Si usted no puede visualizar correctamente este mensaje, presione aquí

Boletín técnico de INDISA S.A.

Medellín, 21 de mayo de 2009 No. 71

EL SOFTWARE MALICIOSO "MALWARE"

Autor: Omar Calvo
Analista de seguridad de Softeam Internacional Panda Security

Malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar el computador sin el conocimiento de su dueño, con finalidades muy diversas. Esta expresión es un término general muy utilizado por profesionales en sistemas para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos usuarios no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware.

El software malicioso ingresa al computador a través de dispositivos de almacenamiento removibles (conectado a puertos USBs), Internet (Correo electrónico, navegación, redes

sociales, mensajería instantánea, entre otros) o a través de redes de datos privadas (empresariales, caseras) o públicas (aeropuertos, redes inalámbricas abiertas).

Las compañías Antimalware detectan a diario aproximadamente el 60% del malware nuevo, es decir, solo se detectan 6 de cada 10, lo cual es aprovechado por los ciberdelincuentes para realizar el ingreso y establecimiento en los sistemas.

Los medios de almacenamiento removibles son el segundo medio de propagación de ataques de malware después de Internet. Todo aquello que se conecte a través de puertos USBs, o de lectores de multitarjetas, es un objetivo para recibir, transportar y ejecutar código malicioso MALWARE.

POSIBLES UBICACIONES DE LOS ARCHIVOS MALWARE

Se establecen en ubicaciones licitas del sistema tratando de mostrarse como archivos no maliciosos a pesar de estar realizando su ataque desde estas, por ejemplo en la carpeta para procesos temporales, en la carpeta de los archivos recibidos del programa de mensajería instantánea, en la carpeta de los archivos del sistema operativo, en la carpeta del entorno de trabajo del usuario, en el directorio principal de los discos duros (C:\, D:\ o en los dispositivos removibles USBs), etc.

También se integran con el navegador de Internet, como un programa requerido por este, por ejemplo como una barra de herramientas (tool bar), un programa necesario para poder disfrutar de contenidos en Internet (videos, sonido, presentaciones en línea, otros). Y en el systray del sistema, donde aparece la hora, para simular una protección que es falsa.

SISTEMAS DE DEFENSA DE LOS ARCHIVOS MALWARE

Muchos de estos softwares maliciosos incluyen sistemas de defensa:

- Atacan la defensa instalada en el sistema, intentando desactivar o bloquear la protección antimalware.
- Detectan cuando están siendo analizados por un sistema antimalware.
- Detectan cuando están siendo ejecutados en sistemas operativos instalados en una máquina virtual.
- Bloquean el acceso a la mayoría de las páginas Web de empresas o servicios de seguridad informática y de análisis de malware en línea (programas antimalware y otros).

FINALIDAD DE LOS ARCHIVOS MALWARE

La finalidad de los archivos malware es obtener ganancias económicas después de ingresar al computador:

- Acceder a la información financiera del usuario, robando sus datos privados.
- Utilizar el computador del usuario para envío de correo SPAM.
- Vender el acceso al computador a través de Internet para almacenar información pirata (pornografía, música, etc.), y para realizar ataques desde este a otros computadores o redes, o realizar fraudes a través de Internet.

LOS SÍNTOMAS PARA SABER QUE HA SIDO ATACADO CON MALWARE

Así como existen los asintomáticos, que a través de sus técnicas de ocultamiento no revelan de manera clara su presencia, también hay algunas señales de alerta a tener en cuenta:

1. Lentitud en el sistema, tareas cotidianas más lentas de lo acostumbrado

2. Aparecen nuevos iconos en el escritorio o al lado de la hora del sistema, sin que el usuario los haya instalado de manera consiente.

3. Cambia la página de inicio del navegador por otra de manera automática.

4. Se observa que hay actividad en Internet y no se tiene abierto el programa de correo, ni el navegador, ni otros programas para realizar descargas.

5. Se desactiva el programa de protección antimalware, en caso de contar con un software de estos instalado.

6. Se desactivan opciones del sistema como: Inicio, Ejecutar, o en el explorador de Windows en la opción "Herramientas" desaparece "Opciones de carpeta…".

7. Al ingresar al navegador cargan páginas de publicidad o de otros contenidos no configurados.

8. Se crean archivos y carpetas automáticamente en los dispositivos de almacenamiento removibles USB.

9. Se alerta la detección de virus en dispositivos removibles que estuvieron conectados en el computador, al conectarlos en otros computadores con un antivirus diferente al instalado en este.

10. Aparecen mensajes de error o programas que solicitan autorización para ejecutarse al inicio del sistema, nunca antes vistos.

11. Aparecen errores en el sistema, relacionados con el bloqueo o detección de un programa que se está ejecutando.

12. Bloqueo al intentar navegar en la Web de fabricantes de soluciones Antimalware.

FACTORES DE VULNERABILIDAD

1. El principal elemento vulnerable es el usuario del computador, para el cual no existen

actualizaciones descargables, ni métodos de corrección de sus fallas de manera automática.

2. Las compañías medianas carecen en su mayoría de procedimientos orientados a mitigar el riesgo implícito en la operación de computadores por usuarios.

3. Falta de capacitación y actualización constante a los usuarios sobre los riesgos implícitos, y el uso adecuado del computador y otras herramientas tecnológicas.

4. No compartir con los usuarios la responsabilidad de las amenazas a los activos de la organización.

5. La apatía o subvaloración del tema de seguridad informática por parte de los altos ejecutivos y usuarios en las empresas.

6. Desconocimiento del tratamiento integral orientado a mitigar los riesgos, obteniendo un riesgo residual con el cual es posible convivir, y tener a salvo los activos de mayor valor para la empresa. No es suficiente con tener un antimalware administrable con protecciones proactivas.

7. La selección de herramientas tecnológicas de seguridad informática que no responden a las necesidades reales de la organización y que no cuentan con el respaldo esperado por el proveedor o el fabricante de la misma.

8. Homogeneidad del sistema operativo.

9. Fallos propios del software y el hardware identificados y menguados por los fabricantes, cuyas actualizaciones no han sido aplicadas por los usuarios o administradores de red.

10. Fallos propios del software y hardware identificados de primera mano por los atacantes.

11. Cuando el usuario tiene privilegios como administrador del sistema, está expuesto a que el Malware logre sus objetivos con la menor resistencia desde el sistema, independientemente de la protección instalada.

Como conclusión no existe solución en el mundo que pueda ofrecer un 100% de efectividad en el reconocimiento de virus y malware en general, pero es muy importante tener en cuenta los siguientes aspectos para una mayor protección:

- Planes de capacitación y actualización constante a las personas, compartir la responsabilidad de la seguridad con estas.

- Procesos escritos claros, acordes a las necesidades reales y riesgos propios del negocio, no solo en el mundo digital, también en el tratamiento de la información vía telefónica o en las conversaciones que se sostienen al interior o exterior de la organización. Manejo adecuado y cuidadoso de medios digitales, de comunicación (acceso remoto a la organización) y computación móvil por fuera de la organización.

- Análisis y selección de un plan que incluya herramientas tecnológicas para el tratamiento integral de los riesgos reales del negocio, en el cual se involucre la alta dirección, las personas al interior de la organización, las familias de los empleados que cuentan con computadores e Internet en sus casas, los proveedores y clientes del negocio.

NOVEDADES

TREINTA MILLONES DE COMPUTADORES INFECTADOS POR LOS FALSOS ANTIVIRUS

- La distribución de más de siete mil variantes de este tipo de malware, que comenzó hace casi un año, hace que millones de internautas pasen alrededor de tres días intentando desinfectar sus equipos.

- En realidad, se trata de una acción para conseguir datos bancarios y estafar dinero, ya que tras el aviso de infección lleva al usuario a páginas de venta de falsos antivirus.

- A un precio medio de 49,95 €, se calcula que los autores de este malware pueden estar ganando más de 10.000.000 de € mensuales, ya que el 3% de los infectados realmente proceden a la compra.

Para mayor información leer la siguiente nota: http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews?noticia=9393

Si usted no recibe esta publicación directamente de INDISA S.A. o si desea recomendarnos a alguien para que la reciba, presione aquí

Para consultar las ediciones anteriores del boletín INDISA On line, puede entrar a http://indisaonline.8m.com/. En esta página se encuentran todos los boletines en formato de página web, para que usted pueda grabarlos en su computador e imprimirlos.

Tel: (574) 2605533
Medellín-Colombia
mercadeo@indisa.com.co
http://www.indisa.com.co/