Los 5 Virus Informáticos Más Destructivos De Todos Los Tiempos

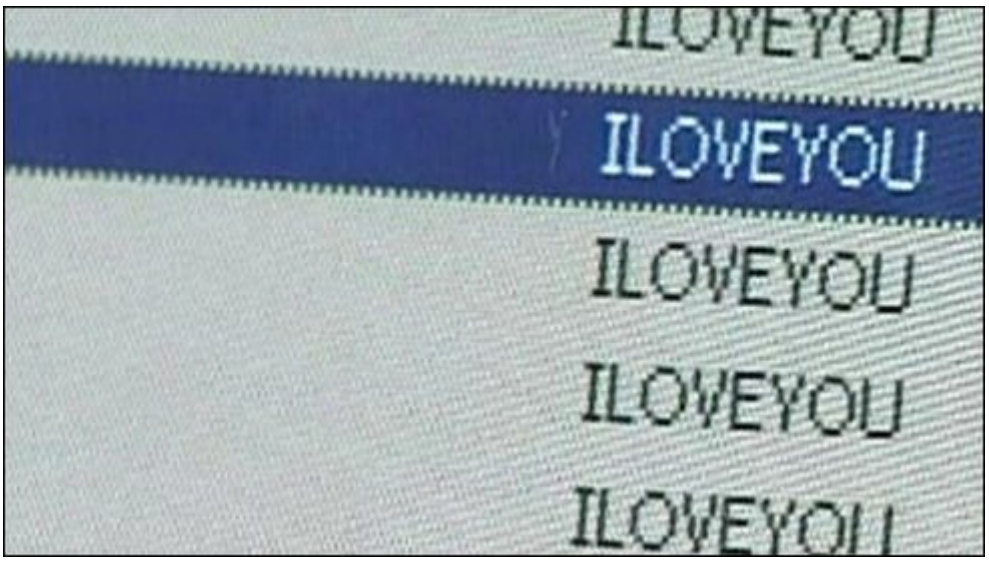
Ser infectado por un virus informático, le ha pasado a cualquier usuario de una forma u otra. Para la mayoría, es simplemente una molestia leve, lo que requiere de una limpieza de programas maliciosos y luego la instalación de algún programa antivirus. En otros casos, puede ser un completo desastre, hasta llegar a que el ordenador se convierta en un ladrillo costoso. Triste, pero puede llegar a suceder.

En esta lista, vamos a destacar algunos de los **peores y populares virus informáticos** que han causado mucho daño en la vida real. Estos **programas maliciosos** han causado daños irreparables, que ascienden a miles de millones de dólares. Aquí están los 5 **virus informáticos más famosos y dañinos** de la historia.

1. ILOVEYOU

El **virus ILOVEYOU** es considerado uno de los virus informáticos más esparcidos en la historia informática. El virus se las arregló para causar estragos en los **sistemas informáticos de todo el mundo**, causando daños por un total estimado de $10 mil millones de dólares. Se cree que el 10% de los ordenadores

conectados a Internet en el mundo han sido infectados por esta **aplicación maliciosa**. Era tan dañino, que los gobiernos y las grandes corporaciones decidieron dejar de lado el uso del correo electrónico, con la finalidad de evitar la conexión a internet.



El virus fue creado por dos programadores filipinos, **Reonel Ramones** y **Onel de Guzmán**. Lo que hicieron, fue utilizar la ingeniería social para conseguir que la gente abriera sin mayor problema el archivo adjunto; en este caso, una confesión de amor. El archivo adjunto era en realidad una secuencia de comandos que se hace pasar por un archivo TXT, el cual ocultaba la extensión real del archivo. Una vez se hace clic, se enviará en sí a todo el mundo en la lista de correo del usuario y procede a sobrescribir archivos, por lo que el equipo deja de funcionar correctamente. Los dos nunca fueron acusados□□, ya que no existían leyes sobre malware. Sin duda esto dejaría un precedente para ahondar sobre la legislación para este tipo de «delitos».

2. Code Red

El **virus Code Red** apareció por primera vez en el 2001 y fue descubierto por dos empleados de **eEye Digital Security**. Fue nombrado **Code Red** porque los empleados que realizaron el descubrimiento estaban bebiendo **Code Red Mountain Dew** en el momento que hallaron el virus. Los ordenadores con el **servidor web Microsoft IIS** instalados, explotaba un problema de desbordamiento de búfer en el sistema. Dejaba muy poco rastro en el disco duro, ya que es capaz de correr por completo en la memoria, con un tamaño de **3.569 bytes**. Una vez infectado, se procederá a realizar un centenar de copias de sí mismo, pero debido a un error en la programación, se duplicaba aún más y consumía una gran cantidad de los recursos de los sistemas.

A continuación, iniciaba un **ataque de denegación de servicio** en varias direcciones IP, famoso entre ellos el sitio web de la Casa Blanca. También permitía el acceso mediante una puerta trasera en el servidor, lo que permite el **acceso remoto a la máquina**. La característica peculiar del virus, era el mensaje

que dejaba atrás en las páginas web afectadas, «**Hacked By chino!**«. Un parche fue liberado más tarde y se estimo que causó $ 2 mil millones de dólares en perdidas. Un total de 1 a 2.000.000 servidores se vieron afectados, lo cual es sorprendente si tenemos en cuenta que había 6 millones de servidores IIS en aquel entonces.

3. Melissa

Fue desarrollado por **David L. Smith** en 1999, comenzó como un documento de Word infectado que fue publicado en el grupo de Usenet en alt.sex, que dice ser una lista de contraseñas para los sitios pornográficos. Esto hizo que la gente curiosa haya descargado y abierto el archivo, se activaría un macro interno y se pusiera en marcha el virus. El virus le enviaba por correo en sí a las 50 personas en la libreta de direcciones de correo electrónico del usuario y esto provocó un aumento del tráfico de correo electrónico, interrumpiendo los servicios de **correo electrónico de los gobiernos y las corporaciones**. También a veces dañado documentos mediante la inserción de una referencia a los Simpsons en ellos.

Smith fue finalmente capturado cuando **rastrearon** el documento de Word a él. El archivo fue subido con una cuenta de AOL robada y con su ayuda, la policía pudo arrestarlo en menos de una semana desde que comenzó el brote. Él cooperó con el FBI en la captura de otros creadores de virus, famosos entre ellos el creador del **virus Anna Kournikova**. Por su cooperación, pagó sólo 20 meses, y una multa de 5.000 dólares de su condena de 10 años. Según informes, el virus causó $ 80 millones de dólares en daños y perjuicios.

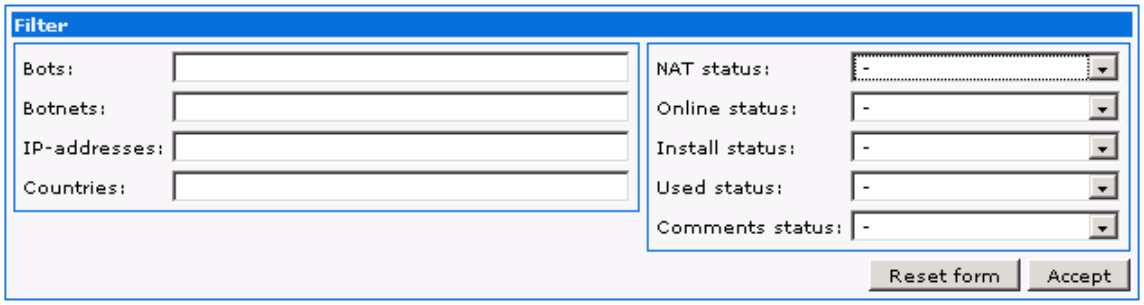
4. Sasser

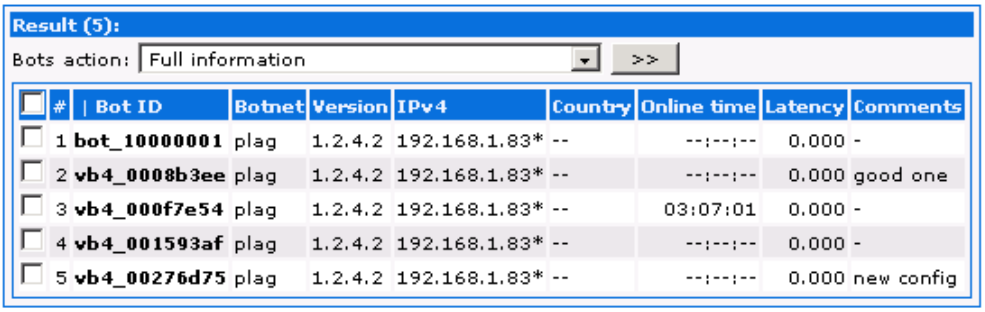
Este **gusano de Windows** se descubrió por primera vez en 2004, fue creado por el estudiante de ciencias de la computación **Sven Jaschan**, que también creó el **gusano Netsky**. Si bien la propia carga útil puede ser visto simplemente como molesto (se ralentiza y se bloquea el equipo, mientras que es difícil de restablecer sin cortar la alimentación), los efectos eran increíblemente perturbadores, con millones de computadoras infectadas. El gusano se aprovechó de una **vulnerabilidad de desbordamiento de búfer** en el servicio de subsistema de autoridad de seguridad local (**LSASS**), que controla la directiva de seguridad de las cuentas locales que causan accidentes en el ordenador. También utilizará los recursos del sistema para propagarse a otras máquinas a través de Internet e infectar a otros automáticamente.

Los efectos del virus se han generalizado mientras que el exploit ya fue parcheado. Esto llevó a más de **un millón de infecciones**, sacando las infraestructuras críticas, como las líneas aéreas, agencias de noticias, el transporte público, hospitales, transporte público, etc En general, se estimó que la avería ha costado $ 18 mil millones de dolares. **Jaschan** fue juzgado como un menor de edad y recibió una sentencia suspendida de 21 meses.

5. Zeus

Zeus es un troyano desarrollado para infectar las computadoras Windows, para llevar a cabo diversas tareas delictivas. La más común de estas tareas son generalmente el **man-in-the-browser** keylogging y realizar robos. La mayoría de los ordenadores estaban infectados ya sea a través de descargas no autorizadas o estafas de phishing. Identificado por primera vez en 2009, logró comprometer a miles de cuentas FTP y los ordenadores de grandes multinacionales y bancos, tales como **Amazon, Oracle, Bank of America, Cisco**, etc. Quienes controlaban la **botnet Zeus** lo usaron para robar las credenciales de acceso de red social , correo electrónico y cuentas bancarias.





Sólo en los EE.UU., se estima que más de **1 millón de computadoras** fueron infectadas, con el 25% en los EE.UU. Toda la operación era sofisticada, con la participación de personas de todo el mundo para actuar como mulas de dinero para el contrabando y la transferencia de dinero en efectivo a los cabecillas de Europa del Este. Unos **$ 70 millones de dólares** fueron robados. 100 personas fueron detenidas en relación de la operación. A finales de 2010, el creador de Zeus anunció su retiro, pero muchos expertos creen que esto es falso.