Evolución del código dañino

EL FRAUDE CIBERNÉTICO ES UN NEGOCIO QUE MANEJA MILLONES DE DÓLARES AL AÑO, CONSIGUIENDO UN BENEFICIO DOCE VECES MAYOR QUE EL FRAUDE TRADICIONAL. AQUÍ RADICA EL INCREMENTO ESPECTACULAR DEL CÓDIGO DAÑINO

Centro Criptológico Nacional
Centro Nacional de Inteligencia

Tal y como recoge el Glosario de la Guía CCN-STIC 401 (Guía de Seguridad de las TIC del Centro Criptológico Nacional), el código dañino o *malware malicious software* es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta *spyware*.

En España, se estima que uno de cada tres ordenadores está infectado, lo que sitúa a nuestro país entre los cinco primeros del mundo con mayor número de ordenadores infectados.

A escala mundial se contabilizan anualmente unos 3.000 incidentes globales. Cada uno de estos afecta en promedio a unas 20.000 máquinas, y supone el robo de cuatro gigabytes de datos. Baste señalar que una de cada diez páginas de Google es portadora de algún tipo de infección. Los propios fabricantes de antivirus reconocen su incapacidad para hacer frente a los miles de códigos maliciosos que surgen cada día.

Para comprender el funcionamiento de los códigos maliciosos es necesario hacer referencia al término "*botnet*" (colección de ordenadores conectados a Internet que interactúan entre sí para lograr la realización de cierta tarea de forma distribuida). Si bien ese conjunto de ordenadores puede ser usado para aplicaciones útiles y constructivas, el término botnet se aplica, típicamente, a un sistema diseñado y utilizado para propósitos maliciosos. Dicho sistema está compuesto por equipos comprometidos que son introducidos en la "botnet" sin conocimiento de sus dueños. Son los llamados ordenadores "*zombie*".

El motivo fundamental del incremento exponencial de los códigos dañinos es que se han convertido en un negocio. De hecho, el fraude cibernético maneja millones de dólares al año y obtiene un beneficio doces veces mayor que el fraude tradicional. Esto ha fomentado la aparición de verdaderas organizaciones criminales con una jerarquía clara: dirección, programadores expertos, spammers, pen-testers, administradores de sistemas, *herders* y mulas.

Hay que tener en cuenta, además, que el tipo de ataque que se realiza en la actualidad implica menos riesgos para los delincuentes porque se enmarca en un entorno distribuido con múltiples intermediarios y resulta muy difícil identificar a los responsables.

Entre los múltiples métodos para secuestrar la información personal de los usuarios de forma fraudulenta, destacan el *phishing*, el *pharming*, el *vishing* y el *ARP Spoofing*.

El ataque con *malware* afecta principalmente a instituciones financieras, al comercio electrónico, a las instituciones públicas, a los sitios de pago *online*, a los sitios de subastas y a los casinos *online*.

Algunos ataques también se realizan por motivos políticos y se centran en recaudar todo tipo de información sensible para dañar determinadas organizaciones o entidades gubernamentales.

Antes se utilizaban virus como *Blaster* o *Sasser* que aprovechaban las vulnerabilidades de los sistemas operativos. Otro método de infección consistía en enviar archivos adjuntos infectados mediante correo electrónico, y también se realizaban descargas no confiables a través de las redes P2P.

En la actualidad, los ataques se dirigen a explotar vulnerabilidades de aplicaciones como Outlook, Powerpoint, Word, PDF o WinZip. Además, el 65% de los ataques se basan en la explotación de vulnerabilidades de los navegadores tales como IE, Firefox y Opera (véase gráfico).

Como método adicional, los delincuentes también recurren a la ingeniería social para distribuir una infección por medio de USB olvidados o cualquier otro dispositivo (consolas, móviles, PDA, etc.). En el futuro, esta acción probablemente se perfeccionará gracias al Bluetooth y a los mensajes multimedia.

Hoy en día, los delitos cibernéticos están amparados por la permisividad de muchos países, como Rusia, Hong-Kong, Panamá o Corea del Norte. En el contexto internacional, son pocos los países que cuentan con una legislación apropiada.

Ejemplo de método de infección: Mpack

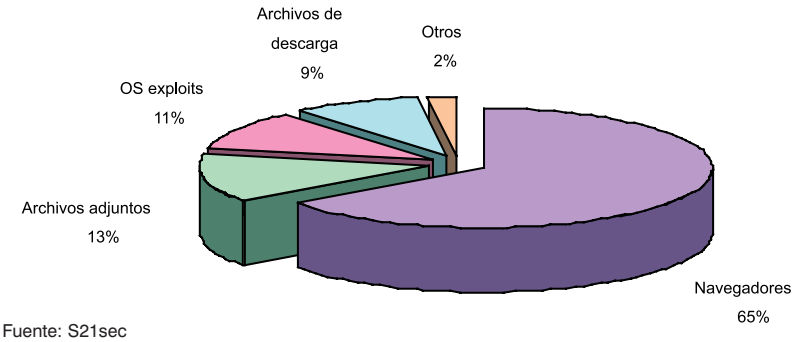
El *toolkit Mpack* es un software malicioso que se vende en foros *underground* de Rusia y se actualiza continuamente con nuevos exploits (mass-exploits, exploits para navegadores web o HTML+Javascript exploits).

Además, el programa incluye PHP+BBDD para estadísticas y permite la inyección de iFrames en sitios originales para redirigir a los usuarios a instalaciones Mpack infectadas.

Por sí sólo, *Mpack* no es capaz de comprometer servidores web, pero sí a los usuarios finales. El comprador del programa debe instalar el *toolkit* en un servidor al que pueda acceder y comprar los nombres de usuario y contraseña para conseguir el acceso a servidores comprometidos. Entonces, el atacante añade etiquetas iFrame a los sitios web de esos servidores, consiguiendo que los visitantes sean redireccionados a servidores maliciosos.

Después de haber logrado esto, otros componentes de *MPack* explotan los potenciales agujeros de seguridad que el usuario tiene en su ordenador, para poder descargar y ejecutar otros códigos maliciosos.

Origen de infección



Fuente: S21sec

La primera versión de este *toolkit*, denominada *Mpack 0.32*, contenía cuatro exploits y se vendía por $700 aproximadamente. Tras ésta, se fueron incorporando nuevos componentes (exploit XML, Quicktime y WinZip, ANI, ofuscación javascript y panel de estadísticas). Como muestra de su perfeccionamiento, en las últimas versiones *Mpack 0.90* y *Mpack 0.99* se ha añadido un exploit más y el coste ha aumentado a $1000.

> "Estamos ante un problema real que engloba una compleja infraestructura y en el que están implicadas numerosas organizaciones criminales"

Un caso real: Storm Worm

Storm Worm es el nombre de un troyano de distribución masiva creado en Rusia, cuya técnica de infección consiste en enviar un mail a las víctimas incitándolas a abrir un archivo adjunto con apariencia de noticia reciente.

El 19 de enero del 2007, el troyano comenzó a infectar miles de ordenadores en Europa y en los Estados Unidos a través de un correo electrónico que contenía el siguiente asunto: "Fallecen 230 personas debido a los fuertes temporales que azotan Europa". El 22 de enero, alcanzó un 8% de las infecciones globales, llegando a controlar hasta 10.000.000 ordenadores que funcionaban con Windows.

Cuando este troyano infecta un ordenador, lo une a una *Botnet* empleando un protocolo P2P que permite al *herder* controlarlo. Su principal objetivo es la difusión por spam y los ataques *DDoS* (puede encontrarse más información en la página web: www.joestewart.org).

Así pues, el ataque mediante código malicioso es un problema real que engloba una compleja infraestructura y en el que están implicadas numerosas organizaciones criminales, por lo que es necesario el desarrollo de unos sistemas de protección eficaces para poder prevenirlos.

Las últimas versiones de *malware* han encendido la alarma en los servidores de organismos públicos, empresas y particulares. Se habla incluso de *Ciber-warfare* o *guerra cibernética*, ante las proporciones cada vez mayores de los ataques y la sofisticación de la ingeniería social.

Es primordial, por tanto, la colaboración entre Equipos de Respuesta ante Incidentes (como el CCN-CERT del Centro Criptológico Nacional), las empresas y las fuerzas de seguridad para crear estrategias eficaces y combatir esta creciente amenaza.