How to work with EZproxy logs in Splunk – a live demonstration

Linda Farrell: linda.farrell@monash.edu

1. Introduction
2. Anonymised dashboard
3. Access from more than one country in the last 7 days
4. Total downloads by users in the last 24 hours
5. Suspicious referrers in the last 7 days
6. Alerts
7. Extra reports

1. Introduction

- At Monash University all access, on campus and off campus, is through EZproxy.
- Monash uses EZproxy logs to gather access statistics and to identify compromised accounts.
- The process after detection of a compromised account:
    - Identify.
    - Block account in EZproxy user.txt.
    - Inform IT security.
    - IT security communicates with user (education).
    - Account password is reset.
    - Unblock when completed by IT security.
- The procedure for excessive downloads:
    - Block account in EZproxy user.txt.
    - Email user (phone staff member where possible).
    - Unblock when satisfactory reply is received via email.
    - If email response raises a concern of a compromised account, compromised account procedure is followed.
- Monash library started using Splunk in August 2017. This document contains a few of Monash's reports and dashboard panels.
- Success with Splunk
    - In 2016 and 2017 each: 25 days of loss of access due to compromised accounts and excessive downloads. In 2018: 0 days of loss of access due to compromised accounts and excessive downloads.
    - IEEE has detected 17 incidents of Sci-Hub activity through Monash in 2017, only 4 so far in 2018. IEEE reports that they have seen an increase at other institutions worldwide.

2. Anonymised dashboard

Linda's EZproxy dashboard (Anon)

Anonymized data for presentation

Edit | Export | ...

EZproxy user access from more than one country or IP (last 7 days)

user	CountryCount	Countries	IPCount	IPs
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	4	Australia China Italy Singapore	15	103.14.185.12 103.14.185.233 117.88.68.14 130.194.236.162 130.194.236.212 130.194.236.243 130.194.236.249 130.194.236.94 130.194.237.106 130.194.237.128 130.194.237.37 31.131.247.138 59.172.155.2 84.18.151.204 93.34.239.56
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	4	Australia Malaysia Mexico Singapore	5	118.139.142.45 128.199.177.201 169.57.0.206 175.136.86.128 60.48.81.28
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	4	Australia Brazil Japan United States	5	137.59.252.149 173.239.230.79 177.234.153.145 185.216.35.67 49.127.159.219
xxxxxxxxxxxxxxxxxxxx	3	Australia Malaysia Singapore	9	118.139.142.112 118.139.142.113 138.75.211.33 175.138.186.211 175.140.158.212 175.141.135.153 175.156.87.150 58.185.74.174 60.50.237.155
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	3	Australia Malaysia New Zealand	8	118.139.142.32 123.136.115.10 123.136.115.124 123.136.115.94 147.158.74.99 161.139.222.166 175.143.31.233 61.6.144.169

« prev 1 2 3 4 5 6 7 8 9 10 next »

Total downloads by users (last 24 hours)

user	TotalDownload	totalGB
xxxxxxxxxxxxxxxxxxxxxxx	331574617	0.3088029259815812
xxxxxxxxxxxxxxxxxxxxxxx	321598115	0.29951158445328474
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	314408126	0.29281538538634777
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	309077981	0.28785130102187395
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	261663092	0.24369274452328682
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	248291457	0.23123943898826838
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	233539850	0.21750093437731266
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	224692369	0.20926107559353113
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	220428327	0.2052898770198226
xxxxxxxxxxxxxxxxxxxxxxx	209427881	0.19504491332918406
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	205118902	0.19103186391294003
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	196663640	0.1831572875380516
xxxxxxxxxxxxxxxxxxx	192515900	0.179294403642416
xxxxxxxxxxxxxxxxxxxxxxx	183405691	0.1708098603412509
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	176126982	0.16403103433549404
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	172112321	0.1602920899167657
xxxxxxxxxxxxxxxxxxx	170265086	0.15857171826064587
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	164067449	0.15279971901327372
xxxxxxxxxxxxxxxxxxx	151157490	0.14077638275921345
xxxxxxxxxxxxxxxxxxxxxxx	147318274	0.1372008342295885

Number of events by sessionid (last 7 days)

sessionID	sessioncnt
15kQLilW3hD7NI9	4334
OkHUSmqjyATnmYe	4268
I7T3dcxg5nJ8vRi	3147
RB4mWRMyvFsGGUQ	2578
Mb1d6Nz1MJTpAKS	2401
idz9MEEDw0hUeCS	2349
ggWGuaoxh2qkicj	2163
CMDr8o0uipGgQdU	2146
P3FhVZk5RoBBU0h	2132
ucEbqCDriM54Gtp	2121
oKpy3yGd6xuatwu	2045
CugSldTZ8hTGCSA	2044
EiTzBh1pi13Z7An	1761
RrHtSHMxPnf6Mlk	1702
ajDdoOG3oPo0Ziv	1683
je0ZFElKRPmPmnJ	1669
cxSUsSwK0qqwLQS	1584
kfHeNNu4e9siqfU	1566
w1SZgZIQNUf0fc3	1564
ujLV2VZliAQzzWx	1541

Number of sessions per user (last 7 days)

user	sessioncnt
xxxxxxxxxxxxxxx	59
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	49
xxxxxxxxxxxxxxxxxxxxxxxxxxxxx	45
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	44
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	44
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	43
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	43
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	42
xxxxxxxxxxxxxxxxxxxxxxxx	41
xxxxxxxxxxxxxxxxxxxxxxxx	41

« prev 1 2 next »

Suspicious Referers (last 7 days)

timestamp	ip	user	Referer
25/May/2018:02:43:33 +1000		xxxxxxxxxxxxxxxxxxxxxxx	http://sci-hub.tw/
23/May/2018:16:41:16 +1000		xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	https://sci-hub.hk/
23/May/2018:13:11:24 +1000		xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	https://scholar-google-com-au.ezproxy.lib.monash.edu.au/scholar?hl=zh-CN&as_sdt=0%2C5&q=+http%3A%2F%2Fsci-hub.tw%2Fhttps%3A%2F%2Fdoi.org%2F10.3390%2Fcatal8050196&btnG=
22/May/2018:21:24:03 +1000		xxxx	http://www.so.com/s?src=new_isearch&q=Googl
22/May/2018:06:38:38 +1000		xxxxxxxxxxxxxxxxxx	http://sci-hub.tw/http://scripts.iucr.org/cgi-bin/paper?S1600577517017568
21/May/2018:14:43:29 +1000		xxxxxxxxxxxxxxxxxxxxxxx	https://sci-hub.tw/

3. Access from more than one country in the last 7 days

```
index="app_ezproxy" source="/srv/home/ezproxy-production/ezproxy.log" user!="-" | iplocation clientip |
   stats values(clientip) as IPs dc(Country) as CountryCount values(Country) as Countries dc(clientip) as
   IPCount by user |search IPCount>1  |fields user, CountryCount, Countries, IPCount, IPs |eval user
   =replace(user,".","xxxx")|sort -CountryCount, -IPCount, -Countries
```

Last 7 days

✓ 8,113,297 events (29/05/2018 13:00:00.000 to 05/06/2018 13:58:53.000) No Event Sampling Job Fast M

Events | Patterns | Statistics (7,807) | Visualization

100 Per Page | Format | Preview

< Prev 1 2 3 4 5 6 7 8 9 ...

user	CountryCount	Countries	IPCount	IPs
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	4	Australia Canada Sweden United States	4	159.89.41.154 209.97.168.10 49.127.52.89 79.142.76.128
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	3	Australia China Philippines	10	112.198.100.24 114.224.247.182 119.94.176.107 130.194.164.102 130.194.236.13 130.194.236.162 202.90.138.107 210.213.241.242 220.239.8.92 49.127.65.206
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	3	Hong Kong Japan United States	9	104.237.86.199 104.237.86.44 104.237.86.79 104.237.91.129 104.237.91.14

4. Total downloads for the last 24 hours

```
index="app_ezproxy" source="/srv/home/ezproxy-production/ezproxy.log" user!="-" |stats sum(bytes) as
   TotalDownload by user |eval totalGB = TotalDownload/1024/1024/1024 |sort 20 -totalGB |eval user
   =replace(user,".","xxxx")
```

Last 24 hours

✓ 1,269,905 events (04/06/2018 13:00:00.000 to 05/06/2018 13:58:53.000) No Event Sampling Job Fast Mode

Events | Patterns | Statistics (20) | Visualization

100 Per Page | Format | Preview

user	TotalDownload	totalGB
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	1030560827	0.9597845626994967
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	860863562	0.8017416689544916
xxxxxxxxxxxxxxxxxxxx	605714430	0.564115522429347
xxxxxxxxxxxxxxxxxxxxxxx	470551321	0.4382350677624345
xxxxxxxxxxxxxxxxxxxxxxxxxxx	454417657	0.4232094222679734
xxxxxxxxxxxxxxx	373096813	0.34747348446398973
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	353603267	0.32931870501488447
xxxxxxxxxxxxxxxxxxxxxx	332351132	0.30952611193060875
xxxxxxxxxxxxxxxxxxxxxxxxxxx	331596754	0.3088235426694155
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	325789436	0.30341505631804466
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	281701712	0.26235516369342804
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	271648234	0.25299213267862797
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	264358552	0.24620308727025986
xxxxxxxxxxxxxxxxxxxxxx	258543036	0.24078696593642235

5. Suspicious referrers in the last 7 days

This query uses the referrers as recorded by Paul Butler:
https://github.com/prbutler/EZProxy_IP_Blacklist

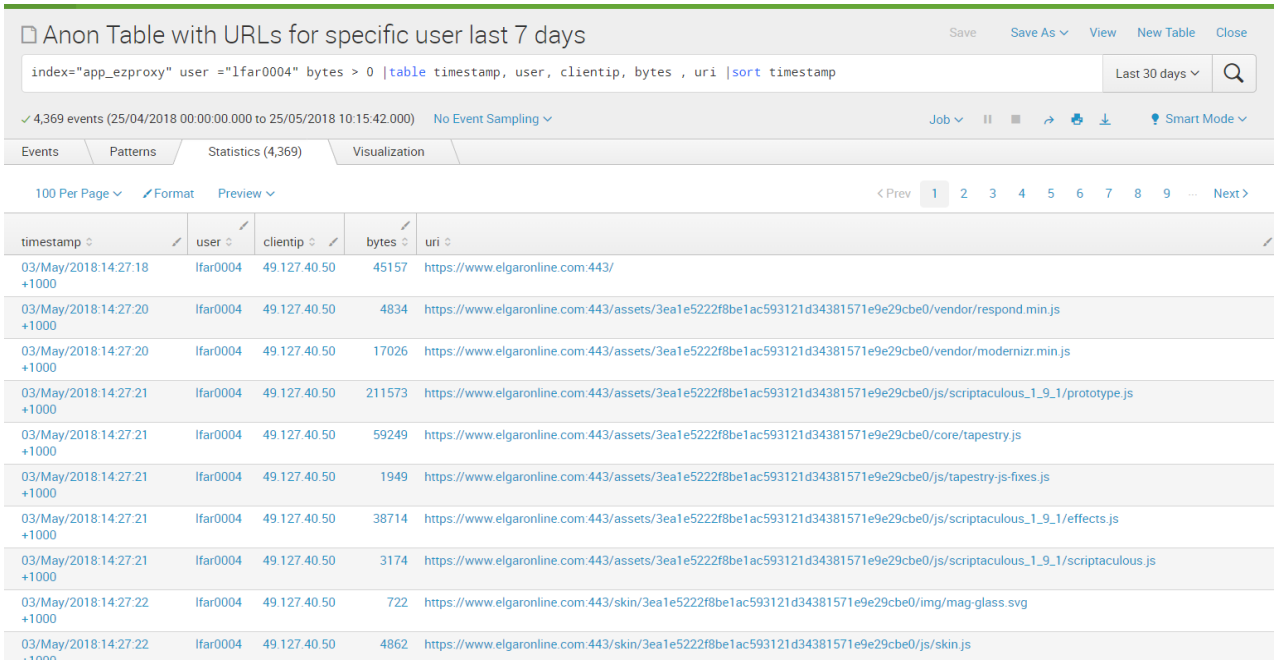
6. Alerts

Alerts can be set up by using any Splunk query or report. At Monash one such alert is set up to send an email when IEEE's activity tracker is detected in the logs. The alert will soon be enhanced to call a script which will add the line of code to the user.txt to automatically block the account. Other alerts in use at Monash are available on request.

7. Other reports

Other reports used by the team to further investigate issues arising from the dashboard:

- URLs accessed by a specific user



Anon Table with URLs for specific user last 7 days

Save | Save As | View | New Table | Close

```
index="app_ezproxy" user ="lfar0004" bytes > 0 |table timestamp, user, clientip, bytes , uri |sort timestamp
```

Last 30 days

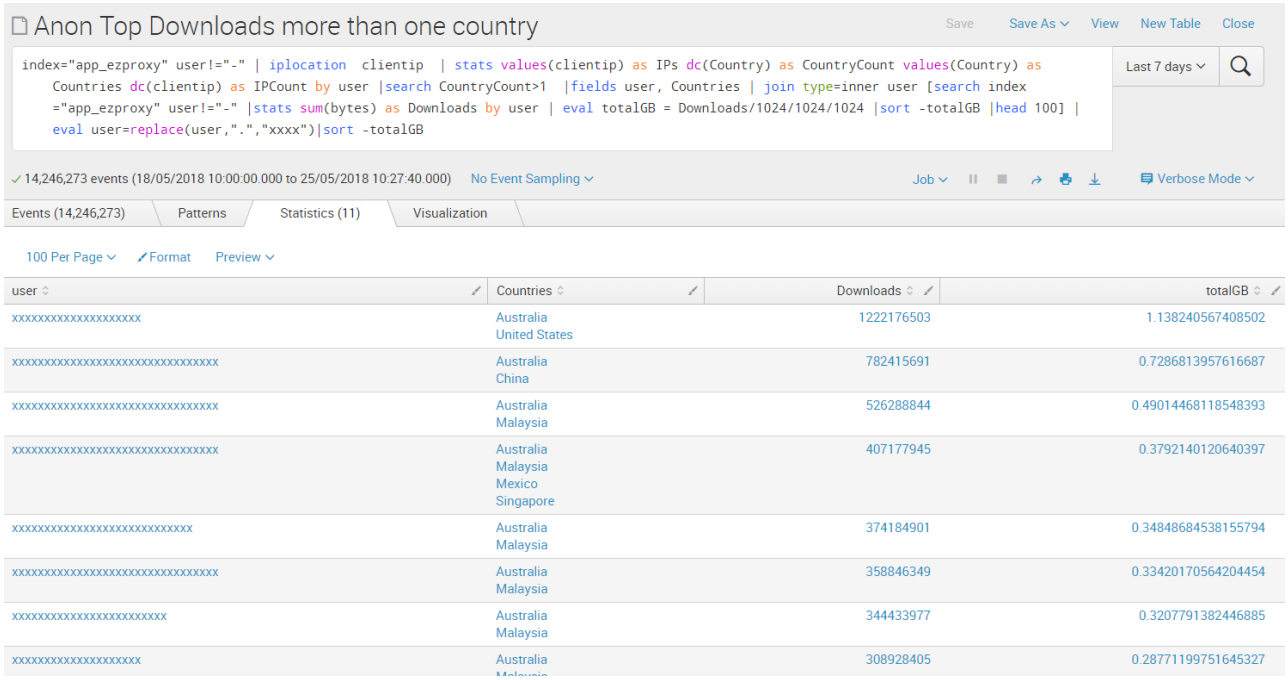
✓ 4,369 events (25/04/2018 00:00:00.000 to 25/05/2018 10:15:42.000) No Event Sampling | Job | Smart Mode

Events | Patterns | Statistics (4,369) | Visualization

100 Per Page | Format | Preview | Prev 1 2 3 4 5 6 7 8 9 Next

timestamp	user	clientip	bytes	uri
03/May/2018:14:27:18 +1000	lfar0004	49.127.40.50	45157	https://www.elgaronline.com:443/
03/May/2018:14:27:20 +1000	lfar0004	49.127.40.50	4834	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/vendor/respond.min.js
03/May/2018:14:27:20 +1000	lfar0004	49.127.40.50	17026	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/vendor/modernizr.min.js
03/May/2018:14:27:21 +1000	lfar0004	49.127.40.50	211573	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/js/scriptaculous_1_9_1/prototype.js
03/May/2018:14:27:21 +1000	lfar0004	49.127.40.50	59249	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/core/tapestry.js
03/May/2018:14:27:21 +1000	lfar0004	49.127.40.50	1949	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/js/tapestry-js-fixes.js
03/May/2018:14:27:21 +1000	lfar0004	49.127.40.50	38714	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/js/scriptaculous_1_9_1/effects.js
03/May/2018:14:27:21 +1000	lfar0004	49.127.40.50	3174	https://www.elgaronline.com:443/assets/3ea1e5222f8be1ac593121d34381571e9e29cbe0/js/scriptaculous_1_9_1/scriptaculous.js
03/May/2018:14:27:22 +1000	lfar0004	49.127.40.50	722	https://www.elgaronline.com:443/skin/3ea1e5222f8be1ac593121d34381571e9e29cbe0/img/mag-glass.svg
03/May/2018:14:27:22 +1000	lfar0004	49.127.40.50	4862	https://www.elgaronline.com:443/skin/3ea1e5222f8be1ac593121d34381571e9e29cbe0/js/skin.js

- Top downloads from more than one country



Anon Top Downloads more than one country

Save | Save As | View | New Table | Close

```
index="app_ezproxy" user!="-" | iplocation clientip | stats values(clientip) as IPs dc(Country) as CountryCount values(Country) as
    Countries dc(clientip) as IPCount by user |search CountryCount>1 |fields user, Countries | join type=inner user [search index
    ="app_ezproxy" user!="-" |stats sum(bytes) as Downloads by user | eval totalGB = Downloads/1024/1024/1024 |sort -totalGB |head 100] |
    eval user=replace(user,".","xxxx")|sort -totalGB
```

Last 7 days

✓ 14,246,273 events (18/05/2018 10:00:00.000 to 25/05/2018 10:27:40.000) No Event Sampling | Job | Verbose Mode

Events (14,246,273) | Patterns | Statistics (11) | Visualization

100 Per Page | Format | Preview

user	Countries	Downloads	totalGB
xxxxxxxxxxxxxxxxxx	Australia United States	1222176503	1.138240567408502
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Australia China	782415691	0.7286813957616687
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Australia Malaysia	526288844	0.49014468118548393
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Australia Malaysia Mexico Singapore	407177945	0.3792140120640397
xxxxxxxxxxxxxxxxxxxxxxxxxxxx	Australia Malaysia	374184901	0.34848684538155794
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Australia Malaysia	358846349	0.33420170564204454
xxxxxxxxxxxxxxxxxxxxxxxx	Australia Malaysia	344433977	0.3207791382446885
xxxxxxxxxxxxxxxxxx	Australia	308928405	0.28771199751645327

- Number of sessions by user

Anon Number of sessions per user

Save | Save As | View | New Table | Close

```
index="app_ezproxy" source="/srv/home/ezproxy-production/ezproxy.log" |stats dc(sessionID) as sessioncnt by user | sort by sessioncnt desc
    |head 20|eval user=replace(user,".","xxxx")
```

Last 7 days

✓ 19,551,675 events (18/05/2018 10:00:00.000 to 25/05/2018 10:27:32.000) No Event Sampling

Job | Fast Mode

Events | Patterns | Statistics (20) | Visualization

100 Per Page | Format | Preview

user	sessioncnt
xxxxxxxxxxxxxxx	59
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	49
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	45
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	44
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	43
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	43
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	43
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	42
xxxxxxxxxxxxxxxxxxxxxxxx	41
xxxxxxxxxxxxxxxxxxxxxxxx	41
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	40

- Number of events by session id

Anon Number of events by sessionid

Save | Save As | View | New Table | Close

```
index="app_ezproxy" source="/srv/home/ezproxy-production/ezproxy.log" bytes > 1000|stats count as sessioncnt by sessionID  |sort -sessioncnt
    |head 20
```

Last 7 days

✓ 8,640,688 events (Partial results for 18/05/2018 10:00:00.000 to 25/05/2018 10:27:31.000) No Event Sampling

Job | Fast Mode

Events | Patterns | Statistics (20) | Visualization

100 Per Page | Format | Preview

sessionID	sessioncnt
15kQLiIW3hD7NI9	4334
OkHUSmqjyATnmYe	4133
I7T3dcxg5nJ8vRi	3091
RB4mWRMyvFsGGUQ	2578
Mb1d6Nz1MJTpAKS	2401
idz9MEEDw0hUeCS	2349
ggWGuaoxh2qkicj	2163
CMDr8o0uipGgQdU	2146
ucEbqCDriM54Gtp	2121
CugSIdTZ8hTGCSA	2044
P3FhVZk5RoBBU0h	1977
oKpy3yGd6xuatwu	1840
EiTzBh1pi13Z7An	1761
RrHtSHMxPnf6Mlk	1690