



La economía
de las botnets

Yuri Namestnikov

KASPERSKY lab

Cómo ganan dinero los propietarios de las botnets	5
Ataques DDoS	5
Captación de información confidencial	6
Phishing	8
Spam	9
Spam de búsqueda	9
Instalación de programas publicitarios y maliciosos	10
Recopilación de “clics”	10
Alquiler y venta de botnets	11
Conclusión	12

En los últimos 10 años, las redes zombi o botnets han experimentado una evolución: de pequeñas redes formadas por una decena de equipos y administradas desde un centro a convertirse en complicados sistemas distribuidos de administración descentralizada que constan de millones de equipos. La pregunta es: ¿para qué se crean estas inmensas redes zombi? La respuesta se resume en una palabra: dinero.

Una botnet o red zombi es una red de equipos infectados por un programa malicioso que permite a los ciberdelincuentes manejar estos equipos a distancia sin que el propietario se dé cuenta. Las botnets se han convertido en una fuente de ingresos estable para muchos grupos de delincuentes informáticos, en gran parte por los mínimos conocimientos y recursos que se necesitan para administrar estas redes.

¿Cuál es el origen de todo esto? Si un delincuente necesita una botnet, ¿qué debe hacer para obtenerla? Hay muchas posibilidades, dependiendo de sus habilidades informáticas. Desgraciadamente, si alguien decide organizar una botnet, en Internet es fácil encontrar instrucciones de cómo hacerlo.

Para crear una nueva red zombi, hay que infectar los equipos de los usuarios con un programa especial, llamado “bot”. Los bot son programas maliciosos que permiten reunir los equipos infectados en “botnets”. Si el delincuente que quiere empezar su “negocio” no tiene habilidades de programador, puede buscar anuncios de venta de bots en los foros.

También puede pedir que se cifre el código de estos programas para evitar que sean detectados por los programas antivirus. Aun más: existe la posibilidad de apoderarse de una botnet ya existente.

El siguiente paso del delincuente es infectar con un programa bot los equipos de los usuarios. Con esta finalidad se usan envíos masivos de spam, se publican mensajes en los foros y en las redes sociales, se organizan descargas «drive-by» o se le agregan a la misma botnet funciones de autopropagación, tales como virus y gusanos.

Cuando se usa spam, foros y redes sociales, en los mensajes se aplican diferentes métodos de ingeniería social para inducir a la potencial víctima a instalar el bot. Por ejemplo, se le ofrece ver un vídeo interesante, pero se le dice que necesita un codec especial. Después de descargar y ejecutar el fichero del “codec” el usuario, por supuesto, no puede ver ningún vídeo y lo más probable es que no note ningún cambio, pero su equipo ya estará infectado. Y de esta manera furtiva su equipo se convierte en un fiel esclavo que ejecuta todas las instrucciones del propietario de la botnet.

El segundo método más popular es el de las descargas “drive-by”, que son imperceptibles para el usuario. En esencia, este método consiste en que el usuario se contagia por el simple hecho de visitar una página web infectada, gracias a diferentes vulnerabilidades del software, sobre todo de los navegadores. Para aprovecharse de las vulnerabilidades se echa mano de programas especiales, llamados exploits los cuales, aparte de descargar en secreto programas nocivos,

los ejecutan de una forma completamente inadvertida. En caso de que el ataque tenga éxito, el usuario ni siquiera sospechará que a su equipo le pasa algo raro. Esta forma de propagar software malicioso es la más peligrosa, puesto que si la página web es muy popular, puede contagiar decenas de miles de usuarios.

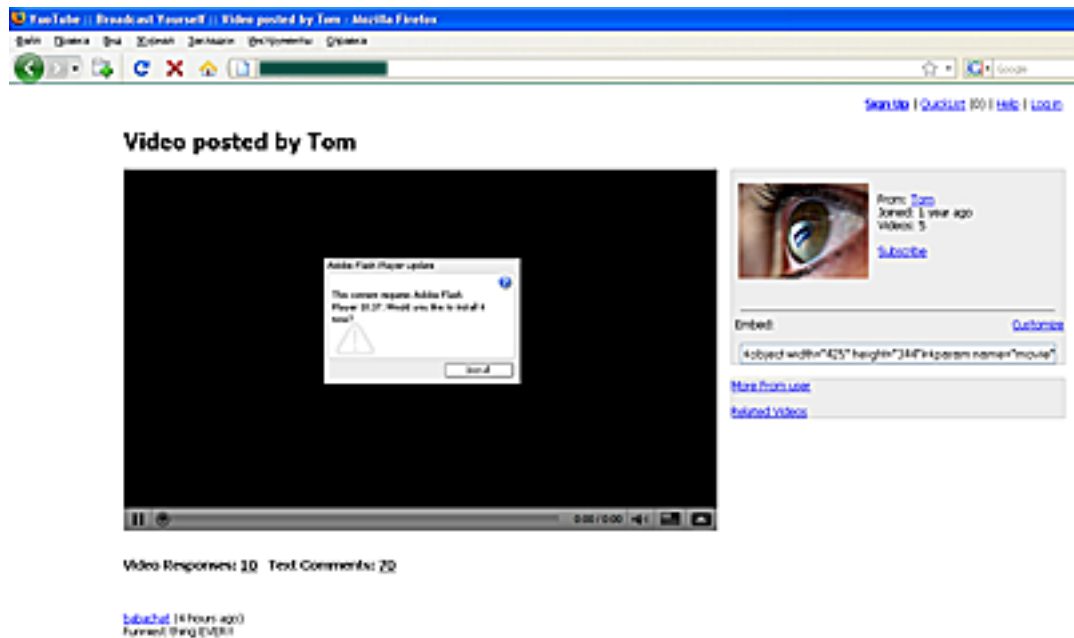


Fig. 1. El cebo para el usuario. (YouTube falsificado)

El bot puede contener funciones de autopropagación a través de redes informáticas. Por ejemplo, el bot puede propagarse infectando todos los ficheros ejecutables o al encontrar y aprovechar las vulnerabilidades de los equipos conectados a la red local. Un buen ejemplo de estos bots son los representantes de la familia Virus. Win32.Virut y Net-Worm.Win32.Kido. El primero es un virus polimórfico que infecta ficheros y el segundo un gusano de red. Es difícil no admitir la efectividad de este método: hoy en día, la red zombi construida por Kido es la de mayores dimensiones en el mundo.

El creador de la botnet puede controlar los equipos de los usuarios mediante un centro de administración que se conecta a los bots usando un canal IRC, una conexión web o cualquier otro medio a su disposición. Basta organizar una red de varias decenas de equipos para que la botnet empiece a generar ganancias a su propietario. Y el lucro obtenido está en relación directa con la estabilidad de la red-zombi y el ritmo de su crecimiento.

Cómo ganan dinero los propietarios de las botnets

Pero ¿de qué forma ganan dinero los propietarios de las botnets con los equipos infectados? Aquí mencionamos las principales tendencias: ataques DDoS, captación de información confidencial, envío de spam, phishing, spam de búsqueda, aprovechamiento de clics y descarga de software publicitario y malicioso. Hay que destacar que cualquiera que sea la forma elegida por el delincuente, la ganancia está garantizada. Y además, ni siquiera es necesario hacer una elección. Las botnets permiten ejecutar todas estas tareas al mismo tiempo.

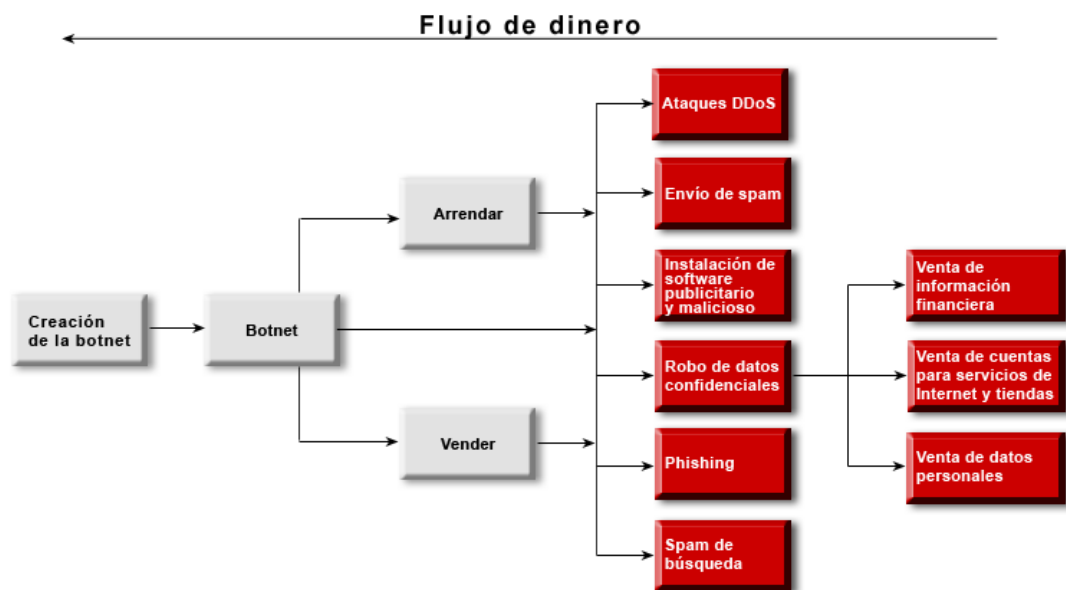


Fig. 2. El negocio de las botnets

Ataques DDoS

Muchos investigadores coinciden en suponer que las primeras botnets ya contaban con funciones de ataques DDoS (Denial of Service, o “denegación de servicio”). Los ataques DDoS tienen como objetivo que un sistema informático deje de responder a las solicitudes que recibe. Uno de los métodos más difundidos para realizarlos es enviar una gran cantidad de solicitudes al equipo “víctima”, lo que provoca que deje de reaccionar si su potencia es insuficiente para procesar todas las solicitudes. Los ataques DDoS son un arma terrible en manos de los hackers y las botnets son un instrumento ideal para este tipo de ataque. Los ataques DDoS pueden ser medios de guerra sucia contra la competencia o manifestaciones de terrorismo informático.

El propietario de la botnet puede ofrecer a un empresario poco escrupuloso un servicio como el siguiente: ejecutar un ataque DDoS dirigido al sitio web de su competidor. El sitio web quedará inhabilitado después de semejante carga y el delincuente recibirá una recompensa.

De la misma manera, los propietarios de botnets pueden usar ataques DDoS para extorsionar a las grandes compañías. Y las compañías prefieren aceptar las exigencias de los delincuentes porque es mucho más caro vérselas con las consecuencias de un ataque DDoS. En enero de 2009 el ataque sufrido por el gran hoster godaddy.com provocó que varios miles de sitios alojados en los servidores de la compañía estuviesen inaccesibles por casi 24 horas. ¿A qué se debió? ¿Fue una maniobra ilegal de otro hoster para garantizarse un lugar, o fue un chantaje de los delincuentes contra Go Daddy? Nos parece que ambas posibilidades son probables. En noviembre de 2005 este mismo hoster sufrió un ataque similar, pero aquella vez el servicio estuvo desactivado sólo una hora. El segundo ataque fue más terrible, sobre todo porque las botnets eran mucho mayores.

En febrero de 2007 se lanzó una serie de ataques a los servidores DNS raíz, de cuyo funcionamiento depende todo Internet. Es poco probable que el objetivo de estos ataques haya sido derrumbar Internet en su totalidad, ya que las botnets pueden funcionar sólo si funciona Internet. Más bien parecía una demostración de la fuerza y las posibilidades de las redes zombi.

La publicidad de servicios de ataques DDoS está a disposición del público en muchos foros dedicados a estos temas. Veamos la lista de precios: un ataque puede costar desde 50 dólares americanos hasta varios miles de dólares por cada día de funcionamiento ininterrumpido de la botnet. La variación de los precios es comprensible y justificada. Para detener por un día el trabajo de una humilde tienda online que no cuente con protección, basta una botnet relativamente pequeña (de unos 1000 equipos). El ataque costará una módica. El precio será otro si la competencia es una gran compañía internacional con un sitio protegido. Para que el ataque DDoS tenga éxito, en este caso se necesitará una cantidad mucho mayor de equipos zombi.

Según los datos de shadowserver.org, en 2008 se llevaron a cabo unos 190.000 ataques DDoS por los que los delincuentes recibieron unos 20 millones de dólares. Por supuesto, en estos cálculos no se tienen en cuenta lo ganado por los chantajistas, porque es muy difícil saber cifras exactas.

Captación de información confidencial

La información confidencial que se guarda en los equipos de los usuarios siempre atraerá a los delincuentes. Representan gran interés los números de tarjetas de crédito, la información financiera y las contraseñas de diferentes servicios: correo electrónico, ftp, mensajeros instantáneos y otros. Los programas maliciosos modernos permiten a los delincuentes seleccionar los datos que necesitan, para lo cual es suficiente instalar en el equipo infectado un módulo ad-hoc.

Los delincuentes pueden vender la información robada o usarla para sus intereses poco lícitos. En los foros underground cada día aparecen miles de anuncios de venta de datos de cuentas bancarias. El precio depende de la cantidad de dinero que hay en la cuenta y va desde 1 hasta 1500 dólares. El precio mínimo muestra que en la lucha competitiva, los delincuentes que se ocupan de este negocio

se han visto obligados a bajar sus precios. Para obtener grandes ganancias, necesitan un flujo estable de datos frescos, que depende sobre todo del crecimiento estable de sus redes zombi.

La información financiera es de especial interés para los carders, personas que se dedican a falsificar tarjetas de crédito. Para darse una idea de cuán lucrativas son estas operaciones, veamos el famoso caso de delincuentes brasileños arrestados hace dos años. Usando información robada de los bancos, se sacaron 4.74 millones de dólares de las cuentas bancarias.

Los delincuentes que se dedican a falsificar documentos, abrir cuentas bancarias ilegales y hacer negocios ilícitos tienen gran interés en adquirir datos personales que no tienen relación directa con el dinero de los usuarios.

El coste de los datos personales robados está en relación directa con el país donde vive su propietario real. Por ejemplo, los datos completos de los habitantes de los EE UU cuestan de 5 a 8 dólares. En el mercado negro son muy apreciados los datos de los habitantes de Europa, que cuestan 2 o 3 veces más que los de EE UU y Canadá. La explicación es que los delincuentes pueden usar estos datos en cualquier país de la Unión Europea. El precio medio mundial de un paquete de datos completos de una persona es de aproximadamente 7 dólares.

Otro tipo de información recopilada por las botnets son las direcciones de correo electrónico. A diferencia de los números de tarjetas y de cuentas, en un equipo infectado se puede conseguir un buen número de direcciones de email. Las direcciones recopiladas se ponen en venta, a veces “al peso”, es decir, por megabytes. Por supuesto, los principales compradores son los spammers. Una lista de un millón de direcciones cuesta de 20 a 100 dólares, mientras que los spammers cobran de 150 a 200 dólares por enviar spam a esta misma cantidad de direcciones. La ganancia es evidente.

Los delincuentes también muestran interés por las cuentas de diversos servicios de pago y tiendas online. Sin duda, son más baratas que los datos de cuentas bancarias, pero su venta tiene menos riesgos de ser advertida por las Autoridades. Por ejemplo, las cuentas de la popular tienda online Steam con diez juegos se venden por entre 7 y 15 dólares la unidad.

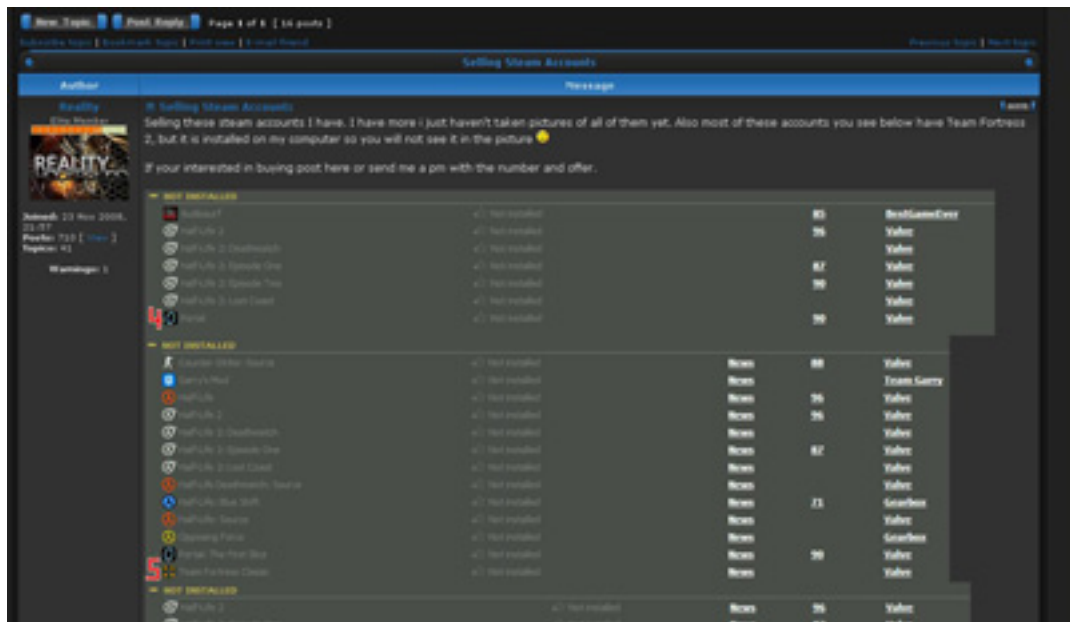


Fig. 3. Anuncio en el forum sobre la venta de cuentas en Steam

Phishing

La creación de sitios phishing está adquiriendo grandes dimensiones, por lo que sus dueños deben tomar medidas para impedir la clausura de estos sitios. Esto se logra con la ayuda de las botnets, que admiten el funcionamiento de las tecnologías Fast-flux, que permiten, de una forma operativa, y cada pocos minutos, cambiar las direcciones IP de los sitios, conservando el nombre de dominio, con lo que se alarga su vida, se dificulta su detección y se evita su clausura. La idea se basa en el uso de ordenadores domésticos (parte de las botnets) en calidad de servidores web con contenido phisher. La tecnología Fast-flux es más efectiva que los servidores proxy en la tarea de ocultar los sitios falsificados en Internet.

Así, el famoso grupo de phishers Rock Phish colabora con los operadores de la botnet Asprox. A mediados del año pasado, estos “roqueros del phishing” (responsables de la mitad de los ataques phishing en Internet que hicieron perder millones de dólares a los usuarios) modernizaron su infraestructura para adaptarla al uso de Fast-flux. Esta tarea les llevó unos cinco meses y fue ejecutada con gran nivel de profesionalidad. Con todo, los phishers no crearon su propia red Fast-flux, sino que usaron una solución ya existente, comprándosela a los propietarios de Asprox.

Los delincuentes, en su mayor parte phishers, pagan a los propietarios de las botnets de 1000 a 2000 dólares mensuales.

La ganancia media del phishing es similar a la obtenida con la ayuda de programas maliciosos y es de millones de dólares anuales.

Spam

Cada año se envían millones de mensajes spam en todo el mundo. El envío de correo no solicitado es una de las principales funciones de las botnets. Según los datos de Kaspersky Lab, cerca del 80% de todo el spam se envía con la ayuda de redes zombi.

Desde los ordenadores de los usuarios se envían miles de millones de mensajes que publicitan Viagra, réplicas de relojes caros, o casinos online que causan embotellamientos de tráfico en la red y llenan los buzones de correo electrónico. Las direcciones desde donde se hacen los envíos masivos pasan a engrosar las listas negras elaboradas por las compañías antivirus.

En estos últimos años también ha crecido la oferta de servicios spam: ha aparecido el spam para ICQ, el spam en las redes sociales, foros y blogs. Y este crecimiento también se debe a las botnets: es muy fácil escribir un módulo adicional para el cliente de software bot que abra nuevos horizontes a nuevos negocios con divisas como “Spam en Facebook, precios económicos”.

Los precios del spam fluctúan dependiendo de cuál es el destinatario final y la cantidad de direcciones a las que se hace el envío masivo. La variación de los precios de los envíos dirigidos a un auditorio en especial empieza desde los 70 dólares por 100.000 direcciones hasta 1.000 dólares por varias decenas de millones de direcciones.

El año pasado los spammers ganaron unos 780.000.000 dólares con los envíos masivos.

Spam de búsqueda

Una variante más del uso de las botnets es la optimización de la búsqueda en Internet. Al trabajar en la optimización de la búsqueda, los webmasters tratan de que su sitio web esté entre los primeros lugares del resultado de la búsqueda, porque mientras más alta sea la posición, más visitantes llegarán a su sitio desde los sistemas de búsqueda.

Los buscadores toman en cuenta varios factores al analizar la relevancia de un sitio web. Uno de los principales parámetros es la cantidad de vínculos al sitio que están publicados en otras páginas o dominios. Mientras más sean estos vínculos, más alto será el rating del sitio desde el punto de vista del robot de búsqueda. En el rating también influyen las palabras del vínculo. Por ejemplo, el vínculo «compre nuestros ordenadores» tendrá más peso que «comprar un ordenador».

En sí, el negocio de SEO (Search Engine Optimization) es un buen negocio. Muchas compañías pagan grandes cantidades de dinero a los webmasters para que su sitio esté en las primeras posiciones en los resultados de los buscadores. Los propietarios de las botnets, por su parte, han observado ciertas regularidades y encontrado métodos de automatizar el proceso de optimización de la búsqueda.

Por esta razón, cuando se ve en los comentarios a la entrada favorita de su blog o fotografía un montón de vínculos creados por un desconocido (o por algún amigo, quizá)... no se sorprenda: es que alguien le pidió popularizar un sitio a los propietarios de la botnet. Un programa creado para este propósito se instala en el equipo zombi y empieza, en nombre del usuario, a dejar comentarios con vínculos al sitio publicitado en los recursos que gozan de popularidad.

El precio medio de los servicios ilegales de spam de búsqueda es de unos 300 dólares al mes.

Instalación de programas publicitarios y maliciosos

Imagínese que está dedicando un momento de tranquilidad a leer su revista favorita de coches cuando de pronto aparece una ventana emergente donde le ofrecen comprar accesorios para su coche. Al parecer, no hay nada malo en esto, y quizá usted no tenga nada en contra de comprarlos, pero no recuerda haber instalado ningún programa para la búsqueda de cosas necesarias (o innecesarias). La respuesta es sencilla: los propietarios de la botnet ya se han preocupado de hacerlo.

Muchas de las compañías que prestan servicios de publicidad online pagan por cada instalación de su software. Por lo general el precio no es demasiado alto, de 30 centavos a 1,5 dólares por cada programa instalado. Sin embargo, cuando una botnet está en manos de un delincuente, éste puede instalar cualquier software en miles de equipos con un par de clics y ganar una gran cantidad de dinero. El famoso delincuente cibernético D.K. Shaifer, condenado en 2007, ganó en sólo mes más de 14.000 dólares por instalar software publicitario en 10.000 ordenadores por medio de una botnet de más de 250.000 equipos.

Los representantes de los negocios cibercriminales que difunden programas nocivos con frecuencia trabajan usando el mismo esquema, pagando dinero por cada instalación de su software. Este tipo de trabajo conjunto de delincuentes recibió el nombre de “asociación”. La instalación de programas en los equipos de los usuarios de diferentes países tiene diferentes precios. Por ejemplo, la instalación de un software malicioso en mil equipos en China cuesta 3 dólares, mientras que en EE UU cuesta 120 dólares. Y es completamente explicable, porque a los usuarios de los países desarrollados se les puede robar información mucho más valiosa en su expresión «monetaria».

Recopilación de “clics”

Las compañías publicitarias que funcionan online según el esquema PPC (Pay-per-Click) pagan dinero por cada clic único en sus anuncios. Para los propietarios de botnets, engañar a estas compañías es una actividad bastante lucrativa.

Como ejemplo podemos tomar la conocida red Google AdSense. Los anunciantes

pagan a Google por los clics en los anuncios, con la esperanza de que el visitante compre algo en sus tiendas online.

Por su parte, Google pone los anuncios contextuales en los diferentes sitios participantes en el programa AdSense y pagan al dueño del sitio por cada clic. Desgraciadamente, no todos los propietarios de sitios son honrados. Así, disponiendo de una botnet, un hacker puede generar miles de clics únicos al día, uno en cada equipo zombi, para no despertar las sospechas de Google. De esta manera, el dinero gastado en la campaña publicitaria pasa al bolsillo del hacker. Y es de lamentar que no haya un solo caso de juicio penal por acciones como esta.

Según los datos de Click Forensics, en 2008 el 16-17% de todos los clics en vínculos publicitarios fueron falsos y de ellos, una tercera parte fue generada por botnets. Unos sencillos cálculos nos permiten comprender que el año pasado los propietarios de las botnets hicieron “clics” por un valor de 33.000.000 dólares. ¡Excelente ganancia por unos cuantos “clics”!

Alquiler y venta de botnets

La conocida fórmula de Marx “mercancía-dinero-mercancía” se convierte en «botnet-dinero-botnet» para los propietarios de grandes botnets. Y es cierto, porque para mantener una botnet, garantizar el flujo de nuevos bots y evitar que sean detectados por los programas antivirus se necesitan inversiones y gastos temporales. El hacker simplemente no tiene tiempo de enviar cartas, instalar programas, robar y vender información. Es más sencillo alquilar la botnet o venderla, pues hay muchas personas interesadas.

El alquiler de una botnet de correo capaz de enviar 1000 mensajes por minuto (con unos 100 equipos zombi online) cuesta cerca de 2000 dólares por mes. El precio de venta o alquiler de una botnet depende de la cantidad de equipos infectados. Las botnets “listas para usar” gozan de gran popularidad en los foros de habla inglesa. Las botnets pequeñas, de unos cuantos cientos de equipos, cuestan de 200 a 700 dólares, con lo que el precio medio de un bot es de 0,5 dólares. Las grandes botnets tienen un precio muy diferente. La red Shadow, creada por un hacker holandés de 19 años y formada por más de 100.000 ordenadores ubicados en todo el mundo fue vendida por 25.000 euros (37.290 dólares).

Conclusión

Cada día, los propietarios de botnets ingresan enormes cantidades de dinero. La lucha contra este negocio se realiza de todas las formas posibles, pero las leyes son extremadamente inefectivas. Las leyes aplicables al spam, la creación y propagación de programas maliciosos y la penetración ilegal en redes informáticas no existen en muchos países. Los propietarios o creadores de botnets que han sido sometidos a juicio se pueden contar con los dedos de una mano. Y es que establecer la cantidad de botnets en funcionamiento es una tarea que dista mucho de ser trivial, porque existen varias decenas de grandes botnets cuyas actividades son notorias, pero también existen muchas de menores dimensiones que son muy difíciles de detectar.

En este momento, la lucha contra las botnets sería mucho más efectiva si los expertos antivirus, los proveedores de Internet y las fuerzas del orden trabajasen de una forma más estrecha. El resultado de esta colaboración fue la clausura de tres compañías: EstDomains, Atrivo y McColo. Destacamos que la clausura de la compañía McColo, en cuyos servidores se encontraban los centros de administración de varias grandes botnets de spam, condujo a que la cantidad de spam en Internet se redujese a la mitad.

Los expertos siguen con atención miles de botnets, los antivirus detectan y destruyen bots en todo el mundo, pero sólo las Autoridades tienen la posibilidad de detener las actividades de los centros de administración y arrestar a los delincuentes, con lo que las botnets desaparecerían por un tiempo. Con todo, la clausura de McColo tuvo un efecto pasajero, porque unas semanas después el flujo de spam volvió a su nivel normal. Los propietarios de las botnets trasladaron los centros de administración a otros Hostings y siguieron dedicándose a su negocio como si nada hubiese pasado. Lo que demuestra que es necesaria una labor constante y no verificaciones aisladas. Por desgracia, cortar una sola cabeza no es suficiente.

Sin la ayuda de los usuarios, la lucha no puede ser efectiva. Y la razón es que los ordenadores domésticos forman la mayor parte del ejército de botnets. Para evitar que los delincuentes conviertan su equipo en zombi, es necesario tomar ciertas medidas, como usar un antivirus, crear contraseñas complicadas, desactivar la ejecución automática de ficheros desde dispositivos extraíbles... ¿Para qué ayudar a los cibercriminales?