

## Virus: engranajes de una cadena criminal

Mercè Molist (\*)

<http://ww2.grn.es/merce/who.html>

28 de septiembre de 2005

Los virus se convierten en engranajes de una cadena criminal donde las grandes empresas son la víctima más débil.

El 17 de agosto, la mujer del tiempo de la cadena CNN se disculpaba porque su pronóstico era poco detallado, debido a que sólo funcionaba uno de sus ordenadores. El responsable era Zotob, un gusano que en pocas horas infectó a corporaciones como Disneylandia, el "New York Times", "ABC News" o el "Financial Times". Zotob ha puesto sobre la mesa una combinación explosiva que los expertos han detectado en el último año: la creación de virus por dinero y la debilidad de las grandes empresas ante ellos.

Zotob es un gusano que no difiere mucho de los de su especie. No se transmite por correo electrónico sino que aprovecha un fallo en los sistemas operativos Windows 2000 para entrar en los ordenadores, saltando de uno a otro sin ayuda humana. Les instala una puerta trasera, para que los atacantes puedan controlarlos remotamente.

Lo que sorprende de Zotob es su rapidez: el 9 de agosto, Microsoft daba a conocer un agujero en Windows 2000 y su correspondiente parche. Cinco días después, cuando pocos habían instalado el parche, aparecía Zotob, que se colaba por el agujero. En tres días infectó a diversas corporaciones de Estados Unidos, mientras surgían gusanos parecidos, como IRCBot y Bozori, y se desencadenaba una guerra de virus.

El 26 de agosto, después de la investigación más veloz en la historia del crimen informático, el FBI detuvo en Marruecos a Farid Essebar (Diablo), de 18 años, y en Turquía a Atilla Ekici (Coder), de 21 años, como presuntos autores de Zotob. Más tarde el número de sospechosos subiría a 16. El FBI afirmó que "Coder" estaba relacionado con redes de robo informático de números de tarjetas bancarias y que pagó a "Diablo" por la creación de Zotob y otro gusano, Mytob.

Mytob, nacido en febrero y aún activo, se propaga por correo electrónico. Es muy parecido a Zotob y a la mayoría de virus que circulan en la actualidad: instalan puertas traseras en los ordenadores, de forma que puedan controlarse remotamente. El objetivo es crear vastas redes de equipos esclavos, por los que compiten diversos grupos en las cada vez más frecuentes guerras entre virus, donde se desactivan los unos a los otros, luchando por el control de los ordenadores.

Su fin último es el dinero. Lo afirma José Manuel Crespo, director de Marketing de Producto de Panda Software: "El mundo de los virus está cambiando desde el año pasado, cuando aparecieron Sober, Netsky, Bagle y Mydoom. Dentro de su código había textos que los creadores se mandaban unos a otros, con mensajes como: "Lo siento, no es nada personal, es por mi trabajo" y otros que relacionaban virus con dinero y negocio".

En este nuevo crimen organizado, los virus son un eslabón. Por una parte, se usan para robar cuentas de correo de las libretas de direcciones, que se venderán para enviarles correo basura, fraudes y más virus. "Después de la aparición de Sober, el 'spam' mundial aumentó un 4%", explica Crespo. Además, instalan programas que espían los comportamientos del usuario, para venderlos a empresas de publicidad, y otros que monitorizan las pulsaciones del teclado, para cazar números de cuentas bancarias y contraseñas.

Por otra parte, instalan puertas traseras en los ordenadores, que los criminales usan en diversos cometidos: mandar correo basura, virus y timos; alojar páginas web fraudulentas que imitan las de bancos o empresas, para que los incautos dejen allí sus datos, o convertirlos en armas para bombardear, en ataques de Denegación Distribuida de Servicio (DDoS), a empresas a las que se pedirá un rescate.

Estas extorsiones son cada vez más frecuentes. El último caso conocido sucedía el 25 de agosto: la empresa de juegos en línea Jaxx.de, de Hamburgo, sufría un ataque DDoS y se veía conminada a pagar 40.000 euros para que cesase. Otra muestra es PGPCoder, un virus aún rudimentario, aparecido en junio, que cifraba todos los documentos del ordenador infectado y pedía un rescate para descifrarlos.

"Antes los virus eran bichitos que te ponían en la pantalla el monstruo de las galletas pidiendo "cookies". Ahora son una herramienta que tiene un proceso de producto. La creación ya no pertenece a una sola persona, es una factoría: uno hace el programa que explota el fallo, otro el virus, otro lo lanza. Cuando leemos que se ha capturado al creador de un virus, nos reímos, probablemente sólo sea uno y de los tontos", afirma Crespo.

Un ordenador infectado se cotiza en el mercado negro por entre 2 y 3 céntimos. Un red de 5.500 equipos se alquila por 350 dólares. Por eso, explica Crespo, "hoy no te vas a enterar de que tu máquina está infectada, los virus están ocultos porque detrás hay negocio, buscan pasar desapercibidos y se van actualizando ellos mismos, convirtiendo el equipo infectado en lo que quieren".

Es el fin de la era de los virus masivos, dice Bernardo Quintero, responsable del servicio VirusTotal de Hispasec Sistemas: "Cuando aparece un virus masivo, en poco tiempo los antivirus distribuyen vacunas. Pero los virus actuales quieren sobrevivir el mayor tiempo posible en los sistemas sin ser detectados. Así, en vez de hacer un virus que llame la atención, hacen muchas variantes con pequeñas modificaciones, para infectar al máximo número de usuarios, mientras se crean las vacunas".

Del virus Mytob han llegado a aparecer cinco nuevas versiones en un mismo día. "Cada una infectará a un grupo reducido de usuarios, pero en conjunto obtienen mejores resultados", explica Quintero. También de Zotob aparecieron rápidas mutaciones. Según el Centro de Alerta Temprana Antivirus, su incidencia en España fue mínima y no aparece en ninguna lista mundial de los virus más masivos de agosto, pero su efecto fue fulminante en sitios localizados, especialmente en los Estados Unidos y concretamente en grandes empresas.

No hay indicios que confirmen que Zotob se concibiese para atacar a corporaciones pero, según Quintero, "las características de la vulnerabilidad que aprovechaba hacían que tuviese más posibilidades de propagación en entornos corporativos. Supongo que sus creadores eran conscientes de ello, aunque su intención fuese atacar todo tipo de sistemas".

Zotob tenía bastantes limitaciones para infectar a usuarios domésticos: debían usar Windows 2000, un sistema operativo más frecuente en las empresas, y tener abierto un puerto que los "routers" de ADSL y cortafuegos cierran siempre. Sólo estaban expuestos los usuarios domésticos de Windows 2000 que se conectasen por módem a la red telefónica básica, sin cortafuegos.

Las corporaciones, con decenas de miles de ordenadores, donde es usual tener un cortafuegos que protege la frontera entre la intranet e Internet, pero sin seguridad en los ordenadores del interior, eran caldo de cultivo para Zotob. Dice Quintero: "Seguramente el gusano entró por la puerta principal del edificio, dentro del portátil de algún periodista que se había infectado en un congreso o similar y, cuando volvió a su puesto de trabajo, enchufó el portátil a la red de la empresa".

En pocos minutos, un sólo ordenador conectado a la intranet generó cientos de infecciones. Lo mismo sucedió en el pasado con otros gusanos, como Blaster, Sasser o SQL Slammer, que llegó a infectar una central nuclear y, según José Manuel Crespo, "estaba diseñado específicamente para las empresas".

Esta situación, dice Quintero, "es el resultado de la falsa sensación de seguridad que existe en las redes corporativas, donde se relaja la seguridad de las estaciones de trabajo por el hecho de tener un cortafuegos corporativo que separa la red local de Internet. Cuando el gusano logra llegar a la red local, se expande rápidamente y puede suponer un colapso global".

Explica Crespo: "De alguna forma, hoy las empresas son más vulnerables a los virus que los usuarios particulares. El problema está en el exceso de confianza de los administradores de sistemas que, por otra parte, deben controlar miles de ordenadores, y en la forma como hay que actualizar los equipos, a mano y gastando mucho tiempo y ancho de banda: el fabricante de "software" debería favorecer a las grandes corporaciones el distribuir cómodamente los parches".

Marcos Gómez, del Centro de Alerta Antivirus, añade: "Parte de la inseguridad de las corporaciones proviene de sus propios usuarios, debido a su desconocimiento o falta de formación en seguridad, con ejemplos tan claros como abrir un correo en un idioma desconocido o adjuntos no solicitados".

David Emm, consultor de Kaspersky Lab, hablaba en un reciente artículo de la nueva era de los "business worms" (gusanos de negocios) que causarán explosiones en redes de grandes corporaciones, sin afectar en cambio a la Internet global: "No vendrá por un cambio en la forma cómo se programan los virus sino por el hecho de que las organizaciones se han puesto detrás de cortafuegos 'impenetrables', creyendo que están seguras ante cualquier ataque. El golpe desde el interior será peor por el hecho de ser totalmente inesperado".

Esta debilidad de las corporaciones se hace más preocupante ante el panorama de criminalidad organizada en el mundo de los virus. Bernardo Quintero no ve difícil que en el futuro se cree más código malicioso dirigido exclusivamente a grandes empresas: "Una vez desarrollé un troyano experimental, para un congreso, que se podía introducir fácilmente en una corporación, mediante muchos métodos, como enviar un correo electrónico con un programa oculto a una estación de trabajo de la empresa, que detectara qué vulnerabilidades tenía".

Una vez introducido el troyano, Quintero podía comunicarse con él y recibir datos sin ser detectado: "En vez de ponerme en contacto con él, era él quien, automáticamente, se comunicaba conmigo para recibir órdenes, visitando una web. De esta forma pasaba los sistemas de seguridad de la empresa, porque sus ordenadores suelen tener permitido navegar por Internet".

No es ciencia ficción. Se han dado ya casos de programas maliciosos hechos a medida para abrir puertas traseras en ordenadores que contienen información sensible. A mediados de mayo, en Israel, detenían a 18 personas, entre ellas altos ejecutivos, por espionaje industrial a empresas de la competencia mediante troyanos. En julio, se desvelaba que 300 departamentos críticos del gobierno británico habían sufrido ataques consistentes en el envío personalizado de troyanos por correo electrónico a altos responsables.

#### Relacionados:

Fuerza bruta contra creatividad, los gusanos buscan el dinero  
<http://www.hispasec.com/unaaldia/2362>

Rise of the "business worm"?  
<http://www.viruslist.com/en/analysis?pubid=168953110>

So, who is Diabl0?  
<http://www.f-secure.com/weblog/archives/archive-082005.html#00000641>

(\*) *Copyleft 2005 Mercè Molist.*  
*Verbatim copying, translation and distribution of this entire article is permitted in any medium, provided this notice is preserved.*