TPAS - Lab 02 - Reconhecimento

Up201505639 – André Rodrigues

Dominio Escolhido: ***.streamlabs.com (**Logitech)

1)

Registros MX é um recurso usado pelo DNS para implementar rotas de email, para permitir que exista um serviço de email. Um serviço de email usa estes registos para saber onde entregar o email endereçado aquele dominio, especificando para isso um dominio de outro serviço de email. Para evitar loops, o registro MX possui um valor de preferencia (sendo o valor mais baixo, o mais desejado).

No nosso caso o dominio streamlabs.com usa o seu nome para receber email, poupando assim os utilizadores de terem de saber os nomes dos dominios do provedor de email. Streamlabs.com usa o gmail como o seu provedor de email. Ou seja, o gmail tem uma lista dos utilizadores que tenham email cadastrado em streamlabs.com para poder assim entregar os emails correspondentes.

Caso o dominio nao tivesse configurado algum registro MX e mesmo assim teria configurado o seu email para ser afiliado ao gmail, o gmail poderia tentar acessar o registro 'A', no caso do dominio streamlabs.com ser Ipv4 ou o registro 'AAAA' no caso de ser Ipv6 para fazer a entrega dos emails, embora nao seja o ideal e poder levar a emails perdidos. Neste caso está bem configurado.

Para além dos registros MX para determinar onde deixar os emails, deve também ser configurado uma forma de authenticação para garantir a creditação do mensageiro pois sem isso alguém pode-se fazer passar por uma outra pessoa para realizar um ataque de phishing.

Uma forma de autenticação é o SPF ("Sender Policy Framework") que especifica quais os dominios que estão autorizados a enviar emails em nome daquele dominio. Assim o provedor de emails pode, dependendo da forma como for configurado o SPF, descartar o email caso venha de outro dominio para além dos mencionados no ficheiro TXT, ou entao enviar mas com resalvas, entre outros.
Foi escolhido o registro TXT porque ainda se trata de algo provisório e os registro TXT sempre existiram e servem para diversos propositos.

No caso do streamlabs.com temos multipos ficheiros TXT, sendo um deles um ficheiro SPF pois está a ser identificado pela string "v=spf1" e faz uso da tag "include", ou seja, está a referir-se a outros SPF para formarem a configuração do seu SPF.

$ dig MX streamlabs.com

;; ANSWER SECTION:
streamlabs.com. 300 IN MX 10 alt4.aspmx.l.google.com.
streamlabs.com. 300 IN MX 1 aspmx.l.google.com.
streamlabs.com. 300 IN MX 5 alt2.aspmx.l.google.com.
streamlabs.com. 300 IN MX 5 alt1.aspmx.l.google.com.
streamlabs.com. 300 IN MX 10 alt3.aspmx.l.google.com.

$ dig TXT streamlabs.com

;; ANSWER SECTION:
streamlabs.com. 300 IN TXT "google-site-verification=SeAFkBj1x5lLFvQ8xNWooBW7aR1G7u2R6yDjXcy6ETQ"
streamlabs.com. 300 IN TXT "dropbox-domain-verification=flv8vdv9ir3f"
streamlabs.com. 300 IN TXT "AF86E73B3D"
streamlabs.com. 300 IN TXT "v=spf1 include:_spf.google.com include:mail.zendesk.com include:amazonses.com include:spf.braintreegateway.com ~all"
streamlabs.com. 300 IN TXT "google-site-verification=0RAZTLJ4d96HU5R6oNNOTk27tzmL1NTuUUwo_6PzL-Q"

2)

O subfinder utiliza fontes passivas disponiveis online para descobrir subdominios de websites. Podemos obter uma lista dessas fontes executando:

$ subfinder -ls

Para realizar a enumeração de subdomínios de streamlabs.com:

$ subfinder -all -d streamlabs.com

A flag -all serve para usarmos todas as fontes disponiveis.

Resultado: Uma lista de subdominios, 61 em concreto.

3)

O comando "traceroute" mostra o caminho que um pacote tomou até chegar ao seu host. O traceroute envia 3 pacotes por isso é que vemos 3 timestamps para cada "salto".

$ traceroute www.streamlabs.com

traceroute to www.streamlabs.com (104.20.83.218), 30 hops max, 60 byte packets

1

2 * * *

3 telepac15-hsi.cprm.net (195.8.30.246) 9.936 ms telepac16-hsi.cprm.net (195.8.30.250) 10.314 ms 10.509 ms

4 bt-cr1-bu10-200.cprm.net (195.8.30.245) 11.360 ms dvs-cr1-bu10-200.cprm.net (195.8.30.249) 12.284 ms 11.821 ms

5 195.8.0.157 (195.8.0.157) 20.256 ms lis1-cr1-hu11-0-0.cprm.net (195.8.1.65) 40.283 ms 195.8.0.157 (195.8.0.157) 20.472 ms

6 195.8.0.157 (195.8.0.157) 20.628 ms 195.8.10.107 (195.8.10.107) 11.051 ms 195.8.0.157 (195.8.0.157) 9.880 ms

7 www.streamlabs.com (104.20.83.218) 10.571 ms 195.8.10.107 (195.8.10.107) 13.017 ms 13.902 ms

telepac15-hsi.cprm.net (195.8.30.246) -> Europa | Portugal | Lisboa

telepac16-hsi.cprm.net (195.8.30.250) -> Europa | Portugal | Lisboa

bt-cr1-bu10-200.cprm.net (195.8.30.245) -> Europa | Portugal | Lisboa

195.8.0.157 -> Europa | Portugal | Lisboa

lis1-cr1-hu11-0-0.cprm.net (195.8.1.65) -> Europa | Portugal | Lisboa

195.8.10.107 -> Europa | Portugal | Lisboa

www.streamlabs.com (104.20.83.218) -> America do Norte | Estados Unidos | Washington

4)

Instalar golang

$ git clone https://github.com/tomnomnom/httprobe.git

$ go build main.go

$ mv main httprobe

$ subfinder -all -d streamlabs.com > subdominios.txt

$ cat subdominios.txt | ./httprobe > alive.txt

alive.txt:

https://sp-dev.streamlabs.com
http://sp-dev.streamlabs.com
https://r2d2.streamlabs.com
http://r2d2.streamlabs.com
https://platform.streamlabs.com

http://platform.streamlabs.com
https://status.streamlabs.com
https://payments-dashboard.streamlabs.com
http://status.streamlabs.com
https://contenthub-cdn.streamlabs.com
http://payments-dashboard.streamlabs.com
https://merch.streamlabs.com
http://contenthub-cdn.streamlabs.com
https://twitch.streamlabs.com
http://merch.streamlabs.com
https://media.streamlabs.com
https://aws-io.streamlabs.com
http://twitch.streamlabs.com
http://media.streamlabs.com
https://streamlabs.com
https://facebook.streamlabs.com
https://platform-cdn.streamlabs.com
http://streamlabs.com
http://facebook.streamlabs.com
http://platform-cdn.streamlabs.com
https://polly.streamlabs.com
https://sprite.streamlabs.com
http://polly.streamlabs.com
http://sprite.streamlabs.com
https://mixer.streamlabs.com
https://obsstudionodes3.streamlabs.com
http://mixer.streamlabs.com
https://chatbot-io.streamlabs.com
http://obsstudionodes3.streamlabs.com
https://ideas.streamlabs.com
http://chatbot-io.streamlabs.com
https://stats.streamlabs.com
http://ideas.streamlabs.com
https://streamlabels.streamlabs.com
https://facemasks-cdn.streamlabs.com
http://stats.streamlabs.com
https://support.streamlabs.com
http://streamlabels.streamlabs.com
https://sockets.streamlabs.com
http://facemasks-cdn.streamlabs.com
https://io.streamlabs.com
https://sp-cdn.streamlabs.com
https://dev.streamlabs.com
https://chatbot-api.streamlabs.com
http://io.streamlabs.com
http://dev.streamlabs.com
http://support.streamlabs.com
http://sp-cdn.streamlabs.com
https://merchcdn.streamlabs.com
http://chatbot-api.streamlabs.com
https://slobs-cdn.streamlabs.com
https://ext-assets.streamlabs.com

http://merchcdn.streamlabs.com
https://overlays.streamlabs.com
https://howto.streamlabs.com
https://sp.streamlabs.com
http://slobs-cdn.streamlabs.com
http://ext-assets.streamlabs.com
http://overlays.streamlabs.com
http://sp.streamlabs.com
http://howto.streamlabs.com
https://beta.streamlabs.com
https://xt.streamlabs.com
https://aws.streamlabs.com
https://www.streamlabs.com
http://beta.streamlabs.com
http://xt.streamlabs.com
http://aws.streamlabs.com
https://youtube.streamlabs.com
http://www.streamlabs.com
http://youtube.streamlabs.com
https://email-stats.streamlabs.com
http://email-stats.streamlabs.com
https://blog.streamlabs.com
https://cdn.streamlabs.com
http://cdn.streamlabs.com
http://blog.streamlabs.com
http://repo.streamlabs.com

5)

$ ./dirsearch.py -E -u streamlabs.com

$ ./dirsearch.py -e php,html,js -u streamlabs.com

[23:33:03] Starting:
[23:33:04] 301 - 0B - /js -> https://streamlabs.com/js
[23:33:04] 301 - 0B - /html -> https://streamlabs.com/html
[23:33:04] 301 - 0B - /php -> https://streamlabs.com/php
[23:33:11] 301 - 0B - /account/login.shtml -> https://streamlabs.com/account/login.shtml
[23:33:11] 301 - 0B - /accounts/login.shtml -> https://streamlabs.com/accounts/login.shtml
[23:33:11] 301 - 0B - /adm.shtml -> https://streamlabs.com/adm.shtml
[23:33:11] 301 - 0B - /adminphp -> https://streamlabs.com/adminphp
[23:33:11] 301 - 0B - /adminhtml -> https://streamlabs.com/adminhtml
[23:33:11] 301 - 0B - /adminjs -> https://streamlabs.com/adminjs
[23:33:12] 301 - 0B - /admin.shtml -> https://streamlabs.com/admin.shtml
[23:33:12] 301 - 0B - /admin/admin.shtml -> https://streamlabs.com/admin/admin.shtml
[23:33:13] 301 - 0B - /admin_js -> https://streamlabs.com/admin_js
[23:33:15] 301 - 0B - /administration.shtml -> https://streamlabs.com/administration.shtml
[23:33:15] 301 - 0B - /administrator.shtml -> https://streamlabs.com/administrator.shtml

[23:33:17] 301 - 0B - /auth/login.shtml -> https://streamlabs.com/auth/login.shtml
[23:33:17] 403 - 1KB - /blog/wp-content/backups/
[23:33:17] 403 - 1KB - /blog/wp-content/backup-db/
[23:33:17] 403 - 1019B - /blog/wp-login.php
[23:33:17] 403 - 1015B - /blog/wp-login
[23:33:18] 301 - 0B - /cache_html -> https://streamlabs.com/cache_html
[23:33:20] 301 - 0B - /controlpanel.shtml -> https://streamlabs.com/controlpanel.shtml
[23:33:20] 301 - 0B - /core/fragments/moduleInfo.phtml -> https://streamlabs.com/core/fragments/moduleInfo.phtml
[23:33:23] 301 - 0B - /host-manager/html -> https://streamlabs.com/host-manager/html
[23:33:23] 301 - 0B - /index.shtml -> https://streamlabs.com/index.shtml
[23:33:25] 301 - 0B - /login.shtml -> https://streamlabs.com/login.shtml
[23:33:25] 301 - 0B - /logon/logon.shtml -> https://streamlabs.com/logon/logon.shtml
[23:33:25] 301 - 0B - /manager/html -> https://streamlabs.com/manager/html
[23:33:25] 301 - 0B - /members.shtml -> https://streamlabs.com/members.shtml
[23:33:26] 301 - 0B - /myadminphp -> https://streamlabs.com/myadminphp
[23:33:26] 301 - 0B - /myadminhtml -> https://streamlabs.com/myadminhtml
[23:33:26] 301 - 0B - /myadminjs -> https://streamlabs.com/myadminjs
[23:33:26] 301 - 0B - /netadmin.shtml -> https://streamlabs.com/netadmin.shtml
[23:33:26] 403 - 1KB - /nwp-content/plugins/disqus-comment-system/disqus.php
[23:33:29] 301 - 0B - /public_html -> https://streamlabs.com/public_html
[23:33:30] 301 - 0B - /signin.shtml -> https://streamlabs.com/signin.shtml
[23:33:33] 403 - 1013B - /wp-content/
[23:33:33] 403 - 1KB - /wp-content/ai1wm-backups/
[23:33:33] 403 - 1KB - /wp-content/backups-dup-pro/
[23:33:33] 403 - 1012B - /wp-content/plugins/akismet/admin.php

...

Extra

Google Dork é uma técnica usada para encontrar informação indexada pelo google que pode ter sido acidentalmente exposta.

Se os recursos de um website não forem bloqueados, usando um robots.txt por exemplo, o google indexa toda a informação presente no website. Por isso é que qualquer pessoa pode acessar a informação se souberem como e o que pesquisar.

O dominio streamlabs.com tem um ficheiro robots.txt configurado. Onde permite ao google indexar o site completo, excepto os ficheiros, directorios ou subdominios marcados por "Disallow":

User-agent: *
Allow: /
Disallow: /widgets/*
Disallow: /alert-box*
Disallow: /logout*
Disallow: /emoticons/*
Disallow: /slobs/download*
Disallow: /slobs/slobs-download*
Disallow: /streamlabs-obs/login-success*

Disallow: /best-donation-clips/*
Sitemap: https://streamlabs.com/sitemap.xml

No Google:

- allintext:username filetype:log inurl:"https://streamlabs.com/"
- llintext:password inurl:https://streamlabs.com/
- allintext:"Index Of" "cookies.txt" inurl:https://streamlabs.com/
- intitle:"Vulnerability Report" "Critical" ext:pdf inurl:https://streamlabs.com/

Ambas as pesquisas foram insucedidas.