Seguridad de los Sistemas Informáticos

Tema 7: Ingeniería Social

En temas anteriores …

Dentro del esquema general de seguridad, hemos estado viendo:

1. Cómo proteger físicamente el hardware para asegurar su funcionamiento.
2. Qué medidas tomar desde el sistema operativo para intentar garantizar la disponibilidad, integridad y confidencialidad de los datos y programas alojados en el sistema.
3. Cómo protegernos de posibles ataques provenientes desde la red interna de la empresa.
4. Cómo proteger a la red de la empresa y a todos sus equipos de los posibles ataques provenientes desde el exterior de la misma.

Existe un punto débil …el factor humano

Todo lo visto anteriormente es necesario y sirve para proteger nuestros activos informáticos. Si seguimos todo lo visto podemos tener una red protegida ante ataques externos e internos que ofrece suficiente seguridad.

Pero hay otro punto a considerar, que muchos autores califican como el eslabón más débil de la cadena de la seguridad.

Debemos protegernos de la torpeza/imprudencia de nuestros propios usuarios.

Existe un punto débil …el factor humano

- "Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido e ingresan en el sistema sin más. Tienen todo en sus manos." Kevin Mitnick.

Existe un punto débil …el factor humano

- En el congreso "Access All Areas" de 1997, un conferenciante aseguraba:

  "Aunque se dice que el único ordenador seguro es el que está desenchufado, los amantes de la **ingeniería social** gustan responder que siempre se puede convencer a alguien para que lo enchufe.

  El factor humano es el **eslabón más débil** de la seguridad informática. Y **no hay un sólo ordenador en el mundo que no dependa de un ser humano**, es una vulnerabilidad universal e independiente de la plataforma tecnológica".

Errores típicos…

¿De qué sirve tener un sistema de claves muy estricto si luego la clave está pegada en un post-it al lado del teclado? ¿o es el nombre de su pareja/el aniversario de su boda/el cumpleaños de su hijo…..?

¿De qué sirve encriptar la información si luego el certificado está junto a la información y sin proteger?

¿De qué sirve proteger nuestra red si luego un usuario recibe un email y responde mandando la información solicitada? ¿o instalando un troyano?

¿Qué ocurre cuando nuestro usuario publica que se va de vacaciones quince días?....

Ingeniería Social…

La mayoría de los ataques se producen a través de lo que se denomina **Ingeniería Social (Traducción de Social Engineering)**.

La Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Con este curioso término se engloba una serie de **tretas, artimañas y engaños elaborados cuyo fin es confundir al usuario o, peor todavía, lograr que comprometa seriamente la seguridad de sus sistemas.**

Ingeniería Social…Algunos ejemplos

(un poco *peliculeros*)

- https://www.youtube.com/watch?v=X1btsM3BWPI (primeros 2:44 minutos)
- https://www.youtube.com/watch?v=F78UdORll-Q (entero, pero muy interesante 1:30-4:00, o 4:45-6:00)
- https://www.youtube.com/watch?v=nxfWA1PC_U0 (película operación takedown)

Ingeniería Social…

- Según Kevin Mitnick la Ingeniería Social se basa en los siguientes cuatro principios
  - **Todos queremos ayudar**.
  - **El primer movimiento es siempre de confianza hacia el otro**.
  - **No nos gusta decir No**.
  - **A todos nos gusta que nos alaben**.
- Otros autores añaden además **el miedo**.

Obtención de Información

- El primer paso suele ser la **observación**, la **obtención de información** sobre el usuario que está disponible libremente.
  - Registro DNS (ej nic.es)
  - Redes sociales
  - Google
  - Hablar con amigos/compañeros
  - Basura……

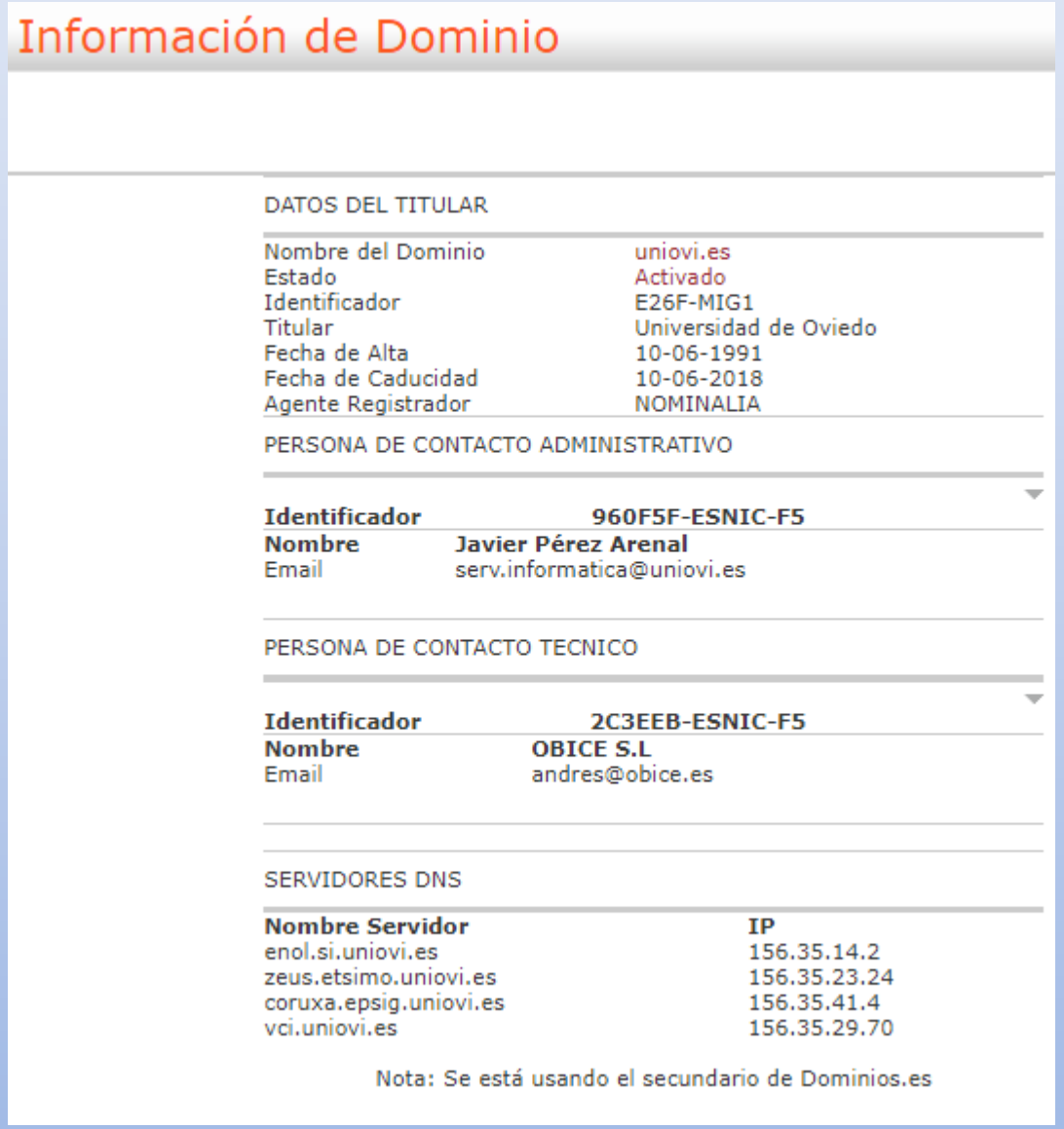
Obtención de Información

- Interesa cualquier información que ayude a conocer a la “víctima” y que permita el engaño.
  - Amistades
  - Familiares
  - Aficiones (hobbies, pertenencia a clubes….)
  - Relaciones (profesionales, afectivas….)
  - Vacaciones (fechas, lugares…..)
  - Cualquier cosa

Obtención de Información

- Engaños
  - Llamada telefónica
  - Email (adjuntos maliciosos, phising, etc.)
  - Fax
  - Correo postal
  - Cara a cara
  - Combinación de las anteriores
- A veces el objetivo del engaño no es la persona de la que tenemos la información

Observación



Información de Dominio

DATOS DEL TITULAR

Nombre del Dominio	uniovi.es
Estado	Activado
Identificador	E26F-MIG1
Titular	Universidad de Oviedo
Fecha de Alta	10-06-1991
Fecha de Caducidad	10-06-2018
Agente Registrador	NOMINALIA

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	**960F5F-ESNIC-F5**
Nombre	**Javier Pérez Arenal**
Email	serv.informatica@uniovi.es

PERSONA DE CONTACTO TECNICO

Identificador	**2C3EEB-ESNIC-F5**
Nombre	**OBICE S.L**
Email	andres@obice.es

SERVIDORES DNS

Nombre Servidor	**IP**
enol.si.uniovi.es	156.35.14.2
zeus.etsimo.uniovi.es	156.35.23.24
coruxa.epsig.uniovi.es	156.35.41.4
vci.uniovi.es	156.35.29.70

Nota: Se está usando el secundario de Dominios.es

Información obtenida en nic.es buscando el dominio uniovi.es (03/2018)
Vamos a buscar ese tal "*andres*" de OBICE S.L. (el otro es demasiado fácil)

Observación

- Empezamos con una búsqueda en google….. “obice.es andres@obice.es”

- Ya sabemos su nombre….. “andres borrego conde”

Observación

- Encontramos su perfil en Linkedin.
- Una foto
- Recaudación en el BOPA (con su NIF/CIF)
- ¿Twitter.. ?
- ¿Club Voleibol Oviedo?

www.cibersociedad.net/congres2004/usuaris/fitxa.php?

Aplicaciones | Oracle | Dani | Solicitud:Vivir en Ast... | Luis | monitora

ANDRÉS BORREGO CONDE

- Main language: castellano
- From: Cayes (LLANERA) - Asturias - Spain
- Birth year: 1972
- Center/Company: B2B Integral
- Profile: Consultor de Integración de Sistemas

Role(s) in the Conference

- Coordinator of the Working Group 13: Data Protection in public administration

Preferred Working Groups

- No information available

Buscar gente, empleos, empresas y demás

Andrés Borrego Conde

Consultor TIC-SEGURIDAD-CONTINUIDAD DE NEGOCIO

Gijón y alrededores, España | Servicios y tecnologías de la información

Actual	OBICE, S.L., Legal Protect, S.L.
Anterior	SIGEA, SISTEMAS DE PROTECCIÓN DE LA INFORMACIÓN, S.L., B2B Integral, S.A.
Educación	Universidad de Oviedo

Conectar | Enviar un mensaje InMail a Andrés | 32 contactos

es.linkedin.com/pub/andrés-borrego-conde/11/366/6a3

Buscar gente, em

Inicio | Perfil | Red | Empleos | Intereses

- ELABORACIÓN y COORDINACIÓN DE PROYECTOS DE
- IMPLANTACIÓN DE SISTEMAS DE GESTIÓN: ISO 2000

Gerente
SIGEA, SISTEMAS DE PROTECCIÓN DE LA INFORMA
noviembre de 2007 – enero de 2011 (3 años 3 meses)

Gerente
B2B Integral, S.A.
octubre de 2002 – agosto de 2005 (2 años 11 meses)

Trayectoria profesional y académica

Experiencia

Gerente
OBICE, S.L.
agosto de 2005 – actualidad (9 años 8 meses)

- GESTIÓN EMPRESARIAL
- ELABORACIÓN y COORDINACIÓN DE PROYECTOS TIC: Telecomunicaciones, Sistemas, Diseño CPD's.
- CONSULTOR y AUDITOR DE SEGURIDAD

Gerente
Legal Protect, S.L.
enero de 2004 – actualidad (11 años 3 meses)

Observación

- En cinco minutos hemos conseguido foto y mucha información libremente accesible
  - Ha dado varias charlas en la Facultad Economía→ posibles contactos
  - En tiempos estuvo en el Club Voleibol Oviedo (como presidente) y luego en otros→aficiones
  - Tenemos su histórico de empresas (Linkedin, http://administradores.eleconomista.es/Administrador_BORREGO-CONDE-ANDRES.html)
  - Su perfil en Linkedin→ con sus contactos
  - Su perfil de ¿Twitter?….

Observación

- Dumpster Diving
  - Consiste en obtener información que se haya “tirado”.
  - Puede ser físico: cubos de basura, papel de impresora, discos duros que se eliminan.
  - O Lógico: por ejemplo examinar el buffer de una impresora.

El PP "rayó, rompió y tiró a la basura" los discos duros de Bárcenas

Multa de 300.000 euros por tirar a la basura datos clínicos

Tira por error a la basura un disco duro con 7,5 millones en Bitcoins

Expediente a cinco tribunales por dejar datos personales en la basura

La Agencia Española de Protección de Datos puede sancionarlos hasta con 600.000 euros - Quedaron expuestos casos de abusos y violencia machista

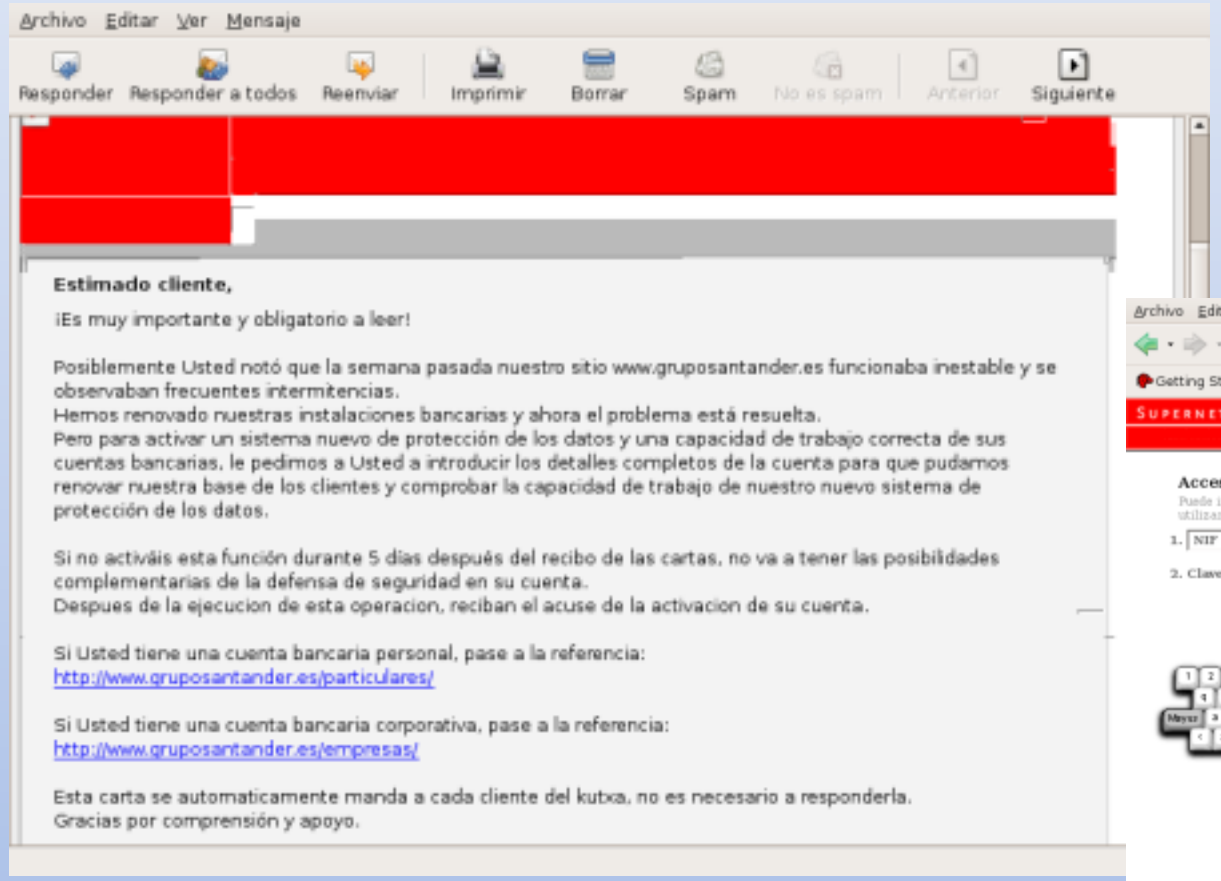
Engaño

- Tras la observación disponemos de información que puede facilitarnos el engaño para conseguir que el usuario haga lo que queremos.
- Se pueden probar distintas técnicas genéricas
  - Phising
  - Pretexting
  - Media Dropping /Baiting
  - Tailgating

Phising

- El *phising* consiste en el envío de un correo al usuario donde se le convence para que haga algo. Normalmente el objetivo es robar algún tipo de contraseña o información valiosa, pero también puede ser instalar algún tipo de malware.
- Normalmente se envía un email fingiendo ser un remitente de confianza y se solicita que se verifique cierta información (cuenta/contraseña…)
  - Bancos
  - Servicios de email
- Existen muchas herramientas para automatizar el proceso como Social Engineering Toolkit (SET) de código abierto.
- También se puede enviar un email notificando una *sanción* que debe abonarse por visualizar contenido inapropiado (http://blog.trendmicro.com/another-russian-ransomware-spotted/)

Phising


Archivo Editar Ver Mensaje
Responder
Responder a todos
Reenviar
Imprimir
Borrar
Spam
No es spam
Anterior
Siguiente
Estimado cliente,
¡Es muy importante y obligatorio a leer!
Posiblemente Usted notó que la semana pasada nuestro sitio www.gruposantander.es funcionaba inestable y se observaban frecuentes intermitencias.
Hemos renovado nuestras instalaciones bancarias y ahora el problema está resuelta.
Pero para activar un sistema nuevo de protección de los datos y una capacidad de trabajo correcta de sus cuentas bancarias, le pedimos a Usted a introducir los detalles completos de la cuenta para que pudamos renovar nuestra base de los clientes y comprobar la capacidad de trabajo de nuestro nuevo sistema de protección de los datos.
Si no activáis esta función durante 5 días después del recibo de las cartas, no va a tener las posibilidades complementarias de la defensa de seguridad en su cuenta.
Despues de la ejecucion de esta operacion, reciban el acuse de la activacion de su cuenta.
Si Usted tiene una cuenta bancaria personal, pase a la referencia:
http://www.gruposantander.es/particulares/
Si Usted tiene una cuenta bancaria corporativa, pase a la referencia:
http://www.gruposantander.es/empresas/
Esta carta se automaticamente manda a cada cliente del kutxa, no es necesario a responderla.
Gracias por comprensión y apoyo.


Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.gruposantahder.com/particulares/
Getting Started
Latest BBC Headlines
SUPERNET
Particulares
Empresas e Instituciones
Acceso para Particulares
Ver Ayuda
1. NIF
2. Clave de Acceso
Entrar
Seguridad
¿Ha olvidado su clave?
Atención al Cliente
Buzón de contacto
Mapa de oficinas
Información sobre Supernet
Visite nuestra DEMO
Contraste:
alto
bajo
Terminado

Pretexting

- Consiste en usar un *pretexto* para conseguir que un usuario ejecute algún tipo de programa o nos proporcione cierta información.
  - Suele ser necesario contar con información previa sobre el objetivo.
  - Se suelen suplantar identidades.
- Ej: Te llama la “policía”/servicio técnico y te pide que entres en una web o que proporciones cierta información.
- Ej: Te llaman para ofrecerte una gran promoción de XXX, te envían el resto de información a tu correo en un adjunto (con malware).

Pretexting


MR. JONES, I'M CALLING FROM YOUR CREDIT CARD COMPANY TO TELL YOU THAT A CROOK HAS STOLEN YOUR IDENTITY!
TO CONFIRM THAT I'M SPEAKING WITH THE REAL MR. JONES, I'LL NEED YOU TO TELL ME YOUR SOCIAL SECURITY NUMBER, DATE OF BIRTH AND MOTHER'S MAIDEN
999-99-9999, 5/22/1949, AND SMITH.....ANY IDEA HOW MY INFORMATION WAS COMPROMISED?
HELLO?
HELLO?
WWW.CALLCENTERCOMICS.COM

Media Dropping/Baiting

- El famoso *caballo de Troya*. Consiste en dejar “olvidado” un USB/DVD/HD en algún sitio que frecuente nuestra víctima (aseos, aparcamiento cerca de su coche, suelo cerca de su mesa..) con alguna etiqueta “jugosa” (RRHH, propuesta de salarios, plan estratégico 2020…). Obviamente al introducirlo en el sistema se intentará instalar algún tipo de malware.

Quid pro Quo

- Ej: Se puede ir llamando aleatoriamente diciendo que eres del “servicio técnico” y llamas por “su problema”. Alguna vez encuentras a alguien que sí que tiene un problema y luego consigues que haga lo que quieras.
- Ej: Existen varias investigaciones que consiguieron que los empleados de una empresa suministraran sus contraseñas a cambio de pequeños regalos (boli, chocolatina…). Con tasas del 90% de éxito.

Tailgating/Shoulder Surfing

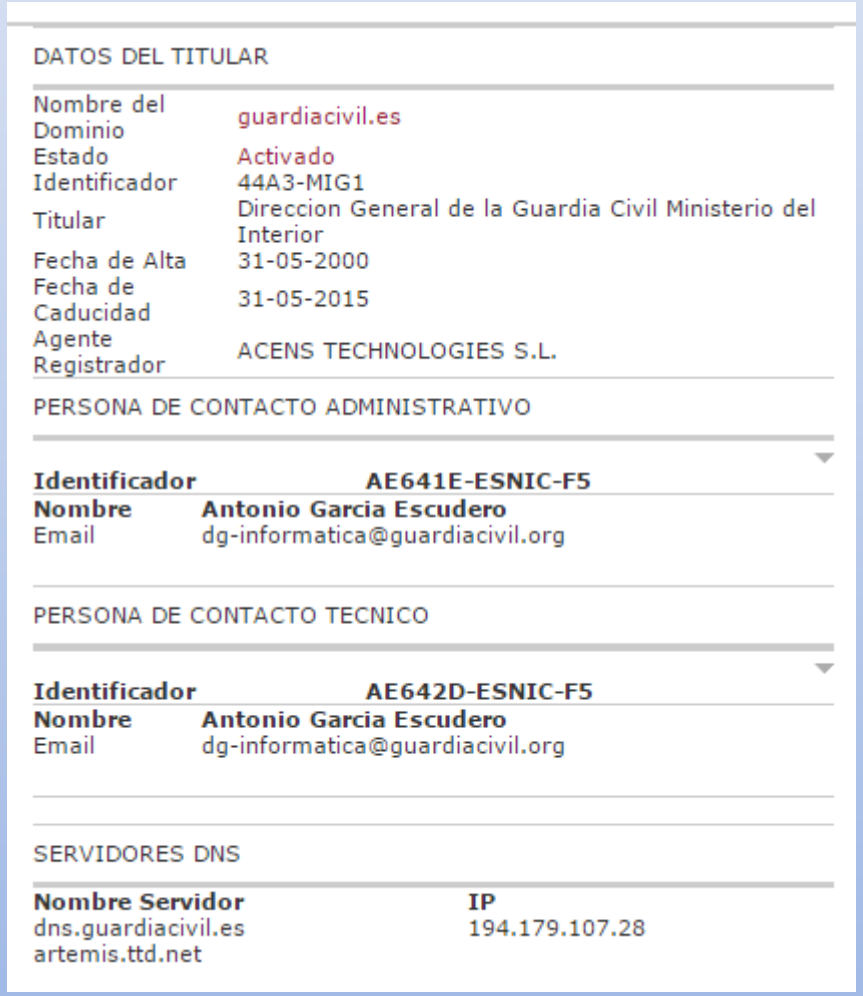
- El Tailgating consiste en “colarse” detrás de alguien a una zona de acceso restringido. Suele funcionar por la cortesía.
- El Shoulder Surfing consiste en “mirar por encima del hombro” mientras el usuario introduce información. Normalmente en lugares públicos.

Un ejemplo real

En 1999 La Guardia Civil sufrió un ataque que redirigió su Web a un sitio gay. http://www.hispahack.com/oldweb/mi029.htm

El ataque no fue directamente contra sus servidores. Engañaron a la empresa que gestionaba el dominio (Network Solutions).

El efecto fue que al intentar acceder a su web se accedía a otra web.



DATOS DEL TITULAR

Nombre del Dominio	guardiacivil.es
Estado	Activado
Identificador	44A3-MIG1
Titular	Direccion General de la Guardia Civil Ministerio del Interior
Fecha de Alta	31-05-2000
Fecha de Caducidad	31-05-2015
Agente Registrador	ACENS TECHNOLOGIES S.L.

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	**AE641E-ESNIC-F5**
Nombre	**Antonio Garcia Escudero**
Email	dg-informatica@guardiacivil.org

PERSONA DE CONTACTO TECNICO

Identificador	**AE642D-ESNIC-F5**
Nombre	**Antonio Garcia Escudero**
Email	dg-informatica@guardiacivil.org

SERVIDORES DNS

Nombre Servidor	**IP**
dns.guardiacivil.es	194.179.107.28
artemis.ttd.net	

Unos ejemplos reales

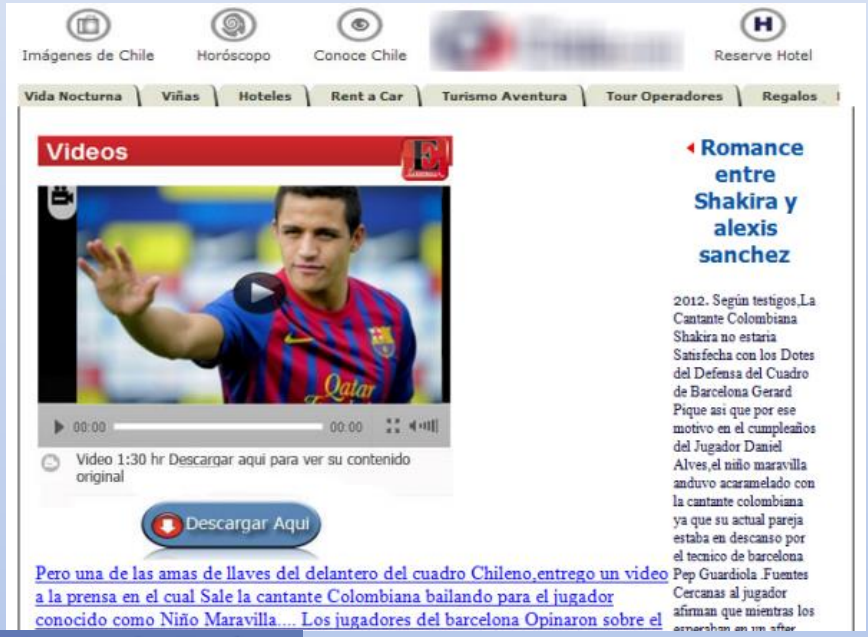
- Pocos minutos después del terremoto de Japón de 2011 varias páginas web “ofrecían” información detallada en tiempo real cuando lo que en realidad hacían era instalar malware (http://blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/)
  - Existen herramientas como SET que te permiten crear una web así en pocos minutos
- Al entrar en una página se te informa de que *se ha detectado un virus,* a la vez que se ofrecen (te venden) a *limpiar* el ordenador mediante su antivirus. En el mejor de los casos es un antivirus real que no necesitabas, en la mayoría es malware (http://blog.trendmicro.com/targeting-the-source-fakeav-affiliate-networks/)

Unos ejemplos reales

El día 23 de Diciembre 2014 a las 12 am. Se regalarán 200 Blanco, 200 Negros y 200 dorados los ganadores se publicaran aquí, luego nos pondremos en contacto con dichos ganadores y les enviaremos el iPhone 6 a la dirección deseada.
¿Quieres uno? Sólo tienes que seguir estos 4 sencillos pasos:
1) "Compartir" esta foto
2) Haga clic en "Me gusta" en esta foto
3) Comenta el color que te guste solo una vez: blanco,negro o dorado

OJO: esta parte es vital, ya que solo los números registrados entrarán al concurso, de esa forma nos comunicaremos con ellos si resultan ser uno de los ganadores.

4)"Enviar su numero de contacto AQUI:▶▶ http://



Unos ejemplos reales

- https://twitter.com/cr3d1tc4rds?lang=es
- https://twitter.com/needadebitcard

Un ejemplo ¿Real?

- A modo de ejemplo de lo que se puede hacer con la información que voluntariamente publica la gente en sus perfiles……

  Sin preguntar el nombre….

  …..Únicamente con una foto….

  …..Y algo de paciencia y pericia

  Parece que es real (solo muestran los casos de éxito)

  - https://www.youtube.com/watch?v=NR279FlzD4s

Protección

- Educar a todo el personal con protocolos de cómo actuar. ¿A todos?→A **todos** incluido el personal de limpieza.
- Analizar con herramientas adecuadas todo el tráfico entrante.
- No informar telefónicamente (ni por otros medios similares) de características técnicas, datos del personal, etc.
- Control de acceso físico a las instalaciones.
- Realizar pruebas para verificar las medidas.