Asociación de Internautas

El virus 'Klez' se expande y el CAT lo cataloga ya de "epidemia"

Fuentes del Centro de Alerta Temprana (CAT) sobre virus informáticos, órgano dependiente del Ministerio de Ciencia y Tecnología (MCYT), señalaron hoy a Europa Press que su propagación en las últimas horas lo asemejan al último virus de gran difusión, el 'Sircam', que causó estragos en el último trimestre del pasado año y que todavía hoy sigue provocando muchas infecciones, por lo que ya cabe referirse a una "epidemia".

Recomendaciones de la Asociación de Internautas

En España, el gusano 'Klez.G' ha sido detectado en más de tres mil correos electrónicos en el día de hoy, según datos del CAT, que apuntó que su crecimiento en las últimas horas ha sido "espectacular". Además, si se contabilizan las más de dos mil infecciones de su variante anterior (Klez.G), el gusano es el responsable de casi una cuarta parte de los virus detectados hoy por el CAT y ha sido detectado por entre el ochenta y el noventa por ciento de los centros de la Red Iris que miden las incidencias en España.

Por su parte, Message Labs, que ayer apenas había detectado unas 1.500 copias del 'Klez.G' frente a las más de 15.000 del 'Sircam', se está viendo hoy desbordado y afirma que las estadísticas de su web van retrasadas debido a la avalancha de detecciones. Así, a media tarde de hoy había detectado ya más de catorce mil copias del gusano, frente a dos mil del 'Sircam' y poco más de mil del 'Klez.F'.

De igual forma, en un muestreo realizado esta mañana por una docena de ordenadores personales de la Asociación de Internautas (AI), se contabilizaron más de un centenar de virus, de los cuales el 71 por ciento correspondía al 'Klez' y el 21 por ciento al 'Sircam'. Según el CAT tiene una peligrosidad media y su daño y dispersabilidad son altos.

VULNERABILIDAD

El 'Klez.G' es un gusano que utiliza su propio motor SMTP para propagarse vía correo electrónico, siendo capaz de infectar carpetas y directorios compartidos en la red local accesibles desde el puesto infectado. Aprovecha una vulnerabilidad del navegador 'Internet Explorer 5' para difundirse y rastrea el equipo en busca de cualquier dirección de 'e-mail' a la que infectar.

Este gusano intenta eliminar antivirus y 'software' de seguridad del PC infectado, dejándolo indefenso frente otras agresiones. El código aprovecha un agujero de seguridad para ejecutarse con sólo abrir el mensaje, sin necesidad de ejecutar el archivo adjunto.

Se trata de una nueva variante del virus aparecido en el último trimestre del pasado año. Cuando es ejecutado realiza copias de sí mismo en el directorio 'WindowsSystem' con el nombre 'WINK?.EXE', donde el asterisco será una combinación aleatoria de caracteres. Después creará una entrada en el registro para ejecutarse automáticamente con cada reinicio.

El virus es capaz de expandirse a través de una red local (LAN) hasta las carpetas y directorios visibles como compartidos desde la máquina infectada y que tengan privilegio de lectura/escritura para copiarse a sí mismo con un nombre generado aleatóriamente y borrar ficheros con extensiones '.EXE', '.PIF', '.COM', '.BAT', '.SCR' y '.RAR'. Ocasionalmente el nombre del fichero puede tener doble extension. DIVERSOS ASUNTOS

El asunto del correo que envía está compuesto de forma compleja por frases muy variadas en inglés. Entonces construye un correo HTML, que contiene una copia del gusano codificado en base64, y genera aleatoriamente el nombre del adjunto.

Entonces manda comandos al servidor SMTP para crear y enviar correo electrónico. El asunto y el cuerpo finales del correo pueden ser compuestos aleatoriamente. Se aprovecha de la conocida vulnerabildad del navegador 'Internet Explorer' que permite ejecutar datos MIME incrustados, de forma que si se recibe con 'Outlook Express' y el 'Explorer' no está parcheado, se ejecuta al visualizar el mensaje.

MEDIDAS

Con ocasión de esta epidemia, la AI emitió hoy un comunicado en el que reitera que "una de las medidas más sencillas y más efectivas" es no ejecutar nunca un fichero adjunto de un correo electrónico mediante el procedimiento de pulsar dos veces directamente sobre él, ni aunque provenga de gente conocida.

Añade que al pulsar sobre lo que parece que es una imagen, un videoclip, un documento de texto, etc., en vez de abrir el programa que lee el archivo, se ejecuta el código del virus con lo que la infección y sus consecuencias son ya irremediables.

La AI recomienda guardar el fichero adjunto, ejecutar el programa que debe abrir el fichero y desde ese programa abrir el fichero adjunto que se ha guardado. Si se trata de un virus, el programa no podrá abrirlo, con lo que se evitará la infección.

En cualquier caso, la asociación apunta que es "imprescindible" tener un antivirus actualizado --"aunque no sea sinónimo de protección absoluta"--, y lamenta que otro "gran problema" es el envío y recepcion de correo con HTML, puesto que el programa más utilizado actualmente --'Outlook Express'-- no dispone de la opción de recepción de correo en modo 'sólo texto plano' si se recibe el mensaje en formato HTML, aunque sí se puede enviar de esa forma.

Por último, la AI afirma que una "posible" solución a la expansión de las infecciones por correo electrónico es la de instalar un servidor de correo saliente en el ordenador, en vez de utilizar el del proveedor de servicios. Con ello asegura que se podría conseguir "fácilmente" que no se envíe correo a no ser que se ejecute el servidor y de este modo se evitaría propagar los virus aunque ya se esté infectado.

Reproducido de Europa Press
