DDoS attacks landscape

Marek Majkowski
@majek04

CLOUDFLARE'S GLOBAL ANYCAST NETWORK

Infinite scalability is the future of the Internet

10%
GLOBAL HTTP
INTERNET REQUESTS

10 Million
REQUESTS / SECOND

15 Tbps
NETWORK CAPACITY

140+
DATA CENTERS
GLOBALLY

CLOUDFLARE

Reverse proxy

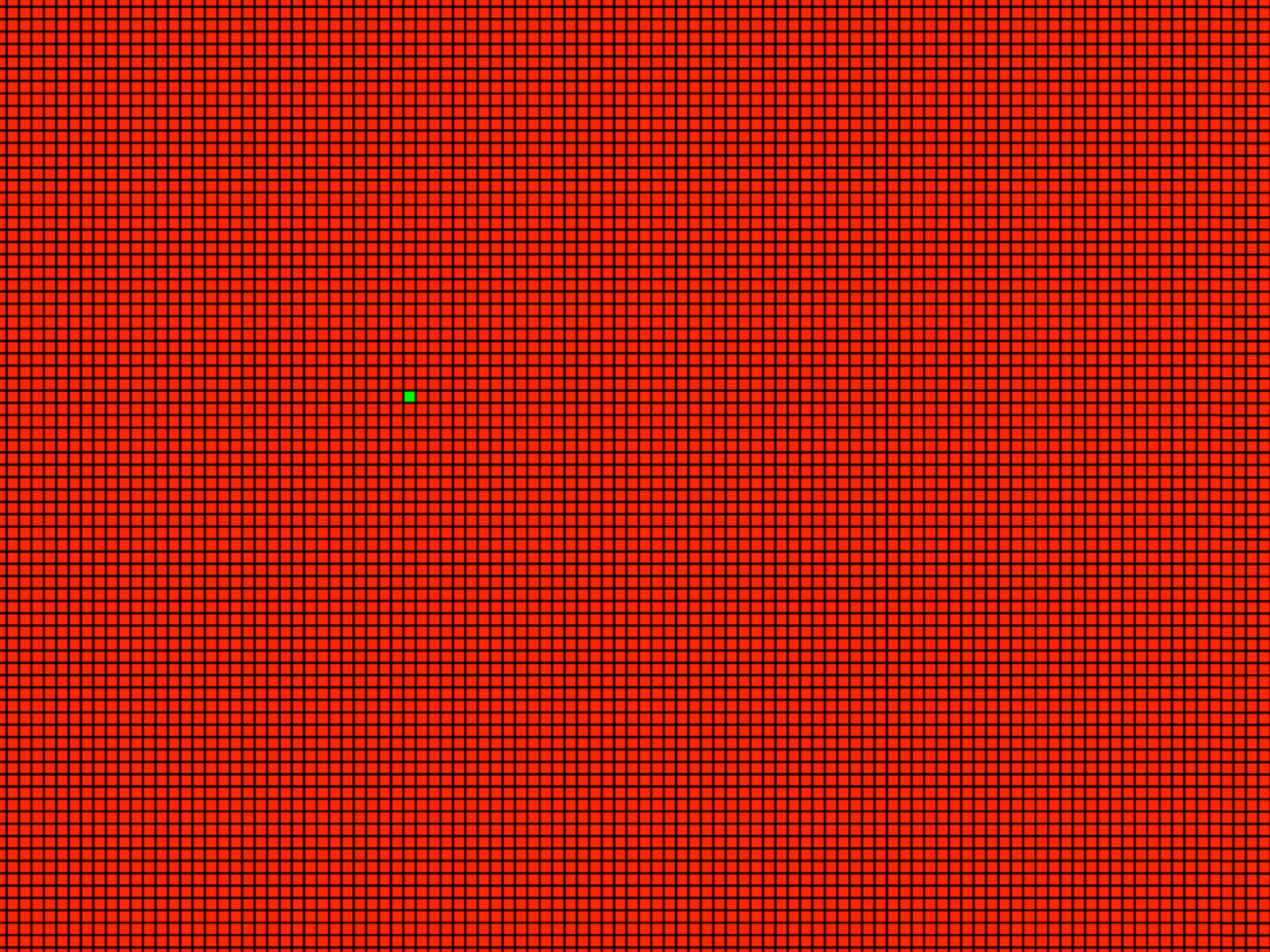
Eyeball **Reverse proxy** **Origin server**

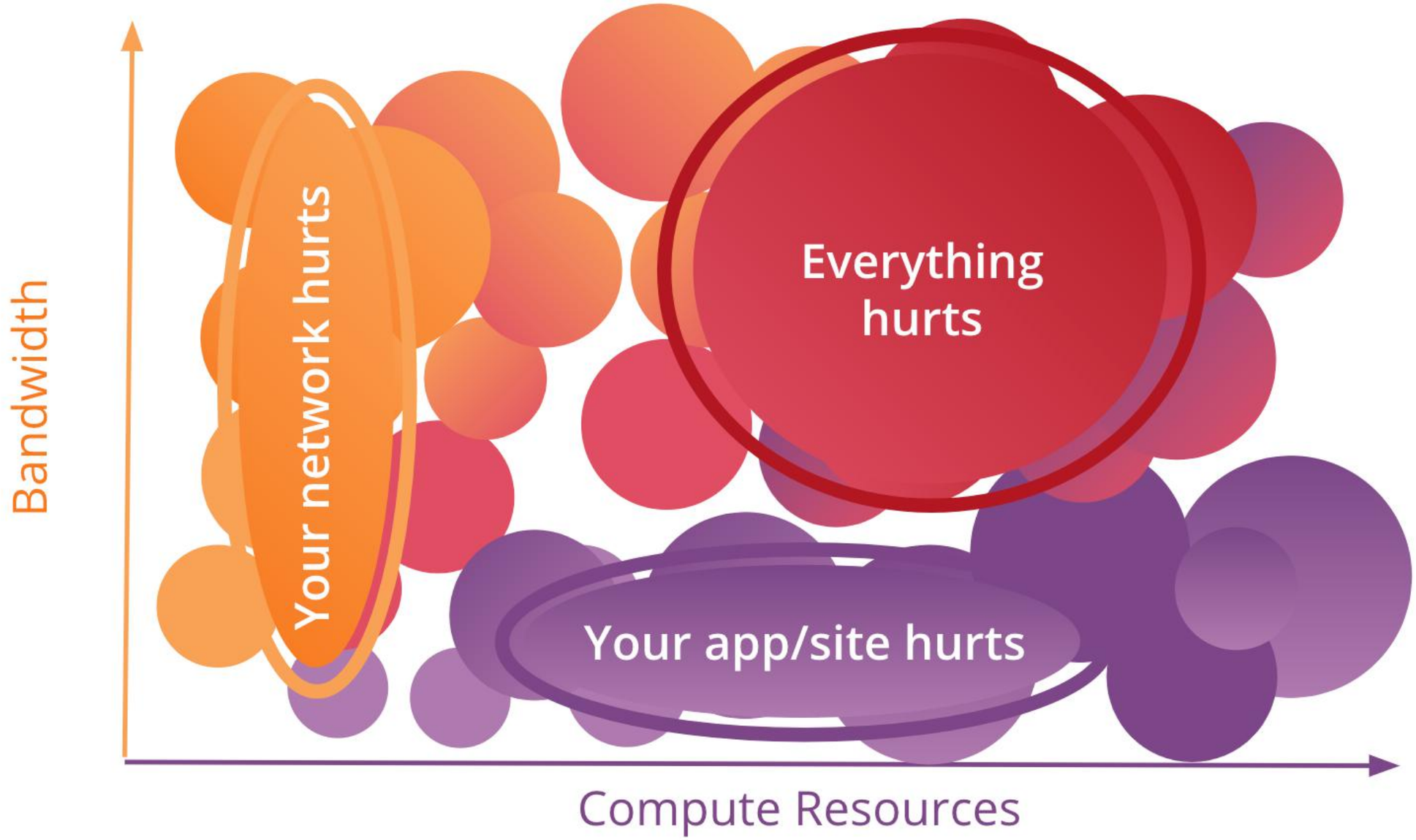
- Optimizations
- Caching
- Security
- DDoS protection

© Getty Images/AFP/N. Kolesnikova

Denial of service

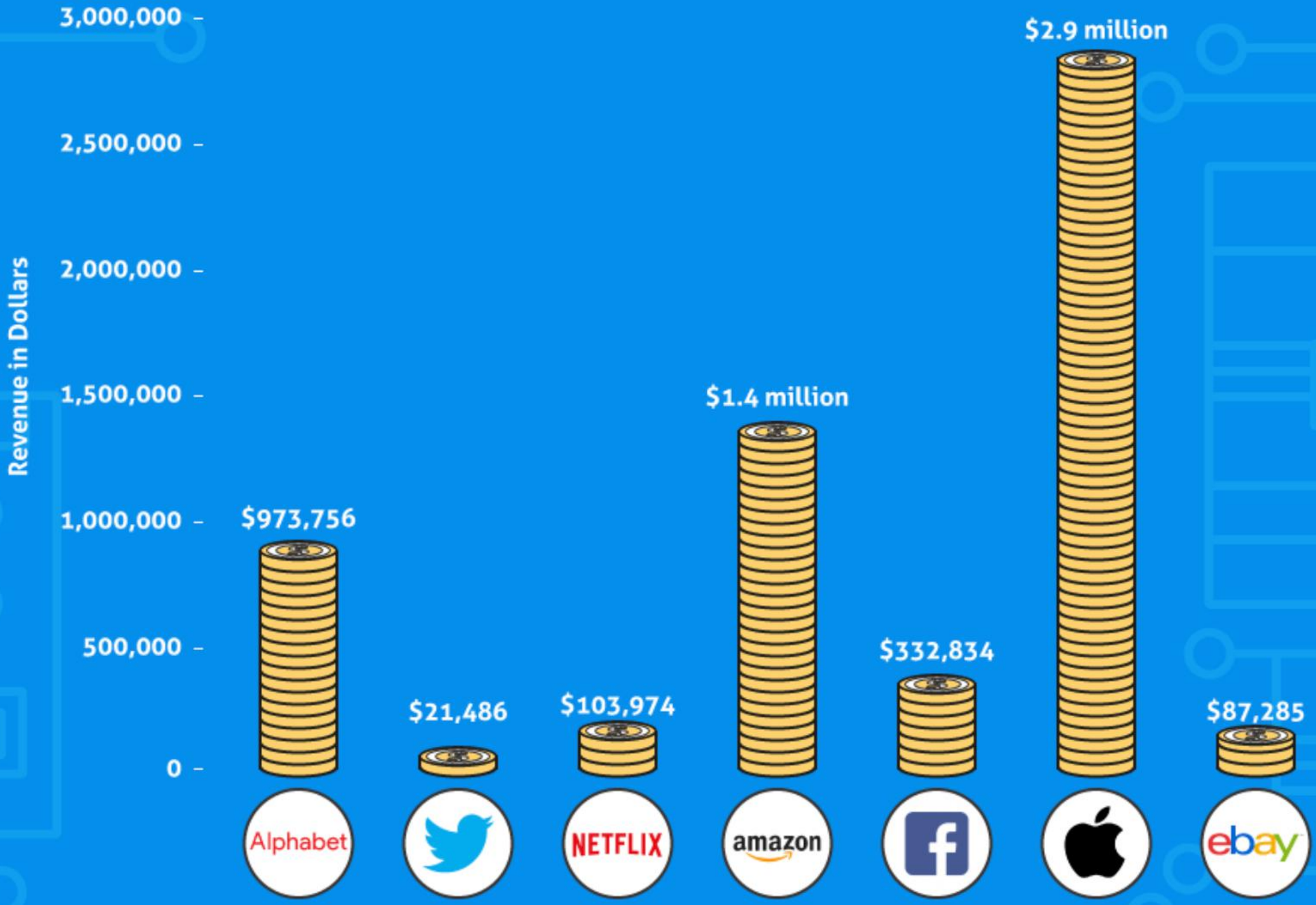
CLOUDFLARE




Bandwidth
Your network hurts
Everything hurts
Your app/site hurts
Compute Resources

Goal?

MONEY LOST DURING A 5-MINUTE OUTAGE



Lloyds bank accounts targeted in huge cybercrime attack

Banking group says none of its 20m
off two-day denial of service attack

The bank says some customers may have had
cyber attack on 11-13 January 2017. Photograph: F

This article is 6 months old

Patrick Collinson

Monday 23 January 2017 12.20 GMT

Lloyds Banking Group suffered 48-

HSBC suffers online banking cyber-attack

Bank admits its internet banking facility was made unavailable following a 'denial of service' attack, but says no transactions were

This is the second time in a month HSBC custom
Frank Augstein/AP

This article is 1 year old

Hilary Osborne

Friday 29 January 2016 11.51 GMT

HSBC customers were locked out of
after the company was targeted by o

Cyber attack hits RBS and NatWest online customers on payday

Banking group says Distributed Denial of Service attack prompted flood of complaints from customers

NatWest bank – victim of cyber attack. Photograph: Jonathan Nicholson/Demotix/Corbis

117 85

This article is 1 year old

Patrick Collinson

Friday 31 July 2015 16.24 BST

9:38
5/4/2013

* DDoS na mBank

Autor: redakcja | Tagi: atak, DDoS, mBank

Dziś od ok. 6.30 serwisy internetowe grupy BRE; mBank i Multibank nie są dostępne. Jak udało nam się nieoficjalnie potwierdzić, powodem jest atak DDoS.

Klientom ww. banków sugerujemy wykonywanie transakcji przez telefon (mLinia). Transakcje kartowe, ponieważ odpowiadają za nie inne systemy informatyczne, powinny działać bez przeszkód.

Niebezpiecznie duży atak DDoS na polskie banki wraz z próbą szantażu

Adam Haertle dodał 9 maja 2016 o 19:38 w kategorii DDoS z tagami: bank • ddos • Kadyrovtsy • Polska

Od weekendu trwają ataki DDoS na największe polskie banki. Tajemniczy sprawcy, podpisujący się pseudonimem *Kadyrovtsy*, nie mają wielkich oczekiwań finansowych, dysponują za to całkiem solidnymi możliwościami ataku.

W ciągu ostatnich kilku dni co najmniej dwa duże polskie banki padły ofiarami ataków DDoS, którym towarzyszyły wiadomości z prośbą o wpłatę kilkudziesięciu bitcoinów na określone rachunki. Klienci banków podobno skutków ataków prawie wcale nie odczuli, lecz atakujący odgrażają się, że to dopiero początek.

Bitfinex
@bitfinex

Bitfinex is under DDoS attack. The DDoS attack started during earlier maintenance and has been ongoing since.

5:03 PM - Nov 26, 2017

445 503 people are talking about this

Bittrex
@BittrexExchange

DDOS attack was detected and being mitigated right now. Sorry for the inconvenience.

8:56 PM - Nov 24, 2017

1,295 2,948 people are talking about this

GDAX under possible DDoS attack - service outage

Incident Report for Coinbase

February 2010 Australian cyberattacks

From Wikipedia, the free encyclopedia

The **February 2010 Australian cyberattacks** were a series of denial-of-service attacks conducted by the Anonymous online community against the Australian government in response to proposed web censorship regulations. **Operation Titstorm** was the name given to the cyber attacks by the perpetrators. They resulted in lapses of access to government websites on 10 and 11 February 2010. This was accompanied by emails, faxes, and phone calls harassing government offices. The actual size of the attack and number of perpetrators involved is unknown but it was estimated that the number of systems involved ranged from the hundreds to the thousands. The amount of traffic caused disruption on multiple government websites.

Australian Telecommunications Minister Stephen Conroy proposed the regulations that would mainly filter sites with pornographic content. Various groups advocating uncensored access to the Internet, along with companies like Google and Yahoo!, object to the proposed filter. A spokesperson for Conroy said that the actions were not a legitimate form of protest and called it irresponsible. The attacks also drew criticism from other filter protest groups. The initial stage was followed by small in-person protests on 20 February that were called "**Project Freeweb**".

Operation Titstorm

A flyer for Operation Titstorm

Date	February 2010
Location	Internet and Australia
Methods	spam, street protests, denial-of-service attacks
Parties to the civil conflict	
Anonymous	Government of Australia

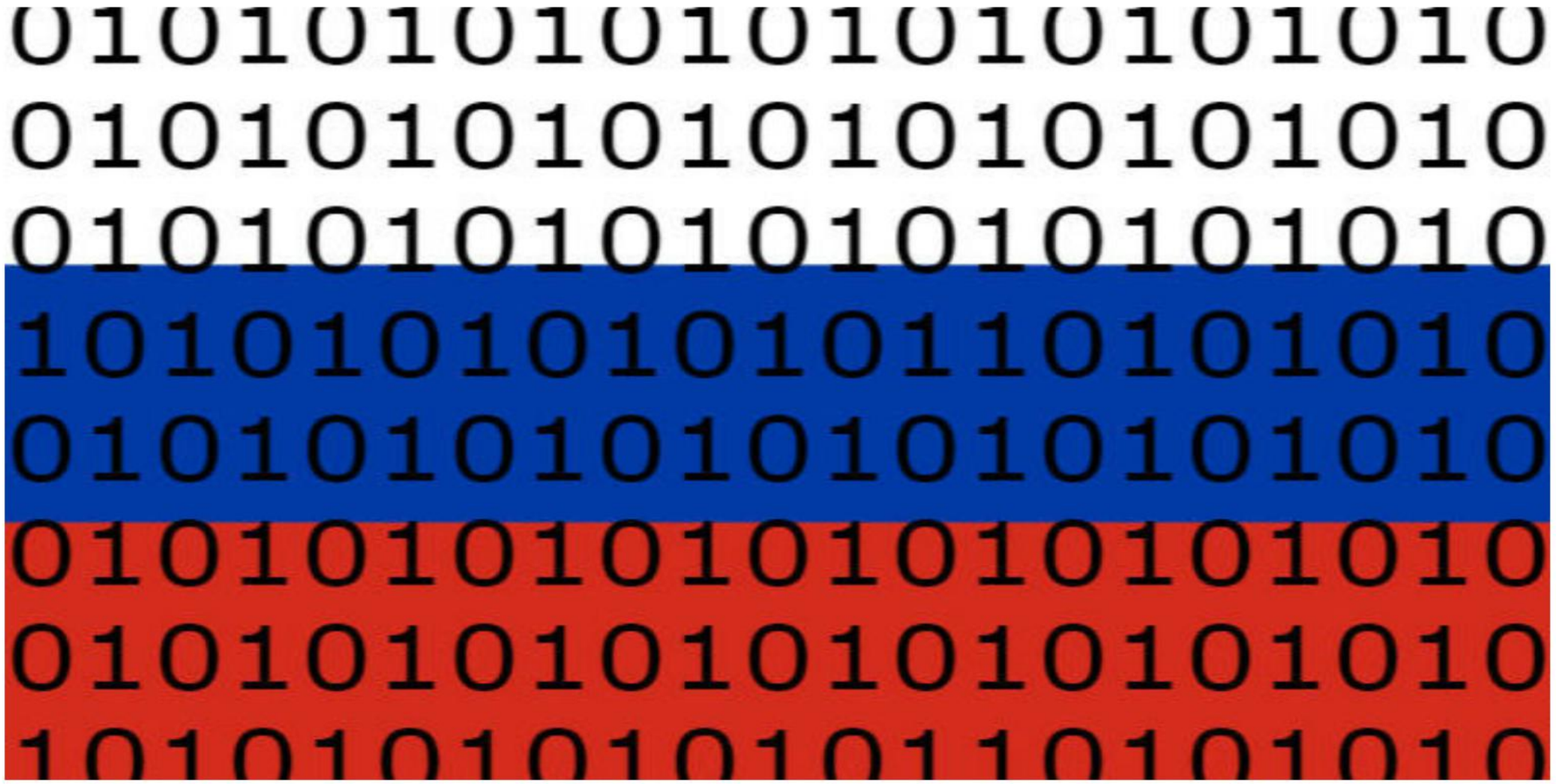
A cyberattack knocked a Tennessee county's election website offline during voting

Taylor Hatmaker @tayhatmaker / May 4, 2018

Comment

Russian Election Suffered DDoS Attack, Putin Still Wins in Landslide

Posted on March 19, 2018 by Ben Canner in Endpoint Security News



Unavailability

Break the internet

Affected services [edit]

Services affected by the attack included:

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

CLOUDFLARE

Internet was built as a trusted environment

https://www.fbi.gov/wanted/cyber

Cyber's Most Wanted

Select the images of suspects to display more information.

Search for

Search for...

Filter by

Year

Filter

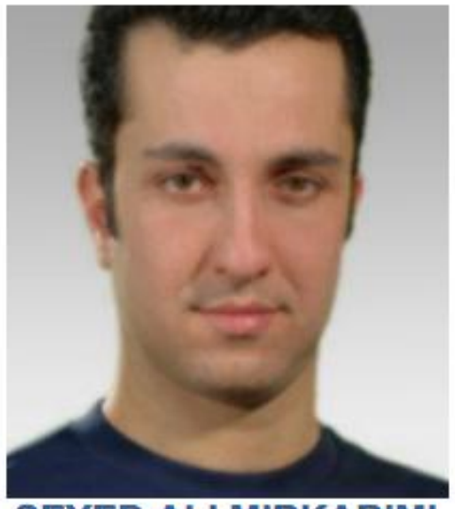
Sort by: Newest

Results: 41 Items

IRANIAN MABNA HACKERS

GHOLAMREZA RAFATNEJAD

EHSAN MOHAMMADI



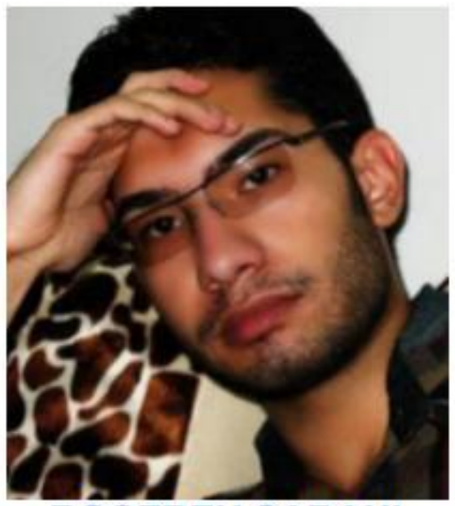
SEYED ALI MIRKARIMI

ABDOLLAH KARIMA

MOSTAFA SADEGHI

SAJJAD TAHMASEBI

MOHAMMED REZA SABAHI



ROOZBEH SABAHI

ABUZAR GOHARI MOQADAM

Five case studies

Amplification is largest

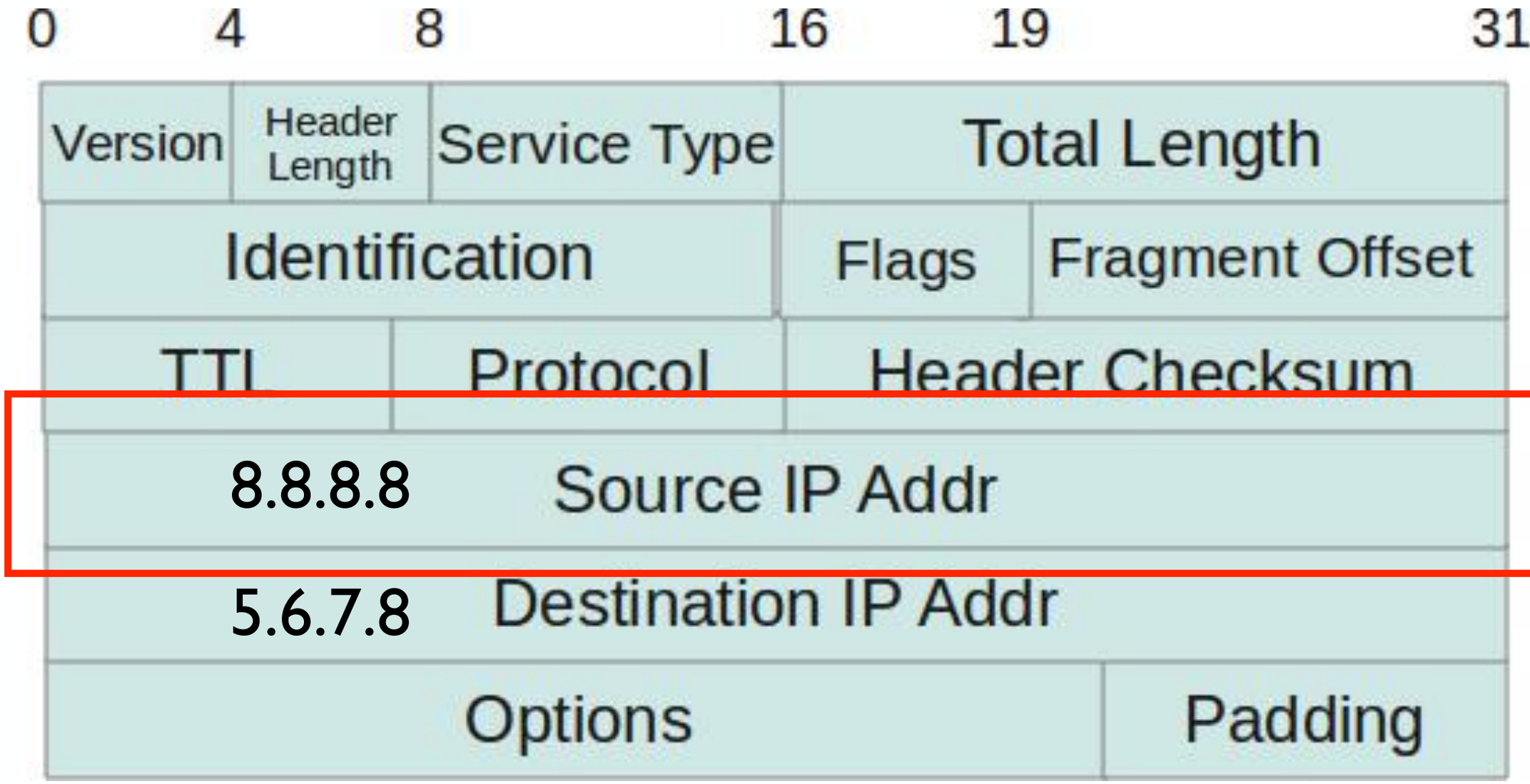
Two things needed:

- IP spoofing
- vulnerable protocol

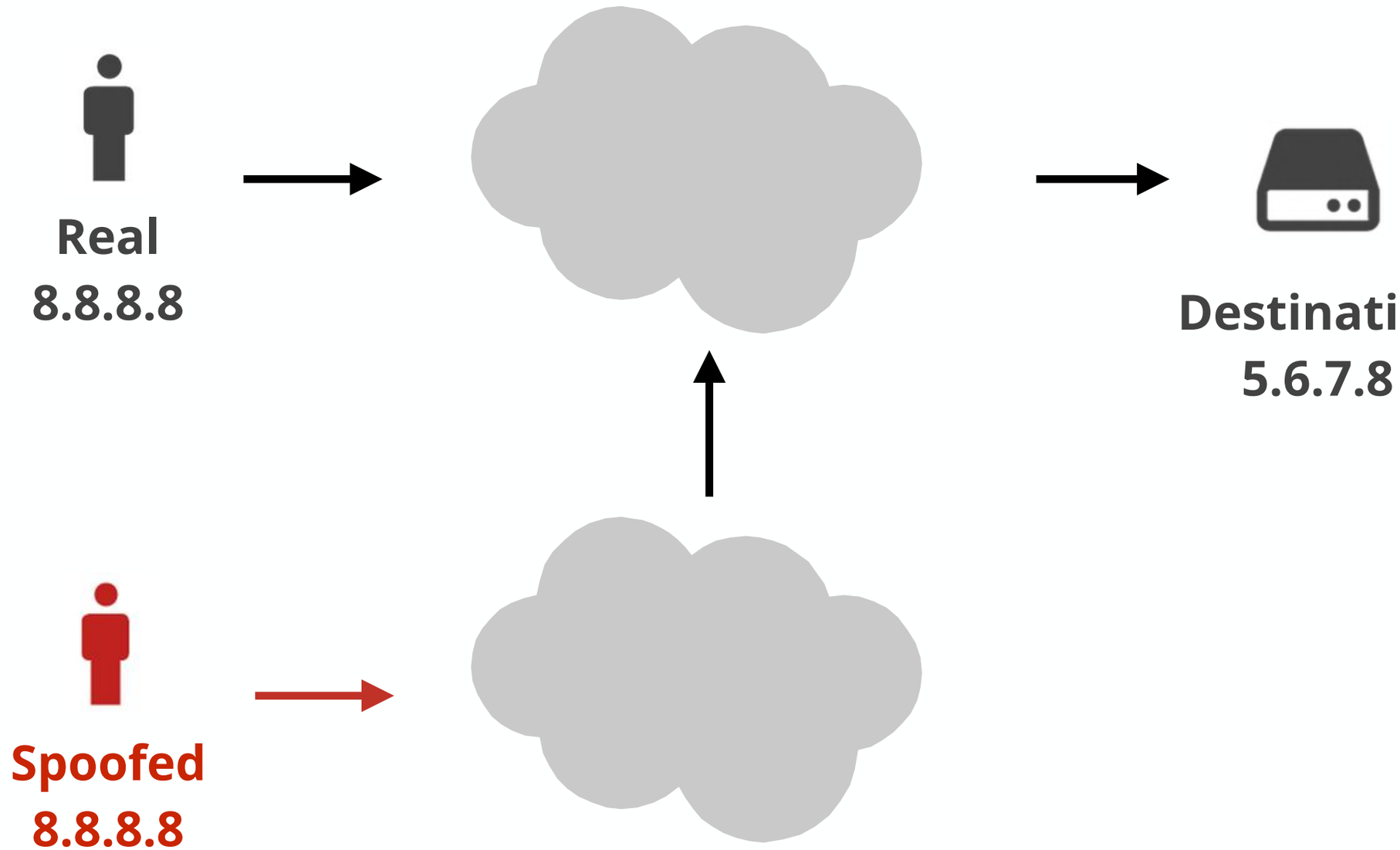
CLOUDFLARE

IP Spoofing

IP Spoofing


0
4
8
16
19
31
Version
Header Length
Service Type
Total Length
Identification
Flags
Fragment Offset
TTL
Protocol
Header Checksum
8.8.8.8
Source IP Addr
5.6.7.8
Destination IP Addr
Options
Padding

Enables impersonation



Spoofed?

(source: DaPuglet)

SPOOFING ENABLED OFFSHORE SERVERS

Dedicated EU Servers Now Available. No Scanning. Buy yours today!

PRICING

OFFSHORE 1GBPS UNMETERED SERVERS

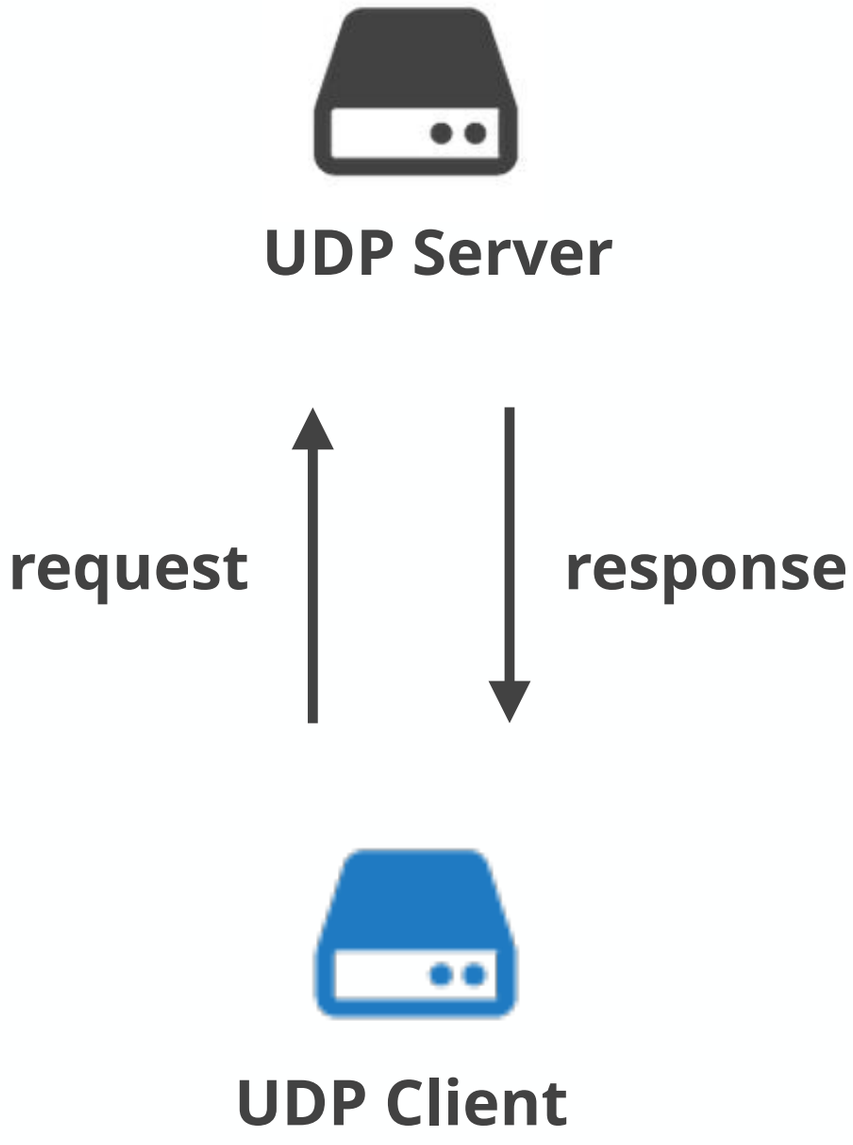
OUR NEWEST PARTNERSHIP IN OUR EXPANDING SERVER RANGE; WE PRESENT OUR NEWEST OFFSHORE LOCATION.

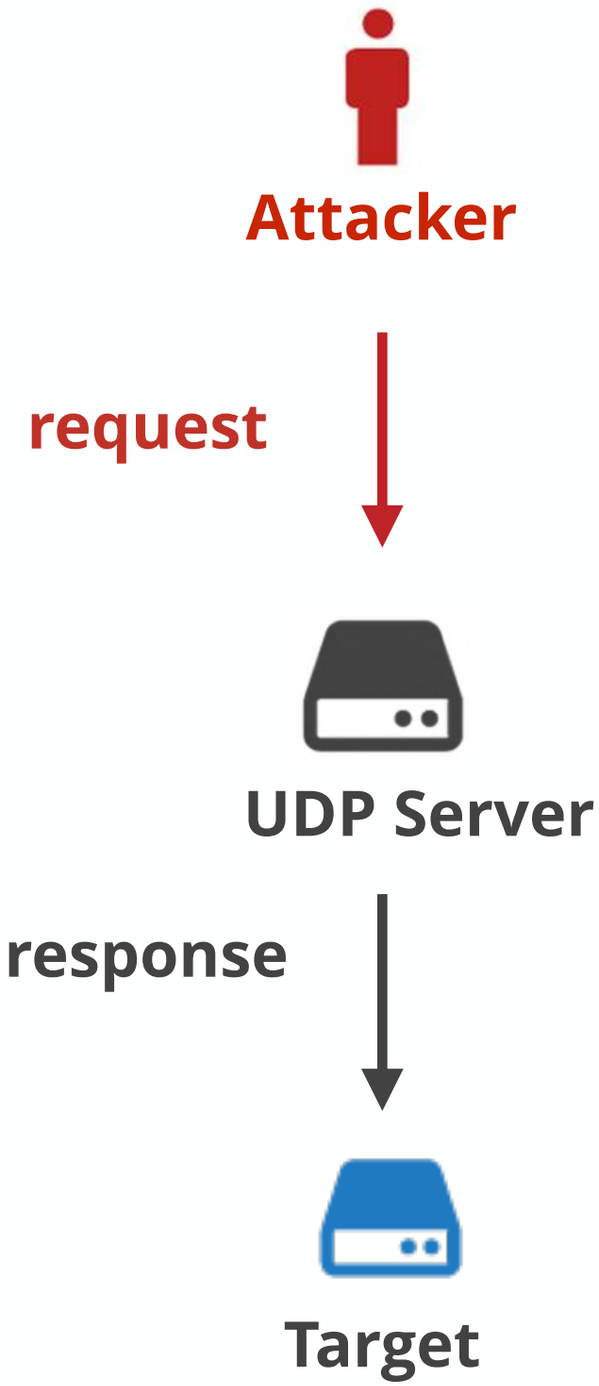
SPOOFER DATA 1 _____SPOOFER DATA 2

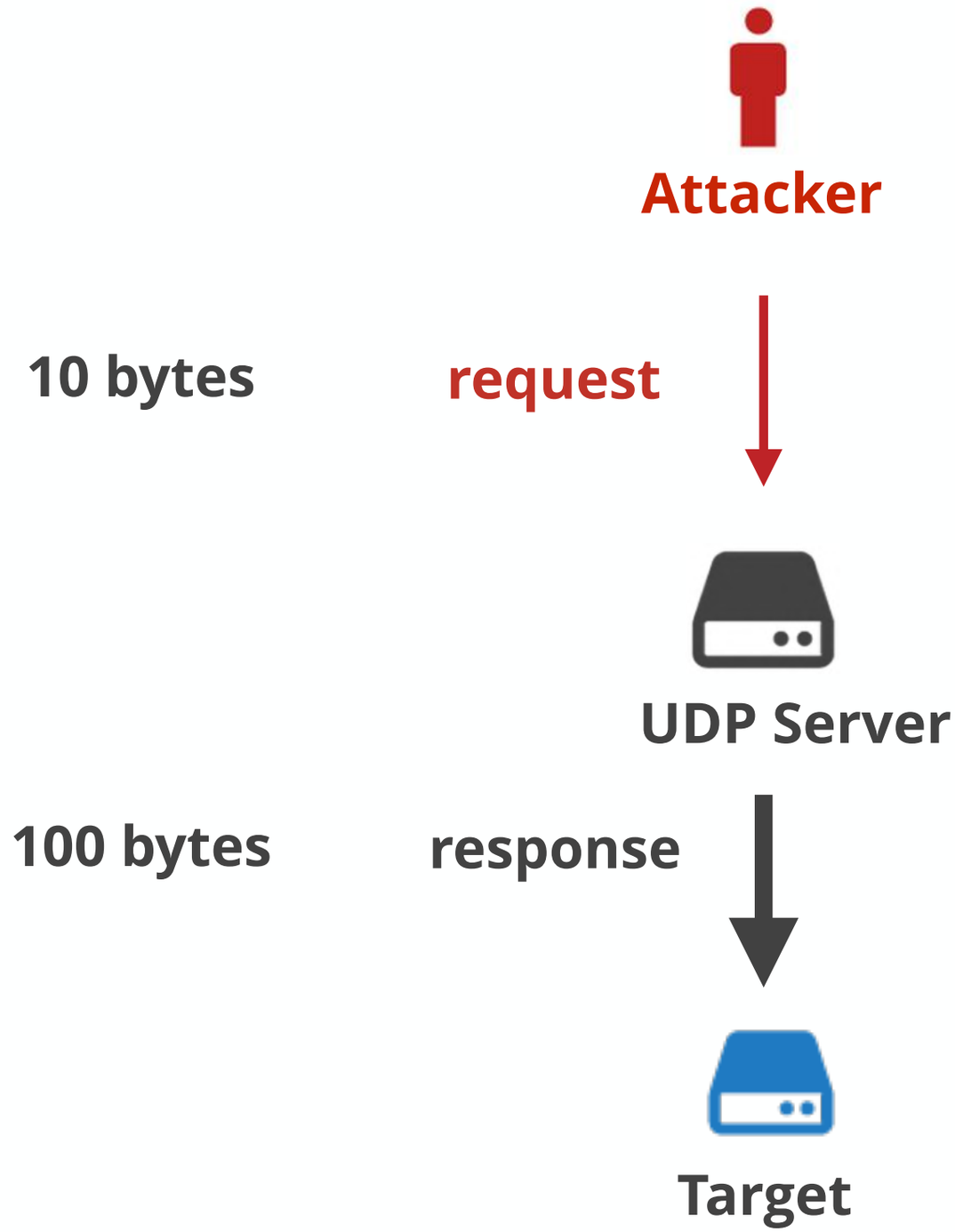
THESE SERVERS ARE STRICTLY BTC PURCHASABLE. ONCE YOU PAY, YOUR SERVER WILL GO INTO PROCESSING. IF THE DC DECIDES TO EVER STOP SPOOFING AT ANY POINT, NO REFUND IS POSSIBLE. THIS DATA CENTER ONLY ACCEPTS BTC FOR THIS REASON AND REQUIRES UPFRONT FINANCES FOR HARDWARE RENTAL. AMPNODE'S TERMS OF SERVICE CLEARLY ADDRESS NO REFUNDS IF SPOOFING IS SUSPENDED ON ANY PARTICULAR NETWORK. THANK YOU

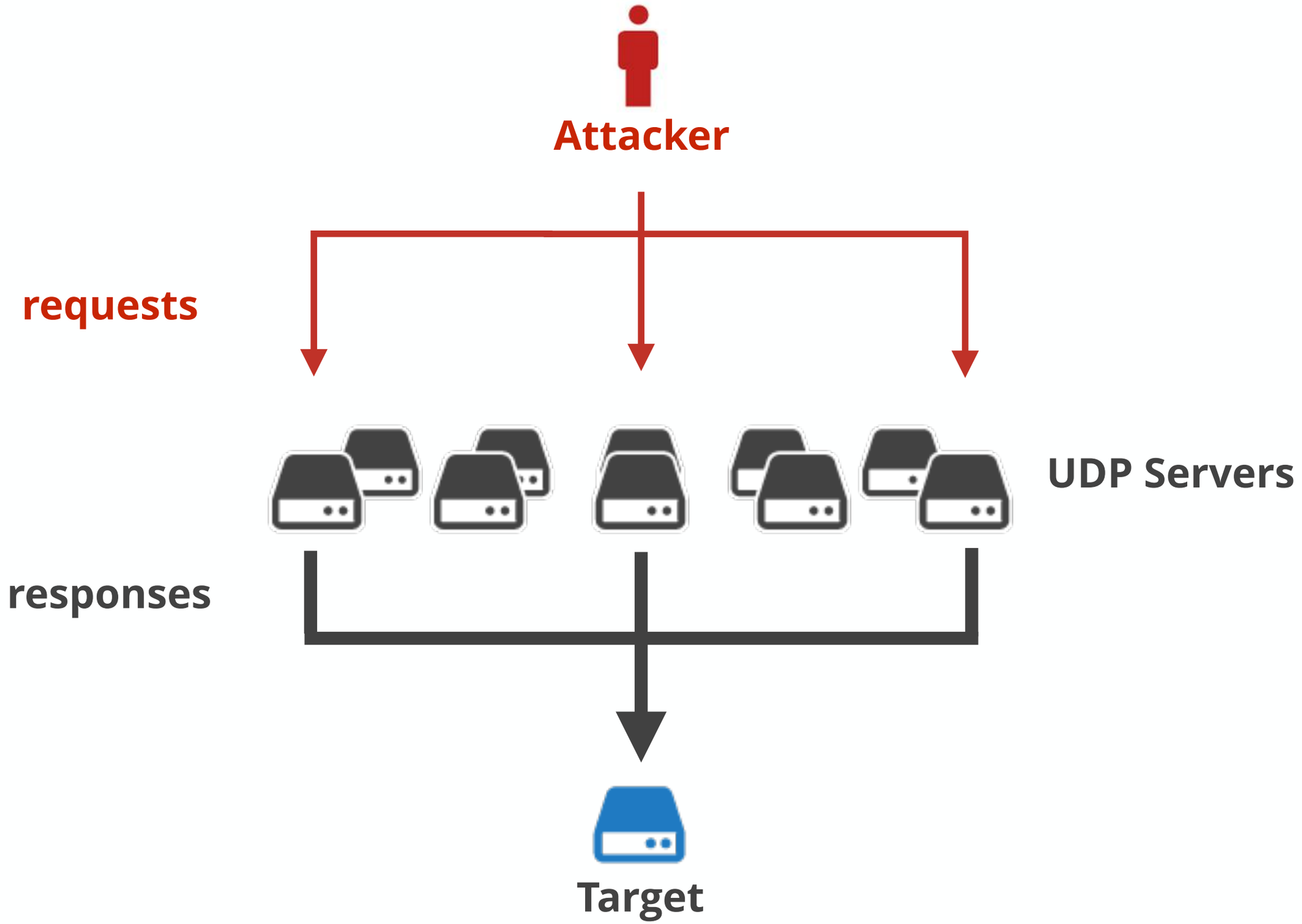
Find a protocol to abuse

- DNS
- NTP
- SSDP


UDP Server
request
response
UDP Client


Attacker
request
UDP Server
response
Target


Attacker
10 bytes
request
UDP Server
100 bytes
response
Target


Attacker
requests
UDP Servers
responses
Target

Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS

28 Jun 2017 by Marek Majkowski.

G+ Share 340 Like 371 Tweet

Last month we shared statistics on some popular ref
SSDP attack size was ~12 Gbps and largest SSDP refl

- 30 Mpps (millions of packets per second)
- 80 Gbps (billions of bits per second)
- using 940k reflector IPs

This changed a couple of days ago when we noticed
It's worth deeper investigation since it crossed the sy

The packets per second chart during the attack looke

The bandwidth usage:

Reflections on reflection (attacks)

24 May 2017 by Marek Majkowski.

G+ Share 116 Like 48 Tweet

Recently Akamai published an article about CLDAP reflection attacks. This got us thinking. We saw attacks from Connectionless LDAP servers back in November 2016 but totally ignored them because our systems were automatically dropping the attack traffic without any impact.

Memcached (1.7 Tbps)

February 2018

Memcached does UDP?

```
1166  UDP protocol
1167  ------------
1168
1169  For very large installations where the number of clients is high enough
1170  that the number of TCP connections causes scaling difficulties, there is
1171  also a UDP-based interface. The UDP interface does not provide guaranteed
1172  delivery, so should only be used for operations that aren't required to
1173  succeed; typically it is used for "get" requests where a missing or
1174  incomplete response can simply be treated as a cache miss.
1175
```

Enable UDP by default, clean up server socket code (Brian Aker)

Browse files

git-svn-id: http://code.sixapart.com/svn/memcached/trunk/server@726 b0b603af-a30f-0410-a34e-baf09ae79d0b

master flash-with-wbuf-stack ··· 1.2.5

BrianAker committed on Feb 27, 2008 — 1 parent a6b35b4 commit 2439472aae5960b9b2f8ef93f3f62047a28700f2

Showing **1 changed file** with **74 additions** and **126 deletions.** Unified Split

200 memcached.c View

```
@@ -64,7 +64,7 @@ std *
64  64    */
65  65   static void drive_machine(conn *c);
66  66   static int new_socket(struct addrinfo *ai);
67      -static int *server_socket(const int port, const bool is_udp, int *count);
    67  +static int server_socket(const int port, const bool is_udp);
```

janreges replied on Feb 27

Hi,

this commit was starter of current biggest UDP amplification attack with impact bigger than DNS amplification attack.

CLOUDFLARE

memcached

Search for product:"Memcached" returned 87,811 results on 26-02-2018

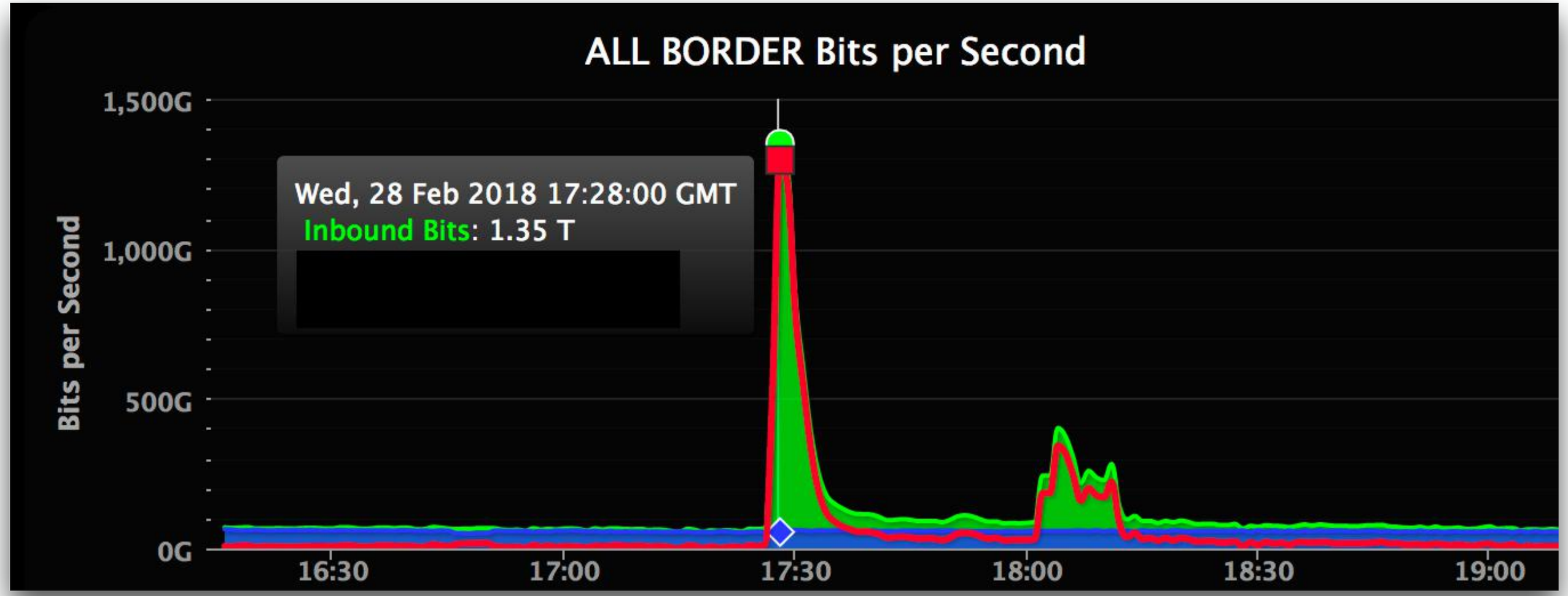
Top Countries

1. United States	25,034
2. China	19,647
3. France	4,038
4. Japan	3,586
5. Hong Kong	3,396
6. Netherlands	2,613
7. Russian Federation	2,306
8. India	2,299
9. Canada	2,181
10. Germany	2,102

Memcrashed - Major amplification attacks from UDP port 11211

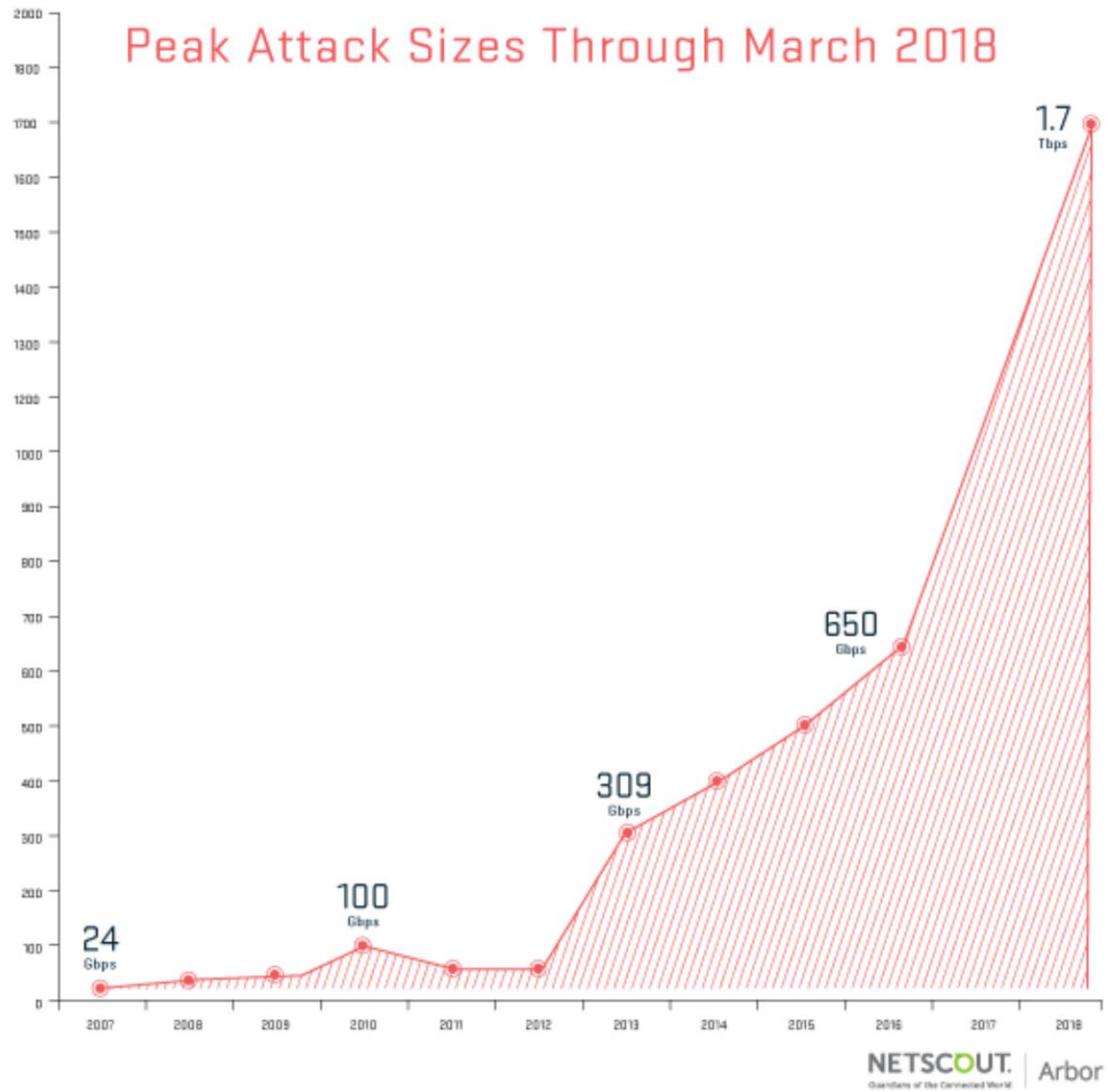
27 Feb 2018 by Marek Majkowski.

Over last couple of days we've seen a big increase in an obscure amplification attack vector - using the memcached protocol, coming from UDP port 11211.


ALL BORDER Bits per Second
Wed, 28 Feb 2018 17:28:00 GMT
Inbound Bits: 1.35 T
Bits per Second
1,500G
1,000G
500G
0G
16:30
17:00
17:30
18:00
18:30
19:00

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

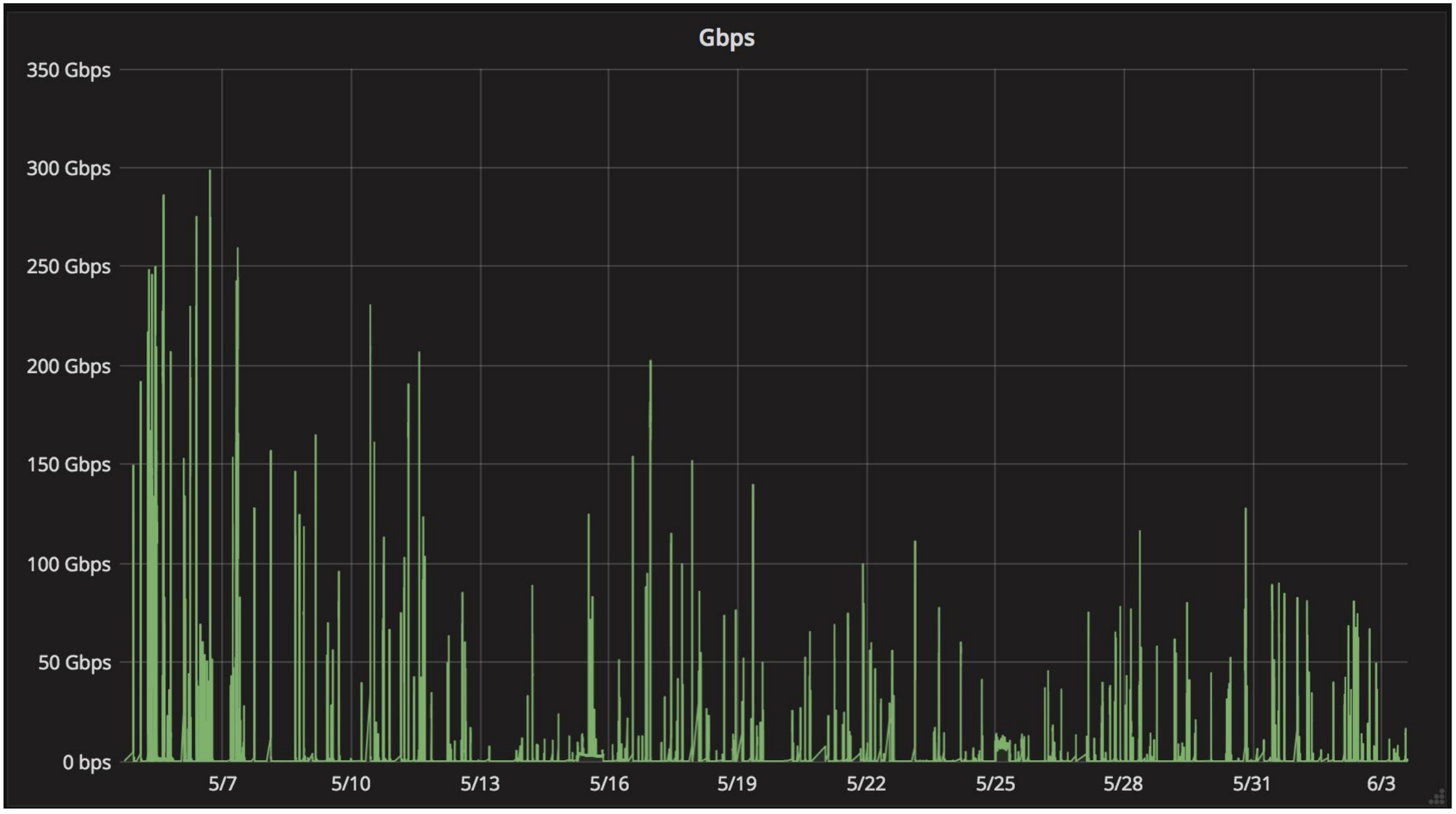
Carlos Morales on March 5, 2018.



Cleanup was well underway

- Digital Ocean
- Linode
- OVH
- Amazon

Memcached today



CLOUDFLARE

CALL OF DUTY®

INFINITE WARFARE

Direct SYN flood

Attacker
500 Gbps

Direct SYN flood

Target
Server

The Daily DDoS: Ten Days of Massive Attacks

02 Dec 2016 by John Graham-Cumming.

G+ Share 143 Like 344 Tweet

Back in March my colleague Marek wrote about a Winte
Attacks where we were seeing 400Gbps attacks occurri
speculated that attackers were busy with something els

This winter we've seen a new pattern, and attackers are
seem to be working regular hours.

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

G+ Share 283 Like 21 Tweet

Over the last month, we've been watching some of the largest distributed denial of service (DDoS) attacks ever seen unfold. As CloudFlare has grown we've brought on line systems capable of absorbing and *accurately measuring* attacks. Since we don't need to resort to crude techniques to block traffic we can measure and filter attacks with accuracy. Our systems sort bad packets from good, keep websites online and keep track of attack packet rates and bits per second.

The current spate of large attacks are all layer 3 (L3) DDoS. Layer 3 attacks consist of a large volume of packets hitting the target network, and the aim is usually to overwhelm the target network hardware or connectivity.

L3 attacks are dangerous because most of the time the only solution is to acquire large network capacity and buy beefy networking hardware, which is simply not an option for most independent website operators. Or, faced with huge packet rates, some providers simply turn off connections or entirely block IP addresses.

John Graham-Cumming
@jgrahamc

Follow

Hello gigantic SYN flood.

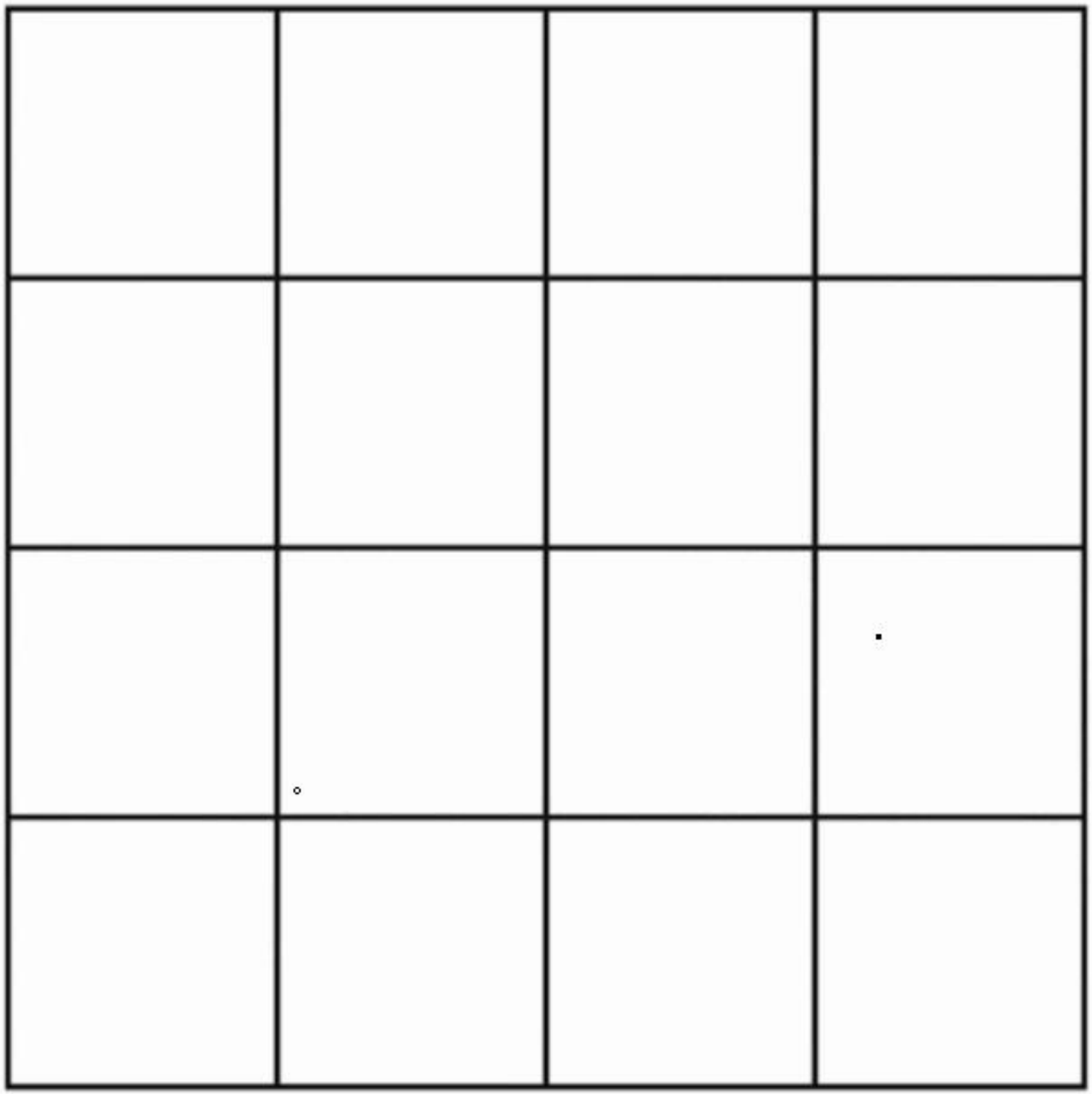
2:40 AM - 9 Apr 2018

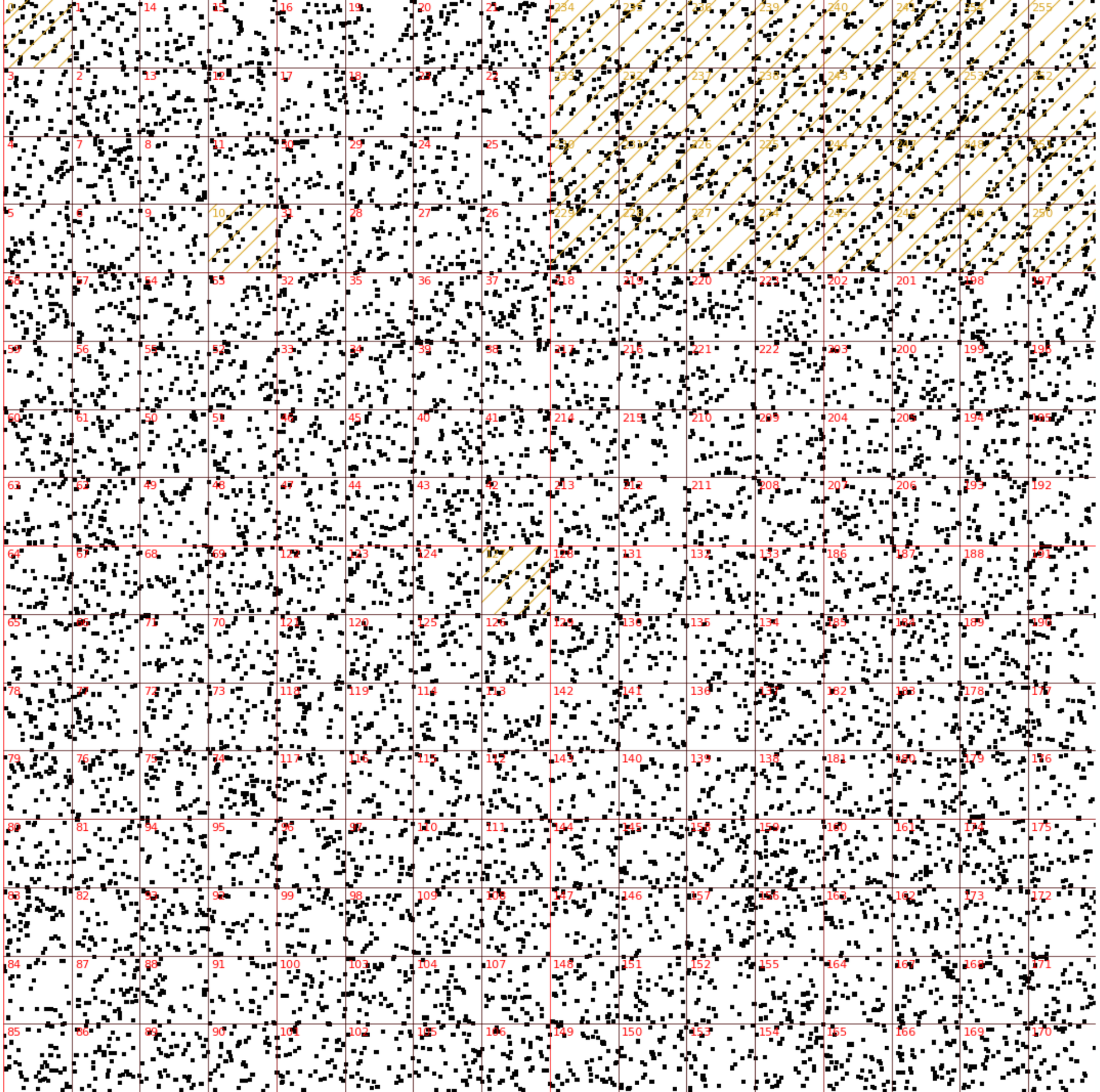
62 Retweets **177** Likes

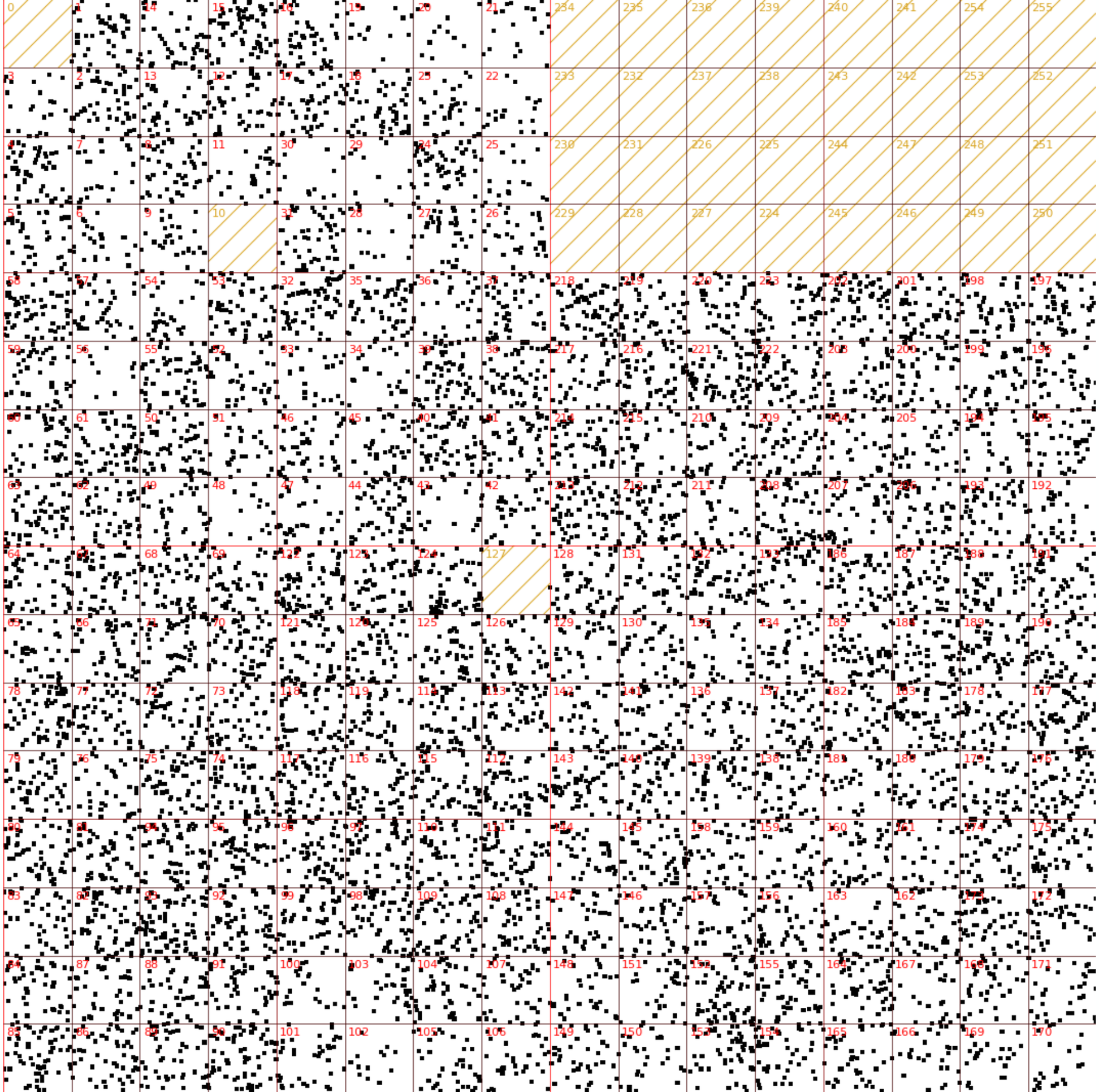
5 62 177

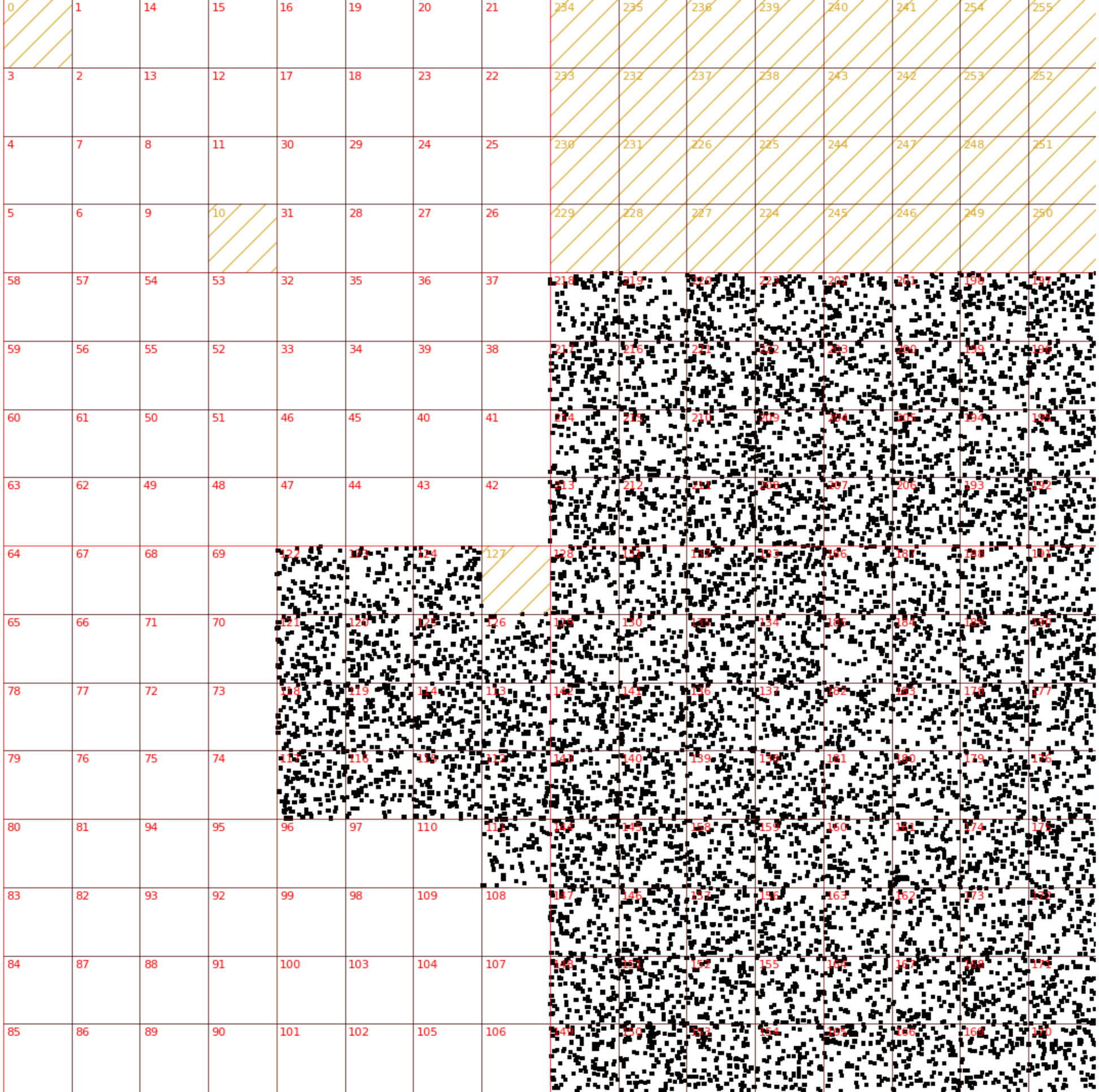
MAP OF THE INTERNET

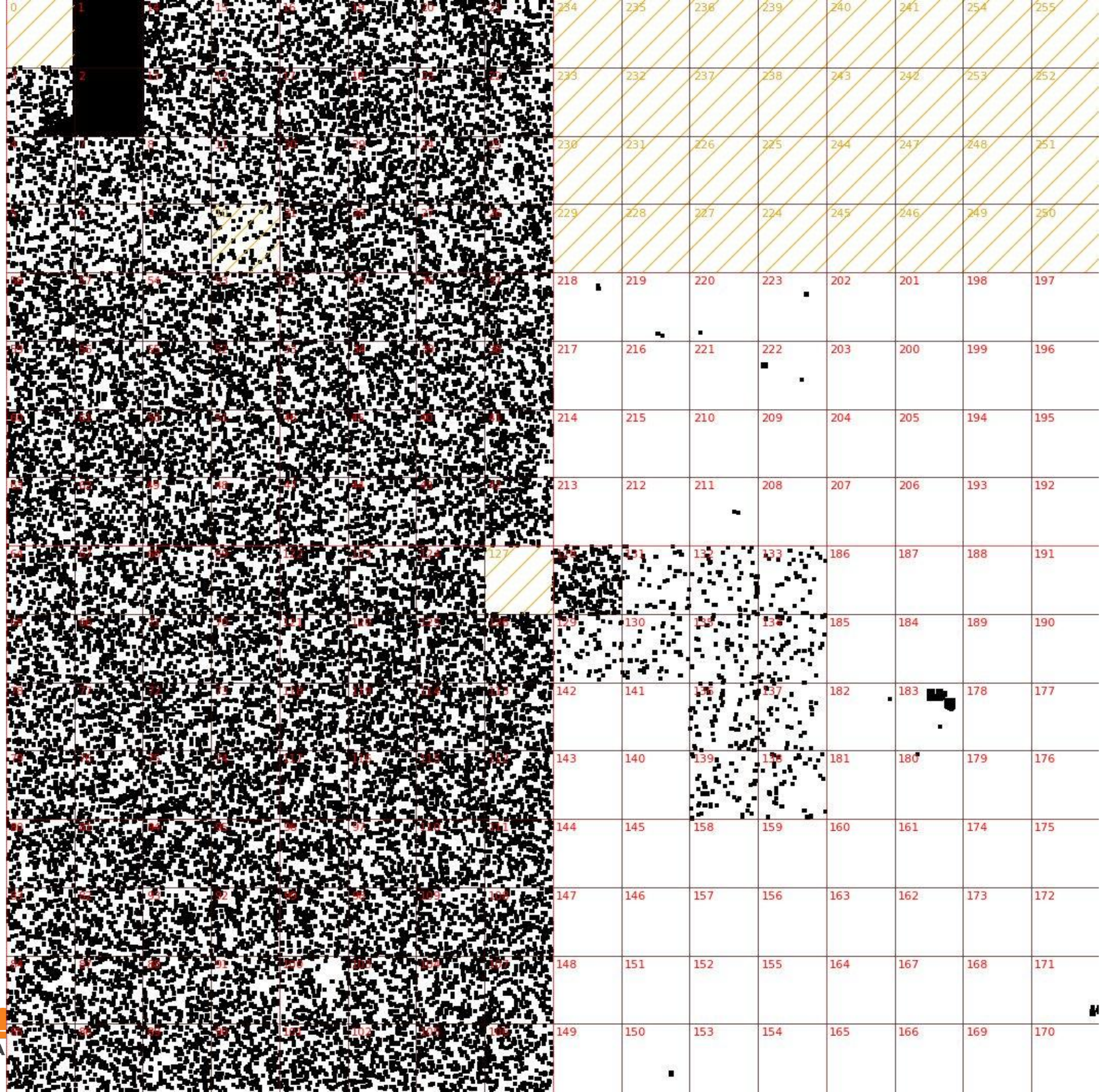
THE IPv4 SPACE, 2006



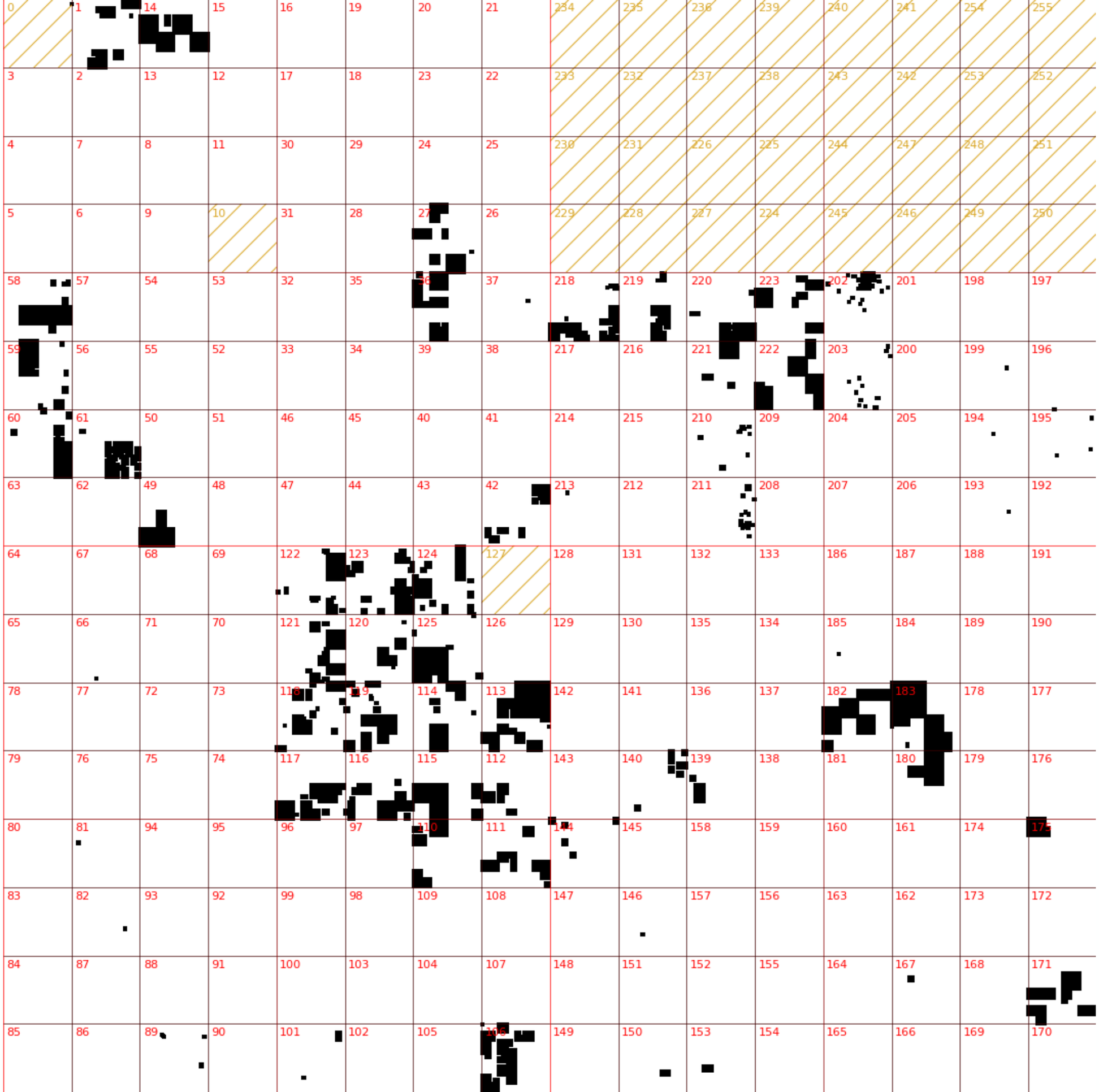


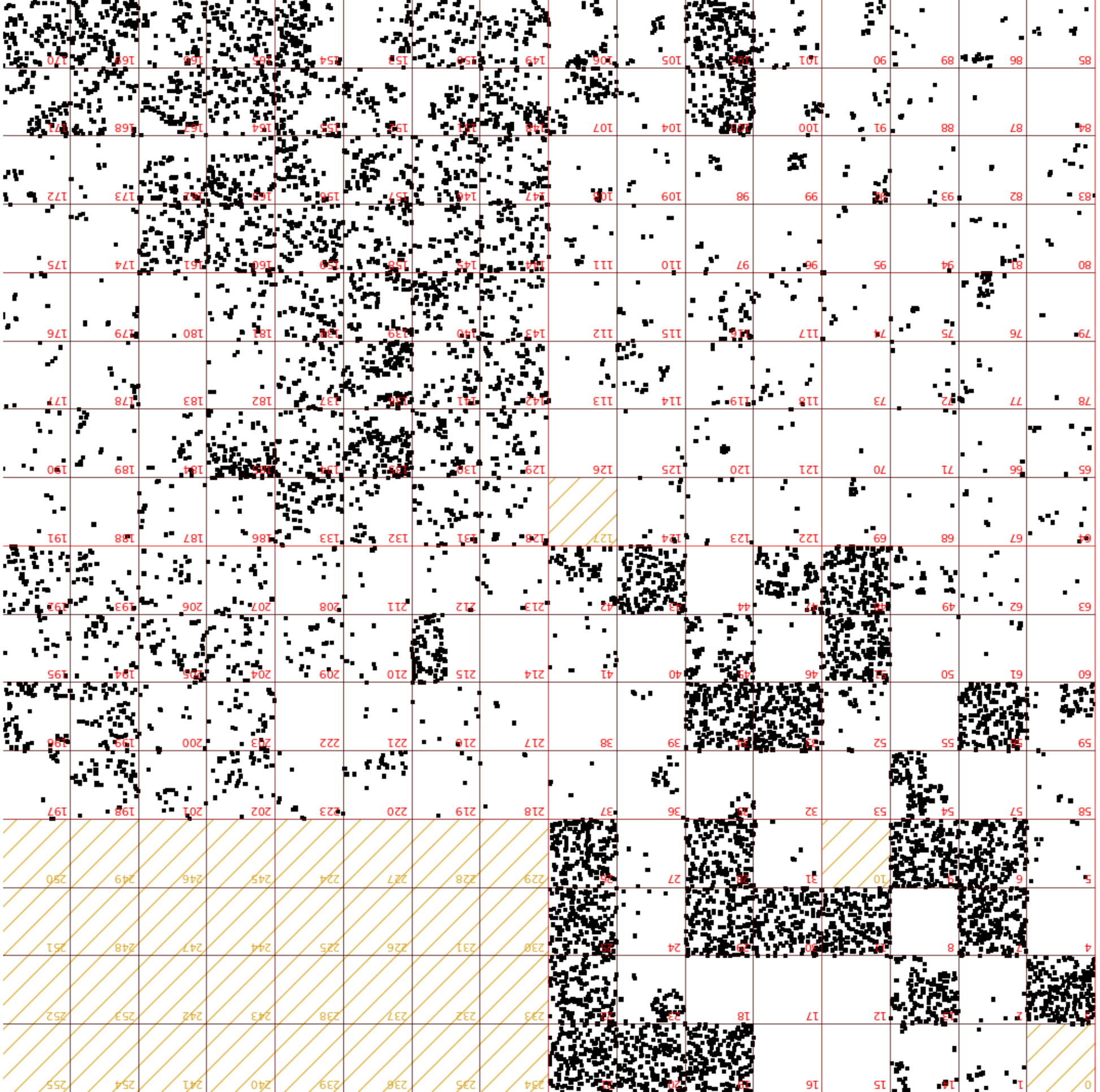



0 1 14 15 16 19 20 21 234 235 236 239 240 241 254 255
3 2 13 12 17 18 23 22 233 232 237 238 243 242 253 252
4 7 8 11 30 29 24 25 230 231 226 225 244 247 248 251
5 6 9 10 31 28 27 26 229 228 227 224 245 246 249 250
58 57 54 53 32 35 36 37
59 56 55 52 33 34 39 38
60 61 50 51 46 45 40 41
63 62 49 48 47 44 43 42
64 67 68 69 127
65 66 71 70
78 77 72 73
79 76 75 74
80 81 94 95 96 97 110
83 82 93 92 99 98 109 108
84 87 88 91 100 103 104 107
85 86 89 90 101 102 105 106

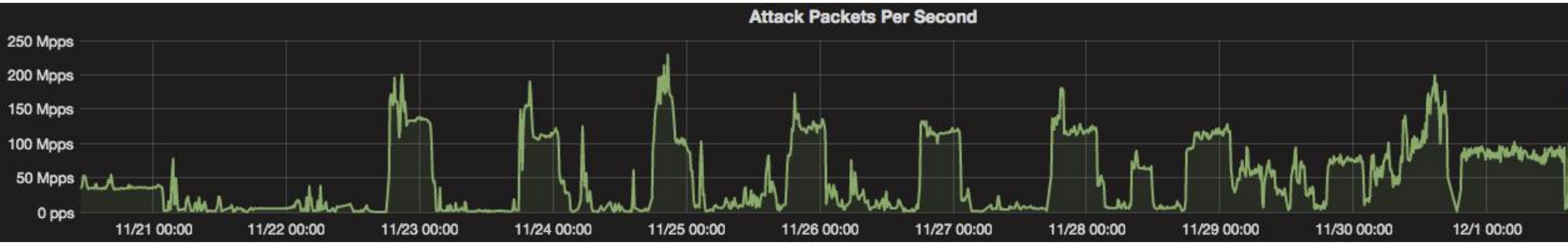

234 235 238 239 240 241 254 255
233 232 237 238 243 242 253 252
230 231 226 225 244 247 248 251
229 228 227 224 245 246 249 250
218 219 220 223 202 201 198 197
217 216 221 222 203 200 199 196
214 215 210 209 204 205 194 195
213 212 211 208 207 206 193 192
127
131 132 133 186 187 188 191
129 130 135 134 185 184 189 190
142 141 136 137 182 183 178 177
143 140 139 138 181 180 179 176
144 145 158 159 160 161 174 175
147 146 157 156 163 162 173 172
148 151 152 155 164 167 168 171
149 150 153 154 165 166 169 170

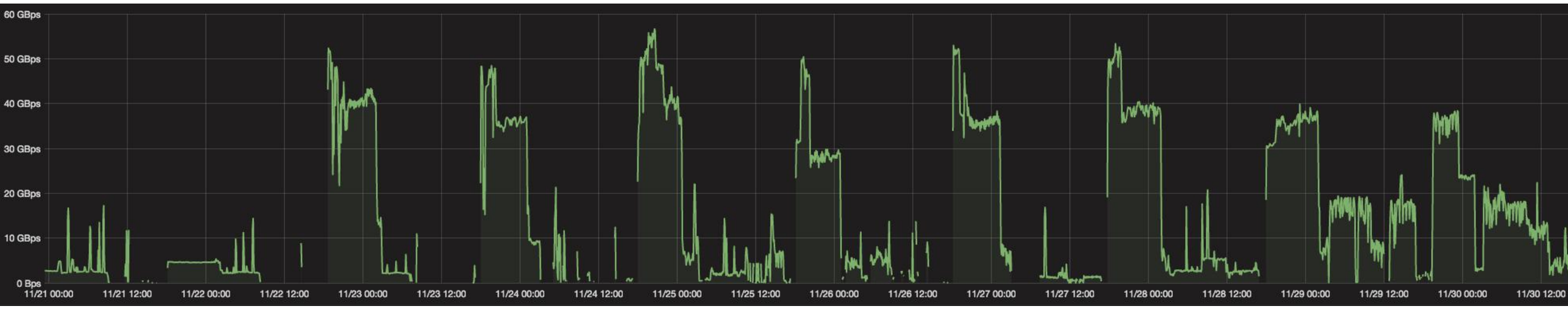
0	1	14	15	16	19	20	21	234	235	236	239	240	241	254	255
3	2	13	12	17	18	23	22	233	232	237	238	243	242	253	252
4	7	8	11	30	29	24	25	230	231	226	225	244	247	248	251
5	6	9	10	31	28	27	26	229	228	227	224	245	246	249	250
58	57	54	53	32	35	36	37	218	219	220	223	202	201	198	197
59	56	55	52	33	34	39	38	217	216	221	222	203	200	199	196
60	61	50	51	46	45	40	41	214	215	210	209	204	205	194	195
63	62	49	48	47	44	43	42	213	212	211	208	207	206	193	192
64	67	68	69	122	123	124	127	128	131	132	133	186	187	188	191
65	66	71	70	121	120	125	126	129	130	135	134	185	184	189	190
78	77	72	73	118	119	114	113	142	141	136	137	182	183	178	177
79	76	75	74	117	116	115	112	143	140	139	138	181	180	179	176
80	81	94	95	96	97	110	111	144	145	158	159	160	161	174	175
83	82	93	92	99	98	109	108	147	146	157	156	163	162	173	172
84	87	88	91	100	103	104	107	148	151	152	155	164	167	168	171
85	86	89	90	101	102	105	106	149	150	153	154	165	166	169	170


0 1 14 15 16 19 20 21 234 235 236 239 240 241 254 255
3 2 13 12 17 18 23 22 233 232 237 238 243 242 253 252
4 7 8 11 30 29 24 25 230 231 226 225 244 247 248 251
5 6 9 10 31 28 27 26 229 228 227 224 245 246 249 250
58 57 54 53 32 35 36 37 218 219 220 223 202 201 198 197
59 56 55 52 33 34 39 38 217 216 221 222 203 200 199 196
60 61 50 51 46 45 40 41 214 215 210 209 204 205 194 195
63 62 49 48 47 44 43 42 213 212 211 208 207 206 193 192
64 67 68 69 122 123 124 127 128 131 132 133 186 187 188 191
65 66 71 70 121 120 125 126 129 130 135 134 185 184 189 190
78 77 72 73 118 119 114 113 142 141 136 137 182 183 178 177
79 76 75 74 117 116 115 112 143 140 139 138 181 180 179 176
80 81 94 95 96 97 110 111 144 145 158 159 160 161 174 175
83 82 93 92 99 98 109 108 147 146 157 156 163 162 173 172
84 87 88 91 100 103 104 107 148 151 152 155 164 167 168 171
85 86 89 90 101 102 105 106 149 150 153 154 165 166 169 170



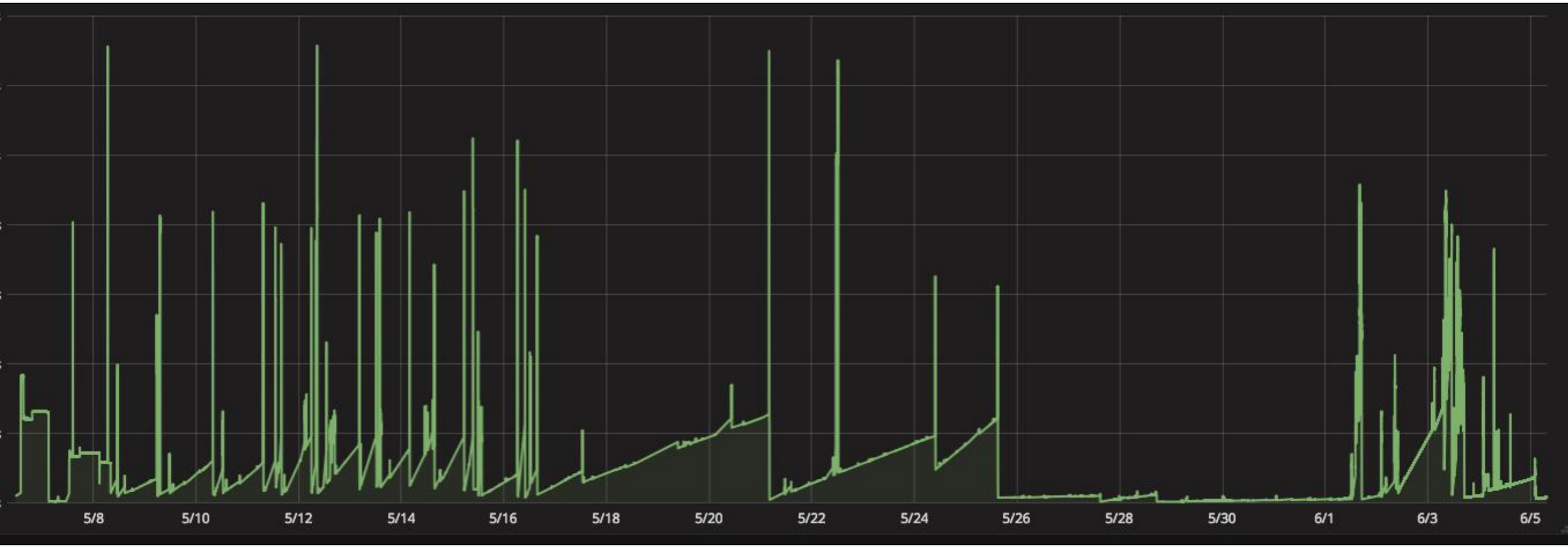
Is it a day job?



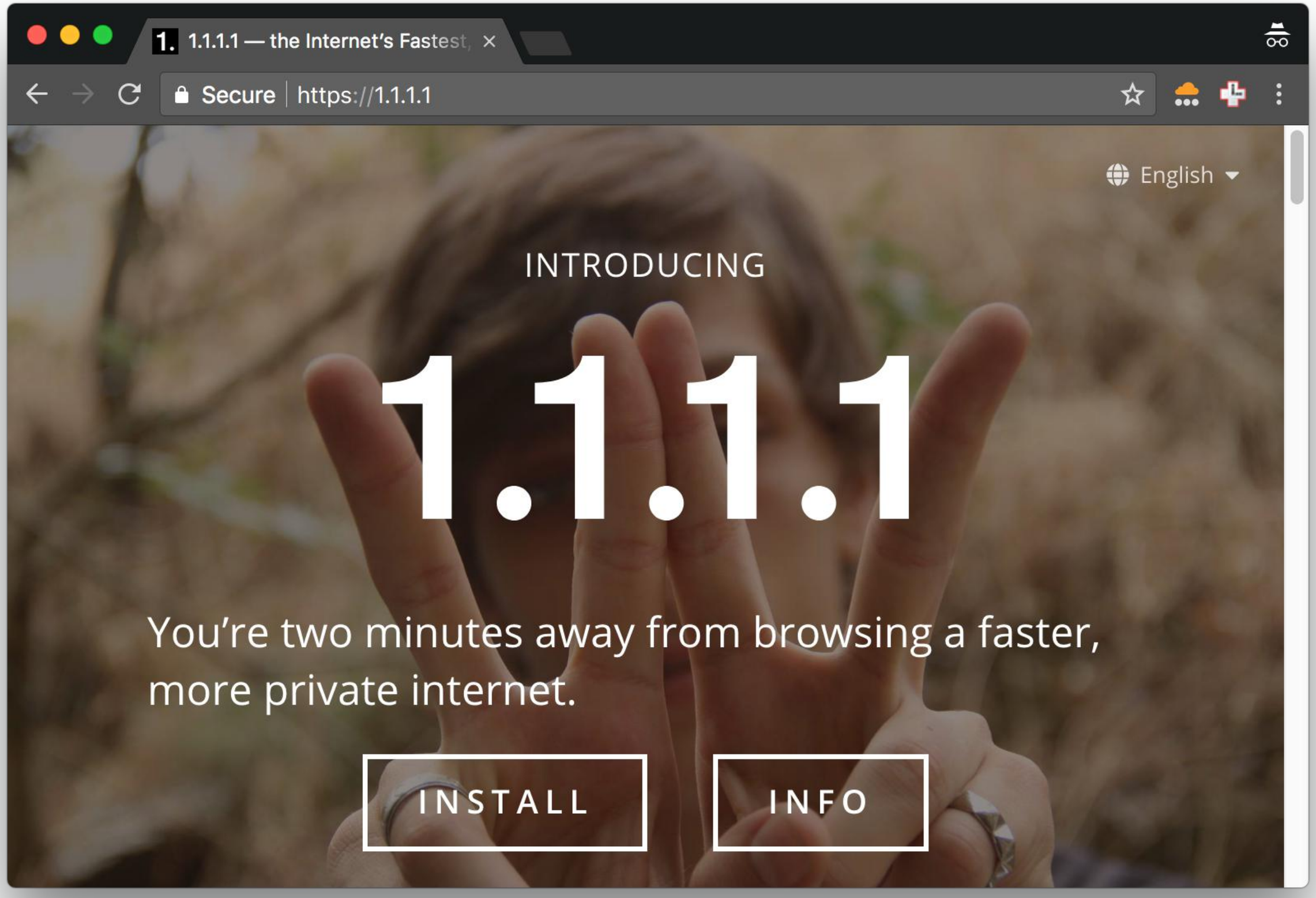


CLOUDFLARE

Direct attack today



Imaginary attacks

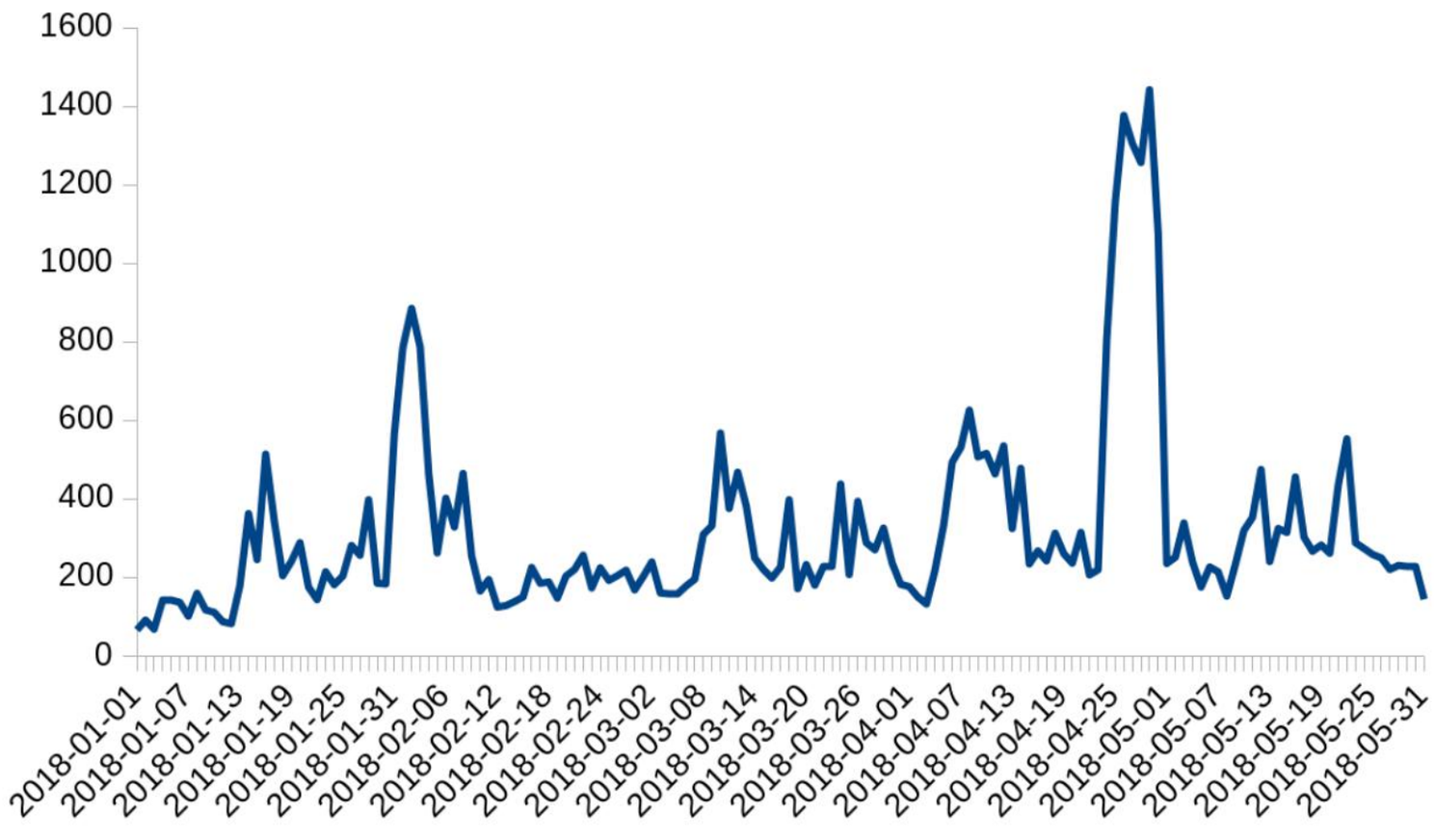

1.1.1.1 — the Internet's Fastest,
Secure
https://1.1.1.1
English
INTRODUCING
1.1.1.1
You're two minutes away from browsing a faster, more private internet.
INSTALL
INFO

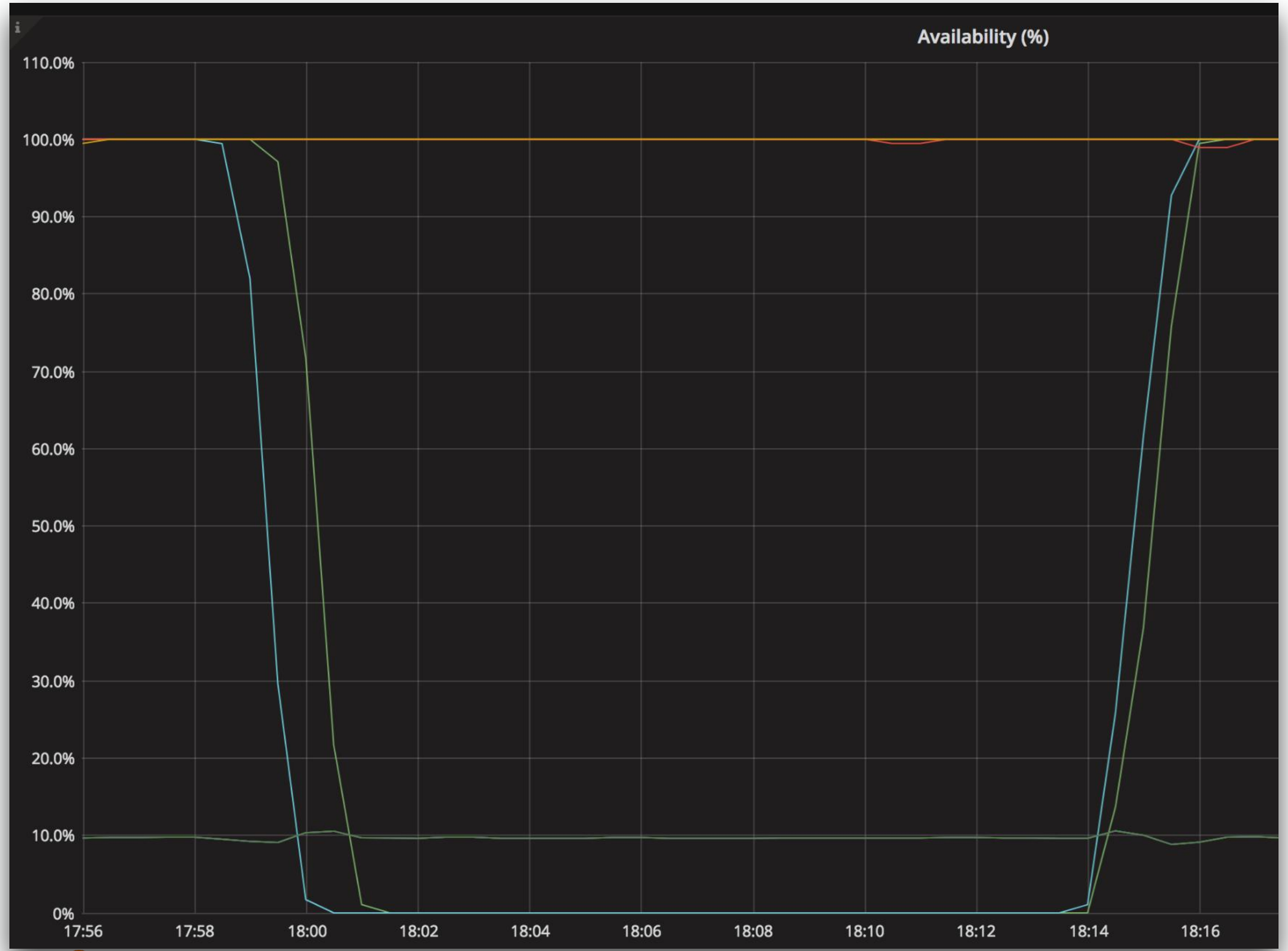
Today we mitigated 1.1.1.1

01 Jun 2018 by Marek Majkowski.

On May 31, 2018 we had a 17 minute outage on our 1.1.1.1 resolver service; this was our doing and not the result of an attack.

Cloudflare is protected from attacks by the Gatebot DDoS mitigation pipeline. Gatebot performs hundreds of mitigations a day, shielding our infrastructure and our customers from L3/L4 and L7 attacks. Here is a chart of a count of daily Gatebot actions this year:

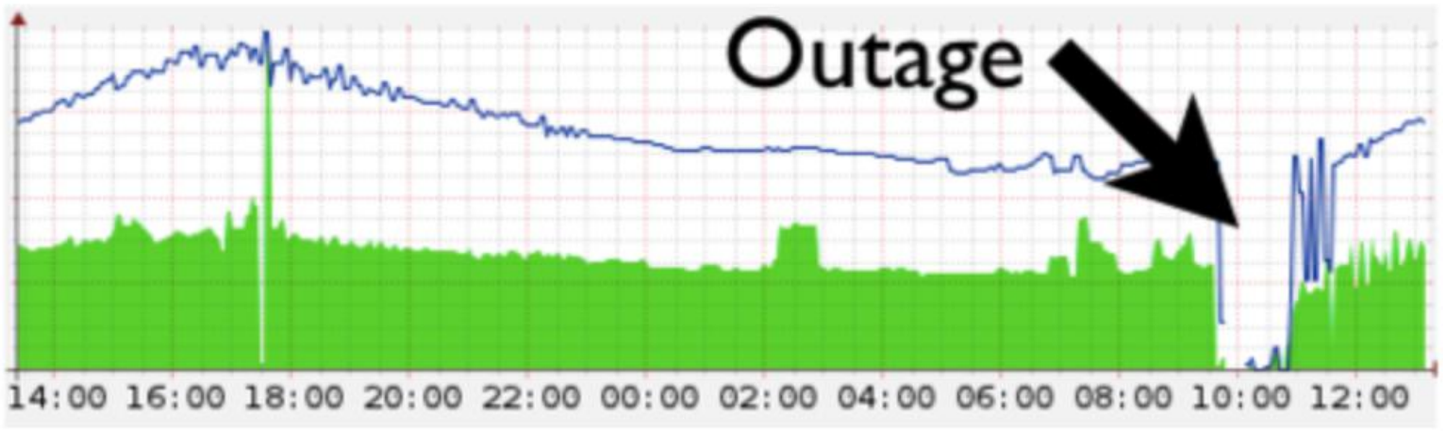



Availability (%)
110.0%
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0%
17:56
17:58
18:00
18:02
18:04
18:06
18:08
18:10
18:12
18:14
18:16

CLOUDFLARE

Today's Outage Post Mortem

03 Mar 2013 by Matthew Prince.



This morning at 09:47 UTC CloudFlare effectively dropped off the Internet. The outage affected all of CloudFlare's services including DNS and any services that rely on our web proxy. During the outage, anyone accessing CloudFlare.com or any site on CloudFlare's network would have received a DNS error. Pings and Traceroutes to CloudFlare's network resulted in a "No Route to Host" error.

Application attacks are small

We know who attacks us!

(source: the internet)

https://www.google.com/searc ×

Secure | https://ipv4.google.com/sorry/index?continue=ht...

I'm not a robot

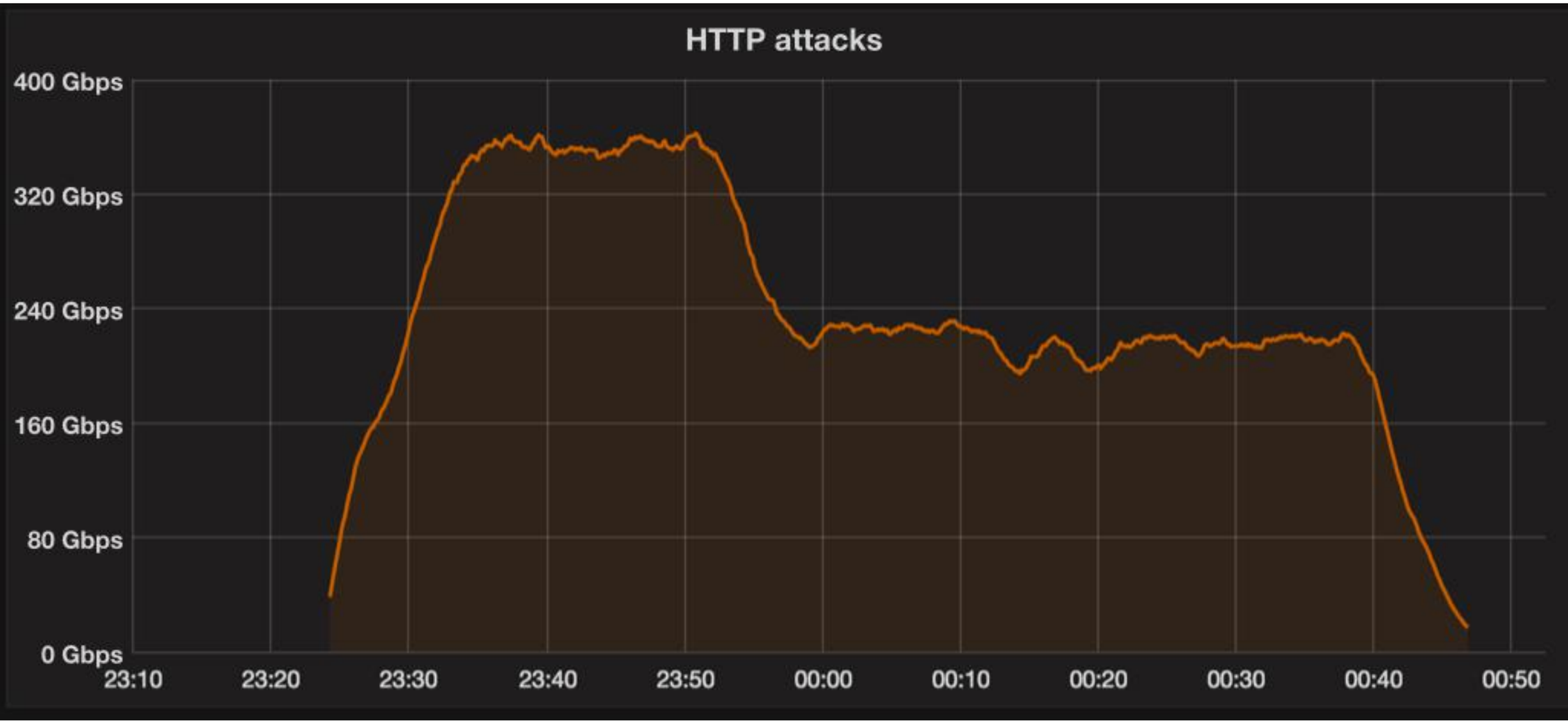
reCAPTCHA
Privacy - Terms

Submit

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 37.47.109.182
Time: 2018-06-06T12:09:06Z
URL: https://www.google.com/search?q=asaaaaa

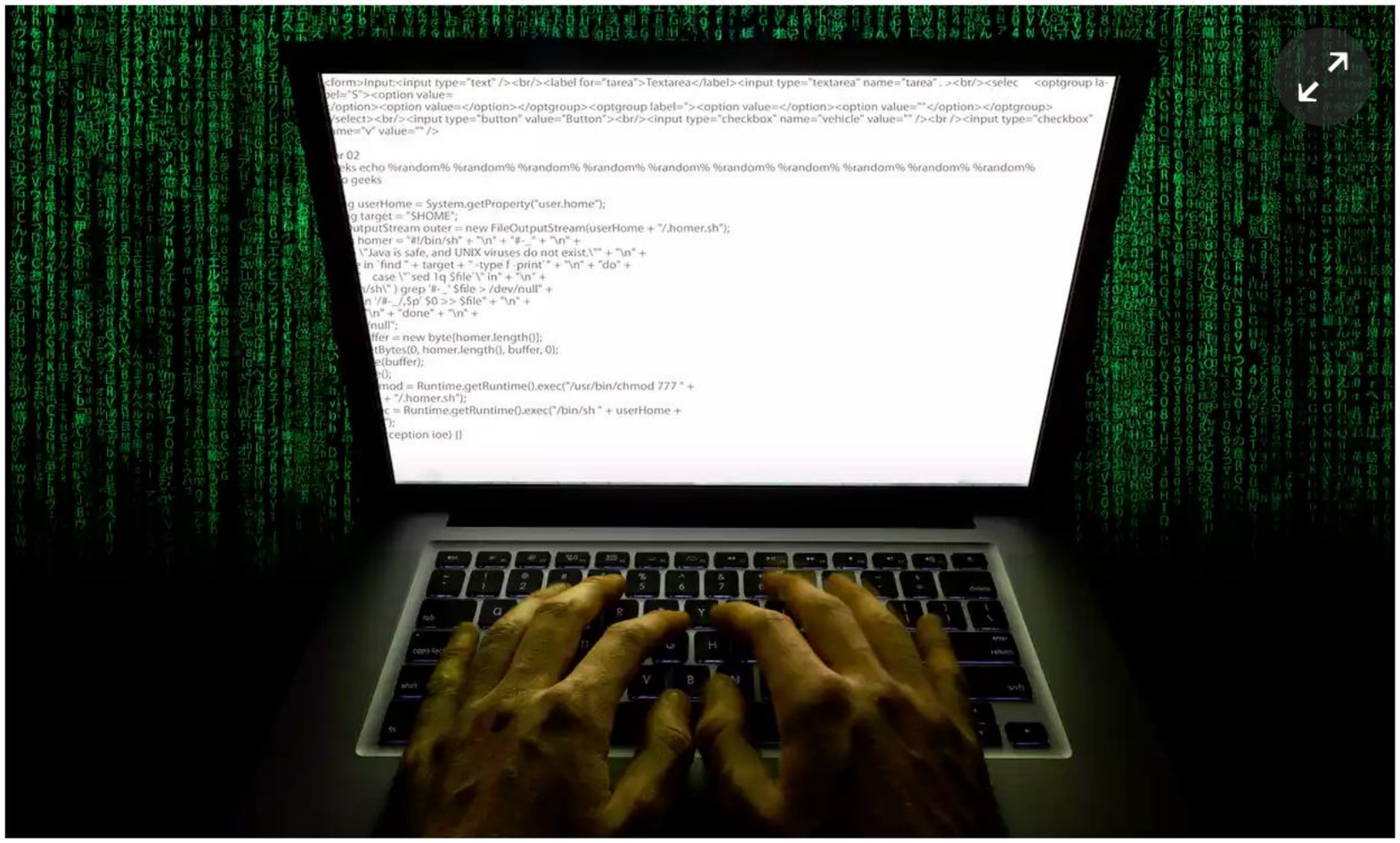

HTTP attacks
400 Gbps
320 Gbps
240 Gbps
160 Gbps
80 Gbps
0 Gbps
23:10
23:20
23:30
23:40
23:50
00:00
00:10
00:20
00:30
00:40
00:50

IoT - Cameras

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US



Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

The cyber-attack that brought down much of America's internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its

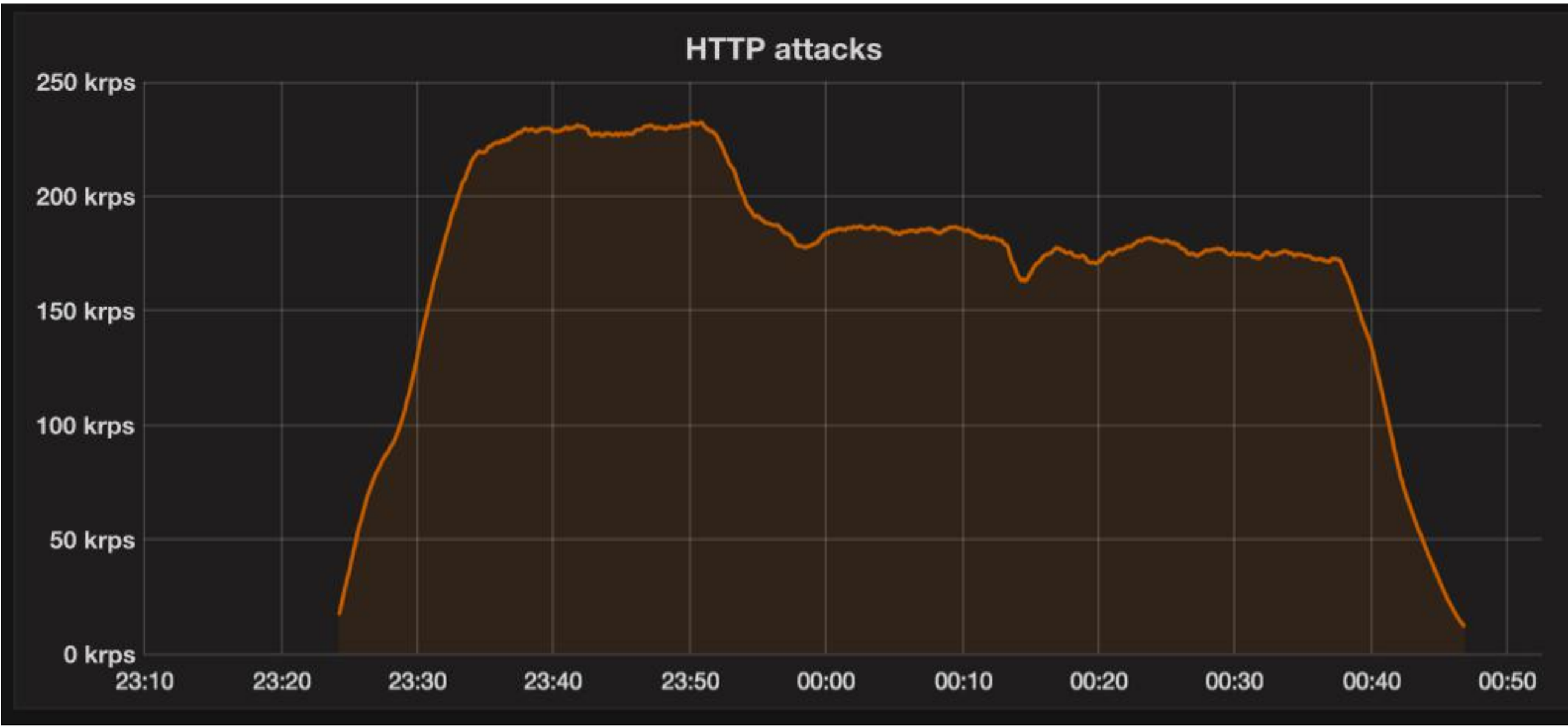
Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras

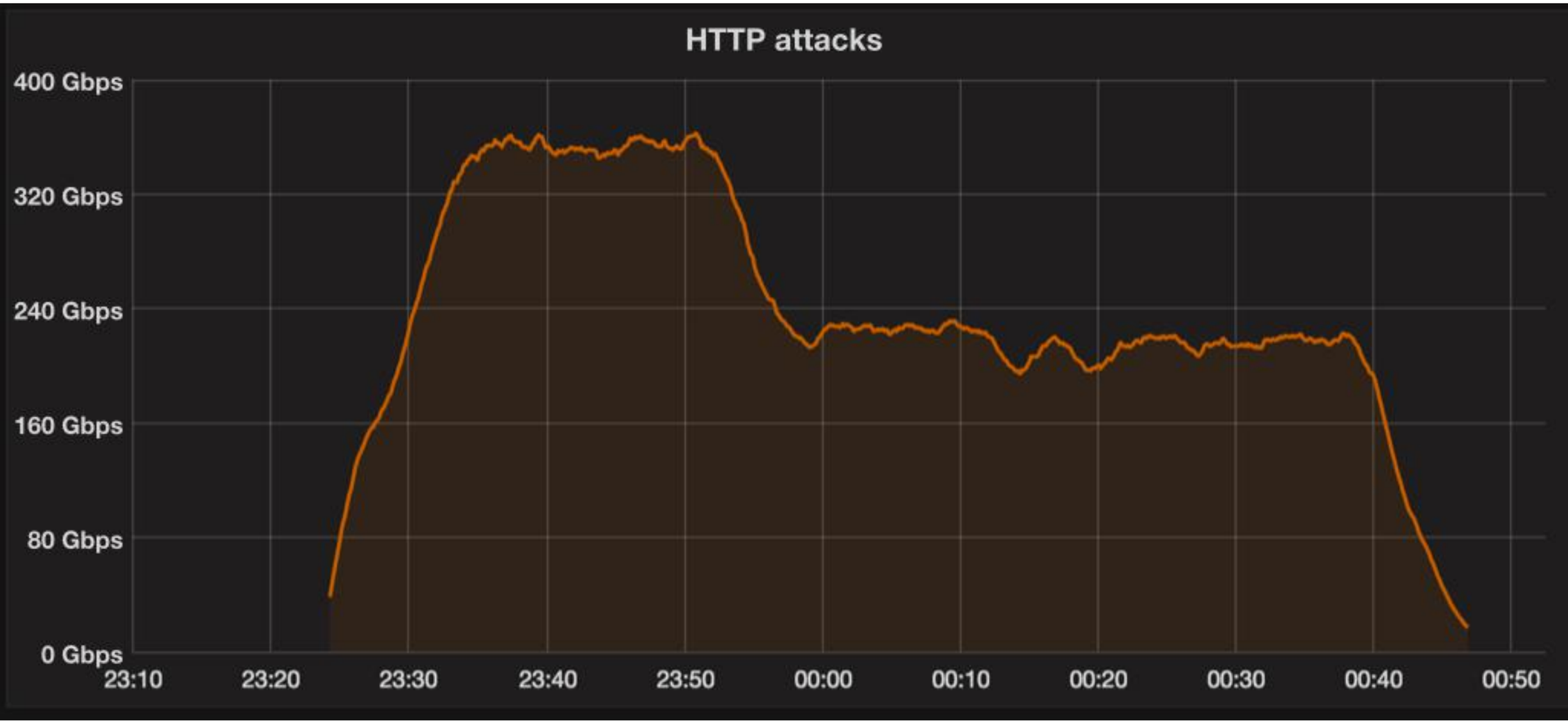
11 Oct 2016 by Marek Majkowski.

Over the last few weeks we've seen DDoS attacks hitting our systems that show that attackers have switched to new, large methods of bringing down web applications. They appear to come from an IoT botnet (like Mirai and relations) which were responsible for the large attacks against Brian Krebs.

Our automatic DDoS mitigation systems have been handling these attacks, but we thought it would be interesting to publish some of the details of what we are seeing. In this article we'll share data on two attacks, which are perfect examples of the new trends in DDoS.

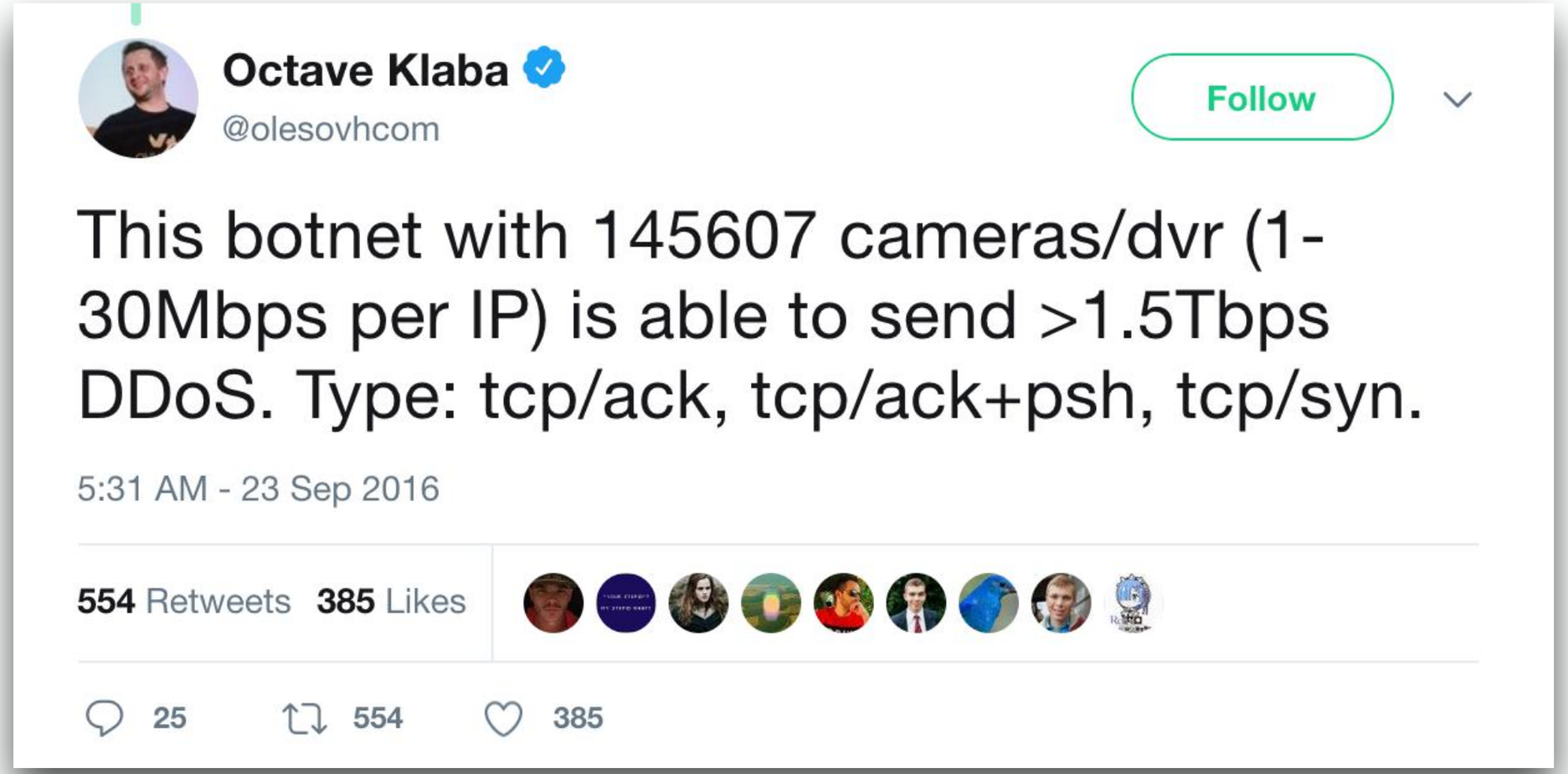

CP PLUS
enhancing vision
The World's Preferred Electronic
Security Equipment
Username:
Password:
Ver 3.0
WEB SERVICE
用户名:
密码:
登录
取消


HTTP attacks
250 krps
200 krps
150 krps
100 krps
50 krps
0 krps
23:10
23:20
23:30
23:40
23:50
00:00
00:10
00:20
00:30
00:40
00:50


HTTP attacks
400 Gbps
320 Gbps
240 Gbps
160 Gbps
80 Gbps
0 Gbps
23:10
23:20
23:30
23:40
23:50
00:00
00:10
00:20
00:30
00:40
00:50

```
GET /en HTTP/1.1
User-Agent: <some string>
Cookie: <some cookie>
Host: example.com
Connection: close
Content-Length: 800000

a[]=&b[]=&a[]=&b[]=&a[]=&b[]=&a[]=&b[]=&a[]=&b[]=&a[]=&b[]=...
```


Octave Klaba
@olesovhcom
Follow
This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.
5:31 AM - 23 Sep 2016
554 Retweets 385 Likes
25
554
385

Newly discovered router flaw being hammered by in-the-wild attacks

Researchers detect barrage of exploits targeting potentially millions of devices.

DAN GOODIN - 11/28/2016, 10:21 PM

Enlarge

Evolution of IoT botnets

- Mirai - cameras
- TR-069/TR-064 Deutsche Telefon - CPE
- Reaper - D-Link, Netgear, and AVTech
- VPNFilter - routers and NAS

WireX - Android malware

The WireX Botnet: How Industry Collaboration Disrupted a DDoS Attack

28 Aug 2017 by Jaime Cochran.

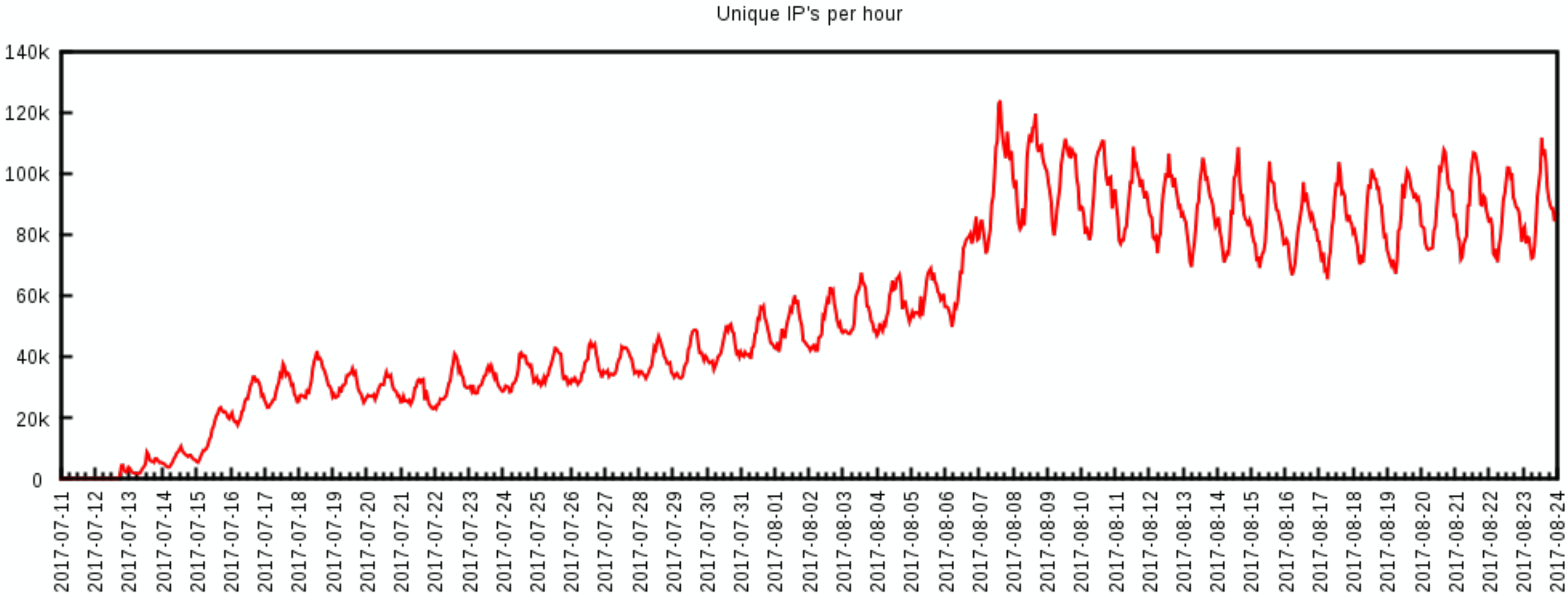
Updated October 2017: The Cyberwire Research Saturday Podcast:

Introduction

On August 17th, 2017, multiple Content Delivery Networks (CDNs) and content providers were subject to significant attacks from a botnet dubbed WireX. The botnet is named for an anagram for one of the delimiter strings in its command and control protocol. The WireX botnet comprises primarily Android devices running malicious applications and is designed to create DDoS traffic. The botnet is sometimes associated with ransom notes to targets.

A few days ago, Google was alerted that this malware was available on its Play Store. Shortly following the notification, Google removed hundreds of affected applications and started the process to remove the applications from all devices.

```
User-Agent: jigpuzbcomkenhvladtwysqfxr
User-Agent: yudjmikcvzoqwsbflghtxpanre
User-Agent: mckvhaflwzbderiysoguxnqtpj
User-Agent: deogjvtynmcxzwfsbahirukqpl
User-Agent: fdmjczoeyarnuqkbgtlivsxhwp
User-Agent: yczfxlrenuqtwmavhojpigkdsb
User-Agent: dnlseufokcgvmajqzpbtrwyxih
```


Unique IP's per hour
140k
120k
100k
80k
60k
40k
20k
0
2017-07-11
2017-07-12
2017-07-13
2017-07-14
2017-07-15
2017-07-16
2017-07-17
2017-07-18
2017-07-19
2017-07-20
2017-07-21
2017-07-22
2017-07-23
2017-07-24
2017-07-25
2017-07-26
2017-07-27
2017-07-28
2017-07-29
2017-07-30
2017-07-31
2017-08-01
2017-08-02
2017-08-03
2017-08-04
2017-08-05
2017-08-06
2017-08-07
2017-08-08
2017-08-09
2017-08-10
2017-08-11
2017-08-12
2017-08-13
2017-08-14
2017-08-15
2017-08-16
2017-08-17
2017-08-18
2017-08-19
2017-08-20
2017-08-21
2017-08-22
2017-08-23
2017-08-24

CLOUDFLARE


October 4

TubeMate 2.2.9 SnapTube Youtube Downloader R所有好玩的安卓 ...
https://m.apkpure.com/.../TubeMate%202.2.9%20SnapTube%20Y... ▾ Translate this page
TubeMate 2.2.9 SnapTube Youtube Downloader R所有安卓游戏免费下载，最新版下载更新。

klzukykr APK Download - Free Tools APP for Android | APKPure.com
https://apkpure.com/klzukykr/com.klzukykr.app ▾
Author: **TubeMate 2.2.9 SnapTube Youtube Downloader R.** Latest Version: 0.0.2. Publish Date: 2017-07-28. Download APK(2.0 MB) · klzukykr safe verified.

rsnpmqgz APK Download - Free Tools APP for Android | APKPure.com
https://apkpure.com/rsnpmqgz/com.rsnpmqgz.app ▾
Author: **TubeMate 2.2.9 SnapTube Youtube Downloader R.** Latest Version: 0.0.1. Publish Date: 2017-07-28. Download APK(2.2 MB) · rsnpmqgz safe verified.

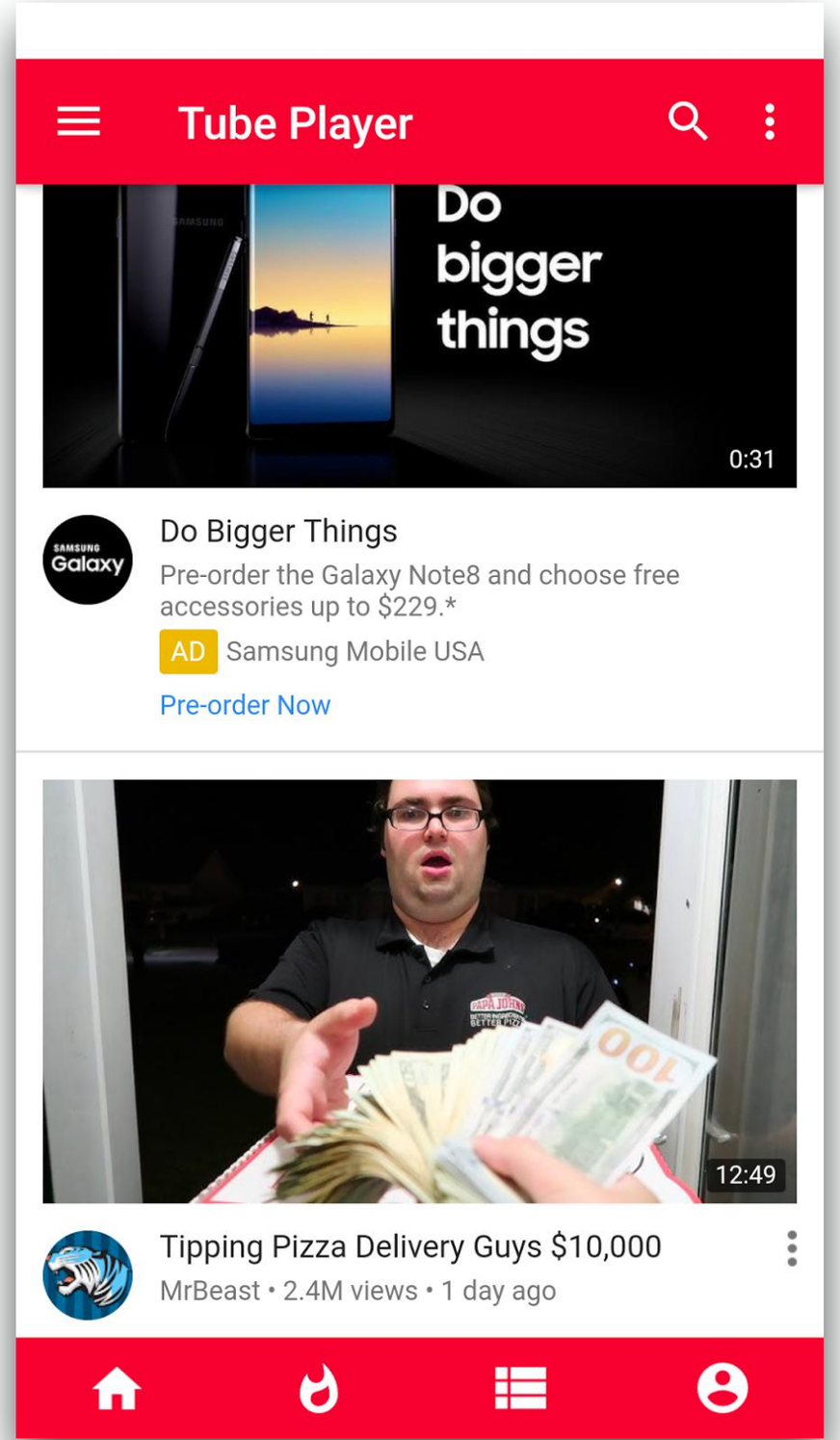
noigznrl 0.0.1 Apk 0.0.1 | Download Only APK file for Android
https://1apk.co › Tools ▾
Aug 13, 2017 - You could visit **TubeMate 2.2.9 SnapTube YouTube Downloader r's** website to know more about the company/developer who developed this.

llkciyyh 0.0.1 Apk 0.0.1 | Download Only APK file for Android
https://1apk.co › Tools ▾
Aug 11, 2017 - You could visit **TubeMate 2.2.9 SnapTube YouTube Downloader r's** website to know more about the company/developer who developed this.

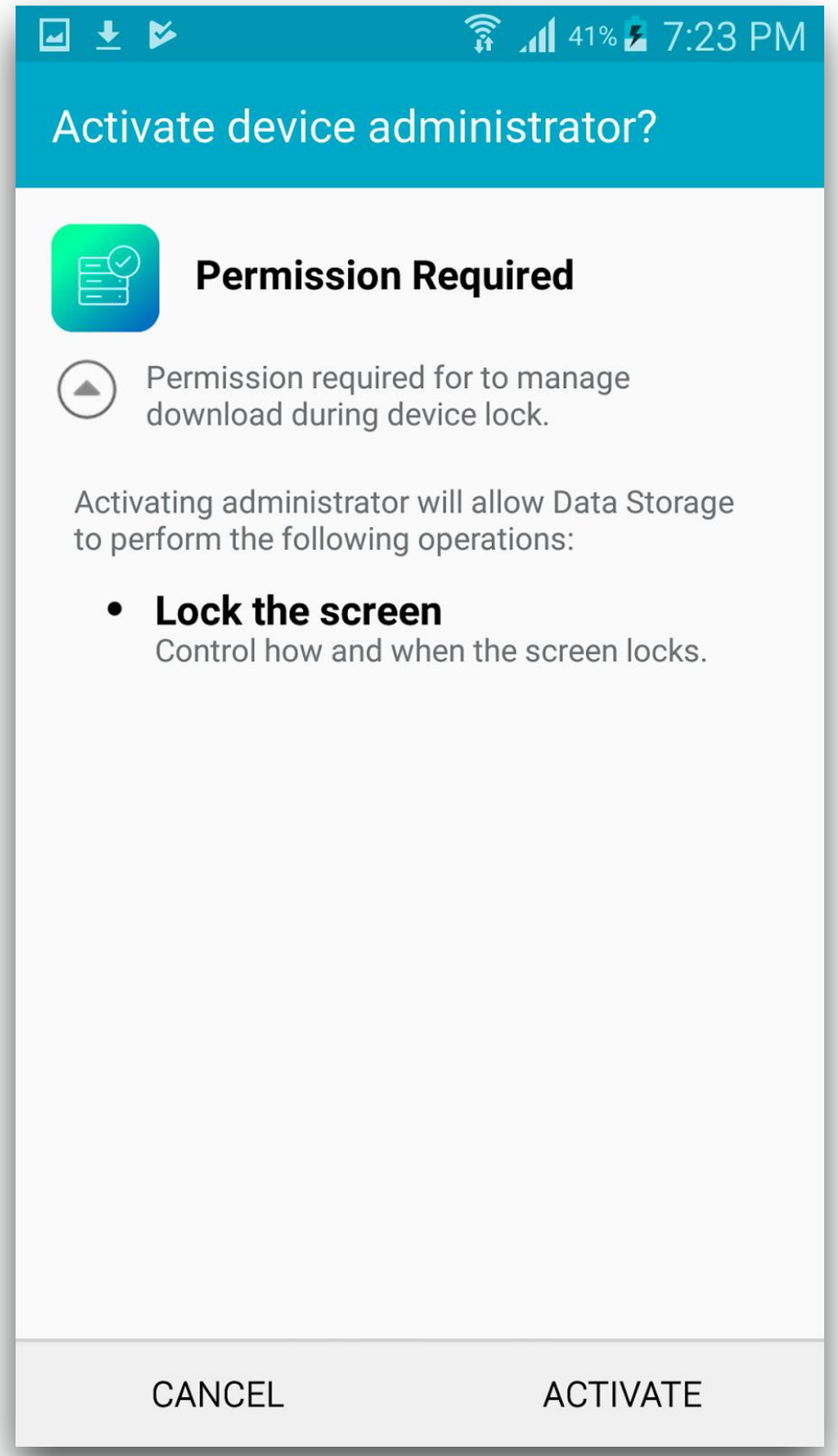
xanbrcua 0.0.1 Apk 0.0.1 | Download Only APK file for Android
https://1apk.co › Tools ▾
Aug 13, 2017 - You could visit **TubeMate 2.2.9 SnapTube YouTube Downloader r's** website to know more about the company/developer who developed this.

Download rsnpmqgz Google Play softwares - aQAalwyeIfMh | mobile9
gallery.mobile9.com › All Devices › Google Play ▾
Developed by **TubeMate 2.2.9 SnapTube Youtube Downloader R.** Imported by mobile9. FREE. FAVOURITE. SHARE. CLAIM. rsnpmqgz ...

скачать rsnpmqgz Google Play softwares - aQAalwyeIfMh | mobile9
ru.mobile9.com › Все устройства › Google Play ▾ Translate this page
Разработанный **TubeMate 2.2.9 SnapTube Youtube Downloader R.** Импортировано mobile9. БЕСПЛАТНО. ЛЮБИМЫЙ. ДОЛЯ. ПРЕТЕНЗИИ. rsnpmqgz ...

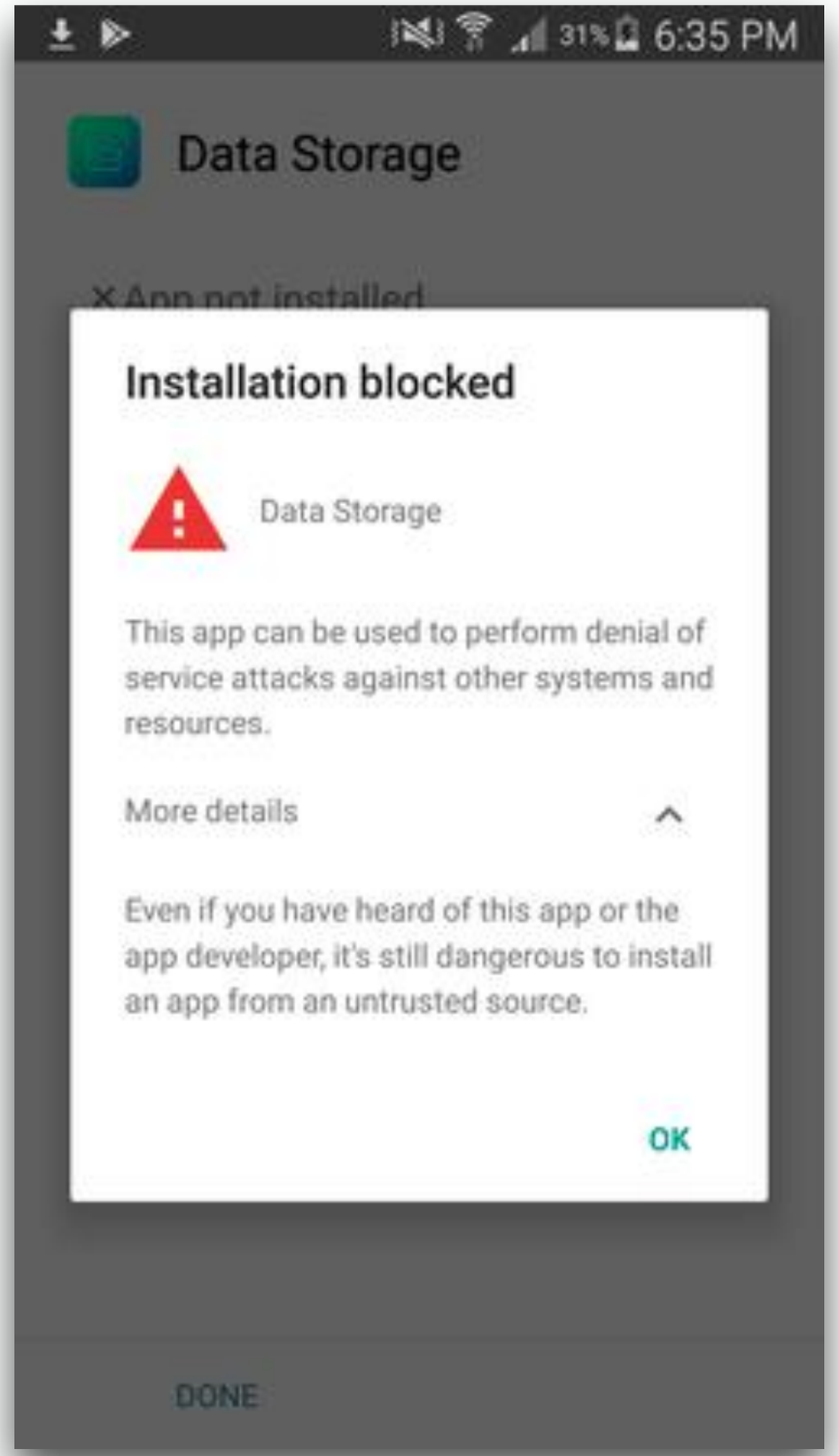

Tube Player
Do bigger things
0:31
Do Bigger Things
Pre-order the Galaxy Note8 and choose free accessories up to $229.*
AD Samsung Mobile USA
Pre-order Now
12:49
Tipping Pizza Delivery Guys $10,000
MrBeast • 2.4M views • 1 day ago


63% 9:05 PM
Google Play Store
Lucky patcher Booster
Lucky Booster
Lucky Booster
Everyone
INSTALL
Contains ads
50
THOUSAND
Downloads
4.0
695
Tools
Similar
Lucky Booster: Control your RAM, Speed Patcher Boost it! Safe kill your tasks..
READ MORE


41% 7:23 PM
Activate device administrator?
Permission Required
Permission required for to manage download during device lock.
Activating administrator will allow Data Storage to perform the following operations:
Lock the screen
Control how and when the screen locks.
CANCEL
ACTIVATE

```
function attack(String target, String userAgent, String referer) {
        HashMap WebViewHeaders = new HashMap();
        WebViewHeaders->put(“Referer”,referer);
        WebViewHeaders->put(“X-Requested-With”,””);
        WebView[] AttackerViews = new WebView[100];
        for (int i=0; i<AttackerViews.length; i++) {
            AttackerViews[i] = new WebView();
            AttackerViews[i]->clearHistory();
            AttackerViews[i]->clearFormData();
            AttackerViews[i]->clearCache(true);
            WebViewSettings AWVS = AttackerViews[i]->getSettings()
            AttackWebViewSettings->setJavaScriptEnabled(true);
            AttackWebViewSettings->setUserAgentString(userAgent);
            AttackWebViewSettings->setCacheMode(LOAD_NO_CACHE);
            this->deleteDatabase(“webview.db”);
            this->deleteDatabase(“webviewCache.db”);
            AttackerViews[i]->loadUrl(target,WebViewHeaders);
        }
    }
}
```

CLOUDFLARE


6:35 PM
Data Storage
App not installed
Installation blocked
Data Storage
This app can be used to perform denial of service attacks against other systems and resources.
More details
Even if you have heard of this app or the app developer, it's still dangerous to install an app from an untrusted source.
OK
DONE

More....

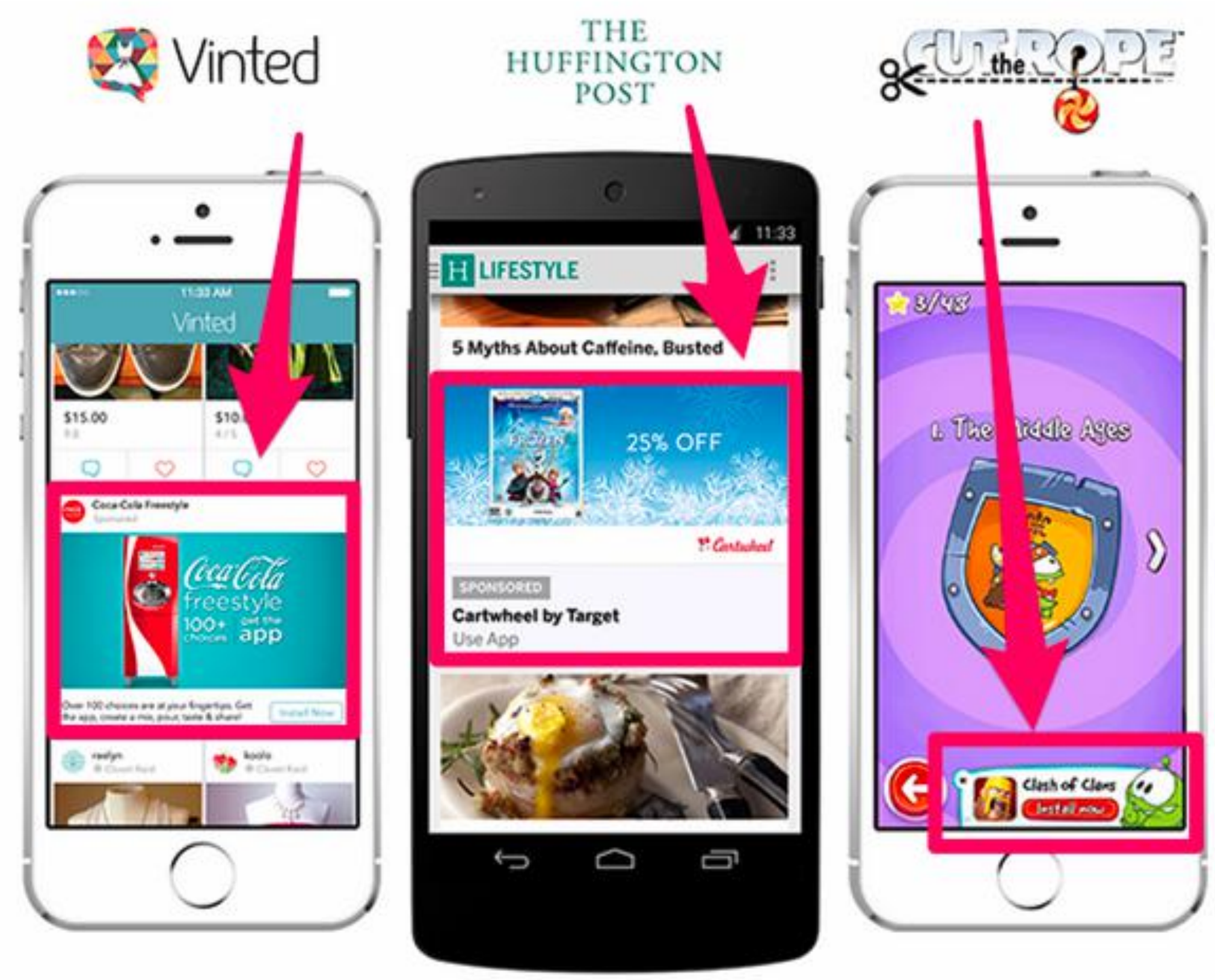
Mobile ads

Mobile Ad Networks as DDoS Vectors: A Case Study

25 Sep 2015 by Marek Majkowski.

CloudFlare servers are constantly being targeted by DDoS'es. We see everything from attempted DNS reflection attacks to L7 HTTP floods involving large botnets.

Recently an unusual flood caught our attention. A site reliability engineer on call noticed a large number of HTTP requests being issued against one of our customers.


Vinted
THE HUFFINGTON POST
CUT the ROPE
11:33 AM
Vinted
$15.00
Coca-Cola Freestyle
Sponsored
Coca-Cola freestyle
100+ choices
get the app
Over 100 choices are at your fingertips. Get the app, create a mix, pour, taste & share!
Install Now
raelyn
kaela
11:33
LIFESTYLE
5 Myths About Caffeine, Busted
25% OFF
Cartwheel
SPONSORED
Cartwheel by Target
Use App
3/43
Clash of Clans
Install now

```
function post_send() {
    var xmlHttp=c_xmlHttp();
    xmlHttp.open("POST",t_url8,true);
    xmlHttp.setRequestHeader("Content-Type", "");
    xmlHttp.send(t_postdata);
    r_send();
}

function r_send() {
    setTimeout("post_send()", 50);
}
```

Hard to mitigate

Porcupine

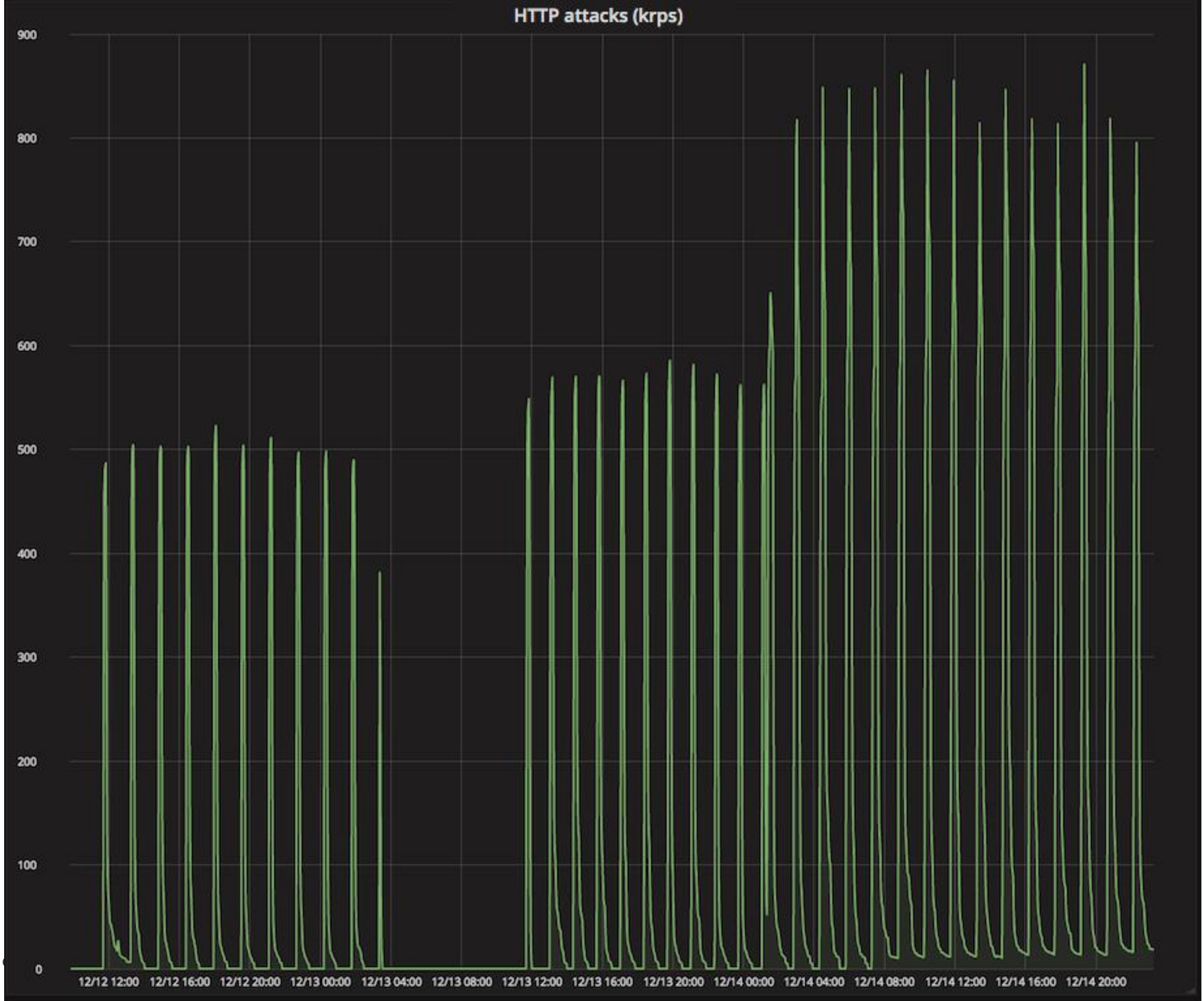
The Porcupine Attack: investigating millions of junk requests

09 Jan 2017 by Marek Majkowski.

We extensively monitor our network and use multiple systems that give us visibility including external monitoring and internal alerts when things go wrong. One of the most useful systems is Grafana that allows us to quickly create arbitrary dashboards. And a heavy user of Grafana we are: at last count we had 645 different Grafana dashboards configured in our system!

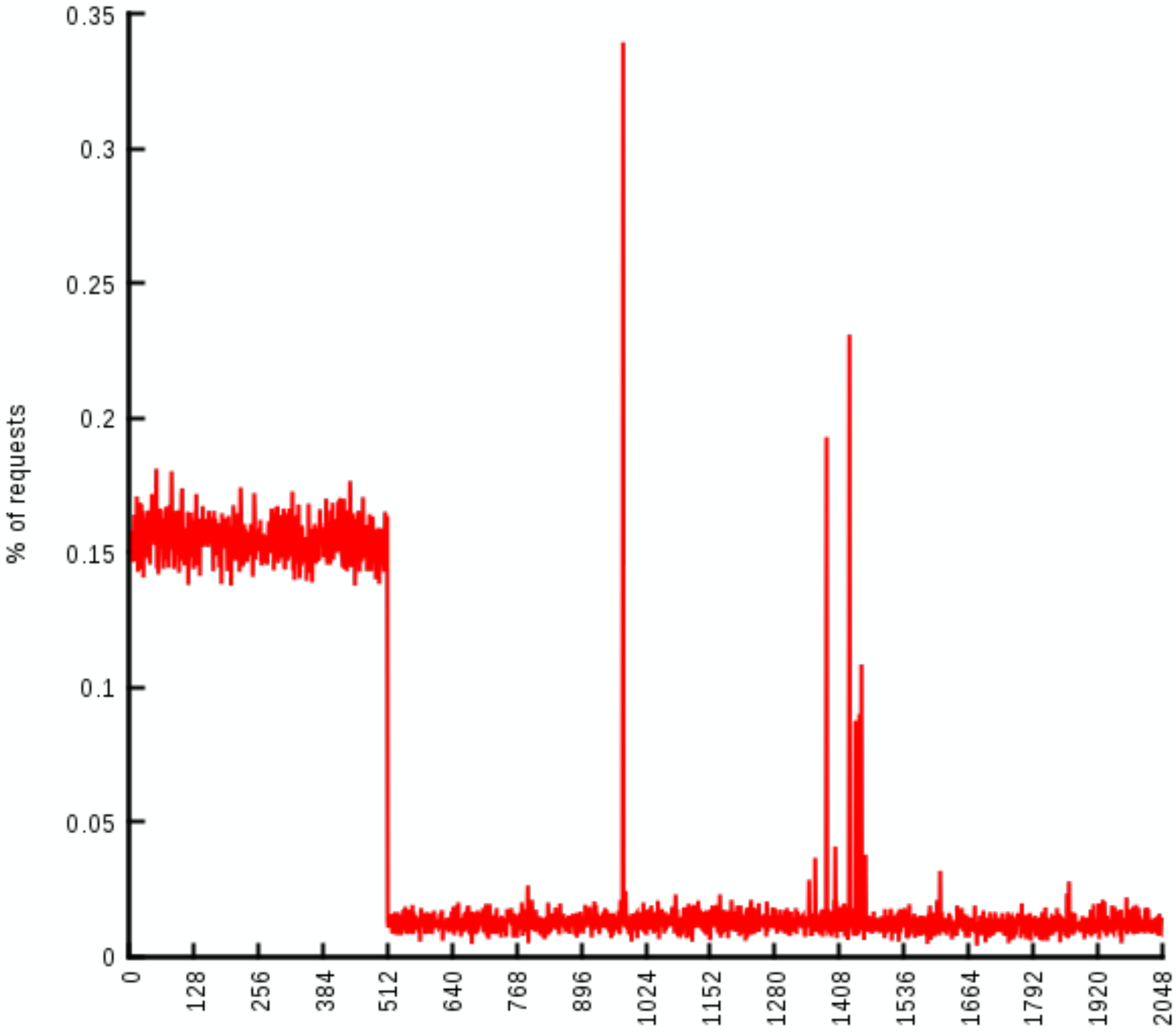
```
grafana=> select count(1) from dashboard;
 count
-------
   645
(1 row)
```

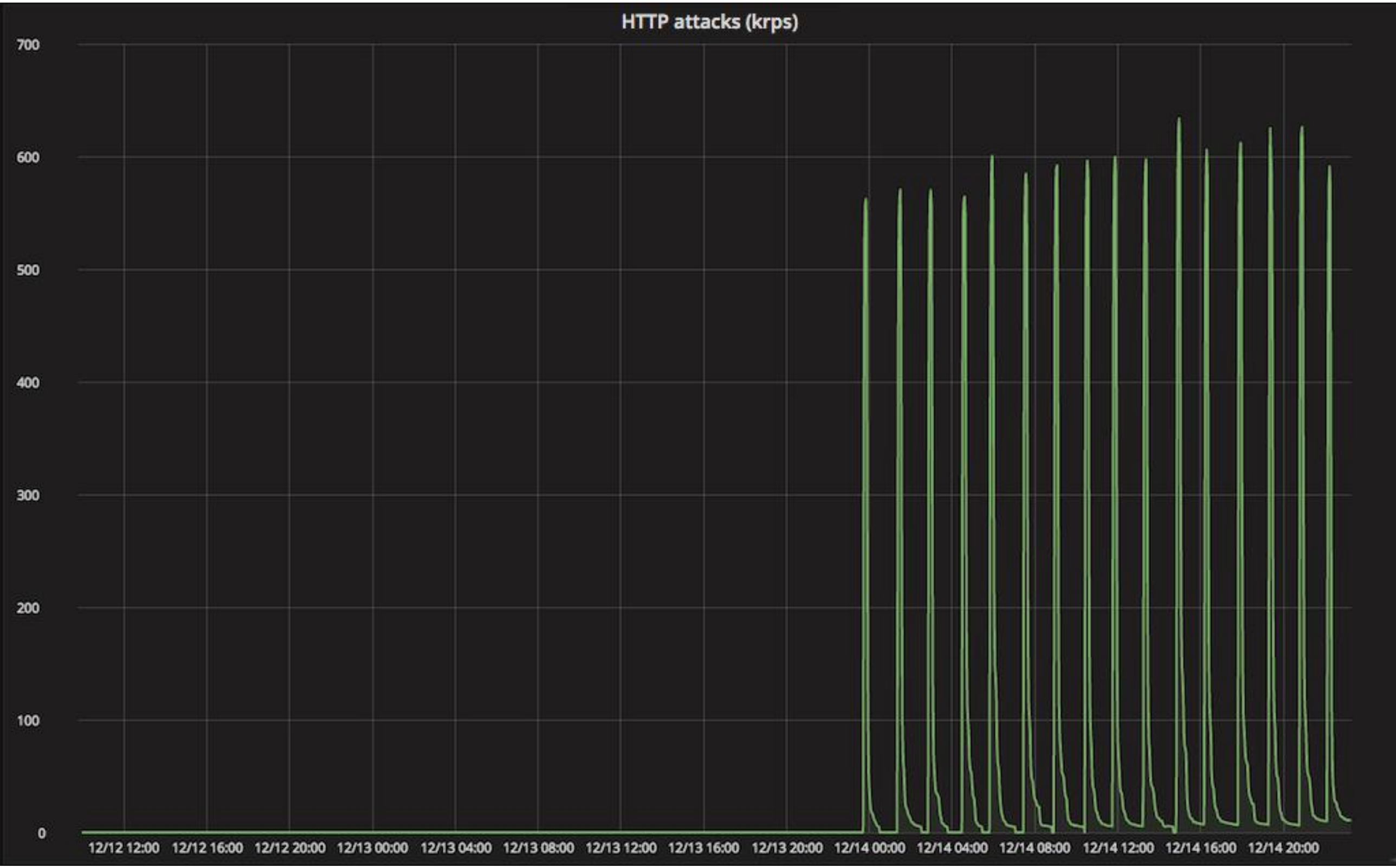
This post is not about our Grafana systems though. It's about something we noticed a few days ago, while looking at one of those dashboards. We noticed this:


HTTP attacks (krps)
900
800
700
600
500
400
300
200
100
0
12/12 12:00
12/12 16:00
12/12 20:00
12/13 00:00
12/13 04:00
12/13 08:00
12/13 12:00
12/13 16:00
12/13 20:00
12/14 00:00
12/14 04:00
12/14 08:00
12/14 12:00
12/14 16:00
12/14 20:00

```
clienip.30460-serverip.00080:
0000: 75a6 cbef 1539 5e82 a7cb f015 3a5e 83a7 ccf0 163a 5f83 a8cc f116 3b5f 84a8 cdf1  u....9^.....:^.....:_.....;_....
0020: 173b 6084 a9cd f217 3c60 85a9 cef2 183c 6185 aace f318 3d61 86aa cff3 193d 6286  .;`.....<`.....<a.....=a.....=b.
0040: abcf f419 3e62 87ab d0f4 1a3e 6387 acd0 f51a 3f63 88ac d1f5 1b3f 6488 add1 f61b  ....>b.....>c.....?c.....?d.....
0060: 4064 89ad d2f6 1c40 6589 aed2 f71c 4165 8aae d3f7 1d41 668a afd3 f81d 4266 8baf  @d.....@e.....Ae.....Af.....Bf..
0080: d4f8 1e42 678b b0d4 f91e 4367                                                    ...Bg.....Cg

serverip.00080-clientip.30460:
0000: 4854 5450 2f31 2e31 2034 3030 2042 6164 2052 6571 7565 7374 0d0a 4461 7465 3a20  HTTP/1.1 400 Bad Request..Date:
0020: 5475 652c 2031 3320 4465 6320 3230 3136 2032 323a 3132 3a31 3420 474d 540d 0a43  Tue, 13 Dec 2016 22:12:14 GMT..C
0040: 6f6e 7465 6e74 2d54 7970 653a 2074 6578 742f 6874 6d6c 0d0a 436f 6e74 656e 742d  ontent-Type: text/html..Content-
0060: 4c65 6e67 7468 3a20 3137 370d 0a43 6f6e 6e65 6374 696f 6e3a 2063 6c6f 7365 0d0a  Length: 177..Connection: close..
0080: 5365 7276 6572 3a20 2d6e 6769 6e78 0d0a 4346 2d52 4159 3a20 2d0d 0a0d 0a3c 6874  Server: -nginx..CF-RAY: -....<ht
00a0: 6d6c 3e0d 0a3c 6865 6164 3e3c 7469 746c 653e 3430 3020 4261 6420 5265 7175 6573  ml>..<head><title>400 Bad Reques
00c0: 743c 2f74 6974 6c65 3e3c 2f68 6561 643e 0d0a 3c62 6f64 7920 6267 636f 6c6f 723d  t</title></head>..<body bgcolor=
00e0: 2277 6869 7465 223e 0d0a 3c63 656e 7465 723e 3c68 313e 3430 3020 4261 6420 5265  "white">..<center><h1>400 Bad Re
0100: 7175 6573 743c 2f68 313e 3c2f 6365 6e74 6572 3e0d 0a3c 6872 3e3c 6365 6e74 6572  quest</h1></center>..<hr><center
0120: 3e63 6c6f 7564 666c 6172 652d 6e67 696e 783c 2f63 656e 7465 723e 0d0a 3c2f 626f  >cloudflare-nginx</center>..</bo
0140: 6479 3e0d 0a3c 2f68 746d 6c3e 0d0a                                               dy>..</html>..
```


0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
% of requests
0
128
256
384
512
640
768
896
1024
1152
1280
1408
1536
1664
1792
1920
2048
Length in bytes


HTTP attacks (krps)
700
600
500
400
300
200
100
0
12/12 12:00
12/12 16:00
12/12 20:00
12/13 00:00
12/13 04:00
12/13 08:00
12/13 12:00
12/13 16:00
12/13 20:00
12/14 00:00
12/14 04:00
12/14 08:00
12/14 12:00
12/14 16:00
12/14 20:00

Porcupine: Profile

- Junk payload L7 attacks
- Pretty large - 1M rps, 200k IP's/h
- Brasil, Algeria, Tunisia, Ukraine
- Attacker: .
- Infection: .

DMYCO®

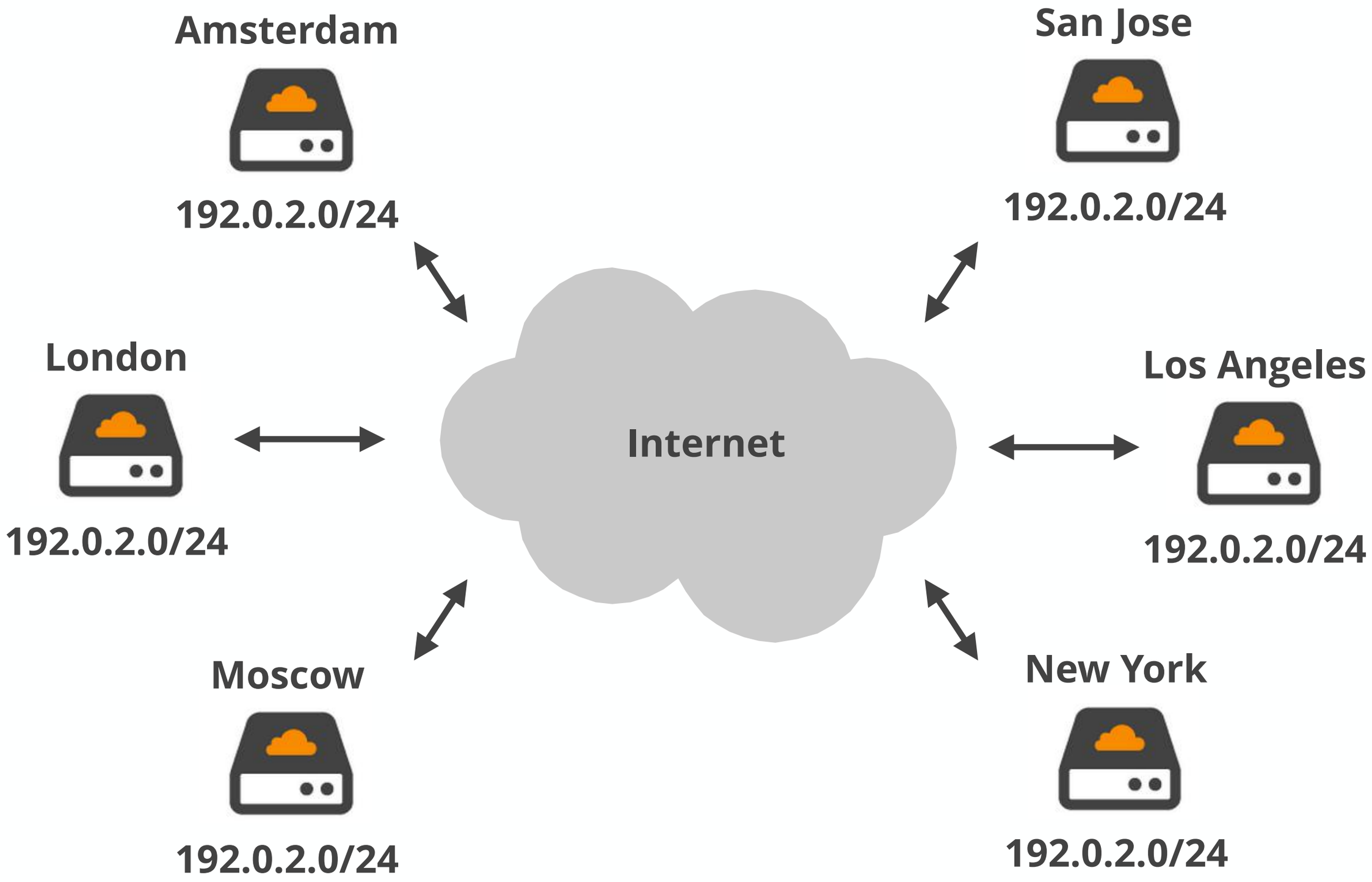
CCCAM EUROPE

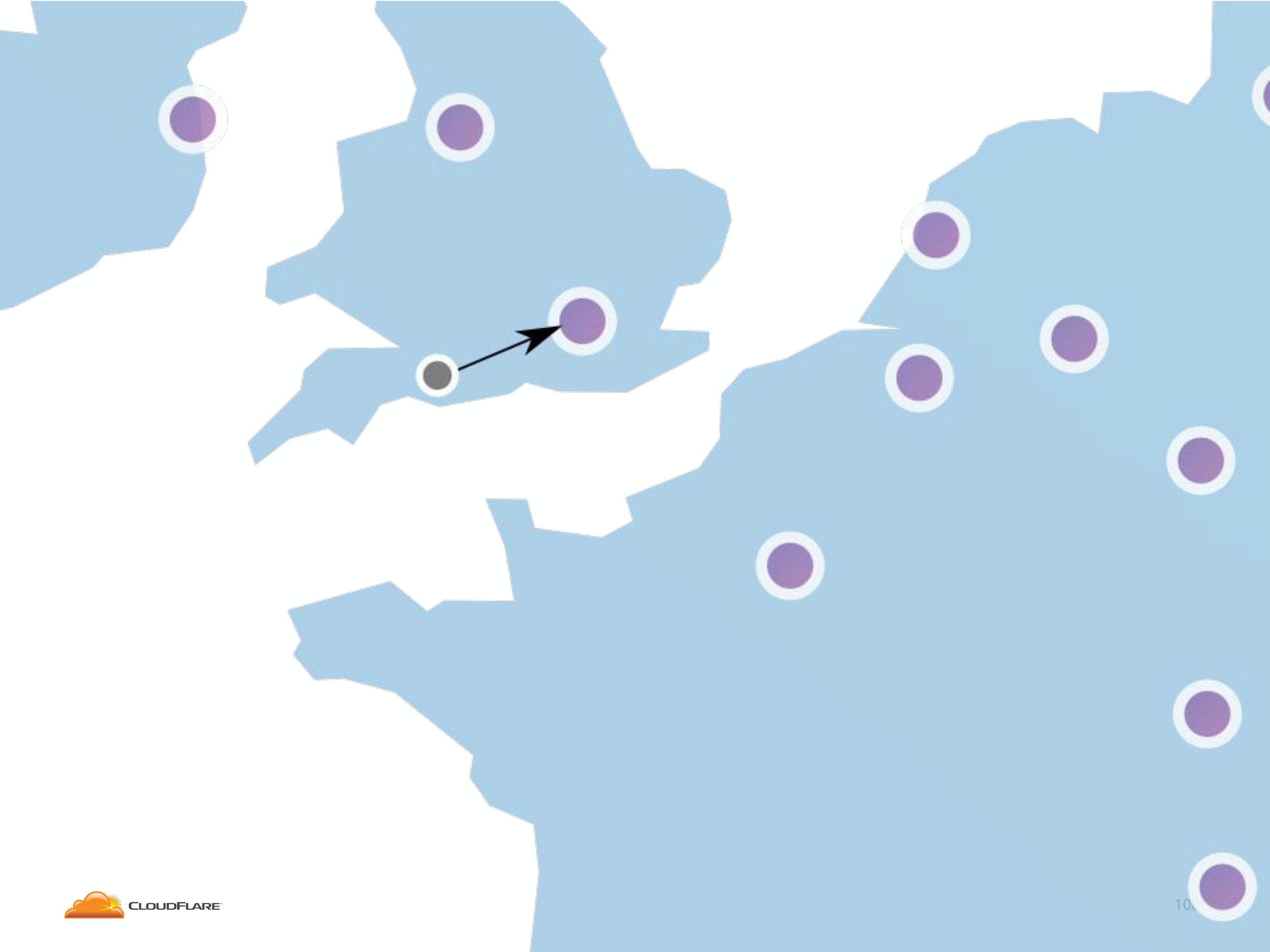
1 Year Europe Cccam

4 Lines Provided

Cloudflare

Anycast Architecture


Amsterdam
192.0.2.0/24
San Jose
192.0.2.0/24
London
192.0.2.0/24
Internet
Los Angeles
192.0.2.0/24
Moscow
192.0.2.0/24
New York
192.0.2.0/24




Berlin
Hamburg
Oslo
Frankfurt
Moscow
Kiev
Milan
Cairo
Zürich
Marseille
Madrid
Dublin
Paris
Sofia
New Delhi
Muscat
Kuwait City
Doha
Dubai
Mumbai
Chennai
Mombasa
Johannesburg
Langfang
Zhengzhou
Jinan
Luoyang
Xi'an
Shijiazhuang
Chengdu
Wuhan
Zhuzhou
Hengyang
Hangzhou
Wuxi
Taipei
Fuzhou
Hong Kong
Dongguan
Foshan
Qingdao
Tokyo
Osaka
Perth
Sydney
Auckland
Vancouver
Seattle
Los Angeles
Phoenix
Denver
Chicago
Dallas
Atlanta
Miami
Ashburn
Medellín
Lima
São Paulo
Valparaíso
Buenos Aires

Divide and conquer

- DNS
  - splits traffic against multiple IPs
- Anycast
  - splits traffic globally
- ECMP
  - splits traffic within datacenter
- Tuned network card
  - splits traffic across CPUs

Automatic Mitigations

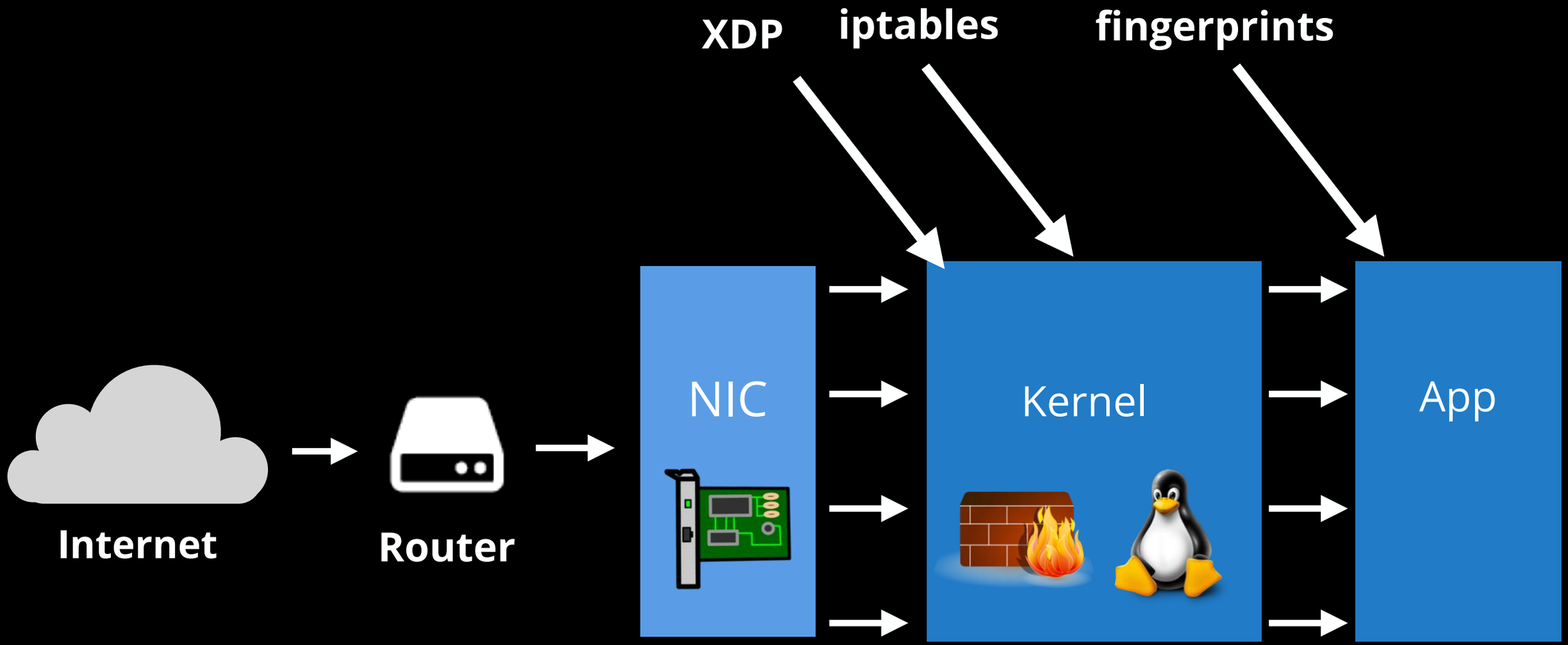
```
iptables -A INPUT \
    --dst 1.2.3.4 \
    -p udp --dport 53 \
    -m bpf --bytecode "14,0 0 0 20,177 0 0 0,12 0 0 0,7
0 0 0,64 0 0 0,21 0 7 124090465,64 0 0 4,21 0 5
1836084325,64 0 0 8,21 0 3 56848237,80 0 0 12,21 0 1
0,6 0 0 1,6 0 0 0" \
   -j DROP
```

```
    ldx 4*([14]&0xf)
    ld #34
    add x
    tax
lb_0:
    ldb [x + 0]
    add x
    add #1
    tax
    ld [x + 0]
    jneq #0x07657861, lb_1
    ld [x + 4]
    jneq #0x6d706c65, lb_1
    ld [x + 8]
    jneq #0x03636f6d, lb_1
    ldb [x + 12]
    jneq #0x00, lb_1
    ret #1
lb_1:
    ret #0
```

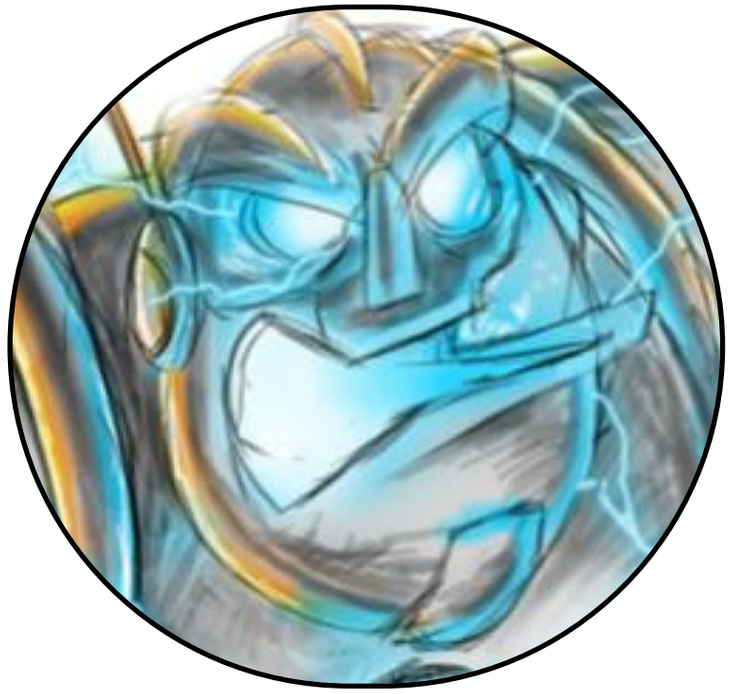
Iptables for application attacks

- Conntrack Connlimit - limit concurrent connections
- Hashlimits - limit rate of connections
  - Rate limit SYN packets per IP
- Ipset - blacklisting of IP addresses
  - Manual blacklisting - feed IP blacklist from HTTP server logs
  - Supports subnets, timeouts
  - Automatic blacklisting hashlimits

CLOUDFLARE


XDP
iptables
fingerprints
NIC
Kernel
App
Internet
Router

Thanks!



- Architected for DDoS
- Iptables are great
- Reduce DNS TTL
- Keep your IoT firmware in check
- Don't install random APKs
- Use 1.1.1.1 resolver :)

marek@cloudflare.com @majek04

CLOUDFLARE