NORTHWAVE
CYBER SECURITY

Revisiting a +++ Decade of DDoS Attacks

and telling the anti-ddos-coalitie history from my 5 turning points.

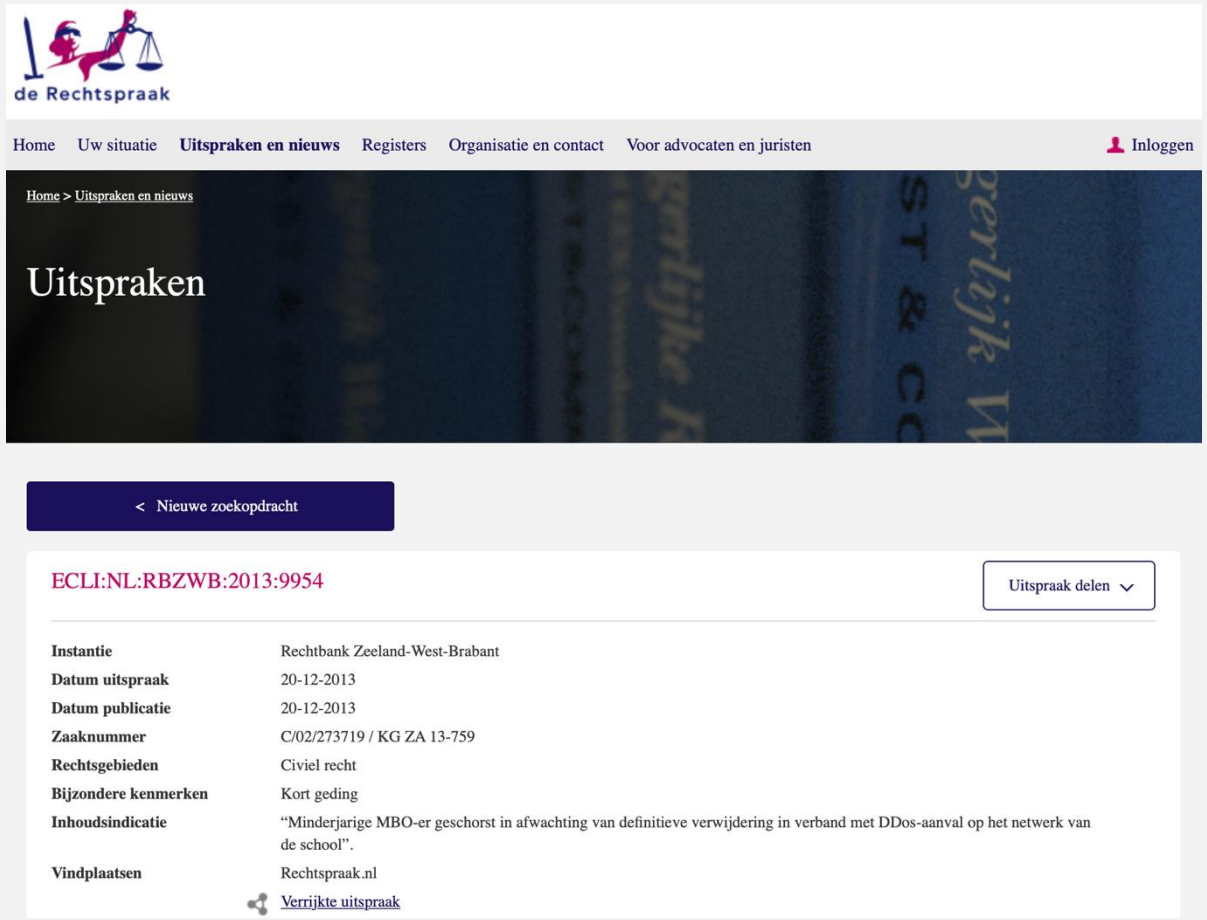
My 1st Turning Point!!

I’ve arrived here!

SURF NET

“Booter"

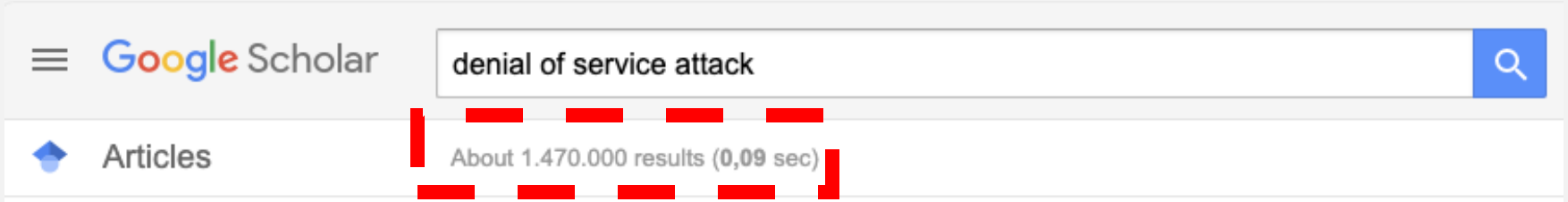
2013 (Mar.)



"Underage MBO student suspended pending final removal in connection with DDos attack on the school's network".

2013

https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2013:9954



‘Detection’
or
‘Mitigation’

How to be innovative?
Who is my ideal target audience?
How to get data?

27/11/2024

2014(Jun.)

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

Jair Santanna and Anna Sperotto

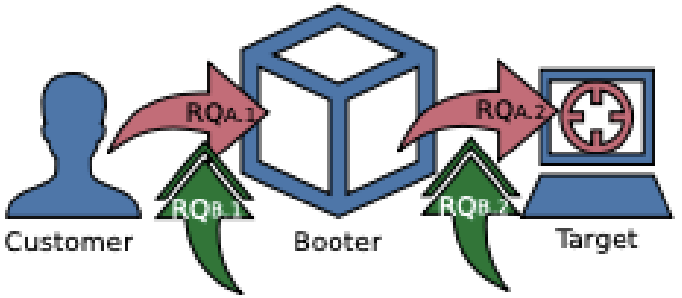
Design and Analysis of Communication Systems (DACS)
University of Twente
Enschede, The Netherlands
{j.j.santanna,a.sperotto}@utwente.nl

Abstract. Distributed Denial of Service (DDoS) attacks are an increasing threat on the Internet. Until a few years ago, these types of attacks were only launched by people with advanced knowledge of computer networks. However, nowadays the ability to launch attacks have been offered as a service to everyone, even to those without any advanced knowledge. *Booters* are online tools that offer *DDoS-as-a-Service*. Some of them advertise, for less than U$ 5, up to 25 Gbps of DDoS traffic, which is more than enough to make most hosts and services on the Internet unavailable. Booters are increasing in popularity and they have shown the success of attacks against third party services, such as government websites; however, there are few mitigation proposals. In addition, existing literature in this area provides only a partial understanding of the threat, for example by analyzing only a few aspects of one specific Booter. In this paper, we propose mitigation solutions against DDoS-as-a-Service that will be achieved after an extensive characterization of Booters. Early results show 59 different Booters, which some of them do not deliver what is offered. This research is still in its initial phase and will contribute to a Ph.D. thesis after four years.

1 Introduction

On March 2013, a Distributed Denial of Service (DDoS) attack almost broke the Internet [1]. The attacker was able to control up to 300 gigabits per second (Gbps) of network traffic and exhaust the communication resources of several hosts and networks, by misusing several services on Internet. Historically, DDoS attacks can be launched only by using advanced technical skills of the attackers, such as computer programming and specific knowledge of computer networks. These skills allow attackers to control several hosts and services with vulnerabilities on the Internet and perform attacks.

However, nowadays, a phenomenon is becoming popular: DDoS attacks are offered as a service (i.e., *DDoS-as-a-Service*), allowing everyone, even those without any kind of advanced knowledge, to launch attacks. Referred to on the Internet as *Booters*, these online tools offer several types of DDoS attacks, with different firepower (network throughput), often by charging low prices, such as



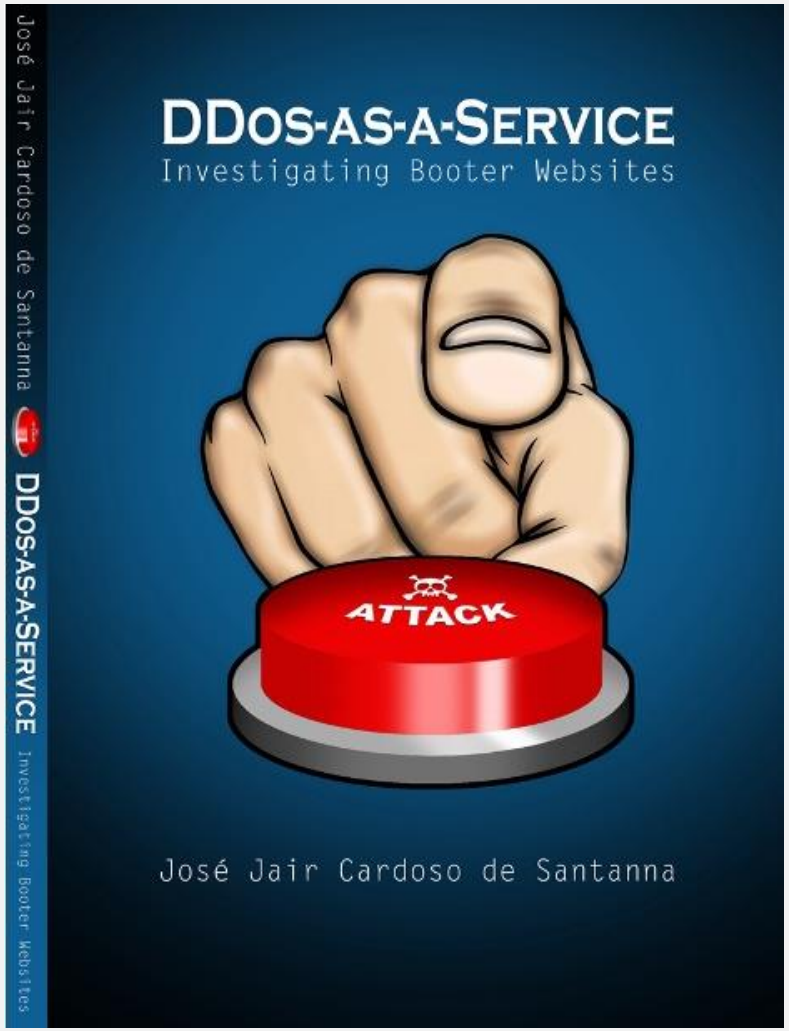
3 Early Results and Final Considerations

We have developed a crawler that uses Google's Custom Search [17] to find information related to the DDoS-as-a-Service phenomenon, such as blogs, videos, reports, and websites. We have used the following keywords: 'booter', 'ddoser', 'stresser', 'ddos-as-a-service', and 'ddos-for-hire'. Through our crawler and manual classifications, we found 59 Booters since October 2013. Among them, we have identified 34 Booters that are continuously reachable, while the other 25 appeared to be at times offline during the measurement period. The reachable Booters offer the most common DDoS attacks observed nowadays [18], which include: SYN floods, DNS amplification attacks, and attacks based on HTTP GET. In addition, experiments, performed against a dummy target at the University of Twente, seem to indicate that Booters do not always deliver what they advertise. For example, Rebel-security [19] offers 3 Gbps of attack traffic while we measured only 1 Gbps. Even worse, some Booters, such as Olympus Stresser [20] and Vdoss [21], charge money to deliver just a handful of ICMP packets, while was ordered amplification attacks based on UDP.

This research is still in its initial phase and the main goal of this work – as described previously – must be achieved within a period of four years, as the core of a Ph.D. research program.

2017

2013



https://bit.ly/jjsantanna_thesis

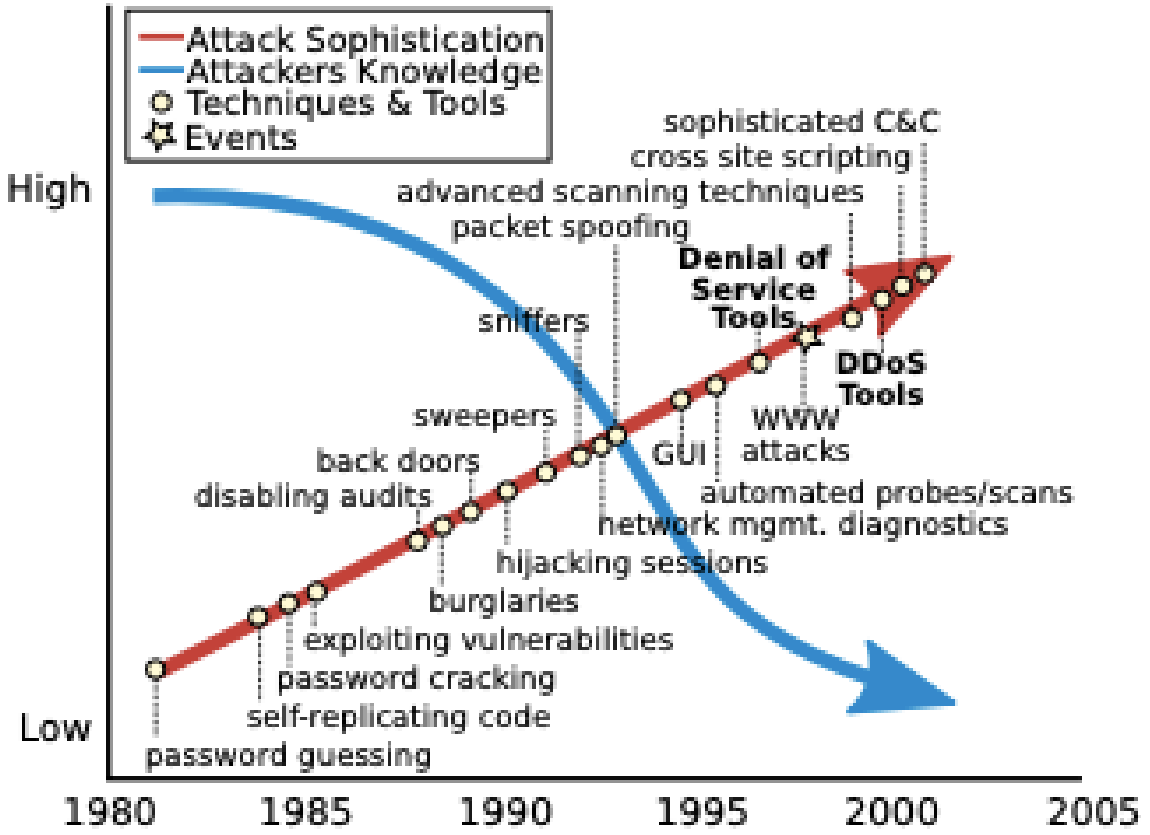


Figure 1.1: Evolution of Internet-based attacks by Lipson [58].

What about AI/LLM??

https://bit.ly/jjsantanna_thesis

p.5

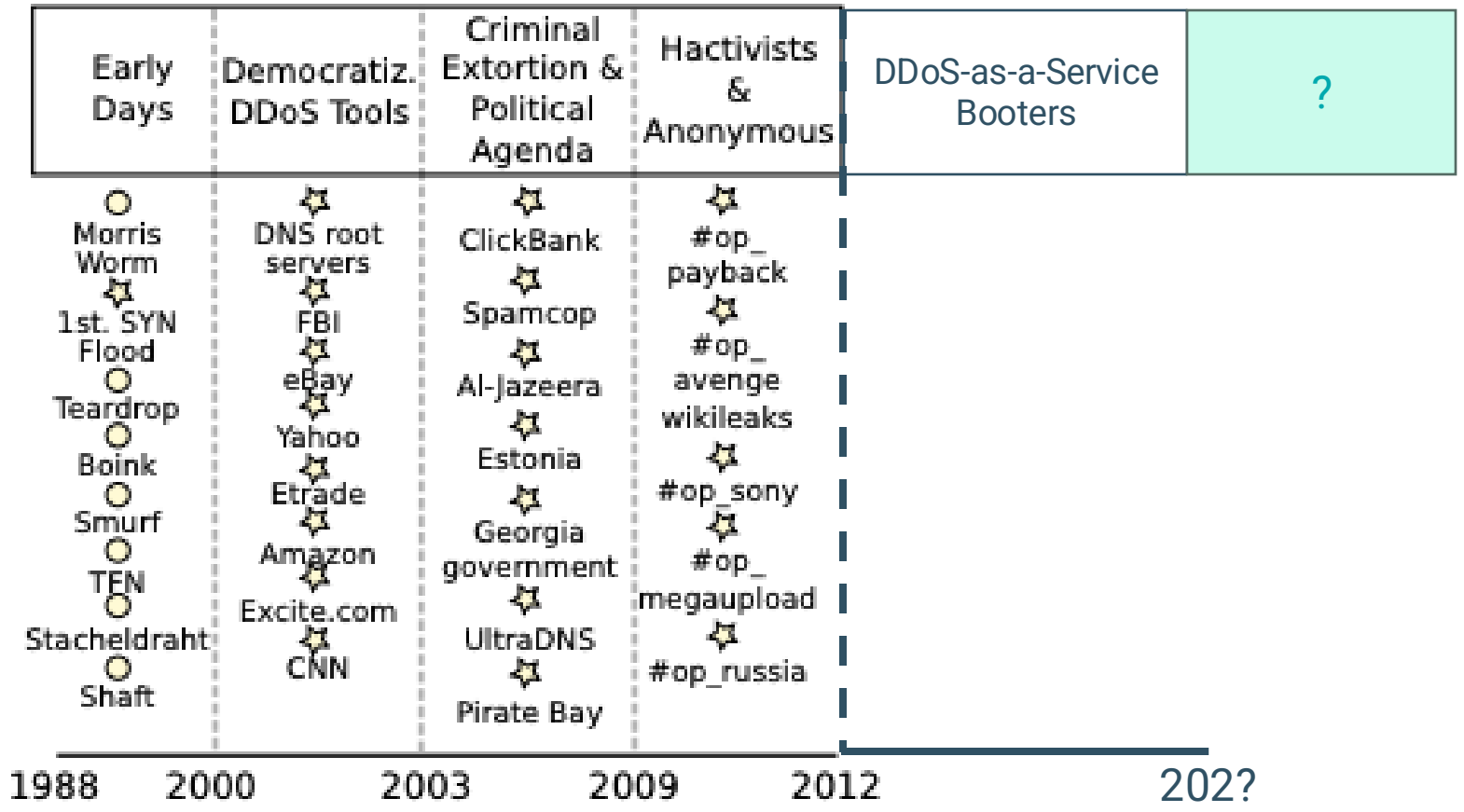
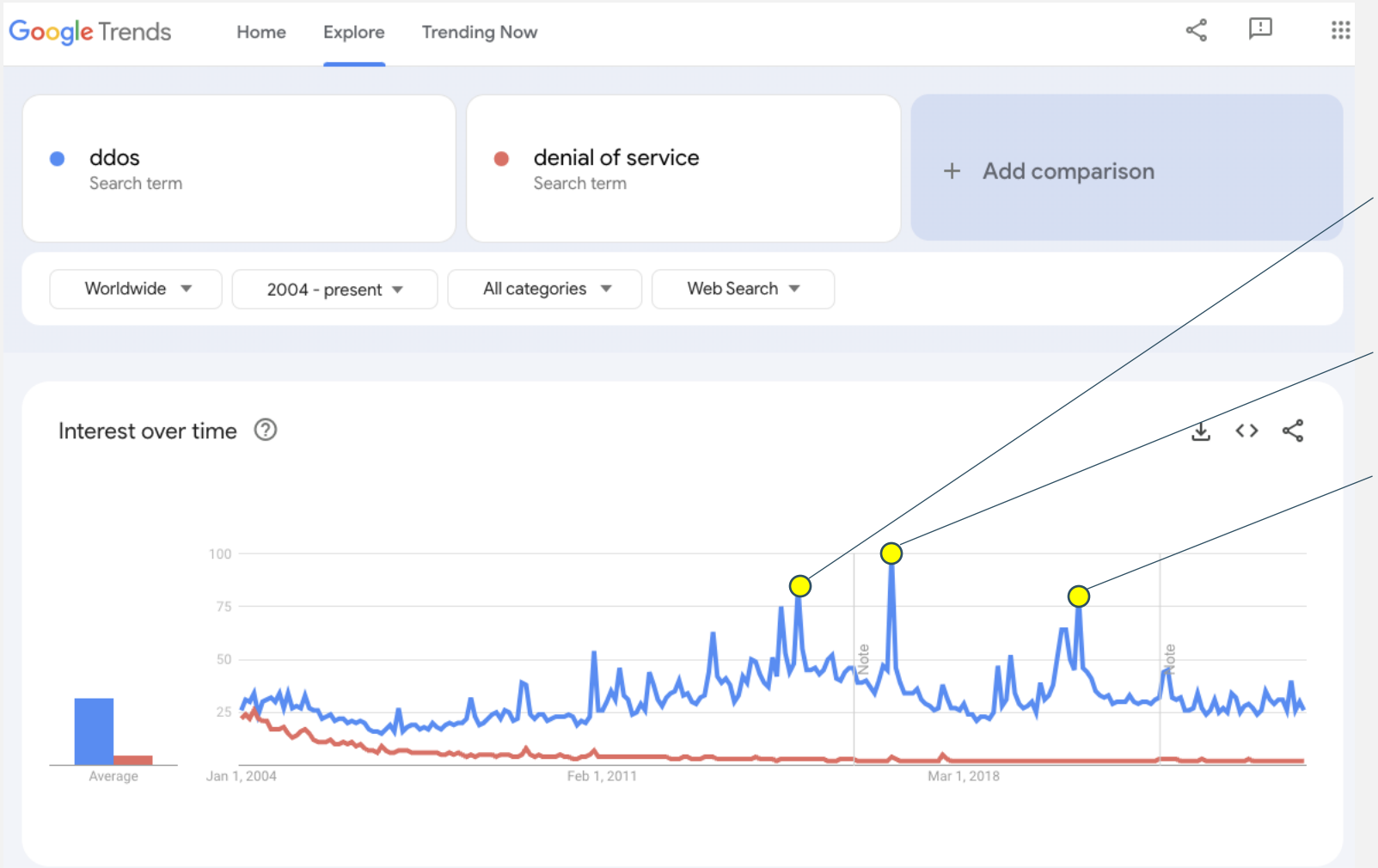


Figure 1.2: Historical evolution of DDoS attacks by Radware [75].

https://bit.ly/jjsantanna_thesis

p.6

Quiz:



Dec.2014: LizardSquad (Sony+Microsoft)

Oct.2016: Mirai botnet (Dyn)

Jun.2020: (AWS)

https://trends.google.com/trends/explore?date=all&q=ddos,denial%20of%20service&hl=en

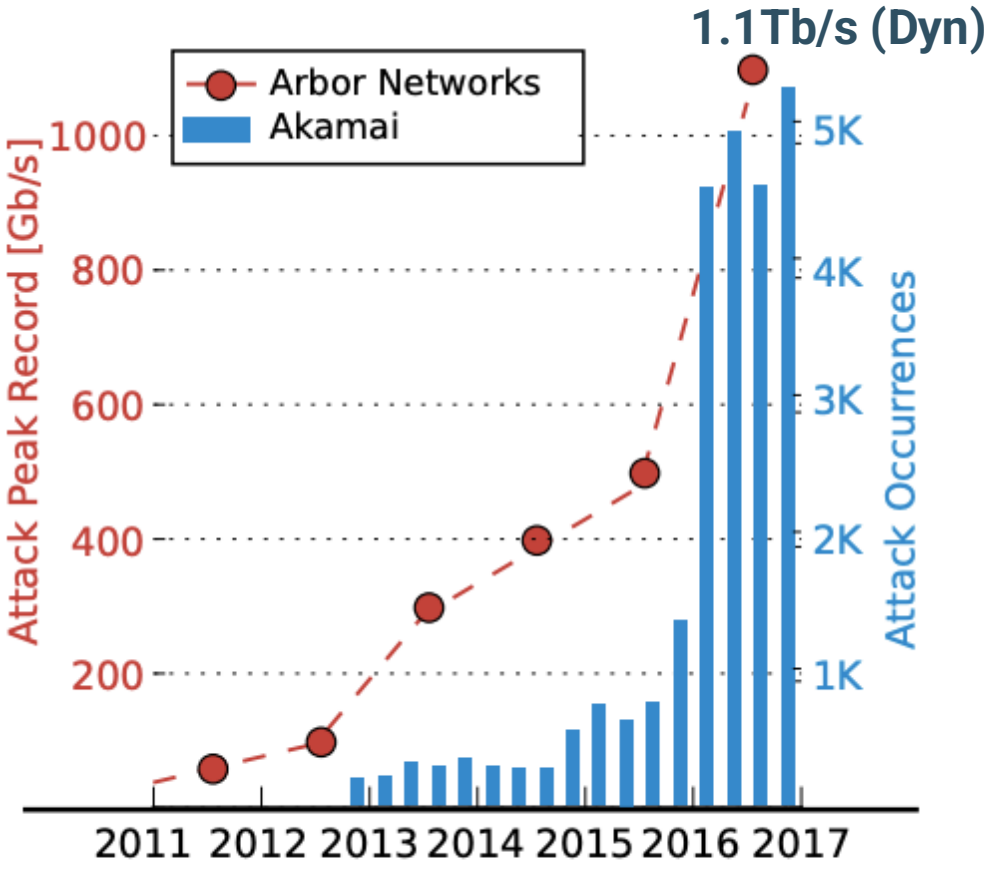
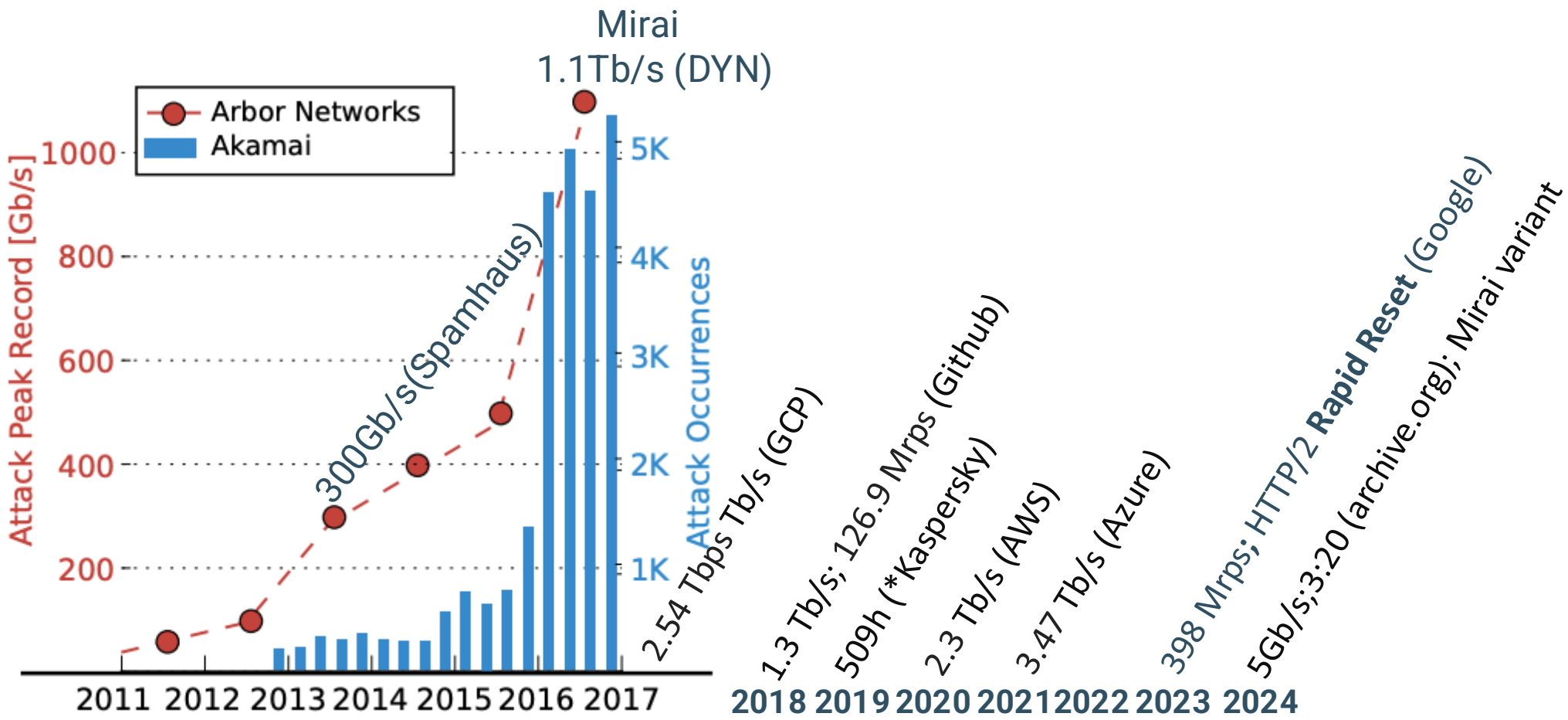


Figure 1.3: Increase of DDoS attacks.

https://bit.ly/jjsantanna_thesis



https://www.cloudflare.com/en-gb/learning/ddos/famous-ddos-attacks/

2015

Meeting (2-10)

PV

Pim van Stam <pim@nbip.nl>

Thursday, 24 September 2015 at 16:06

To: Cardoso de Santanna, J.J. (EWI)

Cc: Gerald Schaapman (NBIP)

Hi Jair,

We have a meeting planned for Oct 2nd.
My colleague Gerald (doing the project management) wants to join our meeting and certainly if your mentor/professor is/are coming too.
He is, however, not able to join at Oct 2nd.
Is it possible to shift to Tuesday Oct 6th in the afternoon?

--
With kind regards,

Pim van Stam

Stichting NBIP
pim@nbip.nl

PO Box 628
6710 BP Ede NL
Tel: +31 318 489350
Fax: +31 318 489351
WWW: http://www.nbip.nl/

nbip

Nationale Beheersorganisatie Internet Providers

My 2nd Turning Point!!

2015

NOS Nieuws Sport

NOS Nieuws • Zondag 29 november 2015, 13:08

Zwaarste DDoS-aanval op NPO ooit

De DDoS-aanval op websites van de NPO was de zwaarste aanval tot nu toe. "We zijn gewend aan grote groepen gebruikers bij groot nieuws, maar dit aantal overtrof alles", laat de publieke omroep in een reactie weten. "En allemaal op hetzelfde moment."

De NPO heeft voor dit soort situaties allerlei maatregelen voorbereid, maar erkent dat het toch fout ging. Daarom bezint de NPO zich op extra maatregelen. "In die zin leren we ook weer van deze aanval."

De NPO wijst erop dat de publieke omroep niet alleen te bereiken is via websites en apps. "De NPO heeft meerdere kanalen. Tv, radio en Twitter deden het nog gewoon."

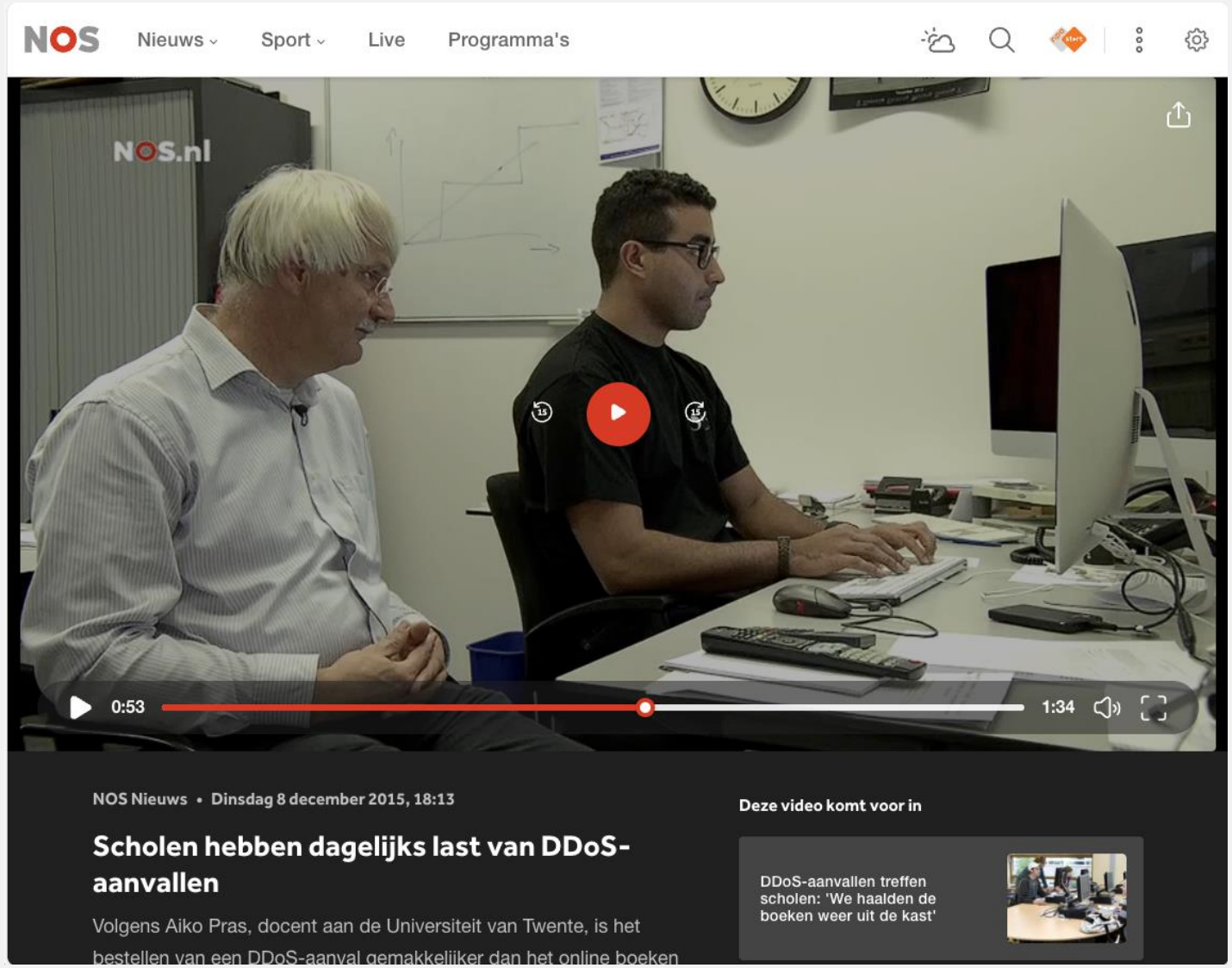
Onbereikbaar

De site en app van de NOS waren gisteravond een tijdlang onbereikbaar. Ook de sites van andere landelijke en regionale omroepen waren slecht bereikbaar.

Bij een DDoS-aanval wordt een computersysteem bestookt met extreem veel bezoeken. Wie achter de aanval zit, is onbekend.

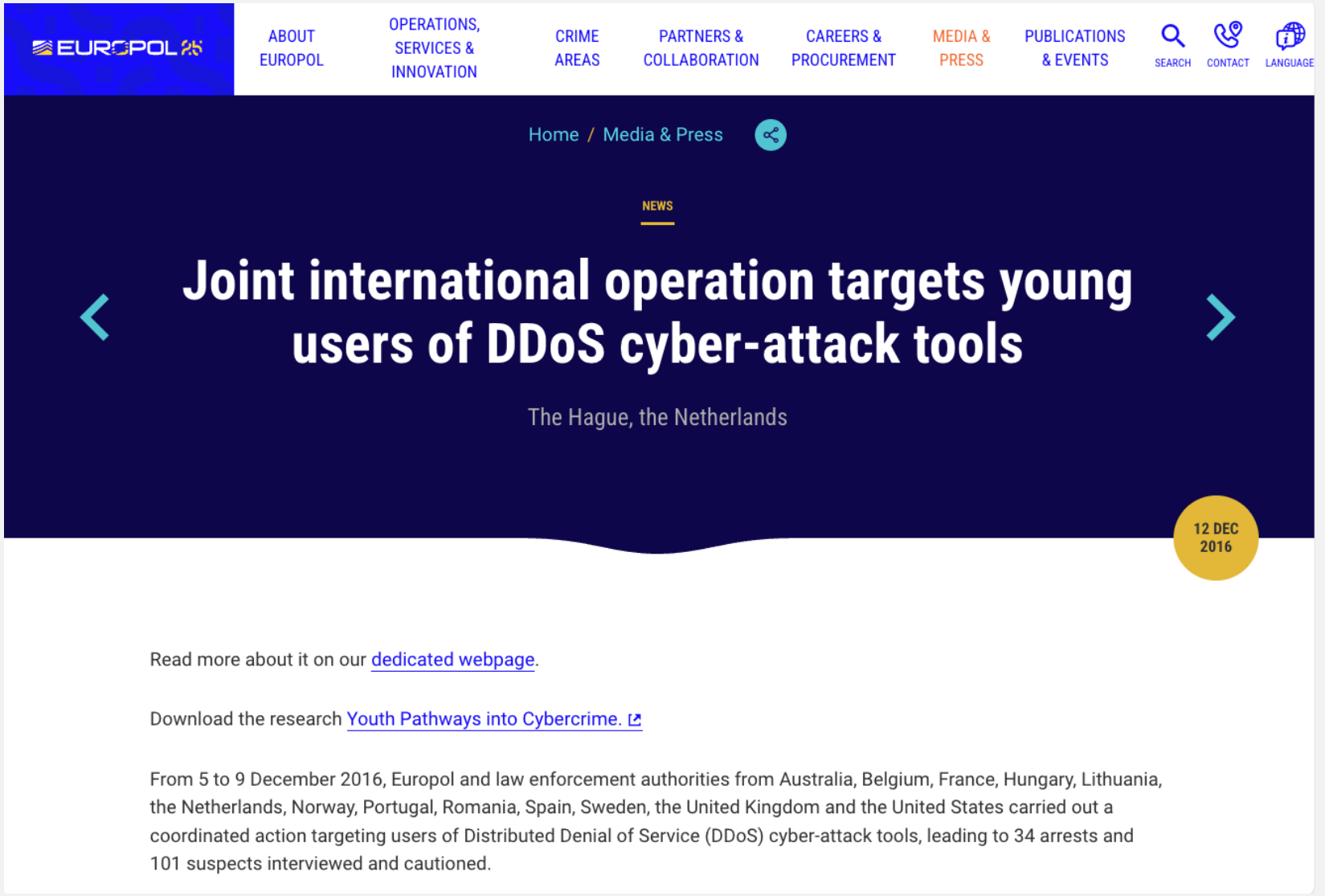
My 3rd Turning Point!!

2015



https://nos.nl/video/2073903-scholen-hebben-dagelijks-last-van-ddos-aanvallen

2016



https://www.europol.europa.eu/media-press/newsroom/news/joint-international-operation-targets-young-users-of-ddos-cyber-attack-tools

‘Operation Tarpit’

2017

Van: j.j.santanna@utwente.nl [mailto:j.j.santanna@utwente.nl]
Verzonden: donderdag 19 januari 2017 10:07
Aan: r.g.j.ruiter@nctv.minvenj.nl; Remco Ruiter
Onderwerp: Project proposal, help each other, and a cup of coffee?

Dear Remco,

We met in the D3 workshop at SURFnet in the end of 2016. I am the researcher that gave an enthusiastic presentation about Booters and DDoS attacks. Yesterday, after write a project proposal to SIDN fonds (attached) I though about you. Would you have time to drink a cup of coffee and talk about the future of DDoS and how we can help each other? Just let me know when and where and I will be there.

Coffee and chat about the future of DDoS (Jair/Floor/Remco)

RR

Remco Ruiter <r.ruiter@betaalvereniging.nl>
Required: Cardoso de Santanna, J.J. (EWI); A. F. Jansen; + 2 more
Friday, 17 February 2017 at 14:20

Wednesday, 22 February 2017 at 10:00 – 11:30. ~~Wednesday, 22 February 2017 at 10:00 – 11:3~~
The Hague, Min. Safety and Justice (see signature), (Room N22-03 Terschelling) ~~The Hagu~~

This event occurs in the past.

My 4rd Turning Point!!

2017 (Jun.)

SIDNfonds Projecten Over het fonds Nieuws Contact Aanvragen EN

DDoSDB - Collecting, Transforming, Applying, and Disseminating DDoS Attack Knowledge

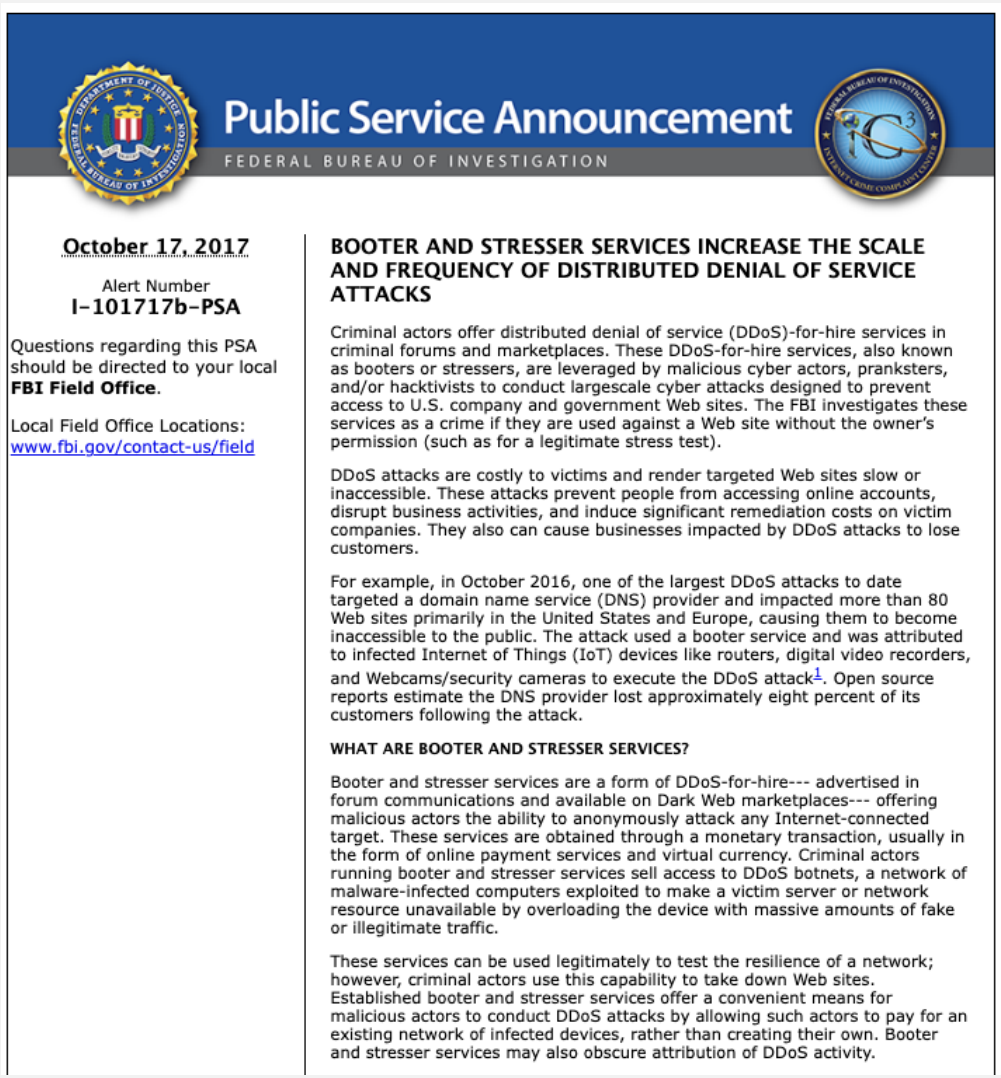
Universiteit Twente https://www.utwente.nl/ Jair Santanna, Ramin Yazsdani 2017

Wetenschappelijk onderzoek

Postdoc onderzoek om beschikbare kennis over DDoS aanvallen bijeen te brengen in een publieke database.

https://www.sidnfonds.nl/projecten/ddosdb-collecting-transforming-applying-and-disseminating-ddos-attack-knowledge

2017 (Oct.)



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 17, 2017

Alert Number
I-101717b-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BOOTER AND STRESSER SERVICES INCREASE THE SCALE AND FREQUENCY OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

Criminal actors offer distributed denial of service (DDoS)-for-hire services in criminal forums and marketplaces. These DDoS-for-hire services, also known as booters or stressers, are leveraged by malicious cyber actors, pranksters, and/or hacktivists to conduct largescale cyber attacks designed to prevent access to U.S. company and government Web sites. The FBI investigates these services as a crime if they are used against a Web site without the owner's permission (such as for a legitimate stress test).

DDoS attacks are costly to victims and render targeted Web sites slow or inaccessible. These attacks prevent people from accessing online accounts, disrupt business activities, and induce significant remediation costs on victim companies. They also can cause businesses impacted by DDoS attacks to lose customers.

For example, in October 2016, one of the largest DDoS attacks to date targeted a domain name service (DNS) provider and impacted more than 80 Web sites primarily in the United States and Europe, causing them to become inaccessible to the public. The attack used a booter service and was attributed to infected Internet of Things (IoT) devices like routers, digital video recorders, and Webcams/security cameras to execute the DDoS attack[1]. Open source reports estimate the DNS provider lost approximately eight percent of its customers following the attack.

WHAT ARE BOOTER AND STRESSER SERVICES?

Booter and stresser services are a form of DDoS-for-hire--- advertised in forum communications and available on Dark Web marketplaces--- offering malicious actors the ability to anonymously attack any Internet-connected target. These services are obtained through a monetary transaction, usually in the form of online payment services and virtual currency. Criminal actors running booter and stresser services sell access to DDoS botnets, a network of malware-infected computers exploited to make a victim server or network resource unavailable by overloading the device with massive amounts of fake or illegitimate traffic.

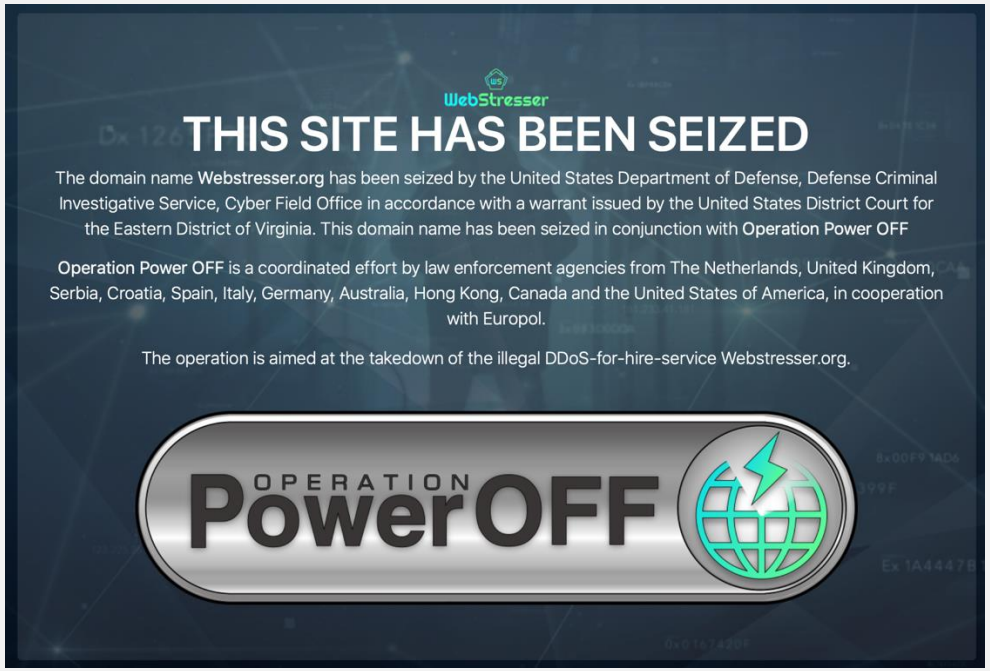
These services can be used legitimately to test the resilience of a network; however, criminal actors use this capability to take down Web sites. Established booter and stresser services offer a convenient means for malicious actors to conduct DDoS attacks by allowing such actors to pay for an existing network of infected devices, rather than creating their own. Booter and stresser services may also obscure attribution of DDoS activity.

https://web.archive.org/web/20181227020304/https://www.ic3.gov/media/2017/171017-2.aspx

2017 (Nov.)

2018

April



webstresser.org

December

anonsecurityteam.com
booter.ninja
bullstresser.net
critical-boot.com
defcon.pro
defianceprotocol.com
downthem.org
layer7-stresser.xyz
netstress.org
quantumstress.net
ragebooter.net
ragebooter.com
str3ssed.me
torsecurityteam.org
vbooter.org
request.rip

https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos

2018

"The embryo"

"NoMoreDDoS"
"Anti-DDos Coalition"
"DDoS Clearing House"

Technically:
DDoS Fingerprints
+
DDoSDB
+
Converters
+
Sharing!

2023

2019

https://www.concordia-h2020.eu/delivers/ddosclearinghouse/

2019

DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown

Daniel Kopp
DE-CIX

Matthias Wichtlhuber
DE-CIX

Ingmar Poese
BENOCS

Jair Santanna
University of Twente

Oliver Hohlfeld
Brandenburg University of Technology

Christoph Dietzel
DE-CIX / MPI for Informatics

https://arxiv.org/pdf/1909.07455

2019

RE: Can we meet earlier?

E

ewoud.smit@kpn.com <ewoud.smit@kpn...

Friday, 22 March 2019 at 10:24

To: Cardoso de Santanna, J.J. (EWI)

No problem, I just had to check it the room I booked was available. See you around 1230.

Ewoud

From: j.j.santanna@utwente.nl <j.j.santanna@utwente.nl>
Sent: vrijdag 22 maart 2019 10:20
To: Smit, Ewoud <ewoud.smit@kpn.com>
Subject: Can we meet earlier?

Hi Ewoud,
My first meeting ended before I expected. I could arrive in Hilversum around 12:30. Would you mind to see me earlier than at 14:00 (as in our appointment)?

See you later,

Jair

--
(José) Jair (Cardoso de) Santanna
Assistant Professor at University of Twente
(53)4892505

“The baby” (2nd composition)

2019

2019

“The baby” (2nd composition)

2020

My 5th Turning Point!!

1st kid
Wife with depression
COVID19

2020

DDOS-dag

HH

Huisstede, Henrique van (H.J.) <henrique.van....

Monday, 27 January 2020 at 08:48

To: 'jairsantanna@gmail.com'

Goedemorgen Jair,

Wij, het cybercrimeteam van Politie Midden Nederland, hebben DDOS als thema geadopteerd. Dat betekent dat wij nauw samen gaan werken met Rien Jansen en THTC.

Ik zie dat jij waardevol werk hebt verzet op het gebied van DDOS. Het lijkt mij heel zinvol een keer af te spreken. Sta jij daarvoor open?

Met vriendelijke groet,

Henrique van Huisstede
Operationeel Specialist B

Politie | Midden Nederland | Team Digitale Opsporing | Cybercrimeteam
Bezoek: Kroonstraat 25, 3511 RC Utrecht
Post: Postbus 8300, 3503 RH Utrecht
Tel: 0623375504

Werkdagen: Maandag, dinsdag, donderdag, vrijdag

2022

48: RoyalStresser.com, Astrostress.com, Booter.sx, Ipstressor.com, TrueSecurityServices.io

https://www.justice.gov/usao-cdca/pr/federal-prosecutors-los-angeles-and-alaska-charge-6-defendants-operating-websites

2023

Infosecurity Magazine

Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

Infosecurity Magazine Home » News » Operation Power Off: 13 More Booter Sites Seized

NEWS 9 MAY 2023

Operation Power Off: 13 More Booter Sites Seized

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

A long-running law enforcement operation continued this week after US authorities announced the seizure of 13 internet domains linked to DDoS-for-hire services.

The Department of Justice (DoJ) yesterday described the action as a "third wave" of disruption, aimed at so-called "booter" services that are designed to make the launching of DDoS attacks relatively easy for any budding cyber-criminal.

Read more on DDoS-for-hire: Booter Boss Banged Up for 13 Months.

However, 10 of the 13 domains taken down by law enforcement were linked to previous ones already seized in a December 2022 sweep that took down 48 booter services. For example, "cyberstress.org" appeared to be the same service as that

agazine.com/news/operation-power-off-13-booter/

You may also like

NEWS 14 MAY 2013
DDoS-for-hire sevices turn to mainstream advertising

NEWS 31 OCT 2022
CISA, FBI, MS-ISAC Publish Guidelines For Federal Agencies on DDoS Attacks

NEWS 23 JUL 2024
Prolific DDoS Marketplace Shut Down by UK Law Enforcement

NEWS 15 DEC 2022
Feds Hit DDoS-for-Hire Services with 48 Domain Seizures

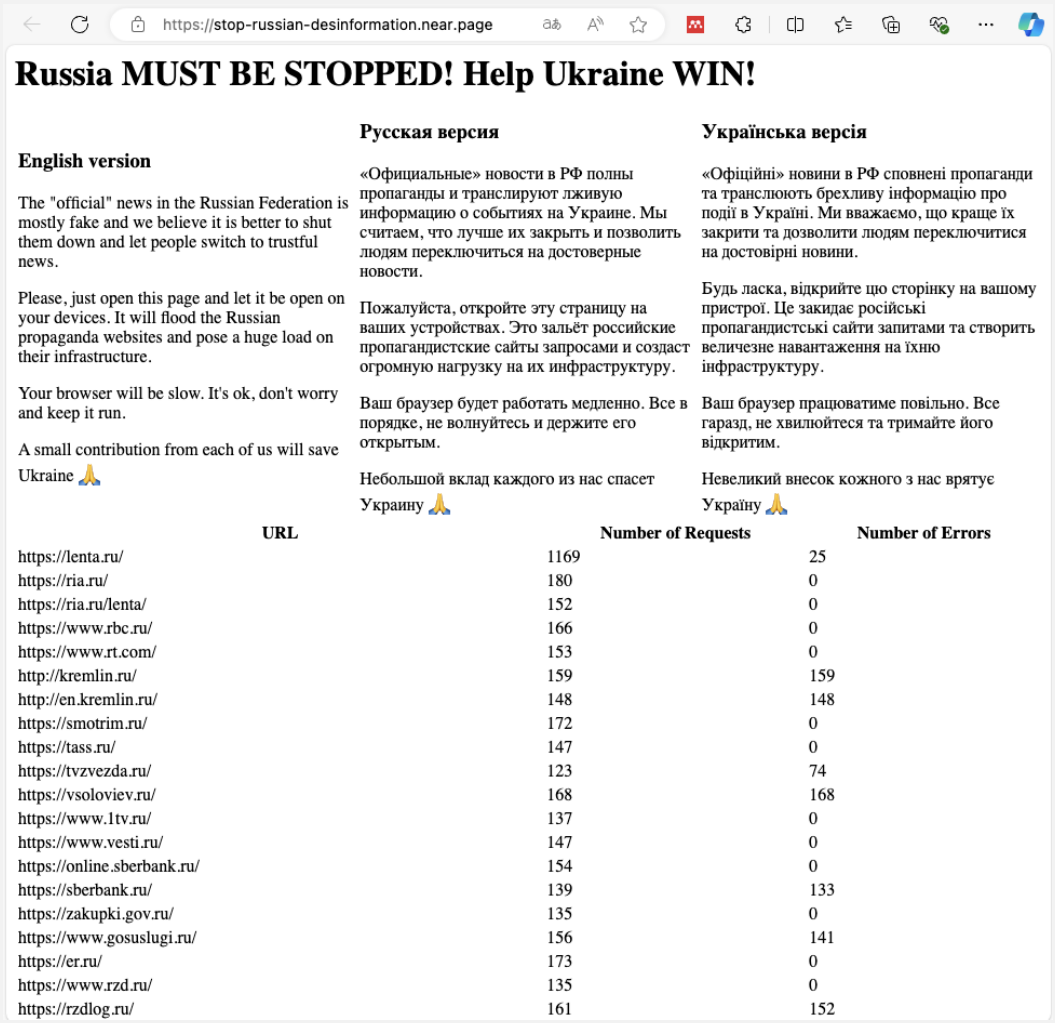
RoyalStresser.com; SecurityTeam.io; Astrostress.com; and Booter.sx

https://www.infosecurity-magazine.com/news/operation-power-off-13-booter/

3 Attacks

2022

https://stop-russian-desinformation.near.page/



https://stop-russian-desinformation.near.page

Russia MUST BE STOPPED! Help Ukraine WIN!

English version

The "official" news in the Russian Federation is mostly fake and we believe it is better to shut them down and let people switch to trustful news.

Please, just open this page and let it be open on your devices. It will flood the Russian propaganda websites and pose a huge load on their infrastructure.

Your browser will be slow. It's ok, don't worry and keep it run.

A small contribution from each of us will save Ukraine 🙏

Русская версия

«Официальные» новости в РФ полны пропаганды и транслируют лживую информацию о событиях на Украине. Мы считаем, что лучше их закрыть и позволить людям переключиться на достоверные новости.

Пожалуйста, откройте эту страницу на ваших устройствах. Это зальёт российские пропагандистские сайты запросами и создаст огромную нагрузку на их инфраструктуру.

Ваш браузер будет работать медленно. Все в порядке, не волнуйтесь и держите его открытым.

Небольшой вклад каждого из нас спасет Украину 🙏

Українська версія

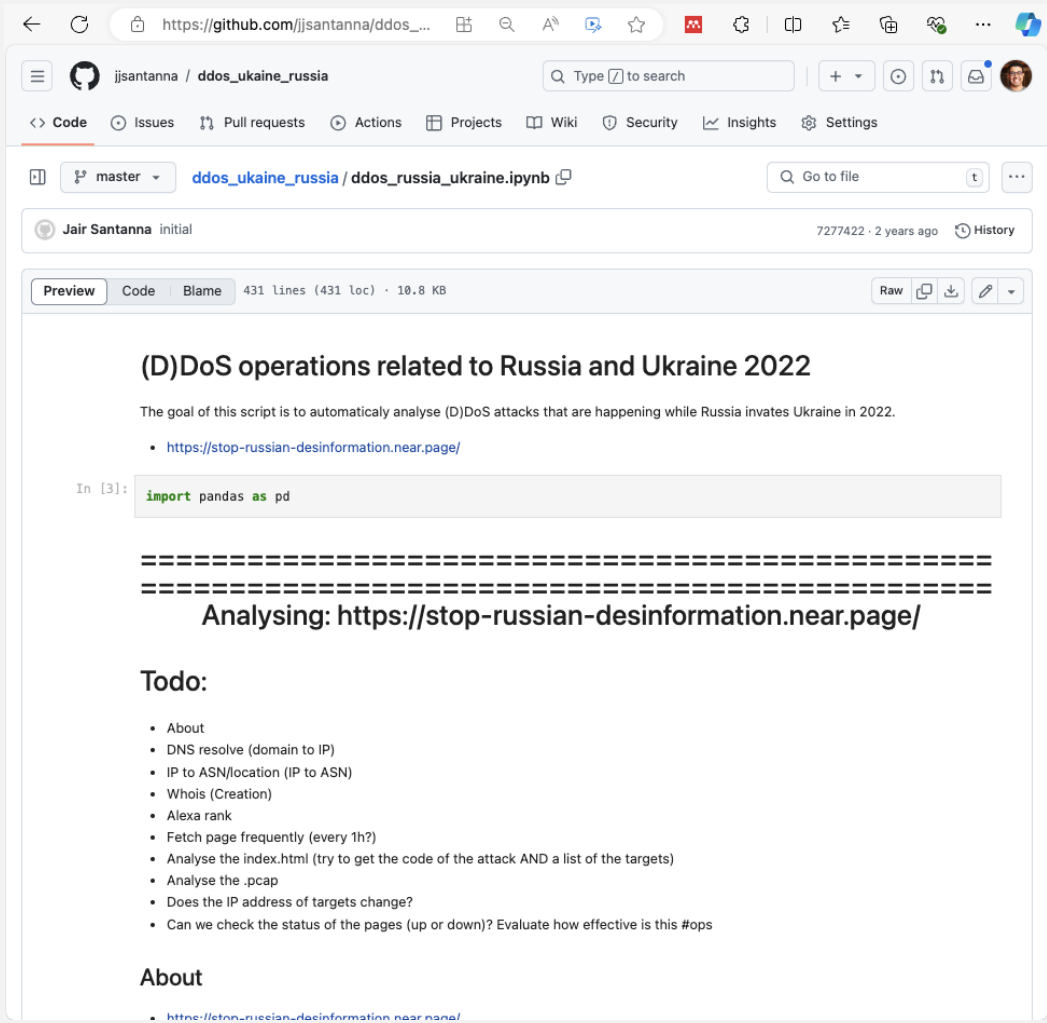
«Офіційні» новини в РФ сповнені пропаганди та транслюють брехливу інформацію про події в Україні. Ми вважаємо, що краще їх закрити та дозволити людям переключитися на достовірні новини.

Будь ласка, відкрийте цю сторінку на вашому пристрої. Це закидає російські пропагандистські сайти запитами та створить величезне навантаження на їхню інфраструктуру.

Ваш браузер працюватиме повільно. Все гаразд, не хвилюйтеся та тримайте його відкритим.

Невеликий внесок кожного з нас врятує Україну 🙏

URL	Number of Requests	Number of Errors
https://lenta.ru/	1169	25
https://ria.ru/	180	0
https://ria.ru/lenta/	152	0
https://www.rbc.ru/	166	0
https://www.rt.com/	153	0
http://kremlin.ru/	159	159
http://en.kremlin.ru/	148	148
https://smotrim.ru/	172	0
https://tass.ru/	147	0
https://tvzvezda.ru/	123	74
https://vsoloviev.ru/	168	168
https://www.1tv.ru/	137	0
https://www.vesti.ru/	147	0
https://online.sberbank.ru/	154	0
https://sberbank.ru/	139	133
https://zakupki.gov.ru/	135	0
https://www.gosuslugi.ru/	156	141
https://er.ru/	173	0
https://www.rzd.ru/	135	0
https://rzdlog.ru/	161	152



https://github.com/jjsantanna/ddos_...

jjsantanna / ddos_ukaine_russia

Type / to search

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master ddos_ukaine_russia / ddos_russia_ukraine.ipynb

Go to file t

Jair Santanna initial 7277422 · 2 years ago History

Preview Code Blame 431 lines (431 loc) · 10.8 KB Raw

(D)DoS operations related to Russia and Ukraine 2022

The goal of this script is to automaticaly analyse (D)DoS attacks that are happening while Russia invates Ukraine in 2022.

- https://stop-russian-desinformation.near.page/

In [3]:

```
import pandas as pd
```

==========
==========

Analysing: https://stop-russian-desinformation.near.page/

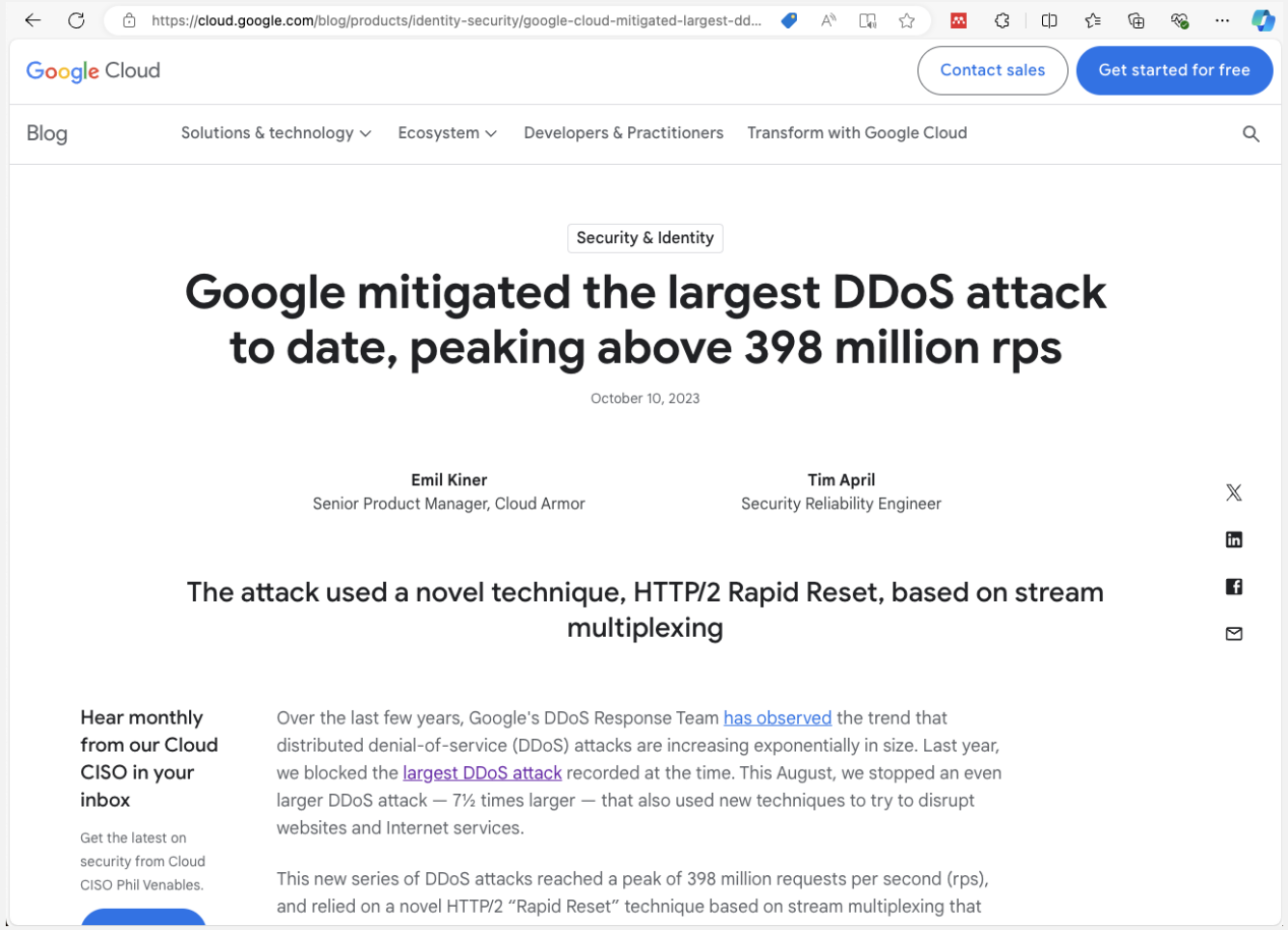
Todo:

- About
- DNS resolve (domain to IP)
- IP to ASN/location (IP to ASN)
- Whois (Creation)
- Alexa rank
- Fetch page frequently (every 1h?)
- Analyse the index.html (try to get the code of the attack AND a list of the targets)
- Analyse the .pcap
- Does the IP address of targets change?
- Can we check the status of the pages (up or down)? Evaluate how effective is this #ops

About

https://github.com/jjsantanna/ddos_ukaine_russia/blob/master/ddos_russia_ukraine.ipynb

2023



https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-dd...

Google Cloud | Contact sales | Get started for free

Blog | Solutions & technology | Ecosystem | Developers & Practitioners | Transform with Google Cloud

Security & Identity

Google mitigated the largest DDoS attack to date, peaking above 398 million rps

October 10, 2023

Emil Kiner
Senior Product Manager, Cloud Armor

Tim April
Security Reliability Engineer

The attack used a novel technique, HTTP/2 Rapid Reset, based on stream multiplexing

Hear monthly from our Cloud CISO in your inbox

Get the latest on security from Cloud CISO Phil Venables.

Over the last few years, Google's DDoS Response Team has observed the trend that distributed denial-of-service (DDoS) attacks are increasing exponentially in size. Last year, we blocked the largest DDoS attack recorded at the time. This August, we stopped an even larger DDoS attack — 7½ times larger — that also used new techniques to try to disrupt websites and Internet services.

This new series of DDoS attacks reached a peak of 398 million requests per second (rps), and relied on a novel HTTP/2 "Rapid Reset" technique based on stream multiplexing that

"Largest-recorded DDoS attack peaked at 46 million rps."

"Zero-day"

"CVE-2023-44487 with a CVSS score of 7.5"

2024

External website breach

CERT-UT (LISA) <CERT@utwente.nl> Thursday, 10 October 2024 at 11:21

To: CERT-UT (LISA)

Dear colleague,

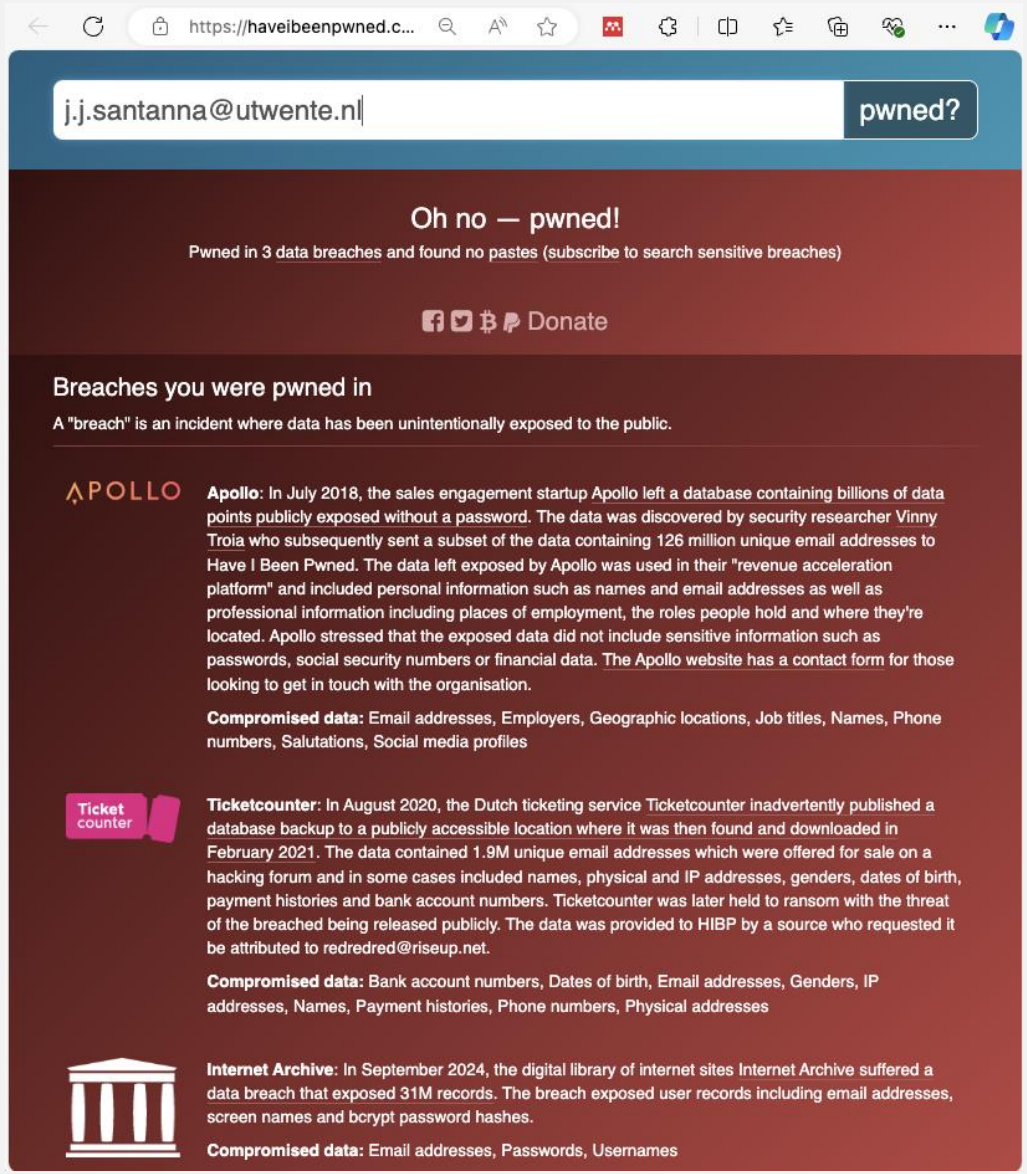
The university received information about a recent security breach affecting the Internet Archive website (archive.org). Among other things, username and password data was leaked.

You're receiving this email because an account that was linked to your university e-mail address was present in the leaked data.

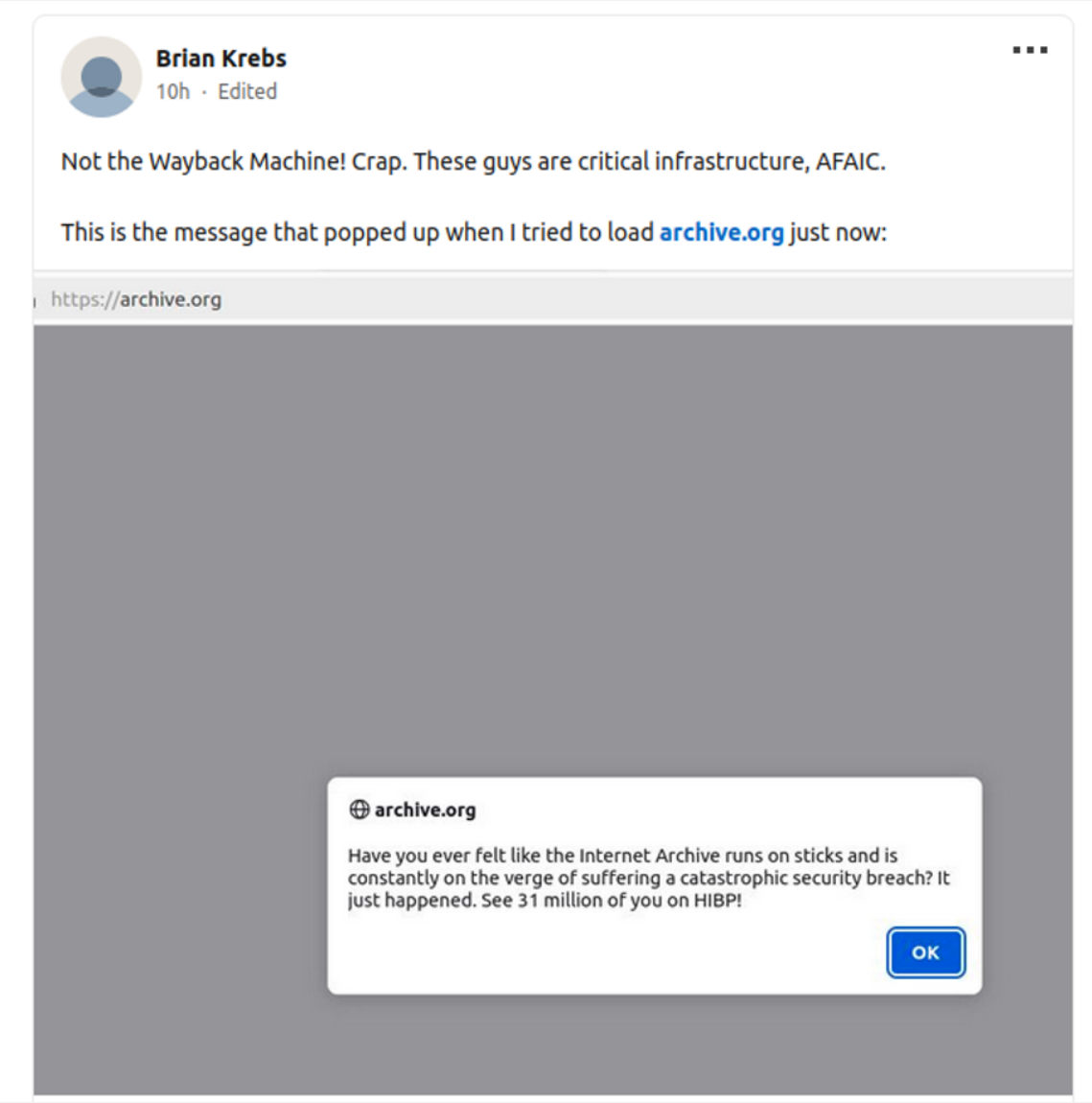
We would like to advise you to change the password for your Internet Archive account. In case you used the old password for other accounts you should change those as well, especially if this applies to your university account.

Kind regards,

Leon Haverkotte | CERT-UT | University of Twente | Library, ICT Services & Archive (LISA) | Campus building Spiegel, room 226 | T: +31 (0)53 - 489 3016 | l.m.c.haverkotte@utwente.nl | www.utwente.nl/lisa



2024



"Have you ever felt like the Internet Archive runs on sticks and is constantly on the verge of suffering a catastrophic security breach? It just . See 31 million of you on HIBP!"

2024


Brewster Kahle @brewster_kahle · Oct 10
Sorry, but DDOS folks are back and knocked archive.org and openlibrary.org offline.
@internetarchive is being cautious and prioritizing keeping data safe at the expense of service availability.
Will share more as we know it.
325
1.1K
6.2K
1.1M
Brewster Kahle
@brewster_kahle
What we know: DDOS attack–fended off for now; defacement of our website via JS library; breach of usernames/email/salted-encrypted passwords.
What we've done: Disabled the JS library, scrubbing systems, upgrading security.
Will share more as we know it.
3:08 AM · Oct 10, 2024 · 1.3M Views
177
1.2K
8.4K
756

2024

NETSCOUT ASERT observed 24 DDoS attacks against the Autonomous System Number (ASN) 7941, the ASN used by the Internet Archive project.

The first attack event started on October 09, 17:02 UTC and continued until 20:23 UTC the same day--at least 3 hours, 20 minutes of active DDoS activity.

During the attack campaign, at least three distinct IP addresses used by archive.org received DDoS attack traffic.

TCP RST floods and HTTPS application layer attacks

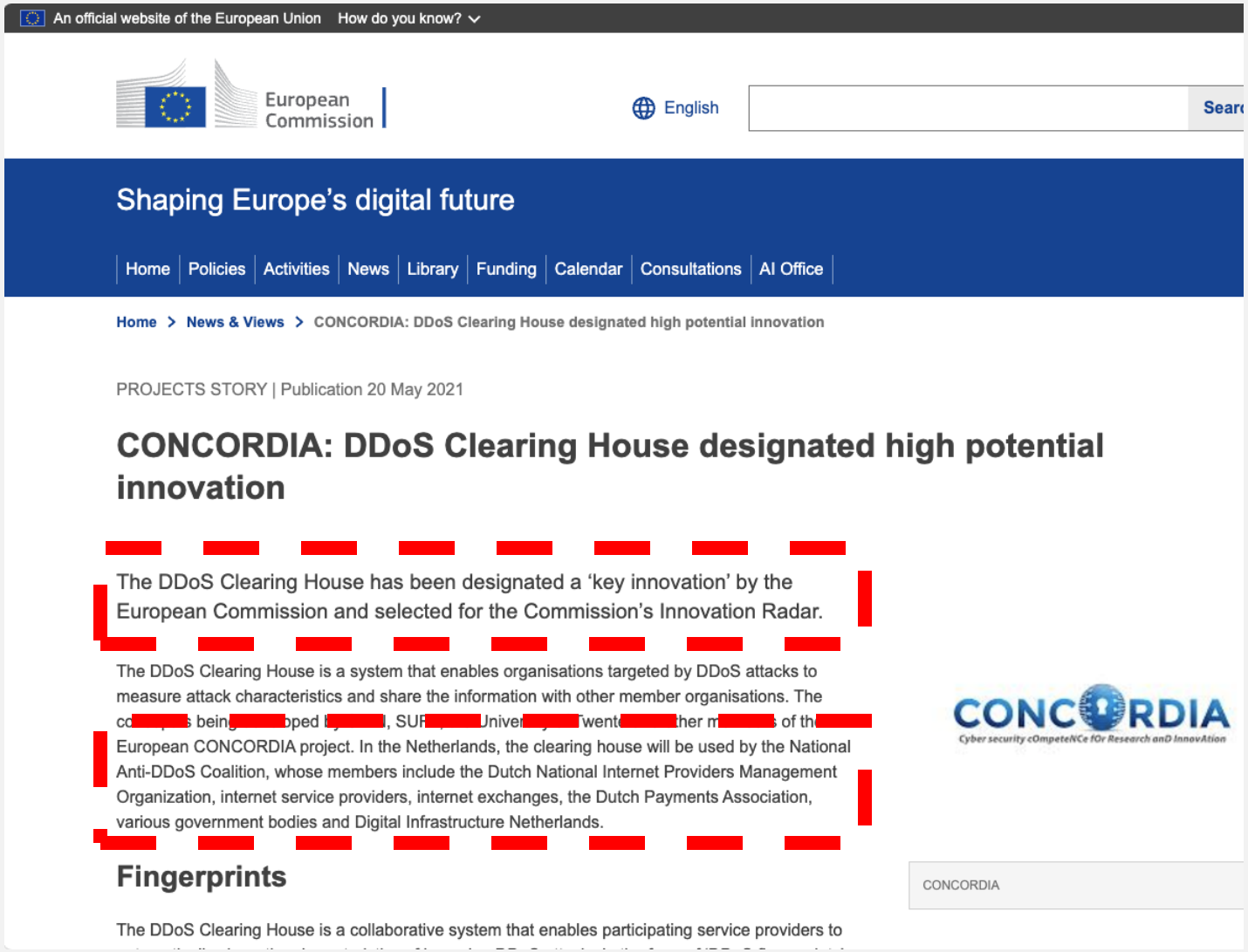
Peak ~5Gbps

Mirai variant; from South Korea, China, and Brazil

https://www.netscout.com/blog/asert/internet-archive-under-assault

Some Reflections

2021



An official website of the European Union How do you know?

European Commission

English

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > News & Views > CONCORDIA: DDoS Clearing House designated high potential innovation

PROJECTS STORY | Publication 20 May 2021

CONCORDIA: DDoS Clearing House designated high potential innovation

The DDoS Clearing House has been designated a 'key innovation' by the European Commission and selected for the Commission's Innovation Radar.

The DDoS Clearing House is a system that enables organisations targeted by DDoS attacks to measure attack characteristics and share the information with other member organisations. The co[redacted]s being [redacted]oped [redacted], SUF[redacted]Univer[redacted]went[redacted]ther m[redacted]s of th[redacted] European CONCORDIA project. In the Netherlands, the clearing house will be used by the National Anti-DDoS Coalition, whose members include the Dutch National Internet Providers Management Organization, internet service providers, internet exchanges, the Dutch Payments Association, various government bodies and Digital Infrastructure Netherlands.

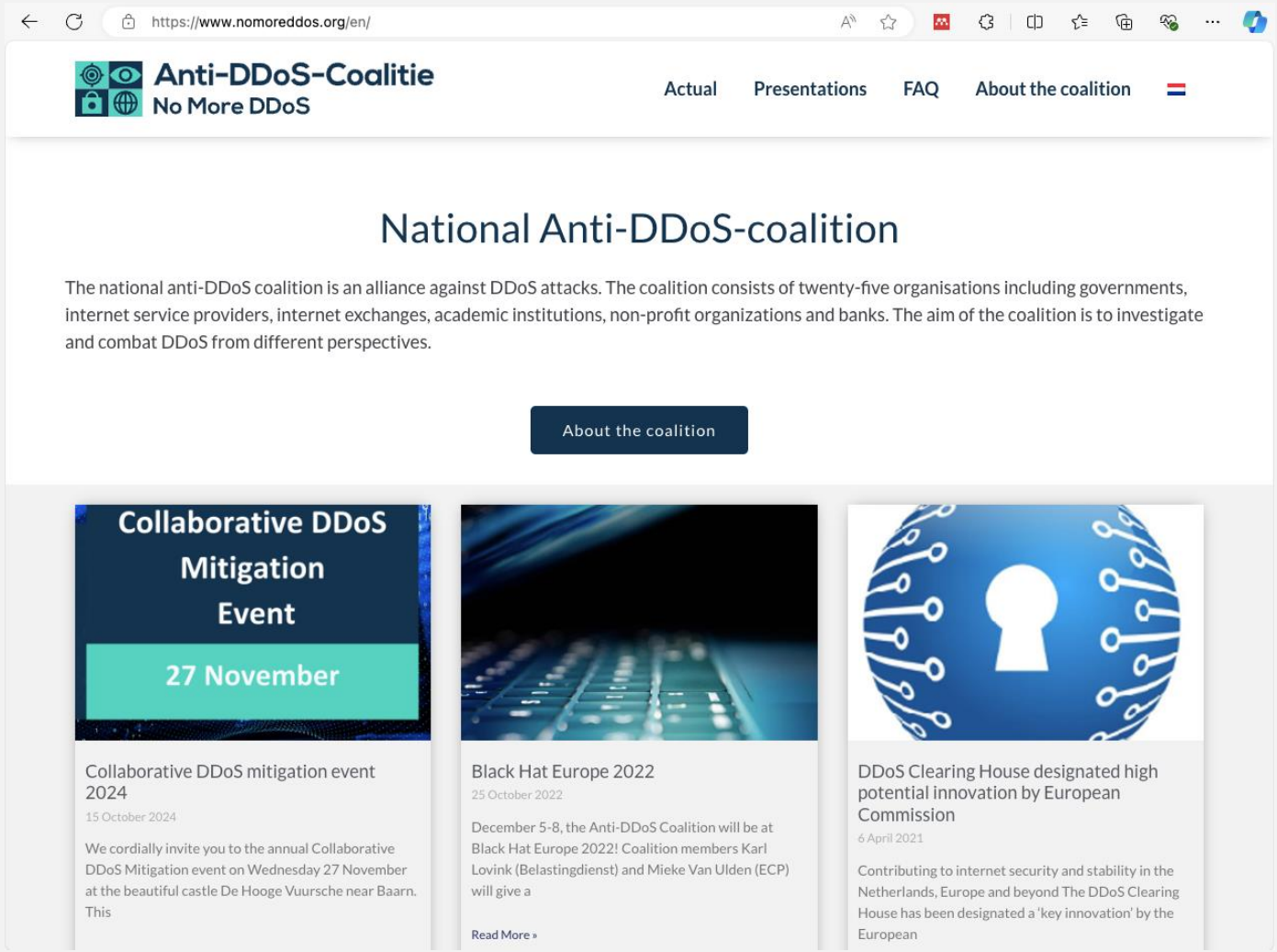
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Fingerprints

CONCORDIA

The DDoS Clearing House is a collaborative system that enables participating service providers to

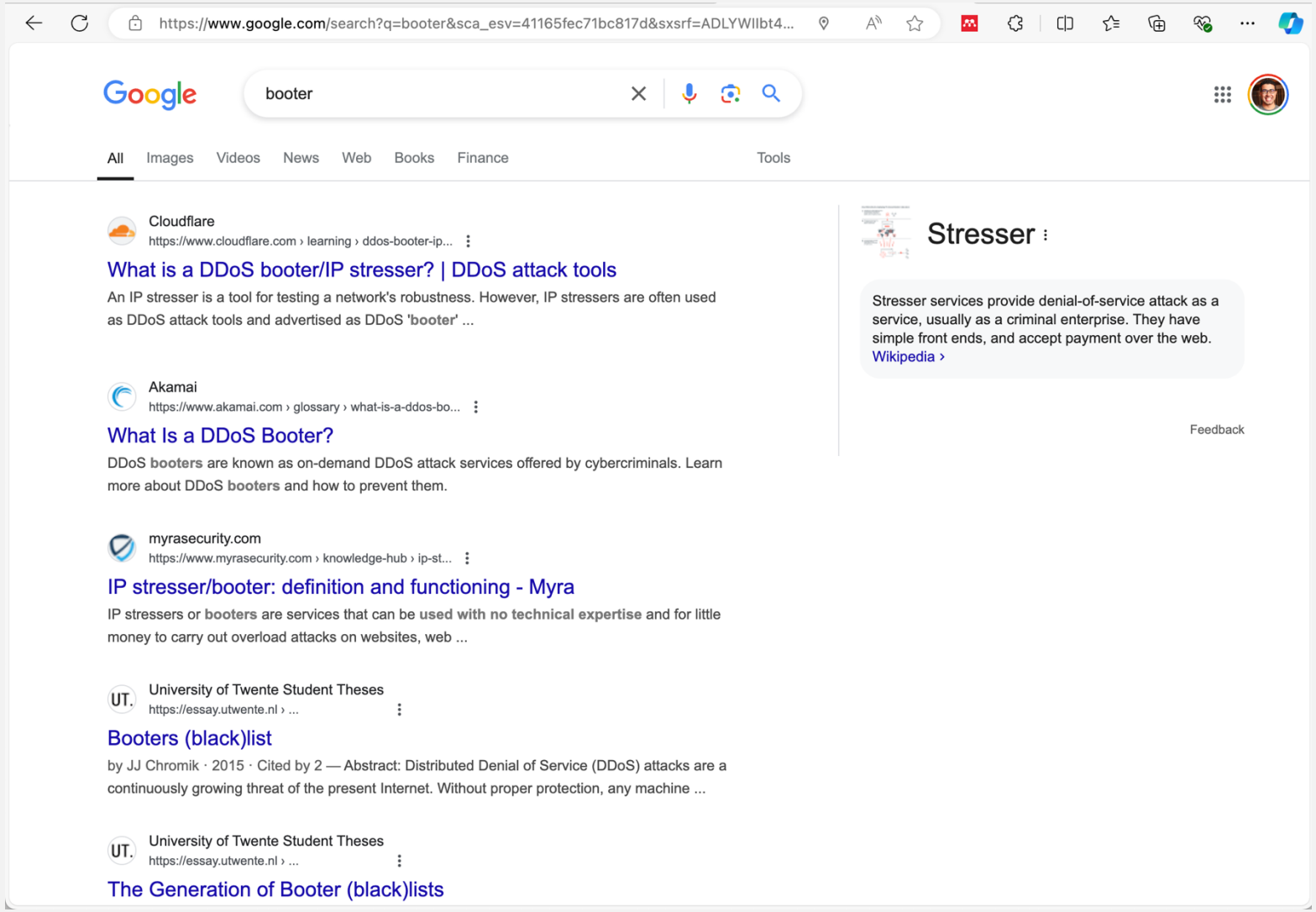
https://digital-strategy.ec.europa.eu/en/news/concordia-ddos-clearing-house-designated-high-potential-innovation



Is there a database with DDoS fingerprints?

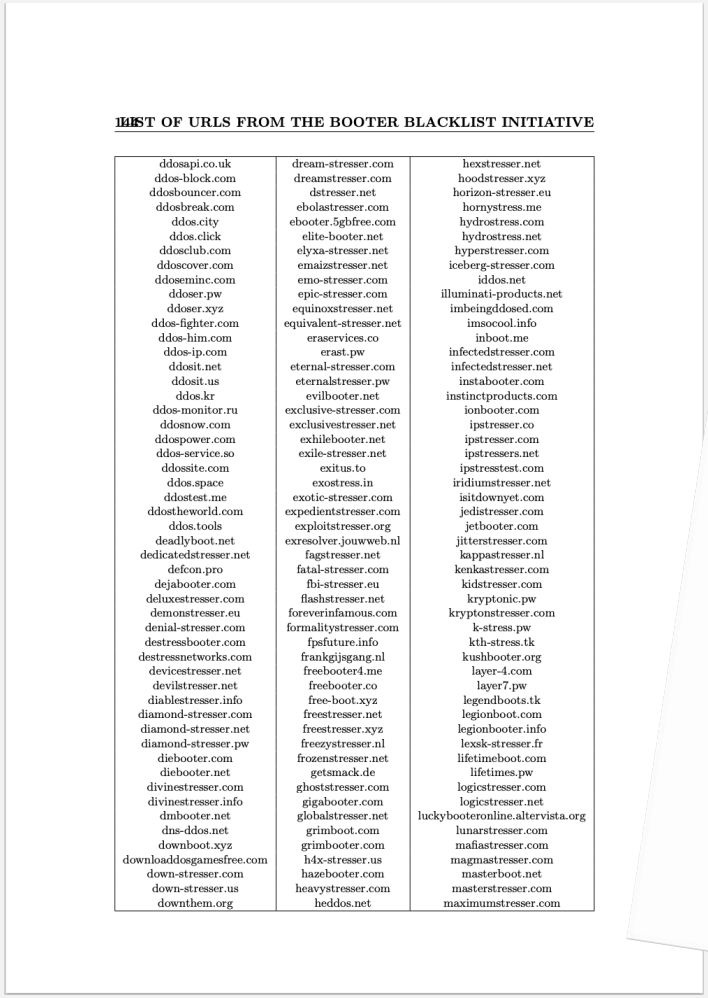
--

Give me an example of a DDoS fingerprint.



NO single Booter in the first page!

450 Booters!



LIST OF URLS FROM THE BOOTER BLACKLIST INITIATIVE

ddosapi.co.uk	dream-stresser.com	hexstresser.net
ddos-block.com	dreamstresser.com	hoodstresser.xyz
ddosbouncer.com	dstresser.net	horizon-stresser.eu
ddosbreak.com	ebolastresser.com	hornystress.me
ddos.city	ebooter.5gbfree.com	hydrostress.com
ddos.click	elite-booter.net	hydrostress.net
ddosclub.com	elyxa-stresser.net	hyperstresser.com
ddoscover.com	emaizstresser.net	iceberg-stresser.com
ddoseminc.com	emo-stresser.com	iddos.net
ddoser.pw	epic-stresser.com	illuminati-products.net
ddoser.xyz	equinoxstresser.net	imbeingddosed.com
ddos-fighter.com	equivalent-stresser.net	imsocool.info
ddos-him.com	eraservices.co	inboot.me
ddos-ip.com	erast.pw	infectedstresser.com
ddosit.net	eternal-stresser.com	infectedstresser.net
ddosit.us	eternalstresser.pw	instabooter.com
ddos.kr	evilbooter.net	instinctproducts.com
ddos-monitor.ru	exclusive-stresser.com	ionbooter.com
ddosnow.com	exclusivestresser.net	ipstresser.co
ddospower.com	exhilebooter.net	ipstresser.com
ddos-service.so	exile-stresser.net	ipstressers.net
ddossite.com	exitus.to	ipstresstest.com
ddos.space	exostress.in	iridiumstresser.net
ddostest.me	exotic-stresser.com	isitdownyet.com
ddostheworld.com	expedientstresser.com	jedistresser.com
ddos.tools	exploitstresser.org	jetbooter.com
deadlyboot.net	exresolver.jouwweb.nl	jitterstresser.com
dedicatedstresser.net	fagstresser.net	kappastresser.nl
defcon.pro	fatal-stresser.com	kenkastresser.com
dejabooter.com	fbi-stresser.eu	kidstresser.com
deluxestresser.com	flashstresser.net	kryptonic.pw
demonstresser.eu	foreverinfamous.com	kryptonstresser.com
denial-stresser.com	formalitystresser.com	k-stress.pw
destressbooter.com	fpsfuture.info	kth-stress.tk
destressnetworks.com	frankgijsgang.nl	kushbooter.org
devicestresser.net	freebooter4.me	layer-4.com
devilstresser.net	freebooter.co	layer7.pw
diablestresser.info	free-boot.xyz	legendboots.tk
diamond-stresser.com	freestresser.net	legionboot.com
diamond-stresser.net	freestresser.xyz	legionbooter.info
diamond-stresser.pw	freezystresser.nl	lexsk-stresser.fr
diebooter.com	frozenstresser.net	lifetimeboot.com
diebooter.net	getsmack.de	lifetimes.pw
divinestresser.com	ghoststresser.com	logicstresser.com
divinestresser.info	gigabooter.com	logicstresser.net
dmbooter.net	globalstresser.net	luckybooteronline.altervista.org
dns-ddos.net	grimboot.com	lunarstresser.com
downboot.xyz	grimbooter.com	mafiastresser.com
downloaddosgamesfree.com	h4x-stresser.us	magmastresser.com
down-stresser.com	hazebooter.com	masterboot.net
down-stresser.us	heavystresser.com	masterstresser.com
downthem.org	heddos.net	maximumstresser.com

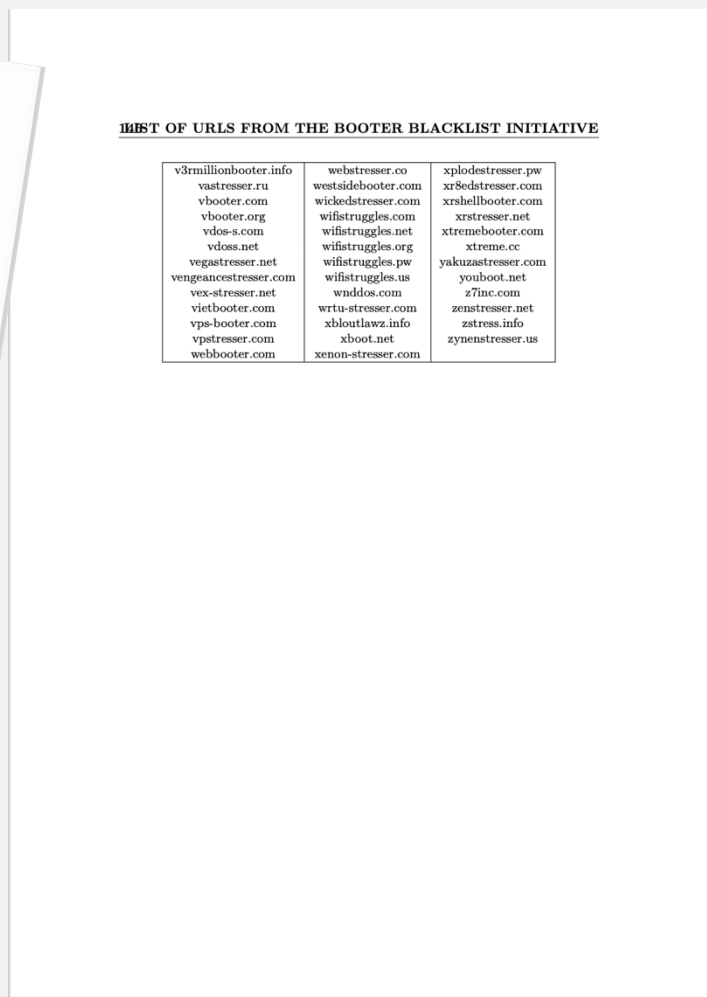
APPENDIX B

List of URLs From the Booter Blacklist Initiative

In this appendix we present the list of URLs retrieved from `http://booterblacklist.com` on 16-July-2017.

Table B.1: List of booter URLs retrived from booterblacklist.com.

1606-stresser.net	beststresser.net	carnagestresser.com
9yrbrfyd.esy.es	bezobooter.webs.com	celerystresser.com
absolut-stresser.net	b-h.us	centexbooter.com
acidstresser.net	bigbangbooter.com	chargen.cf
agonyproducts.com	boganbooter.org	cmdbooter.ml
alien-stresser.com	boot4free.com	cnstresser.com
alphastress.com	booterddos.890m.com	cobra-api.com
ambushproducts.com	booter.eu	connectionstresser.com
ambushstresser.info	booterfull.com	cpubooter.com
america-stresser.us	booter.in	crazyamp.me
animebooter.net	booter.io	critical-boot.com
annonitystresser.com	booter.ninja	critical-stresser.com
anonclan-stresser.net	booter.org	cryptostresser.com
anonmafiastresser.com	booter-sales.hourb.com	crystalstresser.com
anonymousbooter.com	booter.tw	cstress.net
anonymousddos.eu	booter.xyz	cyber-sst.com
anonymous-stresser.com	boot.lu	cyberstresser.org
anonymous-stresser.net	boot.ml	darealbooter.net
anxy-stresser.com	bootr.org	darkbooter.com
apocalypse-solutions.com	bootyou.xyz	darkbooter.fr
apocalypsestresser.webs.com	bullstresser.com	darkbooter.org
asylumstresser.com	bullstresser.ovh	darkmethods.info
aurastresser.com	buybooters.com	darkstresser.info
avanzatostresser.com	buyddos.com	darkstresser.net
avengestresser.com	buz.bugs3.com	darkstresser.nl
baby-booter.com	buzzbooter.fr	darkstresser.org
battle.pw	buzzbooter.info	darkstresser.weebly.com
bemybooter.eu	campingwithkiddos.com	darkunion-booter.net
bestresser.com		databooter.com



LIST OF URLS FROM THE BOOTER BLACKLIST INITIATIVE

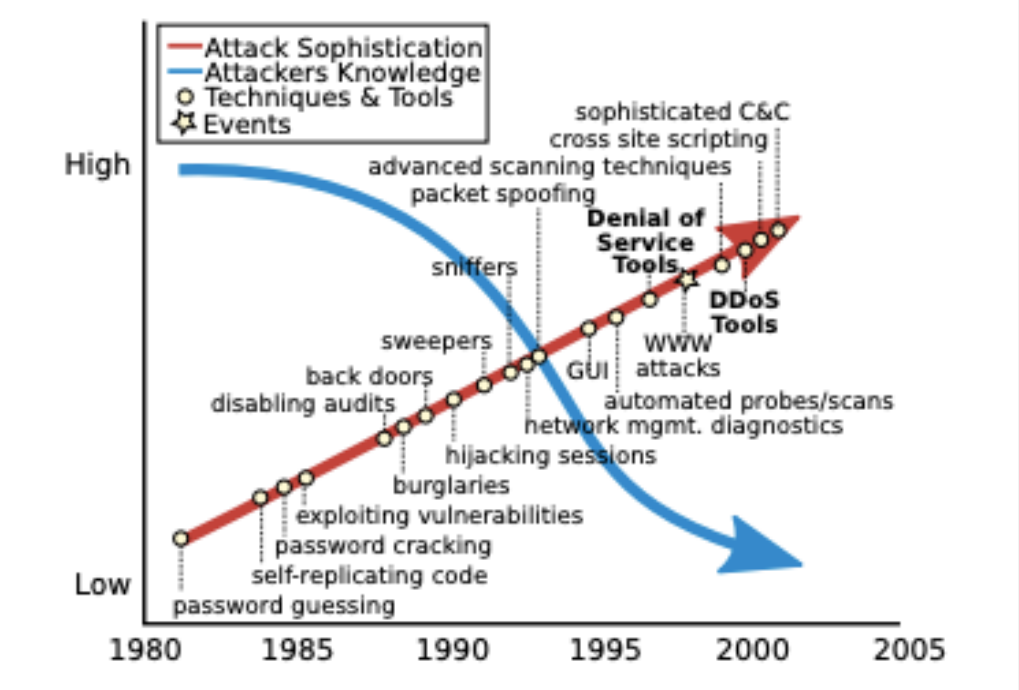
v3rmillionbooter.info	webstresser.co	xplodestresser.pw
vastresser.ru	westsidebooter.com	xr8edstresser.com
vbooter.com	wickedstresser.com	xrshellbooter.com
vbooter.org	wifistruggles.com	xrstresser.net
vdos-s.com	wifistruggles.net	xtremebooter.com
vdoss.net	wifistruggles.org	xtreme.cc
vegastresser.net	wifistruggles.pw	yakuzastresser.com
vengeancestresser.com	wifistruggles.us	youboot.net
vex-stresser.net	wnddos.com	z7inc.com
vietbooter.com	wrtu-stresser.com	zenstresser.net
vps-booter.com	xbloutlawz.info	zstress.info
vpstresser.com	xboot.net	zynenstresser.us
webbooter.com	xenon-stresser.com	

ALL DOWN!

https://bit.ly/jjsantanna_thesis

Final Reflection

2024
2023
2022
2021
2020
2019
2018
2017
2016
2015
2014
2013



"Two decades of Internet but seems that nothing has changed except the scale."

—Bruce Schneider,
In: Data and Goliath—the Hidden Battles to Collect Your Data and Control Your World, 2015

https://bit.ly/jjsantanna_thesis

NORTHWAVE
CYBER SECURITY

Revisiting a +++ Decade of DDoS Attacks

and telling the anti-ddos-coalitie history from my 5 turning points.