

CIBER RIESGOS
FINANCIAL SECTOR CYBER RESILIENCE
WORKSHOP
MEXICO CITY, 6-7 NOVEMBER 2019

Pablo Andrés Palazzi
Socio Allende & Brea
Noviembre 2019

DELITOS INFORMATICOS

- ⇒ Protección de datos personales – identidad - privacy
 - ◆ Robo de identidad
 - ◆ Cesión de datos sin consentimiento
 - ◆ Información inexacta que genera daño
 - ◆ Robo de bases de datos
- ⇒ Delitos informáticos
 - ◆ Acceso no autorizado a datos o sistemas (hacking)
 - ◆ Violación de correo electrónico - interceptación
 - ◆ Fraude informático
 - ◆ Falsedades informáticas
 - ◆ Delitos contra la propiedad intelectual (secreto comercial)

CIBERATAQUES – NORMAS APLICABLES

- ⇒ Violación de información personal
 - ◆ Ley 25326, decreto regl. 1558/2001 y disposiciones de la DNPDP
- ⇒ Violación de información corporativa
 - ◆ Ley 24.766 (ley de secretos comerciales)
- ⇒ Violación de información personal por reclamo de empresas tercerizadas
 - ◆ Ley 25.326 (Protección de datos y reglas de outsourcing)
- ⇒ Responsabilidad por seguridad de datos
 - ◆ Ley 26388 (delitos informáticos)

PROTECCIÓN DE DATOS

- ⇒ Consentimiento
- ⇒ Notificación
- ⇒ Cesión
- ⇒ Seguridad y confidencialidad
- ⇒ *Data breach notification*: notificar eventos.
- ⇒ Transferencia internacional
- ⇒ Organismo regulador: Sanciones, multas, habeas data (individual y colectivo y daños)

PROPIEDAD INTELECTUAL - SECRETOS COMERCIALES

- ⇒ Espionaje industrial
- ⇒ Robo de información
- ⇒ Empleados infieles
- ⇒ Objetivos: listados de clientes, precios, proveedores, productos nuevos, planes de marketing, etc.
- ⇒ Leyes penales y civiles

SECRETOS COMERCIALES CASOS ARGENTINOS

- ⇒ Pepsico v. Redmond – non compete y planes de marketing
- ⇒ Conferencias SRL v. Durruty (base de datos, secreto comercial y competencia desleal)
- ⇒ OLX v. Colli (base de datos, derecho de autor)
- ⇒ Caso Nosis v. Accesor (C. Nac. Crim. y Corr., sala 1^a 31/3/2005, Shakery Rodríguez – derecho de autor - penal)

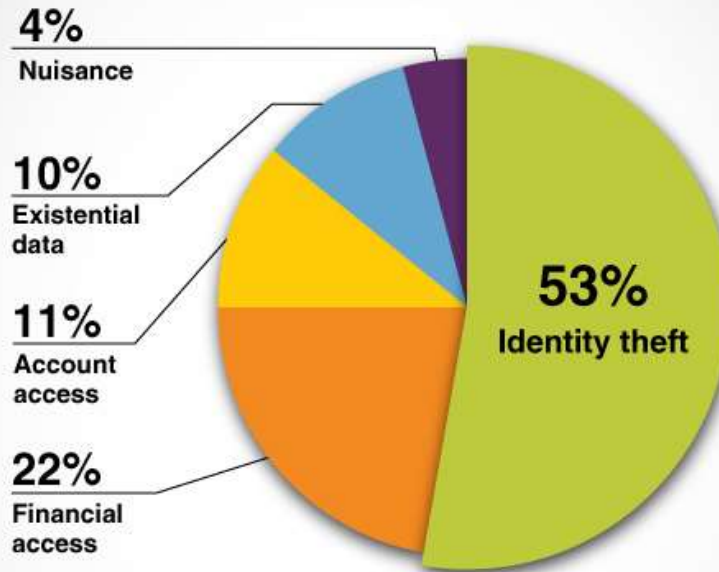
HACKING – ACCESO NO AUTORIZADO

⇒ Casos recientes de hacking

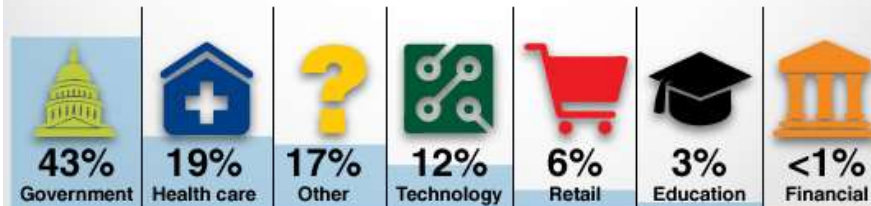
- ◆ Target (Diciembre 2013, 70 millones de cuentas)
- ◆ Hacking de Sony (2014, motivos políticos?)
- ◆ Home Depot data breach (65 millones de TC)
- ◆ Yahoo hacking (2014, 500 millones de cuentas, descuento de 350 millones del posible comprador en el due diligence)
- ◆ Hacking a la Convención demócrata de U.S.A.
- ◆ Krypto locker (mayo 2016)
- ◆ Equifax (mayo 2017) 143 millones de registros

2015 data breaches

Number of data breach incidents by type



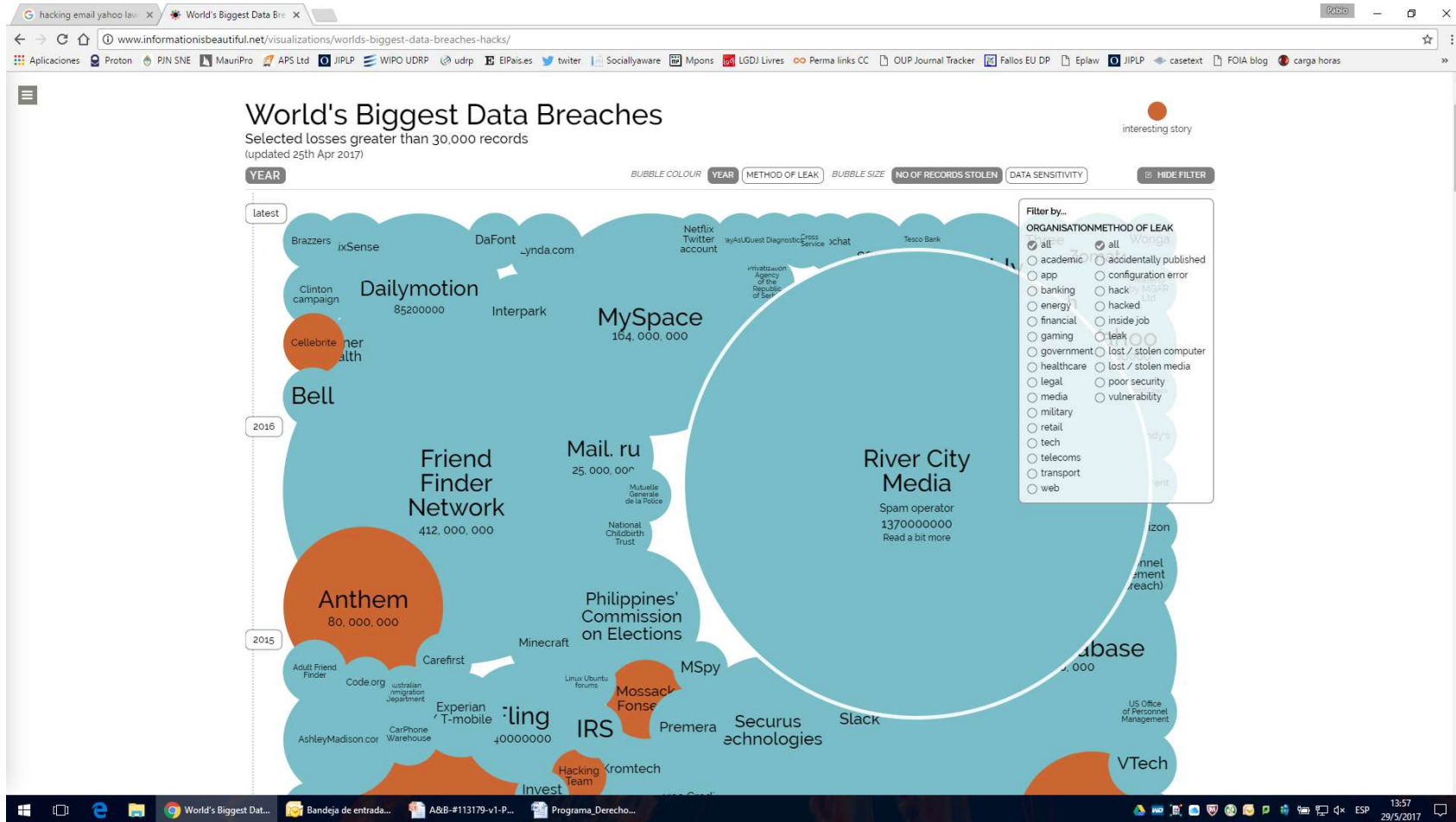
Data records lost/stolen by industry



Source: Gemalto's Breach Level Index 2015

CreditCards.com

PANORAMA GLOBAL



PANORAMA GLOBAL

W List of data breaches - W x

Seguro | https://en.wikipedia.org/wiki/List_of_data_breaches

Aplicaciones CONGIF Proton PJJN WD Drive JIPL WIPO UDRP udrp Drpbx twitter Law sites GOSWIM RNYT Perma links CC OUP Journal Tracker NON TRADITIONAL JIPLP FOIA blog carga horas

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction


Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

Languages  [Add links](#)

List of data breaches

From Wikipedia, the free encyclopedia

For a broader coverage of this topic, see Data breach.

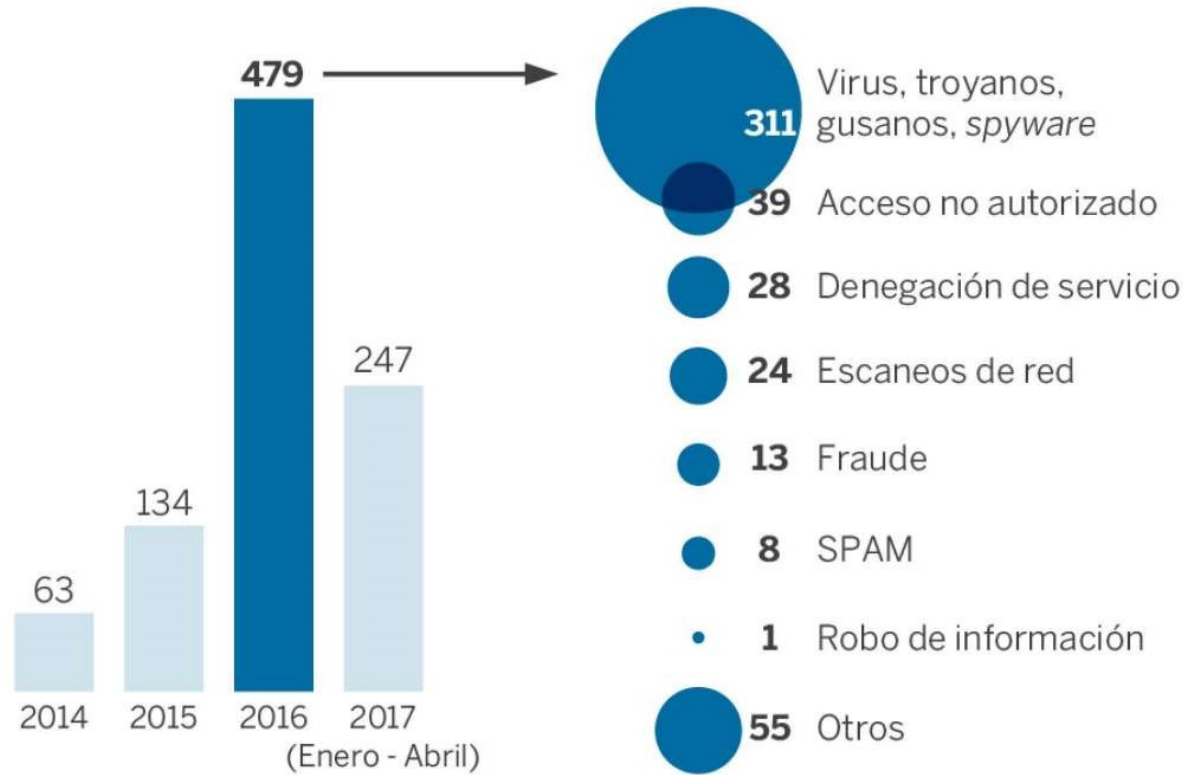
This is a list of **data breaches**, using data compiled from various sources, including press reports, government news releases and mainstream news articles. The list includes those involving the theft or compromise of 30,000 or more records, alth breaches occur continually. Breaches of large organizations where the number of records is still unknown are also listed. The various methods used in the breaches are also listed, with **hacking** being the most common.

Most breaches occur in North America. It is estimated that the average cost of a data breach will be over \$150 million by 2020, with the global annual cost forecast to be \$2.1 trillion.^{[1][2]} It is estimated that in 2015 alone, 707 million records were e breaches.^[3] *Vigilante.pw*^[4] lists over 2,100 websites which have had their databases breached, containing over 2 billion user entries in total.

Entity	Year	Records	Organization type	Method	Sources
Yahoo	2013	3,000,000,000	web	hacked	[260][261]
Yahoo	2014	500,000,000	web	hacked	[262][263][264][265][266]
Friend Finder Networks	2016	412,214,295	web	poor security / hacked	[94][95]
Massive American business hack including 7-Eleven and Nasdaq	2012	160,000,000	financial	hacked	[148]
Adobe Systems	2013	152,000,000	tech	hacked	[11][12]
Under Armour	2018	150,000,000	Consumer Goods	hacked	[235]
eBay	2014	145,000,000	web	hacked	[76]
Equifax	2017	143,000,000	financial, credit reporting	poor security	[82][83]
Heartland	2009	130,000,000	financial	hacked	[114][115]
Rambler.ru	2012	98,167,935	web	hacked	[177][178]
TK / TJ Maxx	2007	94,000,000	retail	hacked	[220][221]
MyHeritage	2018	92,283,889	genealogy	unknown	[5]
AOL	2004	92,000,000	web	inside job, hacked	[19][20]
Anthem Inc.	2015	80,000,000	healthcare	hacked	[18]
Sony PlayStation Network	2011	77,000,000	gaming	hacked	[195]
JP Morgan Chase	2014	76,000,000	financial	hacked	[131]
National Archives and Records Administration (U.S. military veterans' records)	2009	76,000,000	military	lost / stolen media	[245]
Target Corporation	2014	70,000,000	retail	hacked	[211][212]
Tumblr	2013	65,469,298	web	hacked	[225]
Uber	2017	57,000,000	transport	hacked	[229]
Home Depot	2014	56,000,000	retail	hacked	[121]
Philippines Commission on Elections	2016	55,000,000	government	hacked	
	2013	50,000,000	web	hacked	[86][87]

Esperando upload.wikimedia.org...

CIBERATAQUES A INFRAESTRUCTURAS CRÍTICAS



Fuente: INCIBE (Instituto Nacional de Ciberseguridad). EL PAÍS

INCIBE @INCIBE · 9 h
"Los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años" vía @elpais_espana pic.twitter.com/tFZrQL7om1


69 29

TARGET


The screenshot shows a web browser window displaying a MarketWatch article. The browser's address bar shows the URL: www.marketwatch.com/story/target-settles-2013-data-breach-investigation-for-185-million-2017-05-23. The MarketWatch logo is visible in the top left of the page. The article title is "Target settles 2013 data breach investigation for \$18.5 million", published on May 23, 2017, at 2:25 p.m. ET. The author is Nicole Hong. A sub-headline reads: "The settlement is the largest multistate data breach settlement ever". The main image shows red Target shopping carts in a store. A Bloomberg logo is in the bottom right corner of the image. Below the image, the text states: "Target's \$18.5 million settlement is the largest multistate data breach settlement in history". The article text continues: "Target Corp. on Tuesday agreed to pay \$18.5 million to resolve an investigation by state prosecutors into its massive 2013 hack, a deal that represents the largest multistate data breach settlement in history. The investigation, led by the attorney generals in Connecticut and Illinois, focused on allegations that more than 40 million customers had their credit or debit card information compromised in 2013 after Target TGT, +0.37% failed to provide". To the right of the article is a sponsored advertisement for Huawei with the text "Exploration lights the way forward" and "The relentless pursuit of innovation enlightens the intelligent world". Below the ad are sections for "QUOTE REFERENCES" showing TGT stock price (+0.20 +0.37%) and "MOST POPULAR" featuring a quote from Bill Gates and Mark Zuckerberg.

 Target Data Breach Spilled Info On As Many As 70 Million Customers

 Grads of LifeVoice: What We Can Learn From The UK's Approach To Apprenticeship

 LISTEN NOW: Why Trump's Tax Returns Won't Tell You Everything About His Empire

-1 comments in the last hour

 Court Rules That Religious Freedom Law Is Not A Free Pass for Tax Evasion

-7k views in the last 24 hours

 5 Dividend Payers To Sell In May -- And Stay Away Forever

-58k views in the last 24 hours

 New Trump Budget Completely Disappears In An Amazing Just 3 Days

-60k views in the last 24 hours

 The Four Big Millennial Money Mistakes

Target Data Breach Spilled Info On As Many As 70 Million Customers



 **Maggie McGrath**, FORBES STAFF 
Food, retail, and consumerism in an age of voting with dollars [FULL BIO](#) 

The data breach that was the nightmare before Christmas for Target [TGT -0.37%](#) and its millions of customers just got a little bit worse: the retailer said Friday morning that the information stolen between November 27 and December 15, 2013 included personal information of as many as 70 million people -- more than the 40 million the company originally estimated.



On December 19, the retailer said that as many as 40 million credit card and debit card accounts may have been compromised during Black Friday weekend through December 15, and that information stolen included customer names, credit or debit card number, the card's expiration date and CVV (card verification value). Now, in an update on the hacking investigation, Target said that an additional 70 million people were affected, and the stolen customer information includes names, mailing addresses, phone numbers and email addresses. Target said that much of this data is "partial in nature," but it will nonetheless provide one year of free credit monitoring and identity theft protection to all guests who shopped at its U.S. stores.

"I know that it is frustrating for our guests to learn that this information was taken and we are truly sorry they are having to endure this," Gregg Steinhafel, Target's chairman, president and CEO said in a statement Friday morning. "I also want our guests to know that understanding and sharing the facts related to this incident is important to me and the entire Target team."

As a result of the incident, Target is lowering its fourth quarter 2013 earnings guidance, saying





NEWS

CLOSINGS

SEEN ON TV

AM SHOW

NEW DAY

SPORTS

TRAFFIC

CONTESTS

JOBLS

WEATHER

Target CEO Leaves Company

POSTED 8:32 AM, MAY 5, 2014, BY CNNWIRE

FACEBOOK

TWITTER

G+ GOOGLE

PINTEREST

LINKEDIN

This is an archived article and the information in the article may be outdated. Please look at the time stamp on the story to see when it was last updated.

NEW YORK (CNMoney) — Gregg Steinhafel, the chairman and CEO of Target during the retailer's massive breach of customer data last year, has left the company effective immediately.

The company announced that the decision was made after "extensive discussions" between Steinhafel and the board. Chief Financial Officer John Mulligan will serve as interim CEO, while board member Roxanne Austin will serve as interim non-executive chair of the board.

Steinhafel, who had been with Target for 35 years, will serve in an advisory capacity during this transition to a permanent CEO.



Credit: Target via CNN

Discover it for stu
Rewards you'll love. No a



LEARN MORE

*See Rates, Fees and othe

YOU MAY LIKE

Spons



That's How You Find



If you'r

SONY PICTURES HACK

The screenshot shows a web browser window displaying the Wikipedia article "Sony Pictures hack". The browser's address bar shows the URL "https://en.wikipedia.org/wiki/Sony_Pictures_hack". The article text is as follows:

From Wikipedia, the free encyclopedia

On November 24, 2014, a hacker group which identified itself by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information.^[1]

In November 2014, the GOP group demanded that Sony pull its film *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-Un, and threatened terrorist attacks at cinemas screening the film. After major U.S. cinema chains opted not to screen the film in response to these threats, Sony elected to cancel the film's formal premiere and mainstream release, opting to skip directly to a digital release followed by a limited theatrical release the next day.^{[2][3][4]}

United States intelligence officials, after evaluating the software, techniques, and network sources used in the hack, alleged that the attack was sponsored by North Korea.^[5] North Korea has denied all responsibility.

Contents [hide]

- Hack and perpetrators
- Information obtained
- Threats surrounding *The Interview*
- U.S. accusations against North Korea
 - Doubts about accusations against North Korea
 - Other investigations
- Legal responses
- Public discussion
 - About reporting on the hack
 - About pulling *The Interview*
 - Outside the United States
- Documentary
- See also
- References

Hack and perpetrators [edit]

The exact duration of the hack is yet unknown. U.S. investigators say the culprits spent at least two months copying critical files.^[6] A purported member of the Guardians of Peace (GOP) who have claimed to have performed the hack stated that they have had access for at least a year prior to its discovery in November 2014, according to *Wired*.^[7] The hackers involved claim to have taken more than 100 terabytes of data from Sony, but that claim has never been confirmed.^[8] The attack was conducted using malware. Although Sony was not specifically mentioned in its advisory, US-CERT said that the attackers used a *Server Message Block* (SMB) Worm Tool to conduct attacks against a major entertainment company. Components of the attack included a listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. The components clearly suggest an intent to gain repeated entry, extract information, and be destructive, as well as remove evidence of the attack.^[9] The cleaning tool used on Sony's computer infrastructure, *Wiper*, is a malware program designed to erase data from the servers.^[10]

Sony was made aware of the hack on Monday, November 24, 2014, as the malware previously installed rendered many Sony employees' computers inoperable by the software, with the warning by a group calling themselves the Guardians of Peace, along with a portion of the confidential data taken during the hack.^[11] Several Sony-related Twitter accounts were also taken over.^[7] This followed a message that several Sony Pictures executives had received via email on the previous Friday, November 21; the message, coming from a group called "God'sApostls" [sic], demanded "monetary compensation" or otherwise, "Sony Pictures will be bombarded as a whole".^[11] This email message had been mostly ignored by executives, lost in the volume they had received or treated as spam email.^[11] In addition to the activation of the malware on November 24, the message included a warning for Sony to decide on their course of action by 11pm that evening, although no apparent threat was made when that deadline passed.^[11] In the days following this

The image also shows a sidebar with navigation links, a search bar, and a small photo of the Sony Pictures headquarters in Culver City, California.

CASO YAHOO

The screenshot shows a web browser displaying a New York Times article. The browser's address bar shows the URL: https://www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-bonus.html?_r=0. The page header includes the New York Times logo, navigation links (HOME, SEARCH), and a 'SUBSCRIBE NOW' button. The article is categorized under 'TECHNOLOGY' and has the headline: **Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack**. The byline reads 'By VINDU GOEL MARCH 1, 2017'. Below the headline is a large image of Marissa Mayer speaking at a conference with a 'YAHOO!' sign in the background. To the right of the image is a 'RELATED COVERAGE' section with three links: 'Verizon Will Pay \$350 Million Less for Yahoo' (FEB. 21, 2017), 'Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say' (SEPT. 28, 2016), and 'Yahoo Says Hackers Stole Data on 500 Million Users in 2014' (SEPT. 22, 2016). The browser's taskbar at the bottom shows several open applications and the system clock indicating 13:42 on 29/5/2017.

CRIPTOLOCKER



ATAQUE INFORMÁTICO ›

El Gobierno confirma un ciberataque masivo a empresas españolas

El Instituto Nacional de Ciberseguridad informa de que las primeras fases del virus que ha afectado a Telefónica y otras compañías han sido mitigadas



Madrid - 12 MAY 2017 - 17:16 ART

Una decena de grandes empresas españolas de servicios sufrieron este viernes un ciberataque masivo a través de un virus malicioso de tipo ransomware que bloquea los equipos y solicita un

Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

MalwareHunterTeam @malwrhunterteam · 12 may.
There is a new version of WCry/WannaCry ransomware: "WanaCrypt0r 2.0".
Extension: .WNCRY
Note: @Please_Read_Me@.txt
[@BleepinComputer pic.twitter.com/tdq0OBScz4](#)

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

[About bitcoin](#)
[How to buy bitcoins?](#)

[Contact Us](#)

Send \$600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

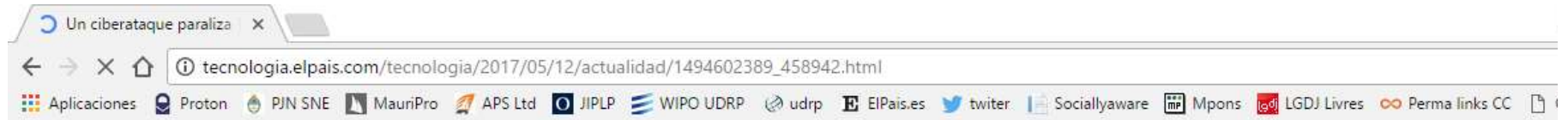
Check Payment **Decrypt**



MalwareHunterTeam @malwrhunterteam · 12 may.
There is a new version of WCry/WannaCry ransomware: "WanaCrypt0r 2.0".
Extension: .WNCRY
Note: @Please_Read_Me@.txt
[@BleepinComputer pic.twitter.com/tdq0OBSz4](https://twitter.com/bleepincomputer)

14 181 105

The screenshot shows a web browser window with the URL www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/minetur/Paginas/2017/120517-ciberataques.aspx. The page title is "Nota informativa sobre los ciberataques a varias compañías españolas". The article is dated "Viernes 12 de mayo de 2017". The main text states: "Tras la confirmación de diversos ciberataques a compañías españolas, el Ministerio de Energía, Turismo y Agenda Digital, a través del Instituto Nacional de Ciberseguridad (Incibe), está trabajando con las empresas afectadas con el objetivo de solucionar cuanto antes la incidencia." The article also mentions that the attack affected computer equipment of workers in various companies, but did not affect services or network operations. It describes the attack as ransomware (malware) that blocks access to files and demands a ransom. The article notes that the Incibe is providing assistance to affected companies and that national cyber incident response teams are in contact with affected organizations. A link to the alert is provided: "Alerta CERTSI: [link]". The website navigation includes "Inicio", "Presidente", "Gobierno", "Consejo de Ministros", "Prensa", "Multimedia", and "España". The sidebar lists various government departments, with "Energía, Turismo y Agenda Digital" selected. The Windows taskbar at the bottom shows several open applications, including the browser, email, and PowerPoint.



MÓVILES REDES SOCIALES BANCO DE PRUEBAS RETINA MERISTATION

ATAQUE INFORMÁTICO >

Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero

May: Es "un ataque internacional en el que varios países y organizaciones se han visto afectadas"



PABLO GUIMÓN

Londres - 12 MAY 2017 - 16:15 ART



Prepaga Médica-Planes de Salud - Cobertura a Nivel Nacional.

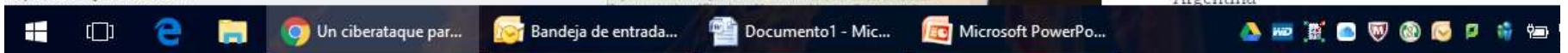
Servicio de Calidad. Amplia Cartilla de Prestadores. Consulte Planes de Salud!

acasalud.com.ar

Linterna Lumify X9

Esta increíble linterna ya está disponible en Argentina

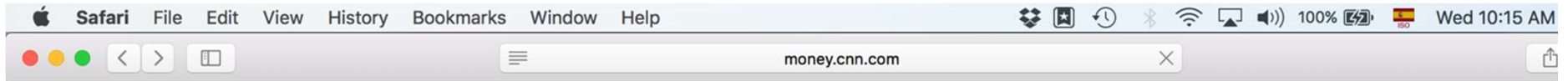
Esperando sync.teads.tv...



ATAQUES INFORMÁTICOS

The screenshot shows a web browser window with the following elements:

- Address Bar:** `tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.htm`
- Navigation Bar:** Includes icons for 'Aplicaciones', 'Proton', 'PJM SNE', 'MauriPro', 'APS Ltd', 'JIPLP', 'WIPO UDRP', 'udrp', 'EIPais.es', 'twitter', 'Sociallyaware', 'Mpons', 'LGDJ Livres', 'Perma links CC', and 'OUP Journal Tracker'.
- Menu:** 'MÓVILES REDES SOCIALES BANCO DE PRUEBAS RETINA MERISTATION'
- Section Header:** 'ATAQUE INFORMÁTICO >' followed by the main title 'El ataque de 'ransomware' se extiende a escala global'.
- Text:** 'España, Portugal, Reino Unido y Rusia, entre los afectados. Estos virus informáticos cifran la información de los ordenadores a cambio de un rescate'.
- Share Buttons:** Facebook, Twitter, and a share icon with a '275' count.
- Author:** 'JOANA OLIVEIRA | ROSA JIMÉNEZ CANO' with social media icons for Twitter and Google+.
- Location/Date:** 'Seattle / Madrid - 12 MAY 2017 - 17:23 ART'.
- Map:** A world map with blue location markers concentrated in North America, Europe, and parts of Asia.
- Error Message:** A white box with a red header 'Request denied by V' and text: 'Reason: request URL path too large. Please contact your administrator for assistance. More Details: Method: GET'.
- Taskbar:** Shows the Windows taskbar with icons for 'Ciberataque mundi...', 'Bandeja de entrada...', 'Documento1 - Mic...', and 'Microsoft PowerPo...'. The system clock shows '17:40 12/5/2017'.



BUSINESS CULTURE GADGETS FUTURE STARTUPS



DESE

Roma y Milán USD 1.330 I/V

Comprá ya

IBERIA

Consultá condiciones.

Giant Equifax data breach: 143 million people could be affected

by Sara Ashley O'Brien @saraashleyo

September 8, 2017: 9:23 AM ET

Recommend 107K

Facebook Twitter LinkedIn

PERSONAL BUSINESS GOVERNMENT ABOUT US

PRODUCTS & SOLUTIONS LEARN & SUPPORT CREDIT REPORT ASSISTANCE

Search Equifax Personal CUSTOMER LOG IN

Equifax Cybersecurity Incident: To learn more about the cybersecurity incident, including whether your personal information was potentially impacted, or to sign up for complimentary identity theft protection and credit file monitoring, [click here](#)

Your Credit, Your Identity.
Take control with a one-stop credit monitoring¹ and ID theft protection solution from Equifax.

- See your Equifax 3-Bureau credit scores in minutes
- Receive alerts about suspicious activities
- Help monitor your credit¹ and Social Security Number²

800 EQUIFAX

789 experian.

Equifax is on your side with a subscription to Equifax Complete™ Premier Plan

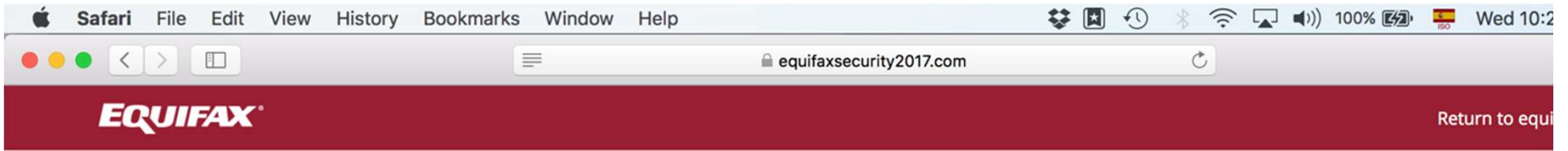
Social Surge - What's Trending

World's second biggest diamond sells for \$53 million

Equifax CEO Richard Smith is out after stunning data breach

Trump says NFL





Cybersecurity Incident & Important Consumer Information

[Consumer Notice](#)
[Am I Impacted?](#)
[What Can I Do?](#)
[News & Updates](#)
[FAQs](#)
[Contact Us](#)

[Enroll to Protect](#)
[Monitor Credit - F](#)

Recent Updates

Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search

September 26, 2017

The Board of Equifax Inc. (NYSE: EFX) today announced that Richard Smith will retire as Chairman of the Board and Chief Executive Officer, effective September 26, 2017. The Board of Directors appointed current Board member, Mark Feidler, to serve as Non-Executive Chairman. Paulino do Rego Barros, Jr., who most recently served as President, Asia Pacific, and is a seven-year veteran of the company, has been appointed

Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search

September 26, 2017

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

September 15, 2017

A Progress Update for Consumers

September 14, 2017

WSJ D.LIVE 2017
 Uber Likely to Reach a Deal With SoftBank in ...

WSJ D.LIVE 2017
 Huffington and Katzenberg Say Weinstein ...

Wireless Carriers' 'Small Cell' Push Hits California Roadblock

Microsoft Adds Surface Book 2 to Its Lineup

Facebook

Face TBH, a T Targeted Poll App



Nestle Waters The Healthy Hydration Company™

WSJ. CUSTOM STUDIOS

Water Country

Learn how a small town in Maine safeguards and shares its legendary spring water.

Watch Video

-
-
-
-
-
-

TECH

Yahoo Says Information on at Least 500 Million User Accounts Was Stolen

Internet company says it believes the 2014 hack was done by a state-sponsored actor; potentially the biggest data breach on record



THE WALL STREET JOURNAL.

Subscribe Now | Sign In

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

Search

WSJ D.LIVE 2017
Uber Likely to Reach a Deal With SoftBank in ...

WSJ D.LIVE 2017
Huffington and Katzenberg Say Weinstein ...

Wireless Carriers' 'Small Cell' Push Hits California Roadblock

Microsoft Adds Surface Book 2 to Its Lineup

Facebook TBH, a Targeted Poll App

IT'S WHO'S ON THE INSIDE THAT COUNTS.
WEEKDAYS PageSixTV.com

PageSix TV
WHERE TO WATCH



TECH

Yahoo Triples Estimate of Breached Accounts to 3 Billion

Company disclosed late last year that 2013 hack exposed private information of over 1 billion users

By *Robert McMillan and Ryan Knutson*

Updated Oct. 3, 2017 9:23 p.m. ET

A massive data breach at Yahoo in 2013 was far more extensive than previously disclosed, affecting all of its 3 billion user accounts, new parent company Verizon Communications Inc. said on Tuesday.

The figure, which Verizon said was based on new information, is three times the 1 billion accounts Yahoo said were affected when it first disclosed the breach in December 2016.

The new disclosure, four months after Verizon completed its acquisition of Yahoo, shows that executives are still coming to grips with the extent of the...

RELATED VIDEO



Latest Yahoo Cyberattack Affects 1 Billion Users

The one billion users affected by Yahoo's cyberattack news in mid-December are the most recent victims of the rising data breach issue across the world. Here's a look back at the last few years' biggest breaches. Photo: Robert Galbraith/Reuters (Originally published Dec.14, 2016)

HUAWEI

HUAWEI CONNECT 2017

Grow with the Cloud
Huawei solutions help transform Longgang into a smart digital city

ALLENDE & BREA

Contacto

Pablo Andrés Palazzi

pap@allendebrea.com.ar