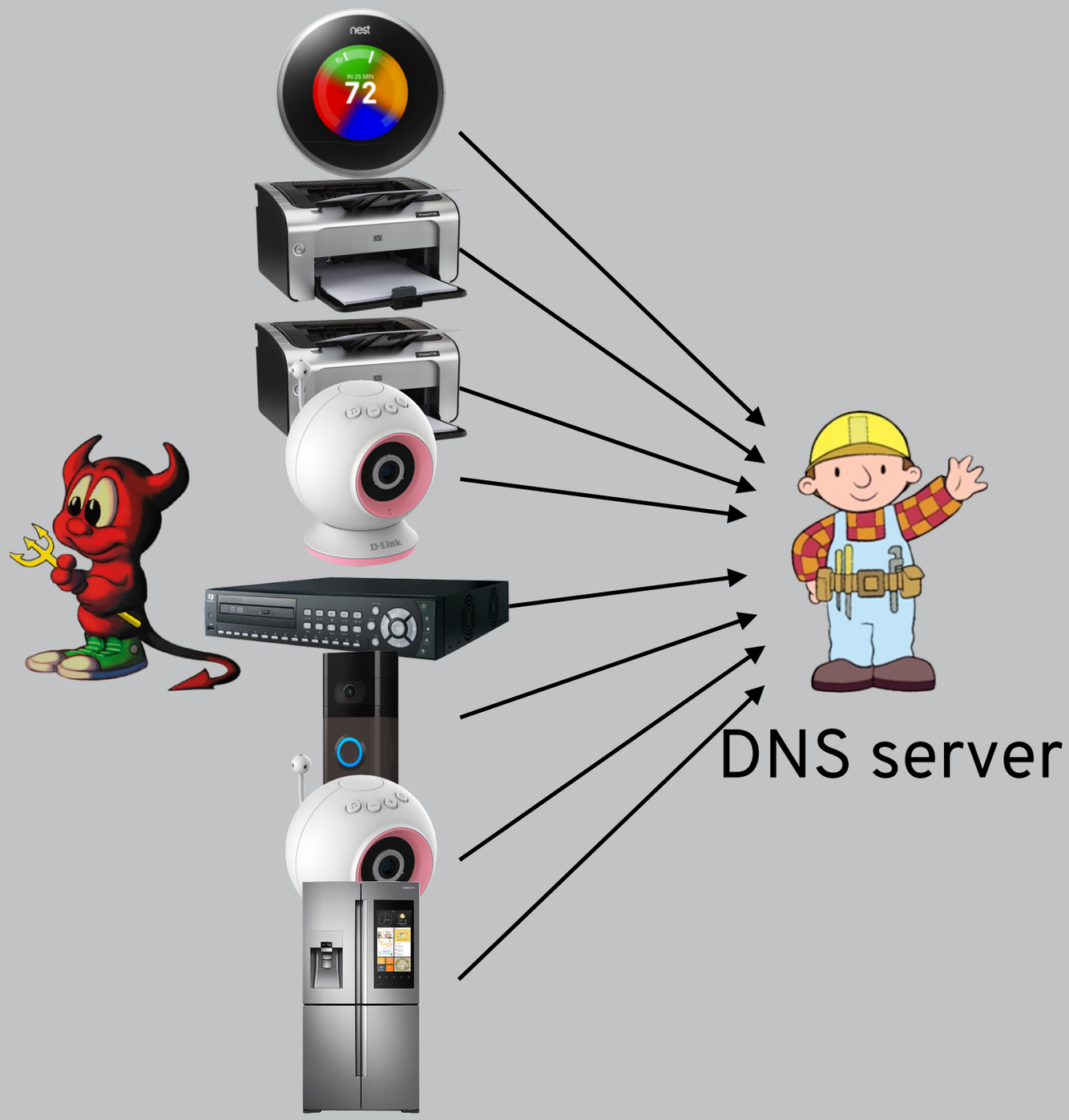
$$$: large amount of computational power

savvy: strong technical ability

protection?

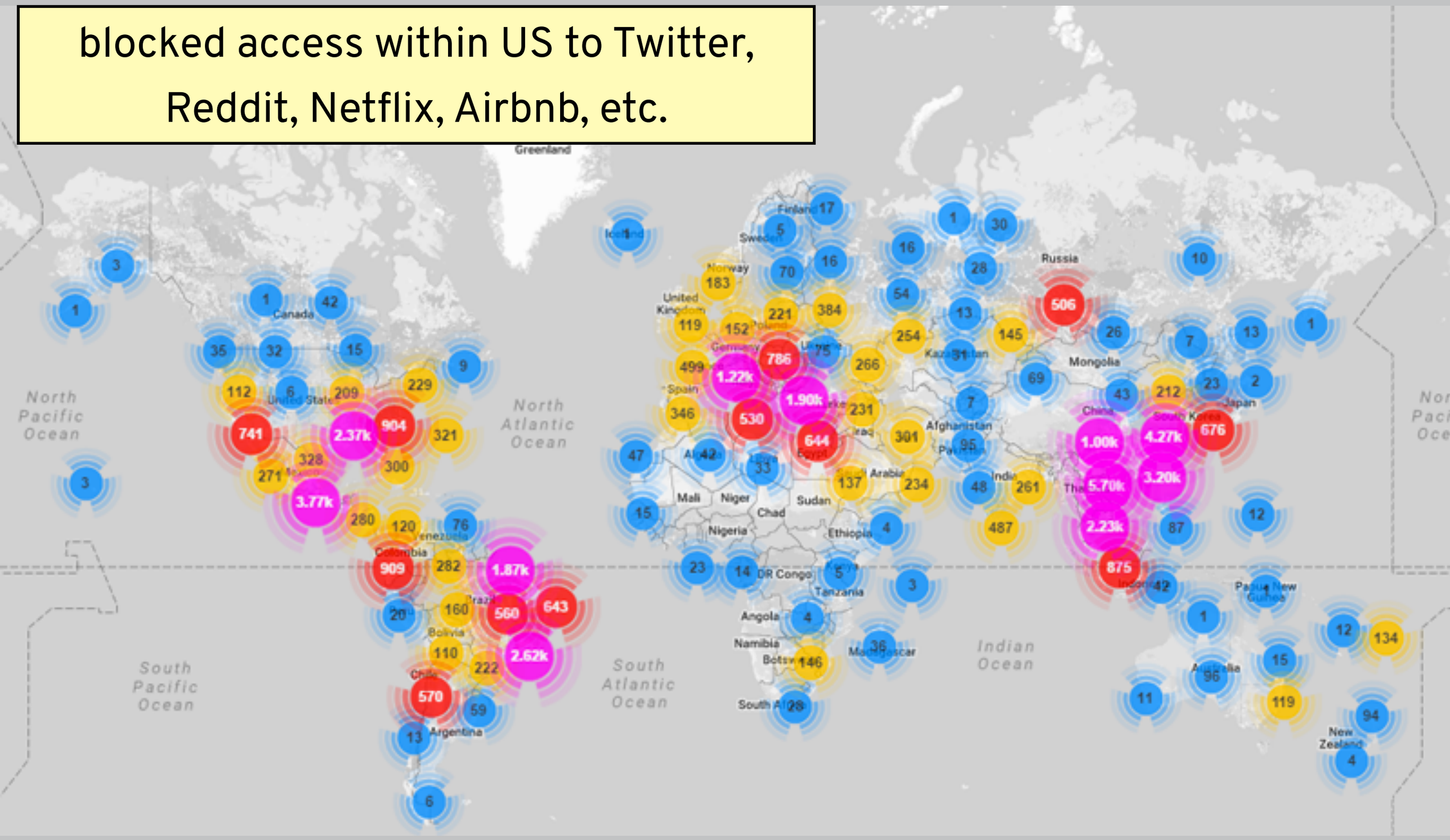
very difficult!

EXAMPLE: MIRAI (2016)



EXAMPLE: MIRAI (2016)

blocked access within US to Twitter, Reddit, Netflix, Airbnb, etc.



EXAMPLE: GITHUB ATTACK (2018)

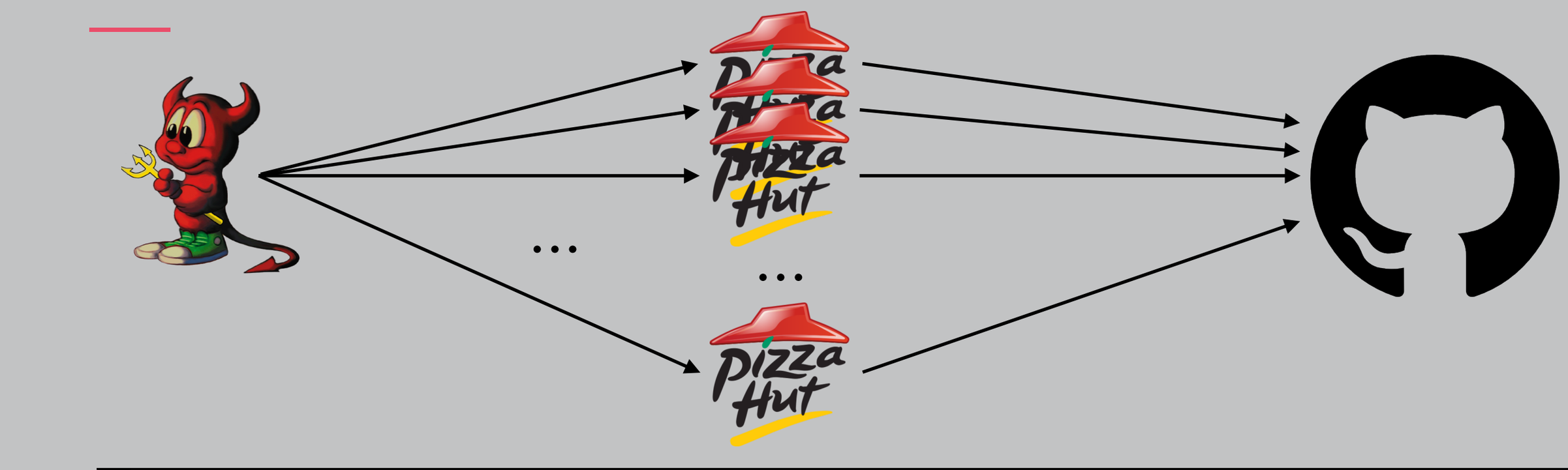
You can achieve amplification without broadcast

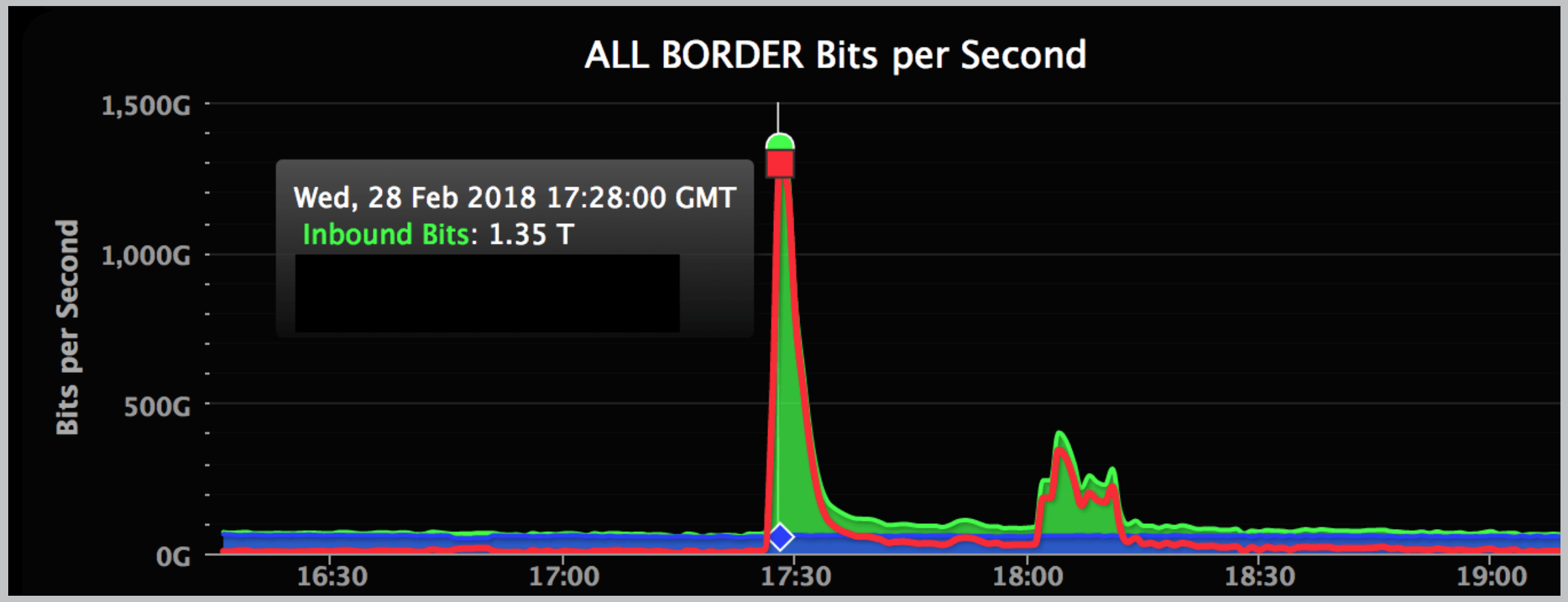
"I'd like one of everything and please call back to list every item of my order"

"Pizza with mushrooms
Pizza with pepperoni
…"

This is the intuition behind a **memcached** attack — no botnets needed!

EXAMPLE: GITHUB ATTACK (2018)





EXAMPLE: GITHUB ATTACK (2018)

You can achieve amplification without broadcast

"I'd like one of everything and please call back to list every item of my order"

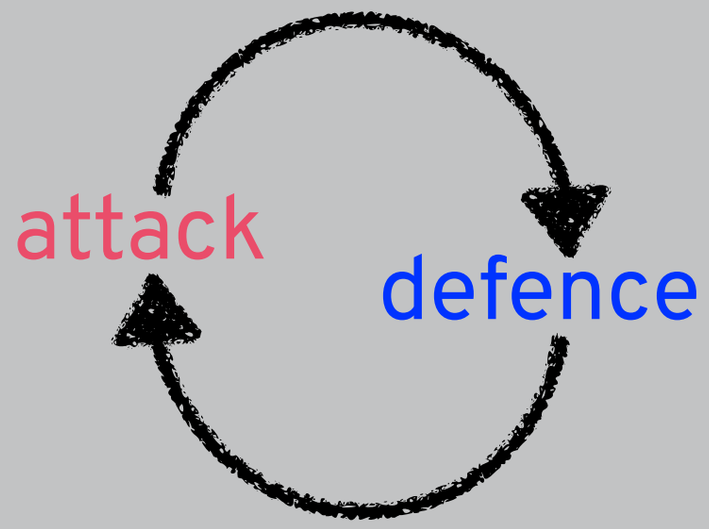
"Pizza with mushrooms
Pizza with pepperoni
…"

This is the intuition behind a **memcached** attack — no botnets needed!

Actually though, Github survived this attack!

DDOS PROTECTION

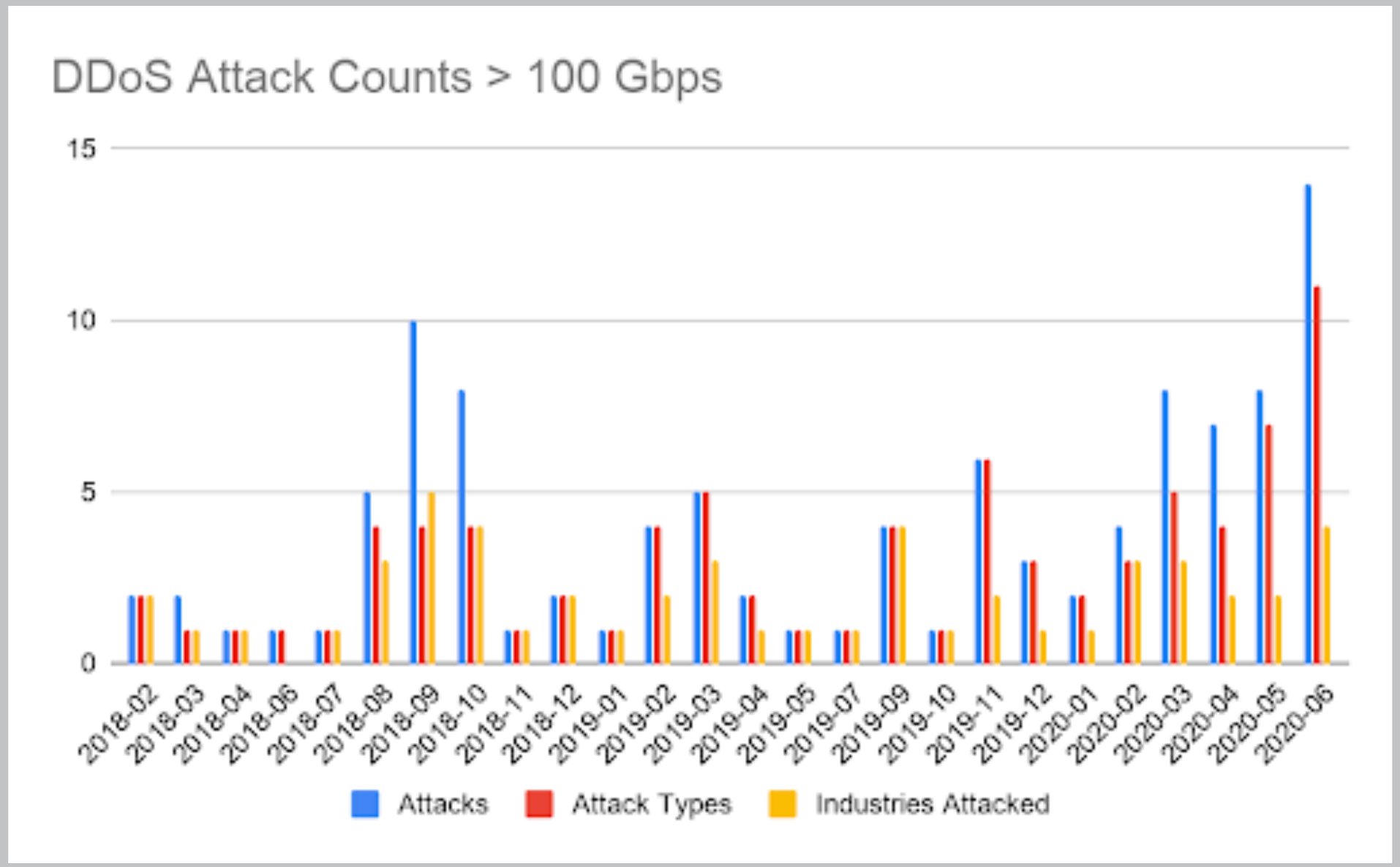
risk management



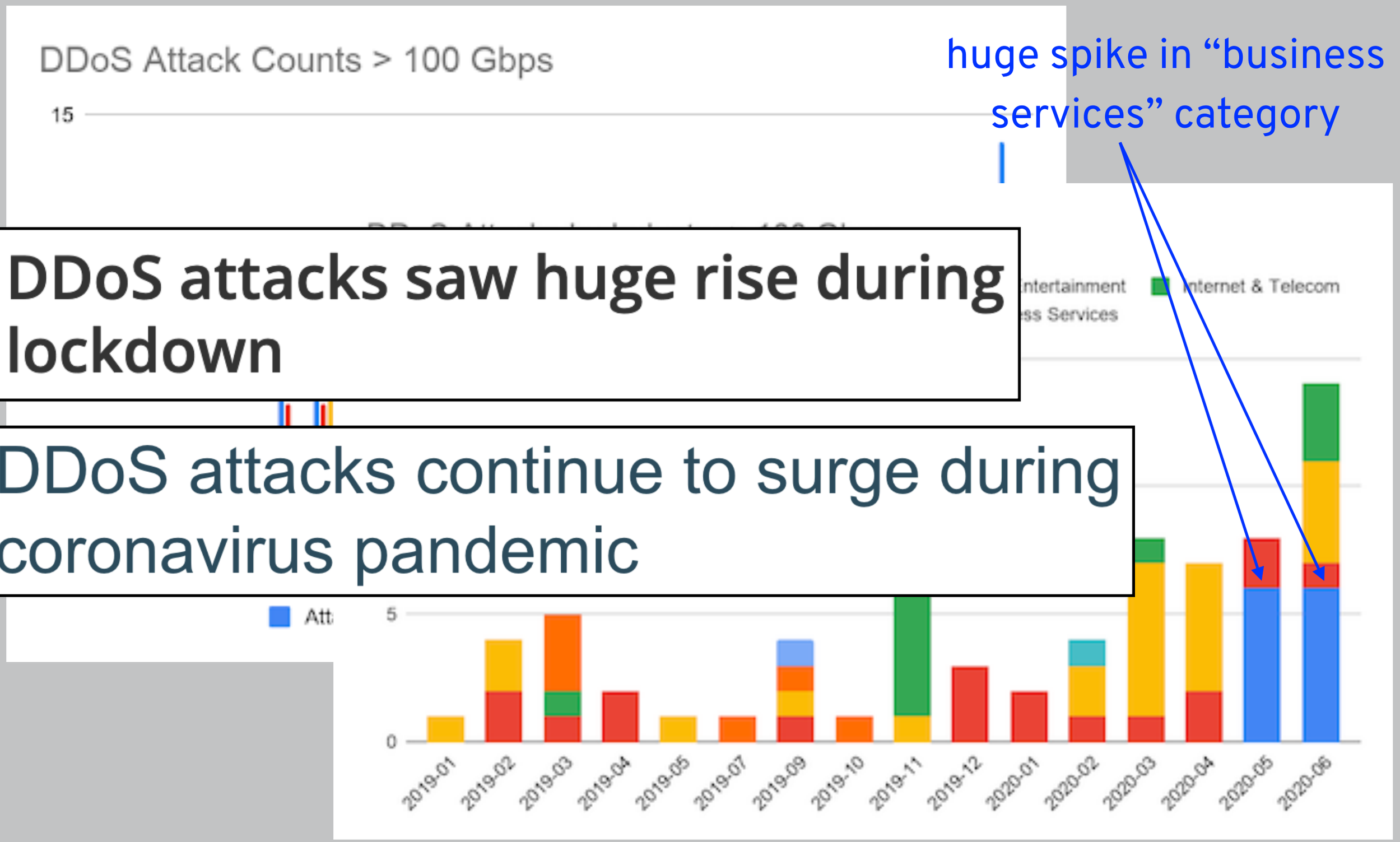
CLOUDFLARE®

Akamai

DDOS IS INCREASINGLY POPULAR



DDOS IS INCREASINGLY POPULAR



huge spike in “business services” category

DDoS attacks saw huge rise during lockdown

DDoS attacks continue to surge during coronavirus pandemic

DDOS AS A SERVICE

threat?

distributed: have many machines

$$$: large amount of ~~computational power~~ money

savvy: strong technical ability

booter (**stresser**) service will do attack for you, hosted with **bulletproof** providers who don't care about content and don't comply with law enforcement

DDOS *NOT* AS A SERVICE

q: but how do booter services work? how to do it myself?

a: use a **botnet**.