100 million secrets

a dive into recent password dumps: what's YOUR secret?

warning – adult language and themes

- passwords often contain adult language
- sometime they say some pretty messed up stuff
- the REALLY bad stuff was removed


believeinyourself
ikilledaman
blowupyourcar
mysisterf*cksme
cheatinghusband
imbroken
myfucknfirebirdrocksyourworld

what's a secret?

- something known only to yourself or few
- something you probably wouldn't share publicly

Sometimes, people choose secrets as their passwords. This is an examination of those secrets.

be warned: adult languages/themes

whoami

- nyxgeek
- pentester for TrustedSec
- password cracking 24/7

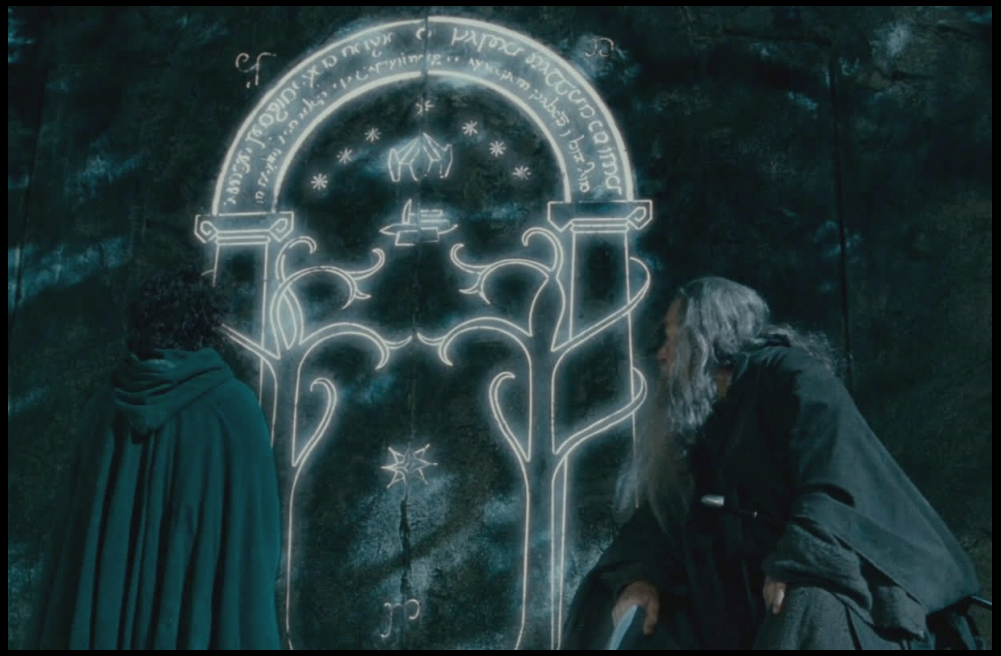
- hackermaps.org

- @nyxgeek

passwords = love

- kind of obsessed
- cracking rigs = hacker hotrods

- cracking passwords has some magic to it
  - words of power
  - Gandalf



Pictured: Gandalf Brute-Forcing a Password

passwords

- Secret by nature
- Passwords are both ancient (abracadabra), and modern
- Secrets, mantras, hidden desires, hatreds and aspirations
  - Important / memorable people, objects, events
  - Sometimes revealing
  - Repetitive nature - reminder

password sources

- Data breaches– leaked hashdumps, or plaintext
- Can complicate giving a talk on this topic
- Efforts made to remove identifying traits:
  - all passwords have been lowercased
  - only alpha and/or common l33tsp34k shown
    - For our purposes, the message is what's important
    - Not a statistical analysis

- Luckily, a perfect source for this talk came along…

Troy Hunt releases megadump

- Troy Hunt released collection of hashes from ’Have I Been Pwned’
- Cracking community promptly solved many of these
- Wordlists available to download online (no cracking required)

notes on Troy's massive dump

- 300 million + entries
  https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/

- passwords are from a variety of sources
  - questionable origins – unknown all who/when/how
  - assumption is that most were real at one time

- passwords lack context
  - at best, small phrases
  - usually just a word

- ambiguity – no usernames attached
  - Password is 'bobswife'
  - Depending on source, could be Bob's wife
  - Could be someone else who likes or dislikes Bob's wife

examining Troy's humungous dump

- it’s not just hashes
- a LOT of garbage is mixed in
  - partial email addresses
  - hash inception
  - LOTS of repeating unicode
- More about it noted in CynosurePrime's write-up

  https://cynosureprime.blogspot.com/2017/08/320-million-hashes-exposed.html

pro tip: review your wordlists

- Lots of free wordlists have garbage lines mixed in
- Garbage lines = wasted cycles, wasted time

dump scrubbing 101

- look for really long strings
  - garbage strings are common
  - some intentional wordlist inflation, some accidental

  ```
  grep -x '.\{24,\}'
  ```

- try removing unicode
  - scrub extended unicode
  - depends on what you're analyzing

- your brain is really good at pattern recognition
  - skim wordlists by hand
  - view sorted in different ways

- removed common domains / email addresses

l33t h4x0r tools

- grep – our primary tool. 'man grep'
- sed – replace elements of text
- awk – manipulate text
- tr – replace or delete characters from text
- comm – compare 2 lists, show lines that are in one but not the other

- REGEX!

locating passwords - goals

- Identify phrases, ideas, trends
- Not so interested in creating password rules from data
- Keyword count examines POPULARITY, not positive/negative views
  - stupiddragons
  - awesomedragons
  - dragonsareokay

- Some restrictions apply:
  - Some words are too short -- high noise:signal ratio
  - Regex only goes so far
  - Lots of data to parse
  - Limited scope to English words

methodology

- Method #1: grep for alpha strings (‘[a-zA-Z]{6,}’)
  - Only matches alpha portions of strings
  - 300m entries -> 180m entries
  - Cleanest results
  - Easiest to analyze
- Method #2: convert wordlist into regex for l33tsp34k
  - Hacks -> [#Hh][aA4@][cC(][kK][sS$5]
  - Good for targeted searches
  - Didn't add much value compared to Method #1
  - A lot more post-processing / complexity than Method #1
- Extra Checks:
  - Credit Card # Search -> Luhn Verification, Card Type Identification
  - Address Regex

other techniques

- Wordlists + grep
  - English dictionary – TOO BIG
  - Wiki Top 100k words
  - Keyword sets
  - Keywords -> l33t regex
- Lots of scrolling/watching cracked passwords
- Sort by line length – look at longest to find phrases
- Word counts (uniq -c)
- Locating phrases programmatically
  - Cutting chars 1-10 | sort | uniq –c | sort –nr

Plain vs l33tsp34k – by the numbers

How popular is the oft-cited l33tsp34k p@ssw0rd?

Word #1(plain):	password		58477
Word #1(l33t):	[pP][aA4@][sS$5][sS$5][wW][oO0][rR][dD)]		71192
		Diff	12715
Word #2(plain):	baseball		13775
Word #2(l33t):	[bB8][aA4@][sS$5][eE3][bB8][aA4@][lL1!][lL1!]		14552
		Diff	777
November (plain):	november		10168
November (l33t):	[nN][oO0][vV][eE3][mM][bB8][eE3][rR]		10533
		Diff	365

’i’ statements

- iwant
- ihope
- iwill
- iwont
- ican
- icant

ilove

- 20462 ilove
- 20116 iloveyou
- 10065 iloveu
- 3769 iloveme
- 3748 ilover
- 1472 ilovehim
- 1367 ilovemy
- 1320 ilovegod
- 1077 iloves
- 964 ilovesex
- 886 ilovejesus
- 866 ilovey

788 ilovej
764 iloveher
760 ilovemom
746 ilovemyself
734 iloveyo
678 ilovem
676 iloved
643 ilovepussy
577 iloveit
527 ilovemymom
518 iloveb
485 ilovelife
485 ilovejoe

483 ilovec
465 ilovea
461 ilovemusic
458 ilovek
455 ilovesam
454 iloveny
452 ilovet
435 ilovedogs
425 iloveyu
400 ilovemykids
389 ilovemylife
386 ilovepink
381 ilovecats

378 ilovejosh
376 ilovemike
372 ilovedad
364 ilovematt
363 ilovemyfamily
361 ilovealex
355 ilovelucy
348 ilovechris
347 ilovejb
343 ilovenick
333 iloveben
328 ilovetom

ihate

- 1537 ihateyou
- 1299 ihateu
- 256 ihateme
- 233 ihatemen
- 216 ihatelife
- 212 ihatehim
- 193 ihatemylife
- 186 ihatelove
- 180 ihatethis
- 169 ihateher
- 132 ihatehackers
- 119 ihateschool

116 ihateboys
113 ihatemyself
99 ihateit
94 ihatepasswords
80 ihateppl
74 ihatey
68 ihatesam
68 ihatepie
67 ihatetom
65 ihatemy
65 ihatej
64 ihatem

61 ihateyu
61 ihatejoe
60 ihatepeople
60 ihateb
59 ihateuall
55 ihatework
55 ihatecats
54 ihated
54 ihateall
53 ihatemom
52 ihateguys
51 ihatealex

50 ihatepink
50 ihatemath
49 ihategirls
47 ihateyouall
47 ihatems
47 ihatemike
46 ihatejay
44 ihateluv
44 ihateben
43 ihatespam
43 ihateneopets
42 ihatedad

ilike

1764 ilike
1031 ilikepie
452 ilikeit
399 ilikeyou
318 ilikeu
223 ilikecheese
191 ilikeme
179 ilikesex
146 ilikepussy
140 ilikegirls
135 ilikecake
129 ilikehim
124 ilikeeggs
114 ilikefood
107 ilikemen
98 ilikecats
94 ilikes
87 ilikeike
87 ilikeher
85 iliketo
85 iliked
82 ilikepizza
81 ilikethat
79 iliketrains
77 iliketurtles
77 ilikepi
77 ilikedogs
76 iliker
76 ilikeboys
76 ilikea
75 ilikem
70 ilikebeer
69 ilikey
69 ilikeb
68 ilikemilk
67 ilikered
66 iliketofuck
65 ilikedick
64 ilikeboobs
62 iliketits
62 ilikefish
61 ilikemike
60 iliketacos
60 ilikeporn
59 ilikepink
58 ilikechicken
57 ilikeham
57 ilikecows
57 ilikecookies
56 ilikethis

ilike – choice cuts

- ilikebigbuttsicannotlie
- ilikedick6inch
- iliketitmilk
- iliketofart
- iliketurtles
- ilikeultrabigbutts
- ilikewatchindrunkguys
- ilikewatchingporno
- ilikezombies

iwant

- 382 iwantyou
- 327 iwantu
- 228 iwantsex
- 160 iwantit
- 125 iwantin
- 103 iwanthim
- 101 iwantpussy
- 88 iwanta
- 82 iwanttofuck
- 69 iwanther
- 68 iwantlove
- 67 iwantto
- 57 iwantsome
- 57 iwantajob
- 56 iwantout
- 48 iwantmore
- 48 iwantitall
- 45 iwantcandy
- 43 iwanttobe
- 43 iwantmoney
- 35 iwanttodie
- 35 iwantitnow
- 32 iwantadog
- 28 iwantsexnow
- 26 iwantpie
- 25 iwantfuck
- 24 iwantme
- 24 iwantfun
- 23 iwantunow
- 23 iwanttofly
- 23 iwantmy
- 22 iwantfood
- 22 iwantdick
- 22 iwantass
- 21 iwanttobelieve
- 20 iwantcock
- 20 iwantaman
- 19 iwantthis
- 19 iwantthat
- 19 iwantluv
- 18 iwanttofuckyou
- 18 iwantjob
- 18 iwantfree
- 17 iwantjoe
- 17 iwanted
- 16 iwantt
- 16 iwanton
- 16 iwantagirl
- 16 iwantacar

ican

- 362 icandoit
- 276 icanfly
- 172 icandy
- 148 icando
- 63 icansee
- 57 icandothis
- 52 icandi
- 42 icanbe
- 41 icanwin
- 39 icancu
- 37 icansing
- 36 icantell
- 29 icanread
- 28 icanseeu
- 22 icanseeyou
- 22 icanplay
- 22 icandrive
- 20 icaniwill
- 20 icandance
- 20 icancount
- 19 icanhas
- 19 icandie
- 18 icanmakeit
- 18 icanlove
- 18 icanican
- 17 icanwait
- 17 icanrun
- 16 icannot
- 15 icantrust
- 15 icankill
- 15 icandobetter
- 14 icanfuck
- 13 icanride
- 13 icandraw
- 13 icandigit
- 12 icanhelp
- 12 icaneat
- 12 icandoanything
- 12 icancook
- 11 icantoo
- 11 icanswim
- 11 icanskate
- 10 icanownu
- 10 icanlive
- 10 icanjump
- 10 icanget
- 10 icanfixit
- 10 icandothat

icant

- 41 icantwait
- 41 icantremember
- 37 icantell
- 28 icanttell
- 23 icantsee
- 22 icanttellyou
- 20 icantsay
- 20 icantdoit
- 17 icantstop
- 16 icantgetenough
- 15 icantrust
- 15 icantlove

- 41 icantwait
- 41 icantremember
- 37 icantell
- 28 icanttell
- 23 icantsee
- 22 icanttellyou
- 20 icantsay
- 20 icantdoit
- 17 icantstop
- 16 icantgetenough
- 15 icantrust
- 15 icantlove

- 15 icantlose
- 14 icantfly
- 14 icantbelieve
- 13 icantwin
- 11 icantoo
- 10 icantdie
- 9 icantthink
- 9 icantread
- 9 icantlive
- 9 icanthearyou
- 9 icanteach
- 9 icantbelieveit

iwill

- 178 iwillwin
- 162 iwillbe
- 87 iwillsurvive
- 69 iwillkillyou
- 56 iwillmakeit
- 52 iwillkill
- 49 iwilldoit
- 43 iwillberich
- 41 iwilldie
- 36 iwillb
- 34 iwillfly
- 32 iwillnot
- 29 iwillkillu
- 29 iwillgo
- 26 iwillwait
- 25 iwillfuckyou
- 25 iwilldo
- 25 iwillbehappy
- 25 iwillalwaysloveyou
- 24 iwillbehere
- 24 iwillbeback
- 22 iwilllive
- 21 iwilltry
- 21 iwillrise
- 20 iwillsucceed
- 20 iwillrule
- 19 iwillrun
- 19 iwillpass
- 19 iwilleatyou
- 18 iwillrock
- 18 iwillloveyou
- 18 iwillbeok
- 17 iwillnotlose
- 17 iwillloveu
- 17 iwillfuck
- 16 iwilleatu
- 15 iwillnever
- 15 iwilllove
- 15 iwillfindyou
- 14 iwillnotdie
- 14 iwillfucku
- 13 iwillgetu
- 12 iwillsing
- 12 iwillluvu
- 12 iwillforget
- 12 iwillalways
- 11 iwillget
- 11 iwillbethe
- 10 iwillrockyou

iwont

- 35 iwontforget
- 32 iwonttell
- 16 iwontdie
- 14 iwontgiveup
- 12 iwontsex
- 9 iwontyou
- 9 iwonttellyou
- 8 iwontstop
- 8 iwontlie
- 7 iwontsay
- 7 iwontell
- 6 iwontu
- 6 iwontgo
- 6 iwontcry
- 5 iwonttellu
- 5 iwontremember
- 5 iwontlove
- 5 iwonthegame
- 4 iwontwin
- 4 iwontlose
- 4 iwonthis
- 4 iwontforgetthis
- 4 iwontforgetit
- 4 iwontfall
- 4 iwontellu
- 4 iwontbite
- 4 iwonta
- 3 iwontusethis
- 3 iwontoday
- 3 iwontmind
- 3 iwontluv
- 3 iwontknow
- 3 iwontit
- 3 iwonther
- 3 iwontforgetyou
- 3 iwontfail
- 3 iwontbe
- 2 iwontyoubaby
- 2 iwontwhine
- 2 iwontwait
- 2 iwonttofuck
- 2 iwonttodie
- 2 iwontto
- 2 iwonttelu
- 2 iwontte
- 2 iwontt
- 2 iwontrem
- 2 iwontr
- 2 iwontquit

youare

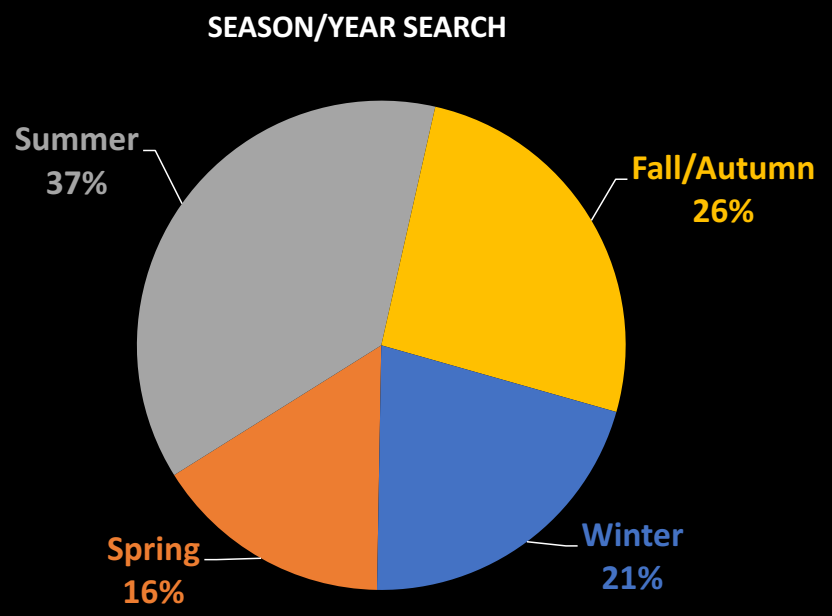
- 470 youare
- 60 youaremine
- 47 youareme
- 46 youaremy
- 44 youaremylove
- 38 youarethe
- 35 youarehot
- 34 youarethebest
- 32 youaremylife
- 28 youarecool
- 27 youarea
- 26 youaretheone
- 26 youareit
- 25 youarefat
- 23 youarenot
- 23 youarebeautiful
- 22 youareso
- 21 youarenotalone
- 20 youarestupid
- 19 youareyou
- 19 youarenoob
- 18 youareloved
- 18 youarecrazy
- 17 youaremysunshine
- 16 youarein
- 16 youaregood
- 16 youaredead
- 16 youarecute
- 16 youarebad
- 15 youaredumb
- 14 youareugly
- 13 youaresocool
- 13 youared
- 12 youareno
- 12 youaremad
- 11 youarenice
- 11 youarehere
- 11 youaregreat
- 11 youareawesome
- 11 youareabitch
- 10 youareu
- 10 youarerad
- 10 youaregod
- 10 youarecoo
- 10 youarebitch
- 10 youarebest
- 9 youaretheman
- 9 youaresexy

Summer2017 - season/year

```
Search example:
grep -i  -e '^summer[0-9]{2,4}'
```

Tried multiple regex variations, same results

- removed leading req (^)
- tried requiring real dates



popularity contest

example: `./popcon.sh cracker scriptkiddie hacker`

output:

```
19993, hacker
6304, cracker
19, scriptkiddie
```

videogames

- pacman 3323
- frogger 2089
- tetris 1196
- metroid 1129
- supermario 887
- galaga 796
- mariobros 416
- paperboy 386
- donkeykong 334
- digdug 295
- qbert 214
- castlevania 162

arkanoid 128
legendofzelda 72
asteroids 71
galaxian 64
mariobrothers 33
spaceinvaders 19
crystalcastles 13
yarsrevenge 3
missilecommand 1

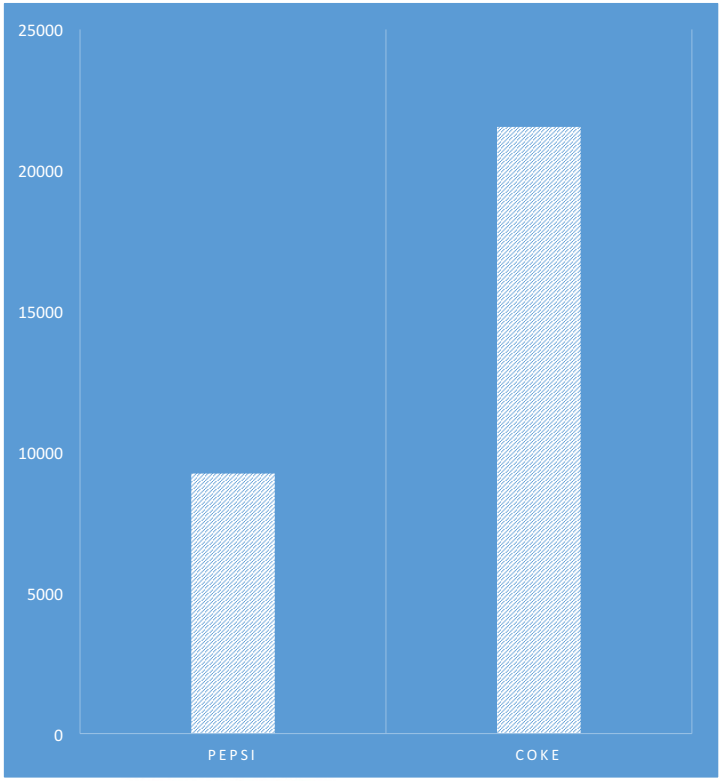
celebrities

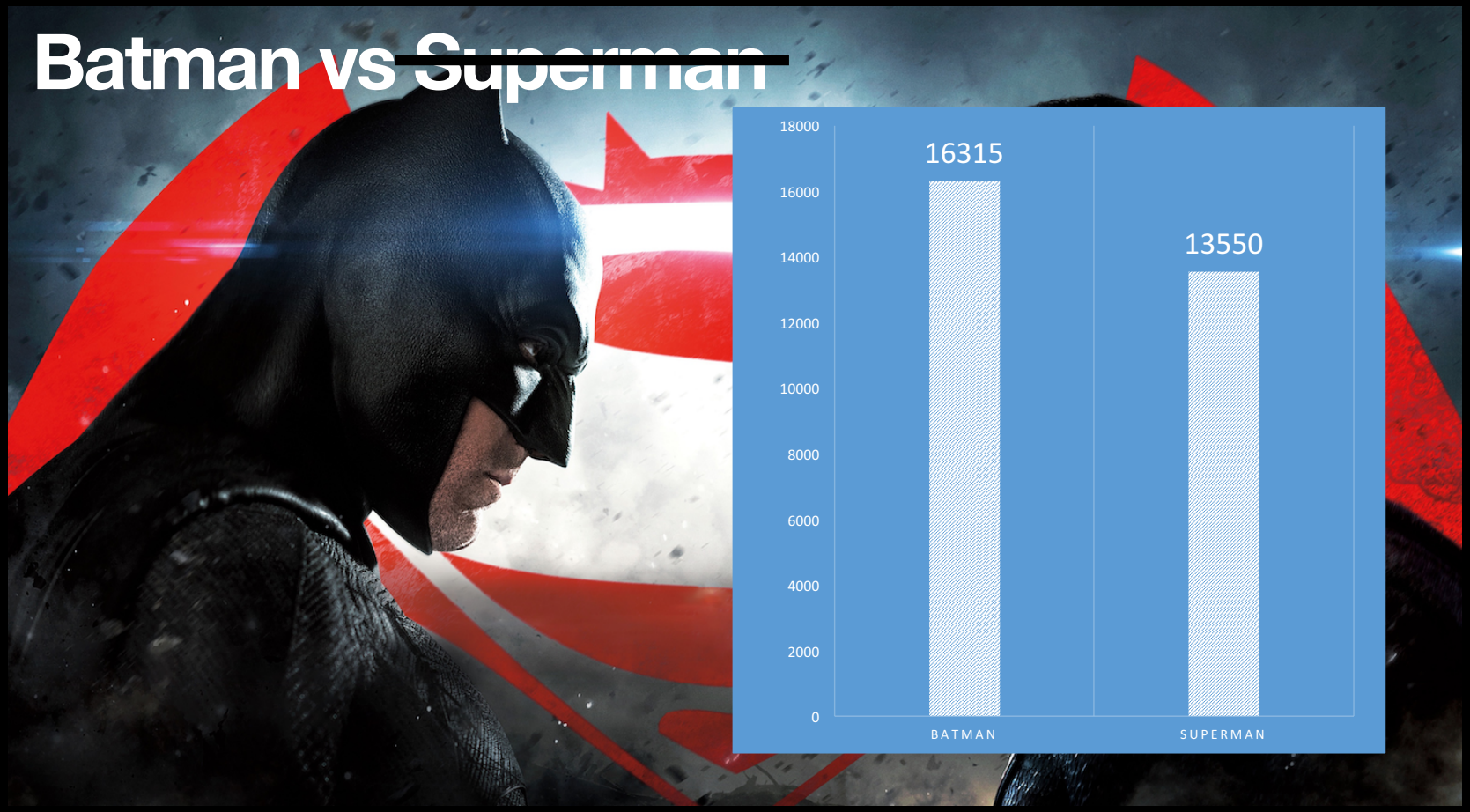
- madonna 4196
- obama 3780
- johncena 2859
- beyonce 2646
- brucelee 1227
- michaeljackson 514
- chucknorris 399
- billgates 314
- britneyspears 230
- stevejobs 144

rivalries

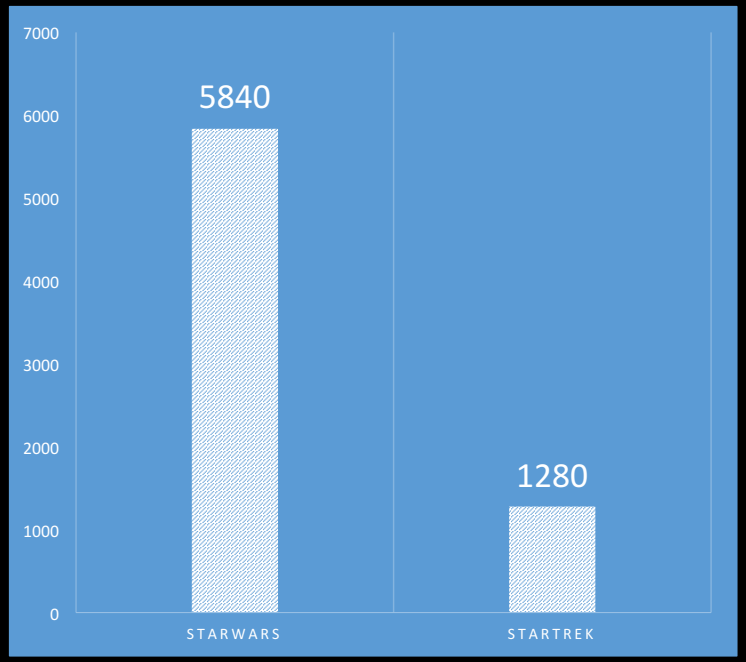
- Pepsi vs Coke
- Superman vs Batman
- Star Wars vs Star Trek
- Yankees vs Red Sox
- Red Vines vs Twizzlers

~~Pepsi vs~~ Coke

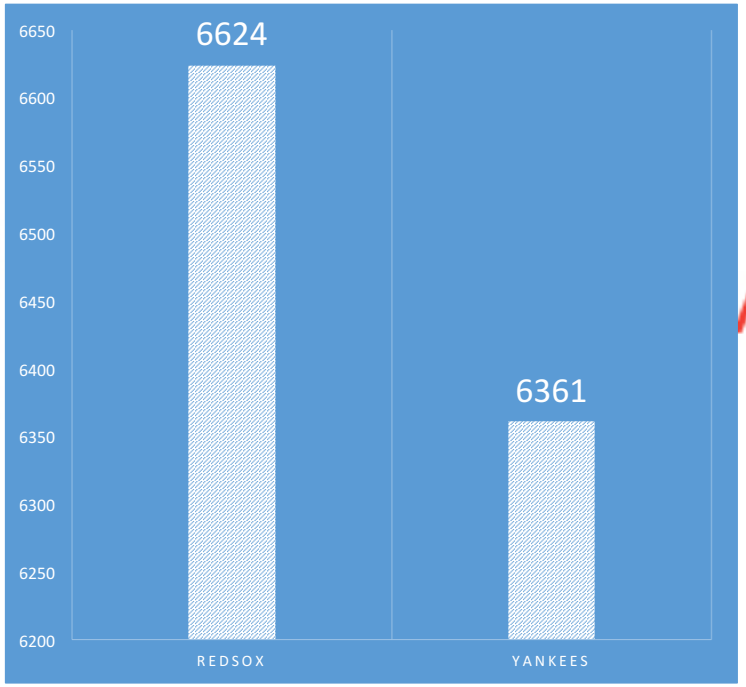



Batman vs Superman
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
16315
13550
BATMAN
SUPERMAN

Star Wars ~~vs Star Trek~~



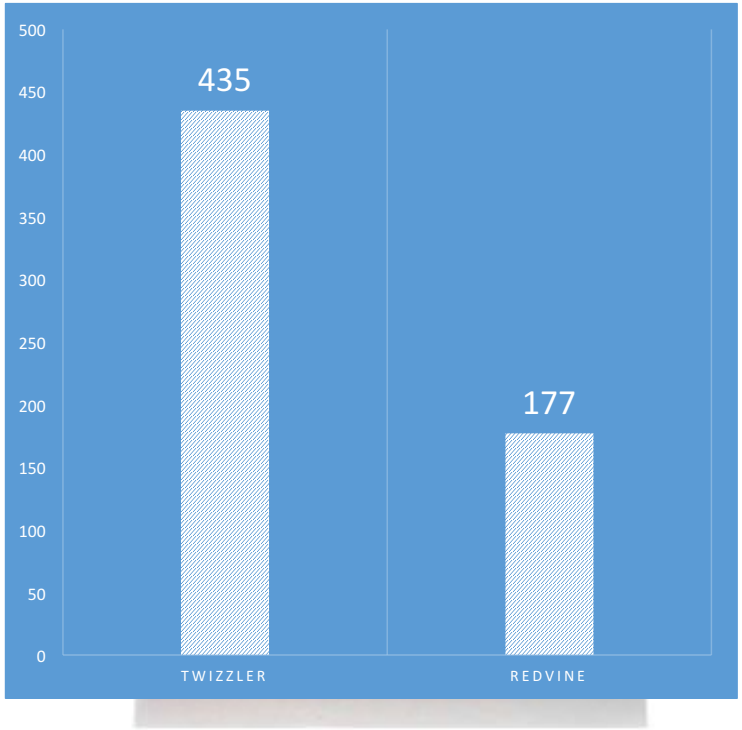
yankees vs red sox



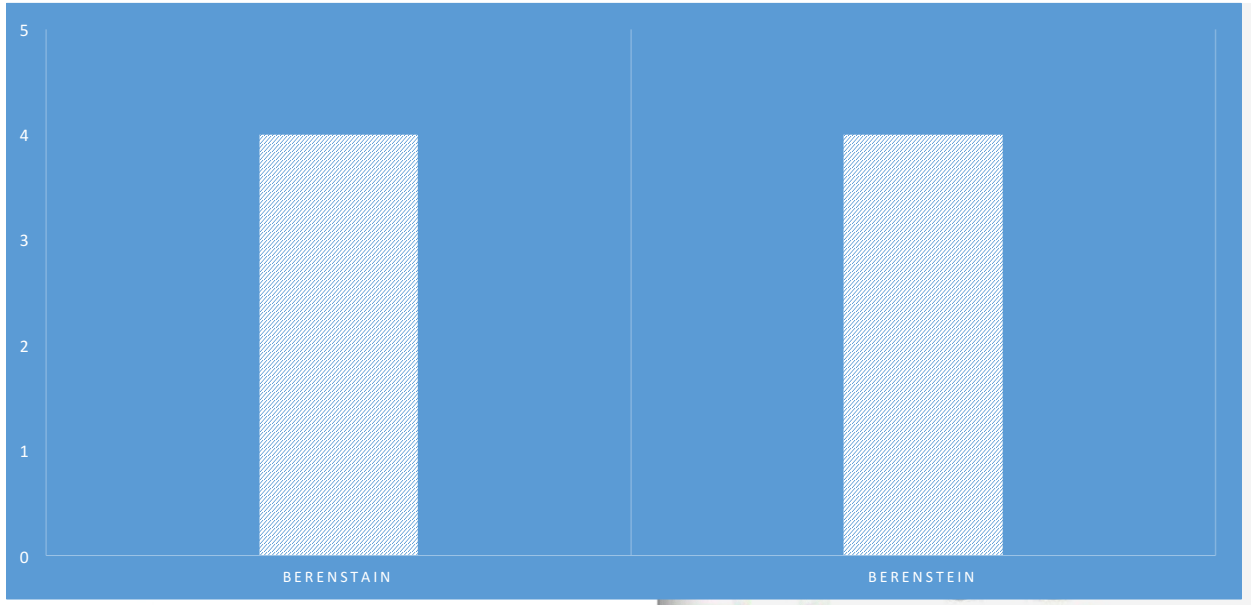
VS

BOSTON RED SOX ™

red vines vs twizzlers

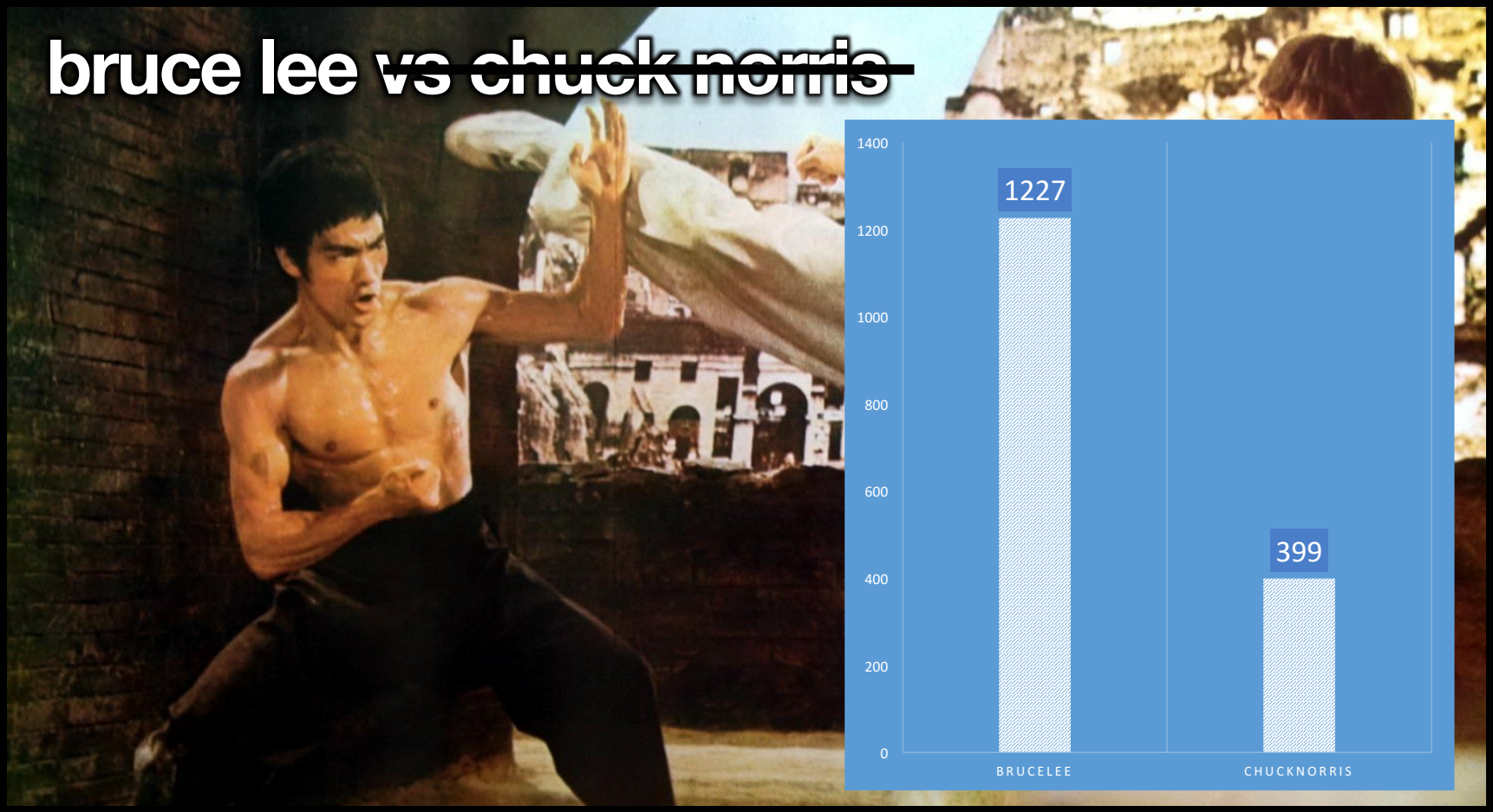


berenstain vs berenstein

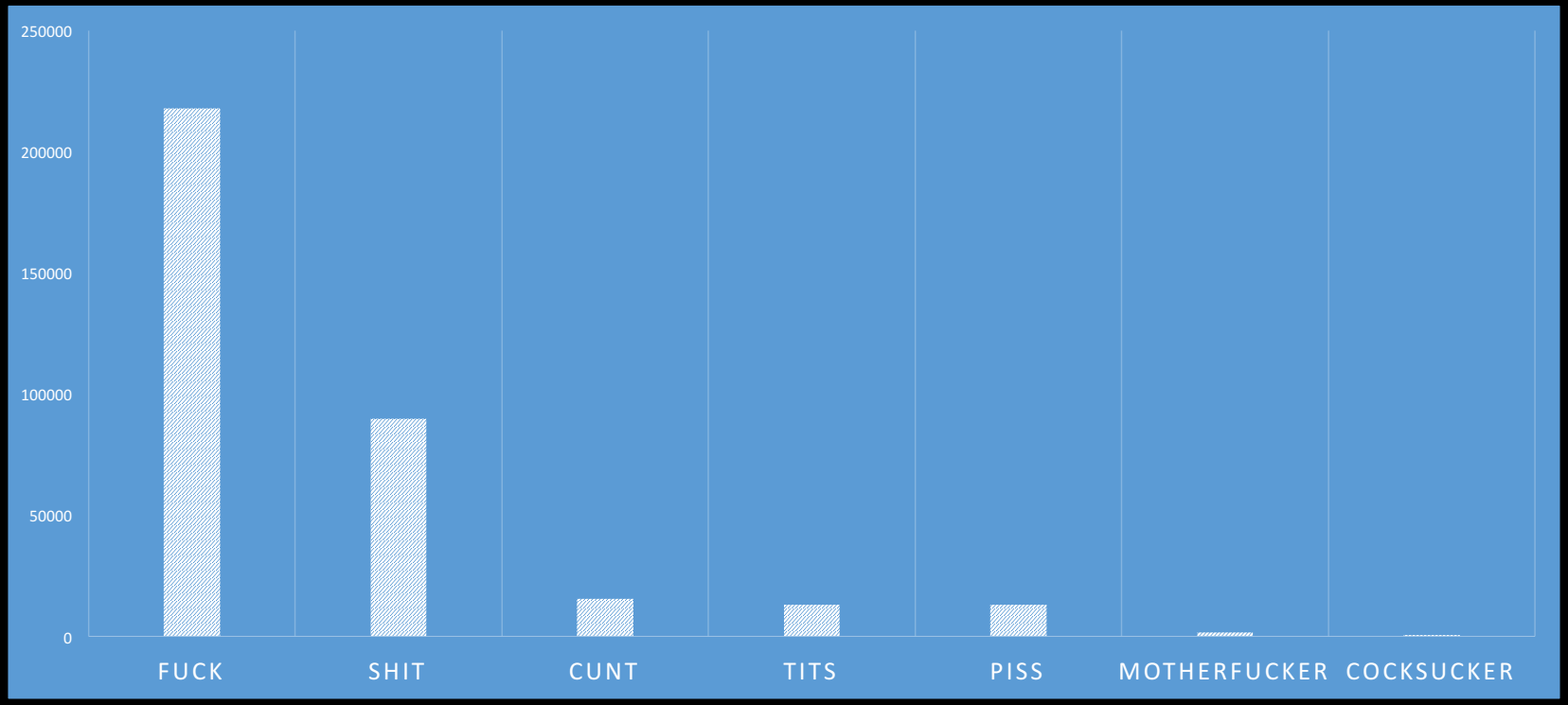


The Berenstain Bears®

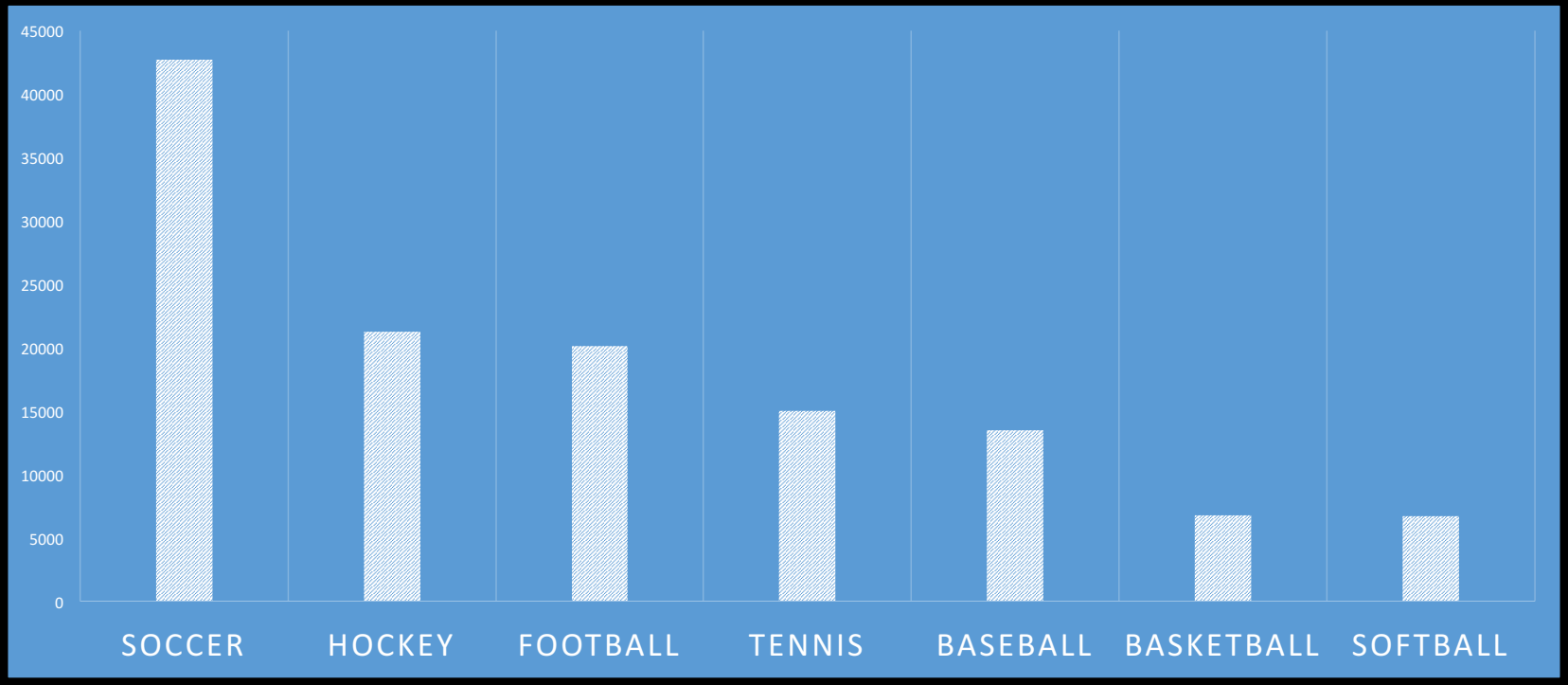
The Berenstein Bears


bruce lee ~~vs chuck norris~~
1400
1200
1000
800
600
400
200
0
1227
399
BRUCELEE
CHUCKNORRIS

profanity


250000
200000
150000
100000
50000
0
FUCK
SHIT
CUNT
TITS
PISS
MOTHERFUCKER
COCKSUCKER

sports


45000
40000
35000
30000
25000
20000
15000
10000
5000
0
SOCCER
HOCKEY
FOOTBALL
TENNIS
BASEBALL
BASKETBALL
SOFTBALL

fictional characters

- watson 8046
- spiderman 4641
- gandalf 3078
- terminator 2996
- harrypotter 2497
- dracula 2472
- godzilla 2414
- sherlock 1819
- jamesbond 1655
- spock 1535
- sauron 1072
- magneto 676
- doctorwho 629
- hagrid 505
- galadriel 462
- elrond 436
- clarkkent 354
- dumbledore 350
- mothra 323
- homersimpson 270
- frankenstein 268
- loislane 239
- greenlantern 222
- bartsimpson 206

dumpsniffer

- Collection of bash tools
  - Create regex of l33t word variations from wordlist
  - Perform word counts
  - Find Possible CC #s
- will be published after talk on
  - https://github.com/nyxgeek/dumpsniffer

last mile password attacks

- Those hard to reach passwords, when you're scraping the 96%+ ranges
- Hashcat Rules
  - i series conversion from JtR
  - Address maker
- Cleverbrute – Combinator Attack Twist

Hashcat Rules – [io][12] series

- i-series of rules from JtR Jumbo (winner from HashKiller)
  - i1 = insert 1 char at each char position
  - i2 = insert 1 char at 2 different positions
  - o1 = overwrite 1 char at each char position
  - o2 = overwrite 1 char 2 different positions
- great with larger wordlists

https://github.com/nyxgeek/nyxgeek-rules/

combinator attack

- Uses two wordlists and joins words

- Example:
  - Wordlist 1: password
  - Wordlist 2: 12345

  - Output: password12345

https://hashcat.net/wiki/doku.php?id=combinator_attack

cleverbrute method

- combinator attack with special wordlists
- wordlists are created from substrings of large wordlists
  - uses a FRONT list and a TAIL list
  - front list are first 1-6 chars, cut from cracked password lists
    - e.g., Password -> Pass, Passw, Passwo
  - tail list are from last 1-6 , 1-5, and 1-4 chars of password lists
    - e.g., Password -> word, sword, ssword
- large lists, but not a full brute force
  - human-generated patterns + human-generated patterns
  - idea is to cover most of the keyspace that is actually used by people

cleverbrute – creating wordlists

- Wordlist 1 (Left Side)
  - Create wordlist of the first 4-6 chars
    - cat wordlist.txt | cut –c 1-6 | sort –u >> FRONT_LIST.txt
    - cat wordlist.txt | cut –c 1-5 | sort –u >> FRONT_LIST.txt
    - cat wordlist.txt | cut –c 1-4 | sort –u >> FRONT_LIST.txt
- Wordlist 2 (Right Side)
  - Create wordlist of the last 4-6 chars
    - cat wordlist.txt | rev | cut –c 1-6 | rev | sort –u >> TAIL_LIST.txt
    - cat wordlist.txt | rev | cut –c 1-5 | rev | sort –u >> TAIL_LIST.txt
    - cat wordlist.txt | rev | cut –c 1-4 | rev | sort –u >> TAIL_LIST.txt

the end of an era?

- we are in a golden era of password cracking
  - cheap GPUs
  - frequent leaks/dumps
  - lots of users who make bad decisions
    - "who would want to hack ME?"
    - "Summer2017"

- passwords are a huge weakness, and will EVENTUALLY be mitigated

looking forward to better security

- multi-factor – taking away a password's power
  - biometrics
  - smart cards
- password managers - 'uncrackable' hashes
  - passwords longer than max length

    https://www.notsosecure.com/maximum-password-length-reached/
  - complex unicode – too large of keyspace to cover

make hay while the sun shines

- that's the future -- here and now, people still suck at passwords
- download and crack dumps
- examine the results, make new rules, share these rules

- compete in cracking competitions:
  - Crack Me If You Can (CMIYC) – KoreLogic
    - Running now!
    - First year at DerbyCon
    - Back after a year hiatus

    https://contest-2017.korelogic.com/

  - HashKiller (last contest was 2016)
    https://hashkiller.co.uk

resources

- 10 Crack Commandments
  http://www.hashcrack.io/blog/10-crack-commandments
- Hashes.org
- Analysis
  - PACK - https://thesprawl.org/projects/pack/
  - Pipal - https://github.com/digininja/pipal/
- Rules
  - nyxgeek-rules – hashcat & john the ripper
    https://github.com/nyxgeek/nyxgeek-rules
  - nsa-rules – hashcat
    https://github.com/NSAKEY/nsa-rules
  - Hob0Rules – hashcat
    https://github.com/praetorian-inc/Hob0Rules