

II CAMPAÑA CONTRA EL FRAUDE ONLINE Y POR LA SEGURIDAD EN LA RED.  
**Analizamos la nueva variante del gusano Win32/Stration.**

**En las ultimas horas se detecto un numero muy elevado de correos electrónicos que contienen una nueva variante del famosos gusano Win32/Stration, muchos profesionales del sector de seguridad alertan que pueden ser la consecuencia de un intento de infectar miles de maquinas con el ultima vulnerabilidad que afecta a Microsoft (ANI).**

El gusano viene por medio de un correo electrónico con el asunto: **Mail server report.**

Este correo simula un problema de seguridad originado por nuestra IP y viene acompañado de un fichero ZIP, Update-KB\*\*\*\*-x86.zip

Si usted no ejecuta este fichero no será infectado.

Después de ejecutar el gusano en nuestro laboratorio de pruebas comprobamos como trabaja.

Primero ejecutamos el fichero que en realidad es el primer enlace para una nueva descargar del verdadero gusano.

El gusano hace varias conexiones a Internet dos de ellas son estos servidores:

<http://buheradesunme.com>  
<http://jikunhetyadeshin.com>

Uno de ellos esta deshabilitado, pero otro aun esta activo y hace la descarga de un nuevo fichero:

<http://buheradesunme.com/ntsrv32.exe>

Cuando finaliza la descarga completa del fichero de autoejecuta y crea nuevos ficheros:

Este busca la direcciones del usuario infectado para reenviar el gusano a nuevas víctimas, el problema es que también nos modifica el fichero HOST (%System%\drivers\etc\hosts) para no dejar acceder a diferente sitios web:

download.microsoft.com  
go.microsoft.com  
msdn.microsoft.com  
office.microsoft.com  
windowsupdate.microsoft.com  
<http://www.microsoft.com/downloads/Search.aspx?displaylang=en>  
avp.ru  
www.avp.ru  
<http://avp.ru>  
<http://www.avp.ru>  
kaspersky.ru  
www.kaspersky.ru  
<http://kaspersky.ru>  
kaspersky.com  
www.kaspersky.com  
<http://kaspersky.com>  
kaspersky-labs.com  
www.kaspersky-labs.com  
<http://kaspersky-labs.com>  
avp.ru/download/  
www.avp.ru/download/  
<http://www.avp.ru/download/>  
<http://www.kaspersky.ru/updates/>  
<http://www.kaspersky-labs.com/updates/>  
<http://kaspersky.ru/updates/>  
<http://kaspersky-labs.com/updates/>  
downloads1.kaspersky-labs.com  
downloads2.kaspersky-labs.com  
downloads3.kaspersky-labs.com  
downloads4.kaspersky-labs.com  
downloads5.kaspersky-labs.com  
<http://downloads1.kaspersky-labs.com>  
<http://downloads2.kaspersky-labs.com>  
<http://downloads3.kaspersky-labs.com>  
<http://downloads4.kaspersky-labs.com>  
<http://downloads5.kaspersky-labs.com>  
<http://downloads1.kaspersky-labs.com/products/>  
<http://downloads2.kaspersky-labs.com/products/>  
<http://downloads3.kaspersky-labs.com/products/>  
<http://downloads4.kaspersky-labs.com/products/>  
<http://downloads5.kaspersky-labs.com/products/>  
<http://downloads1.kaspersky-labs.com/products/>  
<http://downloads2.kaspersky-labs.com/products/>  
<http://downloads3.kaspersky-labs.com/products/>  
<http://downloads4.kaspersky-labs.com/products/>  
<http://downloads5.kaspersky-labs.com/products/>  
downloads1.kaspersky-labs.com/updates/  
downloads2.kaspersky-labs.com/updates/  
downloads3.kaspersky-labs.com/updates/  
downloads4.kaspersky-labs.com/updates/  
downloads5.kaspersky-labs.com/updates/  
<http://downloads1.kaspersky-labs.com/updates/>  
<http://downloads2.kaspersky-labs.com/updates/>

<http://downloads3.kaspersky-labs.com/updates/>  
<http://downloads4.kaspersky-labs.com/updates/>  
<http://downloads5.kaspersky-labs.com/updates/>  
<ftp://downloads1.kaspersky-labs.com>  
<ftp://downloads2.kaspersky-labs.com>  
<ftp://downloads3.kaspersky-labs.com>  
<ftp://downloads4.kaspersky-labs.com>  
<ftp://downloads5.kaspersky-labs.com>  
<ftp://downloads1.kaspersky-labs.com/products/>  
<ftp://downloads2.kaspersky-labs.com/products/>  
<ftp://downloads3.kaspersky-labs.com/products/>  
<ftp://downloads4.kaspersky-labs.com/products/>  
<ftp://downloads5.kaspersky-labs.com/products/>  
<ftp://downloads1.kaspersky-labs.com/updates/>  
<ftp://downloads2.kaspersky-labs.com/updates/>  
<ftp://downloads3.kaspersky-labs.com/updates/>  
<ftp://downloads4.kaspersky-labs.com/updates/>  
<ftp://downloads5.kaspersky-labs.com/updates/>  
<http://updates.kaspersky-labs.com/updates/>  
<http://updates1.kaspersky-labs.com/updates/>  
<http://updates2.kaspersky-labs.com/updates/>  
<http://updates3.kaspersky-labs.com/updates/>  
<http://updates4.kaspersky-labs.com/updates/>  
<ftp://updates.kaspersky-labs.com/updates/>  
<ftp://updates1.kaspersky-labs.com/updates/>  
<ftp://updates2.kaspersky-labs.com/updates/>  
<ftp://updates3.kaspersky-labs.com/updates/>  
<ftp://updates4.kaspersky-labs.com/updates/>  
[viruslist.com](http://viruslist.com)  
[www.viruslist.com](http://www.viruslist.com)  
<http://viruslist.com>  
[viruslist.ru](http://viruslist.ru)  
[www.viruslist.ru](http://www.viruslist.ru)  
<http://viruslist.ru>  
<ftp://ftp.kasperskylab.ru/updates/>  
[symantec.com](http://symantec.com)  
[www.symantec.com](http://www.symantec.com)  
<http://symantec.com>  
[customer.symantec.com](http://customer.symantec.com)  
<http://customer.symantec.com>  
[liveupdate.symantec.com](http://liveupdate.symantec.com)  
<http://liveupdate.symantec.com>  
[liveupdate.symantecliveupdate.com](http://liveupdate.symantecliveupdate.com)  
<http://liveupdate.symantecliveupdate.com>  
[securityresponse.symantec.com](http://securityresponse.symantec.com)  
<http://securityresponse.symantec.com>  
[service1.symantec.com](http://service1.symantec.com)  
<http://service1.symantec.com>  
[symantec.com/updates](http://symantec.com/updates)  
<http://symantec.com/updates>  
[updates.symantec.com](http://updates.symantec.com)  
<http://updates.symantec.com>

eset.com/  
www.eset.com/  
http://www.eset.com/  
eset.com/products/index.php  
www.eset.com/products/index.php  
http://www.eset.com/products/index.php  
eset.com/download/index.php  
www.eset.com/download/index.php  
http://www.eset.com/download/index.php  
eset.com/joomla/  
www.eset.com/joomla/  
http://www.eset.com/joomla/  
u3.eset.com/  
http://u3.eset.com/  
u4.eset.com/  
http://u4.eset.com/  
www.symantec.com/updates

Si usted fue infectado compruebe su fichero HOST el único contenido que tiene dejar es su loopback : 127.0.0.1 localhost

En todos los casos recomendamos la máxima prudencia y que no haga caso de este tipo de correos electrónico y NUNCA pulsar sobre los enlaces que contiene NI TAMPOCO SUS FICHERO ADJUNTOS.

Actualice su antivirus diariamente.

### **Comisión de Seguridad en la Red.**

José María Luque Guerrero

<http://seguridad.internautas.org> - [www.seguridadenlared.org](http://www.seguridadenlared.org) - [www.seguridadpymes.es](http://www.seguridadpymes.es)

Asociación de Internautas. [www.internautas.org](http://www.internautas.org)

## **II CAMPAÑA CONTRA EL FRAUDE ONLINE Y POR LA SEGURIDAD EN LA RED**

*El Instituto Nacional de Tecnologías de la Comunicación (INTECO), la Asociación de Internautas, Panda Software , Telefónica y ONO lanzan la "II CAMPAÑA CONTRA EL FRAUDE ONLINE Y POR LA SEGURIDAD EN LA RED" [www.seguridadenlared.org](http://www.seguridadenlared.org). La misma se desarrollará desde el 15 de marzo hasta el lunes 9 de mayo de 2007*

Fecha artículo: 2007-04-03 17:04:33 - url artículo: <http://www.internautas.org/html/4154.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)