



Malware: tendencias y perspectivas

Sergio A. Becerril

CELE - UNAM

¿De qué estamos hablando?

- MALicious softWARE
 - Virus, gusanos, troyanos, backdoors, rootkits, spyware, scareware, crimeware... *whatware?*
- Software malicioso
 - No lo quiero
 - Actúa sin mi permiso
 - Propósito nocivo

Números: a la alza

- Más de 2.5 millones de *nuevo* malware en 2012.
- 11% más que en el 2011.
- 99.8% para Windows
 - +0.2% sobre 2011

Control y conocimiento

- Spyware ↑ 17.4%
- Troyanos ↑ 20.1%
- Backdoor ↑ 17.2%
- Downloader ↑ 16.9%

Sí es negocio

- Compra
 - “Kits”: \$500 - \$7,000 USD
- Venta
 - Licencia de conducir: \$5.60 USD
 - Tarjeta de crédito (c/info): \$24.50 USD
- Renta
 - Botnets a \$3/día, \$300/semana (USD)

* 2010 – 2011



Líderes del mercado

- Transferencias bancarias: Miles de cuentas, \$59,000,000 USD (Italia/Holanda/Alemania/...)
- Punto de venta 2: 500,000 T.C., \$30,000,000 USD (Australia/Rumania, 2012)
- Punto de venta 1: 80,000 T.C., \$10,000,000 USD (E.U.A./Rumania, 2008-2011)

Ciberterrorismo

- Stuxnet (06/10), Duqu (09/11), Flame (05/12)
- Punta de lanza tecnológica
 - Firmas digitales válidas
 - Cifrado
 - Explotación de Zero-Days
- Evolución: Gauss (08/12)

Respira profundo...



Prevención

- Correos electrónicos
 - URLs
 - Adjuntos
- Almacenamiento extraíble
- Actualizaciones
- Antivirus
 - ¡Actualizado!

Scareware

 Copyright violation alert



Copyright violation: privacy content detected

Windows has detected that you are using content that was downloaded violating copyright of its respective owners. Please follow the following bulleting and try to solve the problem by one of the recommended ways.

What has happened?

During the system scan Antipiracy foundation scanner has detected copyright issues. Please take a look at the list and choose an action: pass the case to a court or solve it in precourtive order by paying the penalty.

How it could occur?

Probably you've been using file-sharing clients, torrents or downloaded the following content straight from the website. Anyway, you've violated the copyright of respective owners. In most countries it follows the court prosecution and high-level penalties. Maximum penalties can be five years in prison and up to \$250,000 in fines.

Files detected

- f-secure.torrent
- ironman2-hd.torrent
- red.torrent

Lawsuites preview



Page 1/2



Page 2/2



A co-project by ICPP foundation



Evidence list

<html>

[Show details...](#)



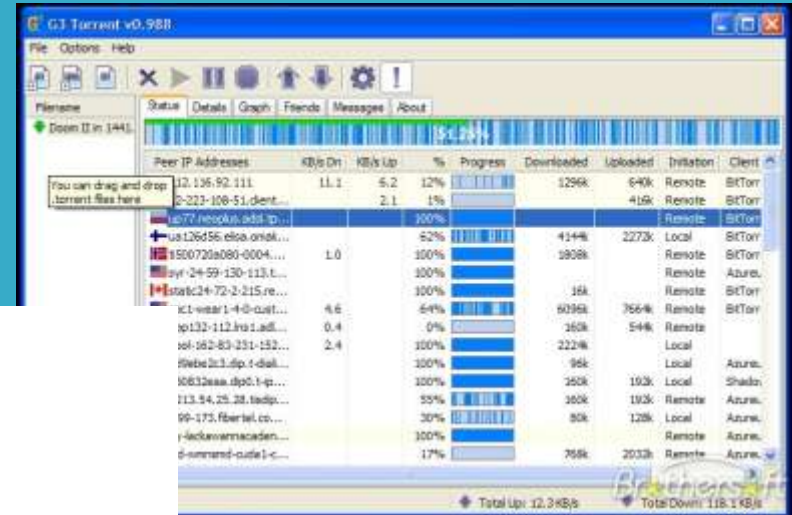
Used IPs log

255.255.255.255
255.255.255.255
255.255.255.255

Type of violation

- p2p\warez movie download
- p2p\warez games download
- p2p\warez mp3 download

Descargas



- 25% de descargas son falsas o troyanizadas



Pero por encima de todo...

¡Usa tu sentido común!



Para más información...



Sergio A. Becerril

sergio@cele.unam.mx

<http://sergiob.org>

<http://urli.st/QX6>