



RSA y Black Hat

Caso: 01.07/09 Autor: S21sec

Durante este mes de abril se han celebrado dos de las conferencias más populares del mundo de la seguridad. Ambas son un excelente indicador para conocer los problemas más candentes en este inicio de año así como las soluciones propuestas por las empresas de seguridad y las tendencias de la industria

Uno de los temas estrella ha sido Conficker. Poco más que añadir a la gran cantidad de información existente respecto a este código malicioso, las charlas relacionadas con el mismo han sido básicamente para mostrar números (se habla de una botnet de hasta 4 millones de equipos infectados), así como para evaluar la evolución de esta red a día de hoy.

Parece que la entrada de otros códigos maliciosos ya está en marcha. Por otra parte, algunos expertos consideran que tanto hablar de esta amenaza en concreto puede despistar la atención de otras mucho más reales y que no se están estudiando con tanto interés.

En cuanto a la lucha contra el cibercrimen, parece que empiezan a aflorar gran cantidad de iniciativas en este aspecto, tanto a nivel gubernamental como privado. Lo que fuera uno de los temas estrella durante el año pasado ha tenido su cimentación durante este 2009. Algunos expertos empiezan a ser incluso más agresivos, pidiendo pasar a la acción para desmontar las mafias detrás de estas redes mediante la infiltración en las mismas. En ese mismo aspecto, expertos del



FBI comentaron su presencia permanente en varias ciudades con equipos especiales dedicados a e-crime, y con buenos resultados que habían provocado la detención de más de 100 personas.

Por otra parte, la proliferación de este tipo de delincuencia está creando un mercado totalmente maduro en el que es posible comprar cualquier tipo de producto y servicio, muchos de ellos especializados. En este sentido, es posible alquilar una botnet por menos de 300\$ al

mes sin tener que hacer nada ni tener conocimientos, eso sí, sin exclusividad para instalar malware en estas máquinas. La popularidad de algunos kits como Zeus o Limbo ha acaparado gran parte del mercado y son usadas por infinidad de pequeños grupos fraudulentos, otros kits mucho más profesionales y avanzados técnicamente, como Sinowal o Bankpatch no están disponibles en el mercado. Todo esto ha hecho que el precio de algunos bienes ofrecidos en el mercado,

como las tarjetas de crédito, hayan bajado su precio desde los 100\$ que llegaron a costar hace no demasiado tiempo a 10\$.

Cambiando un poco de tema, la virtualización ha sido uno de los temas estrella, estando en boca de gran cantidad de profesionales y formando parte de muchas estrategias de negocio. Dado el movimiento que está realizando el mercado a este tipo de entornos por las obvias ventajas que supone, también lo está haciendo el mundo de la seguridad, ofreciendo soluciones y debatiendo posibles problemas que pueden encontrarse. Otro tema íntimamente ligado a la virtualización es el Cloud Computing. De forma muy similar, la industria de la seguridad empieza a aproximarse a este sector para estudiar problemas y ofrecer soluciones.

El debate en cuanto a virtualización se centra en el hipervisor, la pieza de código encargada de virtualizar el entorno del sistema operativo y de interactuar con el sistema operativo externo, así como con el hardware físico. Este elemento es una oportunidad, así como una posible amenaza: en caso de verse comprometido, un código malicioso puede hacerse con el control de la máquina física. Por



otra parte, su ubicación externa al sistema operativo que corre en el entorno virtualizado permite una monitorización única y "a salvo" de código malicioso, al menos el más tradicional, lo que abre toda una nueva rama en cuanto a posibilidades de detección y prevención. No obstante, se trata de un campo virgen que ya se verá cómo evoluciona.

En cuanto a Black Hat, tal vez la charla más destacada (esto es muy subjetivo) fue la referente a técnicas para la creación de troyanos en .NET [1]. Esta presentación describe vulnerabilidades implícitas en el propio framework de ejecución de .NET que pueden ser aprovechadas por código

malicioso para controlar el sistema. El mismo escenario es aplicable a otros entornos, como Java.

Por supuesto, destacar la presentación que no llegó a darse. Y es que se anunció que en una de las charlas se iba a descubrir una vulnerabilidad de dimensiones incluso mayores a la ya famosa de Kaminsky respecto a DNS. Un día antes de la charla, se anunció que no se realizaría ya que era demasiado pronto para poder distribuir una protección efectiva por parte del fabricante implicado, que pidió entre 1 y 3 meses para parchear el problema de forma efectiva. Como siempre en este tipo de asuntos, es difícil saber hasta qué punto es publicidad, así que seguiremos expectantes la publicación de los detalles del problema durante los próximos meses. ♦

Referencias

- [1] <http://www.blackhat.com/presentations/bh-europe-09/Metula/BlackHat-Europe-2009-Metula-NET-Framework-rootkits-whitepaper.pdf>



Koobface ataca de nuevo

Caso: 01.07/09

Autor: S21sec

Koobface es un gusano que apareció a mediados de 2008 en las redes sociales (Facebook, Myspace, Hi5, Tagged, etc.) y que se propagaba a través de mensajes en la propia red realizados por usuarios ya infectados. Ya había resurgido a principios de año pero ha sido durante este mes cuando se ha visto una nueva oleada, un nuevo intento por parte de sus creadores para que este gusano se propague al máximo

Al seguir el enlace incluido en el mensaje el usuario es redirigido a través de diferentes dominios, dependiendo de la red social de la que proceda, y llegando en casi todos los casos a una página que simula a Youtube, con título Secret Video, y que muestra un intento de visualizar un vídeo, fallando supuestamente por la falta de Adobe Flash Player 10.37. De forma instantánea aparece una ventana de descarga con un archivo de nombre setup.exe, dando a entender que es el archivo que necesitamos, pero que resulta ser la nueva variante del gusano.

Una vez instalado, el código malicioso intenta comunicarse con un servidor, descargando nuevas instrucciones y URLs donde descargar más malware.

Actualmente este código malicioso únicamente se descarga falsos antivirus y adware que redirigen las búsquedas de los usuarios infectados hacia sitios de publicidad. Sin embargo, no se puede obviar la posibilidad de que los delincuentes cambien su



facebook

TAGGED

hi5

myspace.com
a place for friends

estrategia e instalen otro tipo de malware más peligroso (troyanos bancarios, por ejemplo), con el objetivo de

aumentar sus beneficios. Por lo tanto, es importante prestar atención a los enlaces de los mensajes de las distintas redes sociales, y no hacer clic sobre los que levanten la más mínima sospecha. ♦

Referencias

[1] <http://blog.s21sec.com/2009/05/koobface-tirando-del-hilo.html>

[2] http://www.f-secure.com/v-descs/net-worm_w32_koobface_es.shtml



Botnet de Sinowal secuestrada

Caso: 01.07/09 Autor: S21sec

A principios de mayo se hizo público el estudio realizado por parte de un grupo de investigadores de seguridad de la Universidad de California en Santa Barbara (UCSB), llamado *Your Botnet is My Botnet: Analysis of a Botnet Takeover*^[1], donde explicaban que habían llevado a cabo el secuestro de la botnet de Sinowal (aka Torpig, Anserin) durante 10 días.

Para realizar el estudio, vista la dificultad para llevar a buen término las comunicaciones con los registradores DNS (que normalmente se desentienden totalmente) y dada la naturaleza de Sinowal, que genera diaria y semanalmente nuevos dominios con los que contactar, lo que se hizo fue registrar dos de estos dominios antes que los propios delincuentes, recibiendo casi desde el primer momento todos los datos provenientes de las máquinas infectadas. Como software del servidor usaron Apache, configurándolo y programando las páginas adecuadas para que las respuestas a los bots fueran las esperadas.

La idea inicial fue la de mantener la infraestructura durante 3 semanas ininterrumpidamente (del 25 de enero al 15 de febrero de 2009), pero después de 10 días los responsables de la botnet distribuyeron un nuevo binario, actualizando el algoritmo de generación de dominios y, por ende, los servidores con los que comunicarse.

Sin embargo, en esos 10 días recolectaron suficientes datos como para realizar este completo

estudio sobre la naturaleza de la información robada, ya que recogieron casi 70GB de tráfico de red (no de datos, como en algunos medios se ha señalado). En este tiempo pudieron identificar casi 183.000 bots, basándose en un identificador propio de Sinowal y en los diferentes parámetros de las máquinas afectadas (sistema operativo, país, versión del binario), eliminando aquellos sospechosos de ser investigadores de seguridad. Gracias a esta métrica se obtuvo un número mucho más real que con el cálculo por IP, que se aleja bastante de la realidad debido al uso de NAT y DHCP, y que en este caso sobrepasaba el 1.200.000 de IPs diferentes. El mayor número de bots se localizaron en Estados Unidos, Italia y Alemania, mientras que España ocupaba la quinta posición con 5.733 máquinas infectadas.

A pesar de que Sinowal tiene como objetivo la recolección de credenciales bancarios en su mayoría, también roba cualquier contraseña transmitida en conexiones FTP, SMTP, POP, HTTP y HTTPS, entre otras. Hablando de entidades financieras los investigadores recolectaron un total de 8.310 cuentas de 410 entidades

diferentes, siendo de nuevo Estados Unidos, Italia y Alemania los países más afectados, seguidos de lejos por España, con 228 cuentas y 18 entidades afectadas.

Además, entre toda la información recibida también se encontraron 1.660 números diferentes de tarjetas de crédito y débito, siendo el 49% pertenecientes a víctimas en Estados Unidos, el 12% italianas y el 8% españolas, estando el resto repartidas entre otros 40 países. La mayor parte de estas tarjetas eran Visa (1.056), Master-Card (447), American Express (81), Maestro (36) y Discover (24).

En total se pudieron recolectar casi 298.000 credenciales diferentes, enviadas por 52.540 bots, siendo google.com el dominio con más credenciales de acceso web (8.291), seguido de cerca por dos de las redes sociales más populares, Facebook (7.812) y Myspace (7.214).

Como conclusiones del informe, aparte de dar una perspectiva más real del tamaño de las botnets y sacar a la luz algo que muchos no sabían, remarcan la falta de cultura de seguridad informática en la mayor parte de los usuarios infectados y la necesidad de más implicación por parte de las diferentes partes y de los gobiernos en este aspecto. ♦

Referencias

[1] <http://www.cs.ucsb.edu/~seclab/projects/torpig/>