Characterizing and Mitigating The DDoS-as-a-Service Phenomenon

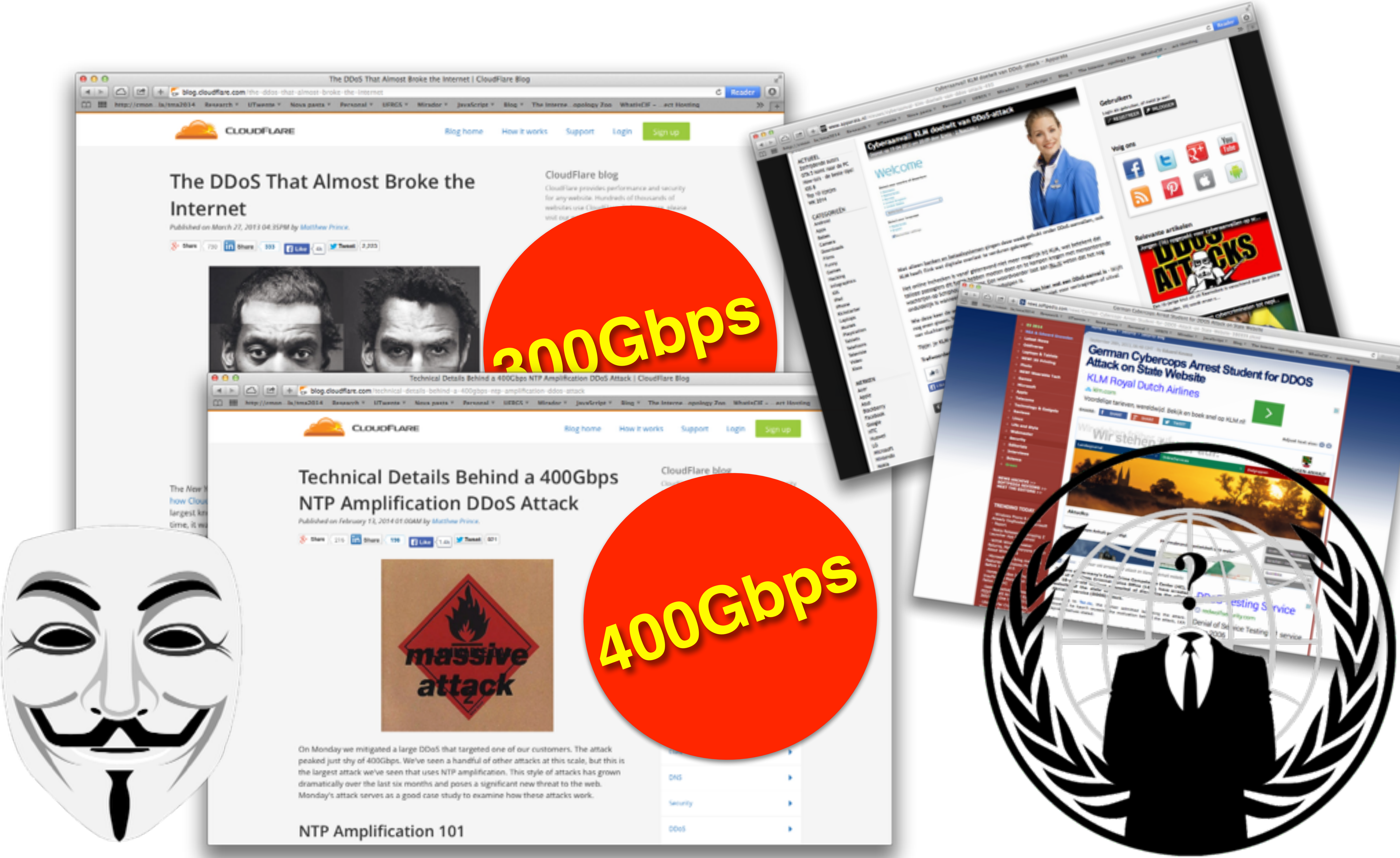
Jair Santanna

j.j.santanna@utwente.nl

Design and Analysis of
Communication Systems

30/06/2014

DDoS attacks!



The DDoS That Almost Broke the Internet | CloudFlare Blog

blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

The DDoS That Almost Broke the Internet

Published on March 27, 2013 04:35PM by Matthew Prince.

CloudFlare blog

CloudFlare provides performance and security for any website. Hundreds of thousands of websites use CloudFlare

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack | CloudFlare Blog

blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

Published on February 13, 2014 01:00AM by Matthew Prince.

On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web. Monday's attack serves as a good case study to examine how these attacks work.

NTP Amplification 101

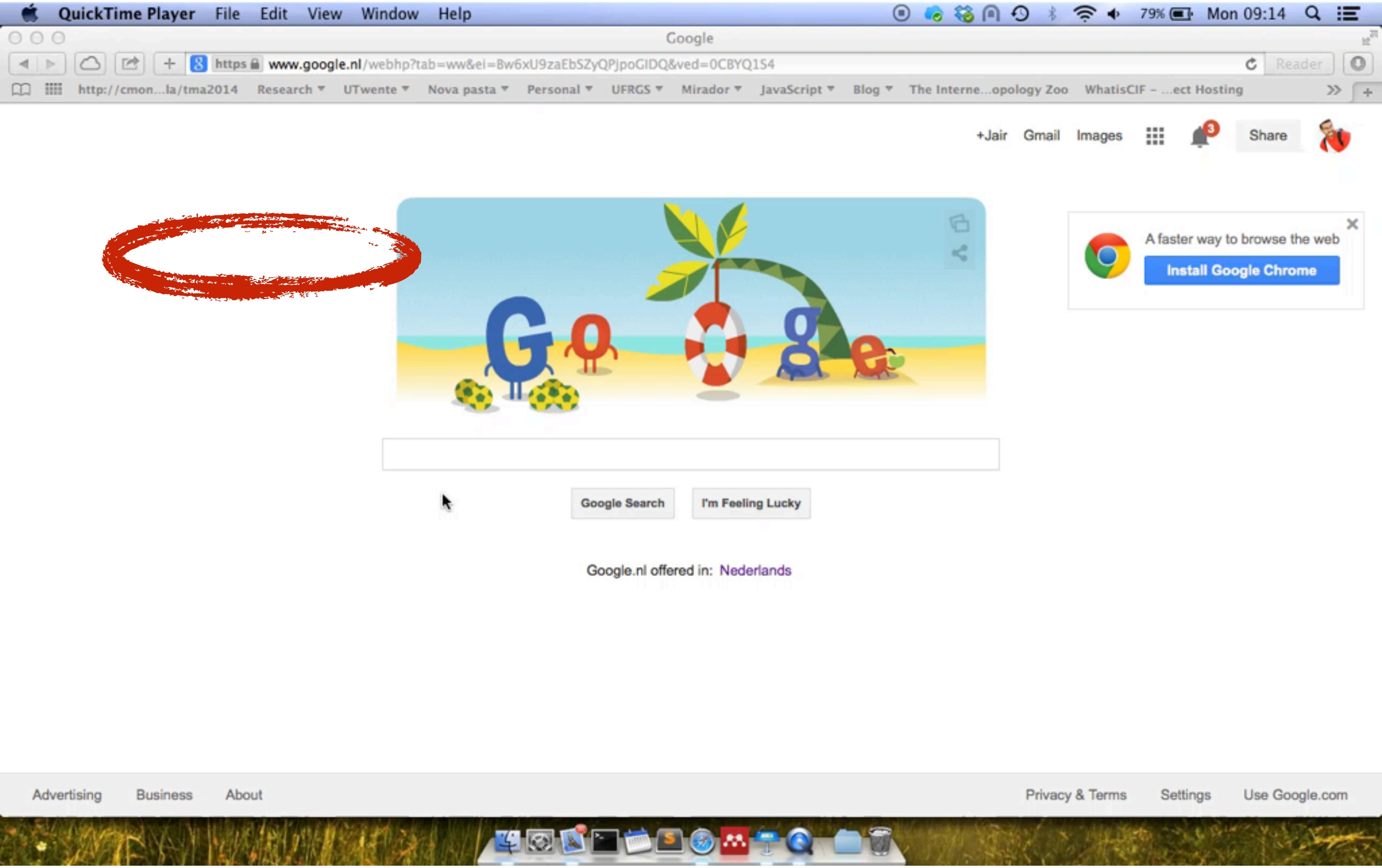
Cyberaanval! KLM doelwit van DDoS-attack

German Cybercops Arrest Student for DDOS Attack on State Website

KLM Royal Dutch Airlines

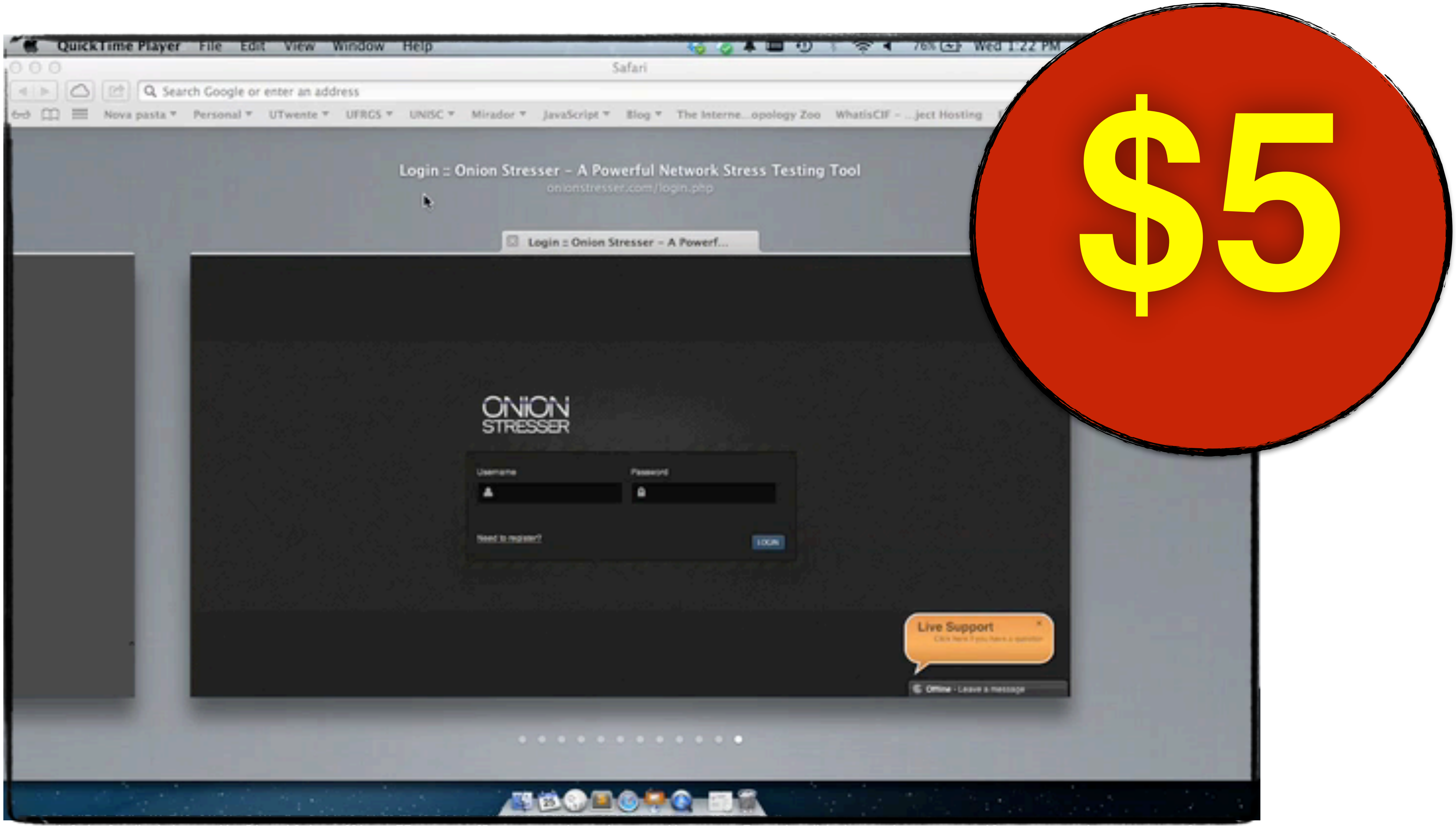
Voordelige tarieven, wereldwijd. Bekijk en boek snel op KLM.nl

ACCOUNT
BANK
IDENTITY
VIRUS
HACK
PASSWORD
*****
VIRUS
SPAM
PHOTO: ALPHASPIRIT/SHUTTERSTO
SVEN OLAF KAMPHUIS
YBERBUNKER SPOKESMAN

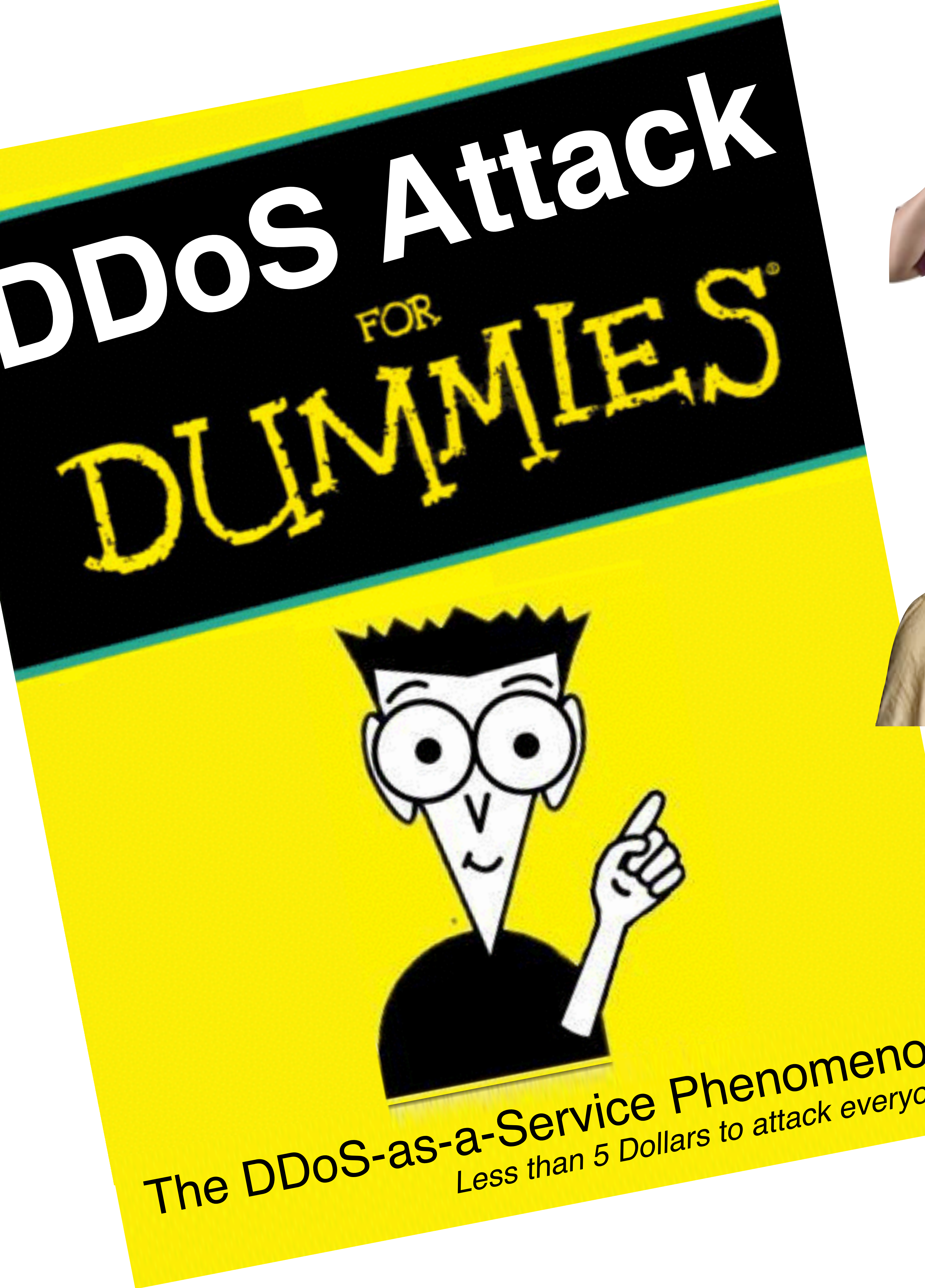


“Booter" | “Stresser" | “DDoSer" | "DDoS-as-a Service”|"DDoS-for-hire"

“Booter" | “Stresser" | “DDoSer" | "DDoS-as-a Service”|"DDoS-for-hire"


QuickTime Player File Edit View Window Help
Wed 1:22 PM
Safari
Search Google or enter an address
Nova pasta Personal UTwente UFRGS UNISC Mirador JavaScript Blog The Interne...opology Zoo WhatisCIF - ...ject Hosting
Login :: Onion Stresser - A Powerful Network Stress Testing Tool
onionstresser.com/login.php
Login :: Onion Stresser - A Powerf...
ONION STRESSER
Username
Password
Need to register?
LOGIN
Live Support
Offline - Leave a message
$5

Online Tools that offer "DDoS-as-a-$ervice".



DDoS Attack

FOR DUMMIES®

The DDoS-as-a-Service Phenomenon

Less than 5 Dollars to attack everyone

No more ONLINE exams!!

No more opponents!!

Economic Impact!!

DDoS Attack FOR DUMMIE

The DDoS-as-a-Service Phenomenon

Less than 5 Dollars to attack everyone

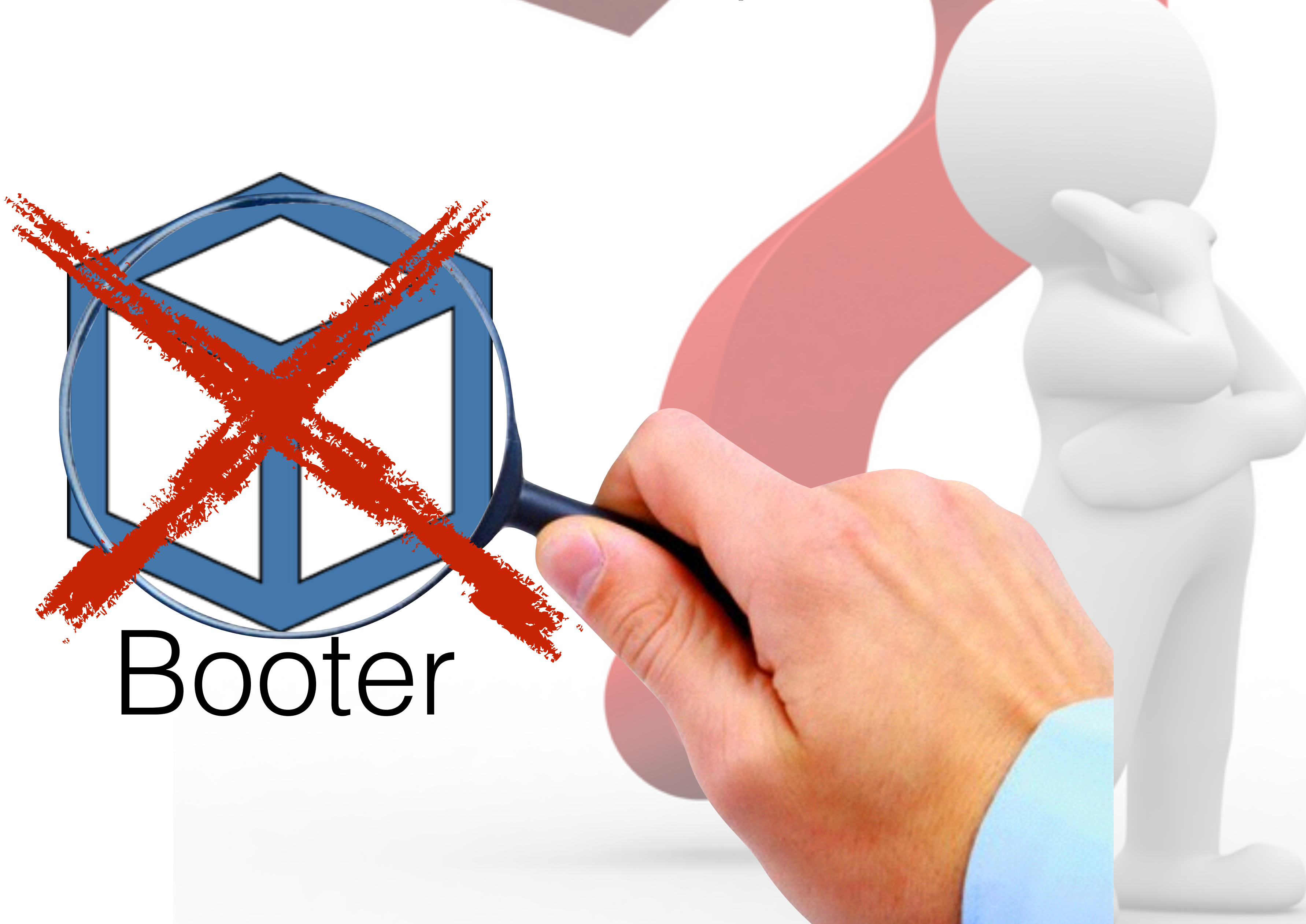
KEEP your boyfriend
far from "Nerd stuff"

More attention to your presentation!!!

Research Questions:

How to **Characterize** the DDoS-as-a-Service phenomenon?

How to **Mitigate** the DDoS-as-a-Service phenomenon?

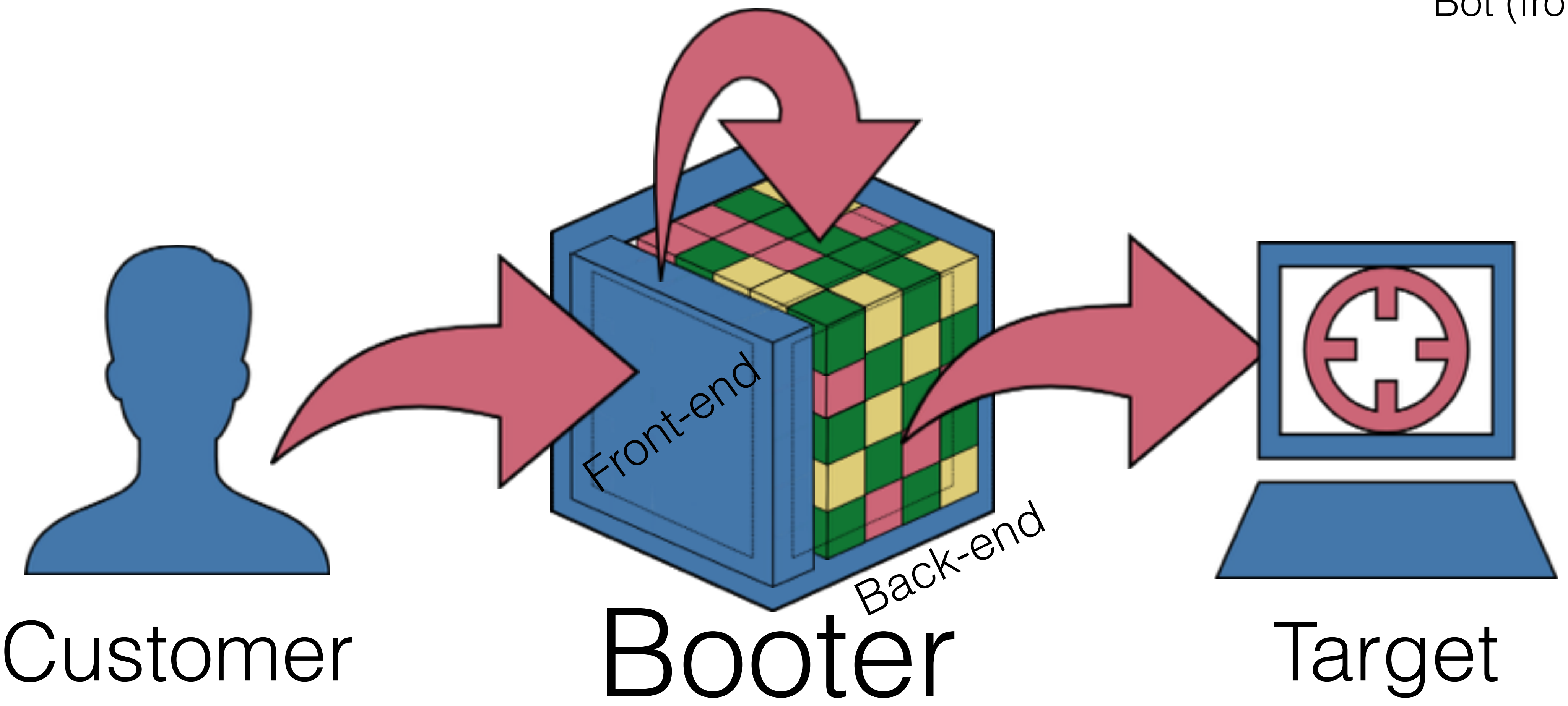


How do Booters work?

DNS Server

NTP Server

Bot (from a botnet)



Characterize

Mitigate

- How **popular** they are and **which services** they offer?
- What are the characteristics of DDoS **attacks** launched by them?
- How do they control **infrastructures** that perform attacks?

...

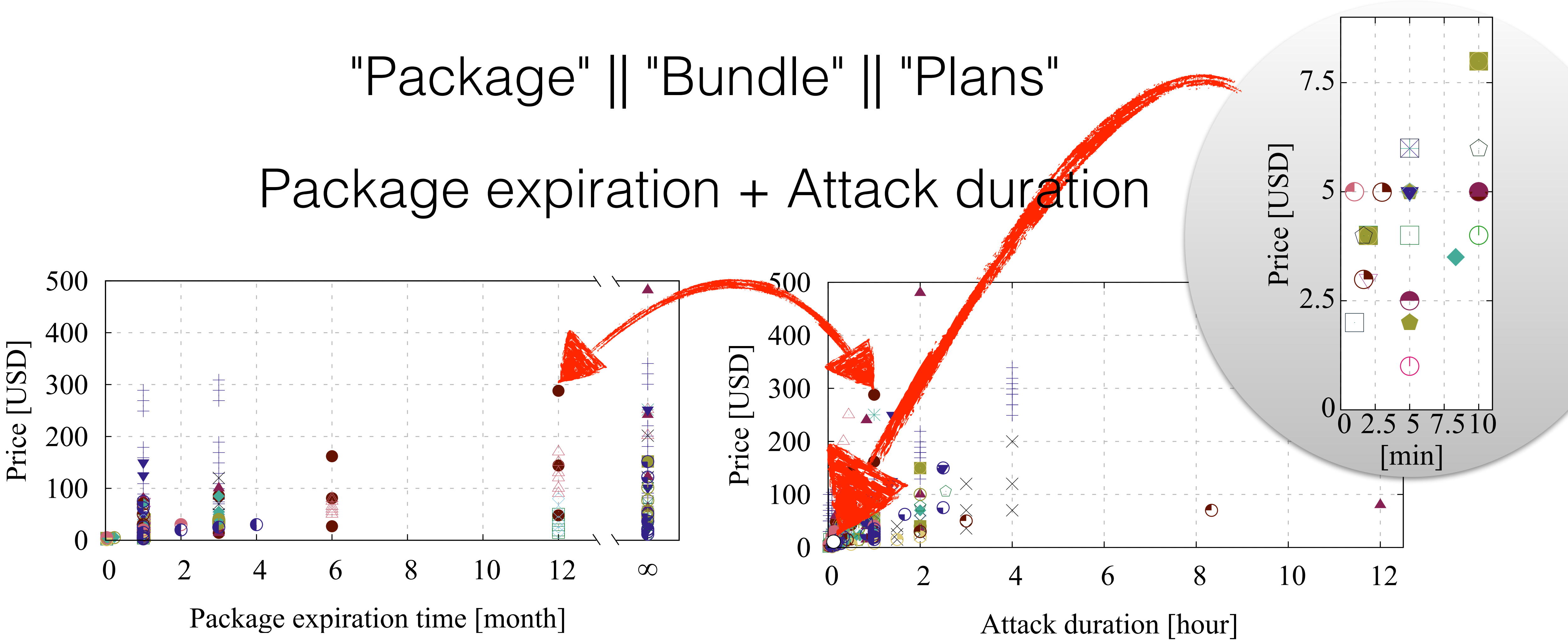
"One more thing…"

TWO

About Price

"Package" || "Bundle" || "Plans"

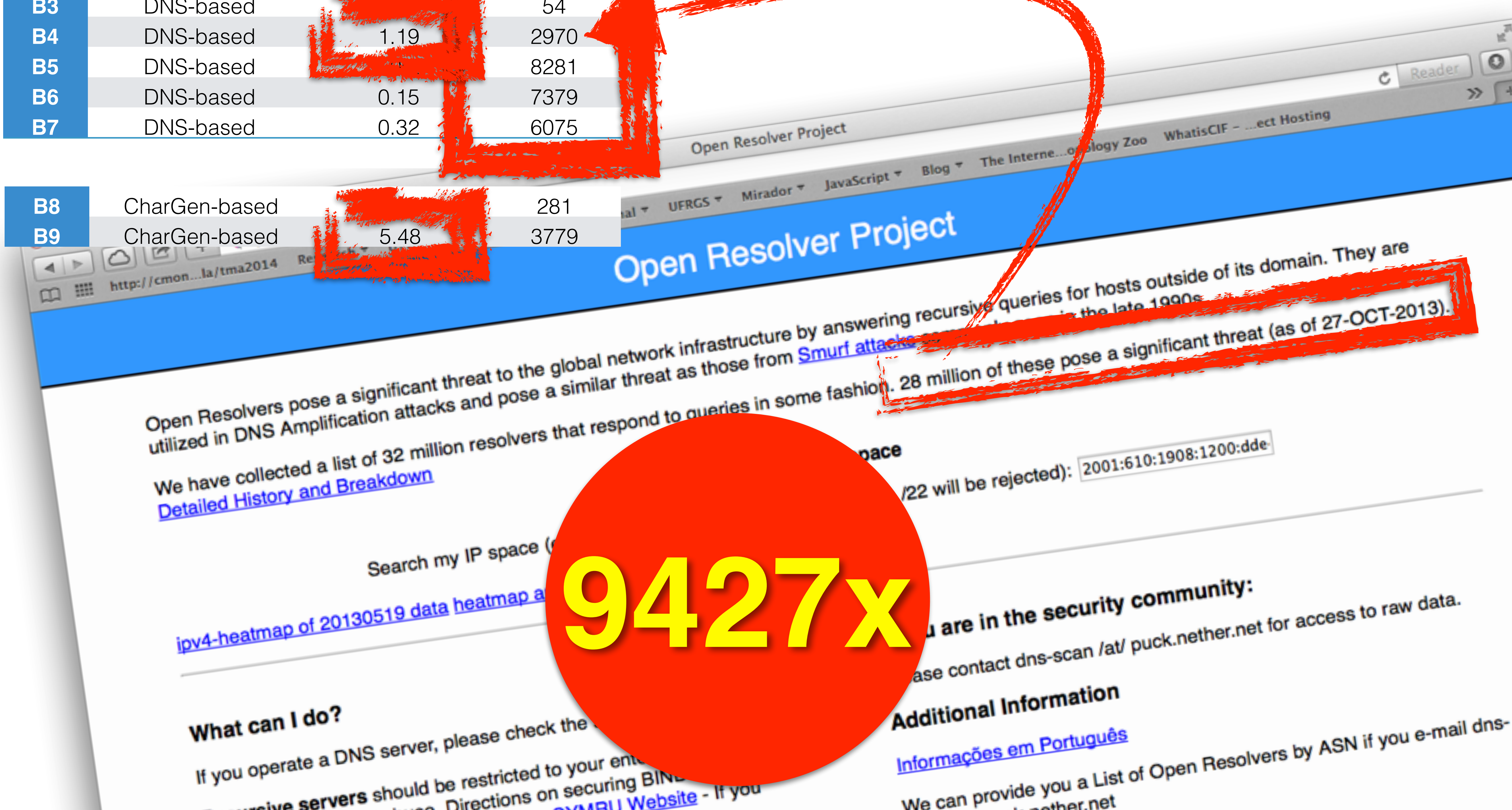
Package expiration + Attack duration



Repeat as much as you want!

Potencial for worse attacks

Booter	Type of Attack	Avg Traffic Rate [Gbps]	N° Misused systems
B1	DNS-based	0.7	4486
B2	DNS-based	0.25	78
B3	DNS-based	[redacted]	54
B4	DNS-based	1.19	2970
B5	DNS-based	[redacted]	8281
B6	DNS-based	0.15	7379
B7	DNS-based	0.32	6075
B8	CharGen-based	[redacted]	281
B9	CharGen-based	5.48	3779



Open Resolver Project

Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks ... the late 1990s.

We have collected a list of 32 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 27-OCT-2013).

Detailed History and Breakdown

...pace

Search my IP space (... /22 will be rejected): 2001:610:1908:1200:dde

ipv4-heatmap of 20130519 data heatmap a...

...u are in the security community:

...ase contact dns-scan /at/ puck.nether.net for access to raw data.

What can I do?

If you operate a DNS server, please check the ...

...rsive servers should be restricted to your ent... Directions on securing BIN... ...CYMRU Website - If you

Additional Information

Informações em Português

We can provide you a List of Open Resolvers by ASN if you e-mail dns-... ...nether.net

9427x

The DDoS-as-a-Service Phenomenon…

Very Cheap
and
Powerful*

SEVENTH FRAMEWORK PROGRAMME

Thanks!

Děkuji!

Jair Santanna
j.j.santanna@utwente.nl