UNIVERSITY
OF TWENTE.

15/05/2015

# The DDoS as a Service Phenomenon.

Everyone can attack you at the press of a button!

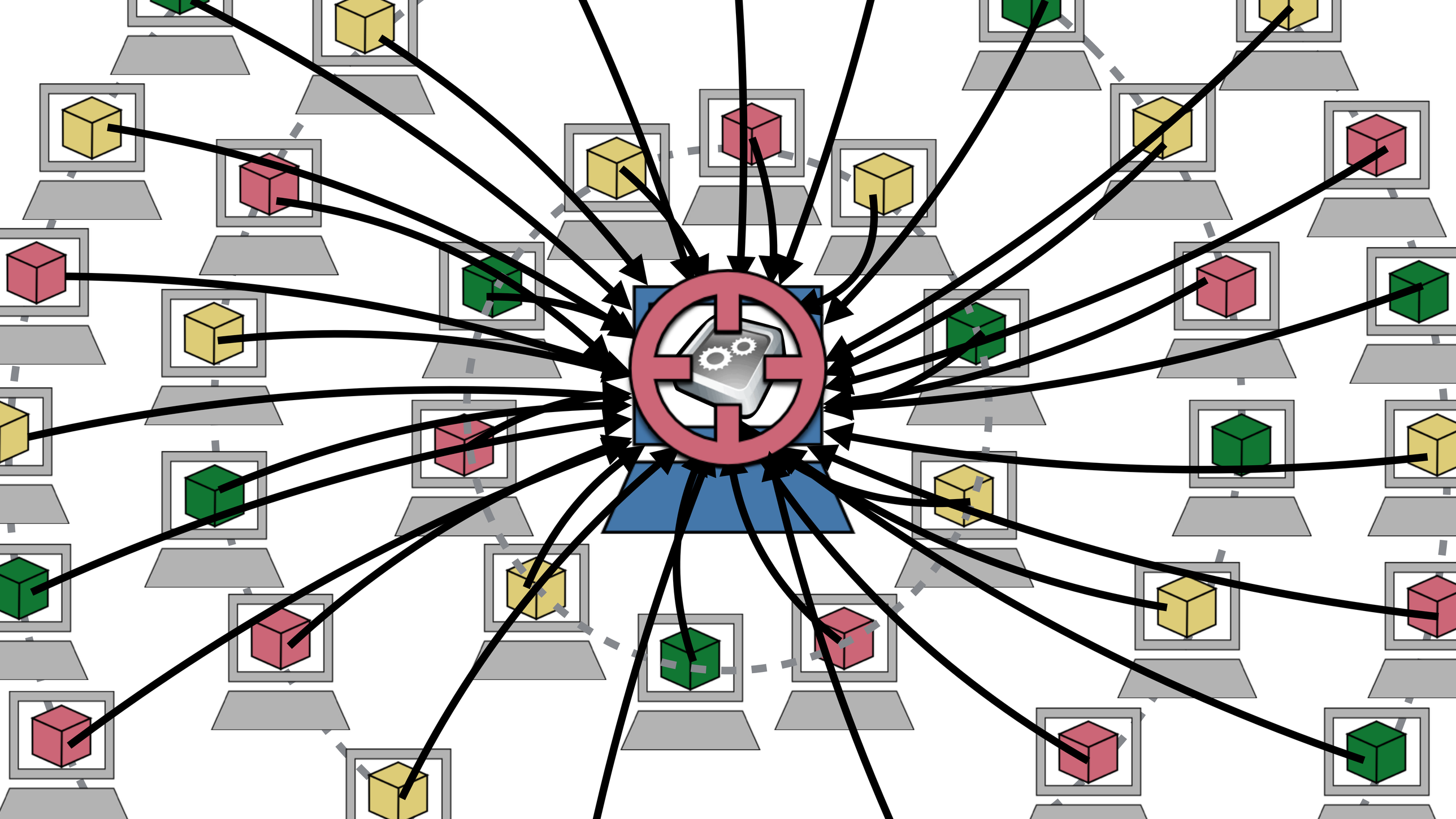
**Jair Santanna**
j.j.santanna@utwente.nl

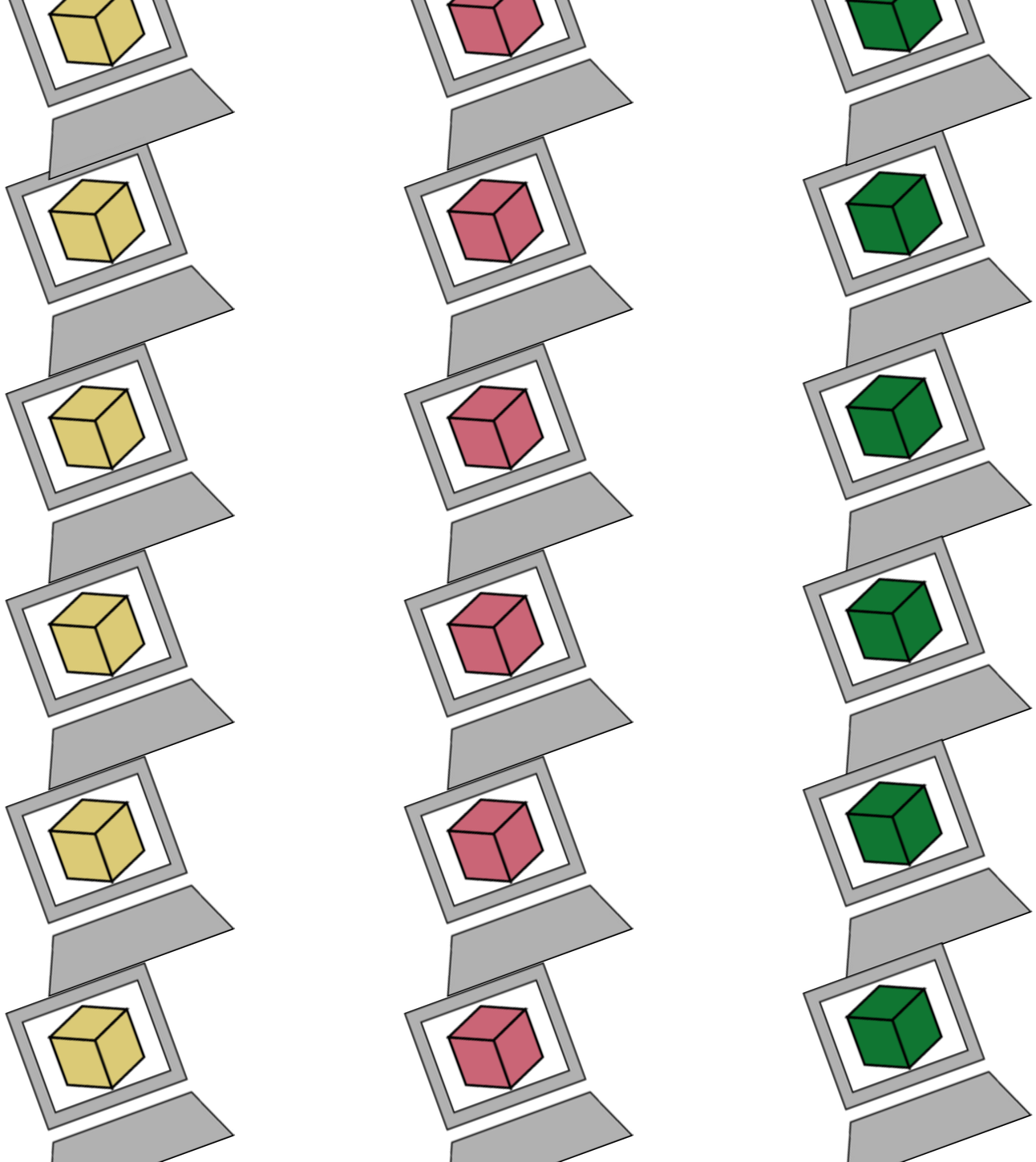


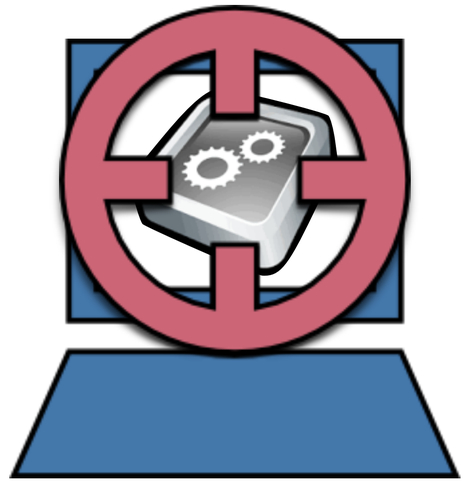
FLAMINGO

# DDoS

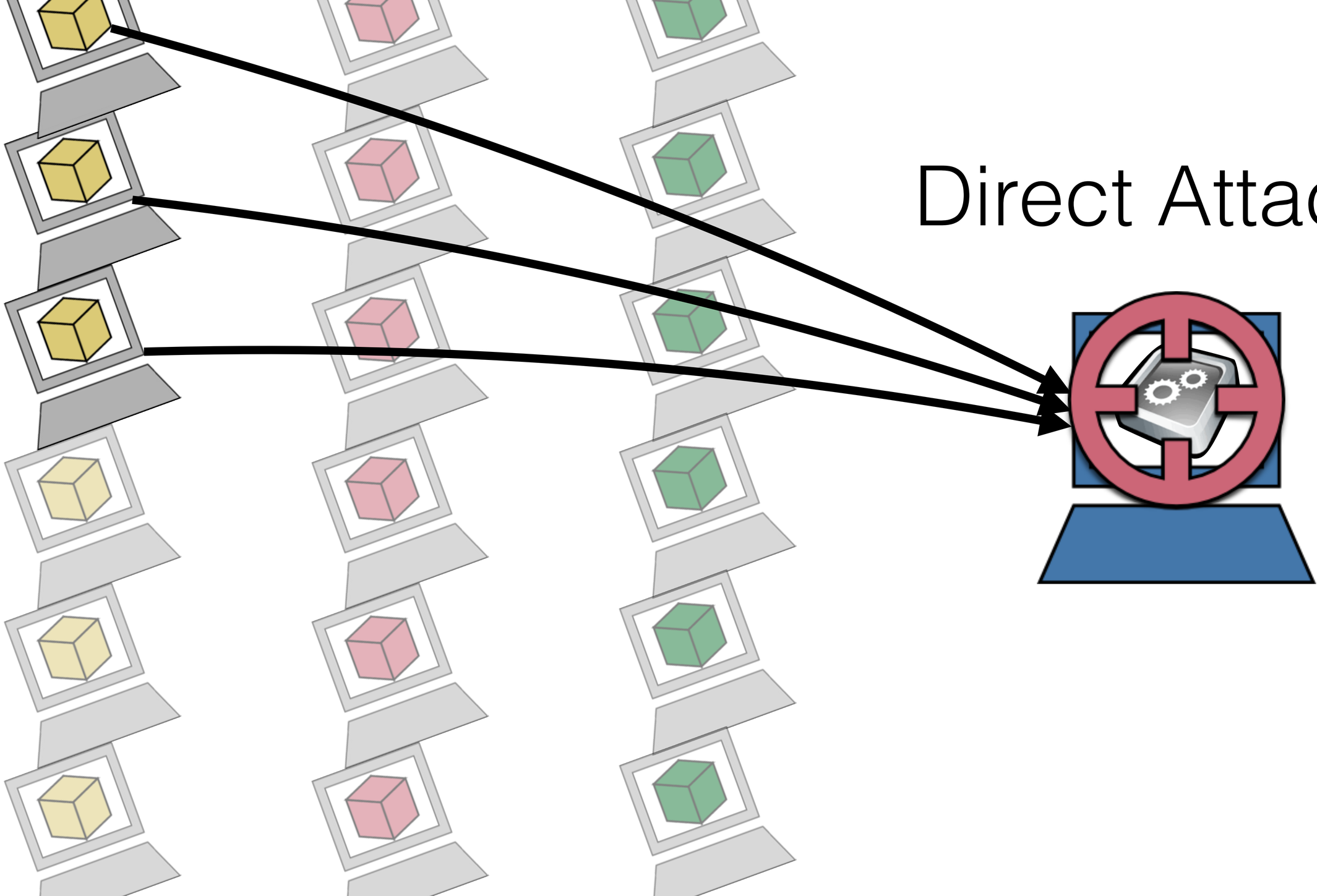
## Distributed Denial of Service



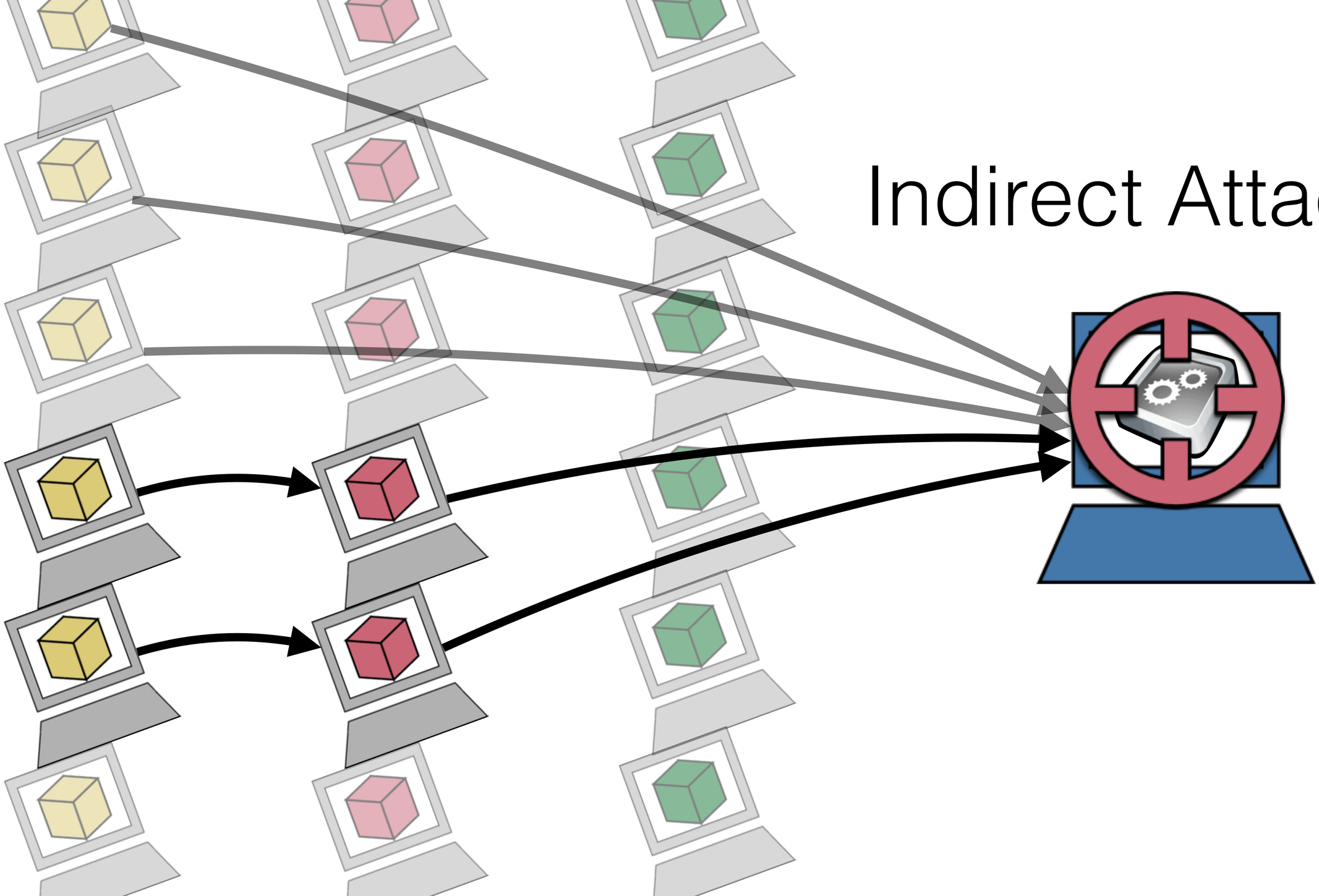




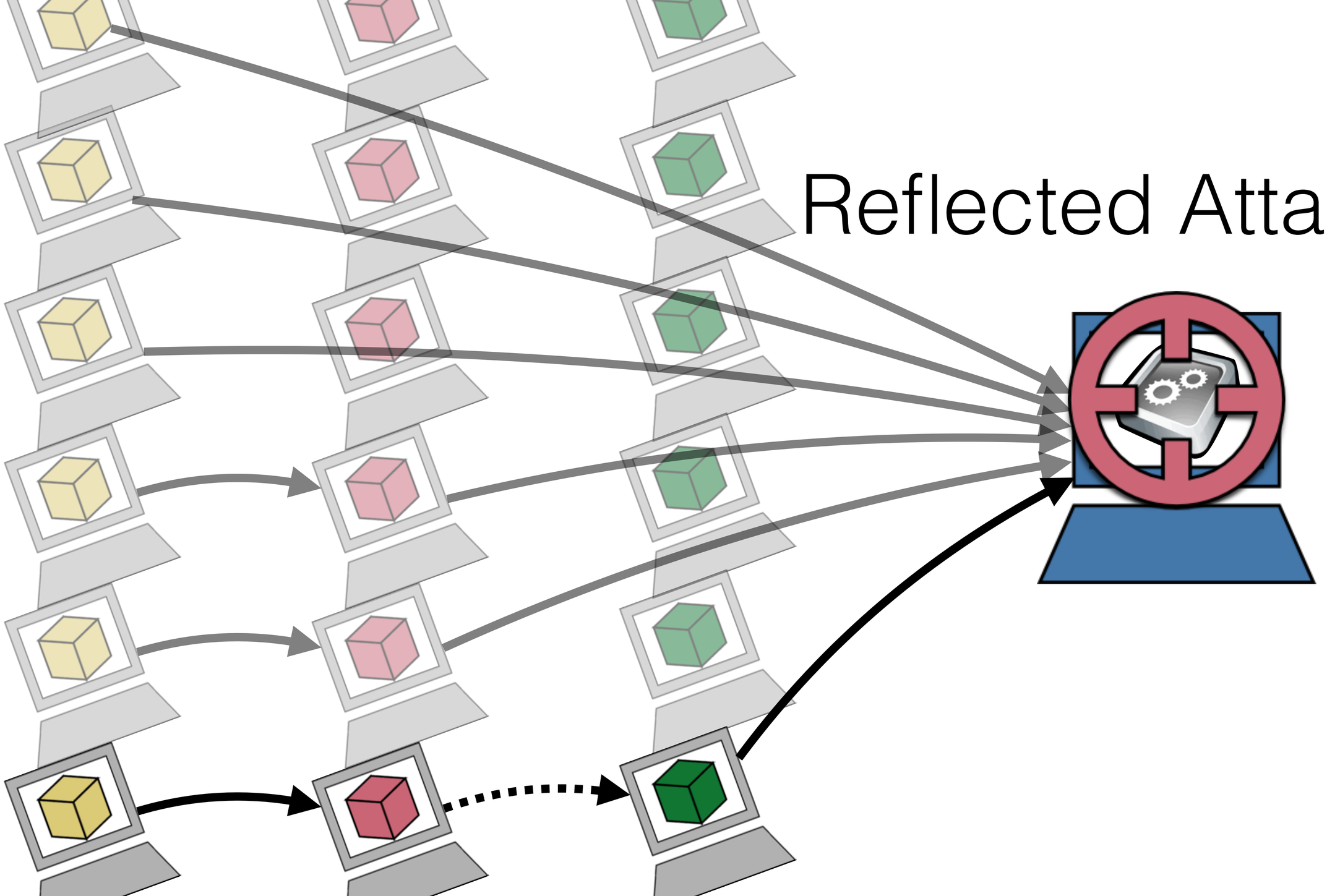
# Direct Attacks



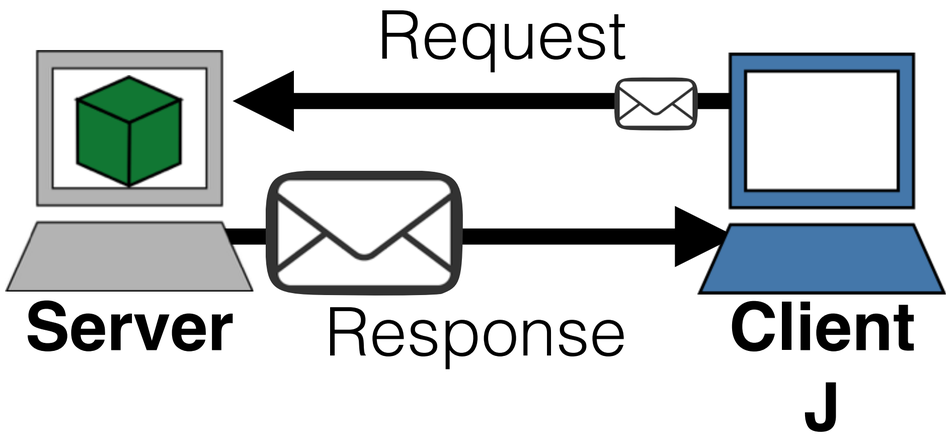
# Indirect Attacks

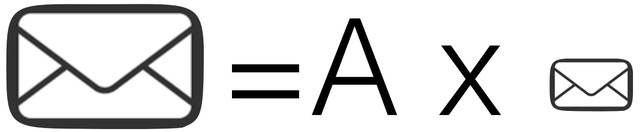


# Reflected Attacks



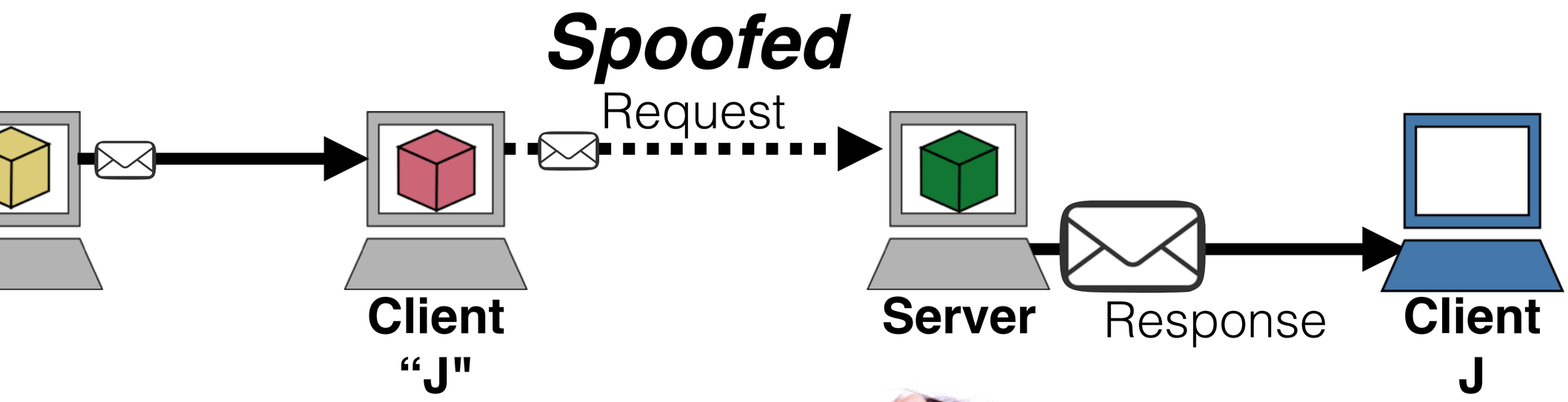
# Client-Server




# Amplification

# Reflection and Amplification



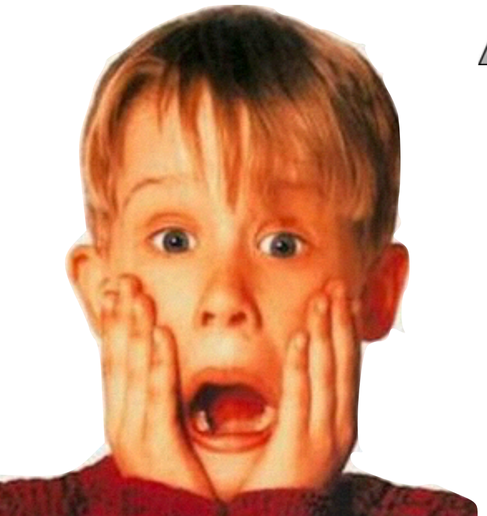



2013: 300Gbps (DNS)

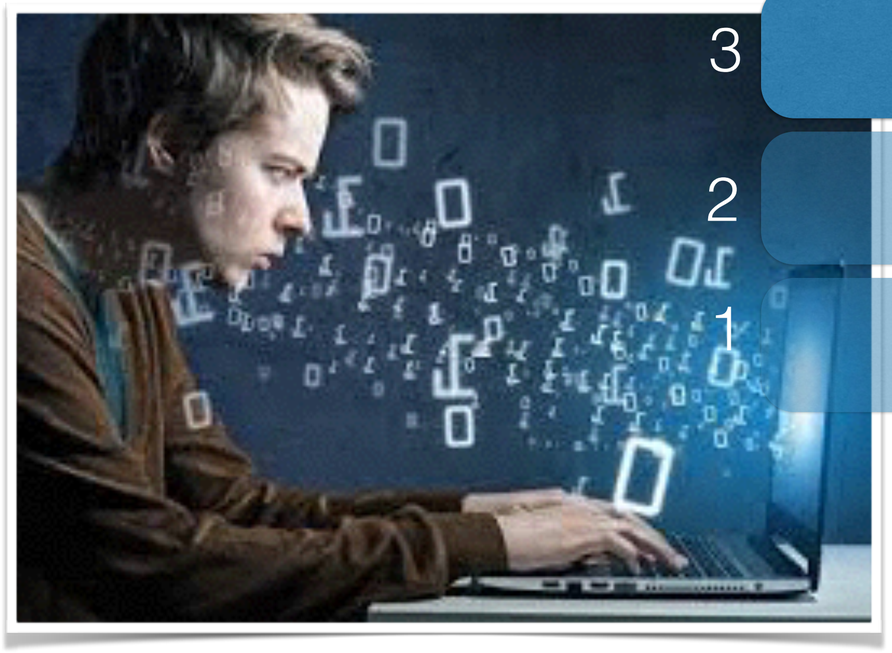
2014: 400Gbps (NTP)

⋮

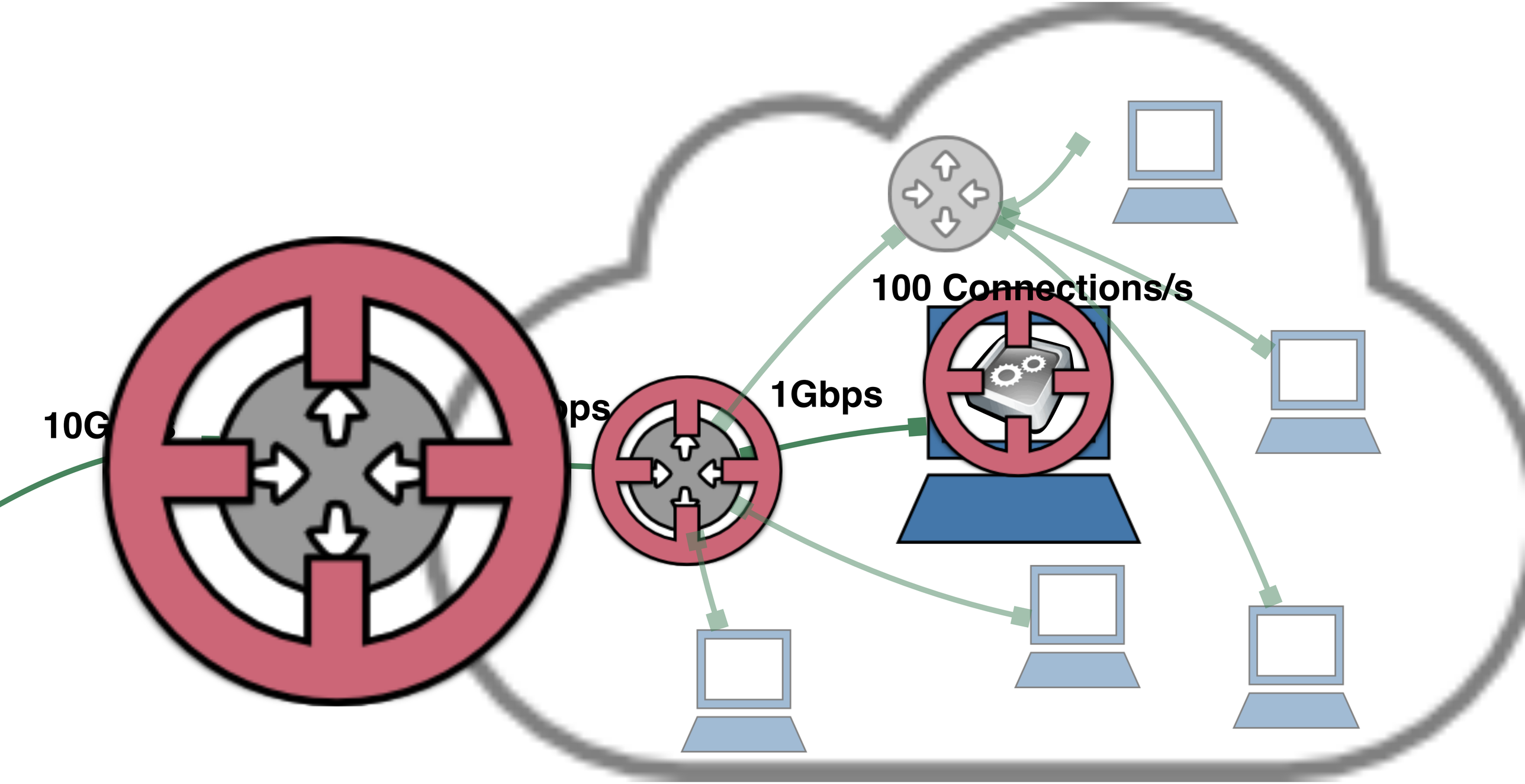
2020:1Tbps!?



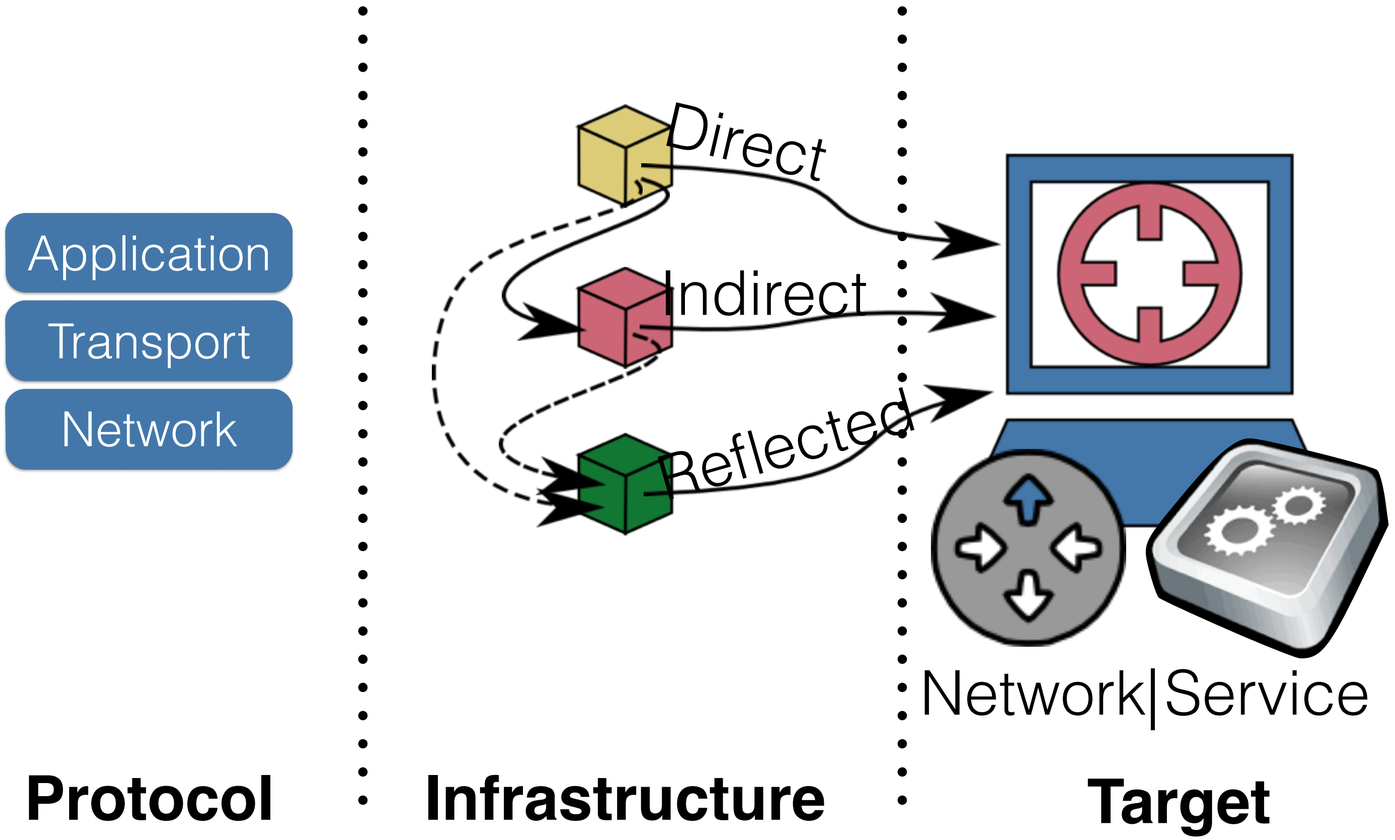




| | | **Protocols:** |
|---|---|---|
| 5 | Application | HTTP, HTTPS |
| 4 | Transport | TCP, UDP |
| 3 | Network | IP, ICMP |
| 2 | | |
| 1 | | |


100 Connections/s
1Gbps

# Summary:


Application
Transport
Network
Direct
Indirect
Reflected
Network|Service
Protocol
Infrastructure
Target







# Who?



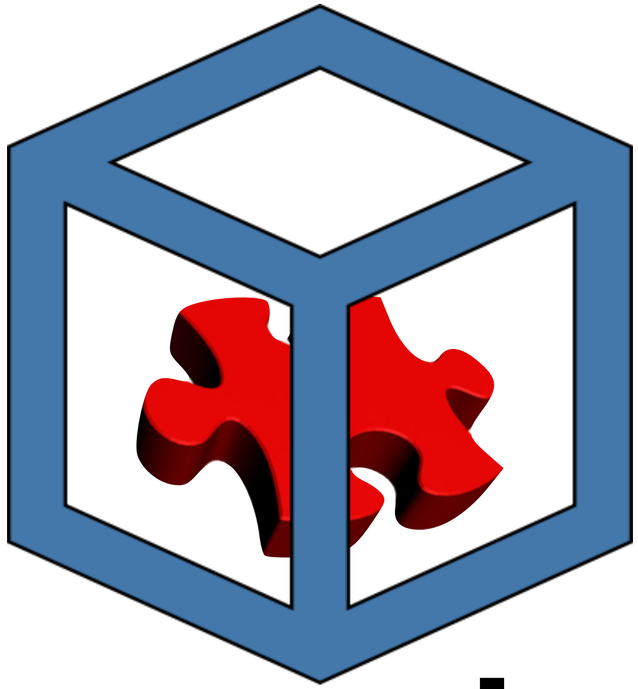





You know nothing, Jon Snow.

# Anyone!





# Booter

DDoS as a $ervice Phenomenon.

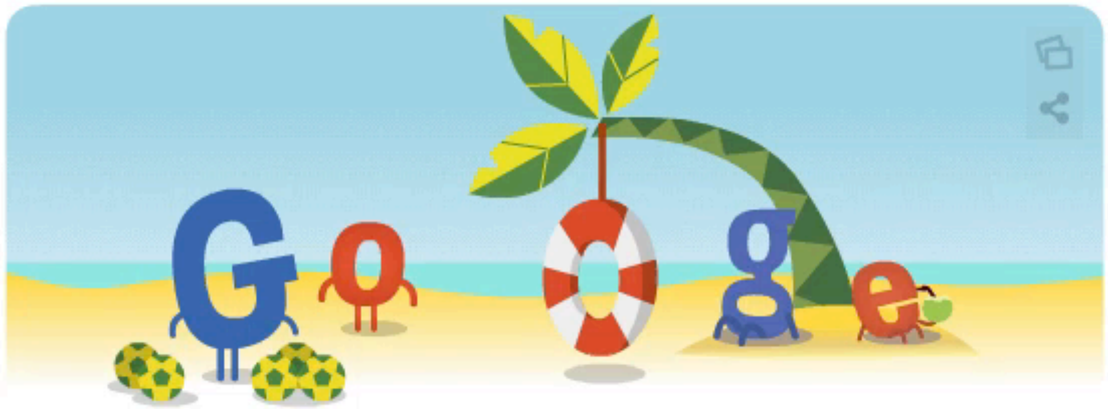
Google

https www.google.nl/webhp?tab=ww&ei=Bw6xU9zaEbSZyQPjpoGIDQ&ved=0CBYQ1S4

Reader

http://cmon...la/tma2014 Research UTwente Nova pasta Personal UFRGS Mirador JavaScript Blog The Interne...opology Zoo WhatisCIF – ...ect Hosting

+Jair Gmail Images 3 Share



A faster way to browse the web

Install Google Chrome

Google Search I'm Feeling Lucky

Google.nl offered in: Nederlands

Advertising Business About Privacy & Terms Settings Use Google.com

Safari

Search Google or enter an address

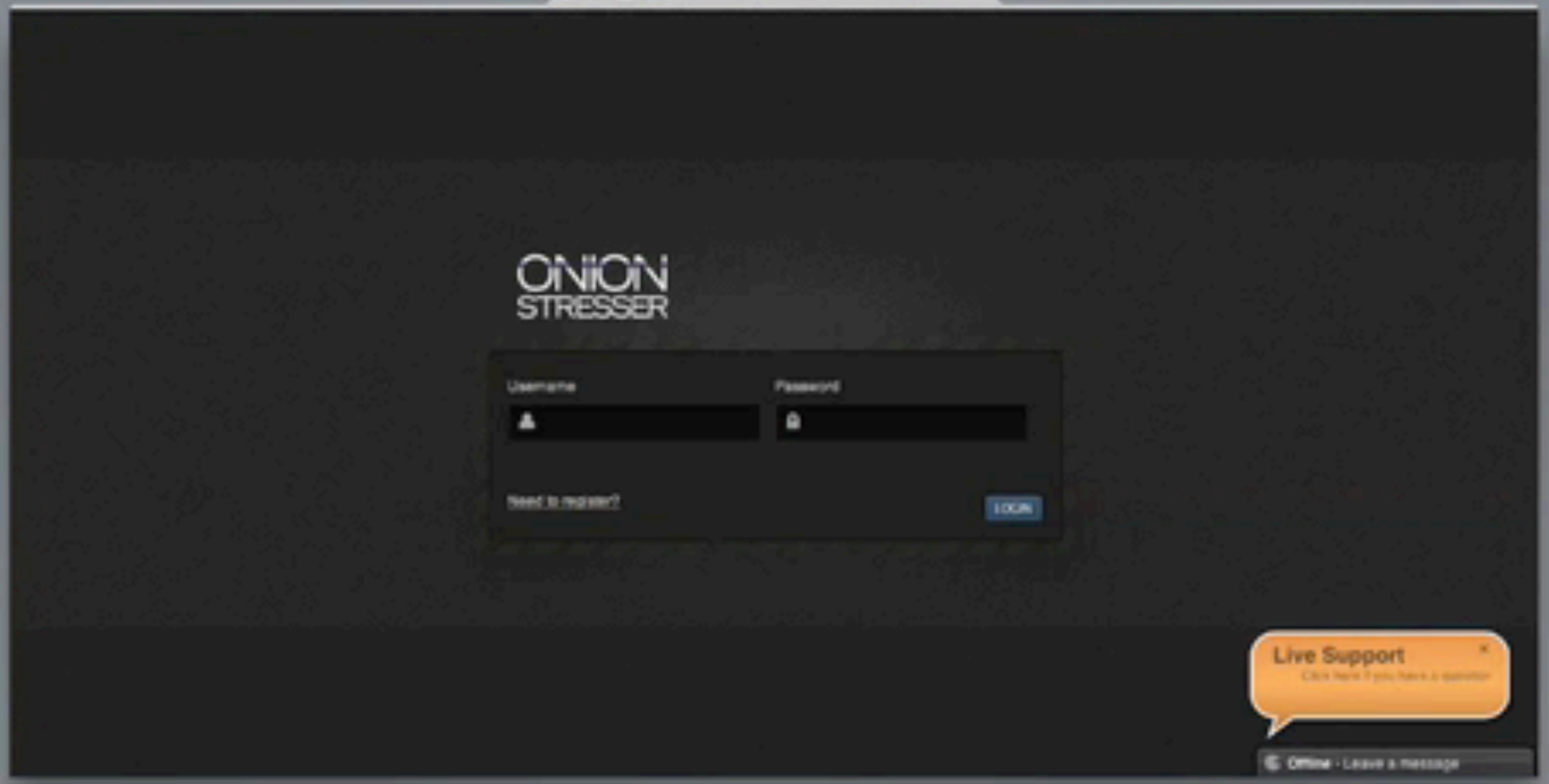
Reader

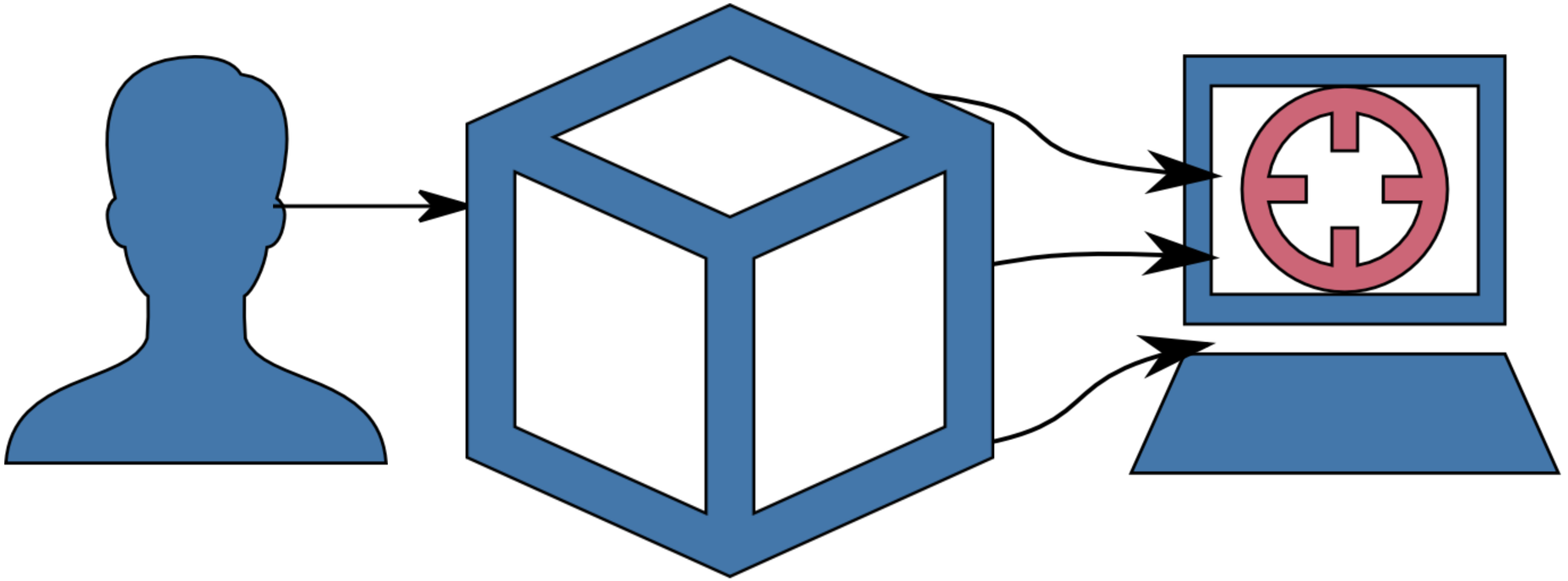
Nova pasta | Personal | UTwente | UFRGS | UNISC | Mirador | JavaScript | Blog | The Interne...opology Zoo | WhatisCIF - ...ject Hosting | Escher in h...useum shop | BlackHat

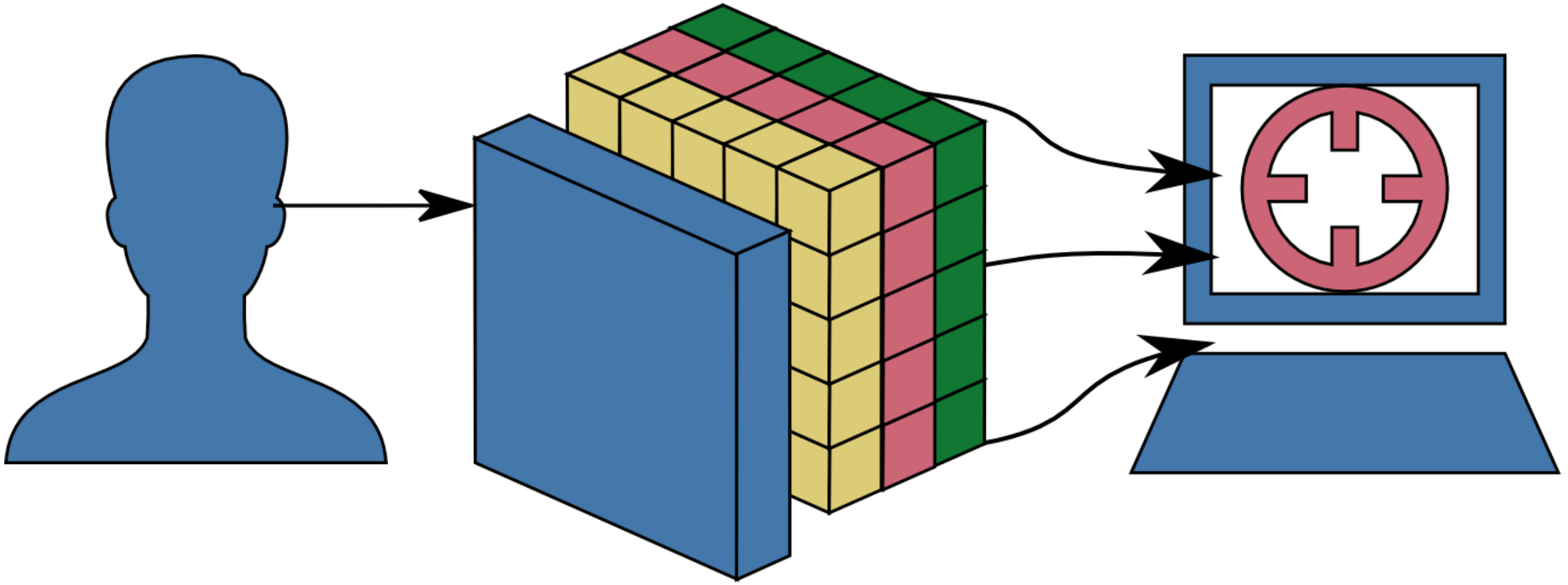
Login :: Onion Stresser - A Powerful Network Stress Testing Tool

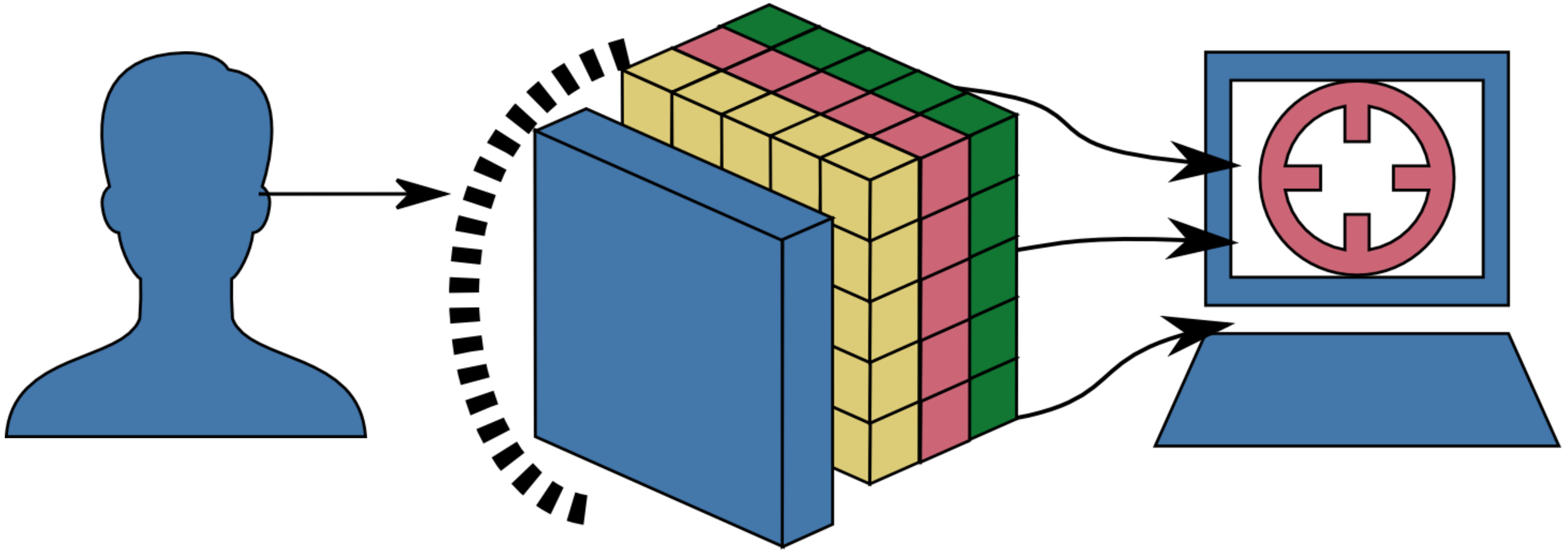
onionstresser.com/login.php

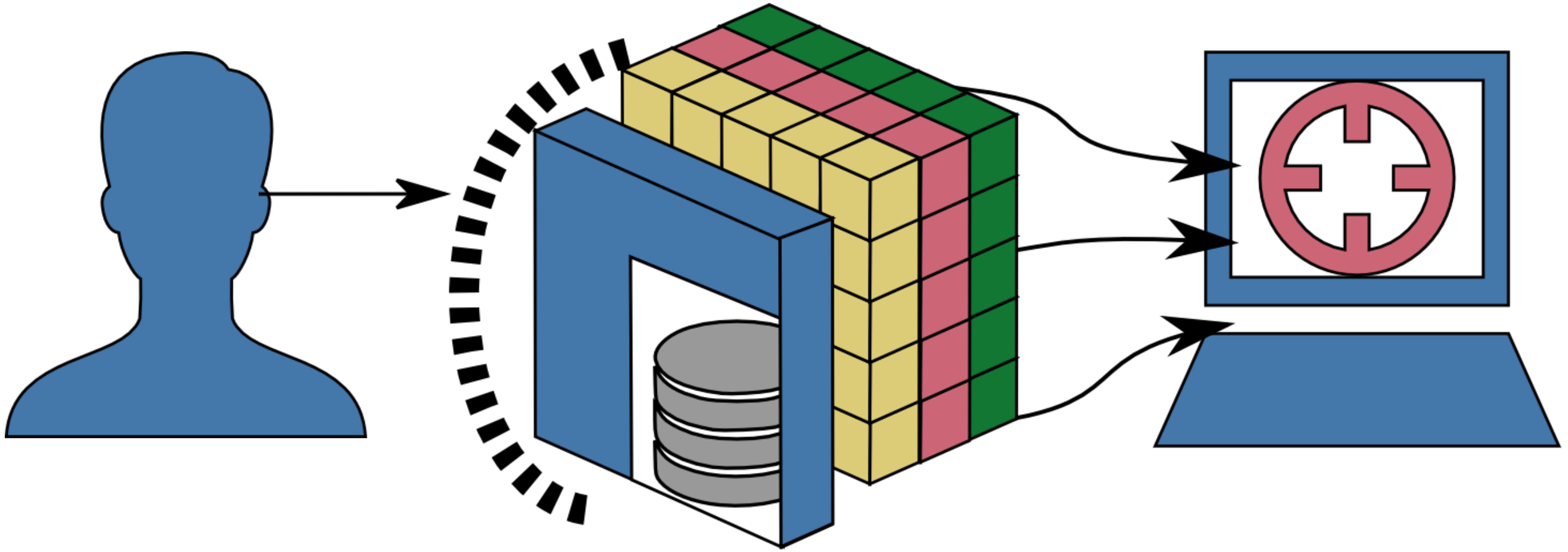
Login :: Onion Stresser - A Powerf...

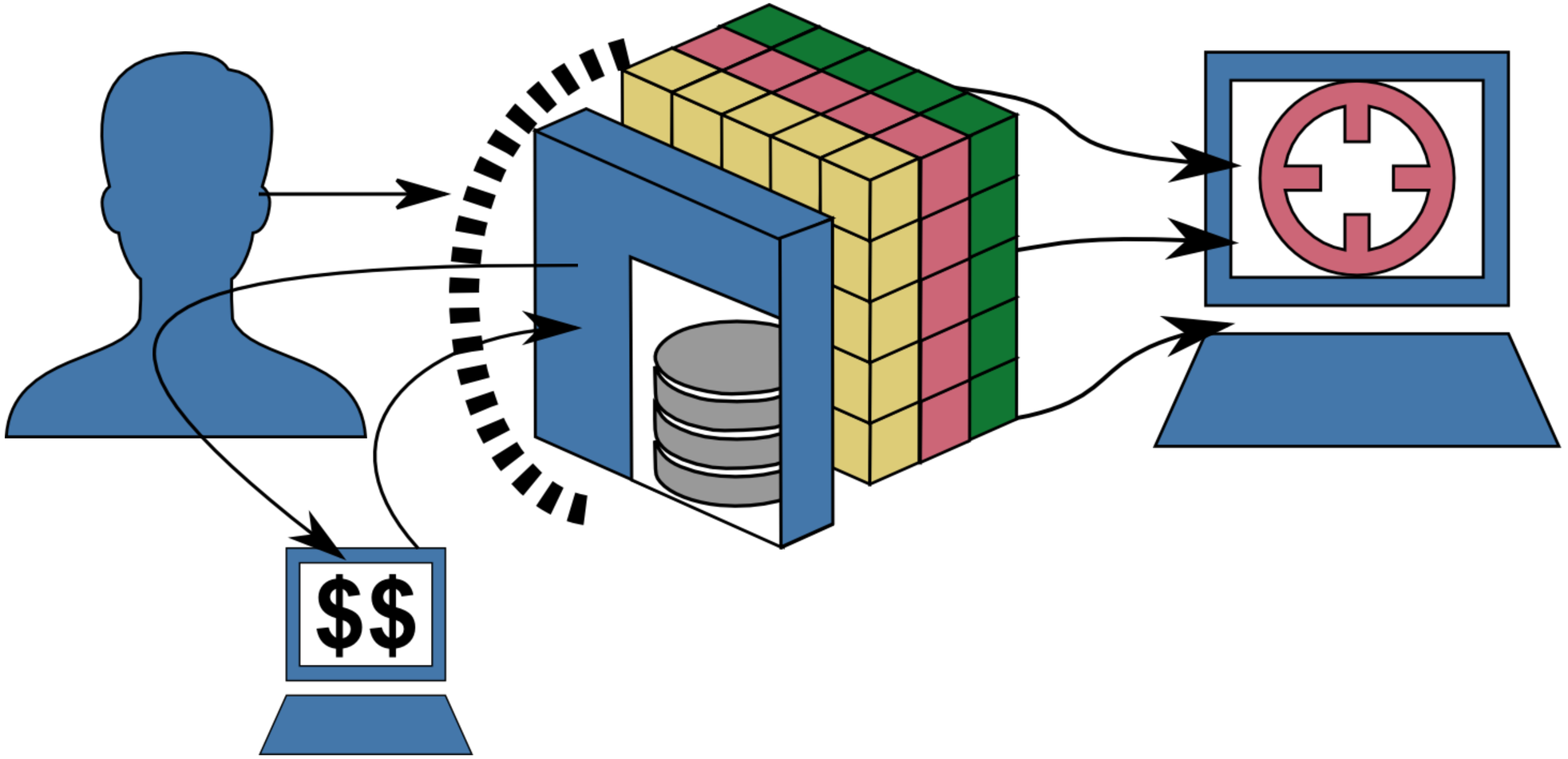


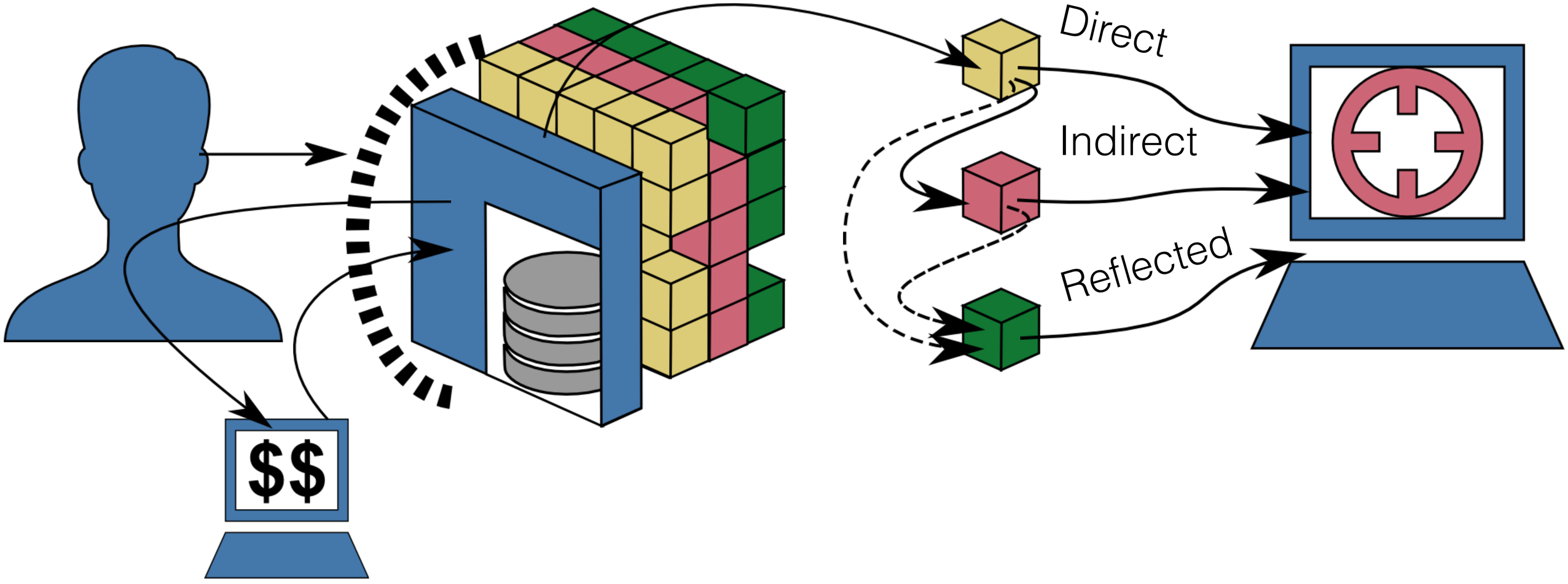


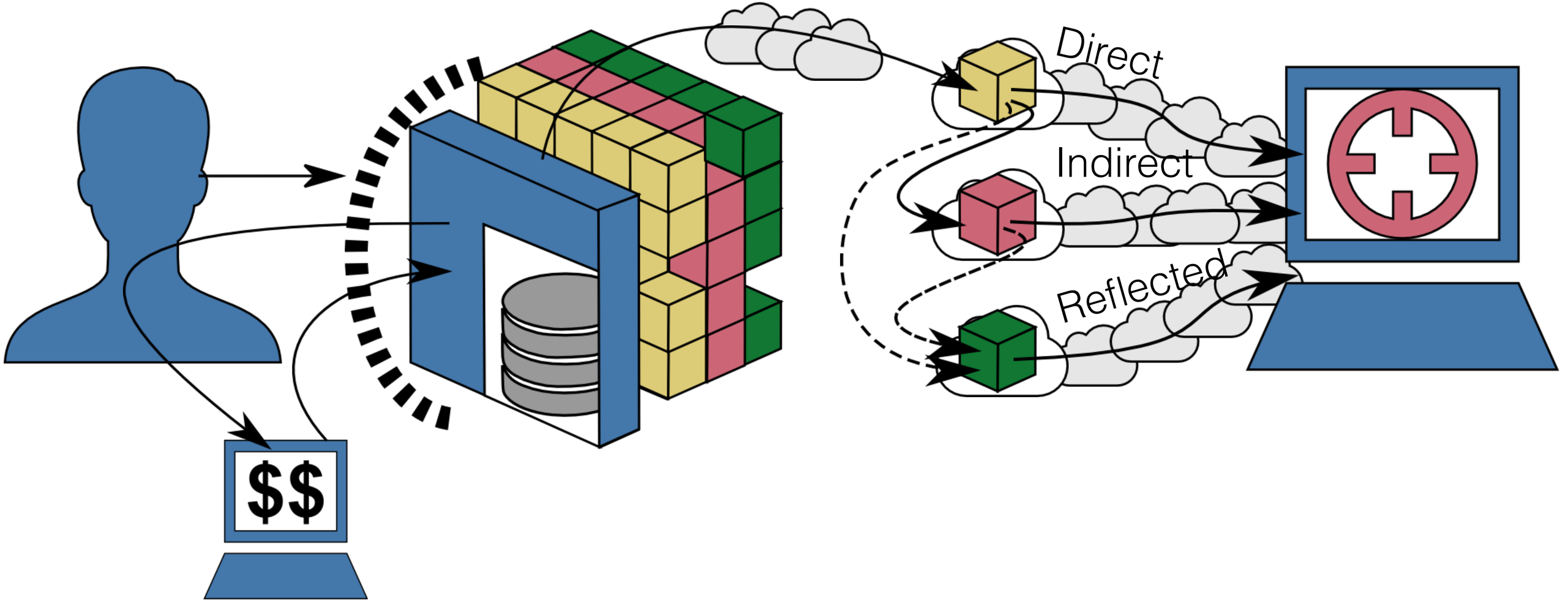









Direct
Indirect
Reflected
$$


Direct
Indirect
Reflected
$$




# 14 Booters

## Hired, Collected, and Analysed

*UDP-based*

| # | Booter URL | Offer [Gbps] | Price [€] |
|---|---|---|---|
| 1 | B1 | ? | 10,90 |
| 2 | B2 | 5 | 1,95 |
| 3 | B3 | 5 | 3,12 |
| 4 | B4 | 25 | 3,89 |
| 5 | B5 | ? | 3,89 |
| 6 | B6 | 10 | 3,89 |
| 7 | B7 | Up to 3 | 3,00 |
| 8 | B8 | 6 | 3,90 |
| 9 | B9 | 1,5 | 8,00 |
| 10 | B10 | Up to 3 | 4,90 |
| 11 | B11 | ? | free |
| 12 | B12 | ? | 3,11 |
| 13 | B13 | 8 | 3,90 |
| 14 | B14 | ? | 3,90 |
| | | | **€58,35** |





| # | Booter URL | Offer [Gbps] | Price [€] | Protocol | Request |
|---|---|---|---|---|---|
| 1 | B1 | ? | 10,90 | *DNS | ddostheinter.net |
| 2 | B2 | 5 | 1,95 | *DNS | anonsc.com |
| 3 | B3 | 5 | 3,12 | *DNS | anonsc.com |
| 4 | B4 | 25 | 3,89 | *DNS | root-server.net |
| 5 | B5 | ? | 3,89 | *Chargen | - |
| 6 | B6 | 10 | 3,89 | *DNS | packetdevil.com |
| 7 | B7 | Up to 3 | 3,00 | *Chargen | - |
| 8 | B8 | 6 | 3,90 | *DNS | root-server.net |
| 9 | B9 | 1,5 | 8,00 | *DNS | root-server.net |
| [redacted] | | | | | |
| [redacted] | | | | | |
| [redacted] | | | | | |
| [redacted] | | | | | |
| [redacted] | | | | | |

# DNS-based attacks

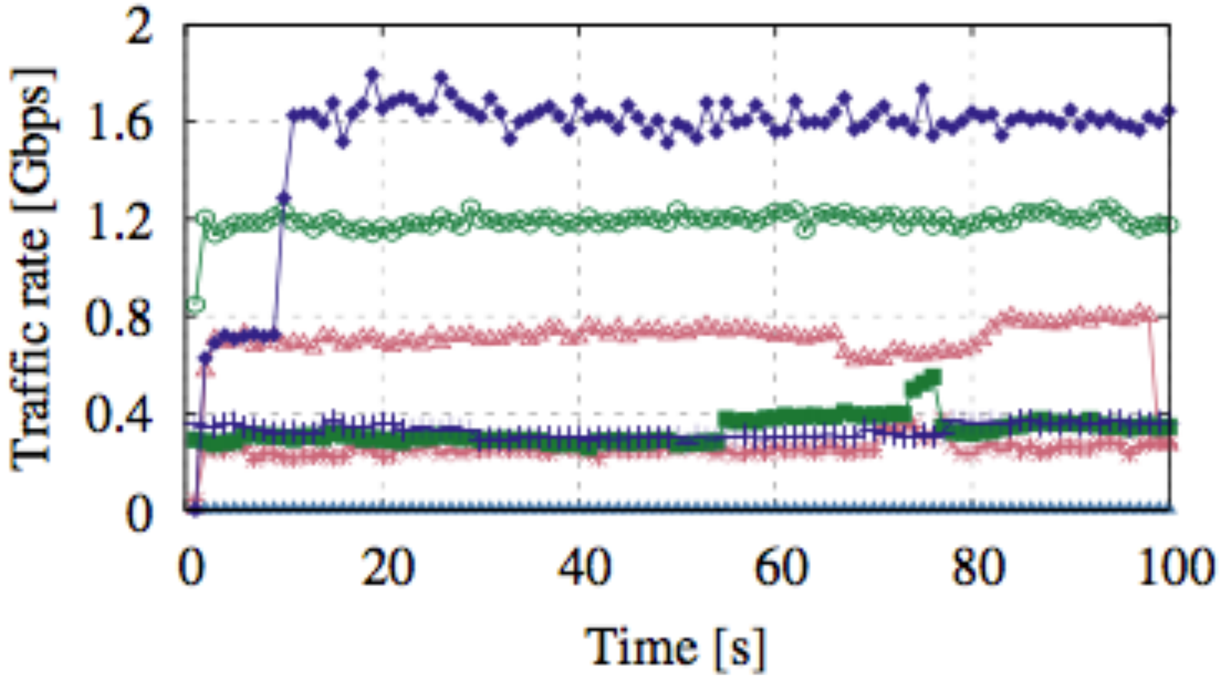



Fig. 2: Traffic rate of DNS-based attacks.

ddostheinter.net

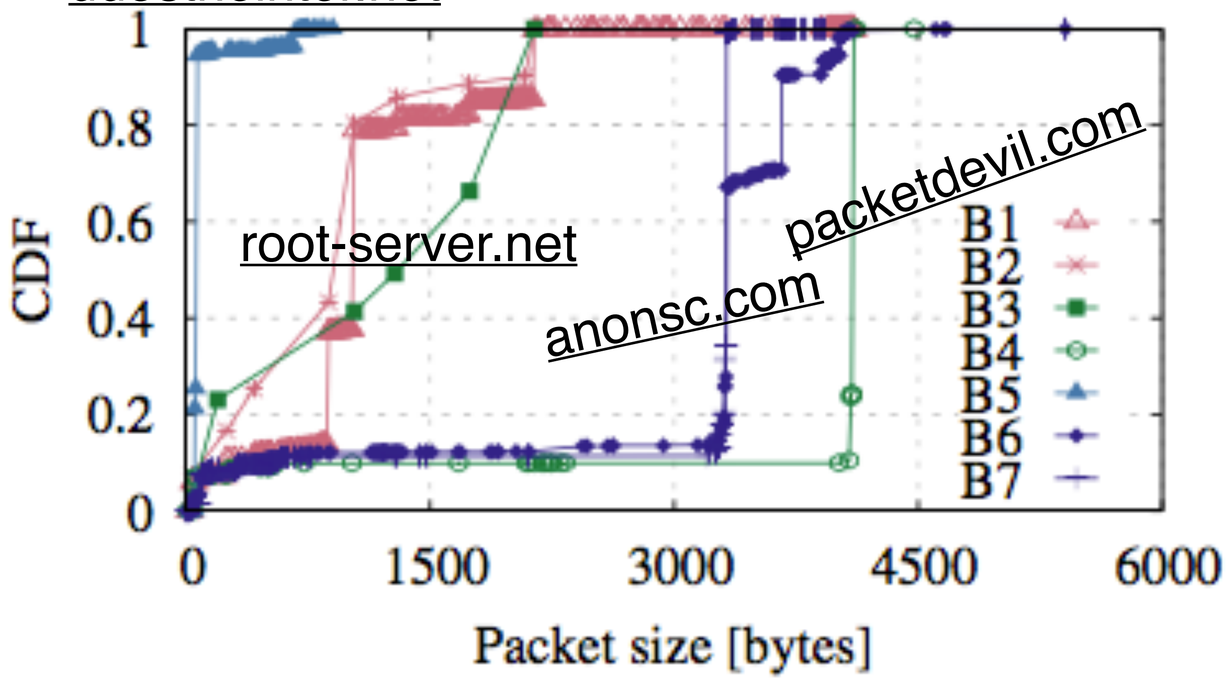



Fig. 3: Packet size distribution (DNS).

# CharGen-based attacks

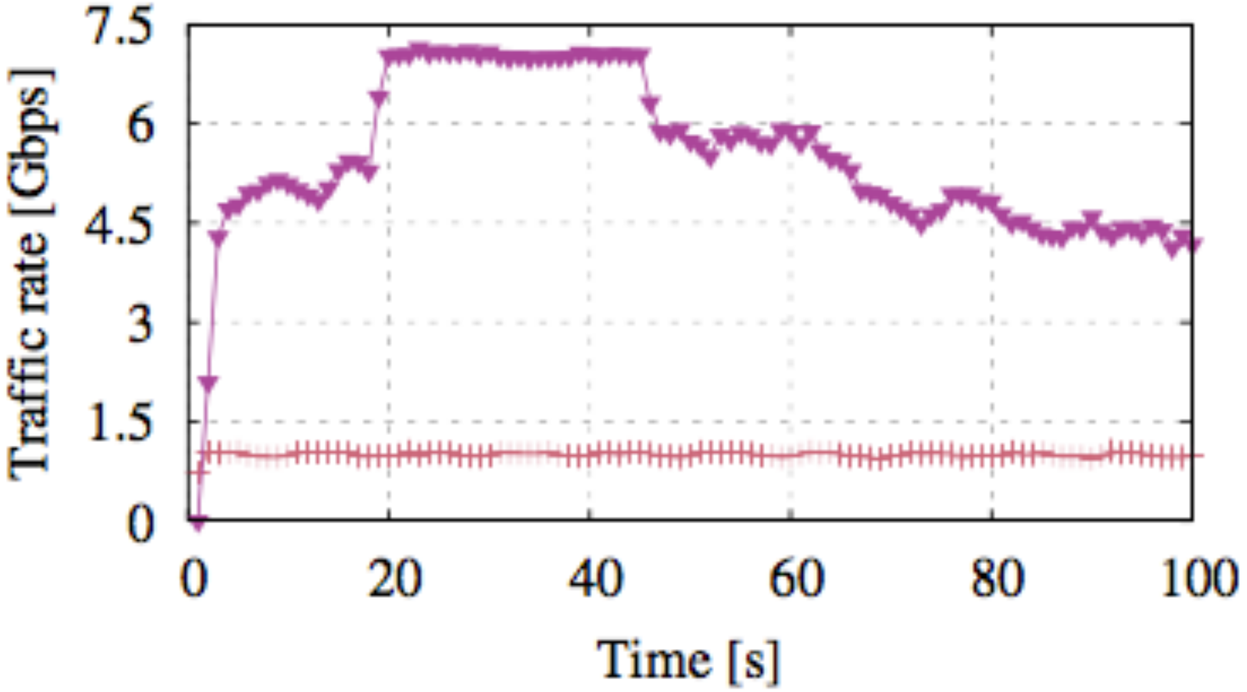



Fig. 4: Traffic rate of CharGen-based attacks.

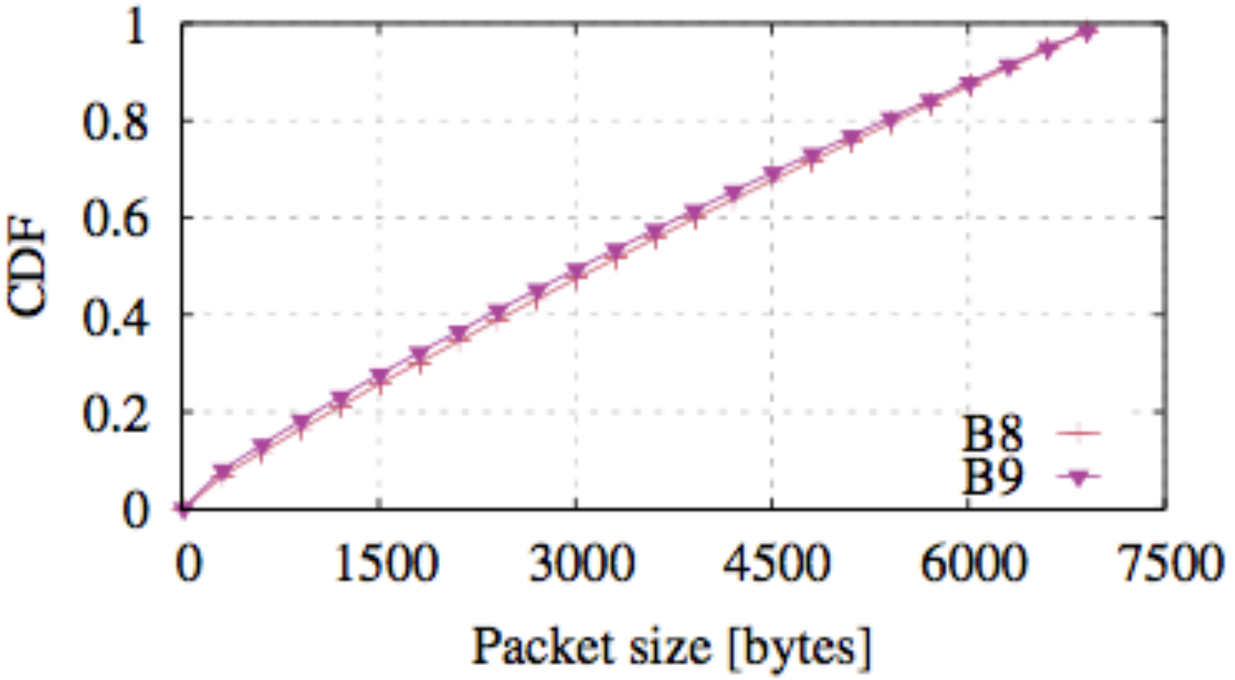
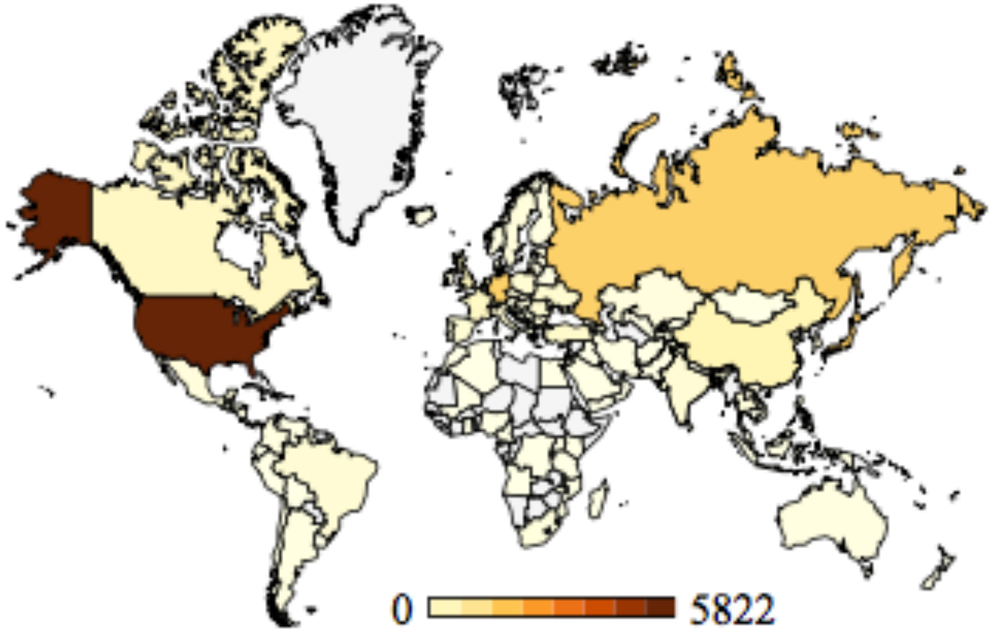



Fig. 5: Packet size distribution (CharGen).



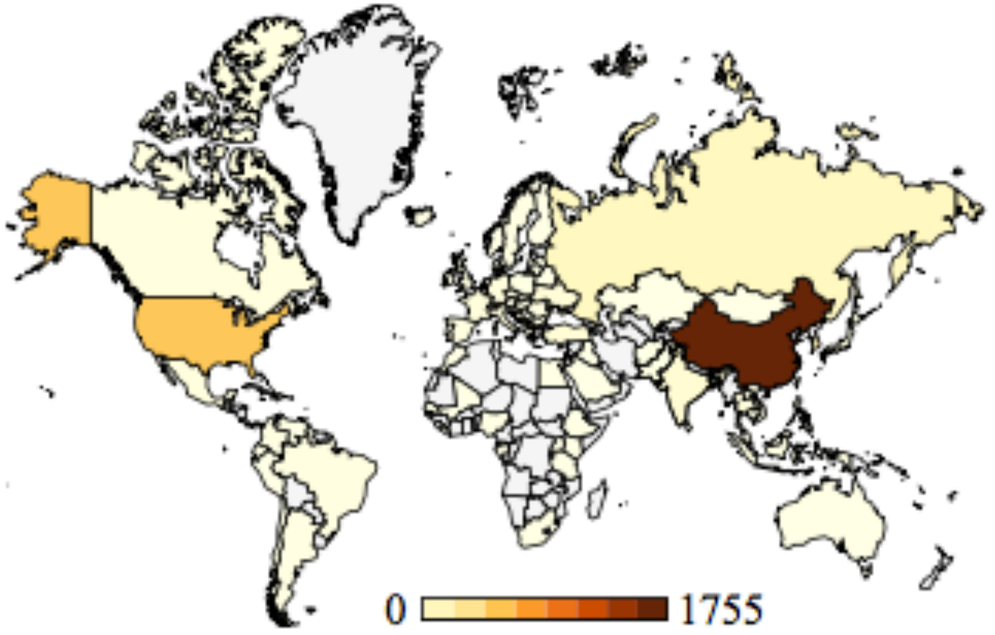
| # | Booter URL | Offer [Gbps] | Price [€] | Protocol | Unique IPs |
|---|---|---|---|---|---|
| 1 | B1 | ? | 10,90 | *DNS | 8281 |
| 2 | B2 | 5 | 1,95 | *DNS | 7369 |
| 3 | B3 | 5 | 3,12 | *DNS | 6075 |
| 4 | B4 | 25 | 3,89 | *DNS | 4486 |
| 5 | B5 | ? | 3,89 | *Chargen | 3779 |
| 6 | B6 | 10 | 3,89 | *DNS | 2970 |
| 7 | B7 | Up to 3 | 3,00 | *Chargen | 281 |
| 8 | B8 | 6 | 3,90 | *DNS | 78 |
| 9 | B9 | 1,5 | 8,00 | *DNS | 54 |
| [redacted] | [redacted] | [redacted] | [redacted] | | |
| [redacted] | [redacted] | [redacted] | free | | |
| [redacted] | [redacted] | [redacted] | 3,11 | | |
| [redacted] | [redacted] | [redacted] | [redacted] | | |
| [redacted] | [redacted] | [redacted] | 3,90 | | |

**€58,35**




| Top 10 | |
|---|---|
| US | 5822 |
| JP | 1986 |
| DE | 1909 |
| RU | 1871 |
| CN | 825 |
| NL | 731 |
| GB | 716 |
| CA | 603 |
| FR | 561 |
| TW | 459 |

(a) DNS per country.




| Top 10 | |
|---|---|
| CN | 1755 |
| US | 630 |
| KR | 275 |
| RU | 192 |
| IN | 105 |
| TR | 81 |
| UA | 76 |
| FR | 56 |
| TH | 55 |
| DE | 53 |

(b) CharGen per country.

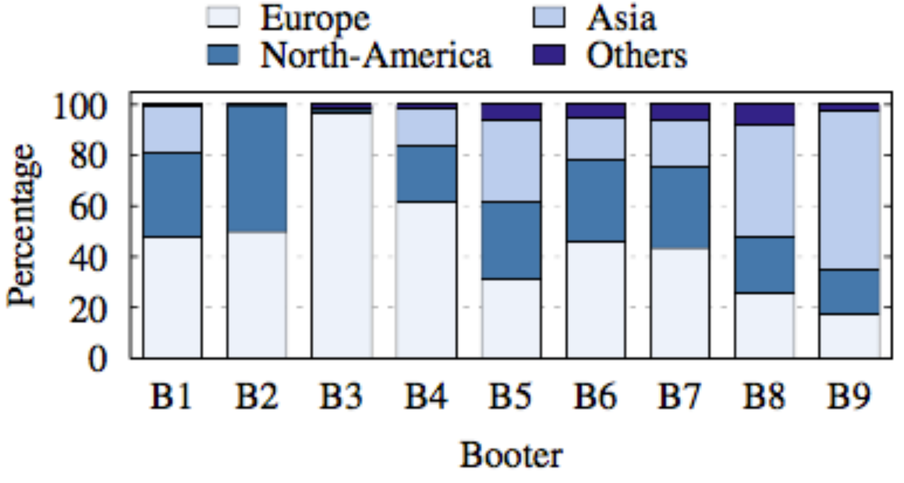



Fig. 7: Continent breakdown per Booter.

| ∩ | B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|---|---|---|---|---|---|---|---|
| B1 | – | 0.20 | 0.20 | 3.88 | 0.02 | 1.07 | 0.73 |
| B2 | 11.54 | – | 0 | 0 | 0 | 0 | 0 |
| B3 | 16.67 | 0 | – | 0 | 0 | 1.85 | 1.85 |
| B4 | 5.86 | 0 | 0 | – | 0 | 1.85 | 1.04 |
| B5 | 0.01 | 0 | 0 | 0 | – | 4.11 | 7.99 |
| B6 | 0.65 | 0 | 0 | 0 | 0.20 | – | 8.38 |
| B7 | 0.54 | 0 | 0 | 0.02 | 0.51 | 10.90 | 98.65 |

98%









## Infrastructure layer attacks

Prolexic data shows the majority of DDoS attacks are directed against the infrastructure layer, accounting for 76.76 percent of attacks in Q4 2013. The UDP protocol was most commonly used with a combined 30.27 percent total in comparison with other protocols. SYN floods placed second as the preferred DDoS infrastructure attack vector with a total of 14.94 percent.

In third place was the ICMP protocol with 9.71 percent followed by DNS with 9.58 percent. PLXsert has previously noted the increase in the use of DNS reflection as an attack vector and this is likely to remain so with new tools being released and adapted by DDoS-for-hire-vendors. In the fifth place, the old but revived CHARGEN protocol continues its rise in popularity, [redacted] percent of the total infrastructure layer attacks this quarter. PLXsert has identified over 110,000 CHARGEN servers on the Internet, and to date most of these servers are still open and vuln[redacted]uting to a 92.31 percent increase of CHARGEN usage between Q3 2013 and Q4 2013.

Following CHARGEN, lesser used attack vectors in DDoS attacks against infrastructure were ACK Floods (2.81 percent), FIN PUSH (1.28 percent), TCP RST (1.4 percent), SYN PUSH (0.38 percent), RIP (0.26 percent), and TCP Fragment (0.13 percent).

## Application attacks

Application layer attacks account for[redacted] launched against Prolexic's global client base. Application-base[redacted]nd sophistication in order to be successful. Recently, there has[redacted]ooter scripts by DDoS-for-hire vendors. This in turn makes[redacted]es without having to build technical resources and spend co[redacted]perform significant attacks.

At 19.91 percent, HTTP GET wa[redacted]tack vector in Q4 2013. This vector was followed by HT[redacted] (0.64 percent), NTP (0.26 percent) and SSL POST wi[redacted]

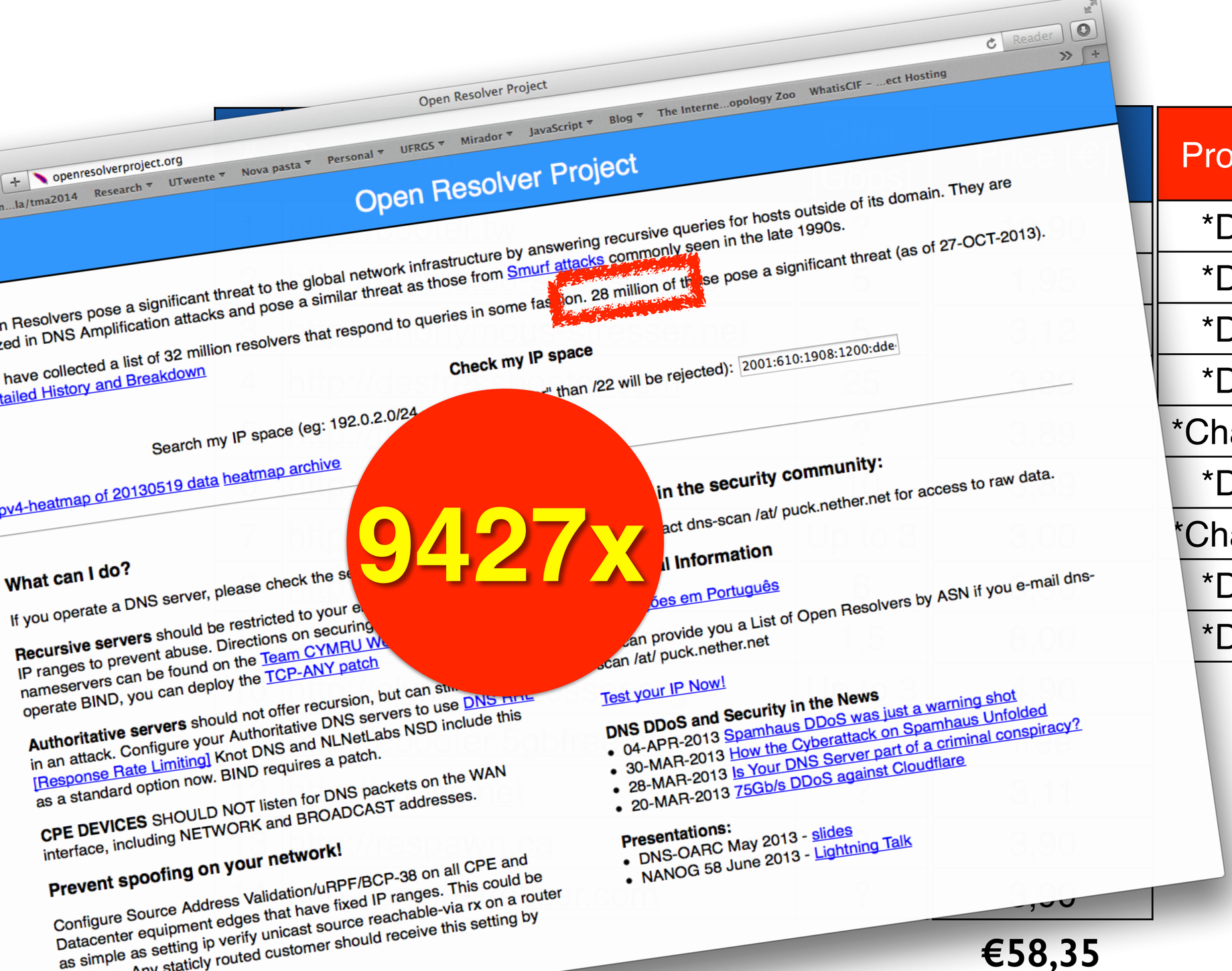
PLXsert has observed an increase [redacted]) as an attack vector. Defined in RFC 958, the NTP protoco[redacted]network clocks on the Internet using a set of distributed clients and se[redacted]gram Protocol (UDP), which provides connectionless transport of data. N[redacted]e Protocol and the ICMP Timestamp message; the NTP protocol acts as a suitable replacement for both.

The NTP protocol is implemented in all major operating systems, network infrastructure devices, and embedded devices. By using UDP, NTP is susceptible to spoofing. In addition, misconfiguration of network equipment can allow enterprise infrastructure to be used as unwilling participants in a DDoS attack. This can be achieved by responding to requests for NTP updates and directing the response to a victim host and overwhelming it with NTP traffic.

[redacted] protocols believed to be obsolete and decommissioned is usually driven by [redacted] tools. These tools eventually get leaked in crimeware [redacted], an increase of use in

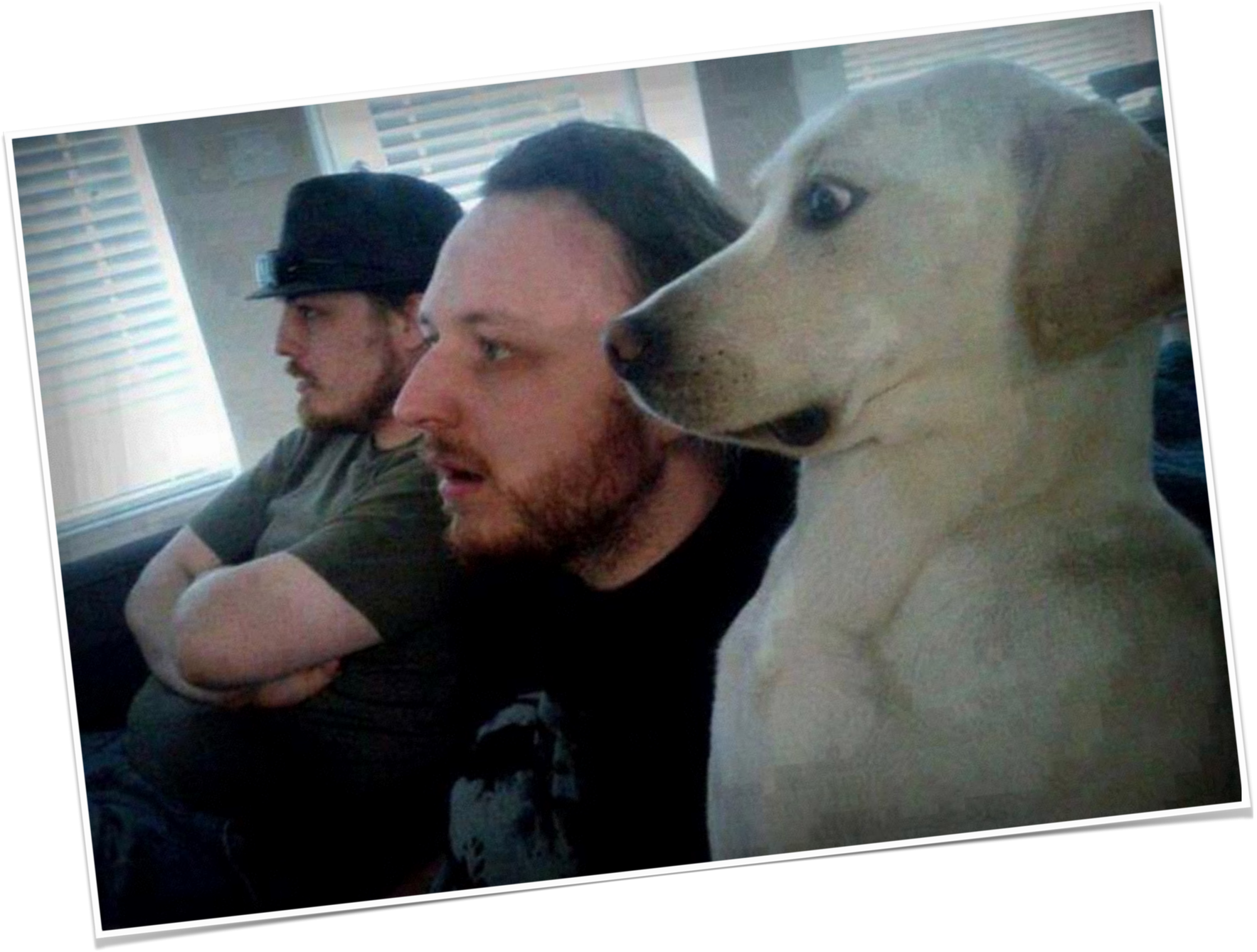
**29x**

| €] | Protocol | Unique IPs |
|---|---|---|
| | *DNS | 8281 |
| | *DNS | 7369 |
| | *DNS | 6075 |
| | *DNS | 4486 |
| | *Chargen | 3779 |
| | *DNS | 2970 |
| | *Chargen | 281 |
| | *DNS | 78 |
| | *DNS | 54 |




| Protocol | Unique IPs |
|---|---|
| *DNS | 8281 |
| *DNS | 7369 |
| *DNS | 6075 |
| *DNS | 4486 |
| *Chargen | 3779 |
| *DNS | 2970 |
| *Chargen | 281 |
| *DNS | 78 |
| *DNS | 54 |

€58,35



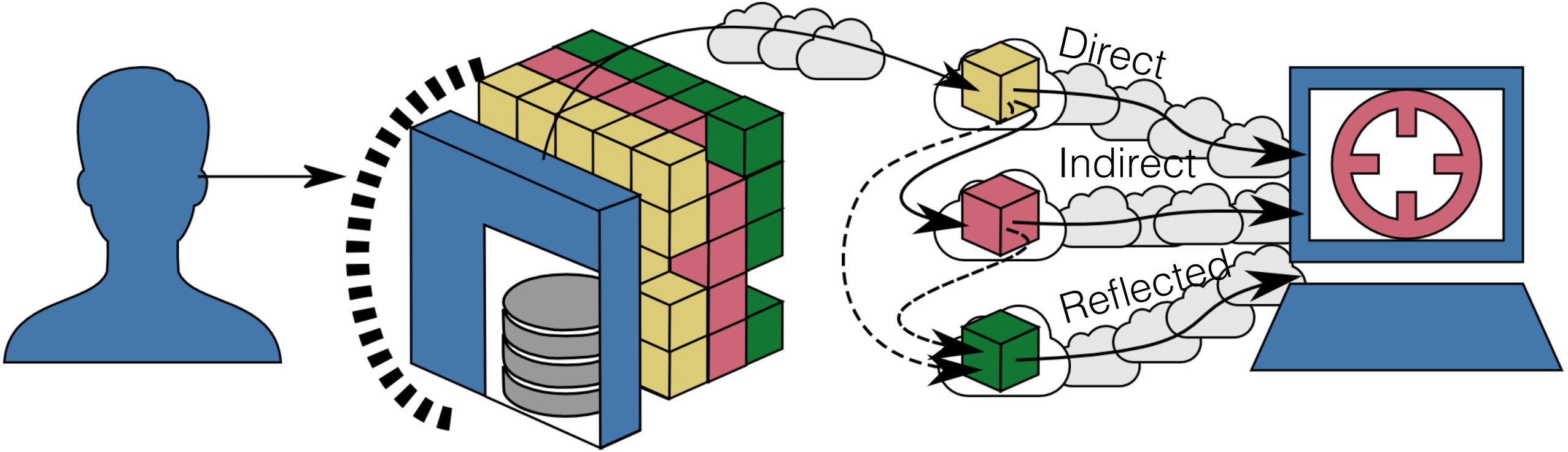


What do you want from me?

What do I want from NMRG?






Direct
Indirect
Reflected

