

La **Información** como arma contra los virus

Presentada por:

Ignacio M. Sbampato

Webmaster de Virus Attack! y de EnciclopediaVirus.com

Sábado 08 de Noviembre de 2003
SIMO - Madrid

Temario de la conferencia:

1) Introducción

- Actualidad de los virus informáticos
- Estadísticas actuales de infecciones a nivel mundial
- Los virus y el correo electrónico
- Los virus y los agujeros de seguridad

2) La información como herramienta

- La información disponible en internet
- Sitios de actualidad antivirus
- Sitios de empresas antivirus
- Alertas y boletines de seguridad
- ¿Qué más hacer?
- Información y desinformación
- La educación del usuario y del administrador

> Actualidad de los virus informáticos

- Tipos de virus como los infectores de archivos, virus polimórficos y macrovirus ya no son tan reportados.
- Los principales virus hoy en día son los gusanos de internet y los troyanos.
- Los virus con mayor índice de reportes son gusanos que aprovechan el correo electrónico y/o los agujeros de seguridad para propagarse
- En muy poco tiempo (horas, minutos) un nuevo virus puede convertirse en una epidemia mundial

> Estadísticas actuales de infecciones a nivel mundial

- 1.9 % de los correos analizados contienen virus, según el Centro de Alerta Temprana del Ministerio de Ciencia y Tecnología.
- 1 de cada 120 mensajes procesados por MessageLabs. posee archivos adjuntos infectados.
- En los rankings de virus más detectados por las compañías antivirus a nivel mundial, al menos 9 de los TOP 10 son gusanos de internet, ya sea de correo electrónico o de redes.
- Los 5 virus más reportados en España son: Dumaru, Gibe.C, Mimail, Mimail.C y Klez.h, en España. (Fuente: CAT)
- En el resto del mundo, los 6 más detectados de la actualidad, según distintas estadísticas, son: Swen, Dumaru, Sobig, Mimail.C, Blaster y Klez.h.
- Menos el Blaster, todos ellos son gusanos que aprovechan el correo electrónico para reproducirse.

> Los virus y el correo electrónico

- Es el medio más utilizado por los virus porque es el más utilizado de internet para comunicarse
- Su rapidez permite que un virus se propague dentro de una empresa en cuestión de segundos, y en el mundo, en cuestión de horas
- Permite incluir archivos adjuntos, código HTML, objetos embebidos; todos medios de transporte de virus informáticos
- Potencialmente hablando, un virus que utilice el correo electrónico puede llegar a **toda internet** porque todos los cibernautas tienen, al menos, una casilla de correo electrónico

> Los virus y los agujeros de seguridad

- Las vulnerabilidades permiten a los virus reproducirse **automáticamente.**
- Pueden ser combinadas con otros medios de reproducción: recursos compartidos, correo electrónico, IRC, mensajeros instantáneos, etc.
- Un gusano que se propague por correo electrónico aprovechando un agujero de seguridad seguramente aumentará su velocidad de reproducción.
- Los virus muchas veces explotan vulnerabilidades antiguas, pero muchos usuarios y administradores olvidan o no saben que deben instalar los parches para corregirlas y evitar problemas de seguridad.
- Toda aplicación o sistema operativo puede contener agujeros de seguridad.

> Herramientas contra los virus

- Antivirus
- Cortafuegos
- Anti-troyanos
- Anti-keyloggers
- Otros productos de seguridad

> La información disponible en internet

- Noticias
- Descripciones de virus
- Artículos técnicos
- Tutoriales
- Estadísticas
- Y muchas otras cosas más...

Algo importante: toda esta información es **¡GRATIS!**.

> Sitios de actualidad antivirus

ENCICLOPEDIA VIRUS
virus informáticos A-Z

VSantivirus
Virus/Ataques/Trucos
Estar enterado para estar seguro

Virus Attack
el mejor lugar para defenderte de los virus

HISPASEC SISTEMAS
SEGURIDAD Y TECNOLOGÍAS
DE LA INFORMACIÓN.



Alerta-Antivirus

Centro de Alerta Temprana sobre Virus y Seguridad Informática

> Sitios de compañías antivirus

- Alertas y descripciones de nuevos virus
- Manuales de usuario
- Tutoriales
- Artículos técnicos
- Resolución de problemas con los productos

> Alertas y boletines de seguridad

- Dan aviso sobre nuevos virus
- Informan cuando un virus aumenta su propagación
- Alertan sobre agujeros de seguridad y parches críticos
- Brindan noticias y artículos de relevancia en su casilla de correo

> ¿Qué más hacer?

- Más componentes de la comunidad de internet deben preocuparse de la seguridad antivirus
- Los ISP deberían proveer manuales básicos de protección antivirus para los usuarios que contraten sus servicios
- Los proveedores de ordenadores deberían hacer lo mismo
- Las empresas conectadas a la red deberían proveer información y políticas de seguridad antivirus a sus empleados

> Información y desinformación

- No todo lo que se lee sobre virus informa, a veces **desinforma**
- En el pasado, empresas han inflado noticias sobre virus para llamar la atención hacia sus productos
- Los virus se han vuelto un tema tan llamativo, que los medios de comunicación no especializados publican artículos relacionados, muchas veces desinformando más de lo que informan
- Las fuentes de información que utilicemos deben ser confiables, imparciales y objetivas

> La educación del usuario y del administrador

- La información debe servir para educar a quienes la lean
- Sin usuarios y administradores informados, la defensa contra los virus siempre será reactiva y nunca proactiva
- Con información, podemos prevenir, en vez de siempre tener que curar

¡GRACIAS POR PARTICIPAR DE ESTA CONFERENCIA PARA EL SIMO 2003 DE MADRID!

¿PREGUNTAS?

Para más información sobre virus informáticos lo invitamos a visitar
<http://www.encyclopediavirus.com>, <http://www.virusattack.com.ar> y
<http://www.alertaantivirus.es>