

Los Reyes Magos trajeron carbón a virus y "phishing", los malos de 2005

Mercè Molist (*)

<http://ww2.grn.es/merce/who.html>

30 de diciembre de 2005

Los virus y el "phishing" (mensajes que simulan venir de una entidad bancaria) han sido lo peor de 2005, junto al aumento de redes de ordenadores asaltados para mandar estos virus, fraudes y correo basura. Destaca la aparición de un nuevo ataque, el "pharming", y la creciente motivación económica de los criminales informáticos.

Las estadísticas de los centros españoles de atención a incidencias (CERTs) son claras: en 2005, las peores amenazas han sido los virus, gusanos y troyanos, el "phishing", los accesos ilegales a ordenadores mediante códigos maliciosos, ataques de fuerza bruta para romper contraseñas débiles y escaneos a puertos con fallos conocidos, los ataques a servidores web, especialmente PHP, y los bombardeos.

Nada nuevo bajo el sol, dice Chelo Malagón, del IRIS-CERT: "Se confirma la tendencia de atacar a usuarios finales, conectados permanentemente y poco protegidos. Esto hace que el número de ordenadores asaltados sea mayor y los ataques realizados con ellos, más masivos. También se ha intensificado la venta de listados de equipos comprometidos y el acceso a servicios de comercio electrónico, para obtener información de sus usuarios".

Manuel García-Cervigón, del esCERT, añade: "El "phishing" se ha duplicado y ha aparecido una nueva modalidad, el "pharming", que consiste en llevar a los usuarios a webs falsas, manipulando el sistema de nombres de dominio (DNS). La ingeniería social continúa siendo la artimaña más utilizada. Muchos virus, el "phishing" y el "pharming" se están sirviendo de estos métodos".

El "pharming" aparecía públicamente en abril, cuando diversos ataques aprovechaban fallos de servidores Microsoft para redirigir a los usuarios de 700 sitios, como Americanexpress.com, Cnn.com o Msn.com, a webs falsas donde les introducían programas espía. Cuando el usuario tecleaba una dirección en su navegador, el servidor DNS atacado ("envenenado", en la jerga) le llevaba al destino falso.

El objetivo era recolectar información de las víctimas para venderla a emisores de correo basura. Un ejemplo más de la creciente motivación económica de los criminales electrónicos y de su uso e interrelación de distintos ataques. Si antes se creaban virus o se asaltaban ordenadores por diversión, ahora se hace para robar información y tomar el control de estos

equipos, creando redes de cientos de miles que se venderán o alquilarán, para enviar correo basura, programas espía y más virus.

La existencia de estas redes de ordenadores esclavos se ha confirmado en 2005, con diversas redadas. En octubre, la policía holandesa detenía a tres hombres, responsables de una red con más de 100.000 equipos comprometidos. En España, las acciones policiales se han centrado en el "phishing", la pornografía infantil y los virus.

En enero, la Guardia Civil detenía en Écija a A.R.B., de 20 años, presunto autor del virus Tasin. Días después, caía en Madrid J.A.S., de 37 años, acusado de difundir un troyano en las redes P2P, para robar datos bancarios. En junio, la Policía Nacional detenía al conocido "P.Power", de 26 años, quien creaba y distribuía códigos que rompían las protecciones de programas comerciales. En Málaga, caía una banda de 310 nigerianos que enviaban mensajes anunciando premios de lotería falsos.

También ha dado qué hablar la sentencia del caso del "Jamón y el Vino". Después de ocho años de instrucción, un juez condenaba a dos años de prisión y multa de 300.000 euros a Fer13 y Maki, por la puesta en circulación de "cracks" y distribución ilegal de programas en su mítica web. Había sido el primer gran caso contra la piratería de "software" en la historia de la red española.

Pero no todo han sido problemas con la ley. Expertos españoles en seguridad han descubierto fallos de alcance mundial, como Hugo Vázquez, que ha denunciado vulnerabilidades en servidores web Cisco y el sistema de certificación SSL de Verisign. Otro español, Anelkaos, destapaba un importante agujero en el correo gratuito de Google, Gmail. Jordi Corrales descubría un fallo en el cliente de chat mIRC que permitía tomar el control del equipo afectado.

Las vulnerabilidades en programas han aumentado un 15%, según esCERT. Las más importantes a nivel de usuario están relacionadas con Windows (Internet Explorer, Microsoft Office y Outlook Express), reproductores multimedia y mensajería instantánea. A nivel de servicios de red, fallos en Windows y equipos Cisco.

Sube el protagonismo de la seguridad informática en los medios, que se han hecho eco del "webdefacement" de la web de Esquerra Republicana de Catalunya, las cámaras de seguridad abiertas a cualquiera por Internet, el asalto a usuarios famosos de la operadora T-Mobile y el robo y publicación en la red de la agenda telefónica de Paris Hilton, el trabajador de Internet Security Systems que dimitió porque no le dejaban informar de un agujero en los enrutadores Cisco, o las afirmaciones y desmentidos sobre el cierre de la legendaria revista "Phrack", donde este año han publicado artículos diversos hackers españoles. A nivel más que anecdótico, la realidad o leyenda urbana del "wannabe" que, en un canal de chat, quiso borrar el disco duro de un contrincante y acabó borrando el suyo.

El año del "phishing"

Este año ha visto la extensión del "phishing" en España, que ha afectado a la mayoría de entidades bancarias, explica José María Luque, responsable de seguridad de la Asociación de Internautas: "Ha evolucionado a gran velocidad, de los primeros correos con fallos ortográficos a los actuales, que emulan ventanas con la dirección de la entidad, dan números de fax para que la víctima envíe sus datos o incluyen falsos certificados de autenticidad".

Lo último, dice, son "las ofertas falsas de trabajo para blanquear el dinero obtenido del robo de datos bancarios mediante "phishing", usando a personas inocentes como intermediarios para enviar a distintos destinos el dinero robado. Tenemos un gran listado de personas estafadas de esta forma".

Según Luque, el 75% de "phishing" ha simulado venir de entidades bancarias, el 20%, de empresas de subastas e intercambio de dinero y el 5% de webs falsas de recargas para móviles: "A principios de 2005 eran ataques esporádicos, en mayo se duplicaron y desde agosto son continuos. Antes aprovechaban los fines de semana y días festivos, ahora es raro que no se produzca un gran ataque casi a diario".

Las entidades más afectadas ha sido BBVA, Caja Madrid, Bancaja y Banesto. "Sólo Caja Madrid y Ibercaja informaron a sus clientes por correo ordinario. Todas han puesto en su web alguna advertencia y cada vez son más rápidas en cerrar las webs falsas donde los estafadores recolectan los datos. A principios de 2005, la vida media de una web falsa era de 7 a 12 días. En los últimos meses es de 24 horas a 2 días".

"SPAM" a discreción

El correo basura ha seguido su crecimiento exponencial en 2005. Jesús Sanz de las Heras, del Centro de Comunicaciones de RedIRIS/Red.es, lo achaca a "los códigos maliciosos, instalados en PCs con conexión residencial, que pueden funcionar como un servidor de correo autónomo, distribuyendo mensajes que simulan proceder de la víctima". El 85% de los correos basura analizados este año por el Centro de Alerta Antivirus correspondían a estos virus.

La novedad de 2005 ha sido el aumento de ataques del tipo "Directory Harvest Attack", para recolectar direcciones a las que mandar correo basura: "Consiste en enviar decenas de miles de mensajes a un dominio, con nombres de usuario al azar. Los que son devueltos como "usuario desconocido" son rechazados por los "spammers" y el resto son incorporados a sus bases de datos, como direcciones correctas. Esto sobrecarga enormemente los servidores de correo", explica el técnico de RedIRIS.

La lucha contra el "spam" se concentra, por una parte, en evitar que se envíe más basura desde ordenadores infectados. Algo difícil, según Sanz de las Heras: "Las operadoras no quieren controlar el tráfico de correo saliente de

las ADSL residenciales, que en un 100% es malicioso, lo que está obligando a los destinatarios a bloquearlo".

Pero, para filtrar este tráfico, es necesario identificar a los emisores, algo también difícil ya que se mezclan emisores auténticos con emisores atacados. Este año se han afianzado dos posibles estándares para hacerlo: SPF (Sender Policy Framework), usado en RedIRIS y avalado por Microsoft y DKIM (Domain Keys Identified Internet Mail), por Cisco y Yahoo.

El año que viene, dice Sanz de las Heras, aparecerán "nuevos tipos de "spam" más sociológicos y enfocados a estafas. También los primeros en Voz IP, cuyas posibilidades para el "spam" son enormes, como las llamadas automáticas, lo que generará la recomendación: "Sólo recoja las llamadas de personas de su confianza", con la diferencia que si no se cogen se colapsan las terminales y no se pueden recibir nuevas llamadas".

Virus por doquier

La producción de código malicioso ha sufrido un espectacular aumento en 2005, que seguirá el próximo año, asegura Bernardo Quintero, responsable del servicio VirusTotal de Hispasec Sistemas: "Los nuevos especímenes y variantes se han duplicado en el último semestre y sólo este año hemos analizado más de medio millón de muestras sospechosas".

Los virus han cambiado, afirma: "Hemos asistido a su profesionalización, enfocada al fraude económico, como el aumento de troyanos destinados al robo de credenciales de banca por Internet. Apenas se han dado casos de propagación masiva, excepto Zotob en agosto y Sober en noviembre, por un cambio de estrategia: en vez de publicar un gusano que cause mucho ruido, distribuyen muchas variantes, para dificultar su detección".

También se han diversificado las vías de contagio: "Aunque el correo electrónico sigue siendo la principal, se ha visto un claro aumento de código malicioso que llega a través de páginas web, dirigido a usuarios con versiones no actualizadas de Internet Explorer. También ha habido más gusanos en la mensajería instantánea y siguen apareciendo pruebas de concepto para teléfonos móviles, un caldo de cultivo ideal para el código malicioso en un futuro próximo".

Según Quintero, este ha sido el año en que los antivirus han perdido la guerra: "No dan abasto. El esquema clásico y reactivo de los antivirus es insuficiente contra la proliferación actual. Algunas empresas han respondido con políticas más agresivas, ofreciendo actualizaciones cada hora. Aún así, no es suficiente. Los usuarios siguen infectándose debido al aumento y diversidad de código malicioso. Según nuestras estadísticas, la media de detección temprana efectiva que ofrecen los antivirus apenas llega a un 50%".

El experto destaca también el aumento de programas espía comerciales, cuya punta del iceberg ha sido el "rootkit" que Sony instalaba en los ordenadores

que ejecutasen sus CDs: "Cada vez son más los productos comerciales que incluyen estas técnicas. No es casualidad que los antivirus hayan tardado en actualizarse para reconocer este "rootkit". Hay controversia sobre qué deben detectar los antivirus, en especial cuando estas tecnologías intrusivas vienen de la mano de una empresa, lo que se traduce en una falta de protección para el usuario".

El último susto del año

Algunos lo han llamado "la pesadilla de Navidad de Microsoft": el 27 de diciembre, se conocía un grave fallo en la forma como Windows maneja los archivos Windows Media File (.WMF). Si se abre o se visualiza una imagen de este tipo que contenga código malicioso, con Internet Explorer, Outlook, el visor de fax e imágenes, el Explorador de Windows o el programa Lotus Notes, abrirá un agujero en el ordenador por donde podrán entrar virus y otros intrusos. Afecta a todas las versiones de Windows, desde la 3.0, especialmente XP, 2000 y 2003.

Lo que hace más peligroso el fallo es que sólo mirar una página web, previsualizar una foto con el programa de correo o guardarla en el ordenador es suficiente para infectarse, sin necesidad de abrirla. Las imágenes, con formato .WMF, llegan enmascaradas como si fuesen los populares .JPG, .GIF o .DOC, por ejemplo "HappyNewYear.jpg". Ya han aparecido programas que crean estas imágenes automáticamente, para usuarios maliciosos inexpertos, quienes después las pondrán en una web, las enviarán por mensajería instantánea o por correo.

En los primeros días del año, la alarma se ha extendido por la red, con cada vez más usuarios y empresas afectados, según el SANS Institute. Aunque se esperaba que Microsoft reaccionase con urgencia, la compañía decidió no ofrecer un parche hasta el 10 de enero y sólo para Windows a partir de XP. Mientras, los weblogs, listas de correo y avisos de las empresas de seguridad bullían con nuevas noticias sobre la multiplicación de código malicioso que aprovechaba esta vulnerabilidad y el asalto a webs de confianza para colgar en ellas imágenes infectadas.

Al ser los ataques tan rápidos y diversificados, la mayoría de programas antivirus no podían detectarlos todos. Además, coincidía con las vacaciones de Navidad. Muchos usuarios no estaban al tanto del problema cuando llegaban a sus oficinas y era más fácil que fuesen víctimas. La primera recomendación de urgencia de los expertos en seguridad fue que se inhabilitase la carga de imágenes en los programas afectados.

El 31 de diciembre, el especialista ruso en Windows Ilfak Guilfanov publicaba un parche para solucionar el problema. Al no ser un parche oficial de Microsoft, la compañía lo desaconsejó. Pero, por primera vez en la historia, las principales empresas y grupos de seguridad, como el Internet Storm Center, F-Secure o Panda Software, desoyeron a Microsoft y recomendaron a

sus clientes que instalasen el remedio no oficial. Finalmente, Microsoft publicó su parche el 5 de enero.

Estadísticas IRIS-CERT (Enero-Octubre 2005)

Sondeos de puertos	751
Denegacion de Servicio (DoS)	14
Troyanos	2
Gusanos	138
Uso no autorizado	19
Acceso no autorizado	67
Otros (warez, phishing, etc)	22

Sitios Recomendados

Kriptopolis - <http://www.kriptopolis.org>

El santanderino José Manuel Gómez es el padre de esta web, nacida en 1996, una de las más veteranas dedicadas a informar en castellano sobre seguridad informática, privacidad, criptografía, ciberderechos y temas parecidos. Actualmente reconvertida en un weblog colectivo, ofrece diariamente información de alta calidad, difícil de encontrar en otros sitios.

Hispasec - <http://www.hispasec.com>

Web nacida en 1998, a raíz de la puesta en marcha de un servicio gratuito inédito en la red española: el boletín "Una-al-día" que, como su nombre indica, informa diariamente sobre la actualidad en seguridad informática. La web ofrece otro servicio gratuito, VirusTotal, al que se pueden mandar archivos para saber si contienen virus.

VSantivirus - <http://www.vsantivirus.com>

Detallado repositorio de información sobre la actualidad en el mundo de los programas maliciosos, creado desde Uruguay. Ofrece también artículos generalistas como "Guía rápida para el blindaje de su PC", "Cómo recuperar archivos borrados" o "Cómo configurar Zone Alarm". Su boletín diario de alertas por correo es muy recomendable.

Centro de Alerta Temprana Antivirus - <http://alerta-antivirus.red.es>

Excelente recurso creado por Red.es que informa en tiempo real sobre los virus detectados en las redes españolas, con su nombre, descripción, índice de peligrosidad y estadísticas. Otras secciones incluyen alertas por correo electrónico, vulnerabilidades en programas, el "Manual de seguridad en Internet" o herramientas gratuitas de protección.

Seguridad Asociación de Internautas - <http://seguridad.internautas.org>

Información completa y comprensible sobre todo tipo de temáticas: programas maliciosos, vulnerabilidades, criptografía, intrusiones, privacidad, correo basura, banca por Internet. Ofrece noticias diarias sobre seguridad informática, con especial atención a la red española.

Rompecadenas - <http://www.rompecadenas.com.ar>

Veterana web argentina especializada en informar sobre los "hoaxes" o mensajes falsos que circulan por correo electrónico, como cartas para ayudar a niños enfermos que no existen, falsas alertas de virus o métodos para hacerse millonario. Contiene extensa información sobre correo basura, leyendas urbanas y consejos para no creer todo lo que circula por la red.

(*) Copyleft 2005 Mercè Molist.

Verbatim copying, translation and distribution of this entire article is permitted in any medium, provided this notice is preserved.