

4. Malware

1. Introducción al Malware

1.1 Introducción

“Malware” son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad de un ordenador. Este término engloba muchas definiciones como “Virus”, “Worm (gusano)” y “Trojan (troyano)” y otras como “Rootkit”, “Logicbomb (bomba lógica)” y “Spyware”. Este capítulo presentará, definirá y explicará cada una de estas subclases de malware, brindará ejemplos y explicará algunas de las contramedidas que pueden ser puestas en práctica para restringir los problemas que causa el malware.

OpenLearning

1.2 Situación del Malware

Antes de empezar a detallar tipos de malware, es interesante conocer la situación y algo de historia sobre este fenómeno.

- España dentro del Top 5 de países infectados
- Uno de cada tres ordenadores está infectado
- Cada incidente global: media de 20.000 máquinas infectadas
- Número de incidentes globales: 3.000
- Google: 10% de las páginas son maliciosas
- Antivirus: reconocen que no pueden soportar el ritmo: miles de nuevos códigos dañinos al día

La evolución del malware ha sido espectacular en los últimos años y ha dejado de ser un software creado por una única persona a estar desarrollado por organizaciones complejas con estructuras jerárquicas donde cada componente tiene perfectamente definidas sus funciones:

- Dirección
- Programadores expertos
- Spammers
- Pen-testers
- Administradores de sistemas
- Herders
- Mulas

Se ha convertido en un negocio que maneja millones de dólares al año (se estima que 12 veces más que el fraude tradicional).

Además, implica menos riesgos que los fraudes “de antes”:

- No hay (casi) leyes internacionales
- Entorno distribuido
- Phishing, pharming, trojans, vishing, ...

Y puede afectar a cualquiera:

- Instituciones financieras
- Telcos
- E-commerce
- Instituciones públicas (gobierno), pagos online, juegos online, subastas, ...
- Cualquier compañía o institución con sitio en Internet (¡¡o no!!)

La evolución del malware ha llevado consigo la aparición de una nueva forma de negocio. La infraestructura para desplegar este malware está en venta o en alquiler:

- Bullet-proof hosting: Hosting en el que se garantiza al cliente que no entregarán sus datos a las autoridades, a cambio de una fuerte suma de dinero, independientemente de lo posiblemente ilegales que puedan ser sus actividades.
- Kits de phishing
- Kits de código dañino
- Redes maliciosas (e.g. Russian Business Network)

Amparados en países permisivos:

- Rusia
- Hong-Kong
- Panamá
- Corea del Norte
- EEUU ¿?

Vamos a ver en el siguiente apartado un ejemplo de esta infraestructura, que quizás quede un poco lejos en el tiempo, pero demuestra la evolución de este negocio y ha sido uno de los casos más estudiados y documentados dentro del malware.

OpenLearning

1.3 Russian Business Network (RBN)

La Russian Business Network (más conocida como la RBN) era una compañía que supuestamente proporcionaba alojamiento e infraestructura web a la creciente industria del malware, convirtiéndose así en una especie de centro de operaciones mundial desde donde se descargaban los troyanos y hacia donde viaja la información robada.

La RBN se encontraba en St. Petersburg y proporcionaba alojamiento web. Su actividad parecía estar íntimamente relacionada con la industria del malware, hasta el punto de que muchos ISP decidieron bloquear directamente toda conexión con direcciones pertenecientes a esta red. Y no sólo malware. Se dice que la mitad del phishing mundial estaba alojado impunemente en alguno de sus servidores.

Entre los años 2000 y 2007 no era fácil encontrar un incidente criminal a gran escala en el que no aparezcan por algún sitio las siglas RBN (o "TooCoin" o "ValueDot", nombres anteriores con los que había sido conocida). En 2005 se estaba aprovechando de forma masiva una vulnerabilidad en Internet Explorer para instalar un keylogger. Se demostró que la mayoría de datos robados iban a parar a un servidor de la RBN. Los servidores de la RBN estaban detrás del incidente contra la HostGator en 2006. Aprovechando un fallo en Cpanel, consiguieron tener acceso a cientos de webs de la compañía.

En 2007, la empresa de hosting gratuito IPOWER también fue atacada y se instalaron en sus páginas "frames" que de forma transparente redirigían a sitios en la RBN donde se intentaban instalar troyanos. Malware como Gozi, Grab, Metaphisher, Ordergun, Pinch, Rustock, Snatch, Torpig... todos se han servido de los servidores de la RBN para "alojarse" o alojar datos. Los ejemplos son muchos y variados.

Mpack la herramienta usada en varios ataques masivos durante 2007, era vendida desde uno de los servidores de la RBN.

Ante tanta evidencia, fueron muchos los administradores que decidieron bloquear por completo el acceso a los servidores alojados en la RBN. Pero no sirvió de mucho. Aprendieron a enrutar las conexiones a través de otras webs comprometidas en Estados Unidos y Europa de forma que, aunque fuese dando un rodeo a través de otras IPs (habitualmente usuarios residenciales troyanizados o webs atacadas), seguían operando de forma normal. Por ejemplo, en el ataque al Banco de la India, al seguir el rastro del malware que se intentaba instalar en los sistemas Windows que visitaban la web, se observó que tras pasar la información a través de varios servidores, finalmente acababa en un servidor de la RBN.

Tras las acusaciones publicadas en el Washington Post, un tal Tim Jaret que decía pertenecer a la RBN lo negaba todo. Decía que no podía entender por qué se le acusaba basándose en suposiciones. El tal Jaret incluso se quejaba de que intentó colaborar con el grupo antispam Spamhaus (que tenía continuamente bloqueadas nada menos que más de 2.000 direcciones IP de la RBN clasificadas como origen de correo basura) sin éxito.

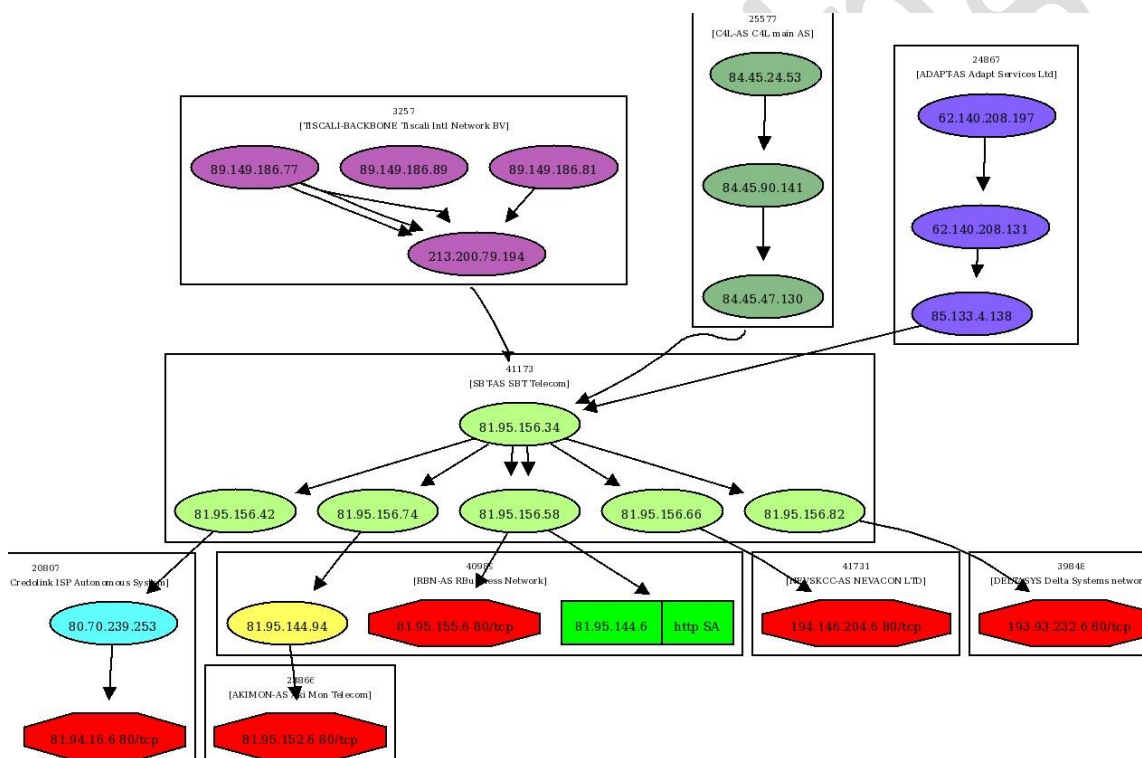
En SANS Internet Storm Center tenían una clara opinión al respecto, no iban a tirar piedras sobre su tejado. Y es que según Verisign, la RBN cobraba hasta 600 dólares mensuales por un alojamiento "a prueba de balas" lo que en este caso significa que no cederá a presiones legales ni será cerrado por muy inapropiado o "infeccioso" que sea su contenido. Aun así, el tal Jaret afirmaba que la RBN tenía el nivel de "criminalidad" habitual en cualquier proveedor web, y que habitualmente cerraba las webs en menos de 24 horas, facilitando el trabajo a los profesionales de la seguridad. Sin embargo, es posible que la única acción de la RBN cuando recibía presiones

para cerrar un sitio web, fuese aumentar el "alquiler" a los delincuentes que se basaban en ella para operar.

La RBN (rusa, como la gran escuela creadora del malware 2.0) se convirtió así en cómplice y centro de operaciones web para la industria del malware, que encontraba un aliado que sabía mantener la boca cerrada y las manos quietas si se le pagaba lo suficiente. Symantec lo llamaba "el refugio para todo tipo de actividades ilegales en la Red".

Por si quedaba alguna duda sobre su intención de permanecer "anónimos", bastaba con comprobar hacia qué IP apunta su dominio principal rbnnetwork.com y una comprobación DNS.

RBN, ofrecía una completa infraestructura para los ciberdelitos. Phishing, malware, ataques DDoS, pornografía infantil...etc eran soportados por este ISP ruso. Para ello, se ponía a disposición del cliente varias botnets, shells remotas en servidores crackeados, servidores centralizados de gestión de estas actividades...etc. Numerosas formas de ataques (CoolWebSearch, vulnerabilidades VML, MPack...etc) eran lanzados o albergados en sus redes.



El 8 de noviembre de 2007, RBN desapareció repentinamente como podemos leer en esta noticia de Trend Micro:

NOVEMBER 8, 2007 | Somewhere around 7 p.m. Pacific time on Tuesday evening, researchers at Trend Micro noticed something very odd: Blocks of IP addresses linked to the notorious Russian Business Network (RBN) had suddenly disappeared off the Net.

But researchers say this is by no means the end of the RBN, which security experts say serves as an ISP and host for Websites that deal in child pornography, spam, and identity theft. Some speculated yesterday that RBN's upstream ISPs may have dropped the controversial provider from their networks, or that RBN is merely relocating to keep a lower profile. "We think they are probably just diversifying their operations due to all of the negative publicity surrounding their

operations the past couple of months," says Paul Ferguson, network architect with Trend Micro Inc. "This block of IP addresses has gone 'poof.' "

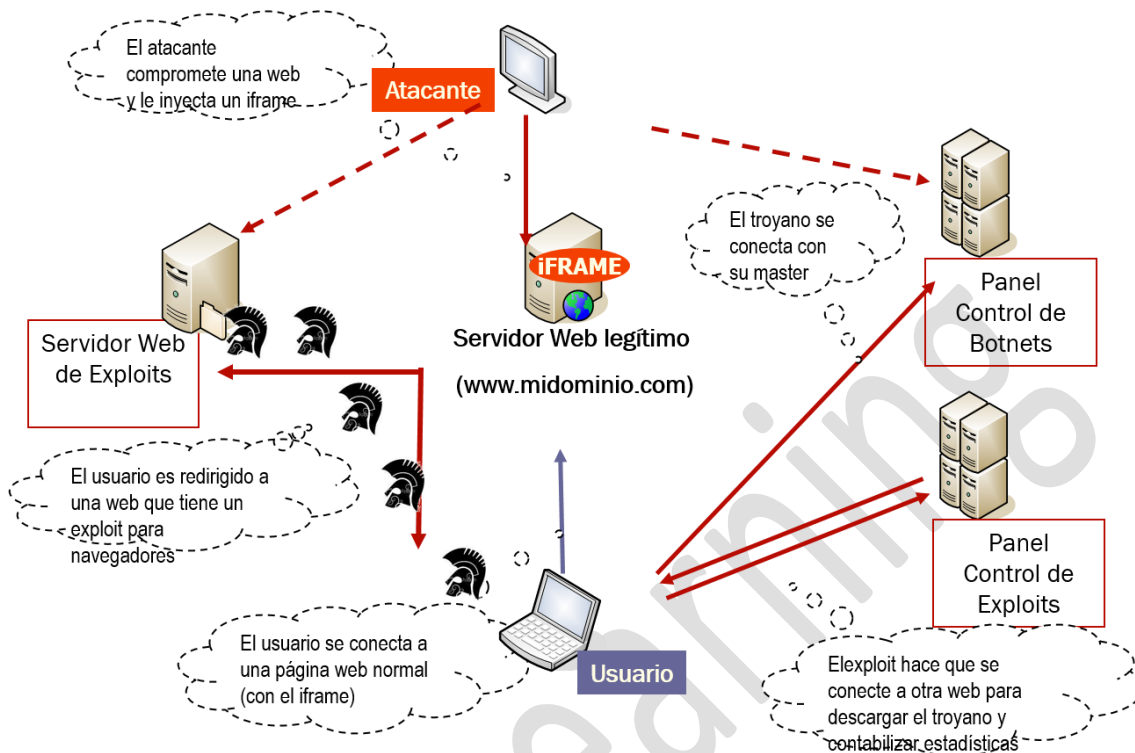
Ferguson says Trend Micro has seen suspicious activity in China and other parts of the Asia/Pacific that indicate RBN is trying to set up shop in more obscure and less regulated regions. "There have been lots of bulk registries of domains in China and Asia/Pacific," Ferguson says. "And we've seen some activities from iFrames similar to what RBN has done in the past to deliver malware. But right now, this is just what we suspect -- there's no way to tie that back to RBN."

Jamz Yaneza, research project manager for Trend Micro, says there are a large number of botnets associated with RBN, and he wouldn't be surprised if those were being used as a backup system for RBN in the interim.

RBN will pop up again, likely under other IP addresses that may make detecting it more difficult, they say. "This doesn't signal any end to their operations -- they are too 'clever' to walk away, and there's lots of money to be made," Ferguson says.

1.4 MPack

MPack es uno de los mejores ejemplos de paquetes de malware que estuvo activo durante varios años y del que se desarrollaron diferentes versiones, que incluían las últimas vulnerabilidades encontradas hasta el momento.



Entre otras características, enumeramos aquí algunas de las funcionalidades más importantes de MPack:

- Mass-exploits
- Exploits para navegadores web
- Actualizado constantemente con nuevos exploits
- HTML+Javascript exploits
- Utiliza PHP+BBDD para las estadísticas
- Los atacantes inyectan iframes en sitios normales para redirigir a los usuarios a instalaciones de Mpack

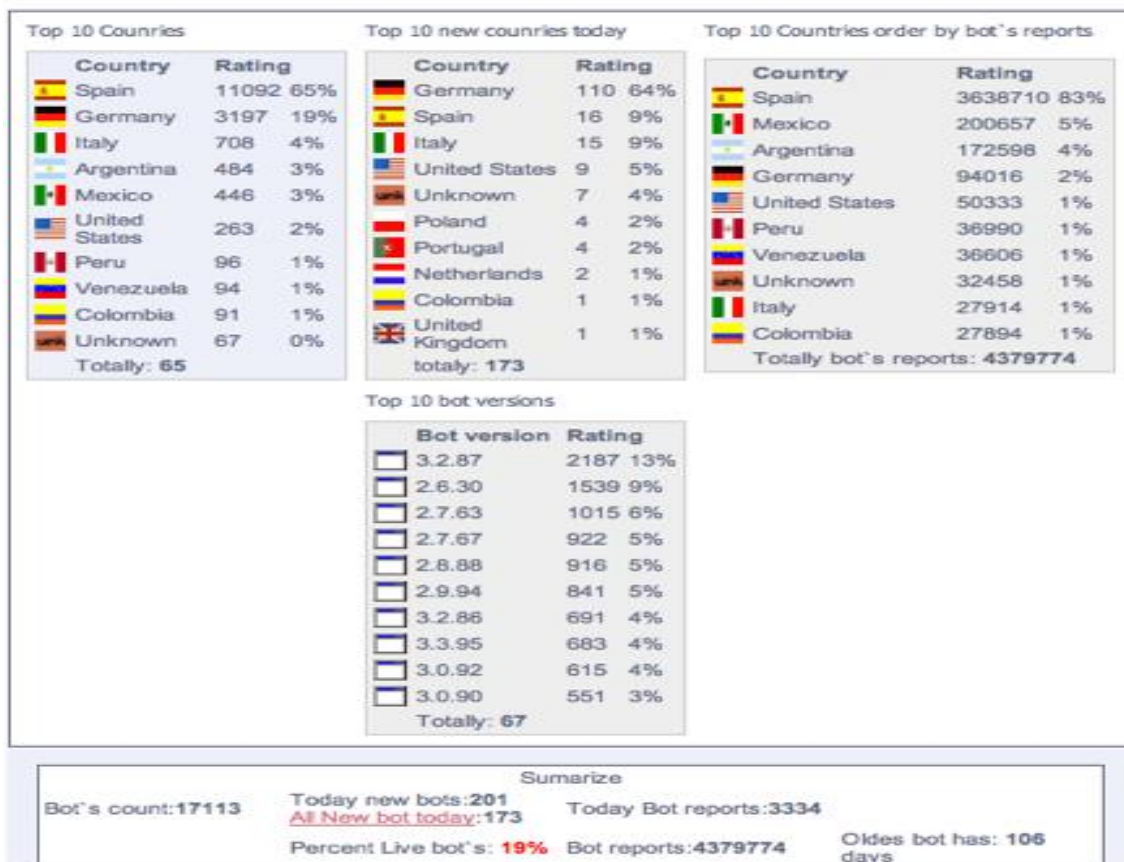
Algunas versiones conocidas:

- 0.32: cuatro exploits
- 0.33 Vale \$700
- 0.44 añade exploit XML
- 0.51 (ya en 2007): Añade Quicktime y WinZip
- 0.80: añade ANI
- 0.84: nueva ofuscación javascript
- 0.86: estadísticas. Esta es la versión usada en los ataques masivos
- 0.90: ya vale \$1000
- 0.99: añade un exploit

Algunos de sus exploits eran:

Exploit	Patch	Añadido a MPack	ID
Firefox 1.5, Opera 7.x	14/02/2006	24/09/2006	MS06-006
IE 6	11/04/2006	24/09/2006	MS06-014
Windows 2000 MMC	08/08/2006	24/09/2006	MS06-044
WebViewFolderIcon	10/10/2006	13/03/2007	MS06-057
IE XML Overflow	11/11/2006	20/12/2006	MS06-071
WinZip ActiveX Overflow	14/11/2006	13/03/2007	CVE-2006-5198
QuickTime Overflow	02/01/2007	13/03/2007	CVE-2007-0015
ANI Overflow	04/04/2007	03/04/2007	MS07-017

Contaba con un completo panel de control:



Que entrega a quien lo controlaba completas estadísticas de su funcionamiento:

Server time/date snapshot: 6-Jun-2007 21:08:39
195.55.122.65 (Spain)
MPack v0.90 stats

Attacked hosts (total - uniq)		Traffic (total - uniq)	
IE XP ALL	10454 - 10047	Total traff	12501 - 11881
QuickTime	1 - 1	Exploited	1502 - 1288
Win2000	428 - 411	Loads count	-
Firefox	1359 - 1332	Loader's response	0% - 0%
Opera7	3 - 3	Efficiency 0% - 0%	

Browser stats (total)		Modules state	
		Statistic type	MySQL-based
		User blocking	ON
		Country blocking	OFF

Country	Traff	Loads	Efficiency
ES - Spain	10748 86%	0 0%	0%
VE - Venezuela	376 3%	0 0%	0%
MX - Mexico	191 1.5%	0 0%	0%
US - United states	148 1.2%	0 0%	0%
PE - Peru	143 1.1%	0 0%	0%
CO - Colombia	131 1%	0 0%	0%
AR - Argentina	93 0.7%	0 0%	0%
PT - Portugal	91 0.7%	0 0%	0%
IS - Iceland	0 0%	0 0%	0%

Referer stats (>1)	
_http://www.playpapua.com/	4733 37.9%
_http://www.carloslatre.com/	2029 16.2%
_http://www.centro-zaragoza.com/	782 6.3%
_No referer	668 5.3%
_http://www.playpapua.com/index.php	638 5.1%
_http://www.dalbau.com/	411 3.3%
_http://www.valgrande-pajares.net/	179 1.4%
_http://www.feyalegria.org/	162 1.3%
_http://www.afirma.biz/	152 1.2%
_http://www.carloslatre.com	136 1.1%
_http://www.playpapua.com	120 1%
_http://www.agsm.es/	118 0.9%
_http://carloslatre.com/	99 0.8%
_http://www.bcnmedia.com/	95 0.8%
_http://playpapua.com/	70 0.6%

1.5 Modelo de Negocio

En capítulos anteriores hemos hablado de campañas internacionales de espionaje y de la ciberguerra, pero el problema del malware sigue afectando y mucho al usuario medio de Internet. Los atacantes no necesitan desplegar un software complejo para hacer dinero, les basta con tener como objetivo los millones de usuarios que diariamente navegan por la red y que no tienen los conocimientos técnicos mínimos o que son tan incautos como para pensar que no pueden ser un objetivo de estafadores.

Un simple ejemplo:

Broma de mal gusto

Virus informático "letal para humanos" causa alarma en Pakistán



[20/04/2007 - 08:10 CET]

Un virus para teléfonos móviles causa alarma entre abonados de telefonía celular en Pakistán, que temen contraerlo personalmente.

Diario Ti: La impresión de algunos usuarios es que al recibir el mensaje que acompaña el virus no solo el aparato quedará fuera de servicio, sino el propio usuario será infectado por el virus.

El Spam sigue siendo una de las formas preferidas de esparcir malware. El Spam contiene virus que dejan "puertas traseras" en el ordenador infectado.

Pero, ¿Quién sería tan estúpido de pulsar en un archivo adjunto? Ya no tiene por qué ser un archivo adjunto.

Algunos de los más extendidos por correo electrónico son hiperenlaces que el usuario pulsa sin darse cuenta de que hay un virus esperándole en el otro lado:

- Supuestos enlaces de pornografía
- Supuestos parches de un fabricante
- Enlaces "demasiado bueno para ser cierto"

Congratulations!

FREE* Sony® Cyber-shot® 5.0-Megapixel Digital Camera!

(Limited Time Offer. Hurry While Supplies Last!)



Sony® Cyber-shot® 5.0-Megapixel Digital Camera

- 5.0-megapixel Super HAD CCD image sensor
- 4x optical zoom/4x Smart Zoom (at VGA size)
- Crisp resolution in a stylishly compact design
- USB 2.0 interface for high-speed transfer

FREE!

FREE
Shipping
by
FedEx.

**Top
Rated
Gifts!**

Retail Price: ~~\$499.99~~ Your Price: FREE*

[Click Here to Continue with your FREE Gift](#)

I certify that I am a U.S. Resident over the age of 18, and I agree to the [privacy policy](#) and [participation terms](#).



*When you complete our offer eligibility requirements.
Offer valid only to residents of the United States who are at least 18 years old. ExclusiveRewards.com is a registered trademark of MetaReward, Inc. All other product and service names mentioned may be trademarks of their respective owners. You can unsubscribe by [clicking here](#). Mailing address: ExclusiveRewards Customer Service, PO Box 1267, San Carlos, CA 94070


ProductTestClub.com

sponsored by Consumer Research Corporation



New Member Incentive Promotion.

Free Sony Vaio A130 Notebook



~~\$1199~~ list price
Intel Celeron Mobile
Technology
15" 4:3 Display
Up to 2GB RAM & 80GB HD

Product Test Club

CRC is looking for new product testers in key US markets subject to the following eligibility requirements.

- **Over 18 years old**
- **Legal United States Resident**
- **Valid Email & Shipping address**

As a member, you will periodically receive promotional products to test from the comfort of home.

Simply complete a short user survey and all products are yours to keep (free) after evaluation.



Join the Product Test Club and receive at least 3 products to evaluate within your first 90 days GUARANTEED!

Click Here

Safe, secure savings on prescription drugs from Canada through a company right here in the U.S.

The only difference you'll notice is the amount of money you save.

<http://www.canadamedplan.com>

Click the link above to see how much money you can save.
If the link doesn't work, just copy and paste it into your browser.



Canada Medplan is a U.S. company organized to bring the substantial savings of drugs sold in Canada to Americans with safety and security. We're here to assist you in placing your order - and to see to it you receive the best, most professional pharmacy services available anywhere.

We've partnered with the largest and most respected direct mail pharmacy in Canada - RXNorth. The brand name drugs you receive from them are the same ones - from the same drug companies - you receive from your local drug store. Generic medications are manufactured in Canada under Health Canada's stringent requirements.

Podemos recomendar a todos los usuarios el uso de programas antimalware, pero este tipo de programas también están siendo usados desde hace varios años para distribuir malware.

¿Cómo pueden encontrar un programa anti-Adware nuestra madre/hermana/amigo que no son técnicos? Los Spammers usan nombres de archivos como "Ad-Aware" y "SpyWare Search & Destroy". ¿Cómo puede saber el usuario si es un programa antimalware legítimo o es falso?

1.6 Malware en Dispositivos Móviles

Actualmente el malware ya no es un fenómeno que afecta a nuestros ordenadores, sino que los dispositivos móviles se han convertido en un objetivo prioritario de estos ataques.

Hoy en día, llevar encima un teléfono móvil inteligente (“smartphone”) equivale a llevar un potente equipo informático en el bolsillo. Un número cada vez mayor de los teléfonos disponibles en el mercado actual, no sólo incluyen una cámara, sino que también ofrecen acceso en línea completo, teclado y otras muchas funciones que hasta ahora eran exclusivas del PC. Sin embargo, esta capacidad y comodidad no van asociadas solamente a ventajas. Al igual que nuestros equipos de sobremesa y portátiles, estos teléfonos móviles también están expuestos a amenazas de seguridad. Lo irónico de la evolución de esta tecnología lo encontramos en el hecho de que a medida que aumenta el número de funciones que incluyen estos teléfonos, más vulnerables se vuelven frente los mismos tipos de amenazas que hacen estragos en nuestros equipos portátiles y de sobremesa.

Tenemos un vídeo relacionado en el que tratamos las “Tendencias del Malware en Android”.