
Generando confianza en el correo electrónico

Miguel Macías Enguïdanos
miguel.macias@upv.es



Red
IRIS



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Jornadas Técnicas
Valladolid, 01/12/2011

Índice

- Scams
 - fraudes a través del e-mail
- Una solución: el procedimiento CFD
- S/MIME
- Aspectos a tener en cuenta
- Conclusiones

La gota que colma el vaso

■ Mensaje de correo recibido en la UPV (agosto 2008)

Estimado **Universidad Politécnica de Valencia los usuarios** de correo web,

Este mensaje es de la Universidad Politécnica de Valencia, **centro de mensajería** para todos Universidad Politécnica de Valencia webmail **users**. **We son** actualmente la mejora de nuestra base de datos y e-mail centro. Estamos suprimiendo todos los no utilizados **upf.edu** correo electrónico, Usted está obligado a verificar y actualizar su mensaje de correo electrónico confirmando su identidad. Esto evitará que su dirección de correo electrónico **de concluidos** durante este ejercicio. Con el fin de confirmar la identidad de correo electrónico que usted, **usted es** para proporcionar los siguientes datos;

Confirmar su identidad **por debajo** de correo electrónico

Nombre :.....

Apellido :.....

Email Nombre de usuario:

E-mail Contraseña:

¡Advertencia! Universidad Politécnica de Valencia

Email usuario que se niega a verificar y, posteriormente, actualizar su correo electrónico dentro de los siete días de haber recibido esta advertencia **perderá su correo electrónico permanentemente**.

Thank you for using Universidad Politécnica de correo electrónico!

Advertencia Código: VX2G99AAJ

Gracias,

Universidad Politécnica de Valencia **Centro de Mensajes...**

La gota que colma el vaso

■ Mensaje de correo recibido en la UPV (agosto 2008)

Estimado **Universidad Politécnica de Valencia los usuarios** de correo web,

Este mensaje es de la Universidad Politécnica de Valencia, **centro de mensajería** para todos Universidad Politécnica de Valencia webmail **users. We son** actualmente la mejora de nuestra base de datos y e-mail centro. Estamos suprimiendo

todos
elect
ejerc
datos

Durante el verano de 2008 varias Universidades Españolas sufrieron una ataque de Phishing dirigido cuyo objetivo era el de recopilar credenciales webmail para realizar, a partir de dichas cuentas, diversos ataques de envío de SPAM indiscriminado, suplantación de identidad, etc..

Conf

Nom
Apel
Ema
E-ma

Fueron 12 las instituciones de RedIRIS afectadas por este ataque, y aunque el número de cuentas de webmail comprometidas no fue muy elevado, el uso de las mismas por los atacantes para enviar SPAM fue extensivo.

¡Adv
Ema
recib

RedIRIS: Informe de incidentes de seguridad año 2008

<http://www.rediris.es/cert/doc/informes/2008/>

Thar

Advertencia Código: VX2G99AAJ

Gracias,

Universidad Politécnica de Valencia **Centro de Mensajes...**

La evolución de los ataques

■ Mensaje recibido en la UJI en julio de 2009

From: UJI LEQUIP DE SUPORT

Benvolgut Propietari **Email UJI**,
Aquest missatge és **UJI del centre de missatges** de correu electrònic a tots els **propietaris UJI**. Ara som la millora de la nostra base de dades i de correu electrònic està esborrant tots els **center.We UJI correu** no utilitzats per crear més espai per a un nou

=====
Per **evitar el tancament del seu compte** vostè haurà d'actualitzar que a continuació per que sabrà que es tracta d'un compte utilitzen actualment

=====
CONFIRMAR SU EMAIL **AVALL**

EMAIL nom d'usuari:

EMAIL CONTRASENYA:

CONFIRM EMAIL CONTRASENYA:

DATA DE NAIXEMENT:

De correu electrònic alternativa:

=====
Advertència! En cas contrari, **fer** immediatament **la seva** compte desactivada del nostre **database.We** disculpes per les molèsties que això causa que durant aquest període, però la confiança que entén que la nostra principal preocupació és per als nostres **clients** i per a la seguretat dels seus **clients data. our** són totalment segurs

Gràcies,

UJI L'EQUIP DE SUPORT

□ <http://blogsi.uji.es/correu/2009/07/>

La evolución de los ataques

■ Primer *phishing* al correo de la UPV (enero 2010)



UNIVERSIDAD
POLITECNICA
DE VALENCIA

Hola,

Debido a la actualización de nuestro SECURITY nuevos y la eliminación de todas las cuentas no utilizadas tendrá que confirmar su dirección de e-mail con la firma en su cuenta. También sería cerrar todas las cuentas no utilizadas.

Lo que hay que hacer:

1. Inicie sesión en su cuenta en <https://webmail.upv.es>, haciendo clic en la URL.
2. Introduzca su ID de usuario y contraseña.
3. Una vez que inicie sesión en un nuevo perfil de seguridad se actualizará para su cuenta.

Después de seguir las instrucciones de la carta, su cuenta no será interrumpido y continuará como normal. Gracias por su atención a esta solicitud. Nos disculpamos por cualquier inconveniente.

Por favor, acceda a su cuenta inmediatamente y seguir utilizando la cuenta de forma habitual mientras disfruta de nuestras nuevas actualizaciones de seguridad.

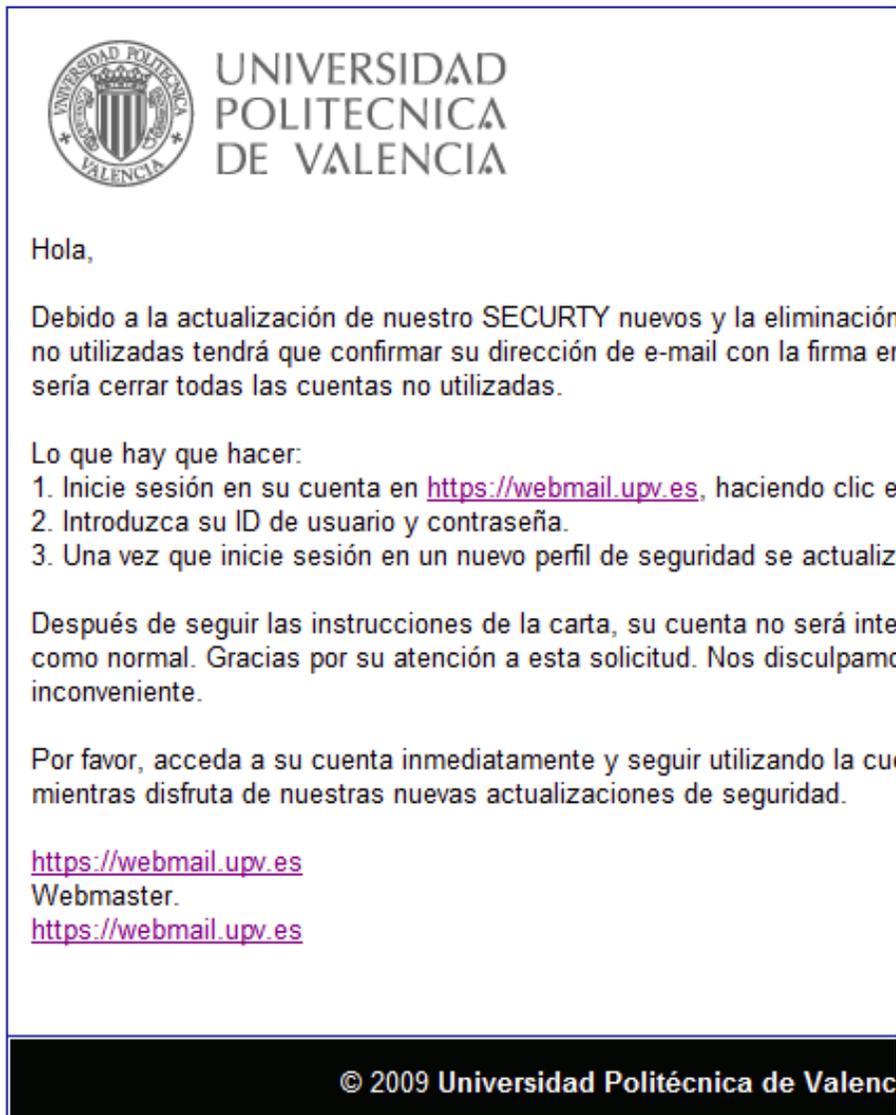
<https://webmail.upv.es>
Webmaster.
<https://webmail.upv.es>

© 2009 Universidad Politécnica de Valencia

■ <http://asic.blogs.upv.es/correo-electronico/¡no-te-dejes-enganar/>

La evolución de los ataques

■ Primer *phishing* al correo de la UPV (enero 2010)



 UNIVERSIDAD
POLITECNICA
DE VALENCIA

Hola,

Debido a la actualización de nuestro SECURITY nuevos y la eliminación no utilizadas tendrá que confirmar su dirección de e-mail con la firma en sería cerrar todas las cuentas no utilizadas.

Lo que hay que hacer:

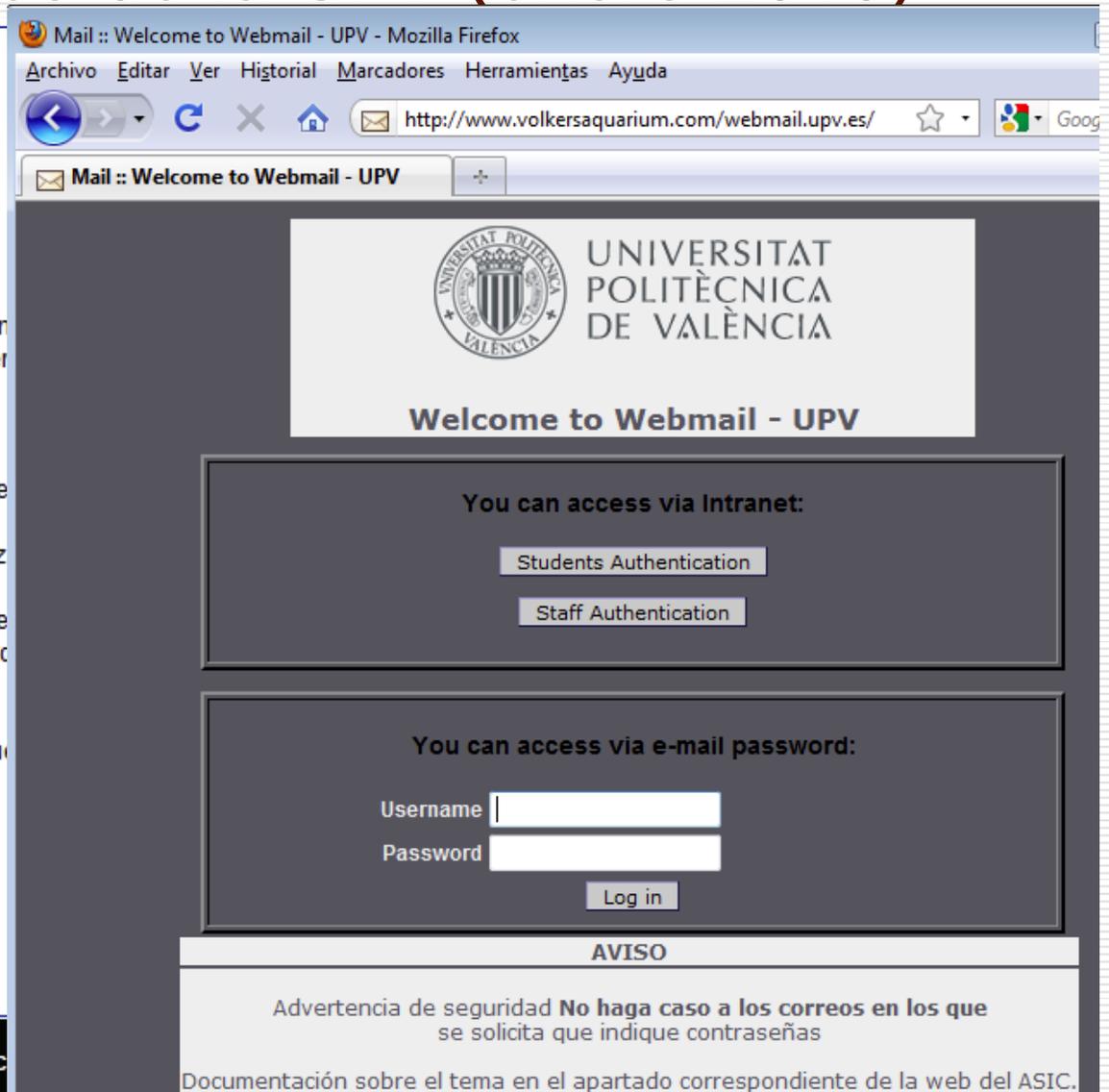
1. Inicie sesión en su cuenta en <https://webmail.upv.es>, haciendo clic e
2. Introduzca su ID de usuario y contraseña.
3. Una vez que inicie sesión en un nuevo perfil de seguridad se actualiz

Después de seguir las instrucciones de la carta, su cuenta no será inte como normal. Gracias por su atención a esta solicitud. Nos disculpamc inconveniente.

Por favor, acceda a su cuenta inmediatamente y seguir utilizando la cu mientras disfruta de nuestras nuevas actualizaciones de seguridad.

<https://webmail.upv.es>
Webmaster.
<https://webmail.upv.es>

© 2009 Universidad Politécnica de Valenc



Mail :: Welcome to Webmail - UPV - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

<http://www.volkersaquarium.com/webmail.upv.es/>

Mail :: Welcome to Webmail - UPV

 UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Welcome to Webmail - UPV

You can access via Intranet:

Students Authentication

Staff Authentication

You can access via e-mail password:

Username

Password

Log in

AVISO

Advertencia de seguridad **No haga caso a los correos en los que se solicita que indique contraseñas**

Documentación sobre el tema en el apartado correspondiente de la web del ASIC.

■ <http://asic.blogs.upv.es/correo-electronico/jno-te-dejes-enganar/>

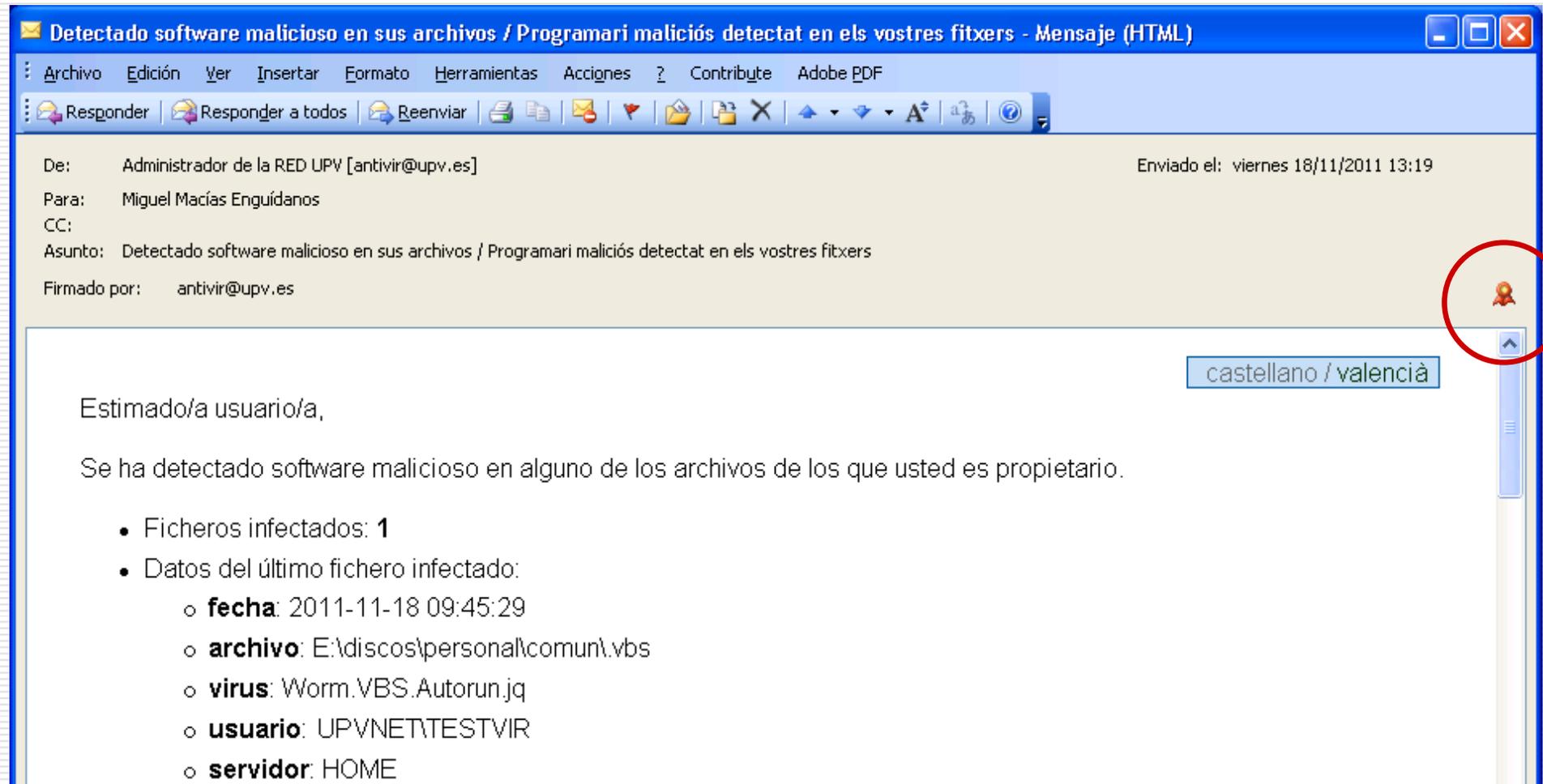
Posibles contramedidas

- Se necesita un sistema que permita al usuario determinar, fácilmente y por su cuenta, si un mensaje de correo es legítimo o no
- Añadir mensajes y advertencias a los propios mensajes y a las páginas web ¡no es efectivo!
 - los usuarios no solemos leer todo el contenido
 - las advertencias se pueden copiar en los fraudes
- S/MIME es el mecanismo ideal...
 - garantiza la integridad del mensaje y la cuenta remitente
- ... si no fuera porque:
 - algunos clientes de correo no dan soporte a S/MIME
 - la mayoría de los usuarios no tiene la cultura necesaria

El procedimiento CFD en la UPV

- La UPV puso en marcha el **procedimiento CFD** (Correos Firmados Digitalmente) en noviembre/2009
- Todos los correos oficiales (correos cuyo remitente es un servicio de la Universidad):
 - se firman digitalmente
 - pueden consultarse desde la Intranet de la UPV
- Así pues, cuando un usuario tiene dudas sobre la autenticidad de un mensaje:
 - puede comprobar si está firmado digitalmente y verificar que la firma es correcta
 - puede entrar en la Intranet y comprobar que el mensaje (con todo el contenido) se ha enviado oficialmente

Mensaje firmado digitalmente



Detectedo software malicioso en sus archivos / Programari maliciós detectat en els vostres fitxers - Mensaje (HTML)

Archivo Edición Ver Insertar Formato Herramientas Acciones ? Contribuye Adobe PDF

Responder Responder a todos Reenviar

De: Administrador de la RED UPV [antivir@upv.es] Enviado el: viernes 18/11/2011 13:19

Para: Miguel Macías Enguídanos

CC:

Asunto: Detectado software malicioso en sus archivos / Programari maliciós detectat en els vostres fitxers

Firmado por: antivir@upv.es

castellano / valencià

Estimado/a usuario/a,

Se ha detectado software malicioso en alguno de los archivos de los que usted es propietario.

- Ficheros infectados: 1
- Datos del último fichero infectado:
 - **fecha:** 2011-11-18 09:45:29
 - **archivo:** E:\discos\personal\comun\.vbs
 - **virus:** Worm.VBS.Autorun.jq
 - **usuario:** UPVNET\TESTVIR
 - **servidor:** HOME

Área de Sistemas de Información y Comunicaciones

Para garantizar su integridad y autenticidad, este correo se ha firmado digitalmente y puede comprobarse su envío, si usted es miembro de la UPV, desde la Intranet.

valencià / castellano

Benvolgut usuari,

Lista de mensajes oficiales

Correos Oficiales de la UPV - Windows Internet Explorer

https://www.upv.es/pls/soalu/sic_cfd.Entrada

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Intranet :: Consulta CFD

Correos Oficiales de la UPV

Correos Oficiales de la UPV

Para comprobar la autenticidad de los correos oficiales que ha recibido desde la UPV, puede consultar los últimos mensajes que se le han enviado en el siguiente listado.
Tenga en cuenta que estos correos también han sido firmados digitalmente, de manera que puede comprobar su autenticidad desde su cliente de correo habitual.

Panel de Entrada

#	Asunto	Remitente	Fecha	Adjunto/s
1	Cuestionario Evaluación Programa Impulso	Administrador de la red UPV	22/11/2011 09:35:04	0
2	Actualización de su buzón de correo Exchange / Actualització de la seua bústia de correu Exchange	Administrador de la red UPV	22/11/2011 00:18:18	0
3	Gaudeix amb la UPV d'un doble descompte del 40% en 'Nunca es tarde', d'Àngel Martín / Disfruta con la UPV de un doble descuento del 40% en 'Nunca es tarde'...	Àrea de Gestió Cultural	19/11/2011 02:03:27	0
4	Detectado software malicioso en sus archivos / Programari maliciós detectat en els vostres fitxers	Administrador de la RED UPV	18/11/2011 13:19:02	0
5	Boletín del Centro de Formación Permanente (MIGUEL MACIAS ENGUIDANOS) (Publicidad)	Info CFP	18/11/2011 01:48:05	0
6	Publicación de OAs libres en Youtube e ItunesU	Docencia en red	16/11/2011 01:56:56	0

Mensaje consultado en la Intranet

The screenshot shows a web browser window titled "Correos Oficiales de la UPV - Windows Internet Explorer". The address bar shows the URL: https://www.upv.es/pls/soalu/sic_cfd.Mensaje?P_ID=83427E90F9E1754797DE008F2A198B1987DEA031. The browser's address bar also shows "Google (España)".

The page header includes the logo of the Universitat Politècnica de València and the text "UNIVERSITAT POLITÈCNICA DE VALÈNCIA". Below the header, there is a navigation bar with the text "Intranet :: Consulta CFD :: Panel de Entrada" and a "Cerrar sesión" button.

Correos Oficiales de la UPV

Panel de Mensaje

Remitente	Administrador de la RED UPV <antivir@upv.es>
Enviado	18/11/2011 13:19:02
Asunto	Detectado software malicioso en sus archivos / Programari maliciós detectat en els vostres fitxers
Versión HTML	Ver Mensaje en formato HTML

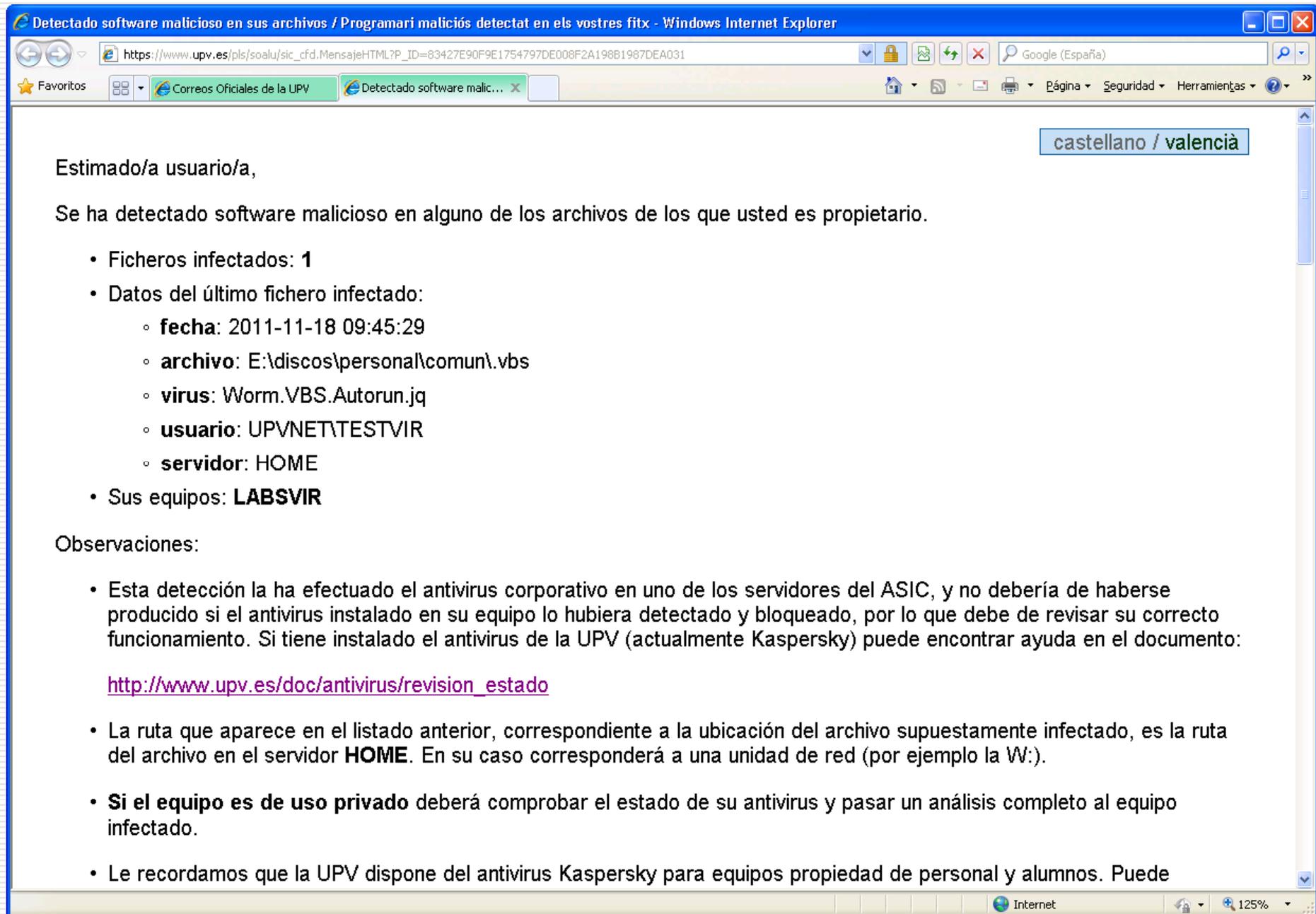
Mensaje

Estimado/a usuario/a,

Se ha detectado software malicioso en alguno de los archivos de los que usted es propietario.

- Ficheros infectados: 1
- Datos del último fichero infectado:
 - fecha: 2011-11-18 09:45:29
 - archivo: E:\discos\personal\comun\vbs
 - virus: Worm.VBS.Autorun.jq
 - usuario: UPVNET\TESTVIR

Mensaje consultado en la Intranet



Detectado software malicioso en sus archivos / Programari maliciós detectat en els vostres fitx - Windows Internet Explorer

https://www.upv.es/pls/soalu/sic_cfd.MensajeHTML?P_ID=83427E90F9E1754797DE008F2A196B1987DEA031

Google (España)

Favoritos

Correos Oficiales de la UPV

Detectado software malici...

castellano / valencià

Estimado/a usuario/a,

Se ha detectado software malicioso en alguno de los archivos de los que usted es propietario.

- Ficheros infectados: **1**
- Datos del último fichero infectado:
 - **fecha:** 2011-11-18 09:45:29
 - **archivo:** E:\discos\personal\comun\.vbs
 - **virus:** Worm.VBS.Autorun.jq
 - **usuario:** UPVNET\TESTVIR
 - **servidor:** HOME
- Sus equipos: **LABSVIR**

Observaciones:

- Esta detección la ha efectuado el antivirus corporativo en uno de los servidores del ASIC, y no debería de haberse producido si el antivirus instalado en su equipo lo hubiera detectado y bloqueado, por lo que debe de revisar su correcto funcionamiento. Si tiene instalado el antivirus de la UPV (actualmente Kaspersky) puede encontrar ayuda en el documento:
http://www.upv.es/doc/antivirus/revision_estado
- La ruta que aparece en el listado anterior, correspondiente a la ubicación del archivo supuestamente infectado, es la ruta del archivo en el servidor **HOME**. En su caso corresponderá a una unidad de red (por ejemplo la W:).
- **Si el equipo es de uso privado** deberá comprobar el estado de su antivirus y pasar un análisis completo al equipo infectado.
- Le recordamos que la UPV dispone del antivirus Kaspersky para equipos propiedad de personal y alumnos. Puede

Internet 125%

Certificados digitales

- S/MIME implica la utilización de certificados digitales para todas las direcciones oficiales de la UPV
 - los certificados tienen que ser válidos y reconocidos por la mayoría de clientes
- Utilizamos los certificados gratuitos de Comodo:
 - Free Secure Email Certificates
<https://www.instantssl.com/>
- Tienen una validez de 1 año
- Pueden renovarse tantas veces como se quiera
- Centralizamos la gestión de los certificados



Información del certificado

Este certificado está destinado a los siguientes propósitos:

- Protege los mensajes de correo electrónico
- 1.3.6.1.4.1.6449.1.2.1.1.1

Enviado a: ras@upv.es

Emitido por: UTN-USERFirst-Client Authentication and Email

Válido desde: 26/04/2011 **hasta:** 26/04/2012

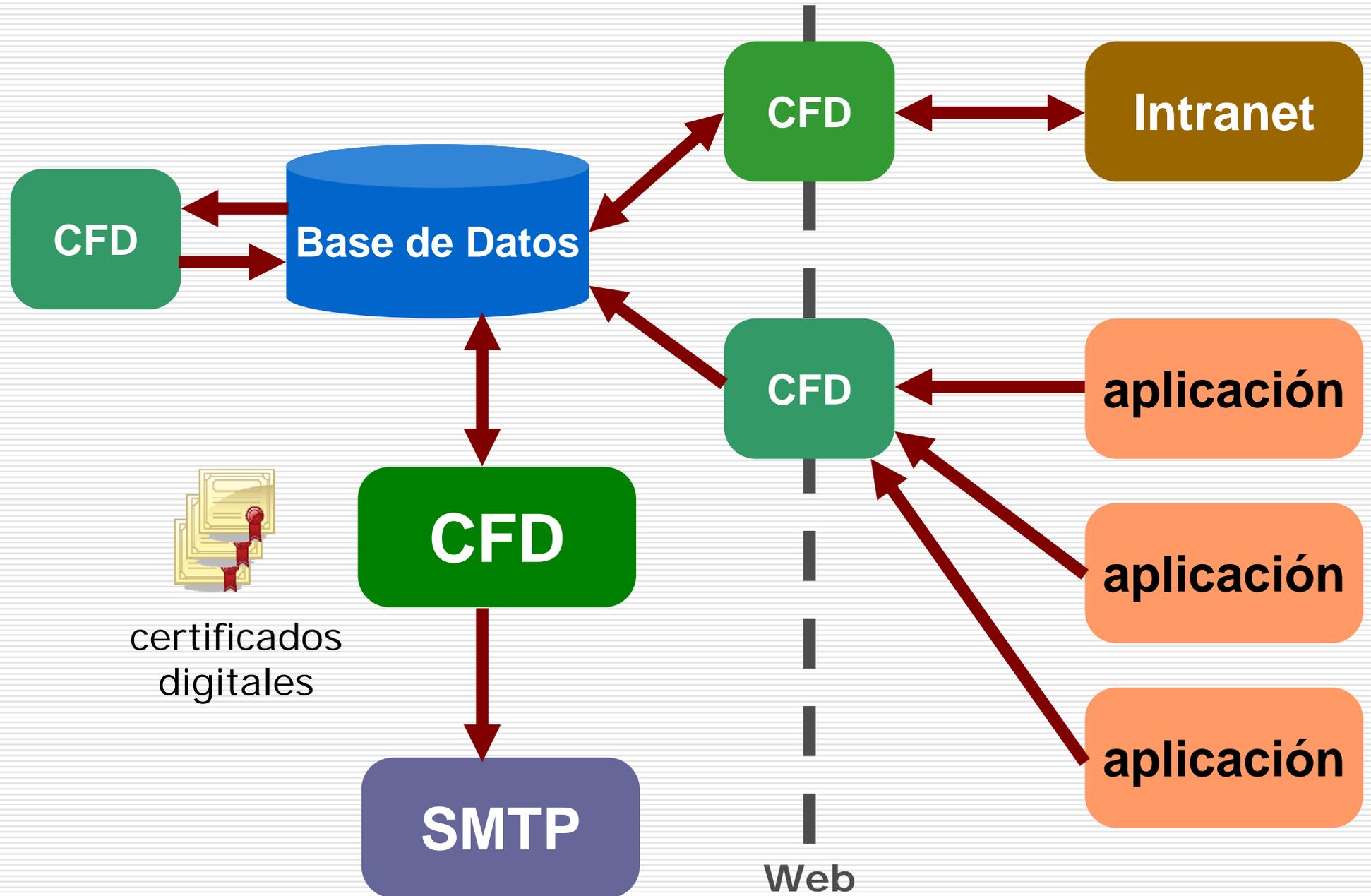
COMODO

- UTN-USERFirst-Client Authentication and Email
- ras@upv.es

Consulta de correos en la Intranet

- La decisión de mostrar los mensajes oficiales en la Intranet ha contribuido al éxito de la iniciativa:
 - los usuarios conocen y confían en la Intranet
- Pero ha 'complicado' la solución necesaria para aportar confianza al correo electrónico
- Todos los mensajes han de conservarse en Base de Datos durante un tiempo mínimo
 - actualmente conservamos los mensajes durante 2 meses
- La escalabilidad de la solución es un factor determinante para el éxito de la misma
 - en estos momentos se están enviando una media de 23000 mensajes de correo, por semana, a través de CFD

Arquitectura de CFD



Las interfaces de CFD

- Para que la solución fuese efectiva, teníamos que permitir que cualquier tipo de aplicación fuese capaz de generar envíos
- Hay aplicaciones corporativas basadas en paquetes de la Base de Datos, así pues, CFD tiene un interfaz de envío en la propia Base de Datos
 - PL/SQL sobre Oracle
- Para el resto de aplicaciones se optó por implementar un servicio Web, con autenticación básica sobre SSL y filtrado de IPs
 - se utiliza XML como formato de intercambio de datos

Plantillas de mensajes

- Para optimizar recursos, CFD gestiona los mensajes a través de plantillas
- Cada plantilla define:
 - el remitente (nombre y dirección de correo)
 - el asunto
 - el cuerpo del mensaje (formatos TEXTO y HTML)
 - adjuntos (si los tiene)
- Para cada envío el asunto y el cuerpo del mensaje pueden personalizarse (con variables de reemplazo)
- También se admite cambiar el remitente (dentro de los admitidos para una plantilla) y añadir adjuntos distintos para cada envío

Destinatarios

- Se admiten destinatarios internos y externos
 - utilizando los campos Para, Copia y Copia oculta
- Para los internos (miembros de la UPV), CFD busca el nombre y dirección de correo oficiales
 - y mantiene los mensajes para que pueden consultarse, posteriormente, desde la Intranet
- Las listas de correo son eficientes para el envío, pero ¡sus miembros cambian con el tiempo!
 - se utiliza la lista para el envío
 - se 'despliega' la lista en Base de Datos, almacenando los miembros de la misma en el momento del envío
- CFD permite detectar direcciones de correo erróneas

Equidad en el reparto de recursos

- Algunas plantillas de correo, en CFD, se utilizan para envíos masivos
 - ej.: boletines a suscriptores
- Otras plantillas tienen un uso mucho menor, pero requieren la inmediatez del envío
 - ej.: códigos de comprobación de direcciones de correo
- Actualmente se está 'penalizando' a los envíos masivos para dar salida inmediata al resto de envíos
- En cada invocación del procedimiento se comprueba el total de envíos pendientes para cada plantilla
- Se envían mensajes pendientes de todas las plantillas, pero con un límite de envíos

Añadiendo un servicio al CFD

- Los pasos que seguimos para añadir un nuevo servicio al procedimiento CFD son:
 - solicitar certificados digitales para todas las cuentas (no personales) que se utilizan desde el servicio
 - generar plantillas de mensajes (normalmente se empieza con una plantilla genérica)
 - dar de alta al usuario y las IP que invocarán a CFD
 - proporcionar código de ejemplo, según la tecnología que se utilice en el servicio, de acceso a CFD
- Se hace una integración gradual, empezando con una cuenta de correo y un tipo de mensajes y se va ampliando, rápidamente, a la totalidad del servicio

A tener en cuenta: certificados

- Para la emisión/renovación de los certificados digitales que utilizamos se comprueba que la dirección de correo pertenece al solicitante
 - se envía un código por correo, necesario para el proceso
- La práctica nos enseña que esta comprobación del correo puede no ser tan sencilla
 - el mensaje de Comodo se trata como spam...
 - los gestores del correo oficial lo tratan como spam...
- Interesa renovar los certificados digitales lo antes posible, antes de que caduquen los actuales
 - para evitar que un mensaje que se ha enviado recientemente aparezca, a los pocos días, como *problemático* por haber caducado el certificado

Conclusiones

- ¿Evita el procedimiento CFD que los usuarios sean víctimas de ataques por correo electrónico?
 - No (o no del todo). Pero este procedimiento va generando una conciencia y un modo de actuar ante mensajes fraudulentos
- ¿Hay constancia de la efectividad del CFD?
 - Sí, hemos tenido comentarios del tipo: 'este mensaje deber ser falso, porque no aparece en la Intranet'
- ¿Proporciona algún valor añadido el CFD?
 - Sí. El hecho de utilizar consistentemente S/MIME hace que los usuarios vayan aprendiendo el funcionamiento del correo firmado/cifrado y que quieran integrarlo en su trabajo cotidiano

Generando confianza en el correo electrónico

GRACIAS POR VUESTRA ATENCIÓN

Miguel Macías Enguádanos

miguel.macias@upv.es

Jornadas Técnicas
Valladolid, 01/12/2011



UNIVERSITATIS
VALENTINAE
DE VALENCIA