Informe de Amenazas CCN-CERT IA-03/14

Ciberamenazas 2013

y

Tendencias 2014

ANEXOS

20 de octubre de 2014

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

ANEXO A. ACTIVIDADES MÁS SIGNIFICATIVAS DEL CCN EN 2013

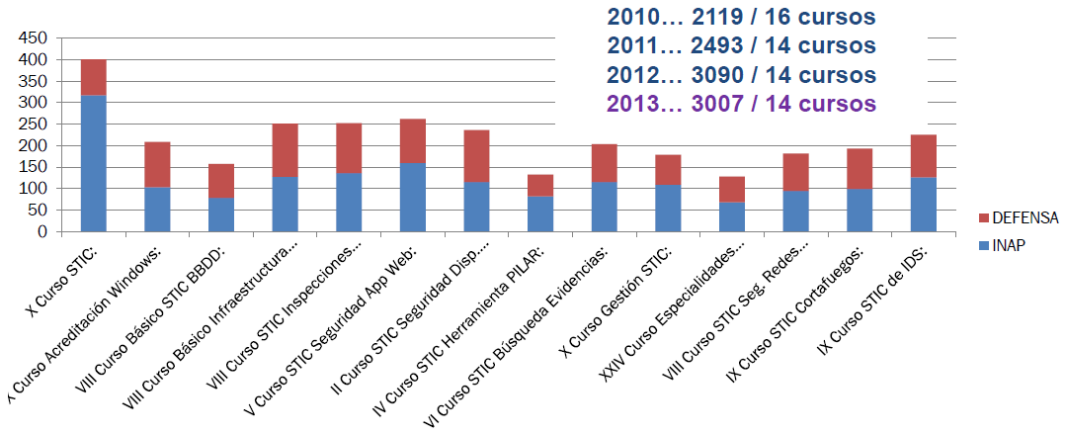
El Centro Criptológico Nacional es un Organismo, adscrito al Centro Nacional de Inteligencia (CNI), creado en el año 2002, con el fin de garantizar la seguridad TIC en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

Entre las funciones que tiene asignadas, se encuentra el elaborar y difundir **normas, instrucciones**, **guías** y recomendaciones (cuenta con más de 200 documentos en este sentido); **formar** al personal de la Administración; constituir el **Organismo de Certificación** de la seguridad de los productos y sistemas utilizados en su ámbito; **valorar y acreditar** la capacidad de los productos de cifra y de los sistemas que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura y velar por el cumplimiento de la normativa relativa a la **protección de la información clasificada**. Junto a ellas, el establecimiento de las necesarias relaciones y firma de acuerdos pertinentes con organizaciones similares de otros países y, a través del **CCN-CERT**, contribuir a la mejora de la ciberseguridad en España, con responsabilidad en los ciberataques sobre **sistemas clasificados** y sobre sistemas de la **Administración** y de **empresas y organizaciones de interés estratégico nacional**. De hecho, en el año 2013, tal y como se ha comentado en el Informe, el CERT Gubernamental español gestionó 7.263 ciberincidentes (un 82% más que el ejercicio anterior) y notificó más de 11.370 vulnerabilidades de hardware y software.

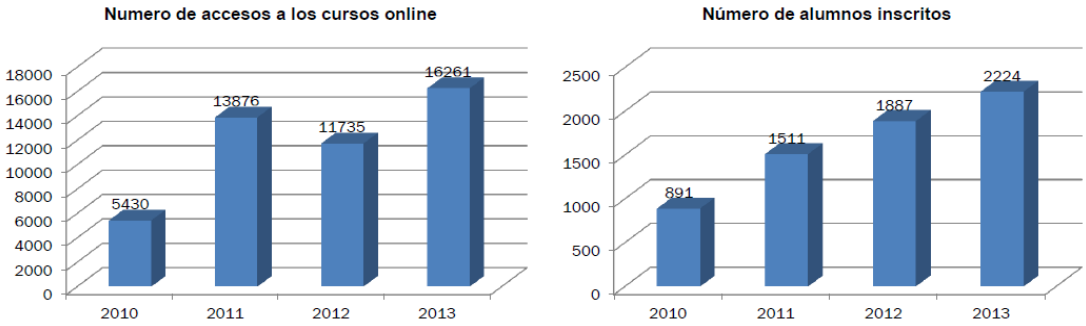
1.1 Formación – Cursos STIC 2013

	2008	2009	2010	2011	2012	2013
Alumnos	380	450	510	500	500	500
Cursos presenciales	17	18	17	14	14	14
Horas lectivas	1200	1400	1200	900	900	1000
Cursos online	-	1	3	5	6	6
Jornadas de sensibilización	2	4	3	6	7	6
Participación en mesas / jornadas	8	10	15	51	64	97

Formación – Solicitantes Cursos 2013



Formación – Cursos Online STIC 2013



	2010	2011	2012	2013
Accesos Cursos Online	5.430	13.876	11.735	16.261
Alumnos Online inscritos	891	1.511	1.887	2.224

1.2 Normativa – Series CCN-STIC

- En 2013 se publicron 38 Guías CCN-STIC, nuevas o actualizaciones
- 222 Guías en total (23 del ENS), todas ellas descargables en el portal del CCN-CERT: www.ccn-cert.cni.es

Guías Generales

A Actualización N Nueva

457	Herramientas de gestión de dispositivos móviles: MDM (BORRADOR)	N
001	Seguridad de las TIC que manejan información nacional clasificada en la Administración	A
526	Exchange Server 2007 en Windows 2008 R2	N
527	W2008 R2 -Clúster de conmutación por error	N
406	Seguridad en redes inalámbricas	A
305	Destrucción y sanitización de soportes informáticos	N
911B	Recomendaciones generales frente a una APT	N
423	Indicadores de Compromiso (IOC)	N
525	Microsoft Exchange Server 2007 en Windows Server 2003	N
422	Desarrollo seguro de aplicaciones web	N
521C	Seguridad en Windows 2008 Core (controlador de dominio)	N
912	Procedimiento de investigación de código dañino	N
530	Seguridad en Microsoft Office 2010	N
521D	Seguridad en Windows 2008 Server modo Core (servidor independiente)	N
304	Baja y destrucción de material criptológico	N
400	Manual STIC	A
453	Seguridad en Dispositivos Móviles: Android	A
455	Seguridad en Dispositivos Móviles: iPhone	A
454	Seguridad en Dispositivos Móviles: iPad	A
450	Seguridad en Dispositivos Móviles	A
957	Recomendaciones de empleo de TrueCrypt	N
531	Seguridad en Sharepoint Server 2007	N
911A	Ciclo de un APT	N
674	Seguridad en GlassFish	N

Guías Esquema Nacional de Seguridad

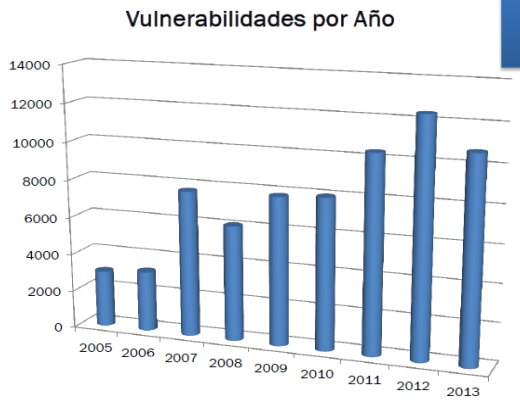
815	Métricas e Indicadores en el Esquema Nacional de Seguridad	A
820	Protección contra Denegación de Servicio	N
823	Seguridad en entorno Cloud	A
804	Medidas de implantación del ENS	A
825	ENS & 27001	N

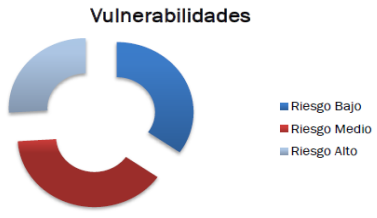
1.3 Gestión de Vulnerabilidades

Vulnerabilidades Portal – Parte Privada

10714 vulnerabilidades
3717 bajo
4214 medio
2783 alto

42 vulnerabilidades propias





1.4 Informes de Seguridad Publicados en 2013

- Informe Actividades 2011-2012
- Informes de Actualidad STIC (CCN-CERT IS) → 24 informes
- Informes de Amenazas (CCN-CERT IA) → 6 informes
  - Análisis de WhatsApp (iPhone). Vulnerabilidades
  - Análisis de Facebook (Android). Vulnerabilidades
  - Análisis de Facebook (iPhone). Vulnerabilidades
  - Ciberamenazas 2012 y Tendencias 2013
  - Riesgos Derivados del Uso de las Redes Sociales (Público)
  - Riesgos y Amenazas del BYOD (Público)
  - Persistencia del Código Dañino

  (Informes de Amenazas Elaborados …26 informes)
- Auditorías Web → 6 informes (12 planificadas)

1.5 Herramienta PILAR

- **PILAR 5.3**
- **PILAR Basic 5.3**
- **RMAT 5.1**
- **µPILAR 5.3**

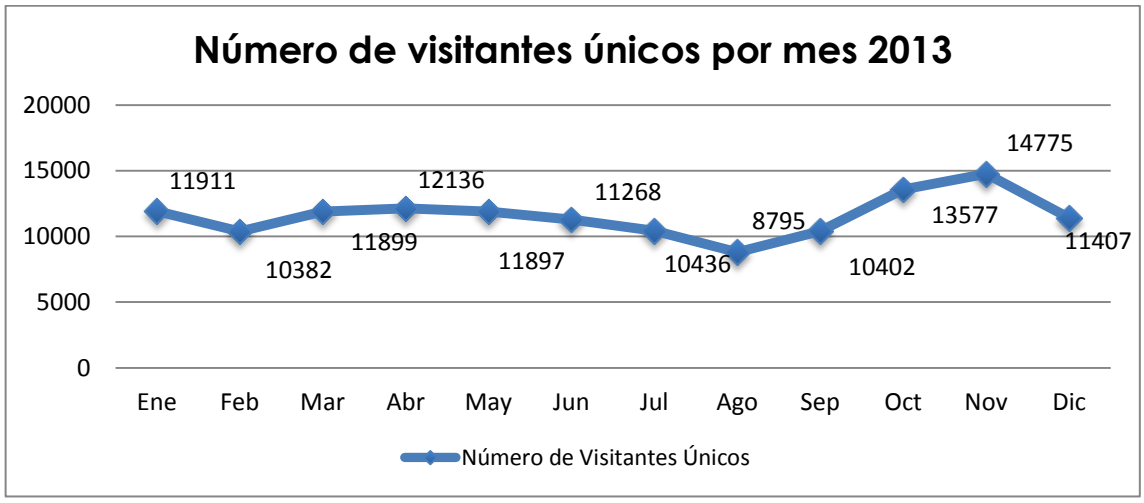
Parte Pública y Privada del Portal

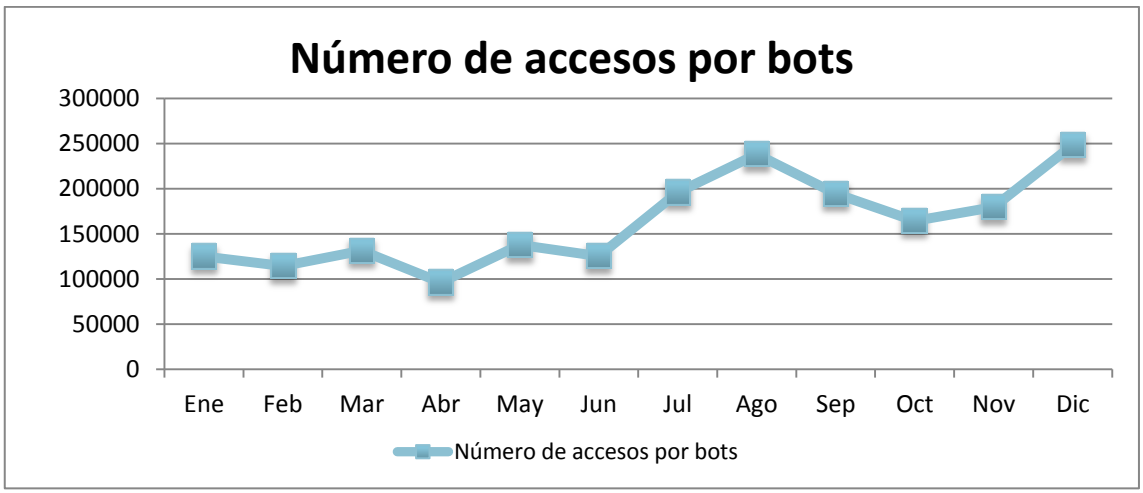
CCN-STIC 470F/1 Manual Usuario PILAR 5.3– Análisis y Gestión de Riesgos
CCN-STIC 470F/2 Manual Usuario PILAR 5.3 – Análisis de Impacto. Continuidad de Operaciones
CCN-STIC 472D Manual Usuario PILAR Basic 5.3
CCN-STIC 473C Manual Usuario µPILAR 5.3

MAGERIT versión 3

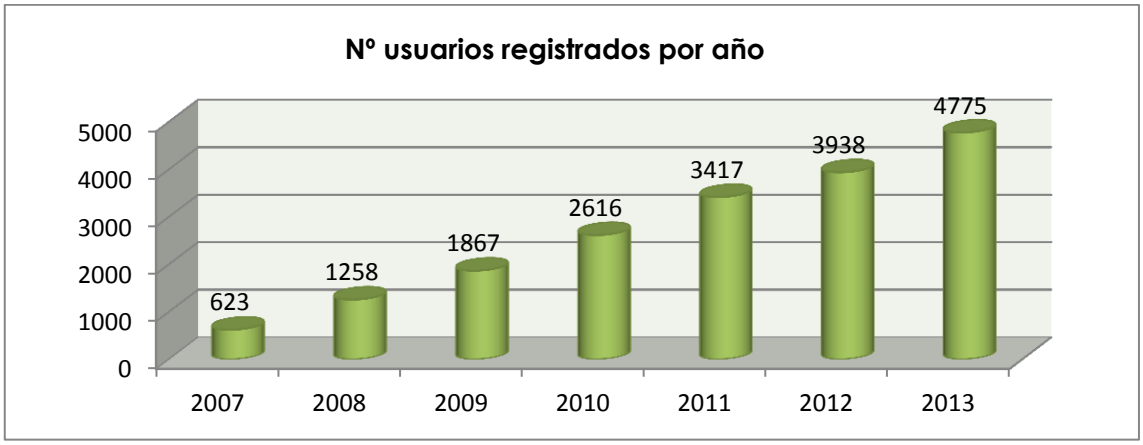
1.6 Portal www.ccn-cert.cni.es

El portal del CCN-CERT es un servicio más puesto a disposición de todos los usuarios, alcanzando por término media, más de 11.500 visitas mensuales de visitantes únicos (aquel que accede al portal con una IP distinta).





Este portal tiene una parte privada, especialmente destinada al personal de las Administraciones Públicas y de empresas y organizaciones de interés estratégico, alcanzando al termino de 2013, los 4.775 usuarios registrados.



LinkedIn – CCN-CERT

1.7 Sistemas de Alerta Temprana (SAT)

RED SARA [SAT- SARA]

- Servicio para la Intranet Administrativa
- Coordinado con MINHAP-SEAP
- 49 áreas de conexión y 54 Organismos adscritos (entre ellos, todos los Ministerios)

SALIDAS DE INTERNET [SAT INET]

Servicio por suscripción

- Basado en despliegue de sondas.
- **52 Organismos / 60 sondas**
- Última incorporación: Gobierno de Cantabria

1.8 CARMEN - Centro de Análisis de Registros y Minería de EveNtos

Primera versión

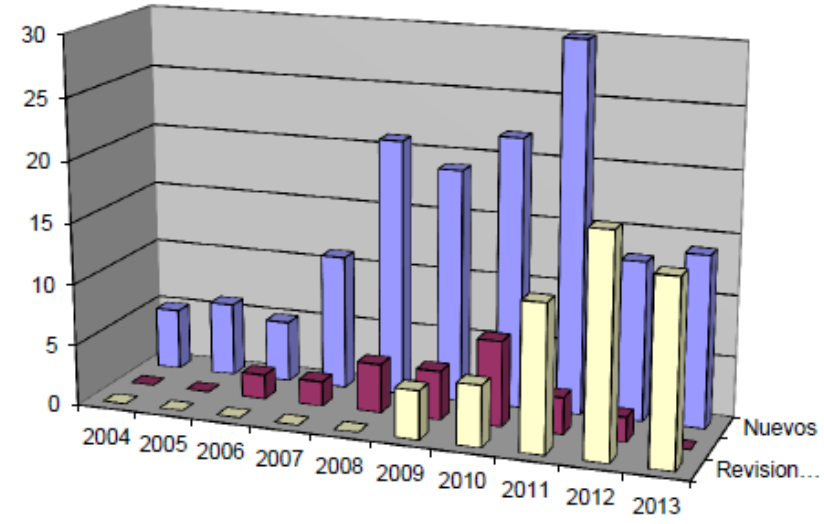
- Basada principalmente en gráficos estadísticos
- Gestión de falsos positivos
- Permite el estudio estadístico del tráfico de navegación
- Piloto: **6 Organismos**

Segunda Versión … Además:

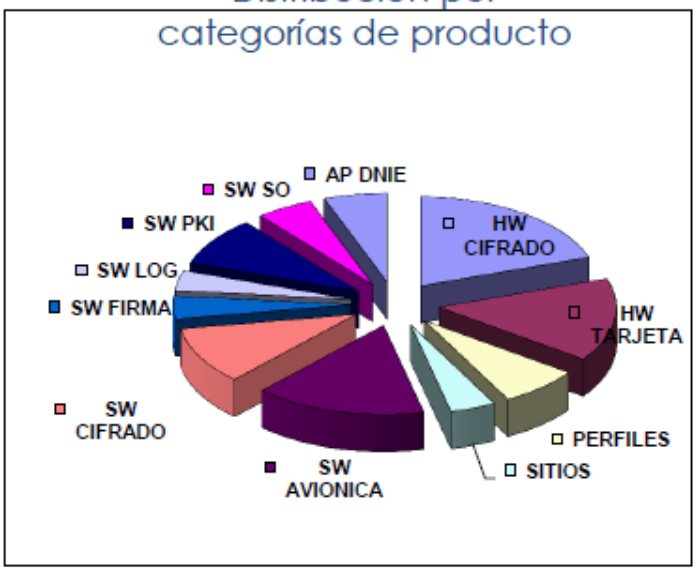
- Mejoras de filtros e interfaz
- Uso de **Complex Event Processing** (CEP)
- Integrada con **Guvnor**
- Generación de **mapas de calor**
- Gestión de Alarmas

1.9 ORGANISMO DE CERTIFICACIÓN

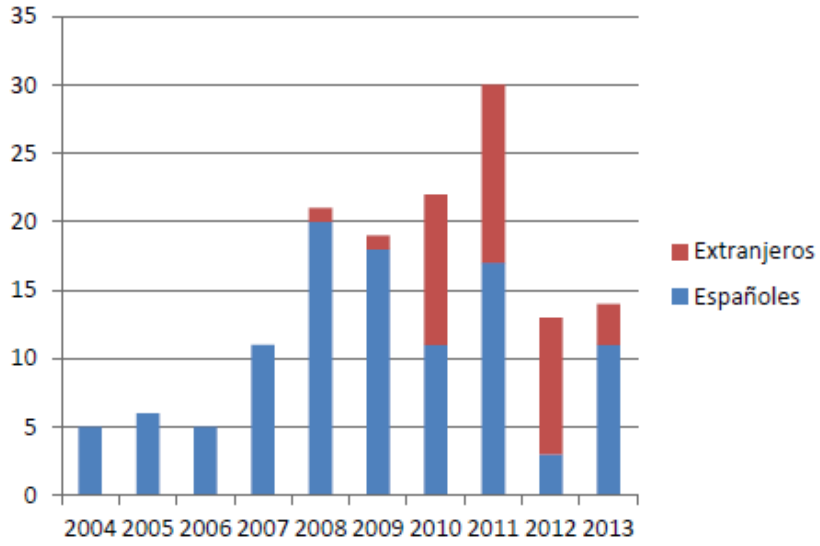
Estadísticas del OC



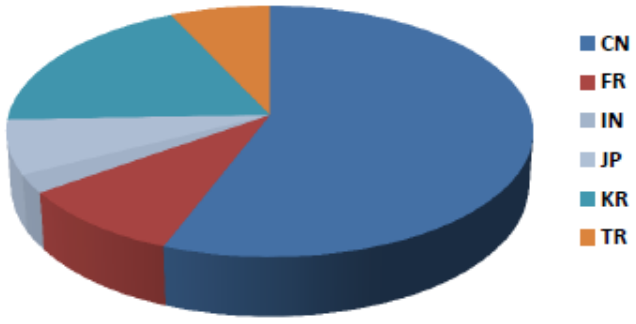
Expedientes de certificación abiertos por año y modalidad



Certificación de Productos Extranjeros



Expedientes de certificación por año españoles vs extranjeros



Distribución por países

1.10 PROYECTOS 2014

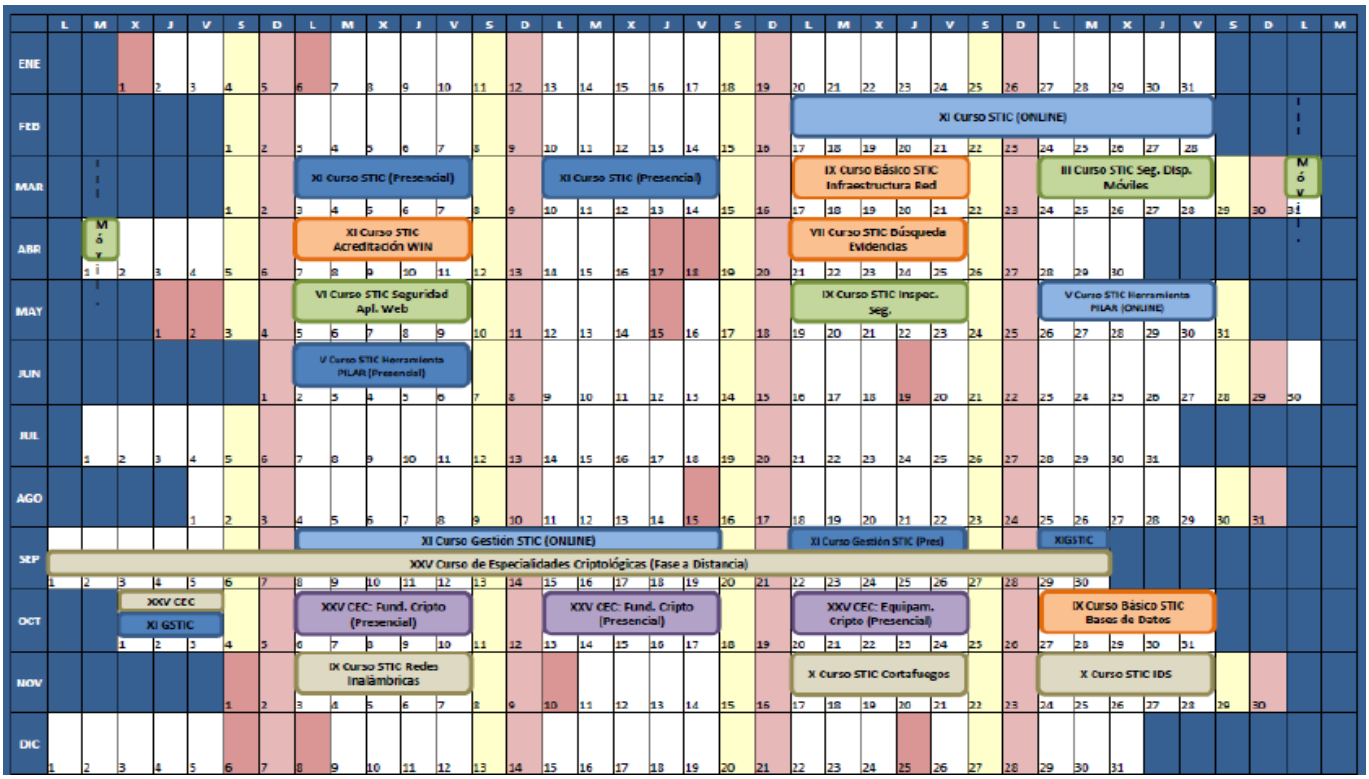
Formación – cursos STIC 2014

- Actualización de los Cursos Online
- Aumento fase online cursos presenciales (acuerdo INAP)
- Curso Seguridad Dispositivos Móviles - 2 días extra
- Oferta final dependiente de los presupuestos

Guías CCN-STIC

- Actualización de las guías dispositivos móviles:
- Android
- iPhone
- iPad

Plan de Formación 2014

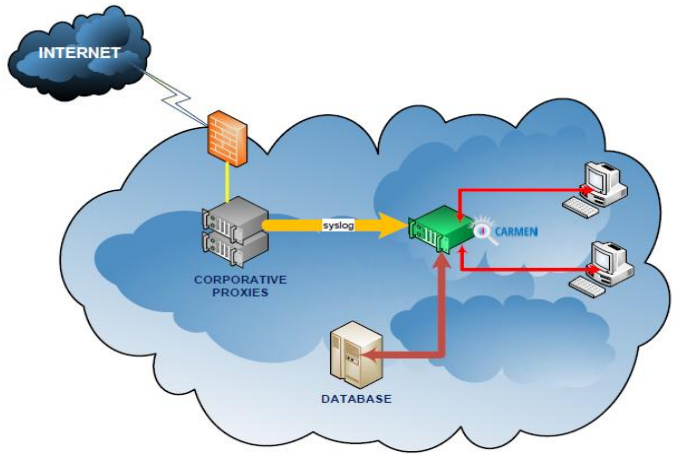


Sistemas de alerta temprana

- Continuar con el despliegue de sondas.
- Incorporar nuevas fuentes.
- Mejoras de la correlación.
- **Mejoras compartición de reglas/IOC** con terceros.

CARMEN v2

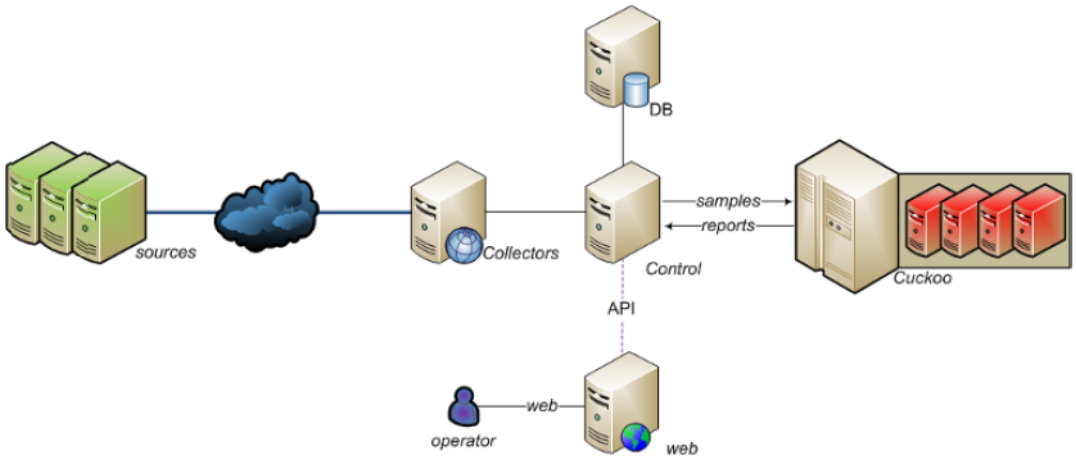
- Incorporar mejoras a la herramienta.
- Despliegue progresivo (VM) CARMEN v2



CARMEN v2 – Arquitectura

MARTA (Motor de Análisis Remoto de Troyanos Avanzados)

- Inyección local y remota de malware
- Soporte a múltiples vías de infección
- Detección de packers
- Extracción de HASH (MD5, SHA256, SHA1)
- Cálculo de fuzzy hashing
- Captura de tramas de red
- Monitorización de cambios en el sistema
- Extracción de registros
- Soporte a múltiples versiones de Sistemas Operativos
- Informes en múltiples formatos
- Múltiples análisis de forma concurrente



MARTA - Arquitectura

Herramientas CCNDroid

Informes código dañino (CCN-CERT ID)

- Informes reducidos de código dañino.
- Asociado a lo más visto en el SAT-INET.
- Enlazado a los tickets para facilitar resolución de incidentes.

LUCIA

- 1ª Fase: Producción en CCN-CERT
- 2º Fase: Piloto con Organismos seleccionados.
- 3ª Fase: Despliegue resto Organismo interesados

ANEXO B: RECOPILACIÓN DE NOTICIAS INCIDENTES MÁS SIGNIFICATIVOS OCURRIDOS DURANTE 2013[1]

ENERO 2013

- **Fallo en el sistema de privacidad de Facebook[2]**

La aplicación New Year's Midnight Delivery, que la compañía desarrolló para enviar mensajes privados automáticamente con el cambio de año, registró problemas y algunos de los mensajes se hicieron públicos. Aunque esta vulneración de la aplicación solo podía realizarse si se tenía constancia del fallo, este nuevo episodio en los problemas de seguridad de Facebook ha hecho mella entre los más de mil millones de usuarios que posee la red social. Por su parte, Facebook registró este problema un día antes de Nochevieja y se vio obligado a dar de baja este servicio. Posteriormente, la red social informó a The Verge que había solventado el problema y que la aplicación volvía a estar disponible a tiempo para las campanadas.

- **Detenido por grabar y colgar en Internet maniobras de conducción temeraria[3]**

La Guardia Civil, en el transcurso de la operación PARAGOLPES, ha procedido en Elche (Alicante) a la detención de una persona como presunto autor de delitos contra la seguridad del tráfico por grabar y colgar en Internet maniobras de conducción temeraria con vehículos. Además, han imputado a otras ocho personas por los mismos hechos.

- **El Ministerio de Hacienda alerta sobre un nuevo caso de phishing[4]**

El Ministerio de Hacienda y Administraciones Públicas ha advertido de un caso de "phishing", mediante la circulación de correos electrónicos falsos en los que se piden datos para la devolución de impuestos y en los que para el pago se solicita cumplimentar un formulario, aparentemente muy similar a los utilizados en la web del Ministerio, con su logo e imagen institucional, en el que se solicitan datos bancarios.

- **Se inaugura el Centro Europeo de Ciberdelincuencia[5]**

El 11 de enero entró en funcionamiento el nuevo Centro Europeo de Ciberdelincuencia (EC3) para contribuir a proteger a las empresas y a los ciudadanos europeos frente a la ciberdelincuencia. Cecilia Malmström, comisaria de la UE para Asuntos de Interior, participará en la inauguración oficial del Centro que tiene su sede en la Oficina Europea de Policía, Europol, en La Haya (Países Bajos). La apertura del Centro Europeo de Ciberdelincuencia (EC3) constituye un cambio importante en la forma en que la UE ha abordado la ciberdelincuencia hasta la fecha. Por encima de todo, el planteamiento del EC3 tendrá más

1 Datos obtenidos de la página web www.ccn-cert.cni.es

2 http://www.elmundo.es/elmundo/2013/01/02/navegante/1357133228.html

3http://www.interior.gob.es/press/detenida-una-persona-por-grabar-y-colgar-en-internet-maniobras-de-conduccion-temeraria-con-vehiculos-14652

4http://www.minhap.gob.es/Documentacion/Publico/GabineteMinistro/Notas%20Prensa/2013/CONVOCATORIAS/04-01-13%20Aviso%20de%20fraude%20en%20correos.pdf

5 http://europa.eu/rapid/press-release_IP-13-13_es.htm

visión de futuro y será más integrador. Se pondrán en común los conocimientos técnicos y la información, se prestará apoyo a las investigaciones criminales y se fomentarán las soluciones a escala de la UE. La actividad del EC3 se centrará en las actividades ilegales en línea de las bandas de delincuencia organizada, especialmente en los ataques dirigidos contra las operaciones bancarias y otras actividades financieras en línea, la explotación sexual infantil en línea y los delitos que afecten a las infraestructuras críticas y a los sistemas de información en la UE. El Centro también facilitará la investigación y el desarrollo y garantizará el refuerzo de las capacidades de las autoridades responsables de la aplicación de la ley, los jueces y los fiscales; asimismo, llevará a cabo evaluaciones de las posibles amenazas, que incluirán análisis, previsiones de tendencias y alertas tempranas. Con el fin de desmantelar un mayor número de redes de delitos informáticos y de perseguir a un mayor número de sospechosos, el EC3 recopilará y tratará los datos relacionados con la ciberdelincuencia y ofrecerá un servicio de asistencia en materia de ciberdelincuencia a las fuerzas de seguridad de los países de la UE. Además, prestará apoyo operativo a los países de la UE (por ejemplo, contra la intrusión, el fraude, el abuso sexual de menores en Internet, etc.) y aportará conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas.

- **Nuevo informe ENISA sobre las principales tendencias en ciberamenazas[6]**

ENISA, la agencia de ciberseguridad de la UE, ha publicado el primer y más completo análisis del panorama de ciberamenazas de 2012, donde se recogen más de 120 informes de amenazas. En el informe se identifican y enumeran las principales, así como sus tendencias, y se concluye que los "drive-by exploits" se han convertido en la amenaza número uno en la web.

- **Detenidas cinco personas que estafaron más de 1.000.000 € con mails enviados desde cuentas secuestradas y cartas nigerianas[7]**

Agentes de la Policía Nacional han detenido en Madrid a cinco personas por estafar más de un millón de euros mediante el envío masivo de mails desde cuentas secuestradas y cartas nigerianas. Pirateaban cuentas de correo desde las que escribían a las personas que figuraban en la agenda pidiéndoles dinero para solventar una situación personal de gravedad. También prometían importantes cantidades de dinero procedentes de fortunas inexistentes a cambio del pago por adelantado del pago de supuestos trámites administrativos. El grupo desarticulado actuaba a nivel internacional. Sus víctimas han sido localizadas en Estados Unidos, Noruega, Polonia, Canadá, Reino Unido, Pakistán e Italia.

- **Nueva vulnerabilidad crítica en Java**

Investigadores de seguridad recomiendan la desactivación inmediata de Java tras detectarse una nueva vulnerabilidad crítica 0-day en la última versión del lenguaje y

6http://www.enisa.europa.eu/media/press-releases/nuevo-informe-sobre-las-principales-tendencias-en-el-primer-panorama-de-ciberamenazas-elaborado-por-la-agencia-enisa-de-la-ue

7 http://www.policia.es/prensa/20130111_1.html

plataforma de Oracle que ya está siendo aprovechada al menos por dos exploits. El código asignado a esta nueva vulnerabilidad 0-day de Java para la que no hay parche es CVE-2013-0422 reportada originalmente en el blog "Malware don't need Coffee". Aunque el responsable del anuncio indica que la vulnerabilidad parece ser exclusiva de la versión 7 update 10, el US-CERT (US Computer Emergency Readiness Team) publicó que las versiones afectadas son "7 update 10 y anteriores". La vulnerabilidad cae en la categoría de ejecución remota de código: A través de una página especialmente diseñada por el atacante, un usuario puede habilitar la ejecución remota de código sin su conocimiento.

- **8 de cada 10 internautas usa las redes sociales[8]**

8 de cada 10 internautas usa las redes sociales, un 5% más que en 2011. El mercado de las redes sociales sigue creciendo, pero con menor intensidad, por lo que se puede considerar que ha entrado en una etapa de madurez. Esta es una de las conclusiones a las que llega la IV Estudio Anual de Redes Sociales publicado por IAB Spain.

- **Agentes de la Policía Nacional se incorporarán a la actividad del recién creado Centro Europeo de Ciberdelincuencia[9]**

Agentes de la Policía Nacional se incorporarán a la actividad del recién creado Centro Europeo de Ciberdelincuencia EC3 como pioneros en la introducción del primer proyecto de investigación sobre redes anónimas en Europol. Cómo enfrentarse de manera más eficaz a los delitos informáticos actual y hacer del ciberespacio un lugar más seguro son algunas de las tareas que desarrollará la Brigada de Investigación Tecnológica. Este nuevo Centro aunará conocimientos, prestará apoyo a las investigaciones y fomentará soluciones válidas en toda la Unión Europea. La prioridad de las investigaciones se centrará en la lucha contra la pornografía infantil en Internet y al fraude a gran escala mediante ataques a servicios bancarios, robo de identidad e intrusión en móviles de última generación.

- **Octubre Rojo: nueva campaña de ciberespionaje avanzado a gran escala[10]**

La empresa de seguridad Kaspersky Lab ha publicado un informe de investigación que identifica una nueva campaña de ciberespionaje dirigida contra organizaciones diplomáticas, centros de investigaciones científicas y organismos gubernamentales en varios países, que lleva operando desde hace al menos cinco años. Esta campaña se dirige principalmente a países de Europa Oriental, las ex repúblicas de la antigua URSS y los países de Asia Central, aunque las víctimas se encuentran en todas partes de Europa Occidental y América del Norte. El principal objetivo de los creadores era obtener documentación sensible de las organizaciones comprometidas, que incluyeran datos de inteligencia geopolítica, así como credenciales de acceso a sistemas clasificados de ordenadores, dispositivos móviles personales y equipos de red.

8 http://www.iabspain.net/noticias/8-de-cada-10-internautas-usa-las-redes-sociales-un-5-mas-que-en-2011/

9 http://www.policia.es/prensa/20130113_1.html

10 http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

- **La guardia civil detuvo en 2012 a 66 cibercriminales**[11]

La Guardia Civil detuvo en 2012 a 66 cibercriminales y explotó un total de 88 operaciones contra la delincuencia en Internet y en el ámbito tecnológico. Estos datos fueron dados a conocer por Arsenio Fernández de Mesa, director general de la Benemérita, quien participó en la inauguración del I Curso Especial Básico de Investigación Tecnológica, que se celebra esta semana en la Universidad de Alcalá de Henares (Madrid).

- **Líneas estratégicas del plan de Administración Electrónica del Gobierno 2013-2015**[12]

El ministro de Hacienda y Administraciones Públicas, Cristóbal Montoro, presidió la semana pasada el Consejo Superior de Administración Electrónica, en el que se aprobaron las líneas maestras del plan de Administración Electrónica del Gobierno para 2013-2015 y ha quedado refrendado el eje de Administración Electrónica de la Agenda Digital para España. Ambos documentos constituyen una hoja de ruta para modernizar la Administración, reducir el déficit público y racionalizar el sector público mediante el impulso de la Administración Electrónica esta Legislatura.

- **Cae la botnet Virut, responsable de infectar 300.000 ordenadores**[13]

Una acción conjunta en la que se han visto envueltos principalmente investigadores del Computer Emergency Response Team (CERT) de Polonia y el Proyecto Spamhaus, ha conseguido interferir por fin las operaciones de Virut, una botnet que hasta ese momento controlaba alrededor de 300.000 equipos. En diciembre, Spamhaus consiguió registrar todos los nombres de dominio de Virut, pero los responsables de la botnet fueron capaces de trasladar las direcciones maliciosas a un nuevo proveedor, obstaculizando los esfuerzo de sus perseguidores. El golpe definitivo llegó cuando NASK, la red académica y de investigación con sede en Polonia que controla el registro del dominio '.pl', comenzó a moverse por la infraestructura de Virut para suspender su actividad. "Además, Spamhaus contactó con el CERT de Austria y Rusia para cerrar los dominios ".at" y ".ru" restantes de Virut", ha explicado uno de sus responsables, Thomas Morrison. "En cooperación con Spamhaus y debido a la evidencia provista, CERT-GIB fue capaz de cerrar todos los dominios de Virut en tan solo unas horas". Ahora falta que el equipo austriaco siga su ejemplo.

- **El 65% de las empresas teme un ataque cibernético en 2013**[14]

Una nueva encuesta publicada por el Business Continuity Institute (BCI) en colaboración con BSI ha revelado que al 65 por ciento de las organizaciones les

11 http://ecodiario.eleconomista.es/interstitial/volver/peugeot508ene/espana/noticias/4543235/01/13/La-guardia-civil-detuvo-en-2012-a-66-cibercriminales.html

12 http://www.minhap.gob.es/es-es/prensa/en%20portada/2013/Paginas/20130115_admonelectronica.aspx

13http://www.siliconweek.es/noticias/cae-la-botnet-virut-responsable-de-infectar-300-000-ordenadores-32288

14 http://www.redseguridad.com/actualidad/info-tic/el-65-de-las-empresas-teme-un-ataque-cibernetico-en-2013

preocupa sufrir un ataque cibernético en 2013. La encuesta también revela que el 71 por ciento de las entidades considera el uso de Internet para "ataques de código dañino" una tendencia importante que requiere una respuesta en materia de continuidad de negocio, siendo un 42 por ciento las que buscan gestionar la prevalencia y la adopción de servicios que dependen de Internet, tales como la nube, dentro de sus actividades de formación y preparación ante dichos ataques.

- **Una variante del troyano bancario Shylock se extiende por Skype[15]**

Un plugin denominado msg.gsm permite que el troyano Shylock pueda enviar mensajes y transferir archivos a través de Skype sin ser detectado, para, una vez instalado en el sistema, robar los datos bancarios de los usuarios. Desde Skype aseguran estar poniendo ya remedio. Expertos de la firma de seguridad CSIS han detectado un aumento en el número de máquinas infectadas por Shylock, un troyano bancario que en su última variante se está expandiendo a través de Skype. Para ello aprovecha un plugin llamado msg.gsm para poder enviar mensajes y ficheros evitando los sistemas de alerta de Skype, además de eliminar el rastro del historial. Una vez en el sistema, el troyano Shylock se hace con las cookies de los servicios bancarios, establece una conexión a distancia y modifica la página de inicio de sesión del banco en tiempo real mediante la inyección de su código específico.

- **El spam se ha reducido un 8,2% en 2012[16]**

Kaspersky Lab ha presentado su Informe de spam del 2012, un periodo en el que el porcentaje de spam disminuyó en el transcurso del año, permaneciendo durante los tres últimos meses por debajo del 70%. Este descenso se debe al gradual abandono de muchos anunciantes que ahora prefieren utilizar otras formas legales para publicitar sus artículos y servicios. Sin embargo, eso no significa que el spam esté condenado a extinguirse. De acuerdo con el informe, el porcentaje medio de "spam" en 2012 ha sido del 72,1%, un 8,2% menos que en 2011, debido principalmente a la mejora de la protección "antispam", ya que casi todos los sistemas de correo, incluso los gratuitos, llevan incorporados filtros antispam, y el nivel de detecciones es del 98%.

- **UE alcanza un acuerdo político sobre nuevo mandato de seguridad informática[17]**

Los Veintisiete alcanzaron el pasado 28 de enero un acuerdo político con el Parlamento Europeo y la Comisión Europea sobre el nuevo mandato de la Agencia Europea de Seguridad de las Redes de la Información (ENISA), que tendrá finalmente una duración de siete años. "Se trata de un acuerdo que llega a tiempo, particularmente de cara a la estrategia de seguridad cibernética y la propuesta legislativa sobre redes y seguridad de la información que serán aprobadas próximamente por la Comisión Europea", señaló la comisaria europea de Agenda Digital, Neelie Kroes, en un breve comunicado.

- **Perfil sociodemográfico de los internautas. Análisis de datos INE 2012[18]**

15 http://www.csospain.es/Una-variante-del-troyano-bancario-Shylock-se-extiende-por-Sk/seccion-alertas/noticia-129717

16 http://www.securelist.com/en/analysis/204792276/Kaspersky_Security_Bulletin_Spam_Evolution_2012

17 http://www.elconfidencial.com/ultima-hora-en-vivo/2013/01/alcanza-acuerdo-politico-sobre-nuevo-mandato-20130129-88616.html

El ONTSI presenta el informe "Perfil sociodemográfico de los internautas. Análisis de datos INE 2012" realizado en virtud del convenio con el Instituto Nacional de Estadística.

FEBRERO

- **Cuentas de Yahoo hackeadas por un ataque XXS[19]**

Una nueva campaña de ataques a través de mensajes de correo electrónico ha explotado una vulnerabilidad de la web de Yahoo con la intención de robar cuentas de correo de sus usuarios y poner en marcha a ataques de spam. El ataque se inició con el envío de correos basura, con el nombre del usuario en la línea de asunto y el mensaje "chequea esta página" con el enlace abreviado "bit.ly". Al pinchar en el link, se iba a una web enmascarada de noticias de MSNBC que contenía un artículo sobre cómo hacer dinero trabajando desde casa, según los expertos de Bitdefender.

- **Un ciberataque afecta a 250.000 cuentas de Twitter[20]**

Twitter reconoció el pasado fin de semana que un total de 250.000 cuentas de sus usuarios, de los 200 millones de usuarios que tiene, se han visto afectadas por "un sofisticado ataque" en el que se han podido robar tanto los nombres de los usuarios, como correo electrónico y otros datos. El director de seguridad de la red social, Bob Lord, ha señalado que el ataque "no es trabajo de aficionados" pero no ha querido vincularlo a los ataques informáticos que sufrieron semanas atrás los periódicos Wall Street Journal y The New York Times. Con todo, Lord ha destacado que "los ladrones han sido extremadamente sofisticados, y creemos que otras empresas y organizaciones han podido sufrir ataques similares".

- **ONTSI presenta dos nuevos estudios sobre Gobierno Abierto[21]**

El 58,6 por ciento de los españoles considera que los canales que actualmente existen para participar en los asuntos públicos a través de Internet son "insuficientes", según un estudio sobre "Gobierno Abierto" presentado este martes por el director del Observatorio Nacional de Telecomunicaciones y Sociedad de la Información (ONTSI), Pedro Martín Jurado.

- **Día Internacional de Internet seguro[22]**

Hoy 5 de Febrero se celebra el "Día Internacional de Internet seguro" o SID (Safer Internet Day). Se trata de un evento promovido por la Comisión Europea y organizado por INSAFE que se celebra cada año para concienciar y promover el uso responsable y seguro de la Red y las Nuevas Tecnologías. Bajo el lema "Conéctate y respeta" se quiere

18 http://www.ontsi.red.es/ontsi/es/estudios-informes/perfil-sociodemogr%C3%A1fico-de-los-internautas-an%C3%A1lisis-de-datos-ine-2012

19 http://www.pcworld.es/seguridad/robos-de-cuentas-de-correo-en-yahoo

20 https://blog.twitter.com/2013/keeping-our-users-secure

21http://www.red.es/redes/sala-de-prensa/nota-de-prensa/el-655-de-los-ciudadanos-considera-como-buena-o-muy-buena-la-calidad-d?quicktabs_1=0

22 http://www.diainternetsegura.es/

dar a conocer a los usuarios los peligros que existen cada día en Internet y animar a los internautas a crear una convivencia pacífica en la que se pueda evitar el uso de la Red como como medio para difundir amenazas, injurias y calumnias o establecerse como soporte para para el acoso, ciberbullying, intromisiones informáticas y otros delitos informáticos.

- **Un virus en Facebook compromete 16.000 contraseñas[23]**

MSIL/Agent.NKY. es un virus que afecta a los usuarios de Facebook y que, hasta el momento, ha conseguido hacerse con las credenciales de miles de usuarios de la red social. Así lo ha hecho saber ESET, quien lleva un año investigando esta red de bots que concentra sus ataques en Israel. Denominado genéricamente MSIL/Agent.NKY, ESET asegura que en el último año ha detectado diferentes variantes del troyano. "Tras el descubrimiento inicial, fuimos capaces de encontrar otras variantes del troyano, unas más antiguas y otras más modernas. También se consiguieron estadísticas de detección, que revelaron a Israel como el país con mayor actividad del código malicioso".

- **La CE quiere que las empresas "críticas" informen sobre los ciberataques[24]**

La Comisión Europea ha presentado un plan destinado a proteger las comunicaciones electrónicas e incrementar la seguridad de las redes y la información. Bruselas quiere obligar a los países a dotarse de capacidades mínimas para proteger sus redes frente a ciberataques. La UE quiere endurecer las normas sobre ciberdelincuencia. La Comisión Europea ha presentado hoy un plan destinado a proteger las comunicaciones electrónicas e incrementar la seguridad de las redes y la información, que ha sido presentado por la jefa de la diplomacia de la UE, Catherine Ashton; la vicepresidenta de la CE y comisaria de la Agenda Digital, Neelie Kroes, y la comisaria europea de Interior, Cecilia Malmström. Las medidas que buscan implantar supondrá que más de 40.000 firmas, incluyendo empresas de energía, transportes, bancos, operadoras de telecomunicaciones y hospitales podrían ser obligados a informar sobre los ciberrobos que hayan podido sufrir bajo una nueva normativa propuesta por Bruselas, según la BBC.

- **Directrices para proteger datos PCI DSS en la nube[25]**

El PCI Security Standards Council (PCI SSC) ha publicado el informe "PCI DSS Cloud Computing Guidelines Information Supplement", de gran importancia para el Cloud Special Interest Group (SIG). En respuesta a las dudas sobre si se puede mantener información de tarjetas de pago (PCI) en un servicio cloud, el PCI Security Standards Council señala que sí, pero hacerlo no es sencillo, explicando en una guía las normas de seguridad que las empresas deben cumplir.

- **Un "hacker" compromete los correos electrónicos de la familia Bush[26]**

23 http://www.csospain.es/Un-virus-en-Facebook-compromete-16.000-contrasenas-/seccion-actualidad/noticia-130185

24 http://cincodias.com/cincodias/2013/02/07/empresas/1360407545_850215.html

25http://www.net-ecurity.org/secworld.php?id=14379&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)

Un pirata informático ha conseguido robar información privada de las cuentas de correo de los ex presidentes George H.W. Bush y su hijo, George W. Bush, y ha procedido a colgar en Internet imágenes íntimas de ambos, entre ellas de Bush padre convaleciente en el hospital donde estuvo ingresado recientemente por complicaciones de una bronquitis que hicieron temer seriamente por su vida, según mensajes privados de la familia.

- **Aparece una nueva versión del botnet Kelihos[27]**

Esta es la tercera vez que Kelihos resurge, un botnet peer-to-peer cuya nueva versión es mucho más resistente a las técnicas de localización, pudiendo permanecer latente en las máquinas infectadas durante un largo período de tiempo.

Analistas de Kaspersky Lab han descubierto una nueva versión del botnet Kelihos, la cual presenta una mayor resistencia a las técnicas de localización y una característica que le permite permanecer en estado latente durante largos períodos en las máquinas infectadas para ayudar a evitar la detección. El botnet también utiliza una avanzada capacidad de flujo rápido para ocultar los dominios que utiliza para el comando y control y la distribución de malware.

- **Golpe policial a una de las mayores redes cibercriminales[28]**

El Cuerpo Nacional de Policía ha llevado a cabo una compleja investigación contra una de las mayores redes de cibercrimen dedicada a infectar con ransomware millones de ordenadores de todo el mundo y obtener unos beneficios que superarían el millón de euros anuales. Una operación que permanece abierta y en la que hasta ahora hay 11 detenidos. El conocido en España como "el virus de la Policía" es un tipo de malware que bloquea el ordenador y solicita el pago de una multa de 100 euros por acceder a páginas que contienen pornografía infantil o webs de intercambio de archivos. Sólo en nuestro país, desde que se detectó el virus en mayo de 2011, se han presentado más de 1.200 denuncias aunque el número de perjudicados es con seguridad mucho mayor. La investigación realizada por la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional se ha desarrollado a nivel internacional y ha afectado al menos a 22 países, siendo de especial importancia la colaboración de EUROPOL e INTERPOL para coordinar los grupos de trabajo en los países implicados.

- **Los usuarios de Internet llegarán a los 4.000 millones en 2020[29]**

Un nuevo estudio revela que los usuarios de Internet llegarán hasta los 4.000 millones en el año 2020, con grandes poblaciones de usuarios ubicadas en China, India y África. Ante ese crecimiento los problemas de seguridad aumentarán y esto hará que los gobiernos tengan que abrir la mente para comprender el impacto de sus decisiones.

- **Nuevo informe ENISA sobre "la nube" en la protección de Infraestructuras Críticas[30]**

26 http://www.europapress.es/portaltic/internet/noticia-hacker-publica-fotos-intimas-familia-bush-20130208131641.html

27 http://www.csospain.es/Aparece-una-nueva-version-del-botnet-Kelihos/seccion-alertas/noticia-130371

28 http://www.interior.gob.es/file/59/59611/59611.pdf

29http://blogs.technet.com/b/trustworthycomputing/archive/2013/02/06/linking-cybersecurity-policy-and-performance-microsoft-releases-special-edition-security-intelligence-report.aspx

ENISA, la agencia de ciberseguridad de la UE, ha publicado un nuevo informe acerca de la informática en la nube desde la perspectiva de la Protección de Infraestructuras de Información Crítica (CIIP, por sus siglas en inglés) en el cual ha identificado tanto el papel fundamental que desempeña la informática en la nube, dada la concentración de usuarios y datos, como el creciente uso que se está haciendo de ella en sectores críticos como el de las finanzas, la sanidad o los seguros.

- **La UE publica su Estrategia de Ciberseguridad[31]**

El programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo Terrorismo de la Organización (CICTE) de los Estados Americanos (OEA), felicitó a la Unión Europea por publicar su Estrategia de Ciberseguridad, adoptada el 7 de febrero de 2013 y que se encuentra disponible en el siguiente enlace http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

- **Facebook reconoce haber sufrido un "sofisticado" ataque informático**

Apenas dos semanas después de que Twitter anunciara la detección de un "ataque sofisticado" que podría haber entregado a los "hackers" información personal de cerca de 250.000 usuarios, Facebook acaba de anunciar lo propio. La red social ha reconocido haber sido objeto de una serie de ciberataques realizados por un grupo de "hackers", aunque no tienen evidencias de que la información de los usuarios haya podido quedar expuesta.

- **La UE anuncia sanciones contra Google[32]**

Las autoridades de protección de datos de los 27 países de la UE han anunciado este lunes que impondrán sanciones a la empresa tecnológica estadounidense Google, antes del verano, por negarse a ajustar su política de privacidad a la legislación comunitaria.

En octubre de 2012, los Veintisiete concluyeron que la política de privacidad de Google incumple las normas de la UE sobre protección de datos y le dieron un plazo de cuatro meses para modificarla. En particular, las agencias europeas de protección de datos pidieron a Google que ofrezca una información más clara y completa sobre los datos que recoge, el plazo de almacenamiento, su utilización, y la combinación de datos recabados por diferentes servicios, como YouTube, Gmail o Google+.

- **El 85% de las webs legítimas fueron comprometidas en 2012[33]**

El número de ataques de malware contra páginas web creció un 600% el año pasado, según WebSense, que también asegura que la tendencia es la creación de sites que incluyan código de ataque automático. Aunque algunas páginas están desarrolladas de manera

30 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

31http://seguridad-informacion.blogspot.com.es/2013/02/union-europea-publica-estrategia-de.html?utm_source=feedburner&utm_medium=email&utm_campaign

32 http://tecnologia.elpais.com/tecnologia/2013/02/19/actualidad/1361260869_404980.html

33 http://www.itespresso.es/paginas-web-comprometidas-106925.html

específica para servidor malware a quienes la visite, WebSense calcula que hay un 85% de páginas web legítimas que han sido comprometidas.

- **Los gobiernos de Reino Unido e India combatirán juntos la ciberdelincuencia[34]**

El Gobierno británico e indio establecerán presuntamente este martes un grupo de trabajo conjunto para combatir la ciberdelincuencia. Londres espera que esta medida ayude a salvaguardar los datos bancarios y telefónicos de millones de británicos, muchos de los cuales están almacenados en servidores indios.

- **Novedades en el código dañino móvil: smartphones que infectan PCs[35]**

Muchos usuarios de smartphones necesitan liberar espacio en sus dispositivos para que éstos sean más rápidos. La gran demanda de este tipo de programas que permiten agilizar el funcionamiento de los smartphones, ha generado un crecimiento de la oferta, que incluye, también, programas maliciosos. En Google Play, además de las aplicaciones legítimas que cumplen esta función, han aparecido otras que sólo fingen que limpian el sistema. El malware para PCs que infecta dispositivos móviles no es novedoso; pero en este caso funciona al revés: una aplicación que se ejecuta en un dispositivo móvil (smartphone), diseñada para infectar PCs. Kaspersky Lab ha descubierto esta aplicación en Google Play y su nombre es "SuperClean".

- **Las APT y los ataques DDoS preocupan a operadores y empresas[36]**

Airbor Networks ha publicado la octava edición de su Informe Mundial de Seguridad de Infraestructura (WISR), del que se desprende que las amenazas persistentes avanzadas (APT) se posicionan como una gran preocupación tanto para los operadores de red como para las empresas, junto con la creciente complejidad de los ataques de denegación de servicio (DDoS). Por un lado, el informe señala que el incremento de las "botnets" o máquinas comprometidas en las redes de los proveedores de servicios está causando un gran nivel de inquietud, dadas las múltiples variantes de malware que existen, su evolución y la incapacidad de sistemas de seguridad para luchar contra ellos de forma efectiva. De cara al futuro, el estudio revela una mayor preocupación por las APT, el espionaje industrial, la exfiltración de datos e los insiders maliciosos ante tendencias como BYOD y las redes sociales, que abren a los hackers aún más puntos de entrada para acceder a la red.

- **Readaptación del código dañino para atacar a varios sectores económicos[37]**

La empresa de seguridad McAfee ha publicado el "Informe de amenazas de McAfee: cuarto trimestre de 2012" en el que McAfee Labs revela que los ataques sofisticados, destinados originalmente al sector de las industrias financieras, ahora se destinan cada vez más a otros sectores críticos de la economía, mientras que se está implementando un conjunto emergente de tácticas y tecnologías nuevas para evadir

34 http://www.europapress.es/epsocial/noticia-gobiernos-reino-unido-india-combatiran-juntos-ciber-delincuencia-20130219115939.html

35 http://www.kaspersky.es/about/news/virus/2013/Novedades_en_el_malware_movil_smartphones_que_infectan_PCs_

36 http://www.csospain.es/Las-APT-y-los-ataques-DDoS-preocupan-a-operadores-y-empresas/seccion-alertas/noticia-130630

37 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf21

las medidas de seguridad estándar del sector. El informe también expone la proliferación continua de troyanos que roban contraseñas y de amenazas persistentes avanzadas (APT), tales como Operation High Roller y Project Bliztkrieg, además de la expansión de sus ataques a blancos del gobierno, la manufactura y la infraestructura de transacciones comerciales.

- **Aumenta el volumen de exploits contra aplicaciones críticas de negocio[38]**

Según Palo Alto Networks, los ataques contra aplicaciones de redes sociales e intercambio de archivos son mínimos en comparación con las que atentan contra aplicaciones de negocio como Microsoft SQL Server o Active Directory. Tras analizar el tráfico de las redes de más de 3.000 organizaciones, la empresa de seguridad concluye que las redes sociales, los videos y el intercambio de archivos no son las principales fuentes de amenazas. Esa es la principal conclusión que se extrae de su Informe sobre Amenazas y Uso de las Aplicaciones, según el cual, los exploits siguen atacando los activos más valiosos de las empresas a través de aplicaciones corporativas de uso común.

- **12,6 millones las víctimas de usurpación de identidad identificadas en los EE.UU.[39]**

En 2012 los incidentes de usurpación o robo de identidad se incrementaron en más de un millón de víctimas y los estafadores robaron más de 21.000 millones de dólares, la cantidad más alta desde 2009, según el estudio presentado por Javelin Strategy & Research. El estudio encontró que han sido 12,6 millones las víctimas de suplantación de identidad en los Estados Unidos en el último año, lo que equivale a una víctima cada 3 segundos. El informe también encontró que casi 1 de cada 4 receptores de emails fraudulentos se convirtió en una víctima de robo de identidad, donde el robo de datos de números del Seguro Social fue la más realizada.

- **El próximo 8 de abril de 2014 finalizará el soporte de Windows XP SP3 y Office 2003**

El próximo 8 de abril de 2014 finalizará el soporte para Windows XP SP3, Microsoft Exchange Server 2003 y Office 2003. Desde esa fecha, Microsoft no publicará ni estarán disponibles nuevos parches de seguridad, actualizaciones de seguridad o el soporte técnico, tanto físico como online, para los citados productos.

- **Kaspersky alerta de la aparición de MiniDuke, un backdoor que espía entidades gubernamentales[40]**

Kaspersky Lab ha alertado de la aparición de MiniDuke, un nuevo programa malicioso que espía a entidades gubernamentales e instituciones de todo el mundo. Así, MiniDuke combina "sofisticadas amenazas de la vieja escuela con exploits avanzados en Adobe Reader para reunir información de inteligencia geopolítica de grandes objetivos".

- **Más de 18 millones de dispositivos HTC son vulnerables a ciberataques[41]**

38 http://www.csospain.es/Se-dispara-el-volumen-de-exploits-contra-aplicaciones-critic/seccion-mercado/noticia-130755

39 http://www.net-security.org/secworld.php?id=14450&utm_source=dlvr.it&utm_medium=twitter

40 http://www.theguardian.com/technology/2013/feb/27/hackers-attack-european-governments-miniduke

Las vulnerabilidades detectadas en muchos dispositivos HTC permiten la instalación de aplicaciones de terceros que podrían robar información personal. La Comisión Federal de Comercio estadounidense acusa a la compañía de no diseñar sus productos pensando en la seguridad.

MARZO

- **El 63 por ciento de las organizaciones están infectadas con bots[42]**

El 63 por ciento de las organizaciones están infectadas con bots. Además, más de la mitad sufre ataques de nuevo malware cada día. Éstas son algunas de las principales conclusiones del Informe de Seguridad 2013 realizado por Check Point.

- **La Guardia Civil detiene a una persona por más de una veintena de delitos de "child grooming"[43]**

La Guardia Civil, en el marco de la operación "SUSOLOKITO", ha detenido a una persona por 23 delitos contra la libertad e indemnidad sexual, conocidos como delitos de "child grooming" o acoso sexual de menores a través de Internet. El detenido, J.M.H., de 22 años de edad, contactaba con niñas menores de edad (entre trece y quince años) a través de una red social, las cuales eran amenazadas en conversaciones privadas, para que se desnudaran ante la webcam.

- **Nace el único Centro de Ciberseguridad Industrial en España y Latinoamérica[44]**

Este mes de marzo se pone en marcha en España el Centro de Ciberseguridad Industrial (CCI), que oficialmente se presentará en junio y que agrupará a las empresas de este sector tanto de la Península Ibérica como de Latinoamérica. El objetivo de este nuevo centro será impulsar y contribuir a la mejora de la ciberseguridad industrial en España y Latinoamérica. Así, el Centro de Ciberseguridad Industrial aspira a convertirse en el punto independiente de encuentro de los organismos, privados y públicos, y profesionales relacionados con las prácticas y tecnologías de la ciberseguridad Industrial. Cabe destacar que son estas industrias las que controlan las torres de refrigeración, los generadores eléctricos que proporcionan la energía necesaria o los sistemas de extinción de incendios, todas ellas infraestructuras críticas muy vulnerables.

- **Desarticulada una red de phishing avanzado que estafó 300.000€ a usuarios de banca online[45]**

Agentes de la Policía Nacional han desarticulado una red de phishing avanzado que estafó 300.000€ a usuarios de banca online de alto poder adquisitivo.

41 http://www.csospain.es/Mas-de-18-millones-de-dispositivos-HTC-son-vulnerables-a-cib/seccion-alertas/noticia-130922

42 http://www.csospain.es/-El-63-por-ciento-de-las-organizaciones-estan-infectadas-con/seccion-actualidad/noticia-130954

43 http://www.guardiacivil.es/es/prensa/noticias/4341.html

44 http://www.cci-es.org/

45 http://www.policia.es/prensa/20130306_1.html

Réplicas casi idénticas de páginas web de diferentes bancos servían para capturar los datos personales y claves bancarias de las víctimas, cuyos móviles comenzaron además a no funcionar correctamente. Este era el último escollo a superar para consumar el fraude; para ello la red duplicaba la tarjeta SIM del teléfono móvil de las víctimas, lo que permitía conocer el código de seguridad enviado en un SMS por la entidad. Hay 10 detenidos en Figueras y Gerona, entre ellos el máximo responsable, sus tres lugartenientes y los encargados de la apertura de cuentas bancarias con documentación falsificada.

- **El botnet Asprox sigue difundiendo spam e infectando ordenadores[46]**

Trend Micro asegura que Asprox se ha actualizado para ser más eficaz, y ahora utiliza una variedad de plantillas de spam en diferentes idiomas con el fin de maximizar su espectro de víctimas.

- **La virtualización y el BYOD centran las preocupaciones en materia de seguridad[47]**

Siete de cada diez directivos de TI a nivel mundial creen que la virtualización es la tendencia con mayor impacto sobre la capacidad de su organización de alcanzar un estado óptimo de seguridad, mismo porcentaje que señala también a la complejidad de los ataques (como los DDoS) como una causa relevante de esta incapacidad de securizar la compañía.

- **La Policía Nacional ha detenido a 750 personas en 2012 por injurias, amenazas y delitos contra la intimidad en Internet[48]**

La Policía Nacional ha detenido a 750 personas en 2012 por injurias, amenazas y delitos contra la intimidad en España, el triple que el año anterior, según los datos del balance realizado por la Brigada de Investigación Tecnológica (BIT).

- **La ICANN establece nuevas directrices de seguridad para los dominios de Internet[49]**

La Corporación para la Asignación de Nombres y Números de Internet (ICANN) está abordando los problemas de seguridad relacionados con el sistema de nombres de dominio (DNS) a través del lanzamiento de una nueva serie de directrices, como informa ZDNet.

En la actualidad, la ICANN gestiona una gran cantidad de servidores raíz de nombres de dominio pero también los ISP y proveedores de servicios de hosting web pueden implementar nombres sencillos de dominio, asociados a direcciones IP de servidores.

- **El código dañino se centra en Android y en la tecnología NFC[50]**

46 http://www.csospain.es/El-botnet-Asprox-sigue-difundiendo-spam-e-infectando-ordenad/seccion-alertas/noticia-131143

47 http://www.f5.com/about/news/surveys/rsa-security-trends-survey-2013/

48 http://www.policia.es/prensa/20130309_1.html

49http://www.siliconnews.es/2013/03/12/la-icann-establece-nuevas-directrices-de-seguridad-para-los-dominios-de-internet/?utm_source=2013-03-12&utm_medium=email&utm_campaign=siliconnews_daily

50 http://www.csospain.es/El-malware-se-centra-en-Android-y-en-la-tecnologia-NFC/seccion-actualidad/noticia-131405

Android se ha convertido en el objetivo preferido de los ciberdelincuentes. Ésta es una de las principales conclusiones de un estudio de G-Data quien advierte que el malware para Android está a punto de convertirse en una epidemia. Además, la tecnología NFC también va a comenzar a ser objetivo.

- **El CNI recibe 200 ciberataques importantes en tres meses**[51]

En lo que va de año el Centro Nacional de Inteligencia (CNI) ha recibido más de 200 ataques cibernéticos importantes frente a la veintena que se producían al año en 2009. Este fue el dato que ofreció ayer el propio director del CNI, Félix Sanz Roldán, durante la clausura del IV Salón Internacional de Tecnologías para Seguridad y Defensa (Homsec).

- **Desarticulada una organización de fraude online**[52]

Agentes de la Policía Nacional han desarticulado una organización que suplantó conocidas web de compraventa y pago online con las que defraudó más de 400.000 euros. Los detenidos imitaban estos prestigiosos portales para ofertar inexistentes aparatos tecnológicos de última generación y otros objetos a precios muy ventajosos con la finalidad de captar la atención de sus potenciales víctimas. Además, copiaban igualmente la apariencia de la pasarela de pago de forma que, mediante técnicas de phishing, los compradores que habían caído en el engaño ingresaban el importe del producto en una de las múltiples cuentas bancarias abiertas por los miembros de la red con identidades falsas.

- **Dos bancos y tres canales de TV surcoreanos, víctimas de un ciberataque masivo**[53]

La policía de Corea del Sur investiga un "ciberataque" masivo contra canales de televisión y varios bancos del país, cuyas redes se han visto paralizadas por completo a las 14.00 hora local (06.00 hora española), en principio por razones desconocidas. "Estamos investigando estos ciberataques en estos momentos", confirmó un portavoz policial después de que la agencia de noticias Yonhap informara de ataques contra tres canales de TV -KBS, MBC y YTN- y dos entidades bancarias -Shinhan y Nonghyup-, en un contexto de tensión con su Corea del Norte.

- **El cibercrimen se consolida como el delito del futuro según la Europol**[54]

El tráfico de drogas sigue siendo el rey entre los delitos a los que se dedican las organizaciones criminales o mafias en la Unión Europea, pero el crimen cibernético está consolidándose como el delito del futuro. Así lo ve la Europol tras investigar a 3.600 grupos dedicados al crimen organizado en la región. De este modo, y a pesar de que siguen involucrados mayoritariamente en el tráfico de drogas o el tráfico de

51 http://www.abc.es/espana/20130316/abci-centro-nacional-inteligencia-recibe-201303152049.html

52http://www.interior.gob.es/press/desarticulada-una-organizacion-que-suplanto-conocidas-web-de-compraventa-y-pago-online-con-las-que-defraudo-mas-de-400-000-euros-14924

53 http://www.elmundo.es/elmundo/2013/03/20/navegante/1363762330.html

54 http://www.csospain.es/El-cibercrimen-se-consolida-como-el-delito-del-futuro-segun-/seccion-actualidad/noticia-131581

mujeres, los delitos cibernéticos están logrando cada vez un mayor peso en su estrategia criminal.

- **Los ciberataques: un nuevo filo para viejas armas**[55]

ENISA, la agencia de ciberseguridad de la UE, ha publicado una nota informativa titulada "Los ciberataques: un nuevo filo para viejas armas" en la que se analiza y lleva a cabo un seguimiento de recientes ciberataques. Según la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), los últimos ciberataques dirigidos contra organismos gubernamentales y empresas de primera línea demuestran la existente necesidad de contar con una mayor concienciación y unos conocimientos técnicos superiores con relación a la seguridad de información y de red.

- **Alertan de ataques de código dañino contra sistemas punto de venta**[56]

Denominado vSkimmer, el troyano está diseñado para infectar ordenadores Windows que dispongan de un lector de tarjetas asociado. El pasado 13 de febrero fue detectado por primera vez este tipo de infección en la red de sensores de McAfee y ya se está promocionando en foros piratas como una versión mejorada de Dexter, un programa malware de ataque a puntos de ventas que se descubrió el pasado mes de diciembre.

- **Utilizan la crisis de Chipre como gancho para ciberamenazas**[57]

Los ciberdelincuentes están aprovechando los problemas económicos de Chipre para distribuir sus ciberamenazas. Se han detectado correos electrónicos que incluyen enlaces a páginas maliciosas que pretenden inyectar malware que aprovecha vulnerabilidades de Adobe Flash Player, Adobe Acrobat Reader y Java.

- **Informe sobre los troyanos bancarios más peligrosos**[58]

Un informe de G Data muestra que ZeuS sigue provocando buena parte de los robos de banca por Internet. ZeuS es un troyano bancario que nació hace más de cinco años. A pesar de su dilatada trayectoria, este veterano troyano (junto a su variante Citadel) ha aglutinado casi el 50% de los ataques contra usuarios de banca online en el segundo semestre de 2012. En cualquier caso, el último Informe de Malware de G Data (que estudia los últimos seis meses de 2012) muestra que el número de este tipo de ataques se redujo considerablemente respecto a la primera mitad del año. Un descenso que podría estar motivado por las detenciones de cibercriminales importantes en este sector durante los primeros meses de 2012, lo que vendría a confirmar que este mercado de los troyanos bancarios está controlado por unos pocos programadores que dirigen la mayor parte de los ataques.

- **Alertan de ataques de spam que utilizan la buena reputación de Google Translate**[59]

55 https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons

56 http://www.csospain.es/Alertan-de-ataques-de-malware-contra-sistemas-punto-de-venta/seccion-Seguridad/noticia-131652

57 http://www.europapress.es/portaltic/software/seguridad-00646/noticia-utilizan-crisis-chipre-gancho-ciberamenazas-20130324100026.html

58 http://www.gdata.es/uploads/media/G_Data_MWR_H2_2012_ES.pdf

Expertos de seguridad de Barracuda han detectado que algunos spamers están aprovechando la buena reputación del traductor de Google para sortear los filtros antispam y redirigir a sus potenciales víctimas a sitios web farmacéuticos.

ABRIL

- **Darkleech, la misteriosa campaña de código dañino que afecta a servidores Apache**[60]

Al menos 20.000 páginas de Internet han sido infectadas durante las últimas semanas por un nuevo, sofisticado y misterioso malware bautizado como Darkleech, que se propaga a través de uno de los servidores web más populares que existen a día de hoy: Apache. El número podría ser mucho mayor, ya que la campaña en cuestión lleva activa desde agosto de 2012. De momento, ningún experto ha sido capaz de identificar la vulnerabilidad de la que se aprovechan sus autores para controlar equipos basados en Apache.

- **La AEPD inicia actuaciones previas de investigación a Google por su política de privacidad**[61]

El director de la Agencia Española de Protección de Datos, José Luis Rodríguez Álvarez, ha remitido hoy una carta a Larry Page, CEO de Google Inc., y a los responsables de Google Spain en la que les comunica la apertura de actuaciones previas de investigación en relación con la nueva política de privacidad de Google implantada en el mes de marzo del año pasado.

- **Mozilla, Google y Opera introducen nuevos motores de navegador**[62]

Según el CTO de Mozilla, Brendan Eich, "Servo es un intento por reconstruir el navegador web para adaptarlo al nuevo hardware" con el objetivo de resolver las vulnerabilidades de seguridad y de "diseñar una plataforma capaz de utilizar al máximo el rendimiento del futuro hardware masivamente paralelo para proporcionar experiencias web más ricas".

- **Nuevo código dañino para Skype convierte a los PCs en mineros de Bitcoins**[63]

La empresa de seguridad Kaspersky ha detectado una nueva amenaza de seguridad que se expande a través del servicio de VoIP Skype al engañar a sus usuarios para que pinchen en enlaces acortados que apuntan a la descarga de archivos desde Hotfile. Dichos enlaces van acompañados de textos con frases como "No me puedo creer que esta foto sea tuya", esto es, aprovechando técnicas de ingeniería social.

59 http://www.csospain.es/Alertan-de-ataques-de-spam-que-utilizan-la-buena-reputacion-/seccion-alertas/noticia-131848

60 http://www.siliconweek.es/noticias/darkleech-la-misteriosa-campana-de-malware-que-afecta-a-servidores-apache-35053

61 http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/abril/130402_NP_Act_prev_Google.pdf

62 http://www.networkworld.es/actualidad/mozilla-google-y-opera-introducen-nuevos-motores-de-navegador

63 http://www.siliconweek.es/noticias/nuevo-malware-para-skype-convierte-a-los-pcs-en-mineros-de-bitcoins-35254

- **Uno de cada cinco sitios visitados por los usuarios móviles presenta amenazas**[64]

Un informe de Blue Coat pone de manifiesto que el panorama de amenazas móviles está creciendo. Según la compañía, a día de hoy el 40 por ciento del código dañino móvil bloqueado por el servicio de seguridad en la nube WebPulse de Blue Coat tiene su origen en malnets conocidas.

- **Nueva denuncia en Bruselas contra Google, ahora por Android**[65]

Cuando aún no se fallado la denuncia contra Google por supuestas prácticas monopolísticas, la Comisión Europea ya tienen una nueva denuncia contra el gigante de Internet, en esta ocasión por sus sistema para móviles Android. El denunciante es el mismo, la coalición Fairsearch.org, que agrupa a Microsoft, Oracle, Nokia y TripAdvisor, entre otros.

- **Nuevo troyano para Android se hace pasar por una actualización de Flash Player**[66]

La botnet Cutwail, que ya ha distribuido el conocido troyano bancario Zeus, está ahora distribuyendo un nuevo troyano para Android llamado Stels. Este troyano infecta dispositivos Android haciéndose pasar por una actualización de Adobe Flash Player. Si las potenciales víctimas no están utilizando un dispositivo Android, los desarrolladores del malware han ideado una alternativa - si los enlaces maliciosos se abren en un navegador como Internet Explorer, en un equipo portátil o de sobremesa, se redirige a los usuarios a páginas web con el exploit-kit Blackhole. El equipo de seguridad de Dell ha publicado un análisis detallado del escenario de ataque.

- **Actualización del documento de Normas ISO**[67]

El portal Criptored recoge la actualización del documento de Normas ISO de Seguridad de la Información, teniendo en cuenta que las normas ISO 27001 y 27002 son la base para la gestión, auditoría y certificación de la seguridad de la información. Dos normas más se destacan. La ISO 27005 que establece la metodología y marco de referencia para la gestión de riesgos y la ISO 27004 que trata las métricas para medir el desempeño del SGSI y controles. Mientras la serie 27k está llegando ya a la treintena, las próximas versiones de las ISO 27002 y 27001 ya pueden comentarse en base a sendos drafts de febrero de 2013.

- **Los proveedores de servicios de Internet no aplican filtros contra los grandes ciberataques**[68]

En su análisis de un reciente ciberataque masivo, ENISA, la agencia de ciberseguridad de la UE, señala que los proveedores de servicios de Internet (PSI) no han aplicado medidas de seguridad conocidas y accesibles desde hace más de una

64 http://www.csospain.es/Uno-de-cada-cinco-sitios-visitados-por-los-usuarios-moviles-/seccion-actualidad/noticia-132075

65 http://tecnologia.elpais.com/tecnologia/2013/04/09/actualidad/1365497857_454544.html

66 http://www.siliconweek.es/noticias/nuevo-troyano-para-android-se-hace-pasar-por-una-actualizacion-de-flash-player-35320

67 http://www.criptored.upm.es/guiateoria/gt_m327a.htm

68 https://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability

década. Este error es uno de los principales factores que explican la incapacidad de contrarrestar los ciberataques más importantes, según subraya la Agencia en su nota informativa "¿Los recientes ciberataques pueden realmente amenazar la disponibilidad de Internet?".

- **El Congreso crea una Subcomisión sobre las Redes Sociales**[69]

El Pleno del Congreso de los Diputados aprobó el pasado 11 de abril la propuesta de crear una Subcomisión sobre las Redes Sociales en el seno de la Comisión de Interior. La propuesta, impulsada por el Grupo Popular y aprobada por la Comisión de Interior en su sesión del día 27 de febrero, tiene como objetivo analizar la situación actual en España y en los países de nuestro entorno respecto a las Redes Sociales.

- **Anteproyecto de Ley de Seguridad Privada**[70]

El titular del Interior, Jorge Fernández Díaz, presentó el pasado 12 de abril al Consejo de Ministros el Anteproyecto de Ley de Seguridad Privada que, por primera vez, regula en una norma de rango legal las medidas de seguridad física, electrónicas, informáticas y que pretende, entre otros objetivos, impulsar la coordinación y cooperación entre los sectores de seguridad pública y privada y abrir a este último la posibilidad de prestar nuevos servicios demandados por la sociedad y que no están recogidos en la normativa actual. De hecho, la normativa vigente no está adaptada al entorno tecnológico esencial para el sector de la seguridad privada y no recoge el régimen actual de distribución de competencias entre el Estado y las autonomías

- **WordPress sufre un ataque de fuerza bruta a gran escala**[71]

Semana tras semanas, los ciberdelincuentes continúan causando estragos en Internet. La última víctima de sus fechorías es la inmensa red de blogs que basan su estructura en la plataforma WordPress. Y es que dicha plataforma está siendo atacada por una botnet de ordenadores que cuenta con alrededor de 90.000 direcciones IP y que emplea la fuerza bruta para intentar adivinar la contraseña de administrador de las distintas instalaciones.

- **Desarticulado un grupo de estafas en Internet**[72]

Agentes de la Policía Nacional han desarticulado un grupo que en solo dos meses estafó más de 40.000 euros mediante cargos bancarios ilícitos a través de Internet. Utilizaban la página web de Loterías y Apuestas del Estado como

69 http://www.congreso.es/portal/page/portal/Congreso/Congreso/SalaPrensa/NotPre?_piref73_7706063_73_1337373_1337373.next_page=/wc/detalleNotaSalaPrensa&idNotaSalaPrensa=9344&anyo=2013&mes=4&pagina=1&mostrarvolver=S&movil=null

70 http://www.interior.gob.es/press/la-nueva-ley-de-seguridad-privada-sera-mas-estricta-y-rigurosa-con-el-sector-y-abrira-la-puerta-a-nuevos-servicios-15021

71 http://www.siliconweek.es/noticias/wordpress-sufre-un-ataque-de-fuerza-bruta-a-gran-escala-35545

72 http://www.interior.gob.es/press/desarticulado-un-grupo-que-en-solo-dos-meses-estafo-mas-de-40-000-euros-mediante-cargos-bancarios-ilicitos-a-traves-de-internet-15031

"monedero virtual", donde cargaban sin autorización de los titulares de las tarjetas cantidades que oscilaban entre los 90 y 180 euros que después desviaban a cuentas bancarias abiertas por la organización. También adquirían artículos electrónicos en la Red la Red de forma fraudulenta.

- **Correo, redes sociales y móviles, entradas del ciberdelito**[73]

Los ciberdelitos están presenten en la red mediante diferentes mecanismos y los cibercriminales diseñan nuevas estrategias para realizar sus ataques y conseguir información de sus víctimas para utilizarla en su beneficio. La vía de entrada de los ciberdelitos principalmente se realiza mediante el correo electrónico, las redes sociales y los terminales móviles, dependiendo de cada uno de las aplicaciones utilizadas por las víctimas la forma de ataque también es diferente.

- **Luz verde del Parlamento Europeo al nuevo Reglamento para ENISA**[74]

El pasado 16 de abril, el Parlamento Europeo votó en sesión plenaria en Estrasburgo la nueva propuesta de Reglamento para fortalecer a ENISA, la agencia europea de ciberseguridad (formalmente conocida como Agencia Europea de Seguridad de la Redes y de la Información). Esta propuesta de Reglamento se aprobó tal y como fue presentada, sin ninguna enmienda adicional, por una abrumadora mayoría de los eurodiputados, con 627 votos a favor de los 687 votos emitidos en total.

- **El Congreso pide al Gobierno que estudie pixelar mapas en Internet por razones de seguridad**[75]

El Congreso de los Diputados, a propuesta del PP y con el apoyo de todos los grupos, acordó el pasado jueves 18 de abril pedir al Gobierno que adopte medidas que propicien que zonas consideradas críticas para la seguridad nacional aparezcan en Internet de forma pixelada o difuminada, con el fin de evitar el riesgo de ataques terroristas.

- **La Policía Nacional detiene a los autores de varios robos gracias a una app de localización y rastreo de smartphones**[76]

Agentes de la Policía Nacional han detenido a tres jóvenes autores de varios robos gracias a una aplicación de localización y rastreo de un smartphone. La dueña del terminal sustraído colaboró con los agentes en la ubicación de los delincuentes facilitando en tiempo real, a través de la aplicación WhatsApp, el itinerario que los

73http://www.delitosinformaticos.com/04/2013/noticias/el-correo-electronico-redes-sociales-y-moviles-la-entrada-de-los-ciberdelitos#.Uq2wl2eA1y1

74http://www.enisa.europa.eu/media/press-releases/green-light-for-new-regulation-for-eu-cyber-security-agency-enisa-given-by-the-european-parliament

75 http://www.congreso.es/public_oficiales/L10/CONG/BOCG/D/BOCG-10-D-236.PDF

76 http://www.policia.es/prensa/20130422_1.html

ladrones iban realizando. Así los policías fueron siguiendo los pasos de los delincuentes desde Málaga, donde se cometieron los robos, hasta Córdoba, donde fueron finalmente detenidos gracias a los datos aportados por la app y comunicados por la víctima a la Policía.

- **Nuevo código dañino detectado en Google Play Store que afecta a 32 apps**[77]

Lookout Security ha detectado una nueva familia de código dañino para Android. Bautizado como BadNews el código dañino se ha encontrado en 32 aplicaciones, de cuatro desarrolladores diferentes, subidas a Google Play la tienda de aplicaciones para el sistema operativo de Google.

- **Japón quiere ayudar al bloqueo del sistema de navegación anónima Tor**[78]

La policía japonesa está instando a los proveedores de Internet a que ayuden a los administradores de sitios web que bloquear voluntariamente el uso de Tor, un sistema que permite navegar por Internet de forma totalmente anónima. La petición viene motivada después de la proliferación de usos de Tor para actividades delictivas, según las autoridades.

- **Las vulnerabilidades de día cero marcan los primeros meses de 2013**[79]

Las vulnerabilidades de día cero permanecen y continúan siendo una amenaza, mientras que la innovación en los ataques sigue creciendo en sofisticación, intensidad y severidad, según un informe de Trend Micro.

- **Detenido en Barcelona el presunto responsable del ciberataque a Spamhaus**[80]

Agentes de la Policía Nacional han detenido en Granollers (Barcelona) al supuesto responsable del ciberataque de denegación de servicio DDOS que colapsó Internet recientemente. La coordinación internacional entre los países afectados fue clave para la investigación que se inició en Holanda debido a una serie de ataques contra la compañía anti-spam, Spamhaus, que también afectó a Estados Unidos y Reino Unido.

- **Hackeados los servidores de LetsBonus**[81]

Según la información publicada por la propia compañía, los servidores de LetsBonus se han visto comprometidos. Sus usuarios han recibido un mensaje de

77 http://www.itespresso.es/nueva-amenaza-fraude-android-badnews-110196.html

78 http://www.elmundo.es/elmundo/2013/04/24/navegante/1366785194.html

79 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-zero-days-hit-users-hard-at-the-start-of-the-year.pdf

80http://www.interior.gob.es/press/la-policia-nacional-detiene-en-barcelona-al-responsable-del-mayor-ciberataque-de-denegacion-de-servicio-ddos-de-la-historia-15089

81 http://www.pcactual.com/articulo/actualidad/noticias/12928/hackeados_los_servidores_lets_bonus.html

correo electrónico por parte de la compañía indicándoles que deben de cambiar de inmediato su contraseña de acceso para evitar posibles accesos no autorizados.

- **Los troyanos alcanzan el 80% de todas las infecciones**[82]

PandaLabs, ha publicado los datos del primer trimestre de 2013, en el que se han recogido más de seis millones y medio de muestras. El estudio confirma que los troyanos siguen siendo los grandes protagonistas del malware, copando la creación de casi tres de cada cuatro muestras, cifras muy similares a las recogidas en 2012.

- **El Sistema de Alerta Temprana, SAT, del CCN-CERT cumple cinco años**[83]

El Sistema de Alerta Temprana, SAT, del CCN-CERT cumple cinco años con la difícil tarea de detener y eliminar las crecientes ciberamenazas. El sistema cuenta con dos vertientes: el SAT de la red SARA , en colaboración con el Ministerio de Hacienda y Administraciones Públicas, y el SAT de Internet. Los objetivos para este año 2013 son proseguir con su implantación en los organismos públicos, especialmente las Comunidades Autónomas y empresas consideradas estratégicas, así como una mejora en las capacidades de detección y de colaboración. Para facilitar la gestión de la información, el portal Web del CERT Gubernamental (www.ccn-cert.cni.es) ha incorporado una nueva sección con información del servicio y sus principales estadísticas.

MAYO

- **La AEPD presenta la primera guía en Europa sobre el uso de cookies**[84]

La Agencia Española de Protección de Datos (AEPD) y las asociaciones Adigital, Autocontrol e IAB Spain presentaron la primera guía en Europa elaborada conjuntamente por la autoridad de protección de datos y los representantes de la industria. La Guía sobre el uso de las cookies recoge las orientaciones, garantías y obligaciones que la industria se compromete a difundir y aplicar para adaptar la instalación de este tipo de archivos a la legislación vigente.

- **Una de cada cinco empresas ha sido víctima de una APT**[85]

Un estudio de seguridad realizado por la asociación ISACA entre 1.500 profesionales asegura que una de cada cinco empresas han sufrido un APT (Advanced Persistent Threat). El estudio señala que un 94% de los encuestados cree que este tipo de ataques representan una amenaza para la estabilidad económica y la seguridad nacional.

- **El porcentaje medio de spam en el tráfico de correo cae al 70 por ciento**[86]

82 http://prensa.pandasecurity.com/2013/04/los-troyanos-baten-un-nuevo-record-al-alcanzar-el-80-de-todas-las-infecciones-registradas-en-el-primer-trimestre-de-2013/

83 https://www.ccn-cert.cni.es/comunicados/NP2-201304-SAT.pdf

84 http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/abril/130429_NP_Guia_Cookies.pdf

85 http://www.isaca.org/Knowledge-Center/Research/Documents/APT_SurveyReport_WP_Spanish.pdf

España vuelve a situarse entre los 20 países generadores de spam, cuya cantidad ha disminuido de forma leve. No así el volumen de mensajes de correo con ficheros maliciosos, que asciende al 4 por ciento, y el phishing, que también se ha duplicado, según Kaspersky. El último informe de spam de Kaspersky Lab revela que la cantidad de spam en el tráfico de correo electrónico volvió a bajar un 1 por ciento en marzo, alcanzando una media del 70,1 por ciento.

- **Estrategias de Ciberseguridad en el mundo[87]**

ENISA ha actualizado un listado con todas las Estrategias de Ciberseguridad en el mundo (en abril del 2013). Algunos de estos documentos todavía están bajo consulta por lo que no han sido traducidos al inglés. Según dicho listado, son 13 los países de la Unión Europea que cuentan con Estrategia y 12 del resto del mundo.

- **Un fallo en Instagram permite a un atacante acceder a cualquier cuenta[88]**

La compañía de seguridad ESET se ha hecho eco de una vulnerabilidad Oauth en Instagram que podría ser explotada para robar la cuenta de cualquier usuario y acceder a sus fotos privadas.

- **Apple, condenada en Alemania a revisar su política de privacidad[89]**

Apple debe cambiar su política de privacidad en Alemania ya que no puede pedir "consentimiento mundial" para usar los datos personales de un cliente ni su ubicación. El documento de política de privacidad de Apple consta de 15 cláusulas en las cuales se explica cómo la compañía recoge información personal con cada movimiento que realiza el cliente a través de las cuentas Apple ID.

- **Hackers roban 34 millones de euros en un ataque a escala mundial[90]**

En uno de los mayores robos bancarios de la historia, una red global de ciberdelincuentes ha conseguido 45 millones de dólares (unos 34 millones de euros) de dos bancos de Oriente Próximos al vulnerar la seguridad de unas empresas de procesamiento de tarjetas de crédito y retirar dinero de cajeros automáticos en 27 países, según han asegurado este jueves fiscales de Estados Unidos. Según la demanda, la banda violó la seguridad de los ordenadores de dos compañías procesadoras de tarjetas de crédito, una en India en diciembre de 2012 y otra en Estados Unidos el pasado mes de febrero. Las compañías no fueron identificadas. Los piratas informáticos aumentaron el balance disponible y el límite de retirada de dinero en tarjetas de crédito de prepago de MasterCard emitidas por Bank of

86 http://www.csospain.es/El-porcentaje-medio-de-spam-en-el-trafico-de-correo-cae-al-7/seccion-actualidad/noticia-132725

87 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

88 http://www.csospain.es/Un-fallo-en-Instagram-permite-a-un-atacante-acceder-a-cualqu/seccion-alertas/noticia-132803

89 http://www.europapress.es/portaltic/sector/noticia-apple-condenada-alemania-revisar-politica-privacidad-20130509130252.html

90 http://www.elmundo.es/elmundo/2013/05/10/navegante/1368173194.html

Muscat de Oman y National Bank of Ras Al Jaimah PSC (RAKBANK) de Emiratos Árabes Unidos, según la demanda. Después distribuyeron tarjetas de crédito falsificadas a personas encargadas de retirar el efectivo en todo el mundo, lo que les permitió sacar millones de dólares desde cajeros automáticos en pocas horas.

- **OEA firma acuerdo sobre ciberseguridad[91]**

La Organización de los Estados Americanos (OEA) y el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) firmaron un acuerdo de cooperación con el objetivo de fortalecer el desarrollo de la seguridad cibernética en el continente americano.

- **El gobierno de India aprueba su Política Nacional de Ciberseguridad[92]**

El gobierno indio ha aprobado su Política Nacional Ciberseguridad, que tiene por objeto la creación de un "entorno informático seguro para una confianza adecuada en las transacciones electrónicas". Está política no sólo se refiere a las entidades del gobierno y a las grandes empresas, También está enfocada a los usuarios domésticos.

- **Estrategia Nacional de Seguridad cibernética de Panamá[93]**

El Gobierno de la República de Panamá adoptó la "Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas", con el fin de hacer frente a posibles ataques cibernéticos a los sistemas tecnológicos que utilizan las infraestructuras críticas del país, tanto del ámbito privado como estatal. La Estrategia Nacional contempla el desarrollo de acciones orientadas a mejorar la seguridad cibernética y hace especial énfasis en aquellas infraestructuras que son vitales para el bienestar de la población, los servicios básicos, el buen funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas.

- **Yahoo Japón confirma el robo de 22 millones de ID de usuarios[94]**

Yahoo Japón, el portal más importante del país asiático, ha confirmado el robo de 22 millones de identificaciones (ID) de usuarios. Eso sí, y tal y como ha asegurado Yahoo Japón, no se ha comprometido ni contraseñas ni datos privados. Al parecer, el ataque se produjo la semana pasada. Yahoo Japón ha reiterado que la información que se ha visto comprometida es pública. Las ID se utilizan junto con la contraseña para iniciar sesión en la página Web, y con frecuencia, se muestran cuando los usuarios dejan comentarios o utilizan sus tiendas o subastas.

- **La Guardia Civil detiene a una persona que difundía en redes sociales información personal de personajes públicos[95]**

91 http://www.voanoticias.com/content/oea-segurida-cibernetica-hackers-piratas/1657437.html

92 http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf

93 http://www.innovacion.gob.pa/noticia/1834

94 http://www.csospain.es/Yahoo-Japon-confirma-el-robo-de-22-millones-de-ID-de-usuario/seccion-actualidad/noticia-132995

La Guardia Civil en el transcurso de la operación "Semillero", ha procedido en Guadalajara a la detención de una persona por difundir a través de redes sociales información de carácter personal de personajes públicos. Al detenido se le imputan delitos de descubrimiento y revelación de secretos. La actividad desarrollada por esta persona estaba vinculada a la utilización de servicios de nuevas tecnologías, haciendo uso de redes sociales, servicios de telefonía de operadoras virtuales, mensajería instantánea, etc., con la finalidad de aprovecharse del anonimato que proporciona el uso de estos canales.

- **La Policía Nacional detiene a los responsables de un grupo que defraudó en Internet más de 750.000 euros con tarjetas clonadas[96]**

Agentes de la Policía Nacional han detenido a los responsables de un grupo que defraudó en Internet más de 750.000 euros con tarjetas clonadas. En esta fase de la investigación han sido arrestadas dos personas -en Palma de Mallorca y en Alicante- que presuntamente formarían la cúpula directiva de la organización en nuestro país. También está imputada una anciana de 82 años, madre de uno de los detenidos, responsable de enviar fuera de España el dinero que obtenían con sus actividades ilícitas. Compraban en la Red productos electrónicos de alta gama con tarjetas de crédito fraudulentas para, posteriormente, venderlos en páginas web de compraventa sirviéndose de empresas pantalla. Se les imputan delitos de falsificación de documento mercantil, blanqueo de capitales, pertenencia a organización criminal, estafa informática y alzamiento de bienes.

- **Las empresas de servicios de energía de EE.UU sufren ciberataques a diario[97]**

Ésta es una de las principales conclusiones de un estudio del Congreso de Estados Unidos, que revela que estos ciberataques ponen en peligro redes de suministro de energías independientes que a más de 300 millones de personas. Así, y según el estudio del Congreso de Estados Unidos, denominado "la vulnerabilidad de la red eléctrica", más de una docena de empresas de servicios públicos aseguró que sufría ciberataques a diario o de manera constante.

- **Detectan una campaña de ataques dirigidos de largo alcance[98]**

Investigadores de los laboratorios de ESET han dado con una amenaza que, utilizando archivos ejecutables firmados, busca robar información confidencial de diferentes organizaciones de todo el mundo, especialmente en Pakistán, pero también en España. Para realizar parte de esta campaña de ataques dirigidos se utilizó un certificado de firma de código para poder firmar archivos ejecutables, con el fin de mejorar su potencial para propagarse. El certificado otorgado a una empresa india se retiró de forma rápida, pero investigadores de ESET localizaron más

95http://www.interior.gob.es/press/la-guardia-civil-detiene-a-una-persona-que-difundia-en-redes-sociales-informacion-personal-de-personajes-publicos-15172

96 http://www.policia.es/prensa/20130521_1.html

97 http://www.csospain.es/Las-empresas-de-servicios-de-energia-de-EE.UU-sufren-ciberat/seccion-actualidad/noticia-133056

98 http://blogs.protegerse.com/laboratorio/2013/05/21/ataques-dirigidos-en-asia-utilizan-ejecutables-firmados-para-conseguir-su-objetivo/

de 70 ejecutables maliciosos que habían sido firmados usando este certificado, así como varias muestras similares sin firmar que fueron usadas en esta campaña.

- **Las Guías CCN-STIC de seguridad en dispositivos móviles accesibles a todos los usuarios[99]**

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN-CERT, ha hecho públicas sus Guías de la Serie CCN-STIC 450 sobre seguridad en dispositivos móviles. Guía CCN-STIC 453 Seguridad en Android, CCN-STIC 454 (iPad) y CCN-STIC 455 (iPhone). El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas, de ahí el interés del CCN en garantizar la seguridad en estos sistemas.

- **Firma del protocolo adicional al convenio sobre ciberdelincuencia del Consejo de Europa[100]**

El Consejo de Ministros ha autorizado la firma del Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Este Protocolo tiene por objeto la lucha contra el racismo, la discriminación racial, la xenofobia y la intolerancia, en el ámbito de los sistemas informáticos, y en particular, Internet, penalizando jurídicamente los actos racistas y xenófobos. Para ello, el Protocolo Adicional armoniza el derecho de los Estados miembros y de los demás estados firmantes, y amplia el ya firmado y ratificado por España Convenio sobre ciberdelincuencia.

- **Hackers chinos han accedido al armamento secreto del Pentágono[101]**

Hackers chinos han accedido a los más avanzados diseños de sistemas armamentísticos secretos de los Estados Unidos, según un informe confidencial elaborado por el Pentágono en colaboración con oficiales del Gobierno y la industria armamentística. Estados Unidos y China parecen librar una guerra cibernética en torno a sus secretos mejor guardados. Ambas naciones se acusan mutuamente de tratar de robar los secretos del otro mediante ciberataques, aunque también niegan las acusaciones que les afectan.

- **Detenido en España el presunto responsable de Liberty Reserve, plataforma de fraude online[102]**

Agentes de la Policía Nacional han detenido a Arthur Budovsky, fundador y máximo responsable de Liberty Reserve, junto a su lugarteniente, en una operación conjunta con Estados Unidos y realizada de forma simultánea en varios países. Liberty Reserve está considerada como la plataforma financiera del cibercrimen y habría sido utilizada como

99 https://www.ccn-cert.cni.es/comunicados/NP3-CCN-CERT-Seguridad-Dispositivos-moviles.pdf

100 http://www.lamoncloa.gob.es/ConsejodeMinistros/Referencias/_2013/refc20130524.htm#Ciberdelincuencia

101http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

102http://www.interior.gob.es/press/la-policia-nacional-detiene-a-arthur-budovsky-fundador-y-maximo-responsable-de-liberty-reserve-la-plataforma-financiera-del-cibercrimen-15221

medio para blanquear más de 6.000 millones de dólares mediante más de 55 millones de transacciones ilegales en todo el mundo.

- **Gusano en Skype: Rodpicom acumula más de 700 mil clics y se confirman nuevos medios de propagación[103]**

Durante la tarde del lunes de la semana pasada, miles de usuarios comenzaron a recibir distintos mensajes de sus contactos con un enlace que suponía ser una foto que los involucraba, pero que en realidad propagan un código malicioso reconocido como una variante de Win32/Gapz.E en realidad perteneciente a una familia de amenazas conocida como Win32/PowerLoader.A. Este código malicioso, infectaba el equipo y comenzaba a propagar los mismos mensajes con los que el usuario se infecto a todos sus contactos, su detección se asocia a la utilización de un avanzado packer conocido como Power Loader, que es capaz de saltar las protecciones del sistema e inyectar un dropper directamente en uno de los procesos principales del sistema: explorer.exe.

- **La ciberseguridad, elemento clave de la nueva Estrategia de Seguridad Nacional del Gobierno[104]**

El Consejo de Ministros ha aprobado este viernes un informe que incluye la nueva Estrategia de Seguridad Nacional, que contempla la creación de un Consejo de Seguridad Nacional que presidirá Mariano Rajoy y contará con la presencia de la mitad de los ministros. Entre los 12 riesgos de seguridad nacional se incluyen conceptos como el ciberterrorismo, los boicots a suministros energéticos, el espionaje, los ataques a infraestructuras críticas, además de los conflictos armados y el terrorismo.

JUNIO

- **El Consejo de Seguridad Nacional, nuevo órgano colegiado del Gobierno[105]**

El Consejo de Ministros del pasado 31 de mayo aprobó, no sólo la nueva Estrategia de Seguridad Nacional de 2013, sino el Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, con el fin de incluir entre las mismas al Consejo de Seguridad Nacional en su condición de Comisión Delegada para la Seguridad Nacional. Este Consejo de Seguridad Nacional nace con la vocación de administrar de una forma más eficaz y eficiente los recursos existentes y estará presidido por el presidente del Gobierno, excepto cuando S.M. el Rey asista a sus reuniones. Se reunirá periódicamente, al menos una vez cada dos meses, y estará compuesto por los siguientes miembros: Vicepresidente del Gobierno, Ministro de Asuntos Exteriores y Cooperación, Ministro de Defensa, Ministro de Hacienda y Administraciones Públicas, Ministro de Interior, Ministro de Fomento, Ministro de Industria, Energía y Turismo, Ministro de Economía y Competitividad, Director del

103 http://blogs.eset-la.com/laboratorio/2013/05/28/gusano-skype-rodpicom-700-mil-mensajeros/

104 http://www.elmundo.es/elmundo/2013/05/31/espana/1369985594.html

105 http://www.lamoncloa.gob.es/ConsejodeMinistros/Referencias/_2013/refc20130531

Gabinete de la Presidencia del Gobierno, que actuará como secretario, Secretario de Estado de Asuntos Exteriores, Jefe de Estado Mayor de la Defensa, Secretario de Estado de Seguridad, Secretario de Estado Director del Centro Nacional de Inteligencia, Responsable del Departamento de Seguridad Nacional

- **Los ataques dirigidos principal amenaza para 2013[106]**

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, adscrito al Centro Nacional de Inteligencia (CNI) ha dado a conocer su informe "Ciberamenazas 2012 y Tendencias 2013", en el que se hace balance del panorama internacional y nacional en el marco de los ciberincidentes. Según dicho informe, durante el año 2012 se han incrementado de un modo preocupante el número de incidentes catalogados con un riesgo muy alto o crítico por el propio CERT Gubernamental. Así, se ha pasado de 93 incidentes de este nivel en 2011, a 233 un año después, representando las **Amenazas Persistentes Avanzadas(o APT)** buena parte de este porcentaje. De hecho, y tal y como señala el documento, durante 2012 los ataques dirigidos se han convertido en la más significativa de las amenazas y la protección contra ellos se ha convertido en una de las principales preocupaciones de los responsables de seguridad de Tecnologías de la Información. Los ataques dirigidos son comúnmente utilizados con fines de espionaje industrial, de cara a obtener acceso a la información confidencial contenida en un sistema de información. Se trata de los ataques más difíciles de combatir.

- **España, entre los diez países con más víctimas de NetTraveler[107]**

Kaspersky Lab acaba de publicar un informe sobre NetTraveler, una familia de programas maliciosos utilizados por APT (Advanced Persistent Threat) que ha comprometido a más de 350 víctimas de alto perfil en 40 países distintos. España se encuentra entre los 10 países con más víctimas. Así, y según anuncian, "el grupo NetTraveler ha infectado a las víctimas tanto en el sector público como en el privado, incluyendo instituciones gubernamentales, embajadas, la industria del petróleo y gas, centros de investigación, contratistas militares y activistas políticos".

- **El troyano Zeus reaparece en Facebook[108]**

El virus Zeus, uno de los troyanos más peligrosos que fue descubierto en 2007 por primera vez, ha vuelto a aparecer con una nueva estrategia. El último ataque de Zeus utiliza Facebook para infectar ordenadores, según ha informado Techspot.com. Provoca que el ordenador del usuario no se apague una vez activado.

- **Microsoft y el FBI desmantelan una de las mayores redes de cibercrimen[109]**

La empresa informática Microsoft y el FBI desmantelaron una de las mayores redes de cibercrimen, responsable de un fraude financiero valorado en más de US$500 millones.

106 https://www.ccn-cert.cni.es/comunicados/NP4-Ciberamenazas.pdf

107 http://www.csospain.es/Espana,-entre-los-diez-paises-con-mas-victimas-de--NetTravel/seccion-actualidad/noticia-133311

108 http://www.europapress.es/portaltic/software/seguridad-00646/noticia-troyano-zeus-reaparece-facebook-20130606111707.html

109 http://www.bbc.co.uk/mundo/ultimas_noticias/2013/06/130606_ultnot_desmantelan_red_de_cibercrimen_bd.shtml

Según aseguró Microsoft en su sitio de internet, la operación de su Unidad contra Crímenes Digitales junto con el FBI consiguió acabar con el software maligno que como herramienta de la estafa en más de 1.000 computadoras infectadas. Estas computadoras fueron utilizadas para robar desde decenas de instituciones como American Express, Bank of America, Citigroup, Credit Suisse, PayPal de eBay, JPMorgan Chase, Royal Bank of Canada y Wells Fargo.

- **Metodología de Respuesta a Incidentes de la OEA[110]**

La Organización de los Estados Americanos, OEA, ha publicado en su portal web unos documentos del Programa de Seguridad Cibernética de la OEA/CICTE, relacionados con metodología de Respuesta ante Incidentes. Se trata de 15 documentos de lectura rápida procedentes del CERT de Societé Generale.

- **El CCN participará en el curso de verano de la Universidad Complutense sobre Ciberseguridad[111]**

Del 1 al 5 de julio tendrá lugar, en la en la localidad de San Lorenzo de El Escorial (Madrid), el curso "Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio" enmarcado dentro de la XXVI edición de los Cursos de Verano de la Universidad Complutense de Madrid y que cuenta con la participación del Centro Criptológico Nacional. En concreto, su Subdirector General Adjunto, Luis Jiménez, abordará una ponencia que lleva por título: "Retos del CNI en el espacio virtual. Perspectivas y soluciones. La Estrategia Nacional de Ciberseguridad".

- **Cada 22 segundos surge una nueva amenaza para Android[112]**

La empresa G Data SecurityLabs ha detectado que se produce una amenaza para el sistema operativo de Android cada 22 segundos. Este código dañino que está constituyendo todo un negocio para los cibercriminales, es capaz de interceptar información personal y llamar y enviar SMS a números de pago.

- **El 7% de los españoles han sido víctimas de robo de identidad en Internet[113]**

Cuantos más detalles personales se comparten en redes sociales, más expuestos están los internautas al robo de identidad, una práctica que permite a los ciberdelincuentes la obtención de bienes y servicios en nombre de la víctima. Kaspersky da las claves para minimizar los riesgos. El robo de identidad online se ha convertido en los últimos años en uno de los objetivos principales de los cibercriminales, ya que les permite desde obtener una tarjeta de crédito a solicitar un pasaporte, o acceder a una cuenta bancaria haciéndose pasar por otra persona. Se trata de una práctica muy lucrativa y, por tanto, habitual. Prueba de ello es que, según datos de Kaspersky Lab, el 7 por ciento de los españoles

110 http://www.oas.org/es/ssm/cyber/docs_irms.asp

111 http://www.ucm.es/data/cont/docs/71-2013-04-24-71113.pdf

112 http://www.europapress.es/portaltic/software/noticia-cada-22-segundos-surge-nueva-amenaza-android-data-20130612135026.html

113 http://www.csospain.es/El-7-por-ciento-de-los-espanoles-han-sido-victimas-de-robo-d/seccion-actualidad/noticia-133474

reconoce que ocasionalmente le han robado su identidad en Internet, y el 1 por ciento admite que esto le ocurre con frecuencia.

- **EEUU pidió datos de hasta 19.000 usuarios de Facebook y 32.000 de Microsoft[114]**

La red social Facebook recibió peticiones de datos de hasta 19.000 usuarios por parte del Gobierno de Estados Unidos y la compañía informática Microsoft de hasta 32.000 personas en el último semestre del año pasado, según han desvelado este sábado ambas compañías. Diversos organismos de la Administración presidida por Barack Obama realizaron, en total, entre 9.000 y 10.000 peticiones de información de entre 18.000 y 19.000 usuarios a Facebook, que ha destapado ahora dichos datos en virtud de un acuerdo alcanzado con las autoridades de Seguridad estadounidenses. Microsoft, por su parte, recibió entre 6.000 y 7.000 peticiones, avisos y órdenes de organismos locales, estatales y federales de Estados Unidos que afectaban a entre 31.000 y 32.000 usuarios. Difunde estos datos, al igual que Facebook, previo acuerdo con la Administración estadounidense. El escándalo sobre el "acceso directo" conseguido por el Gobierno estadounidense a ordenadores a través del programa Prism, de la Agencia Nacional de Seguridad -destapado por los diarios The Guardian y The Washington Post- ha exacerbado la preocupación sobre la privacidad en Internet y la transparencia gubernamental, precisamente en un momento en el que el Congreso debate cómo garantizar la privacidad de los datos de los usuarios en la Red y aumentar la transparencia de la Administración en tareas de Inteligencia.

- **Nuevo Reglamento y responsabilidades para la agencia de ciberseguridad de la Unión Europea ENISA[115]**

ENISA, la agencia de ciberseguridad de la Unión Europea (UE), ha recibido hoy, 18 de junio, un nuevo Reglamento mediante el cual se le encomienda un mandato de siete años dotado de un conjunto ampliado de responsabilidades. El nuevo Reglamento consagra los éxitos alcanzados por ENISA en áreas tales como la de los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés) en los Estados miembros, así como la de sus ejercicios de primera línea en el campo de la ciberseguridad, como por ejemplo la Cyber Europe 2012, que contó con la participación de 600 delegados de toda Europa.

- **Estados Unidos y Rusia firman un acuerdo para luchar contra las ciberamenazas[116]**

Tal y como publica The Washington Post, el acuerdo alcanzado entre Estados Unidos y Rusia, que se ha dado a conocer en el marco de la cumbre que se está celebrando en Irlanda del Norte entre el grupo de los 8, forma parte de los esfuerzos que se están llevando a cabo de manera bilateral para mejorar la cooperación. La experiencia de ambos países en la prevención ante una posible guerra nuclear es la base del acuerdo

114 http://www.europapress.es/portaltic/internet/noticia-eeuu-pidio-datos-19000-usuarios-facebook-32000-microsoft-20130617084841.html

115https://www.enisa.europa.eu/media/press-releases/nuevo-reglamento-y-responsabilidades-para-la-agencia-de-ciberseguridad-de-la-union-europea-enisa

116http://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html

alcanzado entre Estados Unidos y Rusia. El Centro de Reducción de Amenazas Nucleares de Estados Unidos, puesto en marcha en 1987 y que permite alertar a cada país en caso de que se estén realizando pruebas con misiles que podrían ser confundidos con actos de agresión, estará implicado.

- **Microsoft pagará a los hackers por encontrar vulnerabilidades en su software**[117]

Al igual que hace Google, Microsoft ha anunciado que ofrecerá pagos directos a cambio de ser informado acerca de determinados tipos de vulnerabilidades y técnicas de explotación detectadas en sus nuevas soluciones. Concretamente, el 26 de junio la compañía pondrá en marcha los programas de recompensa Mitigation Bypass Bounty, BlueHat Bonus for Defense, e Internet Explorer 11 Preview Bug Bounty. Según la compañía, "tener estos programas de recompensas ofrece una manera de aprovechar la inteligencia colectiva y la capacidad de los investigadores de seguridad para ayudar a proteger aún más a los clientes".

- **Facebook compromete la información de 6 millones de usuarios**[118]

Facebook ha puesto en peligro accidentalmente la información de contacto de 6 millones de usuarios. La red social está enviando mensajes a los afectados. El fallo ha puesto direcciones de correo y números de teléfonos de unos 6 millones de usuarios a disposición de los contactos o los amigos de éstos, que han podido ser conocidos por el algoritmo de recomendación de amistad que utiliza Facebook, según ha reconocido el equipo de seguridad de la compañía el viernes.

- **La justicia de la UE da la razón a Google sobre el derecho al olvido en Internet**[119]

El abogado general del Tribunal de Justicia de la UE se ha pronunciado sobre el alcance del derecho al olvido en Internet en un caso que enfrenta a España, y en concreto a la Agencia de Protección de Datos, con el gigante informático estadounidense Google. Según el dictamen, el buscador de Internet no tiene obligación de borrar contenido a petición de un usuario. El dictamen preliminar publicado por el abogado general del Tribunal no tiene carácter vinculante, aunque los jueces suelen seguir estas recomendaciones en el 80% de los casos. La sentencia final se publicará dentro de unos meses.

- **Los servicios de Yahoo!, Google, Facebook y Amazon acaparan el 30% del phishing**[120]

El phishing va en aumento. Así lo indican los últimos datos aportados por el informe La evolución de los ataques de phishing de 2011 a 2013, elaborado por Kaspersky Lab y que analiza este tipo de fraude online, una práctica que consiste en que los ciberdelincuentes crean una copia falsa de un sitio web popular (un servicio de correo electrónico, una web de banca online, una red social, etc.) y tratan de

117 http://www.csospain.es/Microsoft-pagara-a-los-hackers-por-encontrar-vulnerabilidade/seccion-actualidad/noticia-133563

118 http://www.idg.es/pcworld/Facebook-compromete-la-informacion-de-6-millones-d/doc133599-Seguridad.htm

119 http://sociedad.elpais.com/sociedad/2013/06/25/actualidad/1372142902_959606.html

120 http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf

atraer a los usuarios a estas páginas web de modo que cuando el usuario introduce sus datos de acceso, estos últimos pasan a manos de cibercriminales que los utilizan para robar dinero, distribuir spam y malware a través del correo electrónico o redes sociales o vender sus bases de datos de contraseñas robadas a otros cibercriminales.

- **Detectan primer código dañino que secuestra dispositivos móviles[121]**

Por ser particularmente rentables para los cibercriminales, los falsos antivirus y el malware del tipo ransomware para PC llevan varios años en circulación. Sus creadores han deseado trasladar su éxito a las plataformas móviles, y parece que lo han conseguido, ya que se ha detectado la que se considera la primera amenaza ransomware dirigida a dispositivos móviles. El hallazgo, realizado por Symantec, es un falso antivirus que se está propagando entre dispositivos Android. Al igual que en sus versiones para PC, el falso antivirus, bautizado con el nombre de Android.Fakedefender, utiliza malware que deliberadamente malinterpreta el estatus de la seguridad de un dispositivo e intenta convencer al usuario para que compre una versión completa de dicho software para solventar infecciones inexistentes. Poco después las víctimas descubren que sus dispositivos son bloqueados hasta que pagan un rescate.

JULIO

- **Un certificado digital robado a Opera utilizado para una campaña de spyware[122]**

La noruega Opera Software ha confirmado que la pérdida de al menos un certificado digital a consecuencia de una brecha digital que ha servido para que los hackers hayan realizado una campaña de spyware contra usuarios de Windows. El malware es una de las muchas maneras de utilizar certificados legítimos para superar los sistemas de defensa tradicionales. El año pasado la táctica fue utilizada por el malware Flame, que aprovechó un certificado de actualización de Microsoft para superar las defensas de las víctimas. Y esto mismo es lo que ahora le ha ocurrido a Opera Software."Las actuales evidencias sugieren un impacto limitado", dice Opera. La compañía dice que los atacantes han sido capaces de obtener al menos un certificado que han utilizado para firmar algún malware, lo que les ha permitido distribuir software malicioso "que incorrectamente parecía haber sido publicado por Opera Software, o parecía ser el navegador Opera, explican en un post.

- **El número de aplicaciones maliciosas para smartphones se dispara más de un 600%[123]**

Los usuarios de smartphones no son inmunes a los "ciberdelincuentes" ni mucho menos, y éstos han incrementado sus ataques contra los dispositivos móviles de forma exponencial este año. Entre marzo de 2012 y marzo de 2013, la cantidad de "malware" en forma de aplicaciones maliciosas introducida de forma fraudulenta (mediante engaño,

121 http://www.computerworldmexico.mx/Articulos/29452.htm

122 http://www.itespresso.es/maquinas-windows-infectadas-gracias-opera-113273.html

123 http://newsroom.juniper.net/press-releases/juniper-networks-finds-mobile-threats-continue-ram-nyse-jnpr-1029552

sobre todo) en móviles con conexión a Internet saltó un 614%, según cálculos del fabricante de equipos Juniper Networks.

- **Framework del NIST para Seguridad en Infraestructuras Críticas[124]**

Como resultado de una directiva presidencial de febrero, que busca asegurar infraestructuras críticas de ataques externos, el NIST ha publicado un nuevo framework de trabajo con el objetivo de reducir el riesgo cibernético en estas infraestructuras. El núcleo de este marco (todavía en borrador) se compone de una matriz de funciones y una matriz que muestra el nivel de aplicación de controles. La matriz de funciones contiene las cinco funciones de seguridad cibernética de primer nivel.

- **500.000 euros, coste medio de un ciberataque para las empresas[125]**

Alrededor de 500.000 euros es el coste medio que deben afrontar las grandes empresas tras ser víctimas de un ciberataque, según recogen los datos de la Encuesta Global sobre seguridad TI corporativa – 2013 de B2B Internacional y Kaspersky Lab. Los expertos de B2B Internacional han calculado los daños derivados de los ciberataques, basándose sólo los incidentes ocurridos en los últimos 12 meses y evaluando la información de las pérdidas sufridas como resultado directo de los incidentes de seguridad. Uno de los componentes principales son los daños causados por el incidente en sí, como pérdidas derivadas de la fuga de datos críticos, continuidad de negocio y los costes asociados con la participación de especialistas para solventar el incidente; y que suponen la mayor parte de las pérdidas (alrededor de 431.000 euros). Por otro lado están los costes no planificados para prevenir ataques similares en el futuro, como el personal de contratación/formación, el hardware, el software y otros cambios de infraestructura (unos 69.000 euros) Los daños dependen de la zona geográfica en la que se ubique la empresa, los mayores se han asociado con incidentes sufridos en compañías que operan en América del Norte, con un promedio de 624.000 euros; seguidos de América del Sur, con 620.000 euros. En Europa Occidental se registró una media más baja, pero aún considerable, de las pérdidas derivadas de ciberataques, llegando a 478.000 euros.

- **Microsoft sufre ciberataques aprovechando un error de Windows[126]**

Microsoft ha informado de que piratas informáticos han atacado algunos ordenadores explotando un error de Windows que fue revelado inicialmente hace dos meses por un investigador de Google, quien fue criticado por publicar el fallo sin acudir primero a la compañía de software. Microsoft ha ofrecido pocos detalles sobre los hechos. La compañía ha dicho este martes que piratas informáticos habían lanzado "ataques selectivos", un término generalmente utilizado por expertos en seguridad para referirse a ciberataques contra blancos corporativos o gubernamentales, motivados por sabotaje o espionaje.

- **ENISA colaborará con CENELEC y CEN en material de ciberseguridad[127]**

124 http://blog.segu-info.com.ar/2013/07/framework-del-nist-para-seguridad-en.html#axzz2XyzRFFA6

125 http://www.computerworld.es/tendencias/un-fallo-grave-de-seguridad-ti-puede-costar-500000-euros-a-las-empresas

126 http://www.europapress.es/portaltic/software/noticia-microsoft-sufre-ciberataques-aprovechando-error-windows-20130710085807.html

La agencia de la Unión Europea (UE) ENISA brinda su apoyo al desarrollo de normas para productos y servicios de ciberseguridad mediante el acuerdo de colaboración firmado con dos de los principales organismos de normalización de la UE: el Comité Europeo de Normalización (CEN) y el Comité Europeo de Normalización Electrotécnica (CENELEC). Este acuerdo de cooperación tiene como objetivo contribuir de manera más eficaz a la comprensión y resolución de los problemas de Seguridad de las Redes y de la Información (SRI) relacionados con la normalización, particularmente en determinados sectores de las TIC relevantes para ENISA, y está en consonancia con las nuevas y ampliadas tareas contempladas en el recientemente aprobado Reglamento de ENISA, que otorga a la Agencia un papel más activo en el apoyo a la elaboración de normas en materia de SRI.

- **Se disparan los envíos masivos con redirecciones que llevan a páginas de spam[128]**

Los spammers usan técnicas cada vez más depuradas para aludir los filtros antispam. Una de las más populares es el empleo de redirecciones en los mensajes de correo malicioso, bien utilizando enlaces o páginas html adjuntas, según apunta Kaspersky Lab.

- **ICS-CERT advierte sobre ataques de fuerza bruta contra los Sistemas de Control de Infraestructuras Críticas[129]**

De acuerdo con el último informe del ICS-CERT, han sido reportados más de 200 incidentes de seguridad en todos los sectores de infraestructuras críticas en la primera mitad del año fiscal 2013. El 53% de estos ataques ha tenido como objetivo el sector de la energía. Como ejemplo, ICS-CERT pone de relieve un ataque realizado en febrero contra una estación de compresión de gas. Los agresores habrían intentado acceder a la red de control de procesos de la empresa con el lanzamiento de ataques de fuerza bruta. Después de recibir la notificación del ataque, ICS-CERT publicó 10 direcciones IP en el portal del US-CERT para advertir a otros gestores de activos de infraestructuras críticas. Poco después, otros gestores de infraestructuras críticas empezaron a reportar incidentes similares y se identificaron un total de 39 nuevas direcciones IP maliciosas.

- **España sube a la séptima posición del ranking de países emisores de spam[130]**

Estados Unidos sigue liderando el Dirty Dozen de Sophos, el ranking de los 12 países emisores de spam, en el que hacen su entrada Ucrania, Kazajstán y Argentina, mientras que Bielorrusia asciende a la segunda posición. España también sube dos posiciones, con el 3,4% del spam emitido.

- **Ciberataques a Bolsas de valores ponen a los mercados en riesgo[131]**

127https://www.enisa.europa.eu/media/press-releases/acuerdo-de-colaboracion-sobre-ciberseguridad-entre-enisa-y-los-organismos-europeos-de-normalizacion-cen-y-cenelec

128 http://www.csospain.es/Se-disparan-los-envios-masivos-con-redirecciones-que-llevan-/seccion-actualidad/noticia-133833

129 http://securityaffairs.co/wordpress/15820/security/ics-cert-surge-in-attacks-against-energy-industry.html

130 http://www.csospain.es/Espana-sube-a-la-septima-posicion-del-ranking-de-paises-emis/seccion-actualidad/noticia-133881

131 http://www.europapress.es/portaltic/sector/noticia-ciberataques-bolsas-valores-ponen-mercados-riesgo-20130717094216.html

Cerca de la mitad de las Bolsas de valores del mundo fueron blanco de ciberataques el año pasado, según un artículo divulgado este martes que se basa en un sondeo a 46 de ellas. La frecuencia de los ataques y la naturaleza interconectada de los mercados crea el potencial de un enorme impacto, recoge el documento del departamento de investigación de la Organización Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés) y una oficina de la Federación Mundial de Bolsas de Valores (WFE, por sus siglas en inglés).

- **Los ciberataques pasan a ser una preocupación real para las empresas[132]**

Los ciberataques, que hace apenas un par de años estaban en la cola de las preocupaciones de las multinacionales, muy por detrás de las caídas de ventas o la fiscalidad, se han colado entre las cinco principales preocupaciones de las grandes empresas de todo el planeta, según un informe elaborado por Lloyd's e Ipsos de forma conjunta con varios institutos internacionales.

- **Detenido un joven que estafó miles de euros con una falsa app para espiar conversaciones de mensajería instantánea en smartphones[133]**

Agentes de la Policía Nacional han detenido en Murcia a un joven de 23 años que presuntamente estafó miles de euros con una falsa aplicación para espiar conversaciones de mensajería instantánea en smartphones. WhatsappSPY pedía un número de teléfono con el que se obtendría un supuesto código de activación, pero en realidad lo que hacía era suscribir a su titular a un servicio de SMS Premium. La supuesta aplicación, cuya instalación y manejo se anunciaba como muy sencilla, permitiría ver las conversaciones de otros usuarios en tiempo real.

- **Interior quiere mejorar la seguridad en las escuelas en el uso de Internet[134]**

El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, pondrá en marcha próximamente el nuevo "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos" con el que pretende proteger a los jóvenes de los riesgos derivados del uso de Internet y las nuevas tecnologías, así como otras cuestiones relacionadas con el acoso escolar, las bandas juveniles o el acceso a las drogas y el alcohol, entre otras.

- **Tailandia prohíbe la venta de bitcoins al no considerarla moneda de cambio[135]**

El Banco de Tailandia ha prohibido la venta de bitcoins al no considerarla como una moneda de cambio y debido a la falta de políticas para regular y controlar esta divisa virtual. "Miembros de la Administración de Cambio de Moneda y el Departamento de Políticas recomendaron que debido a la falta de leyes aplicables, control de capital y el hecho de que las Bitcoins se extiendan en múltiples facetas financieras, sus actividades son ilegales en Tailandia", señaló en un

132 http://www.elmundo.es/elmundo/2013/07/18/navegante/1374144747.html

133 http://www.policia.es/prensa/20130720_1.html

134 http://www.europapress.es/portaltic/internet/noticia-interior-quiere-mejorar-seguridad-escuelas-uso-internet-20130723134631.html

135 http://www.elmundo.es/elmundo/2013/07/30/navegante/1375162539.html

comunicado la filial tailandesa de Bitcoin. Por lo tanto, es ilegal utilizar esta divisa virtual para la compra venda de bienes o servicios en el país asiático, así como recibir o emitir transferencias al extranjero, acotó la empresa.

- **25.000 dispositivos podrían haberse infectado por nuevos troyanos en Google Play[136]**

La compañía de antivirus rusa Doctor Web ha descubierto tres programas maliciosos en Google play que instalan troyanos Android.SmsSend en los dispositivos móviles. Por el volumen de descargas realizadas, entre 10.000 y 25.000 smartphones podrían estar afectados. La seguridad Google Play vuelve a estar en entredicho. En este caso, Doctor Web ha localizado en la tienda de aplicaciones varias apps maliciosas que instalan troyanos Android.SmsSend en los dispositivos, los cuales permitirían a los cibercriminales enviar mensajes cortos a números de tarificación adicional y agotar las cuentas de los abonados.

AGOSTO

- **Descubren un posible nuevo troyano bancario llamado KINS[137]**

Una nueva familia de malware bancario denominado KINS busca comprador en el mercado negro. Según investigadores de RSA, el troyano presenta similitudes con predecesores como Zeus, SpyEye y Citadel, aunque el autor asegura que no es una modificación de otro malware.

- **El aeropuerto de Estambul sufre un ciberataque[138]**

El aeropuerto internacional Ataturk, de Estambul, fue objeto de un ciberataque en el que se vieron afectados los sistemas de control de pasaportes en la terminal de salidas. Según la agencia de noticias local Dogan, los pasajeros estuvieron durante horas esperando debido al colapso del sistema. Las autoridades están investigando las causas y el origen del ataque en el que se utilizó código dañino para el robo de datos del usuario.

- **El robo de datos de los clientes amenaza a las empresas[139]**

Se ha dado a conocer el robo de los datos de un millón de clientes de la filial rusa de Zurich, la conocida empresa suiza de seguros. Los atracadores consiguieron el domicilio privado y laboral, y los números de teléfono móvil de los afectados. Mientras, ésta no es la primera fuga importante de datos personales en Rusia, aunque la verdadera magnitud de la catástrofe no se conoce, porque las empresas tiene derecho a no reportar este tipo de incidentes. El robo de datos de los clientes amenaza a las empresas

- **718.000 amenazas conocidas afectan a dispositivos Android[140]**

136 http://www.csospain.es/25.000-dispositivos-podrian-haberse-infectado-por-nuevos-tro/seccion-alertas/noticia-134049

137 http://www.pcworld.com.mx/Articulos/29697.htm

138 http://www.cyberwarzone.com/cyber-attack-hit-turkey-istanbul-international-airport

139 http://rusiahoy.com/sociedad/2013/08/06/las_empresas_amenazadas_por_el_robo_de_datos_de_los_clientes_30807.html

Se espera que los problemas de seguridad asociados a Android en 2013 sigan incrementándose debido a la proliferación del malware y al escaso uso de soluciones de protección. El número de aplicaciones maliciosas para Android continúa batiendo récords con un total de 718.000 amenazas en este momento. El Informe de Amenazas de Trend Micro del segundo trimestre de 2013 destaca la vulnerabilidad de Android y el aumento del malware para banca online.

- **Las centrales energéticas como objetivo[141]**

Centrales eléctricas, hidráulicas, oleoductos, gasoductos y todo tipo de infraestructuras energéticas están en el punto de mira de los hackers. Así ha quedado expuesto en las últimas ediciones de BlackHat y Def Con, las dos conferencias de ciberseguridad que han tenido lugar esta semana pasada en Las Vegas (EEUU). En estas conferencias, las empresas -e incluso gobiernos- se ponen al día de novedades en ciberseguridad y actualizan sus sistemas de defensa gracias a la colaboración de investigadores informáticos -o 'white hackers'- que dan a conocer los últimos errores y vulnerabilidades en el sector.

- **La ciberdelincuencia y el espionaje podrían costar casi medio billón de dólares[142]**

La ciberdelincuencia y el espionaje podrían estar costándole al mundo entre 70.000 y 400.000 millones de dólares en una economía global valorada en 70 billones de dólares, según la última estimación del Centro de Estudios Estratégicos Internacionales (CSIS). En el contexto de la economía de EE.UU., estos daños equivalen a eliminar 500.000 puestos de trabajo, pero en realidad el estudio "El impacto económico de la ciberdelincuencia y el ciberespionaje", patrocinado por McAfee, admite que incluso estos números podrían ser peores al estar afectados por una serie de imponderables.

- **Rusia aprueba un documento de ciberseguridad[143]**

El presidente Vladímir Putin ha firmado un documento que marca las directrices en el ámbito de la ciberseguridad, tal y como recoge el diario Kommersant. El documento tiene el título de "*Principios de la política gubernamental de la Federación Rusa en el ámbito de la seguridad informática internacional hasta el 2020*" y ha sido elaborado por el Consejo de Seguridad con la participación de los ministerios de Asuntos Exteriores, Defensa, Comunicaciones y Justicia. En el documento se reúnen por primera vez las iniciativas clave de Rusia en el ámbito de la ciberseguridad, lo que para sus promotores debería ayudar a promocionarlas en el mundo y a mejorar la colaboración entre departamentos dentro del país.

- **El Departamento de Energía de Estados Unidos hackeado[144]**

140http://www.europapress.es/portaltic/software/seguridad-00646/noticia-718000-amenazas-conocidas-afectan-dispositivos-android-20130807144510.html

141 http://www.elmundo.es/elmundo/2013/08/09/navegante/1376065876.html

142 http://www.ciospain.es/seguridad/la-ciberdelincuencia-y-el-espionaje-podrian-costar-casi-medio-billon-de-dolares

143 http://rusiahoy.com/politica/2013/08/12/rusia_define_las_prioridades_de_su_politica_de_seguridad_informatica_31013.html

Los atacantes han accedido a ordenadores del Departamento de Energía de los Estados Unidos (DoE) y han obtenido información personal de 14.000 empleados. En una breve declaración, la DoE ha confirmado la violación que ocurrió a finales del mes de julio, aunque manifiesta que ningún dato secreto se ha puesto en peligro. Este es el segundo mayor ataque sufrido por este Departamento en lo que va de año, siendo el principal el ocurrido en febrero de este 2013, cuando los atacantes penetraron en 14 servidores y 20 estaciones de trabajo en la oficina central de la DoE.

- **Nuevo informe de ENISA con los principales incidentes de 2012[145]**

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) publicó un nuevo informe con una visión general de los incidentes graves de interrupción ocurridos en la UE en 2012. Este informe global muestra que en el 40% de los 79 incidentes registrados no era posible marcar el número de emergencia «112». La telefonía móvil e Internet móvil fueron los servicios más afectados, con cortes de comunicación para millones de usuarios.

- **Las claves de 15.000 cuentas de twitter al descubierto[146]**

La intención era hacerse con la base de datos completa. De momento, ha conseguido hacerse con más de 15.000 del total de más de 500 millones de usuarios registrados con que cuenta Twitter. El autor de este ataque es un hacker de origen mauritano que ha publicado un archivo con la información robada. El servicio radicado en San Francisco no ha dado una respuesta oficial, tan solo que está trabajando en ello. Se ha limitado a enviar una mensaje a los usuarios con cuenta verificada, algo que solo tienen los que cuentan con un número elevado de seguidores o representan productos e instituciones, es decir, sus VIP, para que incluyan un sistema de doble verificación que hace más segura la contraseña.

- **Revelado el Plan Nacional Australiano contra la ciberdelincuencia[147]**

El Plan Nacional de Lucha contra la ciberdelincuencia obliga al Gobierno australiano a adoptar medidas concretas basadas en seis prioridades: educar a la comunidad para protegerse; asociación con la industria para hacer frente al problema común de los delitos informáticos; fomentar un enfoque basado en el intercambio de información para favorecer una mejor formación; mejora de la capacidad de los organismos para hacer frente a los delitos informáticos; fortalecer el compromiso internacional y asegurar un marco jurídico penal parejo a los continuos cambios tecnológicos.

- **La ciberdelincuencia y el espionaje podrían costar casi medio billón de dólares[148]**

144 http://www.securityweek.com/department-energy-hacked-pii-stolen

145http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012/at_download/fullReport

146 http://tecnologia.elpais.com/tecnologia/2013/08/20/actualidad/1377011520_379395.html

147 http://www.psnews.com.au/Page_psn375f4.html

148 http://www.computerworld.es/negocio/la-ciberdelincuencia-y-el-espionaje-podrian-costar-casi-medio-billon-de-dolares

En el contexto de la economía de EE.UU., estos daños equivalen a eliminar 500.000 puestos de trabajo, pero en realidad el estudio "El impacto económico de la ciberdelincuencia y el ciberespionaje", patrocinado por McAfee, admite que incluso estos números podrían ser peores al estar afectados por una serie de imponderables.

- **España, el país de Europa que recibe más ciberataques dirigidos a gamers**[149]

Kaspersky Lab ha publicado las cifras actuales de las infecciones de juegos online. En ellas se reflejan que existen 4,4 millones de programas maliciosos destinados a los gamers, cifra que ha aumentado considerablemente desde 2012, año en el que se situaba en 3,3 millones. El objetivo principal de este "código dañino" es robar los datos de la cuenta del jugador, así como sus objetos virtuales. Por ello, es fundamental que los gamers tengan en cuenta unas reglas básicas de seguridad que les mantengan protegidos.

- **Detectan dos nuevos programas dañinos para Android**[150]

La marca de antivirus Kaspersky advierte del auge de dos programas maliciosos para teléfonos Android muy peligroso, Backdoor.AndroidOS.Obad.a y Free Calls Update, capaces de apropiarse del teléfono y estafar al usuario.

- **Las empresas españolas no protegen su información como deberían**[151]

Según el Índice de Madurez del Riesgo de la Información 2013, realizado por PwC e Iron Mountain, las empresas europeas están desbordadas por la cantidad de información que crece por todas partes. Esto hace que éstas se expongan a "unos niveles del riesgo sin precedentes", destaca Juan José Mínguez, socio de riesgos tecnológicos de PwC.

- **El Ejército Electrónico Sirio hackea el dominio de Twitter.com**[152]

El Ejército Electrónico Sirio (SEA por sus siglas en inglés) se ha hecho con el dominio de la administración de twitter.com, de nytimes.com y del Huffington Post de Reino Unido, según han informado a través de un "tuit" desde su página de Twitter oficial @Official_SEA16.

- **Los servicios de asistencia son un punto débil de la seguridad TI**[153]

RSA ha publicado los resultados de una encuesta realizada por el Instituto SANS entre más de 900 profesionales encargados de ofrecer servicios de asistencia, de la que se desprende la falta de controles de seguridad de este tipo de servicios.

149 http://www.internautas.org/html/7736.html

150 http://www.abc.es/tecnologia/informatica-software/20130826/abci-programas-maliciosos-android-201308261629.html

151 http://www.csospain.es/Las-empresas-espanolas-no-protegen-su-informacion-como-deber/seccion-pol%C3%ADticas/articulo-207909

152 http://www.europapress.es/portaltic/internet/noticia-ejercito-electronico-sirio-hackea-dominio-twittercom-20130828105102.html

153 http://www.csospain.es/Los-servicios-de-asistencia-son-un-punto-debil-de-la-segurid/seccion-actualidad/noticia-134061

SEPTIEMBRE

- **El FBI confirma que Android es el principal objetivo del código dañino[154]**

Android, el sistema operativo dominante en el mercado móvil, es el principal blanco de ataques de software nocivo, debido a que muchos usuarios aún utilizan versiones antiguas del software, según un estudio del Departamento de Seguridad Nacional y el FBI.

- **El 28,4% de los españoles fueron atacados por amenazas online en el segundo trimestre de 2013[155]**

La cifra total de ataques de código dañino online en España durante el segundo trimestre del año es de 5.172.233. El 28,4 por ciento de los usuarios fueron atacados por amenazas online en este periodo. Estos datos sitúan a España en el puesto 43 del mundo en ataques online. Los ataques a través de navegadores son el método principal para la propagación de código dañino, sobre todo a través de la explotación de vulnerabilidades en navegadores y sus plug-ins o mediante ingeniería social.

- **El código dañino para móviles creció un 30% en el primer semestre[156]**

Fortinet ha dado a conocer los resultados de una investigación realizada por su equipo de detección de ciberamenazas FortiGuard entre el 1 de enero y el 31 de julio de 2013, de la que se desprende que, lejos de disminuir, el código dañino para móvil está en pleno apogeo. Concretamente, el código dañino en dispositivos móviles ha crecido un 30% en los últimos seis meses, un período en el que el equipo ha identificado más de 1.300 muestras cada día y realizó el seguimiento de más de 300 familias de código dañino específicas para Android, detectando unas 250.000 muestras de código dañino solo para Android.

- **Los conflictos en Siria y Egipto provocan un aumento de los ciberataques[157]**

La guerra civil en Siria y las pugnas políticas en Egipto han abierto nuevos campos de batalla en Internet y han provocado un alza de los ciberataques en Oriente Próximo, según informó McAfee. Más de la mitad de los incidentes en el Golfo Pérsico este año fueron los llamados ataques del "hacktivismo" -que representan solo una cuarta parte del cibercrimen mundial- con programadores políticamente motivados que sabotean grupos opositores o instituciones, dijeron este martes ejecutivos de McAfee, la división de software de seguridad de Intel.

- **El cibercrimen le cuesta al mundo 300,000 millones de dólares[158]**

154 http://www.abc.es/tecnologia/informatica-software/20130830/abci-android-malware-201308301659.html

155 http://www.kaspersky.es/about/news/virus/2013/El_284_de_los_espanoles_fueron_atacados_por_amenazas_online_en_el_segundo_trimestre_de_2013

156 http://www.ciospain.es/seguridad/el-malware-para-moviles-crecio-un-30-en-el-primer-semestre

157http://www.europapress.es/portaltic/software/seguridad-00646/noticia-conflictos-siria-egipto-provocan-aumento-ciberataques-20130904155433.html

El cibercrimen provoca pérdidas mundiales de hasta 300,000 millones de dólares, por encima de la piratería y el tráfico de drogas, según el estudio "Impacto Económico de la Ciberdelincuencia y el Ciberespionaje", publicado por el Centro de Estrategia y Estudios Internacionales de Estados Unidos (CSIS) y McAfee. La NSA puede fisgonear el 75 por ciento del tráfico de Internet de Estados Unidos

- **Facebook tiene 18 millones de usuarios en España y el 72% entra con el móvil[159]**

Un total de 18 millones de españoles accede cada mes a la red social Facebook, un 72,2% de los cuales (13 millones) lo hace desde su teléfono móvil. La compañía fundada por Mark Zuckerberg ha anunciado, en un comunicado, que ya cuenta con 1.155 millones de usuarios activos al mes en todo el mundo, de los que el 61% entra a la red social a diario. En el caso de España, cada día 12 millones de internautas acceden a Facebook, 8,1 millones de ellos desde su teléfono móvil.

- **Un nuevo troyano para Android afecta a usuarios de banca electrónica en Europa y Turquía[160]**

El laboratorio de investigación y análisis de código dañino de la sede central de ESET, en Bratislava, ha descubierto un nuevo y peligroso troyano bancario, detectado como Hesperbot, que afecta a usuarios de banca electrónica en Europa y Asia, y que utiliza campañas de propagación bien diseñadas y creíbles relacionadas con entidades de confianza con las que consigue engañar a los usuarios para que ejecuten el código dañino.

- **La Policía Nacional y Google acuerdan impulsar la seguridad de los menores en Internet[161]**

La Policía Nacional y Google han acordado colaborar para impulsar la seguridad de los menores en Internet, a través de distintas acciones. De esta forma, la Policía Nacional se convierte en uno de los partners de Google ofreciendo asesoramiento sobre seguridad y elaboración de consejos para la protección de los menores en el uso de la tecnología. La Policía española y la compañía tecnológica pretenden con esta alianza seguir trabajando por una Red más segura y formar a los internautas con consejos y buenas prácticas en ese ámbito.

- **El Centro Criptológico Nacional, CCN, gestionó 6.250 ciberincidentes en los dos últimos años[162]**

El Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI), creado en el año 2002 con el fin de garantizar la seguridad TIC

158 http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

159 http://www.elmundo.es/elmundo/2013/09/06/navegante/1378465402.html

160 http://blogs.protegerse.com/laboratorio/2013/09/09/hesperbot-analisis-tecnico-1-de-2/

161 http://www.interior.gob.es/press/la-policia-nacional-y-google-acuerdan-impulsar-la-seguridad-de-los-menores-en-internet-15678

162 https://www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-Informe-de-actividades-2011-2012.pdf

en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada acaba de hacer pública su memoria de actividades 2011-2012.

- **Descubren un nuevo Backdoor que intercepta las pulsaciones del teclado[163]**

La compañía Doctor Web advierte a clientes de la existencia del programa maligno BackDoor.Saker.1 que es capaz de pasar por el Control de Cuentas de Usuario (UAC) e interceptar las pulsaciones del teclado (keylogger).

- **El 70% de las empresas creen que el riesgo de sufrir un ataque DDoS es moderado[164]**

Pese a que el volumen de ataques de denegación de servicio distribuido (DDoS) no para de crecer, las empresas no invierten en soluciones de seguridad dirigidas a prevenirlos y mitigarlos. No en vano, el 70% de las empresas europeas consideran que el riesgo de sufrir un ataque DDoS en sus sistemas es moderado, como revela una encuesta conducida por Grupo Exclusive Networks en colaboración con Arbor Networks.

- **Descubierto el primer troyano móvil difundido a través de redes botnet ajenas[165]**

Por primera vez en la historia de la delincuencia informática móvil, un troyano se está extendiendo mediante botnets controladas por otros grupos delictivos. Obad.a se encuentra sobre todo en los países de la Comunidad de Estados Independientes (CEI). En total, el 83 % de los intentos de infección se registraron en Rusia, mientras que también se ha detectado en los dispositivos móviles en Ucrania, Bielorrusia, Uzbekistán y Kazajstán.

- **El Gobierno aprueba la Ley de Telecomunicaciones que agiliza despliegue redes[166]**

El Consejo de Ministros aprobó el pasado viernes el proyecto de Ley General de Telecomunicaciones que, entre otras cosas, persigue simplificar el despliegue de nuevas infraestructuras de telecomunicaciones mediante la eliminación de la necesidad de obtener diversas licencias municipales.

- **Detienen en Londres a ocho ciberdelincuentes por un robo a Barclays[167]**

Ocho hombres han sido detenidos por el presunto robo de 1,3 millones de libras (1,54 millones de euros) al tomar el control del sistema informático de Barclays. El hecho se produce en un momento en que el llamado "cibercrimen" es cada vez más usual, según la policía británica.

- **Sitios web de compañías del sector energético comprometidos por ataques tipo watering hole[168]**

163 http://www.csospain.es/Descubren-un-nuevo-Backdoor-que-intercepta-las-pulsaciones-d/seccion-alertas/noticia-134335

164 http://www.csospain.es/El-70-por-ciento-de-las-empresas-creen-que-el-riesgo-de-sufr/seccion-actualidad/noticia-134370

165 http://www.cioal.com/2013/09/17/kaspersky-lab-descubre-el-primer-troyano-movil-difundido-a-traves-de-redes-botnet-ajenas/

166 http://www.lamoncloa.gob.es/docs/refc/pdf/refc20130913e_3.pdf

167 http://es.reuters.com/article/topNews/idESMAE98J01920130920

168 http://www.net-security.org/secworld.php?id=15618

Los sitios de una docena de compañías del sector energético han sido comprometidos para utilizarlos en ataques denominados "watering holes" (abrevaderos) que descargan código dañino o redirigen a los usuarios que visitan el sitio comprometido a otros sitios que también descargan software malicioso.

- **Se crea la Dirección TIC de la AGE[169]**

El 24 de septiembre se publicó en el BOE el Real Decreto 695/2013, de 20 de septiembre, de modificación del Real Decreto 199/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia y se modifica el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales. Así, el RD introduce como competencia del departamento "la coordinación del proceso de racionalización de las tecnologías de la información y de las comunicaciones (TIC) en la Administración General del Estado", creando la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, con rango de Subsecretaría, que dependerá funcionalmente de los Ministros de la Presidencia y de Hacienda y Administraciones Públicas.

- **Las redes sociales, un gran problema de seguridad para las empresas[170]**

El último estudio presentado por IBM sobre seguridad afirma que las redes sociales serán dentro de un tiempo, una de las principales herramientas que los hackers explotarán para hacer peligrar la seguridad de las empresas.

- **Icefog: una nueva campaña de ciberespionaje[171]**

El equipo de investigación en seguridad de Kaspersky Lab ha publicado un nuevo trabajo de investigación sobre el descubrimiento de "Icefog", un pequeño pero energético grupo de APT (amenazas persistentes y avanzadas, por sus siglas en inglés) que se centra en blancos en Corea del Sur y Japón, atacando a las cadenas de suministro de empresas occidentales. La operación se inició en 2011 y ha crecido en tamaño y alcance en los últimos años.

- **El Mando de Ciberdefensa adquirirá mañana la capacidad operativa inicial[172]**

El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) adquirirá mañana su capacidad operativa inicial tal y como estaba previsto, según ha confirmado hoy su máximo responsable, el general Carlos Medina.

- **Detenidos dos informáticos por comprometer la seguridad de 1.500 empresas[173]**

169 http://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-9885#analisis

170 http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03036usen/WGL03036USEN.PDF

171 http://www.pcworld.com.mx/Articulos/30290.htm

172http://noticias.terra.es/sucesos/el-mando-de-ciberdefensa-adquirira-manana-la-capacidad-operativa-inicial,a5fe347385751410VgnCLD2000000ec6eb0aRCRD.html

Agentes de Policía Nacional, en la segunda fase de la operación "Ransomware", han desarticulado la rama económica responsable del "virus de la Policía" y que había comprometido la seguridad de 1.500 empresas en España. Han sido detenidos en Madrid los líderes de esta rama, dos expertos informáticos ucranianos que vendían el acceso a los servidores de más de 21.000 empresas de 80 países, más de 1.500 de ellas en España.

- **La Agencia Tributaria advierte de un intento de fraude tipo phishing a través de Internet[174]**

La Agencia Tributaria ha detectado un envío de comunicaciones por correo electrónico en el que, suplantando su identidad e imagen, se indica: "Después del último cálculo sobre las actividades fiscales hemos decidido que le corresponde un reembolso del impuesto en valor de 384,56 euros. Para recibir dicho reembolso, completar y mandar el formulario del impuesto a devolver".

OCTUBRE

- **Reino Unido se prepara para la guerra cibernética[175]**

El Gobierno de Reino Unido tiene la intención de contratar a cientos de especialistas en informática para defender su infraestructura central contra las ciberamenazas, según manifestó ayer el secretario de Defensa, Philip Hammond. Este reveló que Reino Unido está dedicando recursos y fondos adicionales para la construcción de un sólido servicio de Inteligencia cibernética y redes de vigilancia, informa Reuters.

- **El 70% de los PC Windows corporativos están expuestos a la vulnerabilidad de IE[176]**

La vulnerabilidad de día cero encontrada en Internet Explorer ya está siendo utilizada por los criminales cibernéticos para atacar a usuarios de IE8 e IE9 que ejecutan sistemas operativos Windows 7 y XP, aunque podría afectar a todas las versiones del navegador, según Websense.

- **Roban datos de 2,9 millones de clientes de Adobe[177]**

Adobe Systems acaba de sufrir un ataque informático. Y es que hackers han logrado entrar en su red y robar información de 2,9 millones de clientes de Adobe además del código fuente de varios de sus productos, entre los que se encuentran Adobe Acrobat, ColdFusion y ColdFusion Builder.

173http://www.interior.gob.es/press/desarticulada-la-rama-economica-responsable-del-virus-de-la-policia-y-que-habia-comprometido-la-seguridad-de-1-500-empresas-en-espana-15771

174 http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/MinisterioHaciendayAdministracionesPublicas/2013/260913Phinsing.htm?gfe=1

175 http://www.itespresso.es/reino-unido-se-prepara-guerra-cibernetica-116253.html

176 http://www.csospain.es/El-70-por-ciento-de-los-PC-Windows-corporativos-estan-expues/seccion-alertas/noticia-134578

177 http://www.idg.es/pcworld/Roban-datos-de-2_9-millones-de-clientes-de-Adobe/doc134604.htm

- **Ya hay un millón de tipos de código dañino para dispositivos móviles[178]**

Trend Micro acaba de presentar su informe de seguridad correspondiente al segundo trimestre de 2013, donde se recoge que actualmente ya hay un millón de tipos de código dañino para móviles (incluidas las modalidades que abusan de los servicios premium) y de aplicaciones de alto riesgo (aplicaciones que obligan a anuncios publicitarios a enlazar con sites dudosos).

- **Baja el spam, pero el volumen de phishing se multiplica por diez[179]**

El aumento de los ataques dirigidos y sofisticados ha propiciado una disminución del spam, aunque ha aumentado su peligrosidad, con la vuelta al cole como gancho. Los ataques de phishing se dispararon, siendo los usuarios de los sitios de redes sociales el blanco más codiciado.

- **Detenido en Rusia el presunto autor del Blackhole Exploit-Kit[180]**

De entre todas las familias de código dañino más activas en los últimos meses, el kit de exploits Blackhole tiene un lugar destacado. Prueba de ello son las continuas variantes que afectan a nuevos sistemas y se aprovechan de nuevas vulnerabilidades. Ahora, y según ha confirmado Europol recientemente, el ciberdelincuente conocido como Paunch y presunto responsable de esta herramienta para el cibercrimen habría sido detenido en Rusia. Esto confirma las teorías de varios investigadores que apuntaban a que su creador era de esta región debido a la forma en la que se encontraba escrito el código dañino.

- **Ataques de phishing inteligente podrían inutilizar la red eléctrica[181]**

En lugar de preocuparse por exóticas armas cibernéticas, como Stuxnet o su hermano mayor, Flame, las empresas que disponen de los sistemas SCADA, de control y adquisición de datos para monitorizar y controlar los procesos industriales, deberían asegurarse de que sus programas de lucha contra la suplantación de identidad están en orden, aseguran los expertos en seguridad.

- **El tráfico Cloud crecerá un 35 por ciento anual entre 2012 y 2017[182]**

La circulación de datos en el la nube global es cada día mayor. El tráfico de los data centers de más rápido crecimiento se multiplicará por 4,5 entre 2012 y 2017, llegando al total de 5,3 Zettabytes anuales desde los 1,2 Zettabytes registrados en 2012, lo que supone una tasa de crecimiento interanual del 35 por ciento.

- **La ciberdelincuencia pone en peligro la moneda virtual Bitcoin[183]**

178 http://www.channelbiz.es/2013/10/04/ya-hay-millon-malware-moviles/

179 http://www.csospain.es/Baja-el-spam,-pero-el-volumen-de-phishing-se-multiplica-por-/seccion-actualidad/noticia-134641

180 http://blogs.protegerse.com/laboratorio/2013/10/09/detenido-en-rusia-el-presunto-autor-del-blackhole-exploit-kit/

181 http://www.pcworld.es/seguridad/ataques-de-phishing-inteligente-podrian-inutilizar-la-red-electrica-advierten-los-expertos

182 http://www.cisco.com/web/ES/about/press/2013/2013-10-15-trafico-cloud-crecera-un-35-por-ciento-anual.html

183 http://www.csospain.es/La-ciberdelincuencia-pone-en-peligro-la-moneda-vir/seccion-actualidad/noticia-134735

En un reciente informe, McAfee expresa sus reservas acerca de que Bitcoin se convierta algún día en la moneda virtual oficial del comercio electrónico. El idealismo y la comodidad que existe detrás de monedas virtuales como Bitcoin está en riesgo, debido a que el abuso por parte de criminales profesionales y grupos de delincuencia virtual organizada está alcanzando a niveles inaceptables en términos de seguridad, señala el estudio.

- **La Eurocámara aprueba reforzar las normas sobre protección de datos[184]**

La comisión de Libertades Civiles de la Eurocámara ha aprobado (por una amplia mayoría de 49 votos a favor, 3 en contra y 1 abstención) reforzar las normas de la UE sobre protección de datos personales.

- **Bug crítico en la aplicación de eBay para Windows 8[185]**

Se ha detectado un fallo de seguridad crítico en la aplicación de eBay para Modern UI de Windows 8. Ya se encuentra disponible una actualización para esta aplicación que, según podemos leer en la Windows Store, debemos asegurarnos de instalar ya que corrige varios fallos graves del cliente de compras online.

- **Los ataques DDoS crecen en número y en tamaño[186]**

En lo que va de año, más de la mitad de los ataques distribuidos de denegación de servicio (DDoS) acontecidos superan el 1Gb/seg, y aquellos superiores a 20Gb/sg han crecido en más de un 350%, según revela un estudio de Arbor Networks.

- **Casi el 70% de los hogares tiene acceso a internet[187]**

Así lo muestra la Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los hogares que hizo pública el Instituto Nacional de Estadística (INE).

- **Los empleados más jóvenes, los más rebeldes con las normas de seguridad de la empresa[188]**

La encuesta, realizada por Fortinet, se ha realizado entre 3.200 individuos, entre edades de 21 y 32 años, y en 20 países distintos, tanto universitarios como empleados a tiempo completo, que son dueños de su propio smartphone, tablet y/ o portátil.

NOVIEMBRE

- **Los PC con Windows XP están seis veces más expuestos al código dañino[189]**

184http://www.europapress.es/portaltic/software/seguridad-00646/noticia-eurocamara-aprueba-reforzar-normas-proteccion-datos-20131021203154.html

185 http://www.softzone.es/2013/10/24/bug-critico-en-la-aplicacion-de-ebay-para-windows-8/

186 http://www.csospain.es/Los-ataques-DDoS-crecen-en-numero-y-en-tamano/seccion-actualidad/noticia-134767

187 http://www.ine.es/prensa/np803.pdf

188 http://www.computerworld.es/tendencias/los-empleados-mas-jovenes-los-mas-rebeldes-con-las-normas-de-seguridad-de-la-empresa

En su afán por animar a la todavía extensa base de usuarios de XP a migrar a la última versión de Windows, Microsoft ha publicado su último informe de inteligencia de seguridad, que refleja la actividad monitorizada por sus herramientas de seguridad de enero a junio, el cual revela que los ordenadores con Windows XP tienen seis veces más probabilidades de infectarse con código dañino que aquellos con las nuevas versiones del sistema operativo.

- **ENISA recomienda el uso de la criptografía para salvaguardar datos personales[190]**

ENISA, la Agencia de "ciberseguridad" de la Unión Europea, ha publicado un informe recomendando que todas las autoridades deberían fomentar más el uso de la criptografía como medida para salvaguardar datos personales. El informe menciona las formas de protección de datos personales y/o confidenciales que han sido adquiridos de manera legítima. Existe un claro vínculo entre la privacidad y la criptografía que demuestra cómo esta última puede jugar un papel fundamental en la protección de datos personales y salvaguardar los datos confidenciales recopilados de forma legítima.

- **El CCN-CERT publica un informe sobre BYOD[191]**

El CCN-CERT, del Centro Criptológico Nacional (CCN), ha hecho público su Informe de Amenazas, IA-21/13 de Riesgos y Amenazas del Bring Your Own Device (BYOD), en el que se adentra en este fenómeno que define la posibilidad de que los empleados de una organización usen los dispositivos de los que son propietarios para desarrollar sus funciones profesionales, accediendo al entorno, servicios y datos corporativos.

- **El 80% de los españoles no comprueba la autenticidad de las web antes de introducir datos personales[192]**

El 80% de los españoles introducen datos confidenciales, incluyendo datos financieros, en páginas web sin comprobar antes si son auténticas. Así revela un estudio de Kaspersky Lab, del que se desprende que los españoles somos los más descuidados de Europa, casi el triple que la media del continente (28%). El país en el que los usuarios son más precavidos es Francia, en el que solo un 9% no se aseguran de la seguridad de las webs antes de introducir información personal.

- **El robo de datos a Adobe podría haber afectado a más de 150 millones de cuentas[193]**

189 http://www.microsoft.com/es-xl/news/Informesobreseguridadcibernetica.aspx

190http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data/at_download/fullReport

191 https://www.ccn-cert.cni.es/index.php?option=com_docman&task=cat_view&gid=147&Itemid=147&lang=es

192 http://www.csospain.es/El-80-por-ciento-de-los-espanoles-no-comprueba-la-autenticid/seccion-actualidad/noticia-134815

193 http://www.reuters.com/article/2013/11/07/us-adobe-cyberattack-idUSBRE9A61D220131107

Tal y como publica Reuters, Adobe ha confirmado que LastPass ha encontrado registros robados de su centro de datos. Eso sí, restó importancia a este hecho. Y es que, Heather Edell, portavoz de Adobe, ha destacado que no es correcto decir que 152 millones de cuentas han sido expuestas, ya que la base de datos atacada era un sistema de copia de seguridad que estaba a punto de ser dada de baja.

- **Más de la mitad de las empresas españolas sufrieron ataques de código dañino y spam[194]**

Lejos de disminuir, las amenazas que se ciernen sobre la seguridad corporativa van en aumento. Así lo indica la última encuesta llevada a cabo por B2B International para Kaspersky Lab, de la que se desprende que los ataques que utilizan programas dañinos, phishing y spam siguen siendo los más frecuentes en las empresas, incluidas las españolas.

- **Facebook ya no permite controlar quién nos puede buscar en la red social[195]**

Facebook ha anunciado que va a eliminar una de sus funciones más antiguas, la denominada "¿Quién puede buscar tu biografía por tu nombre? Esta opción de la configuración controlaba quién podía buscar la biografía de un usuario escribiendo su nombre en el campo de búsqueda. Una vez que se elimine, cualquiera podrá buscar a cualquiera por su nombre.

- **Se dispara el phishing contra Apple iOS[196]**

En su último informe de seguridad trimestral, Trend Micro muestra su preocupación por la incesante proliferación de sitios de phishing para Apple iOS, así como por el repunte considerable en malware bancario. Concretamente, el volumen de sitios de phishing relacionados con Apple ha mantenido un crecimiento constante a lo largo del tercer trimestre, con 4.100 detectados en junio, 1.900 en agosto y 2.500 en septiembre, y para finales de año se espera que aumenten aún más, ya que los analistas estiman que Apple venderá 31 millones de iPhones y 15 millones de iPads en el cuarto trimestre.

- **Una falsa casa de cambio china de bitcoins estafa más de 3,5 millones[197]**

Una casa de cambio de bitcoins china ha desaparecido recientemente y de la noche a la mañana, lo que ha causado que las cuentas de sus usuarios hayan desaparecido y, con ellas, inversiones por valor de hasta 3,5 millones de euros.

- **El Gobierno reformará la ley para proteger a los menores en internet[198]**

194 http://www.csospain.es/Mas-de-la-mitad-de-las-empresas-espanolas-sufrieron-ataques-/seccion-actualidad/noticia-134839

195 http://www.trecebits.com/2013/11/05/facebook-ya-no-permite-controlar-quien-nos-puede-buscar-en-la-red-social/

196http://www.csospain.es/Se-dispara-el-phishing-contra-Apple-iOS/seccion-actualidad/noticia-134854

197 http://www.elmundo.es/tecnologia/2013/11/13/5283376b0ab740633f8b456c.html

El Gobierno trabaja en una reforma del Código Penal para incluir nuevos tipos de delitos vinculados con los menores en la red, en especial los relacionados con la pornografía infantil. De esta forma se tipificará el visionado de estos contenidos en streaming o el contacto virtual con un menor para la obtención de material pornográfico. Pero la modificación legislativa también contemplará de manera más completa nuevos fenómenos como el ciberacoso o la usurpación de la personalidad en las redes.

- **Enisa reclama una mejora de la interoperabilidad y el intercambio de datos entre equipos de respuesta a emergencias informáticas[199]**

La agencia europea ENISA publica su nuevo informe "Detecta, COMPARTE, Protege: Cómo mejorar el intercambio de datos entre CERT", en el que se estudia cómo facilitar y mejorar el intercambio de datos entre "bomberos digitales" (es decir, entre equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés). La Agencia llega a la conclusión de que mejorar el intercambio de información optimizará las soluciones y los esfuerzos de normalización ya existentes en materia de formatos de intercambio de datos, haciéndolos más inter-operativos.

- **La Fiscalía presentó su memoria anual con un apartado dedicado al estado de la criminalidad informática[200]**

La Memoria Anual de la Fiscalía General del Estado fue presentada el pasado 19 de noviembre por el Fiscal General del Estado, Eduardo Torres-Dulce en el Congreso de los Diputados. En dicho documento se le dedica un apartado al estado de la criminalidad informática. El concepto de criminalidad informática abarca no sólo aquellos comportamientos ilícitos cuyo objeto son los datos o sistemas informáticos sino también otras muchas conductas, tipificadas en una diversidad de preceptos del Código Penal, en cuya planificación y desarrollo la utilización de las TIC constituye un factor esencial.

- **Nuevo Real Decreto sobre DNI y sus certificados de firma electrónica[201]**

El 23 de noviembre se publicó en el BOE el Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica. El Real Decreto de 2005 permite a los españoles mayores de edad y que gocen de plena capacidad de obrar acreditar electrónicamente la identidad y demás datos personales del titular que en él

198 http://www.diariodenavarra.es/noticias/mas_actualidad/nacional/2013/11/19/el_gobierno_reformara_ley_para_proteger_los_menores_internet_137423_1031.html

199https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport

200 http://www.fiscal.es/cs/Satellite?c=Page&cid=1242052134611&language=es&pagename=PFiscal/Page/FGE_memorias&selAnio=2013

201 http://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-12320

consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

- **El 30% de los PC en España recibió un ataque de código dañino en Internet[202]**

Kaspersky Lab ha presentado su informe sobre la evolución de las amenazas informáticas en el tercer trimestre de 2013, según el cual en ese periodo detectó y neutralizó 978.628.817 objetos maliciosos. El 45,2 por ciento de los ataques bloqueados se lanzaron desde recursos web ubicados en EE.UU. y Rusia. Si nos centramos en España, los ataques a través de navegadores son la principal vía para la propagación de programas maliciosos. Así, la explotación de vulnerabilidades en los navegadores y sus plugins y la ingeniería social representan las vulnerabilidades más utilizadas para atacar PC en nuestro país.

- **Informe ENISA sobre el uso del roaming nacional para atenuar las interrupciones de servicio de la red de telefonía móvil[203]**

ENISA, la agencia de ciberseguridad de la UE, ha publicado un nuevo informe acerca del uso de roaming a nivel nacional para atenuar las interrupciones importantes de servicio en la red de telefonía móvil. Este informe tiene por finalidad presentar a los reguladores de telecomunicaciones nacionales una variedad de posibles opciones, así como los pros y los contras de los diferentes programas nacionales de roaming desde el punto de vista de la seguridad y la resistencia.

DICIEMBRE

- **Bitcoin, el nuevo objetivo de los ciberdelincuentes[204]**

El Bitcoin es una nueva unidad monetaria, que comenzó a funcionar en el año 2009 y que ha pasado de valer únicamente unos céntimos de dólar hasta alcanzar valores de hasta 1.000 dólares por unidad. Esta moneda ha sido utilizada desde sus inicios en el mercado negro ya que no está controlada por ninguna entidad ni ningún gobierno, lo que da a los traficantes libre compra-venta de mercancía sin peligro de ser registrados ni perseguidos.

- **La privacidad y el cifrado, en alza en 2014[205]**

El recopilatorio de las principales noticias de seguridad tecnológica de 2013 ha servido a Kaspersky Lab para presentar también un informe de lo que serán, para ellos, las principales tendencias de este ámbito durante el próximo año. Algunos de los incidentes en seguridad TI de 2013 tuvieron mucha repercusión y plantearon nuevos interrogantes

202 http://www.csospain.es/El-30-por-ciento-de-los-PC-en-Espana-recibio-un-ataque-de-ma/seccion-actualidad/noticia-134913

203 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience

204 http://www.softzone.es/2013/11/28/bitcoin-el-nuevo-objetivo-de-los-ciberdelincuentes/

205 http://www.ciospain.es/seguridad/la-privacidad-y-el-cifrado-en-alza-en-2014

sobre la forma en la que hoy en día usamos Internet y el tipo de riesgos a los que nos enfrentamos. Continuaron las campañas de ataques avanzados a gran escala, Octubre Rojo o NetTraveler pero se han adoptado nuevas técnicas, como los watering hole y los ataques tipo zero-day. Además, se han hecho fuertes los cibermercenarios, especializados en grupos APT "en alquiler" dedicados a fugaces.

- **Vulnerabilidad en Android 4.3 permite eliminar el bloqueo de seguridad[206]**

El equipo de investigación alemán Curesec Research Team ha descubierto una vulnerabilidad en Android 4.3 que permite quitar los bloqueos de seguridad de los terminales. En el mes de septiembre, Google introdujo en el Android Device Manager una nueva característica que permite bloquear de forma remota el dispositivo mediante contraseña. Una función que se unió a la localización del dispositivo y de interés en caso de pérdida o robo del terminal para proteger la información personal.

- **El Gobierno aprueba la Estrategia de Ciberseguridad Nacional[207]**

El Consejo de Seguridad Nacional, reunido el pasado cinco de diciembre en el Palacio de la Moncloa presidido por el jefe del Gobierno, Mariano Rajoy, aprobó la Estrategia de Ciberseguridad, que persigue responder a las amenazas o agresiones que puedan afectar en el ciberespacio a la seguridad nacional.

- **Amenazas móviles y ataques dirigidos sacudirán 2014[208]**

La empresa de seguridad Trend Micro acaba de presentar su informe de predicciones de seguridad para 2014, "Difuminando los límites: pronósticos de seguridad para 2014 de Trend Micro", en el que prevé que se produzca una gran brecha de datos cada mes durante todo el año, y que aceleren tanto los ataques avanzados a la banca móvil como los ataques dirigidos. Y eso no es todo, porque las amenazas a infraestructuras críticas estarán a la orden del día, así como los nuevos retos de seguridad vinculados al denominado "Internet para Todo" (IoE, por sus siglas en inglés) y a Deep Web.

- **¿Qué peligros tienen las aplicaciones para móviles?[209]**

Un informe realizado por expertos en Seguridad Informática del centro tecnológico Barcelona Digital identifica los principales riesgos de las apps resaltando la necesidad de una mayor conciencia sobre lo que se descarga. Los teléfonos inteligentes se han convertido en una de las principales puertas de acceso al mundo digital y gracias a las apps pueden usarse un gran número de servicios, muchos de ellos gratuitos y populares por su utilidad u originalidad

- **Multado con casi medio millón de euros por subir una película a BitTorrent[210]**

206 http://muyseguridad.net/2013/12/03/vulnerabilidad-en-android-4-3-bloqueo-seguridad/

207 http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/PG/2013/051213ConsejoSeguridadNacional.htm

208 http://www.channelbiz.es/2013/12/12/amenazas-moviles-ataques-dirigidos-sacudiran-2014/

209 http://www.ciospain.es/seguridad/que-peligros-tienen-las-aplicaciones-para-moviles

Subir una película protegida con derechos de autor a BitTorrent ha salido muy caro a un usuario de una comunidad privada sueca dedicada a compartir torrents. La condena confirma que tendrá que pagar el equivalente a lo que hubiesen cobrado sus productores por distribuirla de forma gratuita: cerca de medio millón de euros.

- **Las campañas de phishing son menores en volumen pero mucho más dirigidas[211]**

La infraestructura cloud fácilmente escalable y la disponibilidad de botnets de alquiler asequibles, ha hecho que el coste de la realización de campañas masivas de phishing siga disminuyendo. Incluso si la tasa de retorno es pequeña o la campaña está mal ejecutada, el phishing puede dar mucho dinero a los delincuentes.

- **Qadars, el troyano que es capaz de franquear los sistemas de autenticación[212]**

ESET ha analizado los patrones de comportamiento de un potente troyano denominado Qadars y que está afectando de forma muy activa a bancos europeos, especialmente en Holanda, Francia, Italia, Canadá, India y Australia. Qadars utiliza una amplia variedad de formas de ataque, algunas de las cuales utilizan componentes del sistema operativo Android y que son capaces de sobrepasar los sistemas de doble autenticación que utiliza la banca online.

210 http://www.adslzone.net/article13515-multado-con-casi-medio-millon-de-euros-por-subir-una-pelicula-a-bittorrent.html

211 http://www.csospain.es/Las-campanas-de-phishing-son-menores-en-volumen-pe/seccion-actualidad/noticia-135041

212 http://blogs.protegerse.com/laboratorio/2013/12/19/qadars-un-troyano-bancario-con-los-paises-bajos-en-su-punto-de-mira/

ANEXO C. LAS INVERSIONES EN TIC

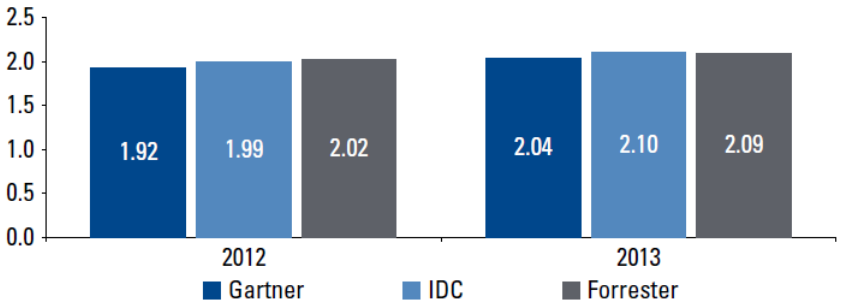
En 2013, el gasto mundial en TIC se recuperó ligeramente, impulsado por las leves mejoras de los parámetros macroeconómicos. Es de esperar que 2014 ratifique esta tendencia.

Como hemos visto con anterioridad, las organizaciones (públicas y privadas) tienden a invertir cada vez más en los ecosistemas construidos alrededor de la computación móvil, los servicios prestados en internet (cloud), las redes sociales y el análisis de grandes volúmenes de datos. A medida que estas tendencias tecnológicas (disruptivas en términos del control de la ciberseguridad) superen su fase de evaluación inicial y se conviertan en elementos esenciales de la política informática de las organizaciones, es presumible que aumente el gasto mundial de tecnologías y, obviamente, de soluciones TIC de ciberseguridad.

1.1 Las inversiones mundiales en TIC[213]

Las previsiones de años anteriores[214] estimaron que el gasto esperado en TIC para 2013 (excluyendo los servicios de comunicaciones) estaría entre 2,04 y 2.10 trillones[215] de dólares, lo que podría suponer un crecimiento respecto de 2012 entre el 3 y el 6%. No obstante, Gartner ha estimado recientemente que el gasto en TIC en todo el mundo en 2013 ha sido de, aproximadamente, 3,7 trillones de dólares, lo que ha supuesto un incremento anual del 4,2%.

La figura siguiente muestra las estimaciones de gasto TIC (en trillones dólares) realizados por distintas fuentes.



1.2 Áreas de crecimiento

Los resultados de una reciente investigación de Gartner[216], "Hunting and Harvesting in a Digital World: The 2013 CIO Agenda", indican que las tecnologías digitales "orientadas desde el exterior" dominarán las prioridades tecnológicas de los CIO[217] en los próximos años.

213 Fuente: KPMG. "013 Spending Predictions Consensus.

214 Gartner: Worldwide IT spending update (Jan, 2013), Global Tech Market Outlook 2013 to 2014 / Forrester, (Jan, 2013) / IDC (Nov, 2012)

215 Trillions americanos (1 trillion americano = 1012)= 1 billón europeo

216 http://www.bankingtech.com/56882/trendy-techs-top-cio-priority-lists-for-2013-says-gartner-study/

217 CIO = Chief Information Officer

Los CIO entrevistados entienden que estas nuevas tecnologías, que ya están modificando en modo de operar de las organizaciones (tecnologías disruptivas), serán su principal objeto de preocupación en los próximos diez años.

Según el citado estudio, las tecnologías más disruptivas serán: las tecnologías móviles (70%), el análisis de grandes volúmenes de datos (55%), las redes sociales (54%) y los servicios cloud (51%), aunque su potencia perturbadora alcanzará su máxima expresión cuando se utilicen combinadamente.

La figura siguiente muestra las áreas clave del gasto TIC, atendiendo a las previsiones de previsiones de diferentes firmas[218].

Key technologies	Gartner	IDC	Forrester	Goldman Sachs	Frost & Sullivan	Nucleus Research
Big Data	+	+	+	+		+
Cloud	+	+	+	+	+	
Bring Your Own Device (BYOD)	+	+	+			-
IT outsourcing	+	+	+			
Virtualization	+	+	+	+		
Tablets		+	+		+	
Data center	+	+	+			
Data security and privacy	+	+	+		+	-
Social media	+	+	+	+	+	+

Top 10 CIO Technology Priorities in 2013	Ranking
Analytics and business intelligence	1
Mobile technologies	2
Cloud computing (Software-as-a-Service, Infrastructure-as-a-Service, Platform-as-a-Service)	3
Collaboration technologies (workflow)	4
Legacy modernization	5
IT management	6
Customer Relationship Management (CRM)	7
Virtualization	8
Security	9
Enterprise Resource Planning (ERP) Applications	10

Servicios en la nube (Cloud)

El 451 *Group's Research Market Monitor* indica[219] que el mercado global de servicios cloud pudo alcanzar en 2013 la cifra de 16,7 miles de millones de dólares, frente a los 8,7 de 2010.

Gartner e IDC señalan que, habiendo ganado madurez los modelos SaaS y IaaS, es probable que el crecimiento venga impulsado por PaaS. TechMarket View y Ovum comparten esta opinión, estimando que la gobernanza de la nube, la gestión y la integración serán reconocidas como prioridades corporativas clave. En este sentido, hay que añadir que, en 2012, las organizaciones tuvieron que aprender a asumir el coste de las interrupciones de determinados proveedores de la nube, tales como Amazon Web Services (AWS), Apple iCloud, GoDaddy, Rackspace, Google, Microsoft y Twitter. Estas interrupciones podrían haber significado un coste medio para las organizaciones de 5.600 dólares por minuto (coste medio en relación con el tiempo de inactividad de los centros de datos, según lo señalado por el Ponemon Institute en 2011220).

En consecuencia, en 2013 los clientes de servicios cloud han exigido de sus proveedores Acuerdos de Nivel de Servicio (SLA) mucho más estrictos, así como garantías adicionales de fiabilidad. Parece claro que, a partir de ahora, una propuesta económica ventajosa no será el único elemento que los clientes tendrán en cuenta a la hora de adjudicar un contrato. La diferenciación vendrá de la mano de otros factores tales como un mejor aprovechamiento de

218 "+" denota aquellas áreas en las que se espera que aumente el gasto en TIC, mientras que "-" denota decrementos de gasto.

219 http://optimipcouk.blogs.experienceproject.com/623081.html

220 http://www.datacentres.com/news/data-centre-outages-generate-big-losses

la infraestructura existente, la extensión a la nube de dispositivos localizados en las instalaciones del cliente, flexibilidad de precios basada en los SLA, recuperación de datos, reglas de control de acceso, etc.

BYOD

En primer lugar, hay que señalar que, según las estimaciones de Gartner[221], en 2013 adquirieron 1.200 millones de dispositivos inteligentes en todo el mundo, entre tablets; frente a los 821 millones de 2012. Forrester Research[222] vaticina que BYOD seguirá auge en los próximos años, estimando en 250 millones los trabajadores que poseerán una tableta en 2016. Ovum[223] mantiene una estimación similar. En un estudio realizado por el Enterprise Strategy Group[224] se indicó que los presupuestos anuales de BYOD se incrementaron en un 36% en 2013.

Sosteniendo una postura distinta, Nucleus Research[225] entiende que la penetración de BYOD se reducirá en los próximos años, cuando pase la moda y madure definitivamente el uso de los dispositivos móviles en las organizaciones[226]. Algunos autores sostienen, además, que la disminución del coste de propiedad de los equipos PCs para las organizaciones contribuirá igualmente al descenso del uso del modelo BYOD[227].

Pese a todo, la mayoría de los analistas sostienen que BYOD seguirá creciendo en 2014, estando también de acuerdo en que la seguridad seguirá siendo una de las mayores preocupaciones en materia de seguridad, por lo que es de esperar que las organizaciones comiencen a redactar y publicar políticas BYOD corporativas. Esta es la opinión de Forrester[228]. IDC[229], más optimista, señala que, en los próximos años, muchas organizaciones aprobarán una política de seguridad BYOD que equilibrará los deseos de los usuarios, la innovación organizacional y la gestión de riesgos de los activos corporativos.

Almacenamiento y minería de grandes volúmenes de datos (Big Data)

Creemos que el concepto de Big Data ya ha superado la fase de novedad de los años precedentes. Así opina Forrester[230]. IDC, por su parte, estima que el mercado de Big Data alcanzará los 24 billones[231] de dólares en 2016, advirtiendo que tal cifra es "conservadora" y que este mercado podría llegar a ser mucho mayor. IDC[232], además,

221 http://www.gartner.com/newsroom/id/2227215

222 http://www.shoretel.com/about/newsroom/industry_news/More_employees_will_want_mobility_options_in_2013.html

223 http://www.cxotoday.com/story/top-2013-tech-trends-that-will-shape-the-enterprise/

224 http://www.shoretel.com/about/newsroom/industry_news/More_employees_will_want_mobility_options_in_2013.html

225 http://www.cio.com/article/721478/2013_Prediction_BYOD_on_the_Decline_

226 Según Nucleus Research: "La realidad es que los costes de soporte, los riesgos de conformidad legal y el ocasional reembolso, conducen a un mayor coste total de propiedad, sin que ello suponga un retorno apreciable en inversión o en aumento de la productividad".

227 La entidad Barclays Capital Ben Reitzes predice que el ciclo de reemplazo de PC será de un año o dos dentro de poco tiempo.

228 http://www.usatoday.com/

229 http://www.idc.com/getdoc.jsp?containerId=prUS23906213

230 http://blogs.forrester.com/mike_gualtieri/13-01-02-big_data_predictions_for_2013

231 Billions americanos (1 billion americano = 109)

232https://idc-insights-community.com/groups/it_agenda/business-analytics-big-data/recapofbigdatapredictions2013infrastructureperspective

predice que el mayor gasto se destinará a análisis predictivo, herramientas de identificación (descubrimiento) de activos y aplicaciones analíticas.

La compañía Ovum[233] estando sustancialmente de acuerdo sobre el potencial de Big Big Data, advierte que, aunque las organizaciones comiencen a preocuparse por temas relativos a la gobernanza de la custodia de grandes volúmenes de datos, la determinación de determinación de "lo que debe gobernarse y cómo debe gobernarse, y la forma de racionalizar el manejo de grandes volúmenes de datos no se resolverá con los modelos actuales".

Redes sociales

Cada vez más los individuos, las organizaciones y los profesionales o personajes notorios utilizan las rede sociales para informar de su actividad, mantener contacto con sus seguidores y mantener su "imagen digital" o "reputación online" con alto valor, y con ello, obtener distintas ventajas y beneficios.

El estudio sobre medios/redes sociales que Gartner[234] realiza anualmente, insiste en que la que la principal razón por la que empresas e instituciones públicas están presentes en redes redes sociales es la de mejorar las relaciones con sus clientes o con los ciudadanos, apreciación apreciación que coincide con la hecha por Forrester. Así, por ejemplo, Twitter se ha convertido convertido en el medio social más usado por líderes de opinión para compartir conocimiento. conocimiento. Con más de 200 millones de usuarios activos (6,5 millones en España) es un medio muy influyente. De hecho, los conocidos como "Trending Topics"[235] o tendencias son utilizados, cada vez más, para conocer la actualidad de forma rápida, como fuente de información y análisis de tendencias, pese a que la manera de cómo se seleccionan son uno de los secretos mejor guardados de Twitter.

Sin embargo, Gartner sostiene que, mientras que las inversiones en marketing social están garantizadas en los próximos dos años, todavía existen demasiadas compañías que, pese a ser conscientes de sus ventajas, no disponen de un plan de utilización de tales medios. La predicción de IDC[236] apunta a que, en los próximos años, las redes sociales seguirán penetrando en el desenvolvimiento de las organizaciones aunque, a menudo, sin la intervención del departamento TIC.

Las perspectivas[237] respecto de la utilización de las redes sociales dentro de las organizaciones también son muy favorables en los próximos años. Los analistas creen que un amplio sector de productos cada vez más maduros –tales como SharePoint, Connections, Jibe, Igloo, Chatter, Tibbr, etc.- contribuirá a dinamizar las plataformas sociales de las organizaciones, especialmente en las grandes empresas y en los organismos públicos más significativos.

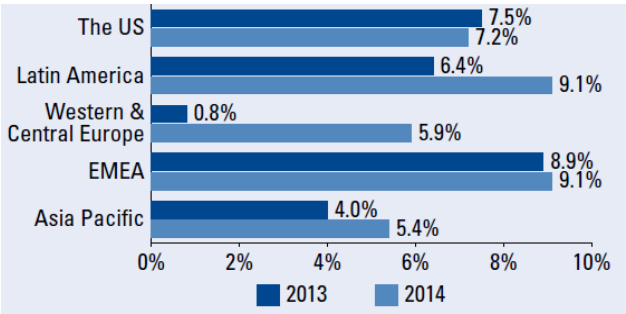
233 http://ovum.com/research/2013-trends-to-watch-big-data/

234 http://blogs.gartner.com/adam-sarner/2013/01/15/social-marketing-in-2013/

235 Aquellas palabras o frases cortas que se repiten más veces entre los mensajes de los tuiteros o usuarios de Twitter.

236 http://www.idc.com/getdoc.jsp?containerId=prSG23819712

237 http://www.slideshare.net/tibbr/16-enterprise-social-networking-predictions-for-2013



Previsiones de gasto IT por regiones mundiales 2013-2016[238]

1.3 Perspectivas del gasto TIC en los principales mercados verticales.

Sector Público

A nivel mundial, Gartner[239] estima que el gasto TIC en el sector público no significativamente en los próximos años[240]. Esta situación debe atribuirse especialmente a las medidas de austeridad que afectan a los gastos de las Administraciones públicas en todo el mundo, especialmente en los EE.UU. y en Europa. Estas medidas de recorte de gasto están alentando a las entidades del sector público a utilizar servicios compartidos, tales como la iniciativa del G-Cloud en el Reino Unido[241].

Pese a lo anterior, es presumible que el gasto en ciberseguridad, comparativamente considerado, seguirá aumentando en los organismos públicos en los próximos años.

Industria

Según las estimaciones de Gartner, el gasto TIC en el sector industrial superó en 2013 el de otros sectores, con una cifra de 478.000 millones de dólares, un 2,3 por ciento más que en 2012. Aunque se trata una cifra muy importante entre los sectores verticales, su crecimiento es relativamente lento ya que las industrias de todo el mundo han ido reduciendo progresivamente sus compras TIC, acompasándose al porcentaje de reducción de sus ventas.

Servicios Financieros

Comparativamente, el sector de servicios financieros invierte en TIC aproximadamente tres veces más que el promedio de todas las industrias. Es de esperar que esta tendencia continúe en los próximos años. IDC[242] señala que los servicios financieros deberán acomodar la forma en que se relacionan con sus clientes a la nueva

238 Fuente: Forrester Global Tech Market Outlook (Jan, 2013).

239 http://www.gartner.com/newsroom/id/2238915

240 Pudiendo disminuir en algunas regiones en torno a un 2% en el periodo 2014-2015.

241 http://gcloud.civilservice.gov.uk/

242 http://www.idc.com/prodserv/insights/financial/index.jsp

realidad impuesta por las tecnologías antes señaladas (cloud, movilidad, big data y redes sociales), sin dejar de reducir costes.

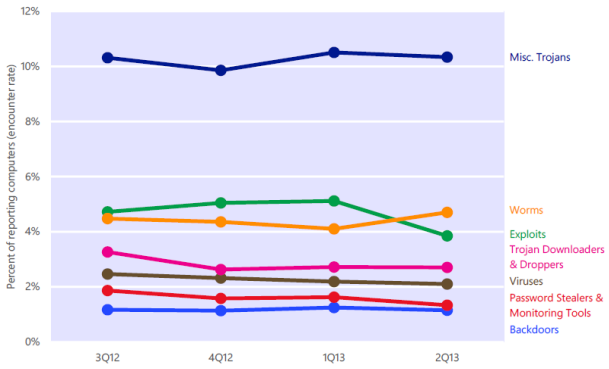
Gartner indica que el gasto TIC en el sector bancario y de valores alcanzó los 460.000 millones de dólares en 2013, un 3,5 por ciento más que en 2012. Por su parte, el gasto TIC en seguros alcanzó los 187.000 millones de dólares en 2013, frente a los 179.000 millones dólares del año anterior.

Servicios de Comunicaciones

En 2013, el gasto de este sector un 3%, alcanzando la cifra de 426.000 millones de dólares. Porcentualmente, el gasto TIC en relación con los ingresos es cinco veces mayor que en otros sectores, muy por encima de la media del sector industrial. Este incremento de gasto se debe principalmente a las inversiones en soluciones de nueva generación, tales como 4G/LTE y banda ancha a través de fibra óptica.

ANEXO D. CATEGORÍAS DEL CÓDIGO DAÑINO

El código dañino puede clasificarse en diferentes tipos, según su forma de propagación y el objeto que persigue. Microsoft utiliza las siguientes siete categorías: Worms (gusanos), Exploits, Misc Trojan (Troyanos genéricos), Trojan Downloaders&Droppers (troyanos), Viruses (virus), Passwords Stealers&Monitoring Tools (ladrones de contraseñas) y Backdoors (puertas traseras).



Tasas de detección de amenazas por categoría[243]

1.1 Categorías de código dañino por localización

La propagación del código dañino y su eficacia dependen en gran medida del idioma y de factores culturales, así como de los métodos utilizados para su distribución. Algunos códigos dañinos se propagan mediante técnicas que se dirigen a las personas que usan un idioma en particular o que utilizan los servicios en línea de una región geográfica específica. Otros se dirigen por el contrario a vulnerabilidades o configuraciones de un determinado sistema operativo o aplicaciones, que se distribuyen de manera desigual en todo el mundo.

La figura siguiente muestra la distribución de las diferentes categorías de código dañino y software potencialmente no deseado en varios lugares del mundo.

Category	Worldwide	United States	Brazil	Russia	Turkey	India	Mexico	Germany	France	China	United Kingdom
Misc. Trojans	10.3%	8.0%	15.1%	23.6%	30.2%	15.8%	14.6%	6.9%	8.9%	16.3%	8.0%
Worms	4.7%	0.7%	8.4%	5.7%	21.4%	18.0%	17.7%	1.2%	2.1%	5.8%	0.9%
Exploits	3.9%	4.0%	3.1%	3.9%	7.7%	5.4%	3.7%	4.6%	3.6%	2.7%	4.1%
Trojan Downloaders & Droppers	2.7%	1.8%	8.2%	3.9%	10.7%	2.1%	5.6%	0.9%	5.1%	3.6%	1.6%
Viruses	2.1%	0.3%	3.3%	2.2%	8.8%	8.8%	3.5%	0.5%	0.8%	6.2%	0.5%
Password Stealers & Monitoring Tools	1.3%	0.8%	3.2%	2.5%	2.5%	2.8%	1.7%	1.2%	1.3%	1.1%	1.0%
Backdoors	1.2%	0.6%	1.7%	1.2%	2.8%	2.4%	2.4%	0.5%	0.9%	3.1%	0.8%

Prevalencia de las categorías de amenazas en el mundo (2Q13)[244]

243 Los totales para cada período de tiempo pueden superar el 100% debido a que algunos equipos han podido reportar más de una categoría de amenaza.

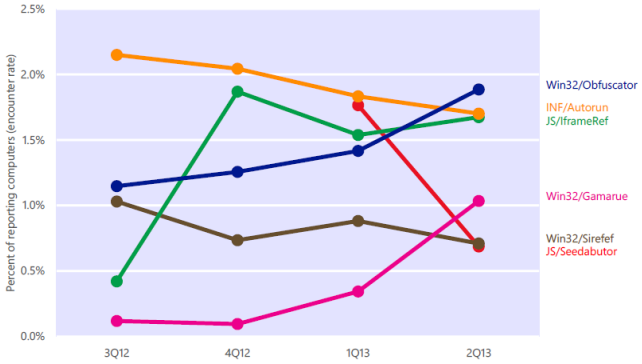
1.2 Familias de código dañino

A título de ejemplo, la figura siguiente muestra las 10 familias de código dañino más detectados por los productos de Microsoft en el primer semestre de 2013.

	Family	Most significant category	3Q12	4Q12	1Q13	2Q13
1	INF/Autorun	Miscellaneous Trojans	2.15%	2.04%	1.83%	1.70%
2	Win32/Obfuscator	Miscellaneous Trojans	1.15%	1.26%	1.42%	1.89%
3	HTML/IframeRef	Exploits	0.42%	1.87%	1.54%	1.67%
4	JS/Seedabutor	Miscellaneous Trojans	—	—	1.76%	0.69%
5	Win32/Dorkbot	Worms	0.95%	1.01%	0.82%	0.95%
6	Win32/Sirefef	Miscellaneous Trojans	1.03%	0.74%	0.88%	0.71%
7	Win32/Sality	Viruses	0.80%	0.81%	0.78%	0.73%
8	Win32/Conficker	Worms	0.86%	0.82%	0.72%	0.68%
9	Win32/Gamarue	Worms	0.12%	0.09%	0.34%	1.03%
10	JS/BlacoleRef	Miscellaneous Trojans	0.87%	0.57%	0.45%	0.74%

Las 10 familias de código dañino más detectadas

De cara a observar su evolución, la figura siguiente muestra las tendencias de detección respecto de ciertas familias de código dañino, que aumentaron o disminuyeron significativamente en los últimos cuatro trimestres.



Tendencias de detección de familias de código dañino (3Q12-2Q13)

1.3 Familias de código dañino por plataforma

El código dañino no afecta a todas las plataformas por igual. Algunas amenazas se propagan por exploits que resultan ineficaces contra una o varias versiones del mismo sistema operativo. Por otro lado, algunas amenazas son más comunes en ciertas partes del mundo, donde las ciertas plataformas son más populares que en otros lugares. En otros casos, las diferencias entre las plataformas pueden ser causadas por una simple variación aleatoria. La

244 Los totales de cada localización pueden exceder del 100% debido a que algunos ordenadores reportaron amenazas en más de una categoría.

figura siguiente muestra cómo las detecciones de las familias de mayor prevalencia en el periodo considerado poseen distintas penetraciones en diferentes versiones del sistema operativo de Microsoft.

Rank 2Q13	Family	Most significant category	Rank (Windows 8 RTM)	Rank (Windows 7 SP1)	Rank (Windows Vista SP2)	Rank (Windows XP SP3)
1	Win32/Obfuscator	Miscellaneous Trojans	1	1	4	6
2	INF/Autorun	Miscellaneous Trojans	2	3	13	1
3	HTML/IframeRef	Exploits	3	2	1	2
4	Win32/Gamarue	Worms	4	4	24	7
5	Win32/Dorkbot	Worms	8	5	25	8
6	JS/BlacoleRef	Miscellaneous Trojans	15	6	6	9
7	Win32/Sality	Viruses	6	12	52	5
8	Win32/Sirefef	Miscellaneous Trojans	20	7	2	12
9	JS/Seedabutor	Miscellaneous Trojans	5	13	26	3
10	Win32/Conficker	Worms	13	10	28	4
13	Java/CVE-2012-1723	Exploits	43	9	3	20

Penetración del código dañino en diferentes plataformas

ANEXO E. LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

La **Estrategia de Ciberseguridad Nacional** es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

La Estrategia consta de **cinco capítulos.**

El primero, bajo el título *El ciberespacio y su seguridad,* presenta las características que definen el ciberespacio, las oportunidades que ofrece y las implicaciones de la dependencia de éste, desde el punto de vista de la seguridad. Este capítulo pone de manifiesto cómo las particularidades que son comunes a las ciberamenazas, la elevada dependencia de la economía y los servicios esenciales del ciberespacio, conllevan a un incremento del número de riesgos y amenazas con un impacto potencialmente grave a la Seguridad Nacional.

El **segundo capítulo** establece el *Propósito y los principios rectores de la ciberseguridad en España.* En cuanto a la primera cuestión, se establece como finalidad la fijación de las directrices generales del uso seguro del ciberespacio, mediante una visión integradora que implique la coordinación de Administraciones Públicas, el sector privado y los ciudadanos y que canalice las iniciativas internacionales en la materia, dentro del respeto al ordenamiento jurídico interno e internacional, y en línea con otros documentos estratégicos nacionales e internacionales.

Por lo que se refiere a los *principios rectores* de la ciberseguridad, se recogen el *liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional* como extensión de los principios informadores de la Estrategia de Seguridad Nacional. Estos principios subrayan la necesaria planificación de desarrollo del contexto actual haciendo especial hincapié en la protección de los valores constitucionales como elemento común.

En el **tercer capítulo,** la Estrategia aborda, con un nivel creciente de detalle, *los Objetivos de la ciberseguridad.* Como objetivo global se establece lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques. A este fin debe servir la Política de Ciberseguridad Nacional.

Seguidamente, la Estrategia fija **seis objetivos específicos:** 1) para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia; 2) para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; 3) en el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio; 4) en materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio; 5) en capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España

para sustentar todos los objetivos de la ciberseguridad; y 6) en lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.

El **capítulo cuarto** recoge las *Líneas de Acción de la Ciberseguridad Nacional*, que con carácter interdependiente y vinculadas a los objetivos establecidos en el capítulo precedente, orienta la acción dirigida a alcanzar los objetivos expuestos.

El **quinto y último capítulo** está dedicado a *La ciberseguridad en el Sistema de*

Seguridad Nacional y establece la estructura orgánica al servicio de la ciberseguridad.

Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: uno ya existente, el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; y dos nuevos: el Comité Especializado de Ciberseguridad, que dará apoyo al Consejo de Seguridad Nacional prestando asistencia a la dirección y coordinación de la Política de Seguridad Nacional en materia de ciberseguridad, así como fomentando la coordinación, cooperación y colaboración entre Administraciones Públicas y entre éstas y el sector privado y el Comité Especializado de Situación, que, con apoyo del Centro de Situación del Departamento de Seguridad Nacional, gestionará las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden las capacidades de respuesta de los mecanismos habituales. Los dos Comités Especializados actuarán de forma complementaria.