

Alerta correos electrónicos que contienen un troyano que está infectando miles de maquinas.

En los próximos días tengan cuidado con los correos electrónicos que reciban con ficheros adjuntos y con asuntos llamativos como:

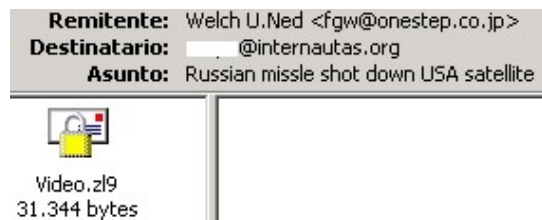
- Fidel Castro dead.
- Hugo Chavez dead.
- Sadam Hussein alive!
- Sadam Hussein safe and sound!

- Russian missile shot down Chinese satellite
- Russian missile shot down USA aircraft
- Russian missile shot down USA satellite
- Chinese missile shot down USA aircraft
- Chinese missile shot down USA satellite
- Radical Muslim drinking enemies' blood.
- U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel
- U.S. Southwest braces for another winter blast. More than 1000 people are dead.
- Venezuelan leader: "Let's the War beginning".
- President of Russia Putin dead
- Third World War just have started!
- The Supreme Court has been attacked by terrorists. Sen. Mark Dayton dead!
- The commander of a U.S. nuclear submarine lunch the rocket by mistake.
- First Nuclear Act of Terrorism!

Este asunto esta cambiando en las ultimas horas.

El correo contiene un fichero ejecutable con algunos de los siguientes nombres;

- **Video.exe**
- **Full Video.exe**
- **Read More.exe**
- **Full Text.exe**
- **Full Clip.exe**



Estos pueden variar en las ultimas horas.

Este fichero ejecutable es un **TROYANO DOWNLOADER** que los antivirus aun no detectan pues tenga el máximo cuidado en los próximos días por este brote de correos infectados.

Como detectar que esta infectado, busque en los siguientes directorios:

WindowsSystem32

WinntSystem32

Los ficheros: wincom32.sys / wincom32.ini y peers.ini

También crea la cadena:

HKLM >SYSTEM >Current Control >Set Services >wincom32

Servicios: wincom32 Agregar wincom32

El troyano utiliza el proceso SERVICES.EXE para saltarse los cortafuegos.



```
6b 6c 69 || ...[blackli
31 37 46 || st].FC4FB9D8817F
35 39 46 || 80482040387B159F
32 46 38 || 193C=5805118E2F8
44 37 36 || E00.F67DDAF10D76
37 41 33 || 6D8C650B9F2EE7A3
32 34 46 || AD63=3E4BF0AD24F
33 46 45 || E00.F046A2B6F3FE

c1 70 87 01 8b 0d || At. | \ - . . | Ap | . | .
2c 11 01 00 83 25 || T - . . | È t . y . . . . | %
6e 00 63 00 6f 00 || T - . . | À w . i . n . c . o .
77 00 69 00 6e 00 || m . 3 . 2 . . . . w . i . n .
00 00 00 00 77 00 || c . o . m . 3 . 2 . . . . w .
33 00 32 00 00 00 || i . n . c . o . m . 3 . 2 . . .
ec 81 ec 08 02 00 || | | | | | | | | y U | | | | | |
8b 5d 1c 56 8b 75 || . | D - . . | M . S | | . V | u
45 fc a1 6c ac 01 || . W | } . S y u . | E u | l - .
15 64 ac 01 00 33 || . V y u . . | À P W y . d - . . 3

04 00 73 00 || | . | - . . 3 À ^ [ È Á . . s .
73 00 2e 00 || e . r . v . i . c . e . s . . .
cc cc 8b ff || e . x . e . . | | | | | | | | y
68 3e 0d 01 || U | | | | . V W | È ó Ph > . .
0f 8c a3 00 || . è " p y y | ø 3 ø : b . | È
89 75 fc ff || . . | È ø P y 5 | - . . | u u y
00 ff 75 f8 || . T . . . : È . | | . . . y u ø
```

Este troyano es de la familia Downloader preparado para descargar un nuevo troyano mas peligroso para obtener el control de una maquina sin el consentimiento del usuario.

La Asociación de Internautas recomienda la máxima prudencia y no ejecuten ningún fichero sospechoso y desconfíe de este tipo de correos llamativos.

Fecha artículo: 2007-01-21 13:52:46 - url artículo: <http://www.internautas.org/html/1024.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