THE SPAMHAUS PROJECT

The role of domains and DNS in large scale abuse

Carel Bitter | ICANN IDS 2019

Let's talk about SMTP

220 emmex.spamhaus.org. ESMTP Postfix (Linux)
HELO definitely.notaspammer.com
250 emmex.spamhaus.org
MAIL FROM: iam@definitely.notaspammer.com
250 Ok
RCPT TO: carel@spamhaus.org
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: iam@definitely.notaspammer.com
To: carel@spamhaus.org
Subject: Fooled you!

Hey Carel,
Buy my stuff at http://definitely.notaspammer.com/offer
.
250 Ok: queued as C2CBD1A5487
QUIT
221 Bye

220 emmex.spamhaus.org. ESMTP Postfix (Linux)
HELO definitely.notaspammer.com
250 emmex.spamhaus.org
MAIL FROM: iam@definitely.notaspammer.com
250 Ok
RCPT TO: carel@spamhaus.org
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: iam@definitely.notaspammer.com
To: carel@spamhaus.org
Subject: Fooled you!

Hey Carel,
Buy my stuff at http://definitely.notaspammer.com/offer
.
250 Ok: queued as C2CBD1A5487
QUIT
221 Bye

```
220 emmex.spamhaus.org. ESMTP Postfix (Linux)
HELO definitely.notaspammer.com
250 emmex.spamhaus.org
MAIL FROM: iam@definitely.notaspammer.com
250 Ok
RCPT TO: carel@spamhaus.org
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: iam@definitely.notaspammer.com
To: carel@spamhaus.org
Subject: Fooled you!

Hey Carel,
Buy my stuff at http://definitely.notaspammer.com/offer
.
250 Ok: queued as C2CBD1A5487
QUIT
221 Bye
```

Domains are excellent filtering hooks

Filtering on domains is well supported and can be deployed during various parts of the process.

Domain-based filtering is precise

By looking at domains we can also deal with bad mail originating from, or forwarded through, legit outbound mail servers.

Authentication catches most forgery

Widely deployed authentication checks make using not-your-own domains hard.

But it boils down to reputation

Reputation is generally attached to domains or FQDNs.

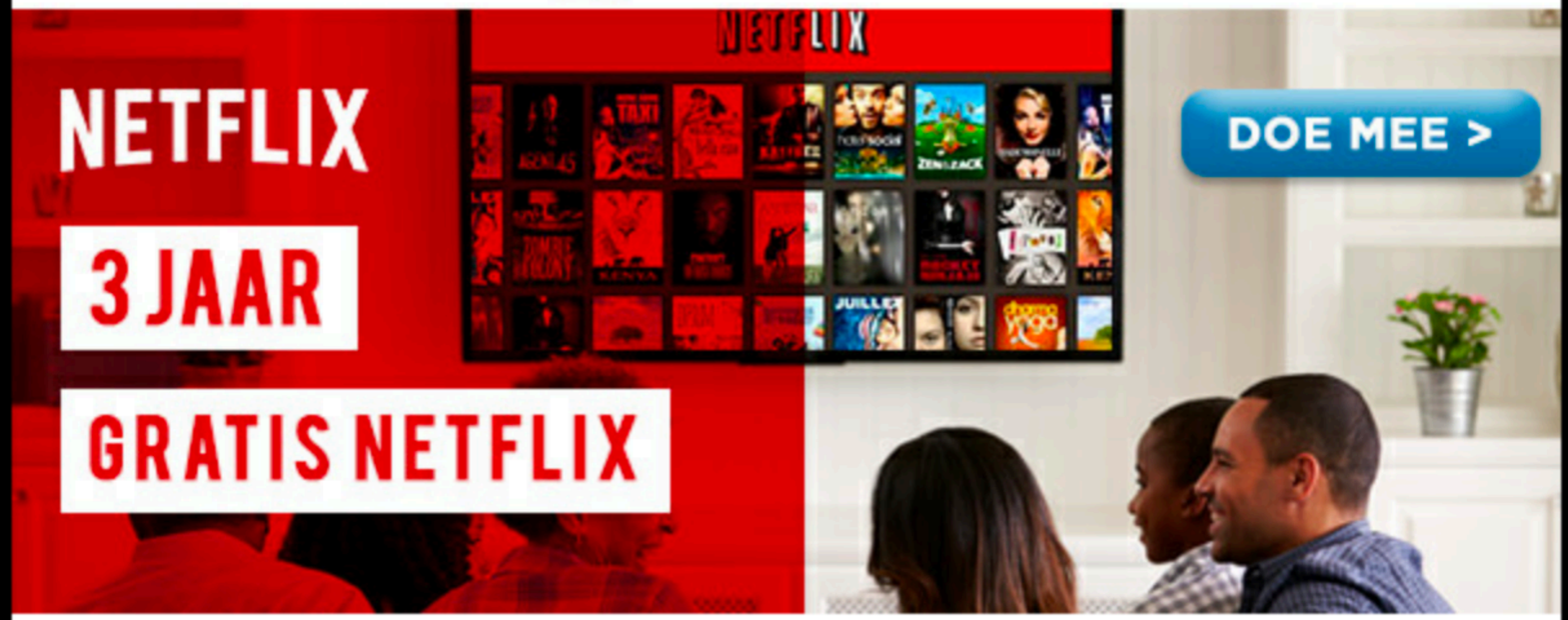
To truly play, you need your own domains. If you do bad things with them, you will need many.

Case 1

Snowshoe type mailer targeting the EU. Sending IP space spread all over, dedicated or VM. Mails fully authenticated.

Casino / dating / streaming

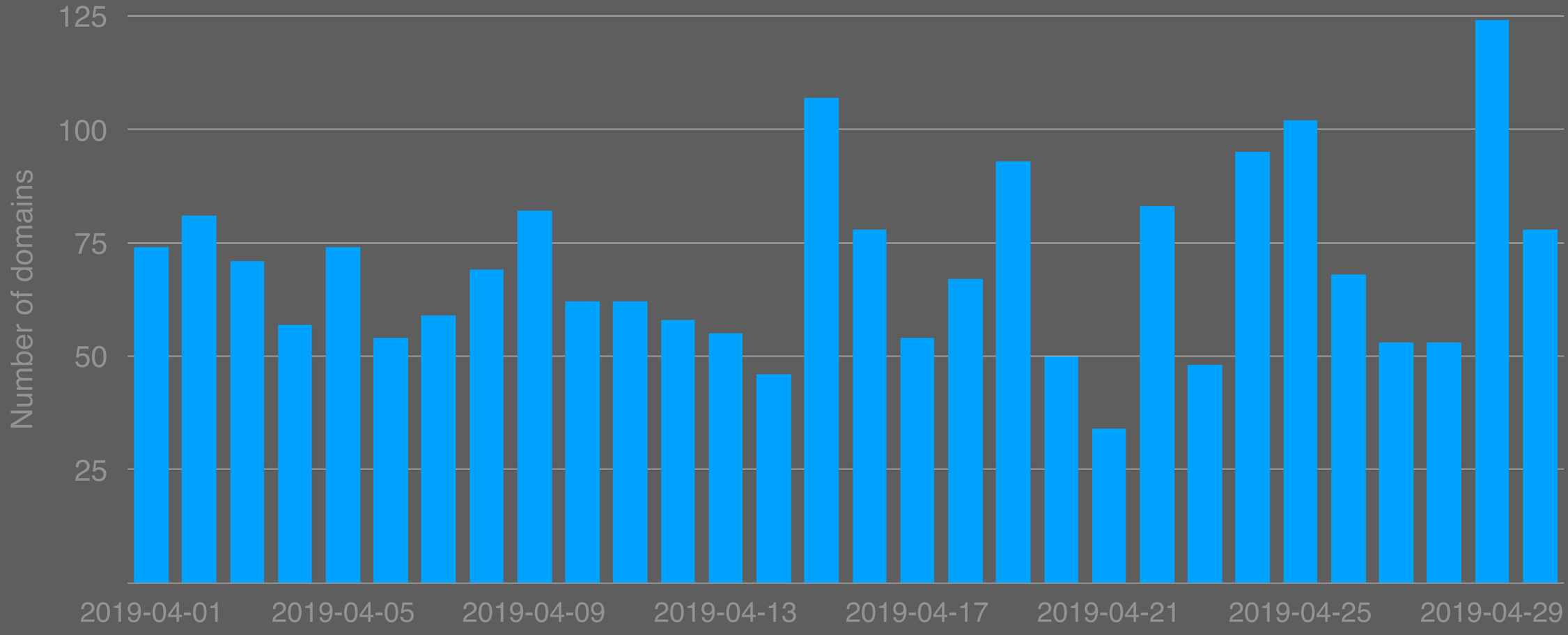
HAPPY BOX



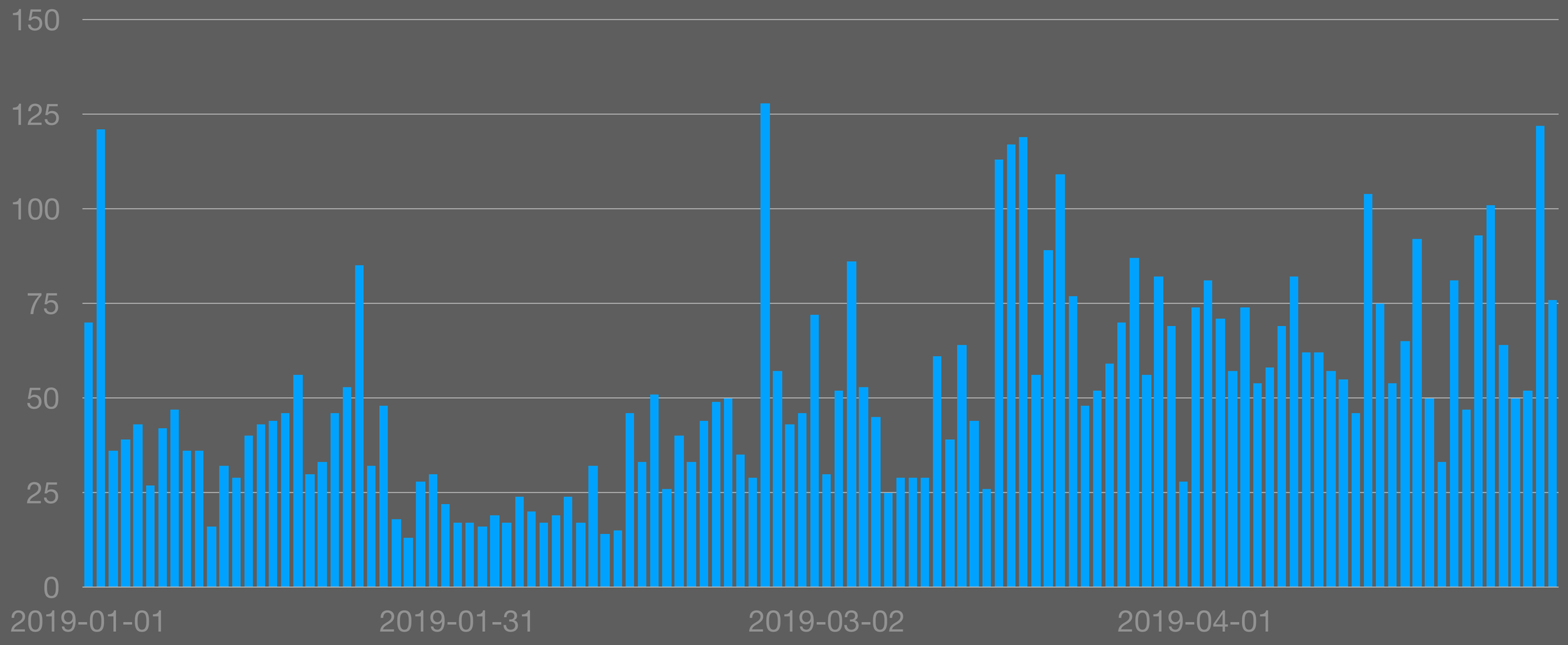
Hi firstname!

Gefeliciteerd! Jij bent een van de kanshebbers om **gratis Netflix toegang te krijgen voor drie jaar!**

Daily domain usage over April 2019 - Unique domains



Daily domain usage over 2019 - Unique domains



6894

Unique domains used in 2019 - at US $5 / domain

A sort of MPD

The number of domains combined with the associated mailing volumes allows the operators to blend in with legit traffic, essentially switching to a new identity whenever one stops working.

Case 1 domain profile

CCTLDs heavily favored

Always using registrar auth NS

Very well partitioned

Domains are aged for a couple of weeks

Registrations lapse on expiry

Like good wine...

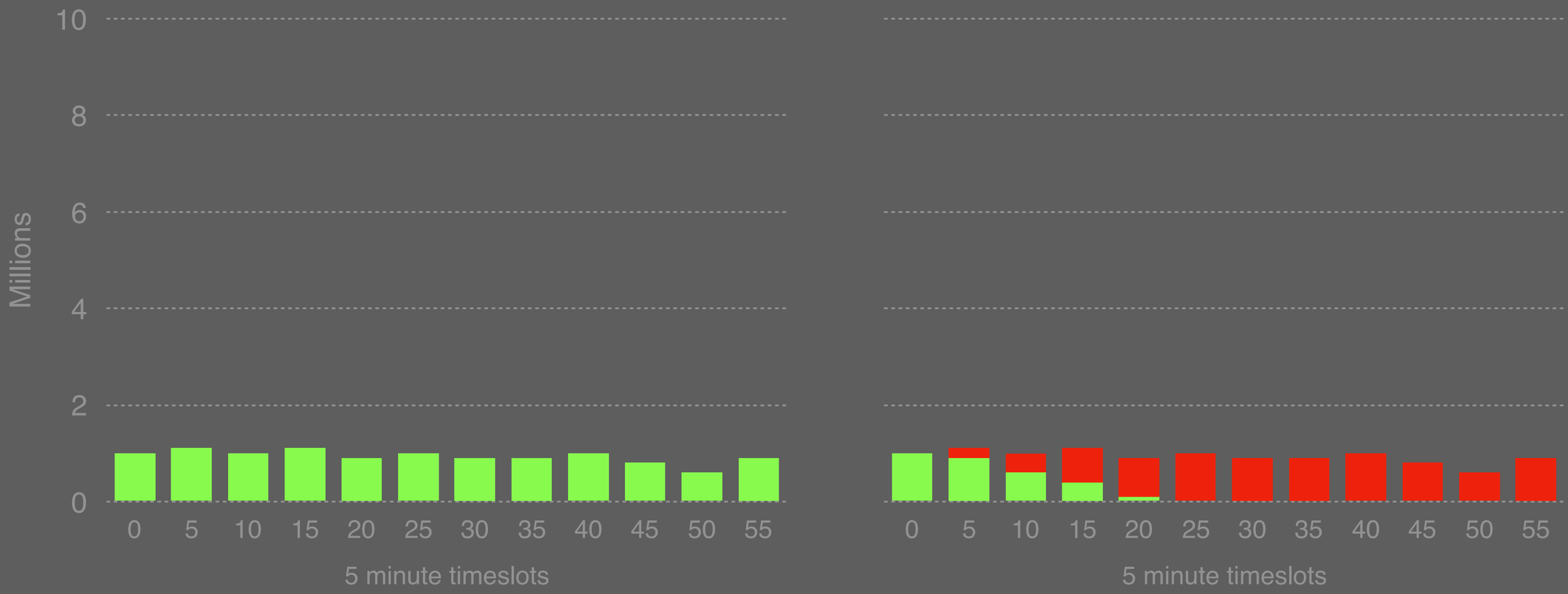
Case 2

Hailstorm type mailer targeting the US. Sending IP space spread all over, prefers a minimum of IPv4 /27, dedicated or VM. Mails fully authenticated.

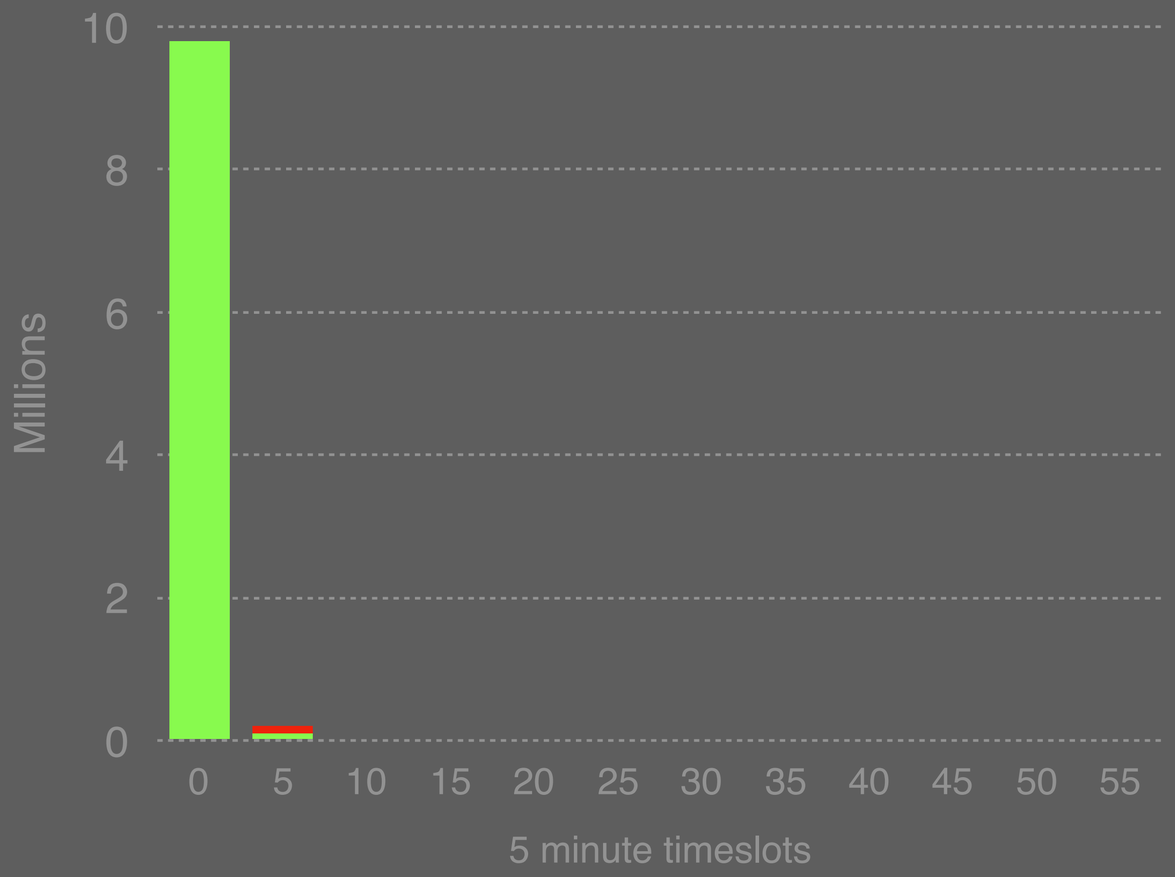
High value leads (Mortgage, insurance, etc)

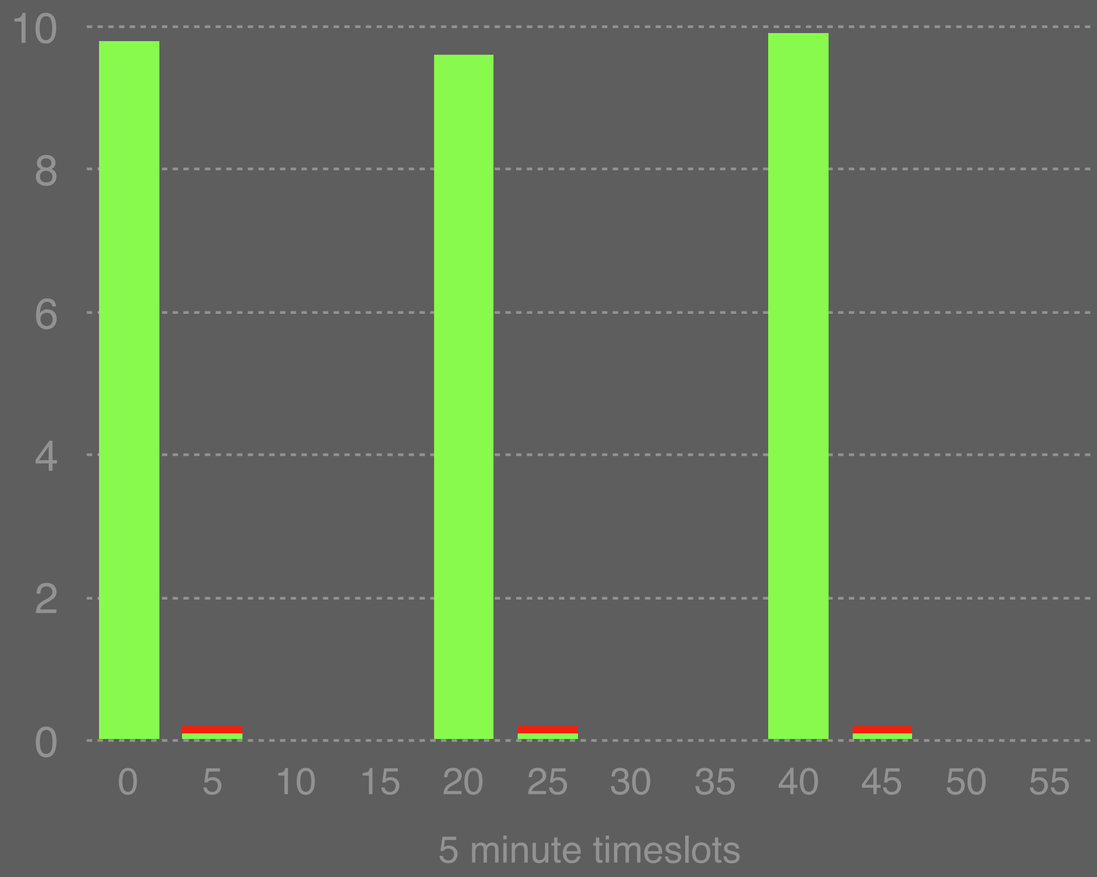
Hailstorm?

Volume vs. time

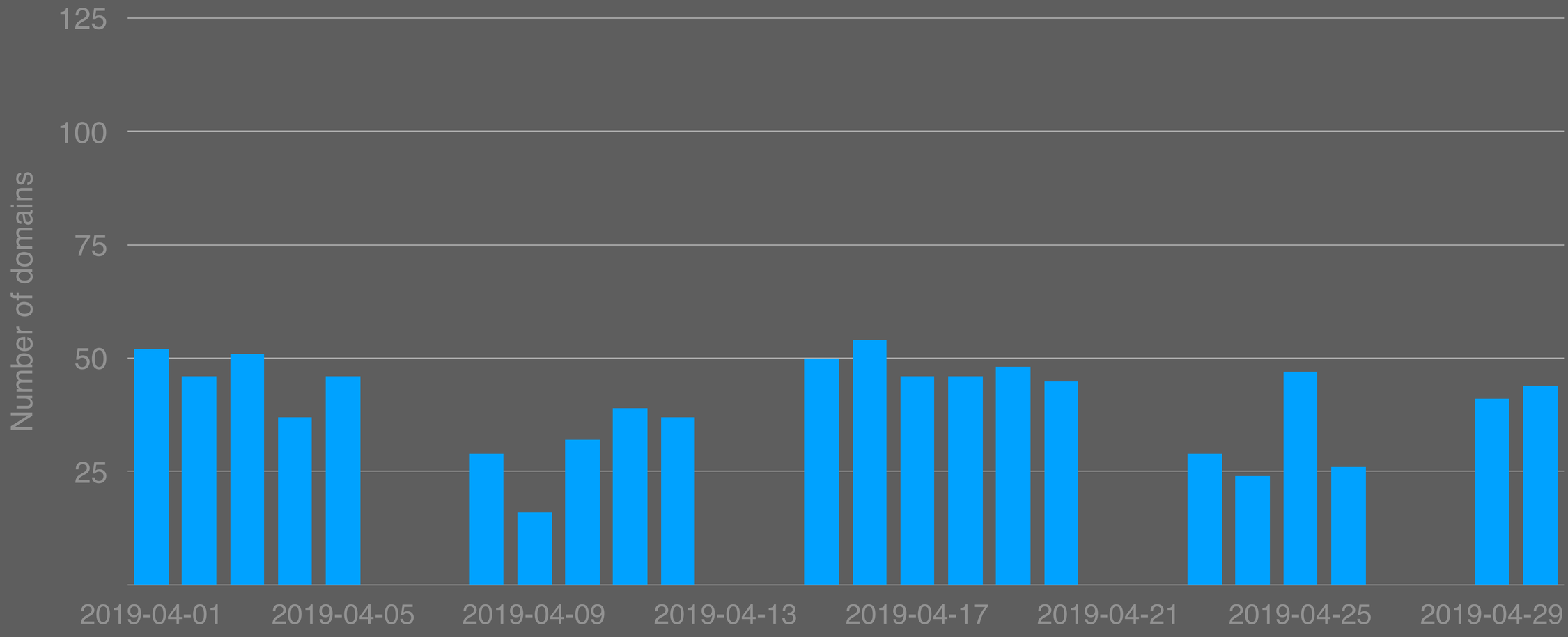


Volume vs. time





Daily domain usage over April 2019 - Unique domains



Some odd artifacts

wwwardashboard.com
wwwrbrall.com
wwwaddfort.com
wwwtheatreticketsdirect.com
wwwjohncoxpaintings.com
wwwsovereignsociety.com
wwwpprbaseball.com
wwwsvarealtors.com

Some odd artifacts

astroworldfest.com

infinitytraininganddevlopment.com

nothmyrtlebeachscvacationsrentals.com

instituteofpositveeducation.com

3825

Unique domains used in 2019 - at ~ US $9 / domain

The benefit of minutes

Extremely short-lived identities make filtering and the correlation between campaigns difficult. While very noisy, as a mailing strategy it seems reasonably succesful.

Case 2 domain profile

.com only

Exclusively second hand domains, 3 registrars

Original registration kept

Self-NS created moments before spam-run

Fire & Forget

Case 3

Botnet spammer using stolen domains. Domains are stolen by getting registrar control panel logins and changing the authorative nameservers.

Dating, cryptocurrencies.

Somewhat fuzzy numbers, but...

ns1.firstdnshoster.com -> 3500+

ns1.fastdnslookup.com -> 7000+

ns1.seconddnshoster.com -> 1800+

Let's talk about authentication

SPF: Which IPs can send mail for $domain.

DKIM: Verify if mail really is from $domain.

DMARC: What to do if authentication fails.

SPF in DNS

"v=spf1 a:mail-out1.spamhaus.org
a:mail-out2.spamhaus.org ~all"

"v=spf1 include:_netblocks.google.com ~all"

"v=spf1 ip4:194.109.24.0/24 ?all"

SPF for botnets - predicted

"v=spf1 ip4:0.0.0.0/0 ~all"

"v=spf1 ip4:0.0.0.0/1 ip4:128.0.0.0/1 ~all"

SPF for botnets - reality

Received: from x-hh1qvvk81.playdaterochester.com
(138-204-199-73.iubtelecom.net.br.[138.204.199.73])
From: YacineaFoucault@x-hh1qvvk81.playdaterochester.com
Subject: Message briskprosp

SPF for botnets - reality

x-hh1qvvk81.playdaterochester.com.
120 IN A 138.204.199.73

Received: from x-hh1qvvk81.playdaterochester.com
(138-204-199-73.iubtelecom.net.br.[138.204.199.73])

x-hh1qvvk81.playdaterochester.com.
120 IN MX 10 mx1.x-hh1qvvk81.playdaterochester.com.
x-hh1qvvk81.playdaterochester.com.
120 IN MX 20 mx2.x-hh1qvvk81.playdaterochester.com.

SPF for botnets - reality

```
$ dig txt x-hh1qvvk81.playdaterochester.com
x-hh1qvvk81.playdaterochester.com.
120 IN TXT   "v=spf1 +ip4:138.204.199.73 -all"

$ dig txt x-hh1qvvk82.playdaterochester.com
x-hh1qvvk82.playdaterochester.com.
120 IN TXT   "v=spf1 +ip4:138.204.199.74 -all"

$ dig txt x-d34db33f.playdaterochester.com
x-d34db33f.playdaterochester.com.
120 IN TXT   "v=spf1 +ip4:107.140.146.15 -all"
```

But how?

```
$ dig version.bind txt chaos @31.148.219.110
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.10.3-P4-Debian <<>> version.bind txt chaos @31.148.219.110
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25032
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available
;; ANSWER SECTION:
version.bind.           120     IN      TXT     "v=spf1 +all"
```

Case 3 domain profile

Any TLD

Domain control taken over from legitimate owner

Control time varies wildy

Custom DNS software to enable abuse

Fire & Forget

This just in (Case 4)

10238 world
2843 us
2661 top
2461 date
1397 biz
875 live
618 nl
562 today
285 com
205 fun

Conclusions

Large domain portfolios are enabling a scale of abuse that would otherwise not be possible.

Registries and registrars have an increasingly important role to play.

Current market conditions favor miscreants.

Thank you!

For domain reputation discussions, things you found in DNS, and any abuse related talk:

carel@spamhaus.org