

¿La voz sobre IP amenazada?



Recientemente ha saltado la alarma por la posibilidad de que estuviera propagándose un código malicioso a través de Skype. Skype es un sistema que permite llevar a cabo conversaciones a través de la conexión de Internet ya establecida, en un entorno que se asemeja mucho a las llamadas telefónicas. Incluso permite efectuar llamadas a teléfonos normales desde el ordenador, con tarifas distintas a las que supondría una llamada normal.

El problema de un código malicioso para Voz sobre IP (o VoIP según sus siglas en inglés, Voice over IP), abre a los hackers un campo realmente espectacular a la hora de concebir nuevos tipos de malware. De entrada, se podría pensar en códigos maliciosos que utilizaran VoIP para propagarse, tal y como ha hecho el troyano que mencionaba al principio. En el fondo, no es más que buscar un nuevo canal de comunicación. ¿Nuevo? ¡No! Ya hay muchísimos gusanos que tratan de propagarse a través de muchos sistemas de mensajería instantánea. Así que este troyano no ha hecho nada que se hiciera ya desde hace mucho tiempo.

El problema es que realmente se utilicen las características de VoIP para propagar códigos maliciosos. Imaginémonos un determinado flujo de datos a través del canal de audio (quizá en una frecuencia no audible por el hombre) que hiciera caer al sistema de voz, produciendo una denegación de servicios. O que ese mismo flujo de datos pudiera servir para producir un estado en el sistema que facilitara la ejecución de código malicioso. Eso sí sería realmente novedoso a la hora de propagar códigos, no utilizar, como otros cientos de códigos, un sistema de mensajería. Pero eso no es más que un futuro, nada más.

Evidentemente, el poder hacer esto supone un gran esfuerzo de innovación, estudio y desarrollo para los creadores de código malicioso, que dudo mucho estén dispuestos a emprender. La situación en la que nos encontramos ahora ha dejado de ser esa especie de “paraíso” en la que los hackers eran buenos y trabajaban únicamente por alcanzar logros personales que les sirvieran de satisfacción personal. Hoy en día las creaciones de códigos maliciosos, en su práctica totalidad, sirven únicamente para conseguir dinero a los autores, mediante engaños, estafas, robos de identidad, captura de contraseñas...

Las precauciones a tomar ante este nuevo panorama no deben ser muy distintas a las adoptadas hasta ahora por la mayoría de los fabricantes de antivirus de cierta calidad. Un buen sistema de análisis de ficheros, un buen conjunto de firmas de virus en la base de datos y listos. Así se ha estado funcionando hasta ahora, y los resultados son medianamente aceptables, la protección tiene unos valores muy adecuados.

Pero los creadores de virus saben muy bien cómo funcionan los antivirus y, evidentemente, idean nuevas estrategias para poder evitarlos. Y como ahora se enfrentan a una elevada rapidez a la hora de detectar los códigos

¿La voz sobre IP amenazada?



por parte de los proveedores de seguridad, necesitan contrarrestar esa rapidez por otro lado.

La solución adoptada hasta ahora es, por un lado, en envío masivo de códigos (generalmente con las mismas técnicas que se envía el spam), y por otro lado, la renovación constante de los códigos. Si hasta hace poco cada ejemplar podía llegar a contar con una o dos docenas de versiones, se están encontrando actualmente cientos de versiones de un mismo gusano, muchas en un mismo día.

Si esa estrategia se implanta en sistemas de telefonía por IP, como Skype, podemos encontrarlos con muchos códigos maliciosos que cambian muy rápidamente, de manera que las tecnologías utilizadas hasta ahora (las que se basan en firmas de virus) no den de sí a la hora de proteger a los usuarios. Si es necesario actualizar el fichero de firmas con la rapidez necesaria para atajar una propagación de códigos de tipo flash que encima cambian en un mismo día, no hay laboratorio de desinfección de virus que pueda con ello. Para poder prevenir la nueva gama de códigos que intenten aprovecharse de los sistemas de telefonía, no debemos confiar exclusivamente en las firmas de virus. Puede ser lento para los objetivos de los hackers.

Imaginémonos un escenario que puede ser muy común en los próximos tiempos: un usuario tiene en su ordenador (tanto el doméstico como el de la empresa) un sistema de telefonía por IP. En su agenda de contactos del ordenador tiene una entrada que, bajo el nombre "Banco", tiene el número 123-45-67. Ahora un hacker lanza un ataque mediante envío masivo de correo electrónico a miles o millones de direcciones de correo electrónico con un código que simplemente entra en la libreta de contactos del usuario y altera el número que pone "Banco" por el número 987-65-43. El problema ya está creado.

Si ahora a esos mismos usuarios se les manda una carta diciéndoles que hay un problema en su cuenta, y que por favor, llamen por teléfono a su banco (la estrategia típica del phishing) el usuario puede que no desconfíe, ya que no está yendo a un link dentro de un correo (como siempre se ha dicho que no se haga, para evitar estafas) ni está llamando a un número que venga en el correo electrónico (otra acción que debe evitarse). Si utiliza su sistema de telefonía VoIP, llamará a "Banco", no a un número especial, y le atenderá un amable sistema informatizado que le capturará todos sus datos.

La protección antivirus clásica puede que no tenga tiempo suficiente para reaccionar si el código es completamente nuevo, ya que el ataque se puede consumir en uno o dos minutos. Si es un código conocido, no habría ningún problema, estaría incluido en la base de datos de firmas y se detectaría. En el caso de un código completamente nuevo es necesario un sistema de protección que vea qué está pasando en el ordenador, y cuando el código

¿La voz sobre IP amenazada?



malicioso intento llevar a cabo una acción peligrosa (en este caso una alteración de la lista de contactos), detenga ese código y lo bloquee de manera automática.

Así es cuando se estará protegido realmente ante la posible oleada de ataques que se ceban en los sistemas de voz sobre IP. Para problemas clásicos (códigos maliciosos conocidos), análisis por firmas; para los nuevos problemas, nuevas tecnologías (detección inteligente de códigos desconocidos).

Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com