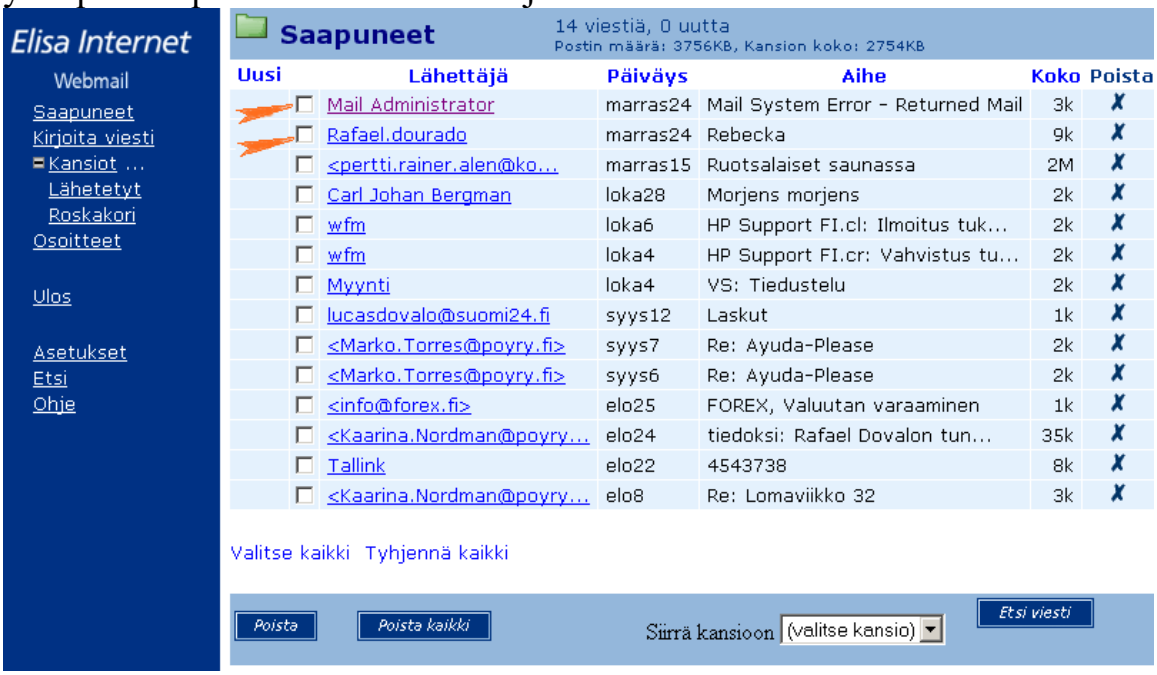
¡CUIDADO CON LOS GUSANILLOS!

Helsinki a 25 de Noviembre de 2005

Como vosotros sabéis dispongo de dos direcciones de correo electrónico: rafael.dovalo@kolumbus.fi que es el que me suministra la conexión ADSL, y rafael.dovalo@gmail.com el correo que más uso, por la simple razón de que es el mejor y además gratis.

Ayer día 24 entré en el correo Kolumbus para ver lo que allí había y simplemente lo que yo aquí marqué con las flechitas rojas.



El primero que abrí fue el de **rafael.dourado** por la curiosidad de un nombre parecido al mío y contenía lo siguiente:

un archivo ZIP normal "**Valentyne.zip**" OK. Como yo nunca abro los ZIPs en el mismo correo lo pasé a una carpeta TEMPORAL. Una vez allí con la mosca detrás de la oreja lo examino con el "**explore**" y observo que contenía dentro un ejecutable pequeñito de 10kb de tamaño llamado "**12.exe**". Inocentemente abro el ZIP y quedo mirando el dichoso ejecutable que salió de dentro "**12.exe**" que me sigue extrañando bastante. Me imaginé, tal vez algo simpático. Pero bastante desconfiado antes de ejecutarlo le pasé el antivirus **F-SECURE** que normalmente actualizo cada semana y no me detecta ningún peligro.
OK, lo ejecuto y el maldito gusanillo me conecta el programa "**Paint Shop Pro**" cargándose una imagen similar al logo de **XP-Windows**. Como el chiste no me causa ninguna gracia lo apago y fuera.

¡Ahá! Ahora llega lo interesante.

Una vez apagado el "**Paint Shop Pro**" lo que me hace el gusanito es **ocultarme** todo el **Desktop**, sin dejarme ni iconos ni barra de herramientas ni nada, sólo una pantalla totalmente cubierta de azul como un cielo. Lo que se me ocurre en ese momento es apagar todo con el interruptor y encender de nuevo. Aparentemente parece que se enciende normal, aparecen los iconos del **Desktop** y la sintonía de entrada en **XP-Windows** y "**paff**" de nuevo todo se queda cubierto de azul. Ya no me quedan dudas, **es un virus**.

Me pasa por la mente la idea de formatear todo y empezar de nuevo la instalación del sistema, pero al pulsar la combinación de teclas **CTRL, ALT y DELETE** se me abre el "**Task Manager**" y descubro que hay otras opciones para apagar con "**Shut Down**" etc. Descubrí que al entrar por la esquina superior izquierda "**File**" seleccionando "**New Task**" y "**Browse**" me daba acceso a las carpetas del disco duro. Esta era mi suerte ya que mandé al perrito a buscar los ejecutables (***.exe**) con fecha del 24-11-2005 y me descubre una docenita de ejecutables que el dichoso gusanillo había creado, los renombro con la terminación en (***.ex0)** para luego destruirlos. Hice lo mismo con los controladores (***.dll)** con la misma fecha renombrándolos por **(*.dl0)** y esta vez he tenido mucha suerte.

¿Qué se aprende de todo esto?

Que nunca se debe abrir un E-mail cuando se desconozca al remitente y menos ejecutar un (archivo.exe) cuando existan dudas de su procedencia.

Hoy he vuelto a entrar en el correo **Kolumbus** para asegurarme de que todavía guardo el gusanillo allí por si alguien lo quiere examinar, y lo más curioso resulta que hay otro mensaje que antes no había leído procedente de **postmaster@vodafon.es**: Al parecer este gusanito había enviado un mensaje en mi nombre a un usuario de **Vodafone.es** con el archivo adjunto "**Cybil.zip**" infectado. Menos mal que el antivirus de **Vodafone.es** lo había detectado y me lo comunica, cosa que **Elisa-Kolumbus** pasó por alto.

Fijarse en el texto que se lee al final de la imagen capturada de Elisa Internet.

Elisa Internet

Webmail

Saapuneet
Kirjoita viesti
Kansiot ...
Lähetetyt
Roskakori
Osoitteet

Ulos

Asetukset
Etsi
Ohje

Lue viesti — Tulostusnäkymä

Lähettäjä: Mail Administrator <postmaster@vodafone.es>
Päiväys: 2005/11/24 to AM 04:31:00 EET
Vastaanottaja: rafael.dovalo@kolumbus.fi
Aihe: Mail System Error - Returned Mail

Vastaa | Vastaa kaikille | Välitä | Poista | Siirrä kansioon (valitse kansio)

This Message was undeliverable due to the following reason:

The following destination addresses were unknown (please check
the addresses and re-mail the message):

SMTP <rafael.dovsa@vodafone.es>

Please reply to <postmaster@vodafone.es>
if you feel this message to be in error.

Reporting-MTA: dns; psismtp7.vodafone.es
Received-From-MTA:dns; smtpas1.vodafone.es (212.166.186.192)
Arrival-Date: Thu, 24 Nov 2005 03:30:57 +0100

Final-Recipient: rfc822;rafael.dovsa@vodafone.es
Diagnostic-Code: smtp;551 User unknown
Action: failed
Status: 5.1.6
Last-Attempt-Date: Thu, 24 Nov 2005 03:31:00 +0100

Lataa liite: liite21

Lähettäjä: "Rafael.dovalo" <rafael.dovalo@kolumbus.fi>
Päiväys: 2005/11/24 to AM 04:29:10 EET
Vastaanottaja: "Rafael.dovsa" <rafael.dovsa@vodafone.es>
Aihe: Alice

FOTO-1

Estimado usuario:
Este correo electronico tenia un archivo adjunto ("Cybil.zip") infectado.
Dicho archivo ha sido eliminado por la plataforma anti-virus de Vodafone.
Por favor, contacte con el remitente para que le envie dicho fichero sin virus.
Muchas gracias.

Dear customer:
This email had an infected file ("Cybil.zip") attached.
It has been removed by the Vodafone anti-virus platform.
Please ask the sender to resend the uninfected file to you again.
Thank you.

Lataa liite: Vodafone-Attachment-Warning.txt