This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

PRACTICAS IDÓNEAS DE MAAWG PARA EL USO DE UNA PARCELA CERCADA

Criterios de entrada/salida, de reparación y de información del abonado

Introducción

Visto el aumento de los abusos de red por parte de los abonados, los proveedores de servicios de Internet (PSI) han tenido que aplicar medidas más proactivas a fin de proteger sus redes y el tráfico cualquiera sea su procedencia. Los programas automáticos o robots ("*bots*") y las colecciones de software robots ("*botnets*") son mecanismos a los que recurren cada vez más los remitentes de correo basura y los piratas para hacer un uso indebido de la red mediante la propagación de correo indeseado, virus y otras formas de software nocivo. Este último se introduce subrepticiamente en los ordenadores personales de los abonados sin que lo sepan y, en consecuencia, los usuarios finales (abonados) son el blanco constante como cómplices involuntarios de esas redes maliciosas.

Para cumplir mejor el cometido de MAAWG de proteger la mensajería electrónica de usos indebidos o abusos en línea, la Subcomisión Botnet/Zombie de MAAWG recomienda las siguientes prácticas idóneas en lo que se refiere a la creación de una parcela cercada, entendiendo por tal un entorno que controla la información y los servicios que un abonado puede utilizar y a qué redes tiene el acceso autorizado. El principal objetivo de estas prácticas es ayudar a los usuarios finales a reconocer y suprimir los programas no deseados o nocivos que residan en sus ordenadores personales, y detener la utilización de la red con fines abusivos. Salvo indicación en contrario, los PSI son responsables de la aplicación de todas las recomendaciones.

Los usos y definiciones de palabras clave como DEBEN, DEBERÍAN y PUEDEN, en este documento han de interpretarse como se indica en RFC 2119.

I. Los criterios de entrada a la parcela cercada y de salida de ésta deben ser concisos

A fin de informar a los usuarios acerca de los riesgos y de toda la problemática asociada a la infección de un ordenador personal por programas malignos, los PSI PUEDEN crear una parcela cercada para nuevas cuentas de usuario o cualquier cuenta que les parezca arriesgada o generadora de tráfico sospechoso. Los criterios de entrada a la parcela cercada y de salida de ésta deben ser claros y concisos de manera que el usuario final los comprenda.

Resumen de las recomendaciones:

a) DEBEN presentar una clara notificación del posible problema; por ejemplo, el de hacer uso de la red sin respetar la Política de Uso Aceptable (AUP). DEBEN también dar una explicación con respecto a la notificación y describir el proceso recomendado para reparar o eliminar los programas malignos que haya en el ordenador.

b) PUEDEN redireccionar HTTP [80] a la correspondiente dirección web o página web en cuarentena, respectivamente.

c) **PUEDEN redireccionar el comando de "*botnet*" y el control de tráfico hacia un sistema trampa de detección para análisis.**

d) **DEBERÍAN dirigir todos los SMTP [25] salientes al Agente de Transferencia de Mensajes (MTA) que actúa como zona de cuarentena o máquina trampa.**

e) **DEBERÍAN permitir el escape instantáneo sobre la base de la confianza. La confianza se puede demostrar a través de una acción que indique un ordenador personal limpio o de una solicitud de utilizar la red "como está" por un periodo de tiempo configurable.**

f) **PUEDEN dar salida siempre y cuando se hayan descargado e instalado algunos programas de limpieza o seguridad aprobados por los PSI.**

g) **El PSI PUEDE utilizar medidas para evaluar la reputación de los abonados (lo que se determina utilizando técnicas de detección tales como filtros de contenido, inspección detallada de paquete, y pautas de comportamiento y utilización) para iniciar eventos de entrada a la parcela cercada o de salida de ésta.**

h) **El PSI PUEDE utilizar tecnologías para identificar automáticamente la posición de seguridad del abonado como se indica en los programas de cliente abonado instalados y seguros.**

II. El proceso de reparación debe ser práctico para el usuario final

Puesto que los PSI se siguen esforzando para proteger sus redes y abonados contra los usos abusivos, es importante que procedan de tal manera que no resulte excesivamente engorroso para el usuario final. A fin de recuperar la inversión, el PSI puede optar también por poner a disposición medios de reparación que implican un coste para el usuario final. Esas herramientas DEBEN ponerse a disposición a través de un medio que concuerde con el entorno característico del PSI. Además, la parcela cercada DEBE permitir el acceso a direcciones web de modo que el usuario final pueda descargar parches y actualizaciones de programas esenciales y aplicables, mediante acceso directo o mecanismos de conexión de aproximación indirecta. (Esto hace posible que el proveedor o el ASP contratado ofrezca reparación a través de un único portal, como lo hace Microsoft con su Windows Update y las múltiples descargas que el nuevo controlador inicia en nombre del usuario.)

Resumen de las recomendaciones:

a) **DEBEN poder ofrecer, gratuitamente o mediante el cobro de una tasa, alternativas de reparación (o enlaces con herramientas en línea existentes).**

b) **DEBEN presentar información que se pueda reconocer y que acredite la experiencia en calidad de PSI oficial para el proceso de notificación y reparación. Esa información incluye, por ejemplo, datos como un número de cuenta o la respuesta a la pregunta secreta.**

c) **DEBEN indicar en detalle como ponerse en contacto con el servicio de ayuda al cliente.**

d) **DEBERÍA no ser necesario el rearranque del ordenador personal del usuario final para que tenga lugar el proceso de reparación.**

e) **DEBEN indicarse los enlaces a URL y dominios que ayuden a resolver la situación no deseada con parches OS (sistema operativo) y actualizaciones de seguridad (si procede).**

f) **DEBERÍAN indicar "pulsar para chatear con el centro de asistencia al cliente" o con un tercero que brinde servicio al cliente en nombre del PSI.**

g) **DEBERÍAN proporcionar los datos del PSI o de la persona a contactar en caso de abusos o para solicitar asistencia (por ejemplo, un número de teléfono).**

h) **DEBERÍAN indicar a los usuarios que envían mensajes SMTP [25] nocivos que reconfiguren los MUA para enviar los correos electrónicos salientes por el puerto 587.**

i) **DEBERÍAN dar a conocer soluciones singulares utilizadas por los usuarios en caso de problemas, de modo que los demás usuarios sepan cómo arreglar el problema o tipo de programa nocivo que se sospecha.**

j) **DEBERÍAN incluir un programa de seguridad que sea mínimamente intrusivo; que permita descargas rápidas; que se instale fácilmente sin entrar en conflicto con otros programas de aplicación, por ejemplo con un programa de seguridad ya configurado; que no obligue a reiniciar el sistema; ni exija un barrido completo del computador para detectar y suprimir programas nocivos.**

k) **DEBEN permitir excepciones de redireccionamiento de manera que el usuario pueda utilizar servicios de emergencia en línea.**

III. El objetivo esencial debería ser informar al usuario final

Dado que el usuario final suele ser el eslabón débil de la cadena de seguridad, el PSI DEBERÍA hacer cuanto esté a su alcance para poner documentación a disposición en su dirección web de manera que el usuario final aprenda de modo proactivo cómo reducir los riesgos de infección a causa de programas nocivos. En concreto, se DEBERÍA poner a disposición del usuario final documentación del tipo "las preguntas más frecuentes" (FAQ), vídeos didácticos, guías, y una base de conocimientos con función de búsqueda. Esa documentación, si se facilita, DEBE ponerse a disposición del usuario final mediante un método que sea consecuente con el aspecto y la sensación que presenta la interfaz de servicio al cliente del PSI. Además, la documentación disponible DEBERÍA ser suficientemente amplia como para abarcar aplicaciones disponibles en diferentes tipos de tecnologías de Internet y en diferentes tipos de sistemas operativos para ordenadores (por ejemplo Windows, MacOS, Linux).

Resumen de recomendaciones:

a) **DEBEN presentar información que se pueda reconocer y que acredite la experiencia en calidad de PSI oficial del proceso de notificación y reparación. Esa información incluye, por ejemplo, datos como un número de cuenta o la respuesta a la pregunta secreta.**

b) **DEBERÍAN incluir información del usuario intuitiva a través de las preguntas más frecuentes (FAQ) y guías.**

c) **DEBERÍAN proporcionar herramientas alternativas que se puedan utilizar en el centro de aprendizaje, como un simple vídeo de bienvenida y centros de conocimientos con motor de búsqueda.**

d) **DEBERÍAN proporcionar información didáctica para múltiples tipos de aplicaciones, incluidos el correo electrónico (POP3/SMTP) y la navegación (HTTP).**