Las tendencias actuales de la amenaza: Resumen de 2005 y previsiones para 2006

Por ***Jaime Lyndon "Jamz" A. Yaneza*** *y* ***David Sancho***
Analista Senior de la Amenaza *Especialista Anti-Malware*

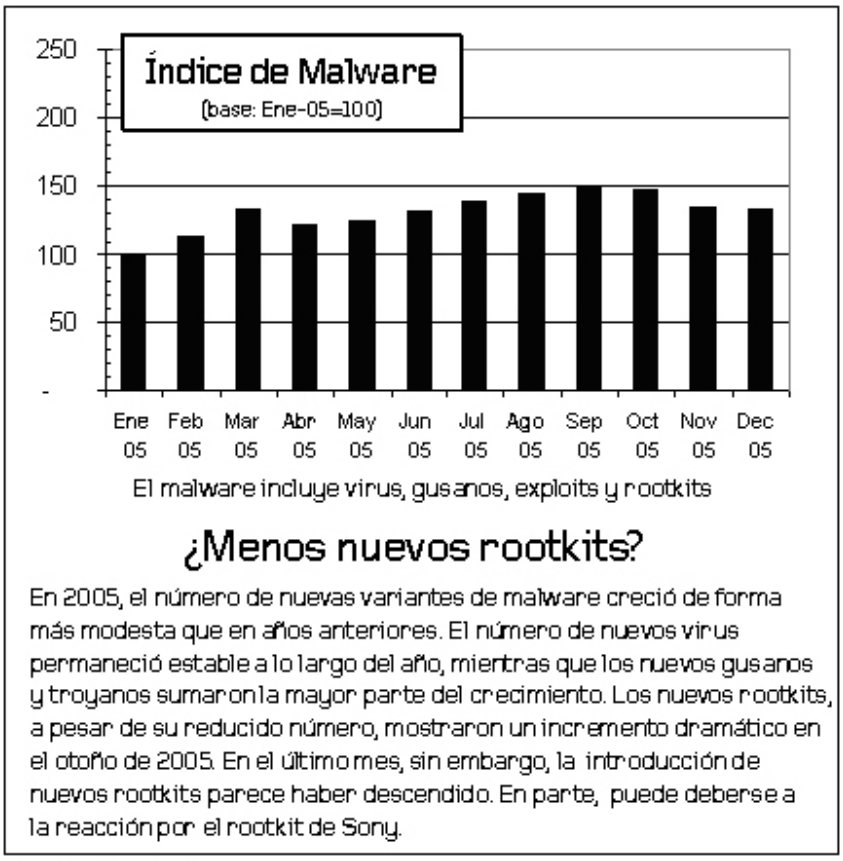
La industria antivirus y de seguridad ha vivido unos cuantos cambios durante el último año –y, más concretamente, en los últimos cinco meses de 2005–. A la luz de recientes acontecimientos, las tendencias están cambiando y han surgido nuevas amenazas. Internet se ha desarrollado realmente como herramienta de marketing, comunicación y comercio mundial. Desafortunadamente, más y más grupos con malas intenciones tratan de abusar del sistema para beneficio propio. Desde la publicidad que vende sus dudosas pastillas de embellecimiento corporal a las organizaciones criminales que roban números de cuentas bancarias, la vida en el ciberespacio está lejos de ser segura. Esta realidad ha llevado a algunos a predecir que esta comunidad sin límites se convertirá en el último "salvaje oeste".

Hace doce meses, Trend Micro previó que las amenazas mixtas continuarían acosando a los usuarios. Esta predicción se comprobó con amenazas como WORM_BAGLE.BE, un tandem de troyano y spam que generó una epidemia en marzo de 2005; con el nacimiento de la familia AGOBOT en enero; con la familia MYTOB, que consiguió hacerse notar con cerca de 300 variantes desde que fue descubierta en febrero, y todavía se clasificó como la de mayor número de variantes entre todos los códigos maliciosos del mes de diciembre. Las predicciones que hablaban de escritores de malware que empleasen tipos de archivo menos comunes también se convirtieron en realidad, al final del año, con la aparición del exploit para Windows Meta File (WMF). Mientras que las amenazas relacionadas con las comunicaciones IRC y P2P sumaron el 16% del total de los sectores de propagación de la amenaza, el spam y el phishing continuaron siendo uno de los mayores problemas a los que se enfrentaron en 2005 tanto los consumidores como las empresas. Además, el gran incremento del spam en lengua no inglesa durante 2005 concede credibilidad a la teoría de que los spammers continuarán con sus intentos de expandir sus logros a nuevos mercados. Hay un peligro inherente asociado a las extraordinarias ventajas de utilizar Internet hoy en día. Los ladrones de contraseñas y los gusanos de red han reemplazado a los virur de script y a los virus infectores de ficheros. El software espía y los programas de adware están ocultos detrás de páginas web sospechosas. *Una fuente de la amenaza, unos objetivos específicos y los efectos colaterales definen una nueva era, la de las "amenazas multipropósito".*

> ***Amenazas Mixtas:*** Un complejo programa que se enfoca en múltiples debilidades de redes de cómputo y utilizan diversos métodos de distribución para propagarse.

El presente informe no es sólo un recuento y análisis de los *incidentes por amenaza*. También sirve como previsión de lo que depararán 2006 y los años siguientes. *Gracias al amplio estudio y análisis de los incidentes de 2005 que hace Trend Micro, este informe documenta cómo las amenazas han evolucionado dentro del régimen de la amenaza multi-propósito y da información a los usuarios corporativos y domésticos sobre qué hacer para que se mantengan protegidos contra amenazas futuras.*

Resumen de indicadores de amenazas



fuente: Trend Micro

2005: ¿El año del Grayware?

Podríamos referirnos a 2005 como el “Año del Grayware”, responsable de un 65% de las 15 principales amenazas mostradas en el gráfico de abajo –con cerca de 11 millones de informes individuales– que incluyen algunos tipos de software espía, adware, códigos de puerta traseta, rootkits y funcionalidades bot.

Algunas otras estadísticas reseñables, respecto al escenario total de la amenaza en 2005:

- El 10% fueron BOTs
- El 11% fueron troyanos de software espía
- El 18% fueron adware
- El 0,6% fueron rootkits
- El 0,6% fueron macros para Office
- El 3% fueron scripts
- El 25% fueron virus o gusanos
- El 27% fueron caballos de Troya (incluidos los rootkits)

15 principales infecciones de 2005 – Por equipos afectados

Nombre de la amenaza	Equipos infectados	Tipo de amenaza
WORM_NETSKY.P	1.602.069	Gusano
JAVA_BYTEVER.A	667.448	Applet de Java
PE_PARITE.A	320.924	Infector de ficheros
TSPY_SMALL.SN	268.171	Grayware
WORM_NETSKY.D	242.243	Gusano
SPYW_GATOR.B	163.495	Grayware
PE_FUNLOVE.4099	147.416	Infector de ficheros
VBS_REDLOF.A	145.701	VBScript
HKTL_RADMIN.A	63.557	Grayware
PE_ZAFI.B	62.708	Infector de ficheros
ADW_SOLU180.A	61.929	Grayware
PE_TENGA.A	44.036	Infector de ficheros
PE_JEEFO.A	27.831	Infector de ficheros
PE_LOVGATE.AC	25.598	Infector de ficheros
PE_NIMDA.A	16.824	Gusano

Fuente: Trend Micro

La tabla anterior muestra las 15 principales amenazas de 2005 por su número de infecciones. WORM_NETSKY.P lleva apareciendo en estas tablas durante casi dos años, desde la aparición de su primera variante en marzo de 2004, y ha permanecido siempre entre las principales amenazas, excepto en septiembre de 2005, cuando variantes de TROJ_AGENT y TROJ_DLOADER ocuparon los puestos de honor. Estas dos amenazas son básicamente descargadores de troyanos y han estado vinculados a ataques de adware y software espía. Su prevalencia se refleja al estar entre las principales amenazas de grayware, con un número combinado de instalaciones muy similar al número de infecciones de NETSKY.

PE_PARITE.A fue descubierto por primera vez en enero de 2001 y ha demostrado ser sorprendentemente tenaz, a pesar de las numerosas soluciones antivirus disponibles actualmente. Introduce su código como parte del fichero .exe de Windows Explorer, haciéndose de este modo parte de cada una de las operaciones normales. Este es un ejemplo de rootkit de modo peudo-usuario. Al afectar al funcionamiento de Explorer.exe, PARITE puede obtener un control previo sobre los procesos e infectar rápidamente otros ejecutables (*.exe) así como los salvapantallas (*.scr).

Detectado por primera vez en noviembre de 1999, PE_FUNLOVE.4099 es el virus de infección de ficheros más antiguo de los que aparecen en el cuadro de arriba. Esta amenaza también ha actuado como gusano de red y así tiene la habilidad de propagarse más fácilmente, ya que las redes compartidas han demostrado históricamente ser el vector de propagación más eficaz para la amenaza. Este virus de infección de ficheros también deja código vírico y parchea los ficheros NTLdr y NTOSKrnl.exe, haciendo que puedan sobrepasar el chequeo de integridad de ficheros de Windows para el Boot Loader Kernel de NT, así como el chequeo de integridad de

ficheros de Windows infectados. Así, a través de funciones similares al modo kernel, este código malicioso fue capaz de vencer los desarrollos de seguridad disponibles en su momento para la protección contra virus de los usuarios de Windows, y continúa estando activo después de más de 5 años. Debido a la complejidad de su rutina de infección, FUNLOVE ha sido usado como carga tanto por WORM_BRAID como por WORM_WINEVAR, y en un hallazgo reciente de doble infección, como portador de la variante WORM_BAGLE.H en lo que resultó una nueva familia llamada WORM_FUNBAG, detectada por primera vez en marzo de 2004.

PE_ZAFI.B, visto por primera vez en junio de 2004, puede que no haya sido el primer código de infección de ficheros y gusano, ni tampoco el primer virus bilingüe de propagación de mensajes de correo electrónico en inglés y alemán. Sin embargo, su combinación de dejar copias infectadas en redes P2P compartidas y de prevenir a los usuarios de chequear sus listas de tareas o el registro de Windows le ha permitido propagarse lo suficiente para convertirse en una de las infecciones más extendidas en 2005.

VBS_REDLOF.A es un caso especial que subraya el peligro de utilizar correo electrónico con formato HTML o de bucear en sitios web no relacionados con el trabajo. Explota una vieja vulnerabilidad de MS Virtual Machine ActiveX que tiene un parche de octubre de 2000, por lo que es sorprendente que esta amenaza (lanzada en agosto de 2004) todavía se las arregle para hacerse notar en nuestro radar. Su carga más peligrosa es que infecta todas las extensiones de webs (*.html, *.htm, *.asp, *.php, *.jsp y *.vbs), así como el Outlook Stationary establecido por defecto, provocando que todos los mensajes salientes estén infectados, y difundiéndose a los receptores.

Alertas mundiales en 2005

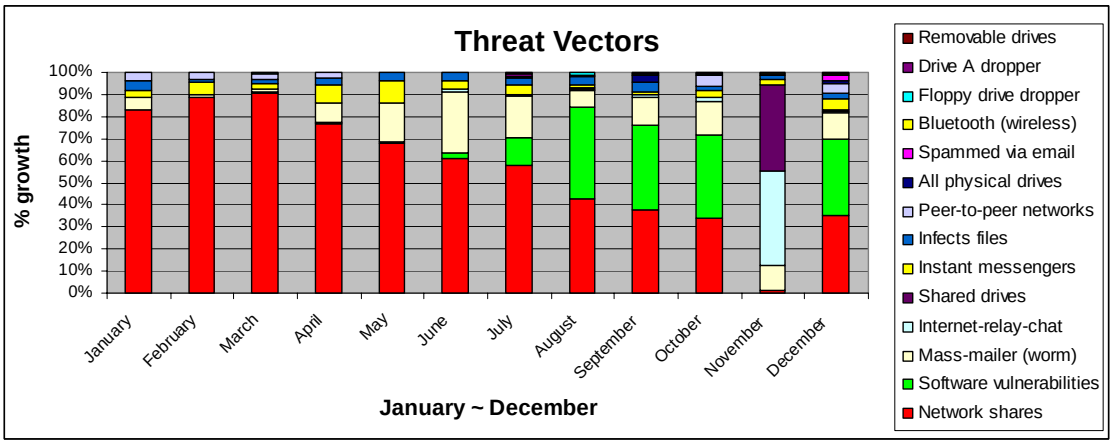
Epidemias de 2005		
Nombre de la amenaza	**Fecha de declaración**	**Trimestralmente**
WORM_BAGLE.AZ	Miércoles, 26 de enero de 2005	Primer trimestre (6)
WORM_BROPIA.F	Miércoles, 2 de febrero de 2005	
WORM_MYDOOM.BB	Miércoles, 16 de febrero de 2005	
WORM_BAGLE.BE	Martes, 1 de marzo de 2005	
WORM_FATSO.A	Lunes, 7 de marzo de 2005	
WORM_KELVIR.B	Lunes, 7 de marzo de 2005	
WORM_KVDBOT.A	Jueves, 28 de abril de 2005	Segundo trimestre (8)
WORM_SOBER.S	Lunes, 2 de mayo de 2005	
WORM_MYTOB.ED	Domingo, 8 de mayo de 2005	
WORM_MYTOB.EG	Lunes, 9 de mayo de 2005	
WORM_WURMARK.J	Miércoles, 11 de mayo de 2005	
WORM_MYTOB.AR	Domingo, 29 de mayo de 2005	
WORM_MYTOB.BI	Martes, 31 de mayo de 2005	
WORM_BOBAX.P	Viernes, 3 de junio de 2004	
WORM_ZOTOB.D	Martes, 16 de agosto de 2005	Tercer trimestre (2)
WORM_RBOT.CBQ	Martes, 16 de agosto de 2005	
WORM_SOBER.AC	Miércoles, 5 de octubre de 2005	Cuarto trimestre (3)
WORM_SOBER.AG	Lunes, 21 de noviembre de 2005	
WORM_MYTOB.MX	Jueves, 24 de noviembre de 2005	

De todas las alertas declaradas durante 2005, el 26% se debieron a variantes de WORM_MYTOB, una amenaza mixta que nace de juntar partes de WORM_MYDOOM, que causó multitud de infecciones en 2004, con componentes BOT (o robot). Su éxito proviene de una gran cantidad de conocidas técnicas de infiltración bastante eficaces, como engañar a los usuarios que buscan ayuda modificando el fichero HOSTS, o como falsificar mensajes de fallo de entrega de correo engañando a los usuarios para que examinen con atención los errores de transmisión.

Las variantes de WORM_SOBER constituyeron el 16% de las epidemias en 2005, debido al enfoque bilingüe en sus mensajes de spam. Al igual que WORM_MYTOB, esta amenaza incluía técnicas de respuesta contra la mayor parte de los productos antivirus, ya que intentaba deshabilitarlos de la memoria y así dejar libremente sus componentes maliciosos no detectados. El uso de grandes eventos mundiales como los encuentros del Mundial de Fútbol de Alemania, una técnica tomada prestada de los creadores de spam, también ha permitido una propagación exitosa de esta amenaza.

A través de la utilización de carpetas compartidas en redes sin seguridad y del amplio uso de aplicaciones P2P, las variantes de WORM_BAGLE sumaron el 11% de las amenazas mundiales a empresas. Parecido a las principales familias que causaron epidemias en 2005, WORM_BAGLE también utilizó técnicas de respuesta así como errores de entrega de correo falsificados para provocar a los usuarios.

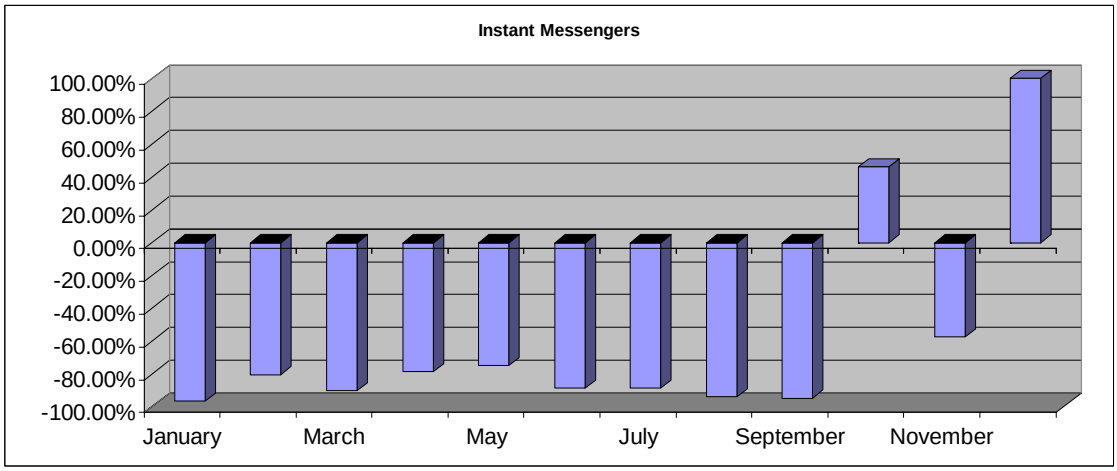
Técnicas de intrusión en redes en 2005



La tabla anterior ofrece un panorama de las técnicas de propagación más empleadas por el código malicioso en 2005, basado en más de nueve mil nuevas piezas de código malicioso dignas de mención y recogidas por Trend Micro durante todo el año. Según nuestro análisis, buscar y dejar de forma recurrente código malicioso en discos de red compartidos es el método más exitoso, con un 37% del total de casos, aproximadamente. Es bastante alarmante, aunque no sorprendente, que la explotación de vulnerabilidades sea el segundo método de mayor éxito, empleados en el 19% de las ocasiones. El uso de código de envío masivo, canales IRC (Internet relay chat) y de compartir por defecto constituyen cada uno el 10% de los métodos de propagación más utilizados. El uso de la mensajería instantánea (IM) como fuente de propagación se hizo sólo en el 4% de las ocasiones, y todo el resto de métodos, como la típica infección de ficheros y las redes compartidas P2P, sólo comprendieron aproximadamente el 2% de los vectores de ataque.

Mensajería instantánea utilizada para ataques de gusanos

En los tres últimos años, los investigadores de Trend Micro han estado avisando a los usuarios sobre el uso esporádico pero en aumento de métodos de infección alternativos. En 2005, fuimos testigos de otra ola de ataques durante el primer trimestre del año, provenientes de los gusanos KELVIR, FATSO y BROPIA, cada uno de los cuales se propagó eficazmente a todos los contractos de MSN Messenger de los ordenadores infectados. A causa del uso de técnicas de falsificación de remitente y del uso todavía inmaduro de la mensajería instantánea, los usuarios fueron sorprendidos al conocer que sus contactos de confianza estaban enviando virus. Este giro de los acontecimientos obligó a Microsoft a lanzar versiones actualizadas del programa con filtros de transferencia de ficheros reforzados para prevenir más ataques en las máquinas de sus clientes.



Arriba se muestran las cifras de crecimiento de la mensajería instantánea como método de infección, basadas en el número de nuevo malware que utiliza esta técnica*. Hubo más de un 100% de aumento en diciembre, frente a las cuato únicas variantes vistas en enero.

*Donde el índice se basa en el 100% en diciembre, denotando el valor más alto.

Tandems de troyanos

En los últimos años, los proveedores de seguridad han recomendado bloquear y filtrar extensiones específicas –unidas a la validación de ficheros adjuntos para eliminar falsos positivos– como la forma más eficaz de prevenir amenazas de envío masivo de correo. Los autores de códigos maliciosos respondieron empleando la compleja técnica de incluir enlaces URL o simples programas de descarga en un intento de frustrar dicha función de seguridad. La técnica tiene su clave en no tener que confiar en el correo electrónico como propagador directo de la amenaza, si no utilizar en su lugar un programa de descarga para dejar ficheros maliciosos en los ordenadores directamente, a través de la web. Esta técnica también lleva el beneficio añadido de hacer posible que el autor actualice el código malicioso, sin el trabajo de tener que reenviar el ataque. Trend Micro le siguió la pista a 54 variantes de código malicioso que utilizaron esta técnica en 2005, y esperamos que esta técnica aumente su popularidad en 2006 y en el futuro.

Aunque WORM_BAGLE.AC fue el primero en utilizar esta técnica, BAGLE.BE fue el primero de su clase en provocar una Alerta Amarilla. Estas variantes utilizan un gusano para hacer spam de un troyano cuya única función era descargar y ejecutar el componente gusano de una lista de sitios web predeterminados. Una vez que el gusano está en marcha, recoge las direcciones objetivo de la libreta de direcciones de Windows (*.WAB) y comienza a reenviar el troyano, repitiendo de esta forma el ciclo. Esta estrategia de dos componentes hace posible que la variante eluda la detección durante el tiempo suficiente para llegar a extenderse más y causar la epidemia consiguiente. Esta técnica de tándem gusano-troyano probó su efectividad de nuevo en mayo con WORM_WURMARK.J y otra vez en junio con WORM_BOBAX.P. Desde entonces ha sido utilizada por la mayor parte de las variantes de BAGLE.

En septiembre, WORM_BAGLE.DA intentó dar un paso más utilizando dos programas de descarga en lugar de uno. Este código malicioso enviaba un troyano, que posteriormente descargaba otro troyano de determinados sitios. El troyano secundario descargaba entonces el verdadero gusano binario, para empezar el ciclo otra vez. Esta técnica en cadena intenta prolongar el proceso de detección, aumentando de este modo el tiempo de vida del ataque. A pesar de ello, los investigadores se dieron cuenta y ya tenían varias soluciones, incluyendo la detección heurística para los troyanos de descarga enviados como spam.

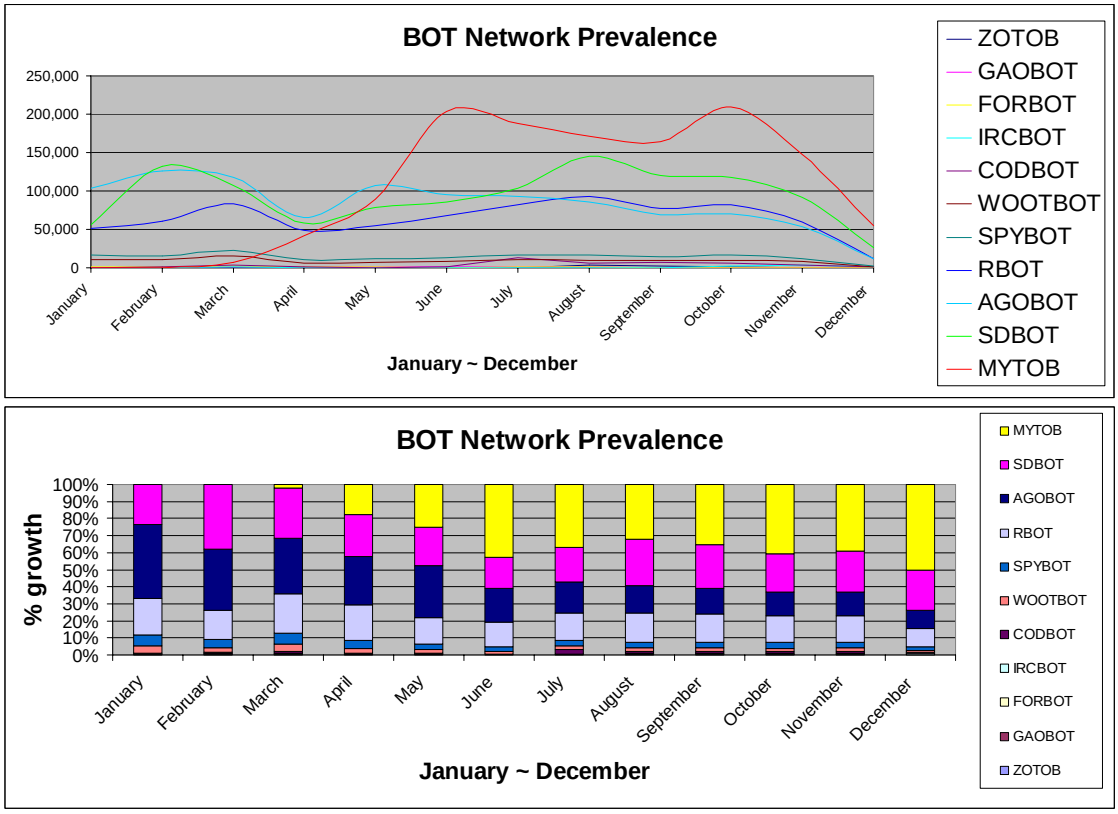
Para atenuar cualquier ataque futuro de este tipo, los usuarios deberían asegurarse de que su solución de seguridad integra habilidades anti-spam y anti-phishing sólidas con sus tradicionales defensas antivirus. La combinación de estas tres funciones permite la calificación de todos los ficheros descargados, neutralizando así esta técnica.

Pequeño es el Nuevo Grande

Los compresores binarios han sido desarrollados para comprimir ficheros ejecutables, haciéndolos así fáciles de distribuir. Aunque este proceso fue pensado en su origen para ficheros de instalación legítimos, el proceso de compresión modifica la estructura interna de un archivo, algo que los autores de códigos maliciosos pueden usar en su propio beneficio. Este es un viejo truco que se convirtió en un lugar común durante la Gerra de los Gusanos del año anterior, a pesar de que un total de siete alertas desde 2002 también emplearon esta técnica.

Los autores de gusanos utilizaron esta táctica para distribuir un fichero de gusano siempre cambiante enmascarado por docenas de empaquetadores diferentes. En este juego del gato y el ratón entre autores maliciosos y compañías de seguridad, tal complejidad retrasó la detección durante el tiempo suficiente para permitir que cuatro variantes de WORM_MYTOB alcanzasen el estado de Alerta Amarilla en mayo. Otro ejemplo notable incluye las variantes de SOBER descubiertas en el último trimestre del año. Trend Micro detectó hasta 64 pruebas de empaquetado diferentes de una sola variante, SOBER.AC, que se convirtieron en epidemia en octubre. En noviembre, SOBER.AG utilizó la técnica con un nivel de éxito similar.

Enredados en las redes BOT



Los datos de arriba detallan algunas de las principales familias BOT (o robot) de 2005. Los BOTs son un tipo especial de amenaza híbrida que incorpora muchas de las técnicas usadas por el código malicioso contemporáneo, con la intención de infectar y retener los parásitos a largo plazo en los sistemas de usuarios afectados. Los BOTs intentan entrar en el sistema a través de métodos como las vulnerabilidades de los sistemas, el spam del correo electrónico o algunos sitios de la red. La mayoría de ellos están preparados para robar información y se extienden hasta el control de administración remoto- presente normalmente a través de una sesión de Chat (IRC). La preocupación de tener uno o más BOTs en el sistema es que con el control administrativo, a menudo llamado control de raíz, un atacante malicioso puede unir sistemas afectados para perjudicar y comprometer otros sistemas a través de un ataque vía denegación de servicio. Además de hacer un gran ataque, esta técnica puede ir más lejos de la red de BOT del autor, permitiendo que futuros ataques se extiendan más.

A principios de 2005 hubo más de mil variantes de AGOBOT, un 43 % de todas las infecciones de BOT. Pero con el increíble crecimiento de BOTS a lo largo del año, la cuota de esta familia de virus se rebajó a sólo un 11% en diciembre. Aparte de sus travesuras habituales, AGOBOT también intentó eliminar las variantes WORM_NETSKY y WORM_BAGLE para evitar conflictos de control de los sistemas infectados. Su lista de aplicaciones de seguridad para cancelar acciones y evitar la detección abarcó casi 600 programas diferentes. Sus autores compitieron con otros clones BOT para mejorar su capacidad.

Asimismo, RBOT supuso el 21 % de las infecciones de enero y cayó de la misma manera hasta el 11 % hacia el final del año – aunque sus variantes habían crecido hasta las 1.500–. El objetivo de RBOT era robar claves de registro para muchos de los juegos de ordenador de entre 2002 y 2004. Las tomaba prestadas de AGOBOT, pero se enfocó más hacia el robo e incluía modificaciones muy básicas de la fuente original.

Otro clon BOT es SDBOT, que tuvo una prevalencia constante del 25 % a lo largo del año, con más de 2.000 variantes. Sus autores parecieron tener más conocimiento del registro interno de Windows y lo modificaron para permitir una propagación más rápida del BOT a través de redes.

Sorprendentemente, la familia de BOTS más prevalente en 2005 fue MYTOB, aunque haya sólo 300 variantes de esta familia. La primera variante de MYTOB fue descubierta en febrero, y combinaba la funcionalidad de WORM_MYDOOM con el uso profundo de la aplicación BOT. El eficaz crecimiento de MYTOB de un mero 2% en marzo a un inquietante 50% en diciembre necesita una revisión. Las modificaciones continuas de su código –incluyendo archivos, comprensión de algoritmos y la introducción de enlaces de la URL en los correos electrónicos con spam para descargar su ejecutable– ha permitido a variantes más recientes evitar ser filtradas en la pasarela de Internet. BAGLE y SOBER utilizaron una técnica similar al final del año. Esta técnica de descarga fue útil para dejar algunos otros programas maliciosos en los sistemas de las víctimas así como para desactivar versiones actualizadas. También utilizó una larga lista de direcciones de correo electrónico para evitar ser descubierto.

Con el descubrimiento de ZOTOB en agosto, se puso de manifiesto que los autores del gusano tenían tanto la tecnología como la intención de añadir exploits de vulnerabilidades a sus creaciones tan pronto éstas fuesen publicadas. Este bot aprovechó la vulnerabilidad del sistema operativo sólo cuatro días después de que Microsoft emitiese un comunicado anunciándola, batiendo el record anterior, situado en dos semanas antes. Dos variantes diferentes de ZOTOB infectaron ordenadores en agosto y Trend Micro tuvo que declarar que la Alerta Amarilla para frenar la epidemia. El gusano aprovechó la vulnerabilidad MS05-39 del Plug-and-Play de los equipos con Windows instalado –incluyendo la última versión de Windows 2003 con ServicePack-1–.

Perdido en la traducción

Al tiempo que nuevos usuarios se unen a Internet, los autores de código malicioso desarrollan nuevas estrategias para ganarse su confianza, en un intento de engañarlos para que ejecuten código malicioso adjunto en el correo electrónico. Las variantes de SOBER fueron especialmente exitosas este año pasado por su uso de diferentes idiomas (tal como hizo ZAFI en diciembre de 2004). SOBER envió correos con texto en alemán a receptores con direcciones de correo germanas, y en inglés a todos los demás. Además, el propio gusano tenía la capacidad de registrar el sistema del usuario infectado para comprobar qué versión de Microsoft OS estaba utilizando. Si detectaba GMX como el dominio, instalaba una de las versiones en alemán; de lo contrario, instalaba una de las versiones inglesas. Tanto la variante AC como la variante AG se generalizaron en Alemania durante el último trimestre del año, desencadenando Alertas Amarillas en ambos casos.

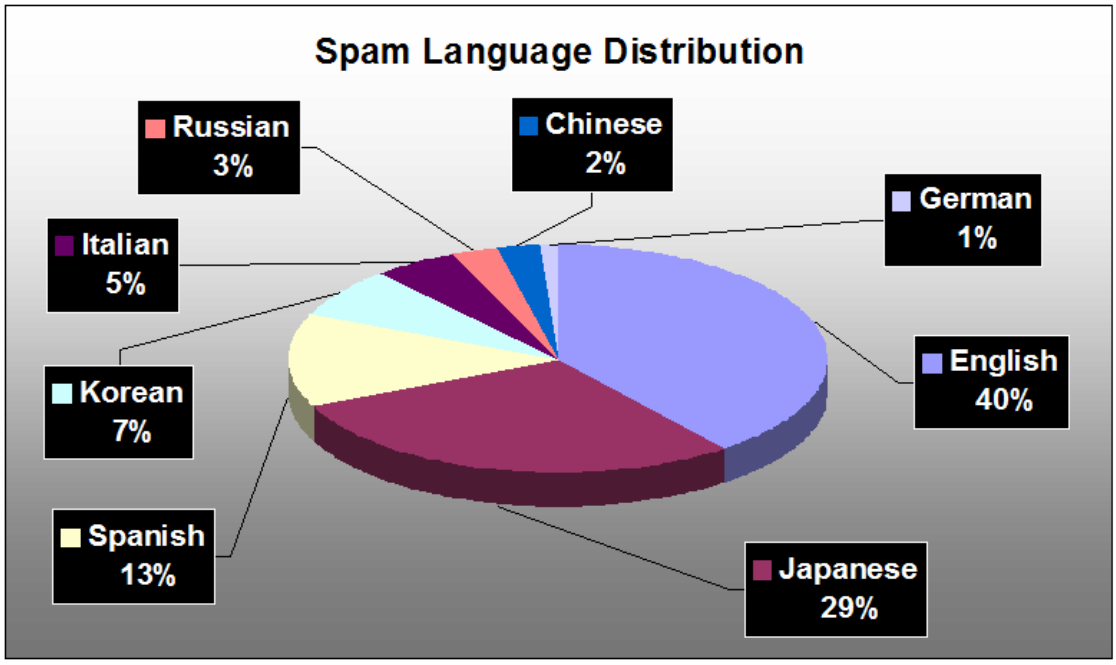
Nuevas técnicas de ingeniería social

En mayo, SOBER.S utilizó una técnica de ingeniería social particularmente exitosa, al prometer entradas gratis para el próximo Mundial de Fútbol de Alemania. La estrategia provocó cientos de aperturas del fichero del gusano, desencadenando una Alerta Amarilla.

Trend Micro también detectó intentos de utilizar noticias de alcance mundial y personalidades de la política como elementos de ingeniería social de correos maliciosos. A pesar de que la técnica sólo tuvo un mínimo impacto en la mayoría de los casos, se convirtió en Alerta Amarilla en junio con WORM_BOBAX.P. Este gusano se inventó noticias de las capturas de Saddam Hussein y Osama Bin Laden.

Desde el tsunami en el sureste asiático en diciembre de 2004 al aparente descubrimiento de Osama Bin Laden, la utilización de noticias de interés general recuerda a técnicas de spam y está convirtiéndose en una tendencia relativamente común para la propagación de numerosas amenazas de seguridad.

El idioma del spam



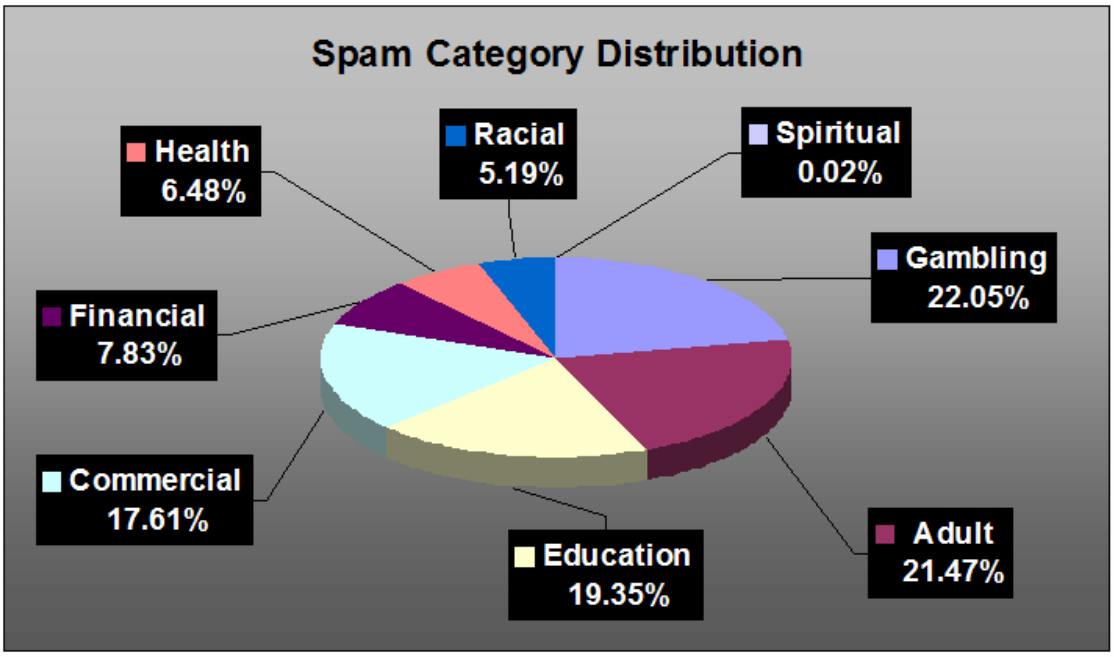
Dados todos los idiomas del mundo, el hecho de que sólo el inglés sume el 40% de todo el spam recibido prueba definitivamente que es también el preferido en el mundo de los negocios. Lo que también es significativo, sin embargo, es que el spam en lengua no inglesa creció en torno a un 20%. Dicho incremento alimenta otros patrones de comportamiento observados, que sugieren que el spam está llegando a ser más traducido para aumentar su eficacia.

La entrada más reciente en la lista de distribución por idiomas de Trend Micro es la del spam compuesto en castellano –con un 13% en 2005, comparado con sólo el 2% el año anterior–. La Organización Europea para la Cooperación Económica y el Desarrollo acaba de presentar sus recomendaciones sobre los factores de tendencia en España,

que incluyen mayor gasto en mejoras en tecnologías de la información y comunicación, así como en áreas relacionadas con la alta tecnología. Se ha observado que el incremento del spam sigue normalmente al crecimiento en TIC (tecnología de la información y la comunicación) y será resuelto una vez que se disponga de las herramientas apropiadas en los sectores privado, público y gubernamental.

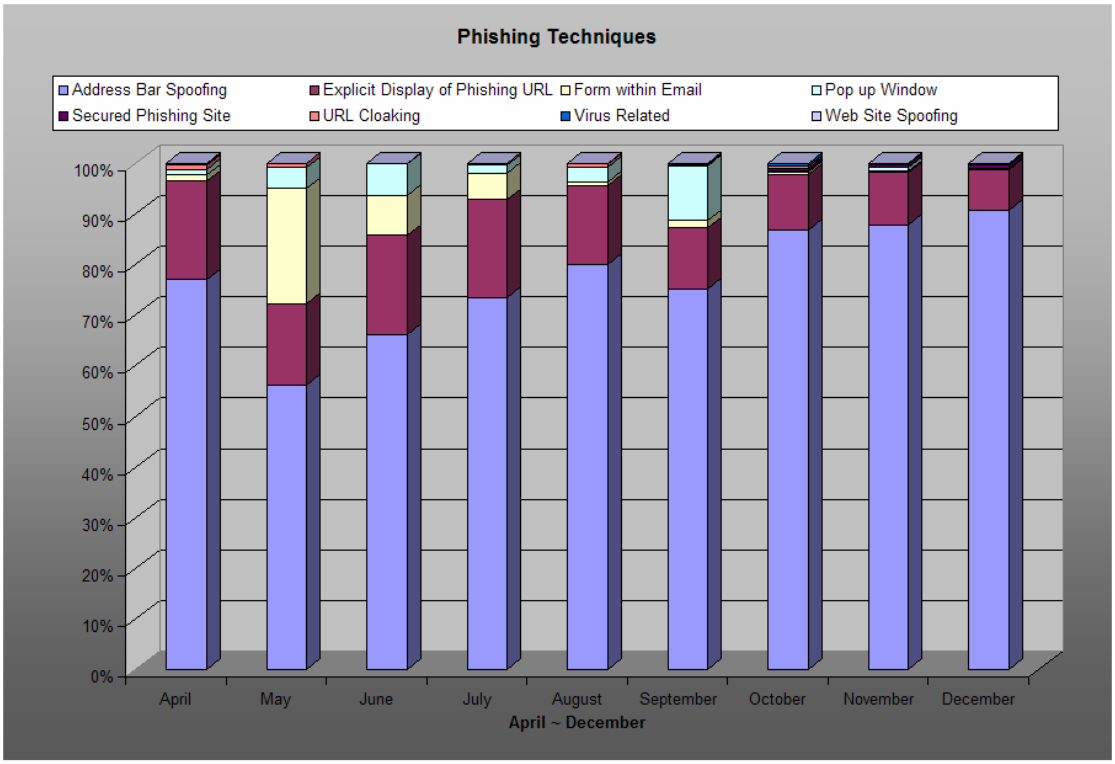
Otra sorpresa es la importante caída del spam en chino, un buen presagio para la región, considerada un área de crecientes oportunidades económicas y cientos de nuevos usuarios online. En septiembre de 2004, China reconoció su problema con el spam y comenzó a trabajar con los principales actores de la industria para reducirlo. En cambio, el spam en japonés continuó su firme subida, situándose unos cuantos puntos por encima de la marca del año anterior.

El asunto del spam



Como en años anteriores, el spam siguió siendo un problema significativo. Sin embargo, hubo cambios importantes en su contenido. En 2005, *el spam comercial* cayó cerca del 50% sobre el año anterior, mientras que *el spam sobre temas académicos y educativos* se incrementó un 100%. *El spam de temática financiera y de salud* bajó unos cuantos puntos respecto al último índice, con *asuntos de salud* reduciéndose hasta un 70%. *El juego y los juegos de azar* suman ahora el 22% del spam, un fuerte contraste frente al escaso 1% visto en 2004. Igualmente, *el spam con contenidos para adultos* creció hasta el 21%, frente al 6% de años anteriores.

Phishing: ¿Qué tenemos aquí?



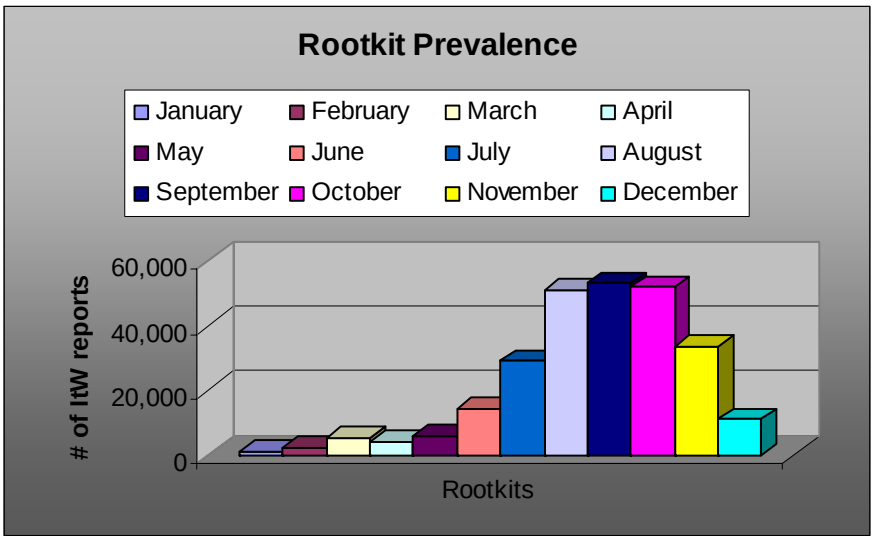
Los ataques de phishing son una subcategoría bajo el paraguas del spam. Las técnicas observadas son aplicables a cualquier idioma y a diversas categorías –aunque la mayoría tienen naturaleza financiera o comercial–. *La falsificación de la barra de direcciones* suma un 81% de todos los ataques de phishing y funciona principalmente en usuarios de Internet Explorer (justificando cerca del 90% de los usuarios en un panorama en el que Microsoft Windows está instalado en el 95% de los ordenadores). Esta técnica hace un mal uso de Active-X cuando las imágenes cubren la URL actual en el buscador mostrando una imagen falsa en la cabecera.

A finales de 2005, *la muestra explícita de la URL de phishing* se ha reducido hasta sólo el 13% de los ataques, comparado con el 76% a principios de año.

El uso de *scripts y formularios rellenables* incrustados en correos con formato HTML sumó cada uno menos del 3%, creciendo dos puntos desde el año anterior.

Los cambios y giros en las técnicas de phishing parecen ser resultado de una evidente combinación de vulnerabilidades de correo que podrían permitir la ejecución automática sin intervención del usuario en los ordenadores de las víctimas –todo lo necesario es que uno abra un mensaje en su formato HTML original para que le acarree todo tipo de problemas–. Algunos de estos problemas son atribuidos incluso al spam y al adware, cuando se considera el crecimiento del grayware y se investigan las vías de infección.

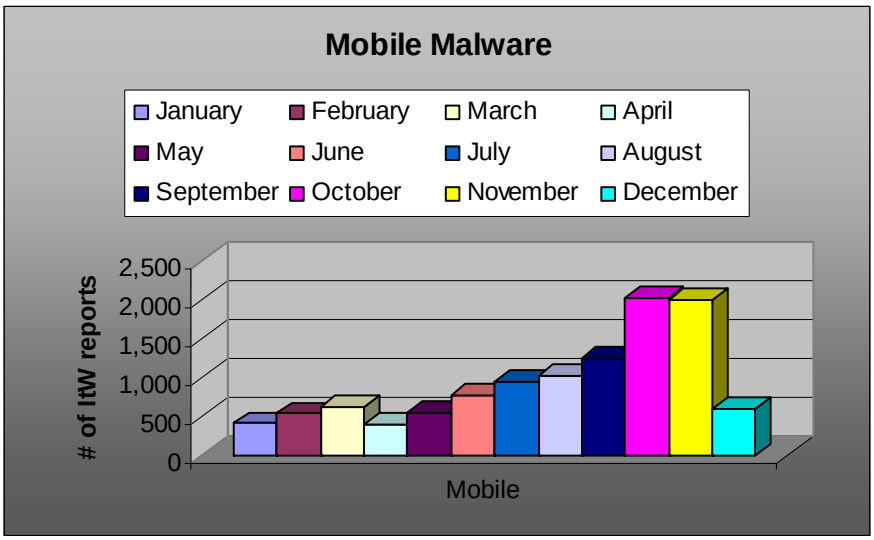
Rootkits



Las funciones asociadas a los rootkits de esconder la presencia de actividad maliciosa no son nada nuevo. Para sobrevivir, los virus y los gusanos de red controlaban en los buenos tiempos los lapsos temporales de la memoria, cuando la memoria de los ordenadores era escasa y el almacenamiento de ficheros era muy caro. En los años siguientes los virus se ejecutaban desde los sectores de arranque del ordenador, dándoles un acceso privilegiado al sistema operativo –permitiéndoles así la capacidad virtual de mantener un cierto bloqueo de la memoria para su uso sin interferir en las operaciones normales de la máquina–. Este tipo de código malicioso de ocultación de procesos ha sido utilizado durante cierto tiempo, pero ahora su uso ha llegado a ser común una vez más después de varios años de letargo. En gran medida, los rootkits que nos encontramos a finales de 2005 estaban emparejados con diferentes tipos de amenazas –todas encaminadas a lograr beneficios económicos como resultado final–. Trend Micro espera que esta tendencia se mantenga en 2006.

Detectar la existencia de uno o varios rootkits en un sistema no es fácil, y el análisis del malware oculto puede ser dificultoso. Consecuentemente, el tiempo en que ejercen de parásitos se puede incrementar exponencialmente. A esto hay que añadir que la mayoría de los rootkits son desarrollos de código abierto y están disponibles de inmediato para cualquiera. Trend Micro descubre continuamente más sobre estas amenazas mientras el uso genera más adeptos entre los autores de malware. Se observó un crecimiento en el uso de rootkits aliados con otras amenazas a mediados de 2005 y es muy probable que esta tendencia continúe en 2006 intentando ocultar spyware y adware.

Las amenazas para móviles



El primer gusano para móviles fue descubierto en agosto de 2004. Etiquetado como SYMBOS_CABIR, utiliza Bluetooth para reenviarse a través de las ondas a víctimas desprevenidas que piensan que han recibido un programa de seguridad y se infectan a sí mismos con la instalación. CABIR y sus variantes operaban originalmente en entornos Symbian 60, presentes en más del 80% de los móviles GSM del mercado. Desde entonces, Trend Micro ha registrado un aumento de cifras de amenazas para móbiles que sacan partido de otras tecnologías de telefonía como los mensajes multimedia (MMS), la capacidad para navegar, así como para descargar adjuntos a los correos electrónicos.

En septiembre de 2005, SYMBOS_CARDTRP.A intentó ser el primer gusano para móviles multiplataforma, dejando gusanos en las tarjetas de memoria infectadas, como WORM_WUKILL.B. Cuando la tarjeta se introduce en un ordenador con Windows, tiene la capacidad de abrir una puerta trasera en el sistema y de distribuir dos gusanos más a través del ordenador. A pesar de que el ataque no fue particularmente exitoso, demostró el actual desarrollo de malware para móviles. Si esta tendencia continúa, podemos esperar ver nuevas formas añadidas a los gusanos para móviles, incrementando mucho más su potencial como forma exitosa de ataque.

En un interesante giro de los acontecimientos, durante noviembre de 2005 Trend Micro recibió pruebas de malware para móviles que intentaban recopilar todos los detalles de contacto y enviarse a cualquier otro teléfono que estuviese al alcance. Trend Micro le llamó SYMBOS_PBSTEAL.A. Este malware fue la primera amenaza para móviles que robó información.

En este momento no está claro lo populares que pueden llegar a ser en el futuro entre los autores de malware los ladrones de agendas telefónicas y los que depositan malware. Sin embargo, es improbable que esta sea la última vez que lo veamos. Por lo tando, es importante seguir alerta para proteger las tecnologías emergentes – particularmente aquellas destinadas a aumentar el ancho de banda de la conectividad de móviles, como WiFi, EDGE/GPRS, 3G/UMTS y la prometedora WiMax.

¿Cuánto cuestan estas vulnerabilidades?

Threat Name	Vulnerability Discovery	Exploit Window	Outbreak Declaration	Damage Cost**
Bugbear	Thursday, March 29, 2001	550	Monday, September 30, 2002	?
Nimda	Tuesday, October 17, 2000	336	Tuesday, September 18, 2001	$635,000,000
SQL Slammer	Wednesday, July 24, 2002	185	Saturday, January 25, 2003	$ 1.3 billion
Slapper	Tuesday, July 30, 2002	46	Saturday, September 14, 2002	?
Blaster	Wednesday, July 16, 2003	26	Monday, August 11, 2003	$ 2 billion
Sasser	Tuesday, April 13, 2004	17	Friday, April 30, 2004	$ 3.5 billion
Zotob	Tuesday, August 09, 2005	4	Saturday, August 13, 2005	$ 500,000,000+

Threat Name	Vulnerability Discovery	Exploit Window	Outbreak Declaration	Damage Cost**
Bugbear	Thursday, March 29, 2001	550	Monday, September 30, 2002	?
Nimda	Tuesday, October 17, 2000	336	Tuesday, September 18, 2001	$635,000,000
SQL Slammer	Wednesday, July 24, 2002	185	Saturday, January 25, 2003	$ 1.3 billion
Slapper	Tuesday, July 30, 2002	46	Saturday, September 14, 2002	?
Blaster	Wednesday, July 16, 2003	26	Monday, August 11, 2003	$ 2 billion
Sasser	Tuesday, April 13, 2004	17	Friday, April 30, 2004	$ 3.5 billion
Zotob	Tuesday, August 09, 2005	4	Saturday, August 13, 2005	$ 500,000,000+

Según las estimaciones de Computer Economics, los costes debidos al daño y recuperación por cada epidemia que tiene éxito se sitúan en los miles de millones de dólares. De hecho, la estimación más reciente para cada año de los siguientes se situará en al menos 11.000 millones de dólares estadounidenses, dados los actuales niveles de propagación de las amenazas. El incremento de costes se debe a la reducción de la ventana de tiempo entre el descubrimiento de la vulnerabilidad y el momento en que se escribe un exploit y se incluye en un gusano de rápida difusión. Esto significa menos tiempo para probar y asegurar la calidad de los parches en sistemas paralelos en un esfuerzo por asegurar que los efectos secundarios no ocurrirán en los sistemas en uso actualmente.

2005: ¿Qué es diferente ahora?

En 2005, la gran mayoría de las amenazas estaban inspiradas por el beneficio económico, en lugar de la notoriedad o el derecho a presumir, que era el comportamiento habitual en años precedentes. Los atacantes acosaron a los usuarios con la intención de robarles información. Así, inventaron todos los trucos que pudieron, como modernos artistas de la estafa en un escenario mundial de millones de víctimas potenciales.

El giro en la motivación cambió el tejido mismo del escenario de la amenaza. El nuevo malware está motivado principalmente por el beneficio económico. Estamos observando cada vez más ataques enfocados a determinadas compañías y sus usuarios, o a un grupo particular con un vínculo común. Troyanos empaquetados de forma especial son difundidos a través de spam a estos objetivos con la esperanza de que los usuarios no precavidos caigan en la trampa. Favorecer este tipo de pequeña distribución en oposición a las grandes infecciones de gusanos aumenta en gran medida las probabilidades de que el malware pase desapercibido durante un mayor periodo de tiempo. Esta estrategia permite reunir más información confidencial antes de que el troyano sea detectado y eliminado.

El año también fue testigo de una nueva clase de ataque, que Trend Micro llama "phishing espía". Tomemos como ejemplo un ataque constituido por estafas de phishing y ataques de pharming donde el objetivo son los bancos online, las instituciones financieras y otros sitios que requieren contraseña. En el "phishing espía" el autor esparce mensajes de correo-e con un troyano o un enlace para descargar el troyano. Una vez descargado y ejecutado, ya sea manualmente o a través de la explotación de una vulnerabilidad, este malware controla el tráfico web hasta que detecta el acceso a la página objetivo. Cuanto esto ocurre, envía cualquier dato de conexión o confidencial que se utilice al atacante. Ha habido diferentes variantes dirigidas a entidades específicas o a webs de compañías afines, todas con el mismo objetivo. El texto del correo spam puede estar relacionado con la compañía objetivo, o emplear otras formas de ingeniería social, similares a aquellas utilizadas por los virus tradicionales. En cualquier caso, el efecto es más peligroso que el del phishing tradicional, ya que no tiene que confiar en engañar al usuario para que visite un sitio falso. Y dado que es mucho más fácil desde el punto de vista técnico que lanzar un ataque de pharming, incluso los conocidos como "script-kiddies" (novatos) pueden lanzar, potencialmente, un ataque exitoso. El *spy-phishing* comienza, de hecho, en la página real del banco, cuando el usuario se registra. Y una vez que el usuario introduce su información, accede al sitio deseado sin ninguna interrupción, por lo que no hay ningún comportamiento inusual que pueda alertarle de un problema potencial. La única diferencia es que la información del usuario también ha sido desviada a un tercero, que ahora tiene el poder de usarla para realizar actividades ilícitas.

Una tendencia importante en 2005 fue el uso de hecho de amenazas combinadas. Motivados por el beneficio económico, los atacantes no han limitado sus actividades al robo de credenciales bancarias y de comercio electrónico. Muchos también infectan los sistemas de las víctimas con software espía, adware y otro grayware. Si el atacante introduce spyware y adware de terceros, pueden participar en campañas de marketing que ofrecen comisiones por cada unidad instalada. Así, cuantos más usuarios infecte el atacante, más dinero ganará. Los ataques multi-troyano comienzan con un programa de descarga (downloader/dropper), cuya única función es traer más archivos al sistema y acaba instalando un surtido de otros troyanos, adware o spyware. No es raro verlo hoy en día, y está directamente enlazado con el cambio en la motivación expuesto antes.

Cada una de las técnicas antedichas comparte un elemento común: cuanto más tiempo permanezcan camufladas, mayores son sus expectativas de éxito. Robar información es una actividad que tiene utilidad limitada, si sus habilidades están activas sólo durante un día. Cuanto más tiempo permanezcan a la escucha, mayor probabilidad tendrán de obtener información valiosa. Esta necesidad de evitar la detección tuvo dos efectos inmediatos en el paisaje de la amenaza en 2005:

1. Los autores de código malicioso aprendieron, ya en el año 2003, a utilizar diferentes compresores para enmascarar la estructura interna de los programas binarios. Estos programas comprimen los archivos ejecutables para hacerlos más pequeños, pero también los hacen diferentes desde el punto de vista de la detección por parte de escáneres tradicionales que no utilizan emulación de código y análisis de comportamiento. Utilizar esta capacidad como un factor de camuflaje puede prolongar potencialmente la vida del programa, mientras que los fabricantes de antivirus necesitan obtener múltiples muestras para detectar

correctamente la variante de código malicioso. Los atacantes lanzan distintas oleadas del mismo troyano malicioso, cada una comprimida con un compresor diferente, si no usan una combinación de todos los diferentes tipos.

2. Los atacantes han buscado otros métodos de camuflaje y han encontrado el más efectivo de todos: los rootkits. Hacia finales de 2005, los rootkits estaban siendo utilizados como la última arma para ayudar a encubrir la actividad del malware y el grayware. Los rootkits modifican el comportamiento del sistema operativo para ocultar determinados procesos, archivos, carpetas y entradas de registro. Esto da un poder a las aplicaciones maliciosas mientras hacen enormemente más complicado detectarlas y eliminarlas. Puesto que los rootkits están disponibles públicamente –muchos utilizan estándares de fuente abierta– incluso los escritores que no poseen las habilidades técnicas requeridas para producir un rootkit pueden utilizarlos porque el trabajo ya lo había hecho para ellos. Como los rootkits se vuelven cada vez más populares entre los escritores de malware, las compañías de seguridad de contenidos deben perfeccionar sus herramientas para detectarlos. Trend Micro ha vigilado los rootkits como parte de los tándem de bot y troyano con una regularidad creciente, particulamente en el tercer trimiestre, en el que fueron descubiertos más de 150.000 ordenadores que habían sido afectados.

Otra tencencia importante el año pasado fue el aumento de la modularidad del malware empleado para los ataques. Los gusanos bot se han desarrollado hasta ser el malware de más rápida difusión, gracias, principalmente, al hecho de que se han convertido en desarrollos de fuente púbica, construyendo una moda modular. Cualquiera puede descargar el código fuente de estos bots, seleccionar los módulos que utilizará y crear una nueva variante.

Añadiendo nuevos módulos para gusanos bot, los escritores maliciosos han elevado a los bots, tradicionalmente un ataque de difusión lenta, a una nueva categoría: la del malware más flexible de todos. Pueden presentarse como gusanos de correo, gusanos de red, gusanos P2P, o como todos ellos al mismo tiempo. Con este aumento de la flexibilidad, han probado algo más este año: pueden añadir nuevos explotadores de vulnerabilidades tan pronto como sean publicados en la Red. En octubre de 2000, el gusano NIMDA empleó casi un año para explotar una vulnerabilidad publicada; en 2004, el lanzamiento de SASSER acortó esa cifra a 117 días; pero en 2005, ZOTOB dibujó un paisaje alarmante en el que empleó sólo 5 días desde el anuncio de la vulnerabilidad hasta el momento en el que se añadió un explotador de la vulnerabilidad al código del gusano.

Ahora que los gusanos bot se han convertido en la navaja suiza de todo el malware con sus habilidades de difusión por correo electrónico, de explotación de vulnerabilidades de red, de añadir rootkits y todo lo demás, las cifras de detección van al alza. Las principales familias bot tienen cientos de variantes diferentes documentadas y las detecciones vinculadas a ellas se cuentan por millones.

El uso de las funcionalidades de los bots en gusanos no ha cambiado respecto al pasado. Los propietarios de redes bot (o “redes zombis”) los utilizan para subir spyware y adware, robar información, crear plataformas de spam y lanzar ataques distribuidos de denegación de servicio contra terceros. Todos estos ofrecen beneficio económico al

dueño de la red en proporción al número de víctimas que tenga. Una vez que la red bot ha alcanzado un tamaño considerable, puede ser vendida o sus partes pueden ser alquiladas para usos maliciosos: como servidores proxy para el envío de correo spam, para el robo de datos privados o para introducir spyware o adware en los equipos infectados.

Desde 2002, los gusanos bot han estado creciendo exponencialmente, y en 2005 puede que hayan alcanzado su cima. Se están convirtiendo cada vez en más complejos y peligrosos y han demostrado su capacidad para utilizar las vulnerabilidades de red tan pronto como son encontradas. El año pasado, la policía y las unidades de investigación descubrieron redes bot de más de 200.000 víctimas en todo el mundo. Los bots se han convertido fácilmente en una de las amenazas más formidables con las que contar y posiblemente poseen el mayor potencial de daño.

¿Qué esperamos en 2006?

Dado el actual escenario de la amenaza, esperamos una continuación de muchas tendencias ya establecidas durante el pasado año:

- Los informes sobre spy-phishing continuarán creciendo mientras los creadores de phishing aprovechen la longevidad que el código parásito le concede al malware actualmente.

- Las redes bot (o redes zombi) aumentarán sus funciones a través del uso de rootkits y del acercamiento entre el descubrimiento de vulnerabilidades y sus técnicas de explotación.

- El phishing a medida se convertirá en la principal preocupación para las compañías.

- El spam se introducirá en otras lenguas locales y dialectos, pero se ceñirá a las cultura más rentable, con mayor capacidad de pago.

- Se utilizarán una mayor variedad de empaquetadores para comprimir y encriptar malware y evitar su detección.

- Los protocolos de mensajería (incluidos IRC, IM y P2P) continuarán abriendo túneles a través de los cortafuegos y serán usados como vías de infección.

- Los periodos de tiempo de las vulnerabilidades seguirán acortándose, razón por la que la industria de seguridad deberá garantizar soluciones más proactivas.

- La difusa línea entre el grayware y el malware hace más fácil a los fabricantes de seguridad establecer criterios para eliminarlo, fortaleciendo sus posiciones sobre los derechos de los usuarios a deshacerse de estas amenazas.

- **Crecimiento de bots y redes bot (o redes zombi).** Mientras su uso recompense a sus creadores con enormes ganancias ilegales, esperamos ver un aumento este año en las cifras de detección de nuevas variantes. Las bases de equipos instalados se consolidarán lentamente mientras que todos los viejos

bots no detectados se reemplazarán por variantes más competitivas o mejoradas.

- **Aumento de los métodos de camuflaje.** Predecimos un crecimiento de rootkits y otras tecnologías de ocultación. La técnica rootkit ha sido más y más popular y permanecerá en un futuro cercano. Como atenuante, cuando Microsoft lance su nuevo sistema operativo Windows este año, los programadores de rootkits podrían necesitar cambiar sus estrategias para el nuevo entorno. Esto no afectará a los actuales rootkits diseñados para las versiones de Windows más populares hoy en día.

- **Más phishing-espía (spy-phishing) y ataques dirigidos** parecidos a las técnicas de phishing. Utilizar trucos similares al phishing y otros de ingeniería social puede aumentar el impacto a nuestra base. También esperamos, a menor escala, más ataques dirigidos, que pueden ayudar a los atacantes a recibir información directa y a permanecer ocultos durante más tiempo. Ambos tipos son peligrosos, porque tienen como objetivo información confidencial a diferencia de la simple destrucción que caracterizaba los ataques en el pasado.

- **Prevalencia de adware y spyware.** Los programas de publicidad han sido muy comunes durante mucho tiempo. Las campañas de publicidad generan grandes cantidades de dinero cada año. Muchas compañías de software de publicidad podrían pagar alegremente para ayudar a instalar sus productos de adware en tantos PCs como fuese posible. Aunque ha habido intentos gubernamentales parar regular y parar esta práctica, ésta ha ido siempre en aumento desde el principio. Ahora, incluso los escritores de código malicioso optan por incluir adware en sus creaciones para aumentar todavía más sus beneficios. Este comportamiento es probable que mantenga su tendencia de crecimiento actual.

Consejos a los usuarios para evitar ser afectados por las tendencias de malware en 2006

Para compañías y corporaciones:

- **Desplegar métodos de escaneo de HTTP.** Muchas amenazas modernas utilizan el protocolo web para difundirse. Es altamente recomendable poner en marcha un sistema de escaneo de virus Web, preferiblemente en la misma línea que los administradores comenzaron a desplegar el análisis de correo hace tiempo. Detectar y parar amenazas antes de que ningún fichero infectado pueda alcanzar al usuario final añade una nueva capa de protección en las infraestructuras de red corporativas. La protección contra el software espía en la capa de red es un añadido porque estas amenazas utilizan exclusivamente HTTP para introducirse en el entorno corporativo.

- **Bloquear protocolos innecesarios para entrar en la red corporativa.** Los más peligrosos son los protocolos de comunicación MI y P2P y el chat IRC. Estas dos son parte del arsenal de armas de los bot para propagarse y comunicarse con el dueño de la red zombi y deberían ser rechazadas por el cortafuegos corporativo.

- **Desplegar sofware de escaneo de vulnerabilidades en la red.** Estar constantemente actualizado puede minimizar el impacto de cualquier nueva vulnerabilidad de red y disminuir el riesgo de ser infectado por esta clase de gusano.

- **No dar privilegios de administrador a todos los usuarios.** El más peligroso de los privilegios es “cargar y descargar drivers para dispositivos”. Esta es la medida más recomendable para prevenir ser afectado por rootkits. Normalmente, los rootkits se implementan como drivers para dispositivos, para tener acceso al interior de todos los sistemas operativos. Rediseñar la política de usuarios para limitar este tipo de privilegios puede ser una de las vías más útiles para asegurar una red. Si el administrador priva a los usuarios de derechos, consigue una bonificación añadida: el código malicioso agresivo no podrá cerrar los procesos de los antivirus.

- **Desplegar un escaner anti-spyware corporativo.** Dado que se están convirtiendo en amenazas prevalentes en los negocios, los administradores necesitan poner en marcha software específico para detectarlas y pararlas.

- **Educar a los usuarios; imponer una estricta política de seguridad en la red.** No sólo tener software y sistemas de defensa ayuda a luchar contra el malware. La mayor parte del tiempo, el usuario necesita realizar acciones de algún tipo para infectar la máquina. Sea una página web que instala spyware o un correo infectado, el usuario necesita conocer con antelación las vías de ataque del nuevo malware. La conciencia de los usuarios es la clave para una red limpia, y los administradores deberían llevar a cabo iniciativas de educación para mantener a los usuarios informados y protegidos con conocimientos actualizados de tecnologías de malware. Esto es especialmente importante con nuevos usuarios, dado que son los objetivos típicos de los escritores de malware.

Para usuarios domésticos:

- Tener cuidado con páginas que exigen la instalación de software. No permitir la instalación de nuevo software desde el buscador a menos que confíe absolutamente tanto en la página web como en el proveedor del software.

- Escanear con software antivirus y anti-spyware actualizados cualquier programa descargado de Internet. Esto incluye cualquier descarga desde redes P2P, a través de la web y de cualquier servidor FTP a pesar de la fuente de la que proceda.

- Tener cuidado con correos electrónicos inesperados y de aspecto extraño, cualquiera que sea su emisor. No abrir nunca archivos adjuntos ni pulsar enlaces contenidos en estos mensajes de correo.

- Activar la función de “Actualización Automática” en Windows e instalar las nuevas actualizaciones tan pronto como estén disponibles.

- Tener siempre un servicio de análisis antivirus en tiempo real. Controlar regularmente que se actualiza y que el servicio funciona.

Acerca de Trend Micro
Trend Micro es líder en software y servicios antivirus para redes y en seguridad de contenidos en Internet. La corporación, con sede en Tokio, cuenta con unidades de negocio en todo el mundo. Los productos de Trend Micro se venden a través de distribuidores corporativos de valor añadido y proveedores autorizados de servicios. Para más información y para solicitar muestras de cualquier producto de Trend Micro, visite: www.trendmicro-europe.com

# # #

Relaciones públicas y prensa

Javier Fraile / Francisco Soto
jfraile@inforpress.es / fsoto@inforpress.es
Tel: +34 91 564 07 25

Directora de Márketing y Comunicación Trend Micro

Mariana Piñeiro
mariana_pineiro@trendmicro.es
Tel: +34 91 369 70 30 / 649 981 554