OWASP
The Open Web Application Security Project

V OWASP Spain
Chapter Meeting
15 de Mayo de 2009
Barcelona

Gestión de Incidentes de Seguridad Web en la Brigada de Investigación Tecnológica.

Jorge Martín
Inspector del Cuerpo Nacional de Policía
Jefe del Grupo de Seguridad Lógica

COMISARIA GENERAL DE POLICÍA JUDICIAL
U.D.E.F. CENTRAL
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA

CUERPO NACIONAL DE POLICÍA

FUNCIONES

GENÉRICAS

- SEGURIDAD CIUDADANA
- POLICÍA JUDICIAL
- INFORMACIÓN
- POLICÍA ADMINISTRATIVA

ESPECÍFICAS

- EXPEDICIÓN DNI Y PASAPORTE
- CONTROL ENTRADA/SALIDA DEL PAIS
- REGIMEN DE EXTRANJERÍA
- CONTROL DEL JUEGO
- LUCHA CONTRA EL TRÁFICO DE DROGAS
- COOPERACIÓN INTERNACIONAL
- CONTROL DE LA SEGURIDAD PRIVADA


DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL
(ámbito del Cuerpo Nacional de Policía)
JUNTA DE GOBIERNO
CONSEJO ASESOR
DIRECCIÓN ADJUNTA OPERATIVA
SUBDIRECCIÓN GENERAL DE RECURSOS HUMANOS
SUBDIRECCIÓN GENERAL DE GESTIÓN ECONÓMICA, TÉCNICA Y DOCUMENTAL
UNIDAD DE COORDINACIÓN
COMISARÍA GENERAL DE INFORMACIÓN
COMISARÍA GENERAL DE POLICÍA. JUDICIAL
COMISARÍA GENERAL DE SEGURIDAD CIUDADANA
COMISARÍA GENERAL DE EXTRANJERÍA Y FRONTERAS
COMISARÍA GENERAL DE POLICÍA CIENTÍFICA
DIVISIÓN DE PERSONAL
DIVISIÓN DE FORMACIÓN Y PERFECCIONAMIENTO
DIVISIÓN DE COORDINACIÓN ECONÓMICA Y TÉCNICA
UNIDAD DE DOCUMENTACIÓN DE ESPAÑOLES Y ARCHIVO
ORGANIZACIÓN PERIFERICA
JEFATURAS SUPERIORES (20)
COMISARÍAS PROVINCIALES (44)
COMISARÍAS LOCALES (126)
COMISARÍAS DE DISTRITO (70)
COMISARÍAS CONJUNTAS (4)
PUESTOS FRONTERIZOS (68)
UNID. EXTRANJERÍA Y DOCUMENTACIÓN (13)
* Real Decreto 1181/2008 de 11 de julio
* Orden INT/2103/2005 de 1 de julio
* Orden INT/161/2008 de 29 de enero

COMISARIA GENERAL DE POLICÍA JUDICIAL

Secretaría General

UDYCO
- Brigada Central de Estupefacientes
- Brigada Central de Crimen Organizado
- Unidad Adscrita Fiscalia General del Estado

UDEV
- Brigada de Delincuencia Especializada y Violenta
- Brigada de Patrimonio Histórico
- Unidad Adscrita a la Audiencia Nacional

UDEF
- Brigada de Delincuencia Económica y Fiscal
- Brigada de Inteligencia Financiera
- Brigada del Banco de España
- Brigada de Investigación Tecnológica
- Unidad Adscrita Fiscalía Anticorrupción y Crimen Organizado.

UCIC

UCPI
- Oficina Central Nacional de Interpol
- Unidad Nacional de Europol
- Oficina Sirene

Unidades Territoriales de Policía Judicial

FUNCIONES OPERATIVAS

- DIRECCIÓN TÉCNICA Y OPERATIVA
- INVESTIGACIONES COMPLEJAS Y ESPECIALIZADAS
- COORDINACIÓN DE LOS GRUPOS TERRITORIALES Y APOYO A LAS INVESTIGACIONES
- RASTREOS EN INTERNET PARA PREVENCIÓN DE DELITOS.

La cooperación internacional

- Puntos de contacto 24X7 en el G-8, Interpol y Europol
- EWPITC en Interpol.
- Participación en diferentes Subgrupos de Investigación de delitos en Interpol.
- Legislación de la Unión, fundamentalmente en forma de directivas que se han de trasponer al ordenamiento español.
- Cursos de formación para investigación de delitos tecnológicos.
- Participación en la Convención sobre Ciberdelincuencia del Consejo de Europa.
- Relaciones bilaterales con múltiples países: Argentina, El Salvador, EE.UU, Canadá, Chile, México, Reino Unido…

COMISARÍA GENERAL DE POLICÍA JUDICIAL

Unidad Central de Delincuencia Económica y Financiera

B I T

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA

SECCIÓN OPERATIVA I
- PROTECCIÓN AL MENOR I
- PROTECCIÓN AL MENOR II
- FRAUDE A LAS TELECOMUNICACIONES
- REDES ABIERTAS

SECCIÓN OPERATIVA II
- FRAUDES EN INTERNET I
- FRAUDES EN INTERNET II
- SEGURIDAD LÓGICA
- PROPIEDAD INTELECTUAL

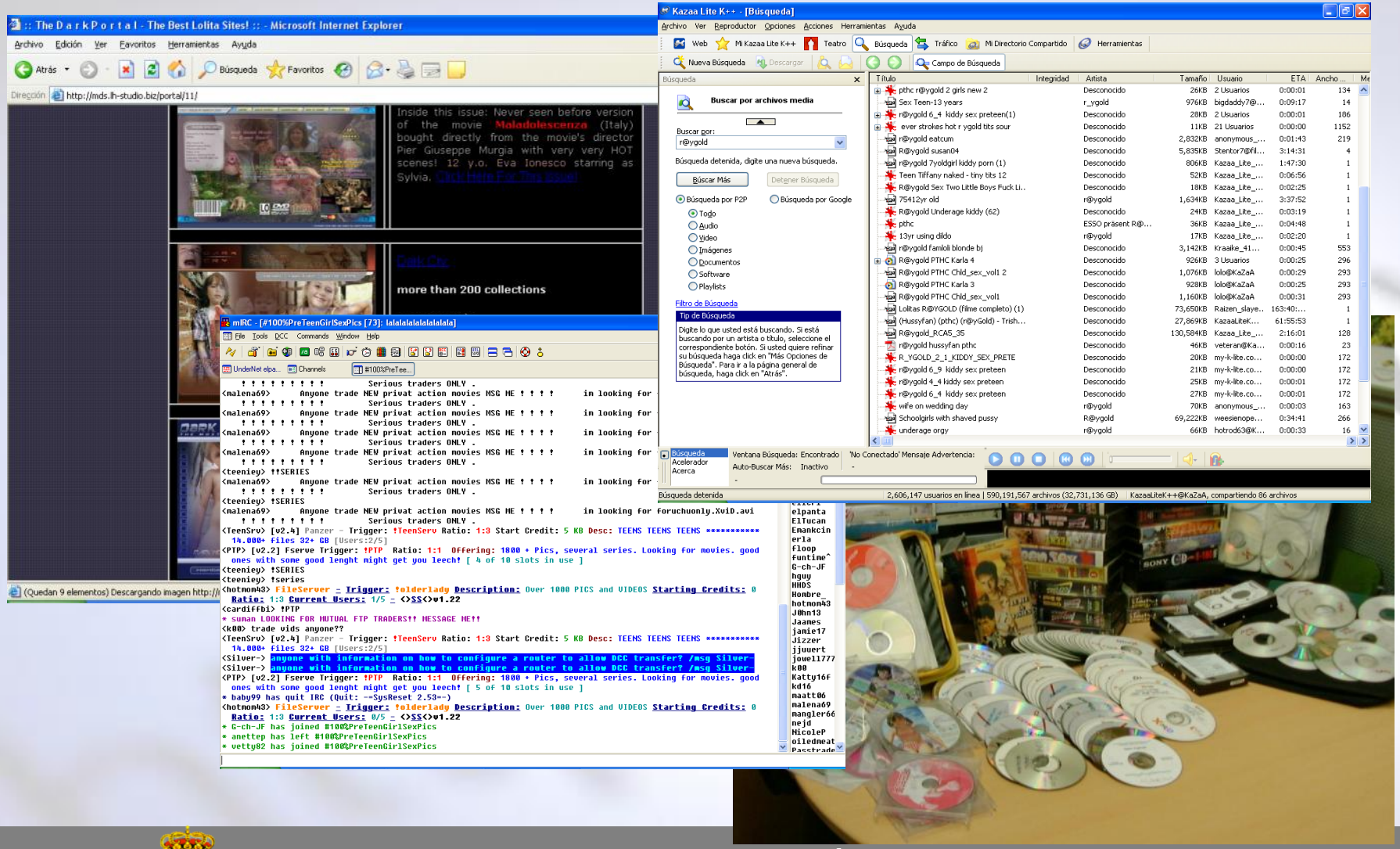
SECCIÓN TÉCNICA
- INFORMES
- APOYO TÉCNICO
- FORMACIÓN
- ESTUDIOS
- I + D

ORGANIZACIÓN TERRITORIAL P.J. (Jefaturas Superiores de Policía)
"GRUPOS DE DELITOS INFORMÁTICOS"

PROTECCIÓN AL MENOR

- **Posesión, producción, distribución o difusión de pornografía infantil.**
  - Inclusión de imágenes en web sites, comunidades basadas en web etc...
  - Inclusión de enlaces a otros webs
  - Servicios de redireccionamiento de web.
  - Correo electrónico y listas de distribución.
  - Grupos de noticias o de discusión.
  - Almacenamiento en servidores ftp.
  - Intercambio en Canales irc o similares
  - Intercambio mediante mensajería instantánea Messenger, Gtalk, Icq …

PROTECCIÓN AL MENOR



Detenidas 121 personas en la mayor operación contra la pornografía infantil | elmundo.es - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://www.elmundo.es/elmundo/2008/10/01/espana/1222842737.html

elmundo.es España

ESPAÑA | INTERNACIONAL | ECONOMÍA | CULTURA | CIENCIA | TECNOLOGÍA | DEPORTES | SALUD | COMUNICACIÓN | TV | MADRID | BCN | IB | CVA | CYL | más secciones | Fotos | Vídeos | Gráficos

Buscar en Google en elmundo.es Hemeroteca Versión texto Personalizar RSS Haga elmundo.es su página de inicio

Portada > España

EN TODA ESPAÑA | MILLONES DE ARCHIVOS INTERVENIDOS

Detenidas 121 personas en la mayor operación contra la pornografía infantil

- El perfil de los detenidos es amplio: pilotos comerciales, conserjes, taxistas...
- En la macro-operación han participado más de 800 agentes
- Entre los archivos incautados se han hallado agresiones a menores de extrema dureza

Actualizado miércoles 01/10/2008 13:17 (CET)

ELMUNDO.ES

MADRID.- La Policía Nacional ha detenido a 121 personas imputadas por tenencia y distribución de material pedófilo en la Red en un amplio operativo desarrollado en España.

La operación se ha realizado mediante una actuación coordinada por la **Brigada de Investigación Tecnológica** (BIT), de la Comisaría General de Policía Judicial, que ha contado con el apoyo de las brigadas provinciales de policía judicial de las localidades implicadas y en el que han participado más de 800 agentes.

Según la Dirección General de la Policía y la Guardia Civil, se han intervenido millones de archivos de vídeo y fotografías, algunos de ellos con agresiones a menores de extrema dureza. Además, dos de los detenidos producían su propio material y se ha logrado identificar a las víctimas **pertenecientes**

ADEMÁS

La mancha negra de la pornografía 'online'

Noticias relacionadas en elmundo.es

Noticias relacionadas en otros medios

Noticias más leídas | Más votadas

1. La Falange demandará al 'Follonero' y a La Sexta
2. Porno para mujeres
3. Un portero: 'Pitoño' se tiró a propósito sobre...
4. Pamela se desnuda para Hefner
5. Un suicidio retransmitido por 'webcam'
6. La dificultad de entrar en los PC de 'Txeroki'
7. Feliciano desmonta a Del Potro

FRAUDE EN LAS TELECOMUNICACIONES

Telefonía

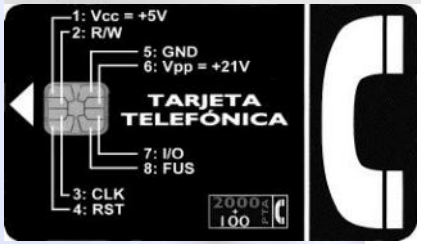
- Defraudaciones a las compañías telefónicas.
  - Estafa en la contratación.
  - Uso de routers voz sobre IP para redirigir llamadas.
  - Locutorios clandestinos para realizar llamadas a 3
  - Llamadas a líneas de tarificación adicional.
- Tarjetas telefónicas recargadas o de validez ilimitada.

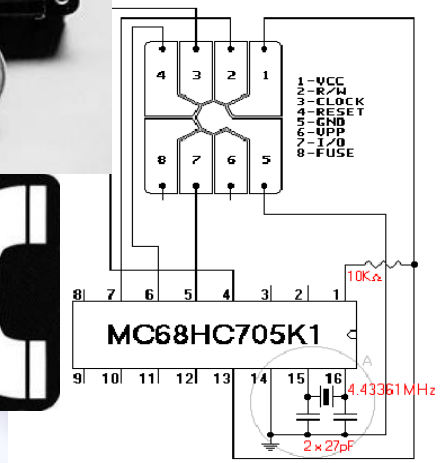
TV

- Decodificación no autorizada de canales de televisión con señal codificada.

Amenazas, calumnias e injurias

FRAUDE EN LAS TELECOMUNICACIONES





NOTA: Las conecciones en la vista A, deben ser lo mas cortas posibles.

Materiales:

1 Tarjeta de Telefonica o Telecom
2 Capacitores de 27pF
1 Cristal de 4.43361 MHz
1 Resistencia de 10Kohm
1 MC68HC705K1 (Microcontrolador)

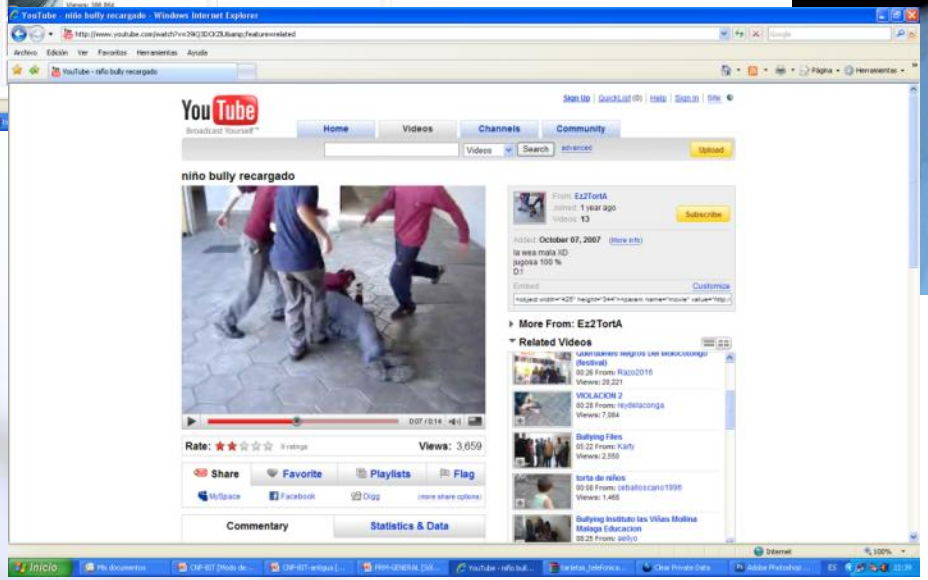
By Bugs Bunny
[DAN]

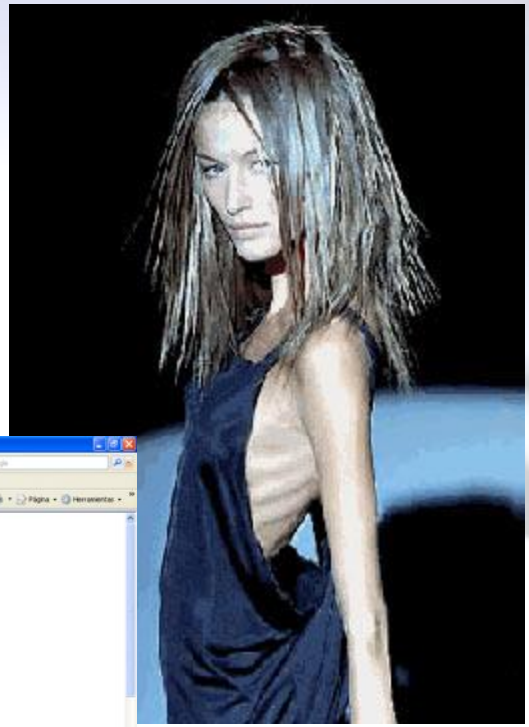
REDES ABIERTAS

- Grupo de reciente creación dedicado al rastreo de la red en busca de contenidos ilícitos y nuevas formas delictivas.

- Asuntos recientes:
  - Publicación de videos de agresiones, vejaciones, carreras ilegales.
  - Bulling (maltrato en el ambito escolar)
  - Apologia del racismo, anorexia y bulimia.

REDES ABIERTAS

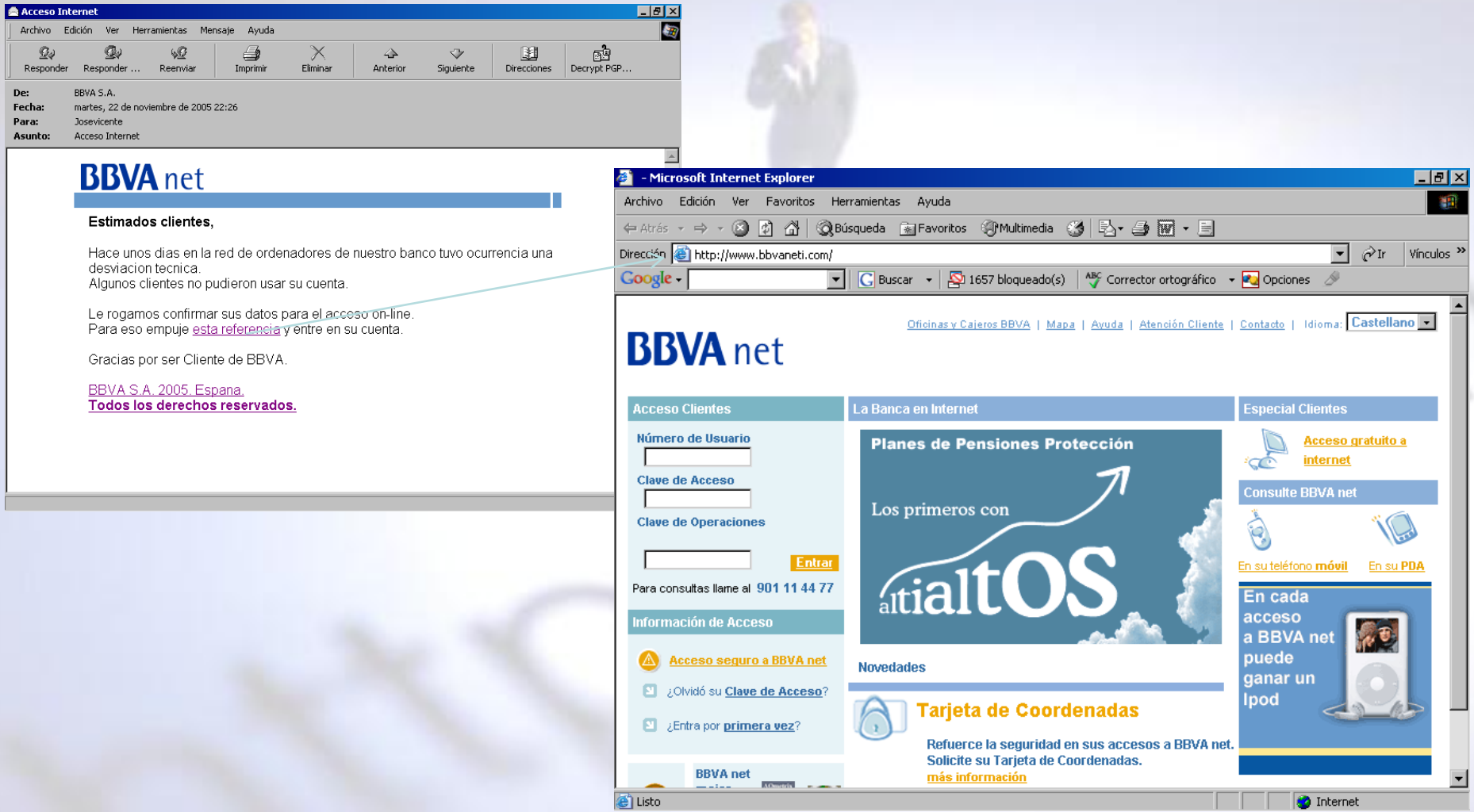




FRAUDES EN INTERNET

- Adquisición de bienes y servicios a través de Internet con números de tarjeta válidos: carding
- Phishing y pharming
- Distribuciones piramidales
- Ventas y Subastas ficticias
- Cartas nigerianas
- Casinos virtuales

FRAUDES EN INTERNET



FRAUDES EN INTERNET

Estimado amigo.

Sé que esta carta puede venirle como una sorpresa. Conseguí su dirección por un directorio Comercial local en la web. Debo pedir perdón por tomar un poco de su tiempo valioso para explicarle esta oferta que creo será de la ventaja suma a ambos nosotros.

Soy Ex,Capt David Amossou, el Director de Operación y la Entrega de Trans Seguridad y Compañía Financiera en COTONOU – la REPÚBLICA DE BENÍN, ÁFRICA DE OESTE En nuestra compañía descubrimos dos Caja Galvaniza y una de la Caja contiene una suma del USD de 1,300,000.00 dólares (Once millón trescientos mil dólares americanos) y la otra caja que contiene 150 kilogramos de Oro de 18 quilates que pertenece a uno de nuestro cliente extranjero Sr. Mohammed Al--Fuhard un libanés que murió junto con su familia entera en un accidente de avión que ocurrió el jueves por la tarde como Boeing 727 salió del aeropuerto en Cotonou, la capital comercial de Benín en las orillas del Océano Atlántico. En el 25 / 12 / 2003.Usted mismo puedes confirmar en este dos sitio Web:

http://www.cnn.com/2003/WORLD/africa/12/26/benin.crash/index.html
http://www.rfi.fr/actufr/articles/048/article_25680.asp

Ya que nuestra compañía consiguió la información sobre su muerte hemos estado esperando que su familiar más cercano venga y reclame sus dos remesas porque no podemos liberar este remesas a alguien a menos que alguien los solicite como familiar más cercano o relación a Sr., Mohammed Al--Fuhard como indicado en nuestras pautas de compañía y leyes pero lamentablemente aprendimos que todos su supuesto el familiar más cercano murió al lado de él en el accidente de avión no que deja a nadie para la reclamación y nuestro derecho de compañías y la pauta aquí estipula que si tal remesa permanece sin reclamar después de dos años, tal remesa será confiscada como la propiedad sin reclamar. En este caso que no podemos localizar ninguna de su relación como su familiar más cercano, me gustará presentarle a nuestra compañía como, el Socio de negocio de Sr, Mohammed Al--Fuhard Mohammed y su representante de familia y asi todos los viejos documentos de Sr, Mohammed serán cambio en su nombre como el nuevo beneficiario de las dos remesas. immediatamente concluimos el trato usted será autorizan al 50 % del total mientras el 50 % restante será mi propio porcentaje. Esto significa 50/50

También querré informarle que todo el documento legal que cubrirá esta transacción será proporcionado legalmente por un abogado respetable aquí en Cotonou sin problema niguno. Note: exijo la confianza más alta de usted para guardar este negocio estrictamente confidencial para razones de seguridad y también querer que usted supiera que nuestra compañía no sabrá que soy el que quién se puso en contacto con usted para significar esta reclamación.

Por fabor ponga en contacto conmigo via este correo urgentemente cuando recibir este correo E-mail: excapt_david@zwallet.com

FRAUDES EN INTERNET

CNN.com - 111 killed in Benin plane crash - Dec. 26, 2003 - Bon Echo

File Edit View History Bookmarks Tools Help

http://www.cnn.com/2003/WORLD/africa/12/26/benin.crash/index.html

Comenzar a usar Fire... Últimas noticias

International Edition | Netscape

CNN.com Member Center: Sign In | Register MAKE CNN.com YOUR HOME PAGE

SEARCH The Web CNN.com Search

Home Page
World
U.S.
Weather
Business at CNNMONEY
Sports at SI.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports
Autos with EDMUNDS.com

SERVICES
Video
E-mail Newsletters
Your E-mail Alerts
RSS
CNNtoGO
TV Commercials
Contact Us

SEARCH
Web CNN.com
Search

WORLD

111 killed in Benin plane crash

Friday, December 26, 2003 Posted: 11:15 AM EST (1615 GMT)

COTONOU, Benin -- Rescuers are searching for survivors after a Beirut-bound charter jet crashed on takeoff from a coastal airport in the West African country of Benin, killing at least 111, officials say.

About two dozens bodies and the plane's cockpit were found on the beach after the crash, which occurred Thursday afternoon as the Boeing 727 took off from the airport in Cotonou, Benin's commercial capital on the shores of the Atlantic Ocean.

Divers and fishermen -- braving dark and cold waters -- swam through scattered pieces of luggage, clothes and wrapped Christmas gifts, while tractors tied chains to parts of the plane, including an engine, to clear away the wreckage, The Associated Press reported.

Benin Health Minister Celine Seignon Kandissounon told reporters that 111 people were now confirmed dead. At least 20 people survived, said Transport Minister Ahmed Akobi.

It was unclear exactly how many people were aboard the aircraft. Akobi said the plane's manifest listed 156 passengers and an unknown number of crew, AP reported.

Two boats approach the wreckage from the plane crash near Benin.

Story Tools
SAVE THIS E-MAIL THIS
PRINT THIS MOST POPULAR

VIDEO MORE VIDEO

CNN's Daryn Kagan on rescuers' search for survivors after a Beirut-bound charter jet crashed at a coastal airport in West Africa's Benin.

PLAY VIDEO

RELATED

advertisement

Done

Inicio | Mis documentos | CNP-BIT [Modo de ... | CNP-BIT-antigua [... | PRM-GENERAL [Sól... | Presentación de Po... | 419 Scam: fraude ... | Adobe Photoshop ... | CNN.com - 111 kille... | ES | 23:56

• FRAUDES EN INTERNET

Mesquida felicita a la Brigada de Investigación Tecnológica por la "operación Ulises" - Noticias sobre Tecnología en hoyTecnologíaa - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://www.hoytecnologia.com/noticias/Mesquida-felicita-Brigada-Investigacion/44284

hoyTecnología

Contraseña IR

¿olvidaste contraseña? | Regístrate

Portada | Actualidad | Blogs | Multimedia | Productos | Descargas | Links | Servicios | Especiales | Movilidad | Neoteo

Estás en: Actualidad > Noticia

Sábado, 22 de Noviembre de 2008

2 Votos

VOTAR

Mesquida felicita a la Brigada de Investigación Tecnológica por la "operación Ulises"

Noticias EFE | 12/02/2008|13:01h

El director general de la Policía y la Guardia Civil, Joan Mesquida, y el director general de la Agencia Tributaria, Luis Pedroche, han felicitado hoy a los agentes de la Brigada de Investigación Tecnológica responsables de la "operación Ulises", la mayor realizada en España contra el fraude en la red.

Esta investigación, que culminó el pasado fin de semana con la detención de 76 personas en quince comunidades autónomas, se centró en las estafas -por un importe total de más de tres millones de euros- cometidas mediante ventas, subastas y transferencias bancarias no consentidas a través de la creación de páginas web falsas o técnicas como el "phising".

El acto de hoy coincide con el Día Internacional de la Internet Segura, un evento que, en su quinta edición, apela a la responsabilidad final del usuario de la red en su buen uso y en el que participan decenas de países de todo el mundo.

La Brigada de Investigación Tecnológica (BIT), que depende de la Unidad de Delincuencia Económica y Fiscal (UDEF) de la Comisaría General de Policía Judicial, cuenta con más de cuarenta agentes especializados en la investigación de las actividades delictivas relacionadas con la utilización de las nuevas tecnologías y el ciberdelito.

Mesquida - Brigada - Estafa

Buscar IR

en hoytecnología noXtrum

BUSCADOR

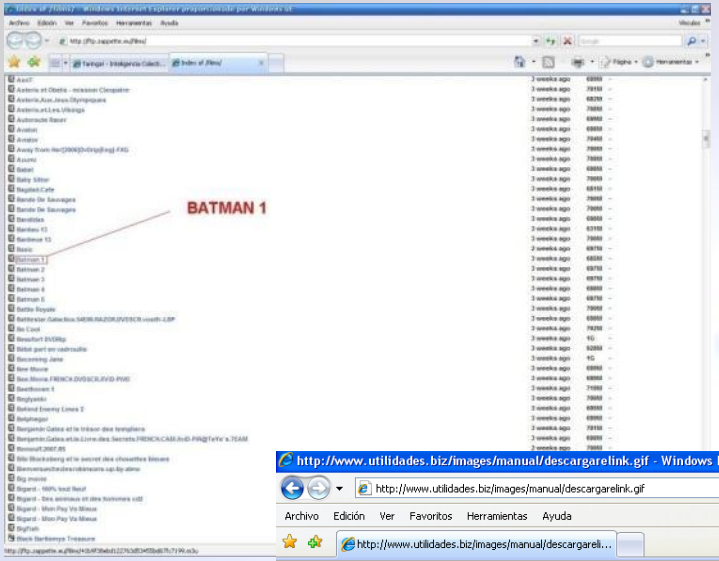
NOTICIAS RELACIONADAS

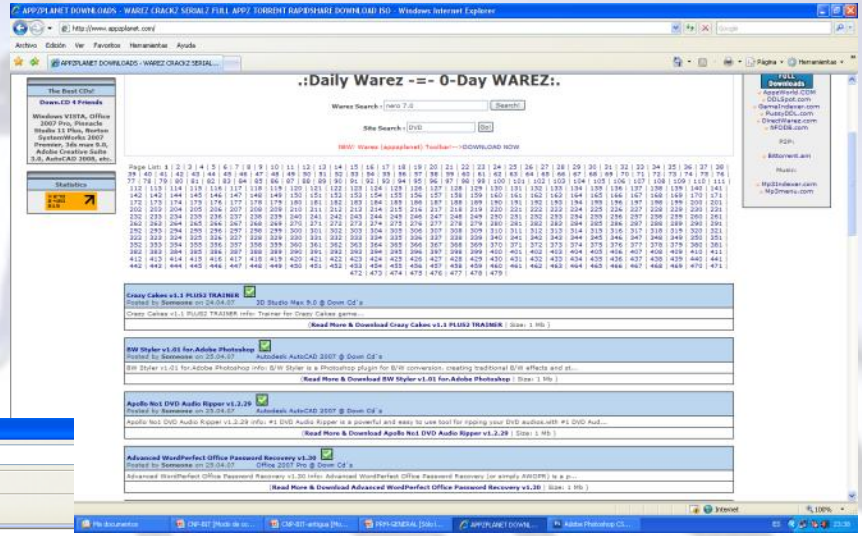
- Detenidos por estafar 39.000 euros a través de Internet en La Rioja
- Tres detenidos por una estafa por Internet de productos electrónicos
- La Policia advierte de un aumento de las denuncias por estafa en compras a través de internet
- La Policía Nacional detiene en Pamplona a cuatro acusados de estafa por Internet

PROPIEDAD INTELECTUAL

- Reproducción, plagio, distribución o comunicación pública de una obra literaria, artística o científica con fines lucrativos.
  - Web
  - FTP
  - Newsgroups
  - IRC
  - P2P
- Fabricación, distribución o posesión de medios especificos de desprotección.
  - Warez
  - Cracks
  - Keygens

PROPIEDAD INTELECTUAL





24 detenidos en una operación a nivel nacional contra la propiedad intelectual | elmundo.es - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://www.elmundo.es/elmundo/2008/03/08/espana/1204969647.html

elmundo.es España

ELECCIONES 9M | ESPAÑA | INTERNACIONAL | ECONOMÍA | CULTURA | CIENCIA | TECNOLOGÍA | DEPORTES | SALUD | COMUNICACIÓN | TV | MADRID | más secciones | BCN | IB | CVA | CYL

Buscar en Google en elmundo.es Hemeroteca Versión texto Personalizar RSS Haga elmundo.es su página de inicio

Portada > España

LA POLICÍA SE INCAUTA DE 750 SOPORTES PIRATAS

24 detenidos en una operación a nivel nacional contra la propiedad intelectual

Actualizado sábado 08/03/2008 10:47 (CET)

EUROPA PRESS

MADRID.- Agentes de la Policía Nacional han detenido a 24 personas por delitos contra la propiedad intelectual en una operación a escala nacional contra la instalación de software pirata descargado de Internet en tiendas de informática, que se ha saldado con la incautación de 750 soportes que podrían causar un perjuicio de más de 200.000 euros a los legítimos titulares de los derechos.

La investigación **se desarrolló sobre 14 empresas** que presuntamente realizaban estas prácticas y culminó con once registros en Madrid (2), Barcelona (4), Andalucía (3) y Murcia (2) en los que se han intervenido aproximadamente 750 productos, entre CD's y DVD's, con copias de software pirata utilizado como máster para su instalación ilícita en equipos.

La **operación 'Búho'** ha sido realizada por la Brigada de Investigación Tecnológica (BIT) de la Comisaría General de Policía Judicial, con la colaboración de agentes de las Jefaturas Superiores de Policía de Cataluña, Andalucía y Murcia.

Los investigadores también han realizado acciones preventivas contra la distribución de 'malware' en la Red y han alertado sobre la instalación de programas ilícitos que pueden facilitar la captura por extraños de datos sensibles de los usuarios. Los programas maliciosos **se instalan en el núcleo del sistema** y no se pueden detectar a pesar de la utilización posterior de programas antivirus.

La investigación se inició a mediados de 2007 tras las denuncias presentadas por los legítimos

Noticias relacionadas en elmundo.es

Noticias relacionadas en otros medios

Noticias más leídas | Más votadas

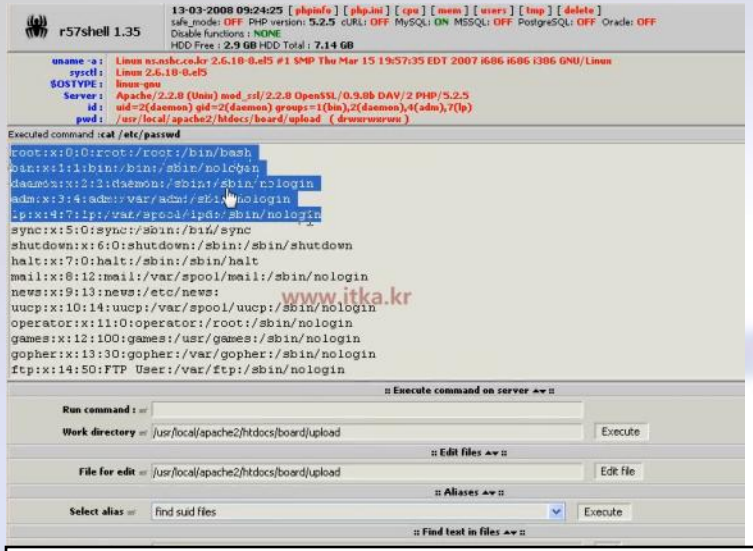
1. La Falange demandará al 'Follonero' y a La Sexta
2. Porno para mujeres
3. Un portero: 'Pitoño' se tiró a propósito sobre...
4. Pamela se desnuda para Hefner
5. Un suicidio retransmitido por 'webcam'
6. La dificultad de entrar en los PC de 'Txeroki'
7. Feliciano desmonta a Del Potro
8. Acoso a Gallas, el 'indigno capitán' del Arsenal
9. Lukoil se hará con Repsol sin invertir un euro
10. Gallardón cierra varios locales y discotecas

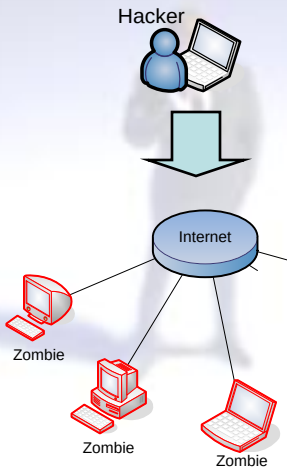
SEGURIDAD LOGICA

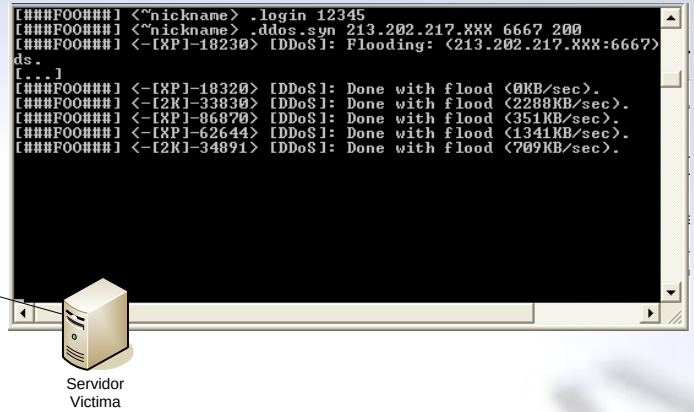
Investigación de:

- Intrusiones
- Ataques
- Daños Informáticos
- Sustracción de datos
- Troyanos
- Virus

SEGURIDAD LOGICA







Dear Sir/Madam, Hello! We are xxxxxxx crew

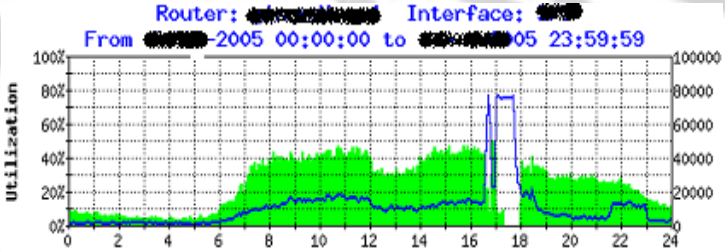
We propose you for sale some interesting things:

- private exploits

- we infect users pc's with your trojan for low prices (10000 infected pc's for 25$)

- bulletproof domain + hosting. You can use this hosting for any scam/fraud and nobody will close it!

We are now spaming 5 000 000 people, look out the domain is alive as always and never gonna be down !! Please go and order our services at: http://xxxx.xxxx-.ru



elmundo.es

SON LOS AUTORES DEL ATAQUE A LA PÁGINA DE IZQUIERDA UNIDA

Detenidos en España cinco de los 'hackers' más activos del mundo, dos de ellos menores

- **Firmaban sus ataques con los seudónimos 'ka0x, an0de, xarnuz y Piker'**
- **Dos de ellos son hermanos y otros dos tienen sólo 16 años**
- **Vivían en Sabadell, Burgos, Málaga y Valencia y se coordinaban a través de Internet**
- **Habían atacado más de 21.000 páginas y ocupaban el 5º puesto en un ránking mundial**
- **elmundo.es contactó con ellos y les hizo una entrevista hace dos meses**

Actualizado lunes 19/05/2008 15:11 (CET)

DANIEL G. LIFONA

MADRID.- Algunos de ellos se hacían llamar **'ka0x, an0de, xarnuz y Piker'**, y en dos años habían atacado más de 21.000 páginas web, entre ellas la de Izquierda Unida justo antes de las elecciones generales del 9 de marzo.

En una **entrevista concedida hace dos meses a elmundo.es** se definieron como "amantes de la informática y la seguridad web", pero ahora han sido detenidos por la Brigada española de Investigación Tecnológica como autores de un delito de daños informáticos.

Los cinco jóvenes, **dos de ellos de 16 años**, pertenecían a uno de los grupos de 'hackers' más activos de la Red, 'D.O.M. Team 2008', que ostentaba **el quinto puesto en el ránking mundial** de ataques informáticos según 'Zone-H', una página web que mantiene una base de datos de sabotajes a sitios de Internet.

Habían atacado la web de **Jazztel, la Compañía Nacional de Teléfonos de Venezuela, un dominio de la NASA y otros sitios gubernamentales** de EEUU, Latinoamérica y Asia. En su última acción, el pasado 30 de abril, accedieron a la página de Esquerra Unida de Buñol, y dos días antes protagonizaron uno de sus mayores ataques masivos. **En un solo día penetraron en cerca de 800 sitios**.

Fotomontaje insertado por los 'hackers' en la página web de IU pocos días antes de las elecciones generales del 9M.

elmundo.es

Portada > Navegante

DELITO DE REVELACIÓN DE SECRETOS

Detenido un empresario gallego por 'espiar' a su competencia mediante un troyano

- **Recibía del ordenador infectado informes periódicos de su actividad**

Actualizado miércoles 30/07/2008 11:19 (CET)

ELMUNDO.ES

MADRID.- La dura competencia entre dos empresas de reparaciones urgentes del hogar de Vigo no se limita a ver quién coloca más pegatinas al lado de los telefonillos, sino que ha pasado a utilizar técnicas de espionaje más sofisticadas.

Así, la Policía ha anunciado en una nota l**a detención del gerente** de una de estas empresas, acusado de haber espiado a través de Internet a su competidor mediante el uso de un troyano, una aplicación instalada en el ordenador de la víctima sin su permiso que **monitorizaba cualquier operación que se efectuara en el citado ordenador**.

La aplicación enviaba periódicamente informes de su actividad a varias cuentas de correo electrónico que controlaba el detenido.

De esta forma el arrestado obtuvo distintas contraseñas de acceso a cuentas de correo, bancarias y otros servicios de Internet, gracias a la que consiguió una **gran cantidad de información privilegiada sobre clientes, proveedores y otras relaciones comerciales** de la empresa espiada.

Denuncia inicial

La investigación se inició tras la **denuncia de un empresario gallego**, en la que explicaba que se había accedido de forma fraudulenta a distintas cuentas de correo electrónico y a varias cuentas bancarias de las que era titular.

El programa espía se había instalado de forma automática cuando el denunciante abrió un correo electrónico que contenía una supuesta factura de uno de sus proveedores.

Agentes de la Policía Nacional, tras analizar los equipos informáticos de la empresa denunciante, pudieron constatar que el ordenador del denunciante estaba infectado por un troyano que controlaba su actividad.

El arrestado está acusado de un **delito de descubrimiento y revelación de secretos**.

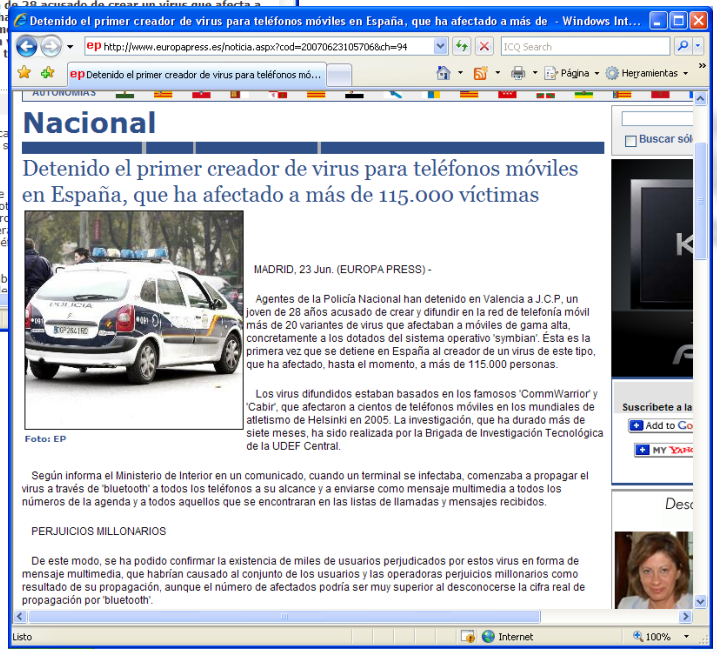
La investigación se inició hace más de un año y ha sido realizada por agentes del Grupo de Seguridad Lógica de la Brigada de Investigación Tecnológica de la Comisaría General de Policía Judicial, con la colaboración de la Brigada Local de Policía Judicial de Vigo.


Detenido por primera vez en España un creador de virus de móviles / EL MUNDO - Windows Internet Explorer
EL MUNDO
ESPAÑA
Detenido por primera vez en España un creador de virus de móviles
Una nueva forma de jugar a La Primitiva arrasa por internet


Detenen al primer creador de virus para teléfonos móviles en España - ELPAIS.com - Windows Internet Explorer
EL PAIS.com Tecnología
ESPECIAL
EL PAÍS que viene. El periódico cambia a partir del día 21
Detienen al primer creador de virus para teléfonos móviles en


Libertad Digital: Detienen en Valencia al primer hacker de teléfonos móviles en España - Windows Internet Explorer
http://www.libertaddigital.com/noticias/noticia_1276308308.html
Noticias y opinión en la Red
29/08/2007 14:58
Libertad Digital.es
Portada Opinión España Mundo Economía Internet Sociedad Deportes Discapacitados
CAUSA PÉRDIDAS MILLONARIAS A LAS OPERADORAS
Detienen en Valencia al primer hacker de teléfonos móviles en España
Noticia publicada el 23-06-2007


Detenido el primer creador de virus para móviles de España - Noticias sobre Tecn
hoyTecnología
Portada Actualidad Blogs Multimedia Productos
Detenido el primer creador de virus para móviles de España
La Policía Nacional ha detenido en Valencia, por primera vez en España, a un joven de 28 años, acusado de crear un virus que afectaba a teléfonos móviles de gama alta y que ha perjudicado a unas 115.000 personas y provocado perjuicios millonarios a las operadoras de móviles y a los propios usuarios.


Detenido el primer creador de virus para teléfonos móviles en España, que ha afectado a más de - Windows Int...
http://www.europapress.es/noticia.aspx?cod=200706231057068ch=94
Nacional
Detenido el primer creador de virus para teléfonos móviles en España, que ha afectado a más de 115.000 víctimas
MADRID, 23 Jun. (EUROPA PRESS) -
Agentes de la Policía Nacional han detenido en Valencia a J.C.P, un joven de 28 años acusado de crear y difundir en la red de telefonía móvil más de 20 variantes de virus que afectaban a móviles de gama alta, concretamente a los dotados del sistema operativo 'symbian'. Esta es la primera vez que se detiene en España al creador de un virus de este tipo, que ha afectado, hasta el momento, a más de 115.000 personas.
Los virus difundidos estaban basados en los famosos 'CommWarrior' y 'Cabir', que afectaron a cientos de teléfonos móviles en los mundiales de atletismo de Helsinki en 2005. La investigación, que ha durado más de siete meses, ha sido realizada por la Brigada de Investigación Tecnológica de la UDEF Central.
Foto: EP
Según informa el Ministerio de Interior en un comunicado, cuando un terminal se infectaba, comenzaba a propagar el virus a través de 'bluetooth' a todos los teléfonos a su alcance y a enviarse como mensaje multimedia a todos los números de la agenda y a todos aquellos que se encontraran en las listas de llamadas y mensajes recibidos.
PERJUICIOS MILLONARIOS
De este modo, se ha podido confirmar la existencia de miles de usuarios perjudicados por estos virus en forma de mensaje multimedia, que habrían causado al conjunto de los usuarios y las operadoras perjuicios millonarios como resultado de su propagación, aunque el número de afectados podría ser muy superior al desconocerse la cifra real de propagación por 'bluetooth'.

CONTACTAR

CENTRO POLICIAL DE CANILLAS
C/Julián González Segador, s/n
28043 - Madrid
Tel. 915 822 751/752/753 /754/755
Fax.915 822 756

- **CONSULTAS GENÉRICAS**
  delitos.tecnologicos@policia.es

- **FRAUDES EN LAS TELECOMUNICACIONES**
  delitos.telecomunicaciones@policia.es

- **PORNOGRAFÍA INFANTIL**
  denuncias.pornografia.infantil@policia.es

- **FRAUDES EN INTERNET**
  fraudeinternet@policia.es

- **VIRUS, ATAQUES, SEGURIDAD LÓGICA**
  seguridad.logica@policia.es

- **ANTIPIRATERÍA**
  antipirateria@policia.es

http://www.policia.es

Además estamos a su servicio en:

Comisarías del Cuerpo Nacional de Policía
Centro de Alerta Tecnológica, 24 horas: 91 582 29 00

Gestión de incidentes:

- Atendemos consultas por correo electrónico con diferentes buzones por especialidades delictivas.
- Disponemos de un Centro Alerta Tecnológica con atención telefónica 24x7
- Colaboramos con otras entidades:

- Participamos en foros especializados:

Metodología:

- Análisis de logs
- Análisis forense de equipos
- Replicación y virtualización de entornos.
- Análisis de malware: Dinámico (+) y reversing (-)

Medidas que contribuyen a una investigación exitosa.

- Una buena política de seguridad bien documentada.
- Adecuada gestión de contraseñas.
- Adecuada gestión de logs, correlación, timestamping, replicación, controles de integridad…
- Detección temprana: revisión habitual de logs, estadisticas, graficas …

Incidentes mas frecuentes

- Ataques a la integridad: Defaces
- Ataques a la disponibilidad: DDOS
- Ataques a la confidencialidad: Compromiso de contraseñas
- Distribución de malware

Objetivos:

- Fundamentalmente económicos:
  - Phising
  - Spam
  - Robo de B.D. de comercios online
  - Robo de credenciales
  - Juegos Online

Vulnerabilidades mas frecuentes

- Técnicas de inyección: Especialmente SQL
- XSS (Cross Site Scripting)
- RFI (Remote File Inclusion)

CONSEJOS GENERALES

- Deshabilitar servicios y cuentas no utilizados.
- Actualización de S.O. y aplicaciones (parches).
- Uso de "buenas" contraseñas.
- Utilización de Firewalls
- Chequeo de integridad de aplicaciones y S.O.
- Back-ups periódicos.
- Análisis periódico de logs, monitorizar y graficar estadísticas.
- Auditorias, escaners de vulnerabilidades
- Consultar Listas de vulnerabilidades
- Limitar y controlar uso de programación del lado del cliente (javascript)
- Desactivar información de errores
- Limitar tiempo querys
- Desarrollo seguro de aplicaciones web.
- Encriptación del tráfico

CONTACTAR

CENTRO POLICIAL DE CANILLAS
C/Julián González Segador, s/n
28043 - Madrid
Tel. 915 822 751/752/753 /754/755
Fax.915 822 756

- **CONSULTAS GENÉRICAS**
  delitos.tecnologicos@policia.es

- **FRAUDES EN LAS TELECOMUNICACIONES**
  delitos.telecomunicaciones@policia.es

- **PORNOGRAFÍA INFANTIL**
  denuncias.pornografia.infantil@policia.es

- **FRAUDES EN INTERNET**
  fraudeinternet@policia.es

- **VIRUS, ATAQUES, SEGURIDAD LÓGICA**
  seguridad.logica@policia.es

- **ANTIPIRATERÍA**
  antipirateria@policia.es

http://www.policia.es

Además estamos a su servicio en:

Comisarías del Cuerpo Nacional de Policía
Centro de Alerta Tecnológica, 24 horas: 91 582 29 00