Assessing the Aftermath

Evaluating the effects of a global DDoS-for-hire service takedown

Dr. Richard Clayton, University of Cambridge

John Kristoff, *Principal Analyst*, NETSCOUT ASERT

December 15, 2022

DDoS-for-hire services: booters/stressers

‘Booters/stressers’ (they often **claim to be** network stress-testing services to appear **legitimate**) are websites offering DDoS attacks for a nominal fee.

- Typical prices would be $20 for unlimited attacks/month
- Attack types offered are UDP reflection/amplification (DNS, NTP, LDAP etc), SYN- and ACK-floods, HTTP & HTTP/S layer-7 attacks, etc.
- *Operating* a booter services is **illegal in most jurisdictions** (people have been jailed in USA, UK, NL, etc.).
- *Using* a booter is also illegal — but **users** who are caught **are often minors**, and prosecuting them generally results in little in the way of real consequences.

Law Enforcement actions against booters/stressers

Oct 2016	Operators of lizardstresser.su (and associated botnet) arrested
Apr 2018	webstresser.org (biggest booter in the world) taken down by UK/NL
Dec 2018	FBI seize 15 domain names (taking 8 booters offline) also 3 arrests announced.
Dec 2022	FBI seize 49 domain names (and 54 booters, out of 108, go offline) also 6 arrests announced.

Previously, law enforcement had concentrated on high-profile booters where arrests were believed possible. Dec **2022 action emphasised disruption** in attack services; arrests were also made.

Evidence-based policing

1	stresser.app	23166
2	blackstresser.net	10809
3	brrsecurity.org	6672
4	zerostresser.com	5641
5	nightmarestresser.com	5003
6	dragonstresser.com	4919
7	sunstresser.com	3422
8	defconpro.net	3118
9	xxxxxxxxxxxx.xxx	2886
10	stresser.top	2680
11	yyyyyyyyyyy.yyy	2616
12	stresser.gg	2455
13	kraysec.com	2238
14	quantum-stresser.net	2207
15	mcstorm.io	1843

About 70% of booters publish attack volume numbers. Table shows the most **active booters on Mon 12 Dec** (two days before FBI action) with the average attacks per day for the previous week. Their domains were (almost) all seized.

#9 was not taken down because it didn't actually work ! Jurisdictional issues spared #11 (for the moment)

~Half the booters quickly returned with new domain names

1	NEW name for stresser.app	12949	was	23166
2	NEW name for stresser.best	9066	usually	15000+
3	NEW name for cyberstress.us	7659	usually	20000+
4	NEW name for quantum-stresser.net	4470	was	2207
5	NEW name for zerostresser.com	3927	was	5641
6	zzzzzzzzzzzz.zzz	2814	was	1638
7	xxxxxxxxxxx.xxx	1850	was	2886
8	NEW name for nightmarestresser.com	1766	was	5003
9	NEW name for dreams-stresser.io	1694	was	1651
10	vvvvvvvvvvv.vvv	1578	usually	1200
11	wwwwwwww.www	1329	was	1789
12	NEW name for mcstorm.io	1074	was	1843
13	NEW name for stresser.gg	1056	was	2455
14	NEW name for redstresser.cc	1049	usually	1000

Table shows the most **active booters on Mon 26 Dec** (ten days after FBI action) with the average attacks per day for the previous week.

For most booters activity down by 50% (and usually we see more DDoS at Xmas)

Overall NETSCOUT DDoS Attack Observations

Currently averaging ~38,000 DDoS attacks/day, ~13M DDoS attacks/year.

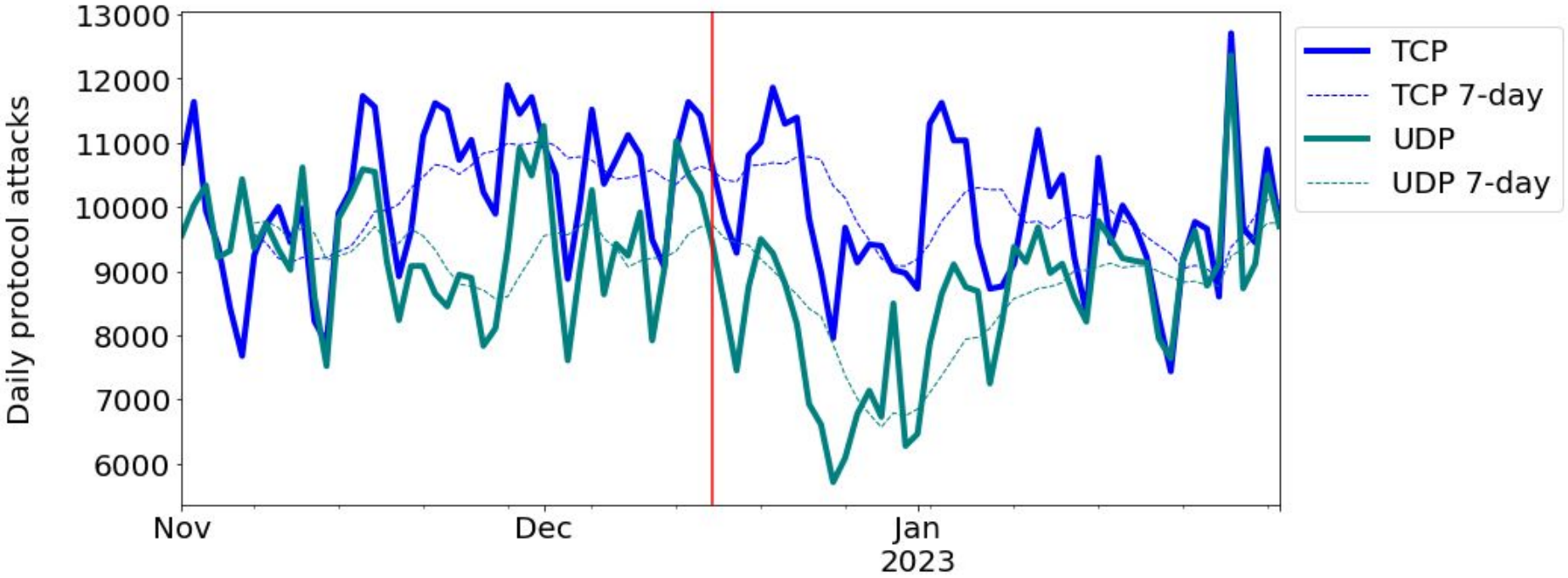
‘Great Rebalancing’ away from total dominance of UDP reflection/amplification vectors (DNS reflection/amplification, ntp reflection/amplification, CLDAP reflection/amplification, et. al.) towards more balance with direct-path vectors such as SYN-floods, ACK-floods, small- and large-packet UDP floods, GRE floods, et. al.

Direct result of a concerted drive within the operational community to encourage the deployment of source-address validation (SAV) — i.e., anti-spoofing — by network operators who haven’t yet done so (reflection/amplification attacks require the ability to spoof).

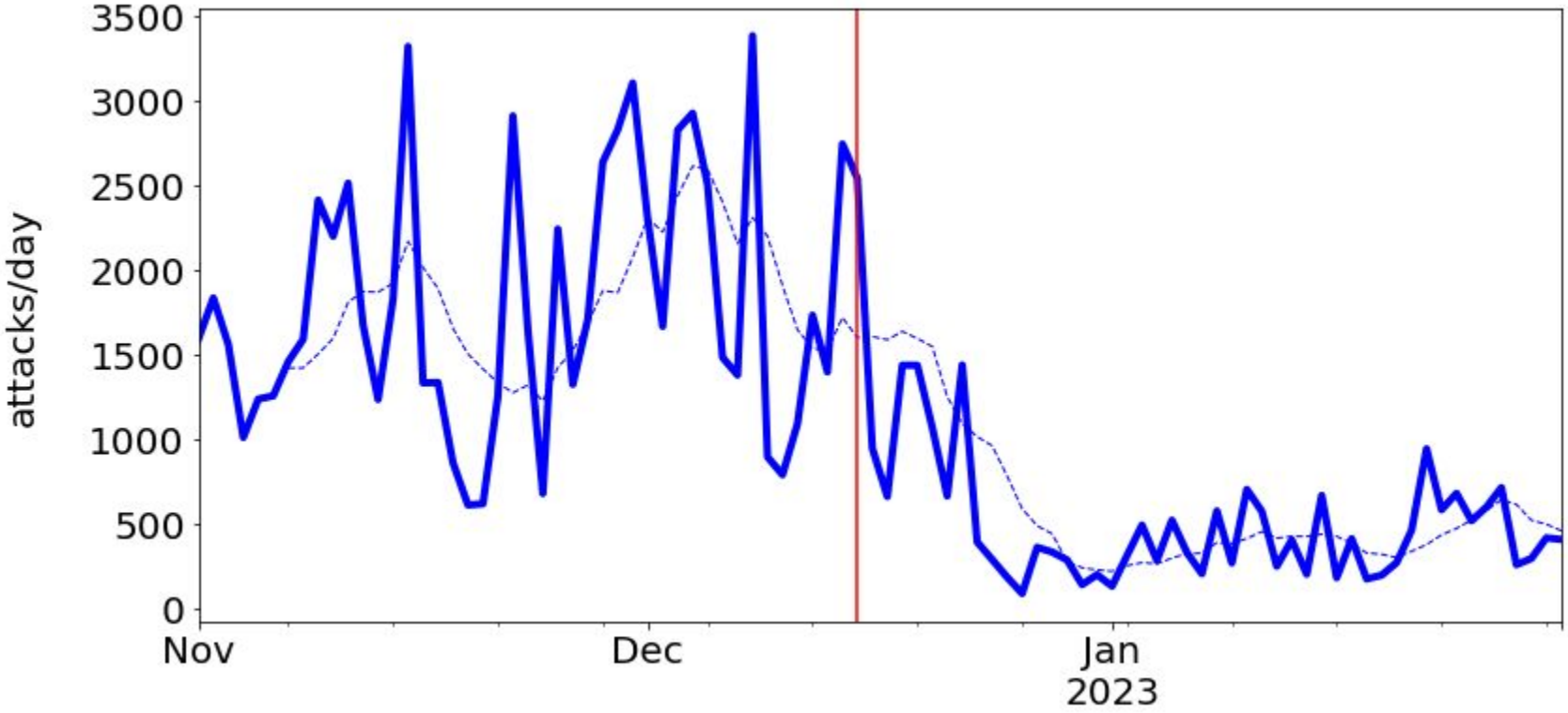
More details on this shift in attack vector prevalence at http://www.netscout.com/threatreport (free access; registration required).

Overall, DDoS attacks are ‘up and to the right’; but there are observable change in attack vectors and methodologies over time.

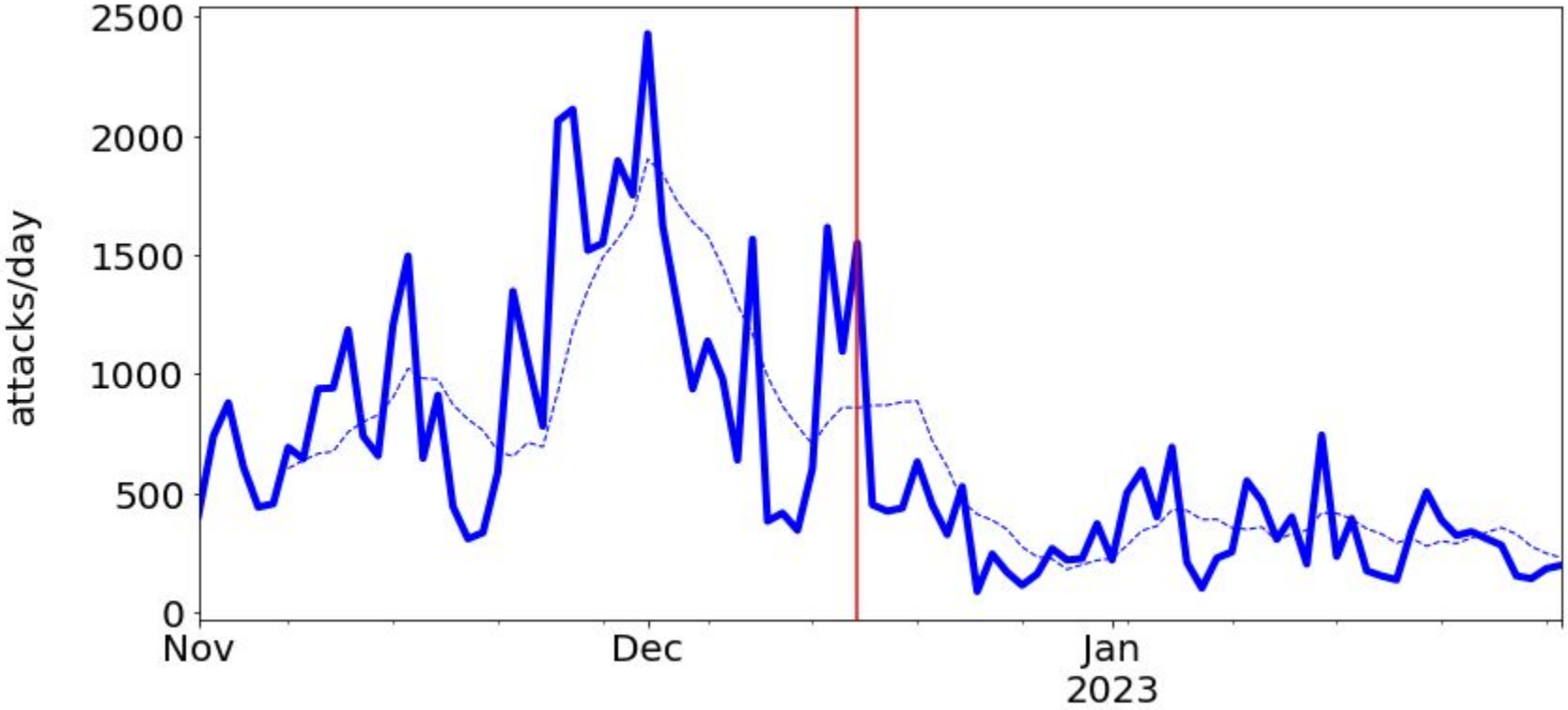
TCP- v. UDP-based DDoS attacks Nov 2022 - Jan 2023



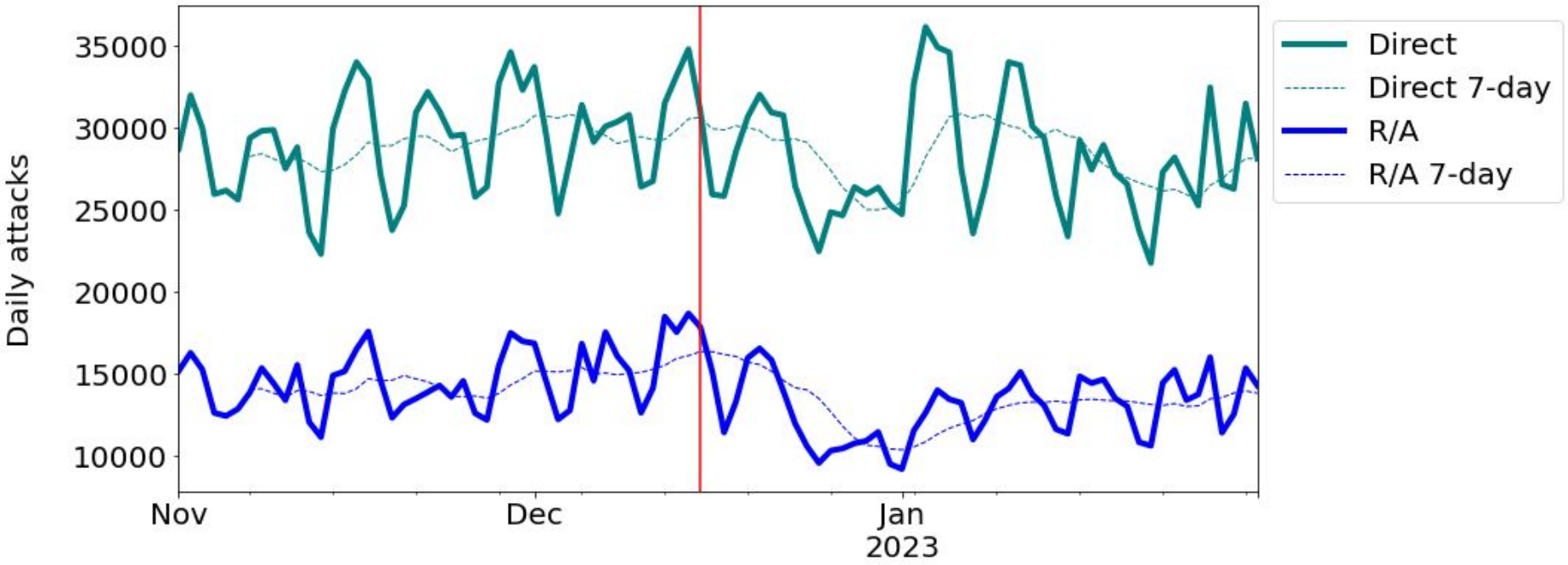
Attacks targeting a well-known US eyeball network



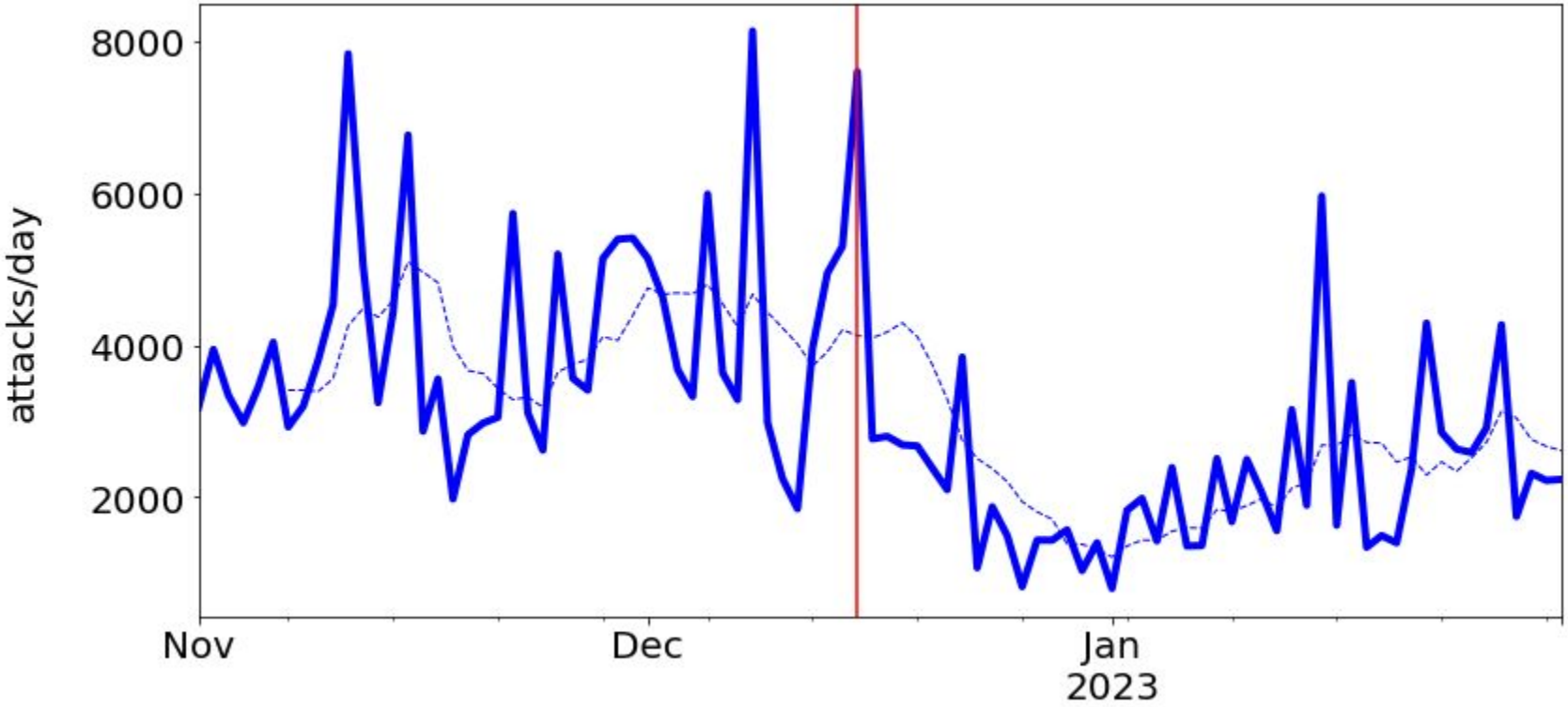
Attacks targeting a well-known EU hosting provider



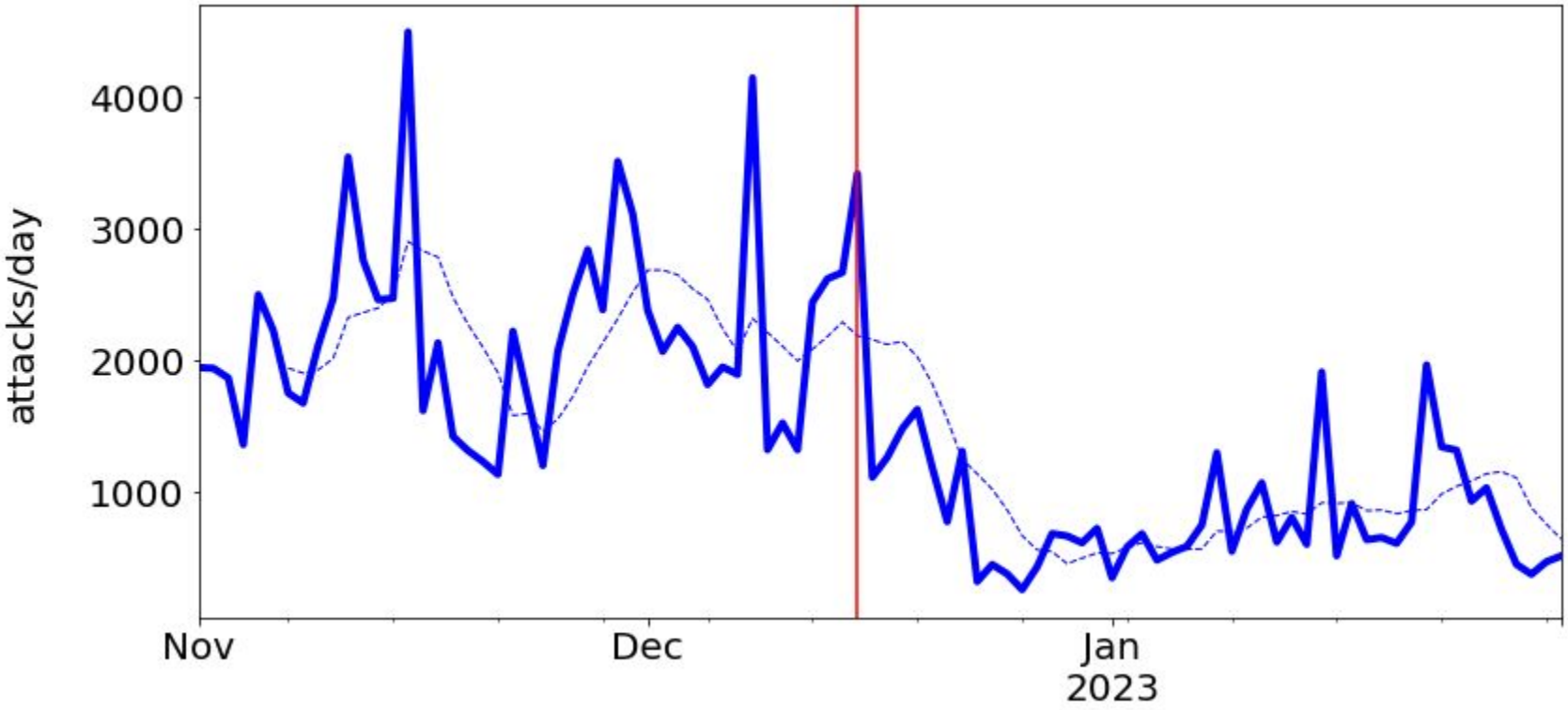
Reflection/amplification attacks vs. direct-path attacks



DNS reflection/amplification attacks



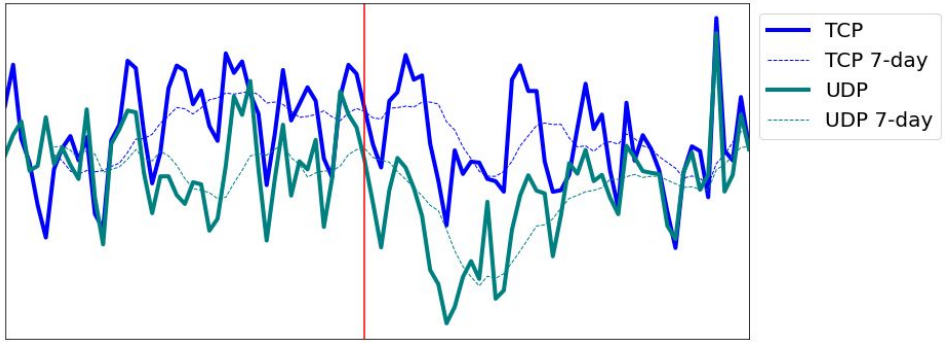
NTP reflection/amplification attacks



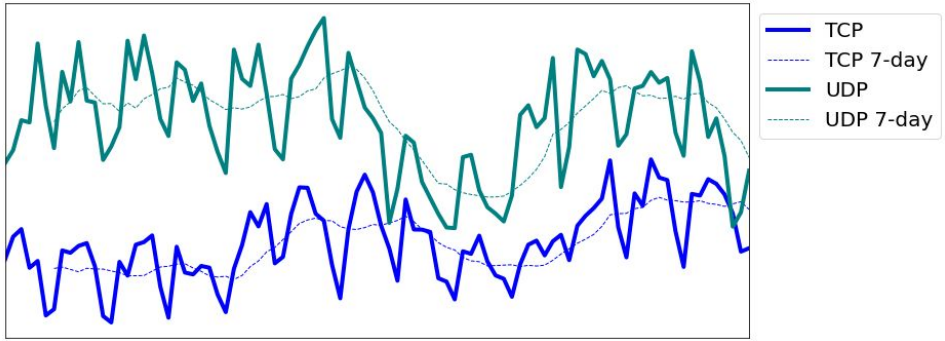
Comparing Year-over-year Change

Year-over-year TCP- v. UDP-based DDoS attacks

2022/2023

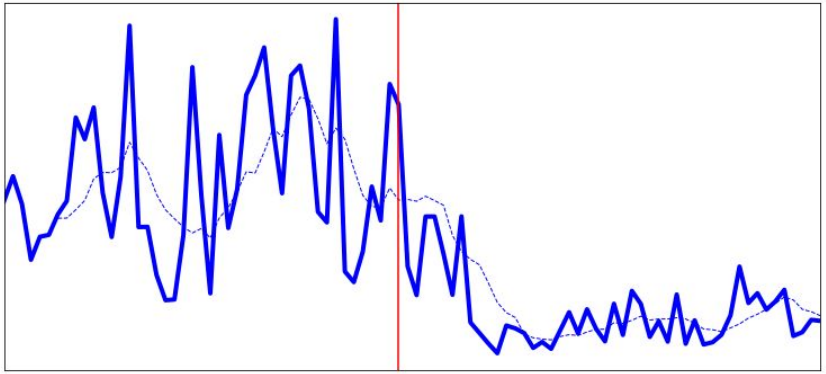


2021/2022

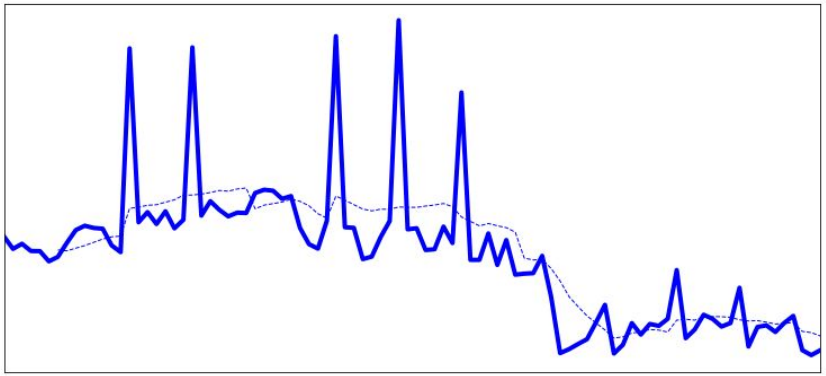


Attacks targeting well-known US eyeball network

2022/2023

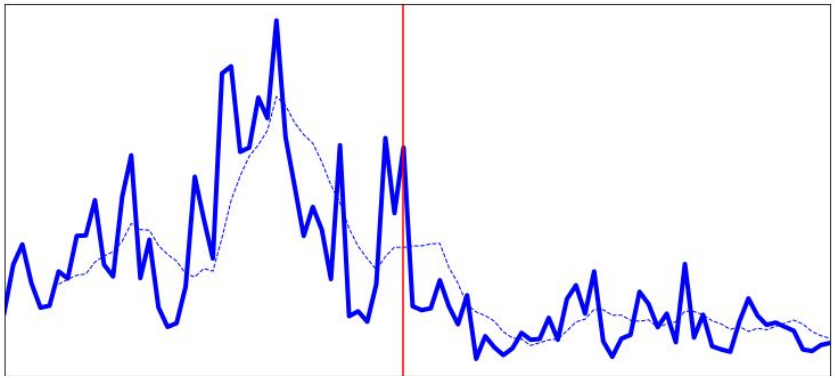


2021/2022

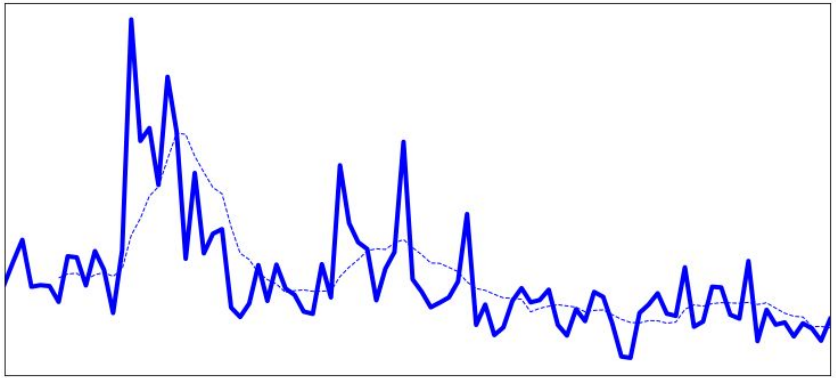


Attacks targeting well-known EU hosting provider

2022/2023

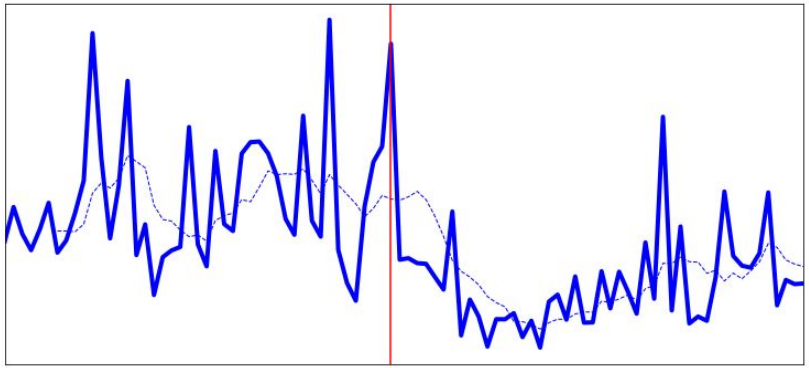


2021/2022

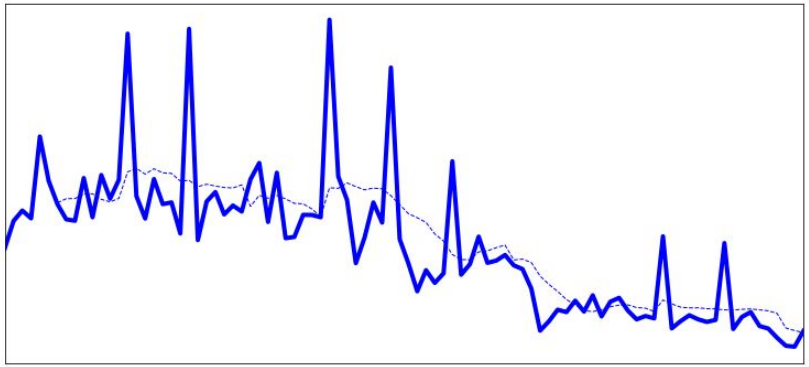


DNS reflection/amplification attacks

2022/2023

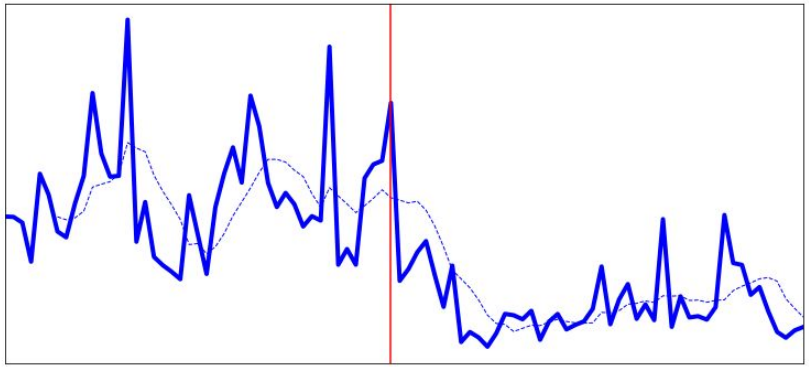


2021/2022

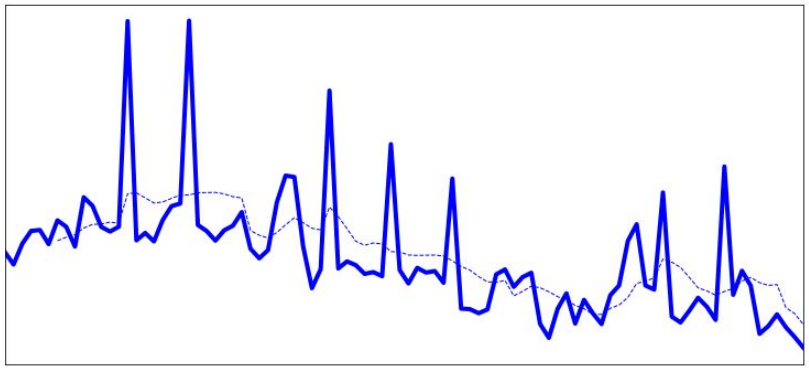


NTP reflection/amplification attacks

2022/2023



2021/2022



Conclusions

***Probable* decrease** in global DDoS attack numbers resulting from the takedown — seasonal variations in attack frequency largely related to school holiday schedules make it difficult to quantify more precisely.

Best evidence is focused and targeted, i.e.,

- Specific networks prone to booter/stresser attacks
- UDP-based reflection/amplification attacks
- Self-reporting by DDoS-for-hire services

Disruption moves the attacker **goal posts**, helpful in the near term, some deterrent value.

Next steps?