



Nuevas formas de infección

Caso: 01.06/09

Autor: S21sec

Durante el último mes han aparecido algunos artículos que ponen de relieve que las técnicas de infección empleada por troyanos y demás malware están en continua evolución

El primer artículo http://i.zdnet.com/blogs/core_bios.pdf hace referencia a la posibilidad de instalar un troyano en la propia Bios de la placa base del PC. En este caso, se trata de una demostración que hicieron los investigadores argentinos de Core Security Technologies, Alfredo Ortega y Anibal Sacco en la conferencia de seguridad CanSecWest.

Se trata de una demostración teórica con una implementación a modo de prueba de concepto, mediante la que es posible infectar la Bios con código malicioso. De este modo, es posible sobrevivir a un reinicio del sistema, a una reinstalación del sistema operativo e incluso a un borrado total del disco duro.

Esta técnica es efectiva contra cualquier sistema operativo, incluyendo los virtualizados. No obstante, requiere de permisos de root o de administrador para lograr la infección de la Bios. No se trata de ninguna vulnerabilidad como tal, simplemente aprovecha las debilidades en el sistema de parcheo de la Bios con actualizaciones de firmware para introducir su propio código.

En este otro artículo <http://dronebl.org/blog/8> encontramos un análisis de un gusano que afecta a dispositivos



de red domésticos, como *routers* ADSL. Realmente esta investigación ha generado cierta controversia, pero más allá de cualquier otra consideración, la realidad es que empieza a distribuirse este tipo de malware al que a menudo no se le da la importancia que puede llegar a tener.

En muchas ocasiones, no se consideran los dispositivos de red como vulnerables a malware ni existe software específico de protección para los mismos. La realidad es que todo el tráfico de red pasa por ellos, y en muchas

ocasiones son también los que proporcionan las direcciones de los DNS para todos los PCs conectados a la red. Una infección masiva en este sentido podría comprometer la seguridad de miles de usuarios domésticos sin ni siquiera ser conscientes de estar infectados y con sus máquinas totalmente limpias y actualizadas.

Por lo tanto, lo más interesante de este asunto es que se abre un camino sobre el que se especulaba desde hace tiempo, y que habrá que seguir de cerca. ♦



Análisis gusano W32-Downadup

Caso: 02.06/09 Autor: S21sec

En este apartado vamos a analizar el ataque de un gusano que explota la vulnerabilidad descrita en el boletín MS08-067 de Microsoft, que permite la ejecución de código al enviar una petición RPC especialmente creada, sin necesidad de autenticación previa. A continuación se describe el comportamiento de 3 mutaciones diferentes de este malware.

Análisis técnico

Tras la instalación en el sistema a través de un loader, seguramente descargado a través de un sitio malicioso o a través de un correo electrónico mediante adjunto, el gusano se copia a sí mismo en el directorio del sistema de Windows, en forma de DLL con un nombre aleatorio. Además, se crea un nuevo servicio también con un nombre aleatorio que permite la ejecución de la DLL en cada inicio del sistema. El servicio creado es de la forma siguiente:

Tras la instalación en el sistema a través de un loader, seguramente descargado a través de un sitio malicioso o a través de un correo electrónico mediante adjunto, el gusano se copia a sí mismo en el directorio del sistema de Windows, en forma de DLL con un nombre aleatorio. Además, se crea un nuevo servicio también con un nombre aleatorio que permite la ejecución de la DLL en cada inicio del sistema. El servicio creado es de la forma siguiente:

Nombre: netsvcs aunque también puede ser un nombre aleatorio en minúsculas

Ruta de la imagen:
%SystemRoot%\system32\svchost.exe -k netsvcs



Creando a su vez una entrada en el registro donde se especifica la ruta que se ejecutará al iniciarse el servicio:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netsvcs\Parameters\"ServiceDll" = "[RutaDelGusano]"
```

[RutaDelGusano] es C:\Windows\System32\nombre_aleatorio.dll, también en minúsculas, con un tamaño de

62976 bytes y una fecha aleatoria (al menos en la versión analizada)

Tras la ejecución en un entorno controlado, se puede comprobar cómo el gusano realiza diversas peticiones HTTP para obtener la IP externa de la máquina infectada:

<http://checkip.dyndns.org>
<http://getmyip.co.uk>
<http://www.getmyip.org>



Con esta información deja a la escucha un servidor web en un puerto aleatorio del equipo, enviando una URL del tipo `http://IP_EXTERNA:puerto_aleatorio` al intentar explotar nuevos equipos, y sirviendo desde aquí una copia

de datos de geolocalización de IPs desde:

<http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz>

<http://64.246.48.99/download/geoip/database/GeoIP.dat.gz>

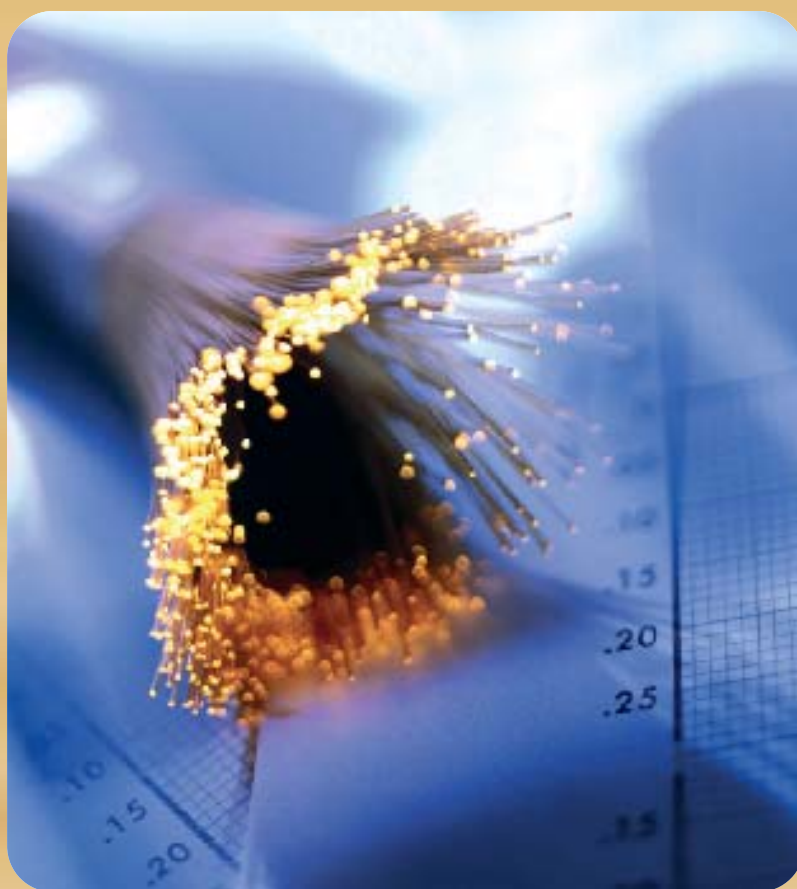
falsos escaneos proporcionará ciertos resultados indicando que es necesaria una limpieza del equipo e invitando al usuario a comprar la versión completa del producto.

También existen evidencias de que se realizan otras peticiones a los dominios siguientes con el objetivo de obtener la fecha actual, generando ciertos dominios desde los que se descarga más malware.

- <http://www.w3.org>
- <http://www.ask.com>
- <http://www.msn.com>
- <http://www.yahoo.com>
- <http://www.google.com>
- <http://www.baidu.com>

Además de todo esto, el gusano coloca ciertos hooks en funciones conocidas del sistema, destacando las colocadas para controlar los movimientos del ratón y las pulsaciones del teclado en el ámbito del proceso `iexplore.exe`, que podrían usarse para el robo de credenciales e información sensible enviadas a través de Internet.

Como ya se ha comentado brevemente en párrafos anteriores, el gusano intenta propagarse a través de la explotación de la vulnerabilidad de RPC en los equipos vecinos. Para ello intenta infectar al segmento local donde se encuentra, probando una a una de forma secuencial la explotación. Si la explotación tiene éxito, el equipo infectado se descargará desde el servidor web instalado en la máquina



del malware en su intento de propagación. De esta forma, no es necesario un servidor externo para expandirse, sino que cada máquina infectada ayuda en esta tarea.

Además, realiza peticiones adicionales HTTP, una de ellas intentando descargarse una base

Otra de las peticiones que llama la atención es la que se dirige hacia la URL:

<http://trafficconverter.biz/4vir/antispyware/loadadv.exe>

Desde aquí el gusano intenta descargarse y ejecutar un falso Anti-Spyware que tras realizar



propagadora una copia de él mismo, continuando así su infección masiva.

También se ha observado capacidad de propagarse buscando unidades compartidas e interacción mediante uPnP con los routers de salida (generalmente ADSL), aunque todavía no se ha podido analizar en profundidad este comportamiento.

Denegación de servicio

Una vez la máquina es infectada, el gusano intenta propagarse masivamente, enviando paquetes de inicio de sesión al puerto 445 TCP con su propio código, lo que provoca un desbordamiento del buffer de la pila TCP/IP de Windows obteniendo una auto denegación de servicio que no permite ningún otro intento de conexión.

Algoritmo

El gusano incorpora un algoritmo para la búsqueda de dominios con su panel de control, a los que envía una petición específica. Como en otros casos de malware, la generación es pseudo-aleatoria para dificultar el cierre de los paneles de control, así como para hacer posible la comunicación aún en caso de no disponer de archivos de configuración o de haberse cerrado los paneles de control descubiertos anteriormente.

Sin embargo, la aleatoriedad no viene dada simplemente por el reloj del sistema en el que se ejecuta el troyano, sino que se trata de algo más complicado. El gusano contacta con uno de los siguientes dominios:

- baidu.com
- google.com
- yahoo.com
- msn.com
- ask.com
- w3.org

Para decidir a cuál acceder, genera un número aleatorio entre 1 y 6 para acceder al índice correspondiente de la anterior lista.

Una vez recibe la respuesta, utiliza la llamada `HttpQueryInfo` con `HTTP_QUERY_DATE` para extraer la cabecera "Date" de la respuesta del servidor. Construye una estructura `SYSTEMTIME` con el día, mes y año, quedando todos los otros campos a 0.

El gusano realiza una conversión de la estructura `SYSTEMTIME` a `FILETIME` mediante la llamada `SystemTimeToFileTime`. Realiza una serie de operaciones matemáticas de coma flotante con dichos valores y finalmente obtiene dos "claves" de 32 bits.

Utiliza dichas "claves" para alimentar PRNG para generar caracteres de dominios. Genera unos 250 dominios al día y añade al final uno de los siguientes TLDs:

- .biz
- .info
- .org
- .net
- .com

Finalmente, elige un número aleatorio entre 1 y 250 e intenta conectar al puerto HTTP del nombre de dominio generado. En caso de tener éxito, envía una petición de la forma:

```
/search?q=[number]&aq=[number]
```

Hasta la fecha, las llamadas a los paneles de control no obtienen respuesta, por lo que se desconoce qué se pretende mediante esta petición y qué tipo de respuesta se puede obtener en un futuro.

Conclusiones técnicas

Como se ha comentado ya, este gusano está haciendo estragos en las redes de todo el mundo debido al uso de una vulnerabilidad reciente y que muy posiblemente esté sin parchear en muchos equipos. A la hora de prevenir este ataque basta con aplicar el citado parche, que se puede descargar desde:

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx>

Una vez que el equipo se encuentra infectado, se deberá aplicar el parche igualmente, y borrar la entrada del registro creada por el gusano, así como la DLL ubicada en el directorio del sistema de Windows. Hay que tener en cuenta que es necesario parar el servicio antes de realizar estas acciones. ♦