InSeguridad Informática
Piratas detrás del teclado: el gran negocio del hacker

Alejandra Stolk

Seguridad informática

- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo".
- A partir de estas definiciones no podríamos aceptar que seguridad informática es "la cualidad de un sistema informático exento de peligro", por lo que habrá que buscar una definición más apropiada.
- Algo básico: la seguridad no es un producto, sino un proceso.
- Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:

  "Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico."

- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

Jorge Ramió

Libro Electrónico de Seguridad Informática y Criptografía
Versión 4.1 de 1 de marzo de 2006

¿Qué es un hacker?

El concepto "hacker" surgió a finales de la década de los 60 y principios de la década de los 70 del siglo pasado, cuando algunos programadores del Massachussets Institute of Technology (MIT) se llamaron a sí mismos hackers, para mostrar que podían realizar programas o acciones que nadie había podido hacer antes, específicamente para hacer uso de acceso telefónico a redes.

A pesar de que existen diversas connotaciones para el término “hacker”, es comúnmente aceptado que un “hacker” es una persona que trata de conseguir acceso a un sistema, equipo o aplicación de forma remota y sin autorización.

¿Qué es un hacker?

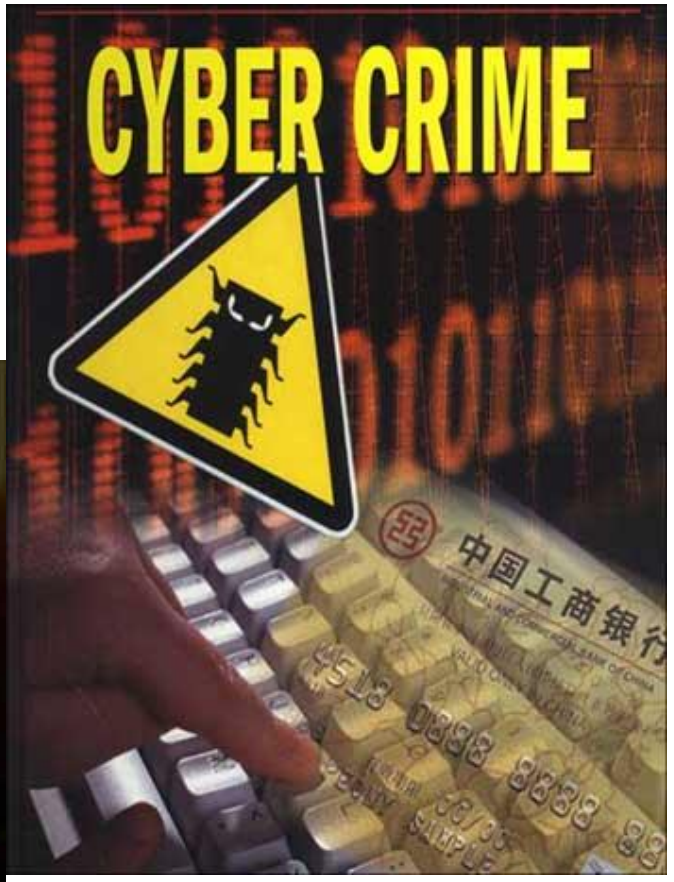
El concepto "hacker" surgió a finales de la década de los 60 y principios de la década de los 70 del siglo pasado, cuando algunos programadores del Massachussets Institute of Technology (MIT) se llamaron a sí mismos hackers, para mostrar que podían realizar programas o acciones que nadie había podido hacer antes, específicamente para hacer uso de acceso telefónico a redes.

A pesar de que existen diversas connotaciones para el término “hacker”, es comúnmente aceptado que un “hacker” es una persona que trata de conseguir acceso a un sistema, equipo o aplicación de forma remota y sin autorización.

¿Es un hacker bueno o malo?

Un hacker es "bueno" o "malo" dependiendo del **propósito** que tenga al entrar en un sistema:

De sombrero negro (Cracker): entra a los sistemas con el objetivo de obtener información clasificada o confidencial, destruir sistemas, causar una denegación de servicios. Sus intenciones son de carácter delictivo y fraudulento.



ParqueTecnologico
Mérida - Venezuela

¿Es un hacker bueno o malo?

De sombrero gris: es un hacker que utiliza sus conocimientos de forma ofensiva y defensiva. Normalmente, sus acciones ofensivas no tienen cómo objetivo el lucro o fraude sino la demostración de una vulnerabilidad o debilidad en un sistema operativo, aplicación, etc.

También entran en este grupo crackers "reformados" aquellos que comenzaron con sombrero negro y fueron moviéndose hacia el lado bueno de la "fuerza"

¿Es un hacker bueno o malo?

De sombrero blanco: Son aquellos individuos que se encargan de detectar vulnerabilidades y contrarrestarlas. Asimismo, publica sus hallazgos para que las debilidades encontradas sean solventadas.

Su propósito fundamental es mejorar los niveles de seguridad de sistemas operativos, aplicaciones, etc.

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Existen grupo de hackers que se dedican a:

Hackivist, o hacktivismo, actividad en la que grupos de hackers se dedican principalmente a realizar cambios en las páginas web (mascaradas o dephacements) de sitios con los que no están de acuerdo.

Normalmente, éstos hackers tienen razones políticas y normalmente no son objeto de persuciones policiales o arrestos

ParqueTecnologico
Mérida - Venezuela

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Hacktivismo

ParqueTecnologico
Mérida - Venezuela

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Hacktivismo

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Hacktivismo en Venezuela

ParqueTecnologico
Mérida - Venezuela

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Hacktivismo en Venezuela

ParqueTecnologico
Mérida - Venezuela

El crimen organizado en la Internet

Los cybercrimenes y su organizaciones

Hacktivismo en Venezuela

ParqueTecnologico
Mérida - Venezuela

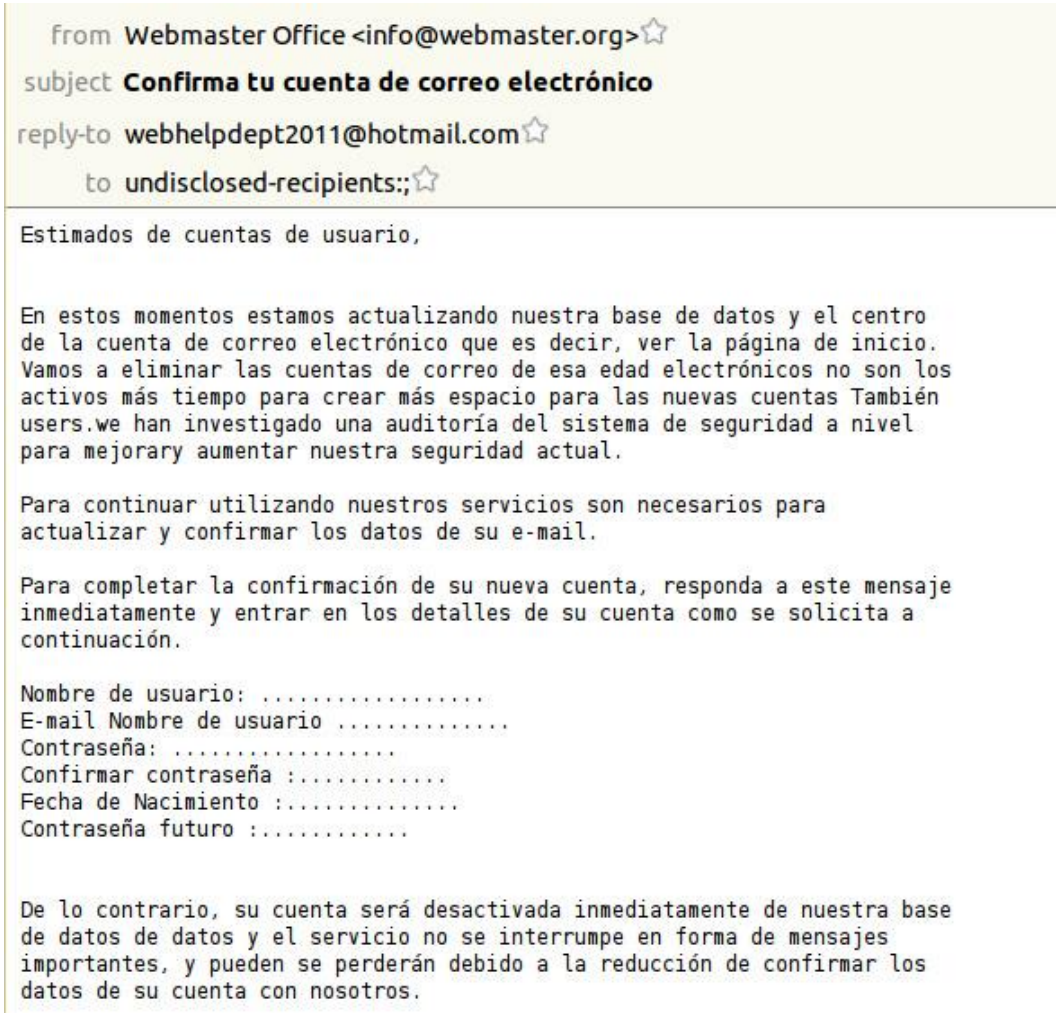
El crimen organizado en la Internet

El Phishing

Es un intento de obtener información de identificación personal a través del teléfono, correo electrónico, mensajería instantánea (IM) o fax, con el fin de robar la identidad, propiedad intelectual y, en última instancia, el dinero de los usuarios.

La mayoría de estos intentos adoptan la forma de acciones legítimas, es decir, parecen legales, pero en realidad son acciones delictivas.

Clásicos del Phishing:
...Se quedará sin acceso al email a menos que responda este correo....



from Webmaster Office <info@webmaster.org>
subject **Confirma tu cuenta de correo electrónico**
reply-to webhelpdept2011@hotmail.com
to undisclosed-recipients:;

Estimados de cuentas de usuario,

En estos momentos estamos actualizando nuestra base de datos y el centro de la cuenta de correo electrónico que es decir, ver la página de inicio. Vamos a eliminar las cuentas de correo de esa edad electrónicos no son los activos más tiempo para crear más espacio para las nuevas cuentas También users.we han investigado una auditoría del sistema de seguridad a nivel para mejorary aumentar nuestra seguridad actual.

Para continuar utilizando nuestros servicios son necesarios para actualizar y confirmar los datos de su e-mail.

Para completar la confirmación de su nueva cuenta, responda a este mensaje inmediatamente y entrar en los detalles de su cuenta como se solicita a continuación.

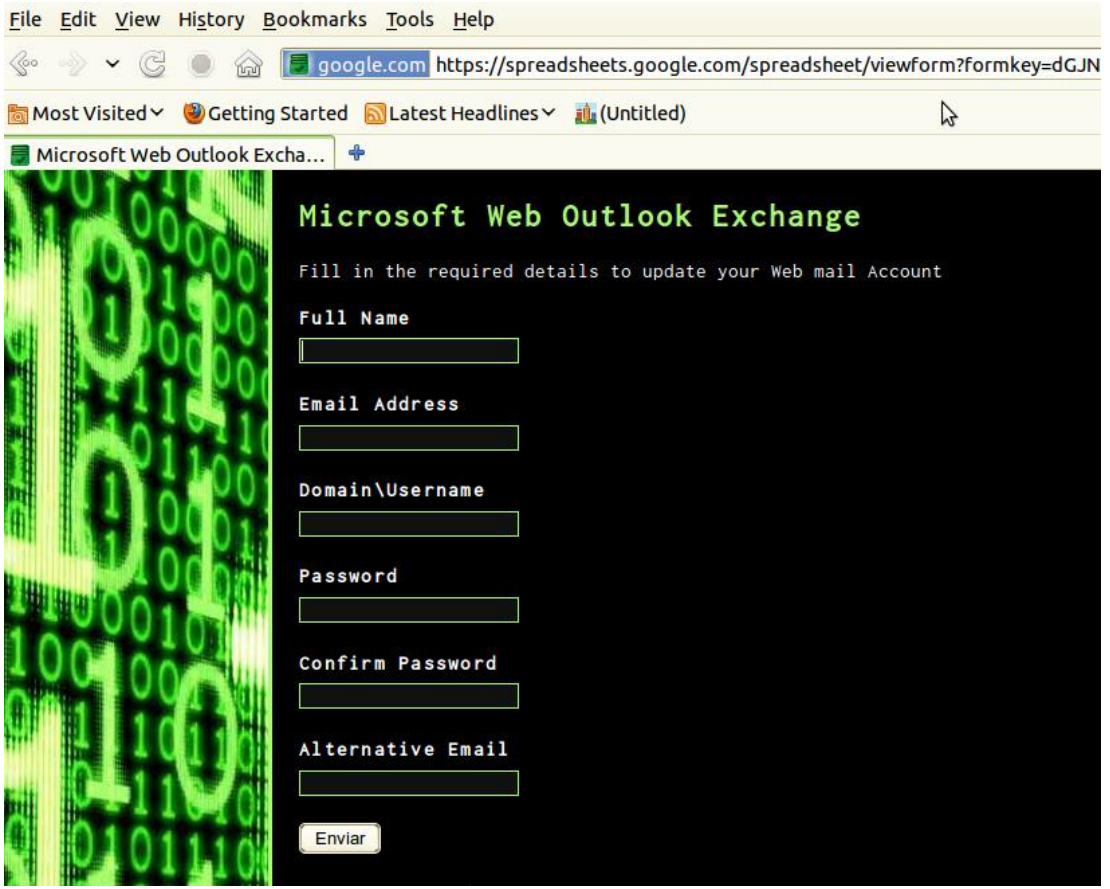
Nombre de usuario: .....
E-mail Nombre de usuario .....
Contraseña: .....
Confirmar contraseña :.....
Fecha de Nacimiento :.....
Contraseña futuro :.....

De lo contrario, su cuenta será desactivada inmediatamente de nuestra base de datos de datos y el servicio no se interrumpe en forma de mensajes importantes, y pueden se perderán debido a la reducción de confirmar los datos de su cuenta con nosotros.

El crimen organizado en la Internet

Pharming

El pharming es parecido al phishing, pero en lugar de solicitar directamente información personal o corporativa, secuestra las direcciones URL legítimas, como por ejemplo "www.mybank.com", para redirigirlas, a través de un servidor de nombres de dominio, hacia direcciones IP fraudulentas que falsean las direcciones originales. Acto seguido, estas direcciones URL falseadas se encargan de recopilar, por medio de una interfaz gráfica de usuario, la información protegida sin que los usuarios se den cuenta. Puesto que el pharming requiere un mayor grado de habilidad técnica para llevarse a cabo y los DNS son muy difíciles de manipular, es mucho menos común que el phishing.



El crimen organizado en la Internet

Phreaking

Phreaking es un término se utiliza para denominar la actividad de aquellos hackers que se dedican al aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último; electrónica aplicada a sistemas telefónicos.

Con éstos conocimientos logran realizar ataques de hombre en el medio para escuhar conversaciones, re-enrutar conversaciones, obtener conexiones, etc.

Los primeros hackers eran phreakers!

ParqueTecnologico
Mérida - Venezuela

Para estar claros

Amenaza

Cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Ejemplos de amenazas son los ataques humanos, los desastres naturales, los errores humanos inadvertidos, fallas internas del hardware o el software, etc.

Vulnerabilidad

Consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema.

Ataque

Es cualquier acción que explota una vulnerabilidad.

Exploit

Un exploit es un método específico para hacer uso de una vulnerabilidad. Pueden encontrarse en el mercado en forma de scripts, archivos ejecutables, macros, etc.

Para estar claros

Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. Normalmente, el autor no logra beneficios económicos pero pone en jaque mate a la organización.

Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

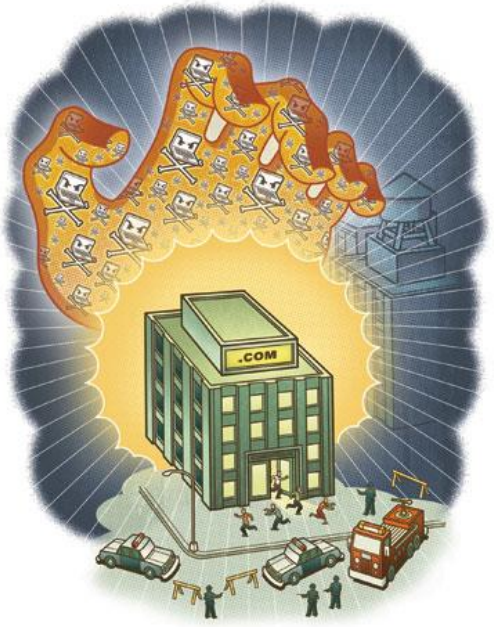
Tipos de ataques

Flujo Normal

Interrupción

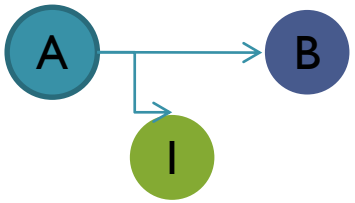
Interrupción

En el caso de una interrupción un activo del sistema se pierde, se hace no disponible o inutilizable. Un ejemplo de ello puede ser la destrucción malicios hardware o el borrado de un programa o archi



Tipos de ataques

Flujo Normal



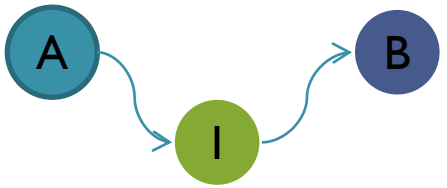
Intercepción

Intercepción

En el caso de una intercepción implica que alguien logre acceso no autorizado a un activo del sistema. Esta parte no autorizada puede ser una persona, programa, dispositivo, etc. Un ejemplo de ella puede ser el copiado de datos, la intervención de un canal de red.

Tipos de ataques

Flujo Normal



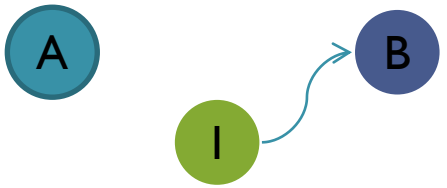
Modificación

Modificación

En el caso de que se realiza una intercepción y la parte no autorizada logra acceso a un activo del sistema y tiene la capacidad de manipularlo se trata de una amenaza por modificación.

Tipos de ataques

Flujo Normal



Fabricación

Fabricación

La parte no autorizada que accede al sistema también puede crear objetos falsos en un sistema. Ejemplo de ello son la inserción de transacciones en un sistema o BD, fabricación de paquetes de datos, etc.

Para estar claros


Image courtesy of: Tech Tips.com

Virus

Es un software diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, macros de aplicaciones y archivos ejecutables.

Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o memoria RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red ya que tienen la facultad de multiplicarse sin la intervención del usuario como el caso de Sasser

Para estar claros

Caballos de Troya

Es un virus que entra al computador y actúa de forma similar a este hecho de la mitología griega.

Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa, pasan de ser inadvertidos por algún tiempo. Sin embargo, cuando se comienzan a sentir sus efectos muchos equipos quedan inservibles y deben re-instalarse sus sistemas operativos

Image courtesy of: Tech Tips.com

Para estar claros


Image courtesy of: Tech Tips.com

Spyware

El spyware es un software que instenta recopilar información confidencial sobre los usuarios y sus claves en los equipo, pueden ser tan sofisticados que pueden tomar nota del contenido de archivo en donde encuentre la palabra password o clave.

Spam

El spam o correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y muchos dolores de cabeza.

Fases del Hackeo

1 Reconocimiento  

2 Escáneo 

3 Tomar acceso 

4 Mantener acceso 

5 Limpieza de trazas 

ParqueTecnologico
Mérida - Venezuela

Reconocimiento

El reconocimiento en términos de hackeo se refiere al levatamiento de información de la víctima de forma metodológica. Normalmente, la fase de recocimiento se refiere a la fase preparatoria en la que el hacker se documenta sobre su víctima, recolecta toda la información que le pueda ser útil sobre ella:

- Páginas web
- Correos electrónicos
- Dominios
- Harware
- Software, Actualizaciones
- Compras, Ventas
- Socios
- Búsqueda de empleados

Reconocimiento

El reconocimiento es una de las tres fases preparatorias al ataque. En estas 3 etapas el atacante puede gastar hasta el 90% de su tiempo. Existen dos formas de hacer reconocimiento:

Pasivo: en este tipo de reconocimiento se busca información de la víctima sin hacer contacto directo con ella.

Por ejemplo: En los avisos de empleo se busca personal con calificaciones específicas como programadores web de java, python, php
Publicaciones de prensa en los que se anuncian proyectos: "La empresa xxx pionera en el uso de Microsoft Vista..."

Activo: en este tipo de reconocimiento el hacker hace contacto con la víctima, se utilizan principalmente técnicas de ingeniería social para obtener información de utilidad para el hacker, principalmente se usa la vía telefónica o correos electrónicos para obtener información de la misma.

Escaneo

Durante la fase de escáneo el hacker intenta descubrir, enumerar e inventariar los equipos de la red a la que quiere acceder. Específicamente, el atacante desea recolectar información acerca de las direcciones Ips de la víctima, su sistema operativo, la arquitectura de sistemas de la víctima y los servicios que cada equipo de su red está ejecutando.

Los objetivos del escaneo son:

- Detectar los sistemas activos de una red
- Descubrir los puertos activos de un equipo
- Descubrir el sistema operativo de un equipo
- Descubrir los servicios activos en un equipo

Tomar acceso

Para la toma de acceso el hacker rompe la contraseñas de las cuentas de usuario que logró encontrar.

Para ello se utilizan 4 técnicas:

1. Ataque en línea pasivo

2. Ataque en línea activo

3. Ataque fuera de línea

4. Ataque no-electrónico

Mantener acceso

Luego de lograr el acceso el hacker tratará de escalar privilegios y ejecutar aplicaciones o exploits de forma encubierta.

Una forma común de encrubrimiento son los rootkits. Los rootkits se instalan en el corazón del sistema operativo y tienen la habilidad de esconderse y encubrir sus actividades.

Cuando se instala un rookit se reemplazan llamados del sistema operativo por versiones o rutinas modificadas que contienen la ejecución de script o aplicación adicional al llamado natural que realiza la función.

Un rootkit puede: Esconder procesos, archivos, entradas en el registro interceptar comandos, solicitar debug (causando los famosos pantallazos azules), redirigir archivos .exe.

Limpieza de trazas

- La fase de limpieza de trazas muchas veces determina la experiencia de un hacker. Un buen atacante no deja huellas de lo que realizó.

- En esta etapa, el hacker borrará los registros del sistema que indiquen que estuvo allí, eliminará las cuentas de usuario que creó, los registros de los privilegios que obtuvo, etc.

- Para limpieza de trazas:

- 1. Eliminación del log de eventos, deshabilitación de auditorias antes de comenzar el ataque

- 2. Utilización de herramientas como elsave.exe, evidence eliminator, traceless y winzapper

Rentabilidad de los cybercrímenes

El FBI estimó en el 2004 que más del 50% de correo que circula en los Estados Unidos es: "no deseado", un phishing o un correo con un malware anexo!

Una de cada 5 computadores tiene algún tipo de malware instalado!

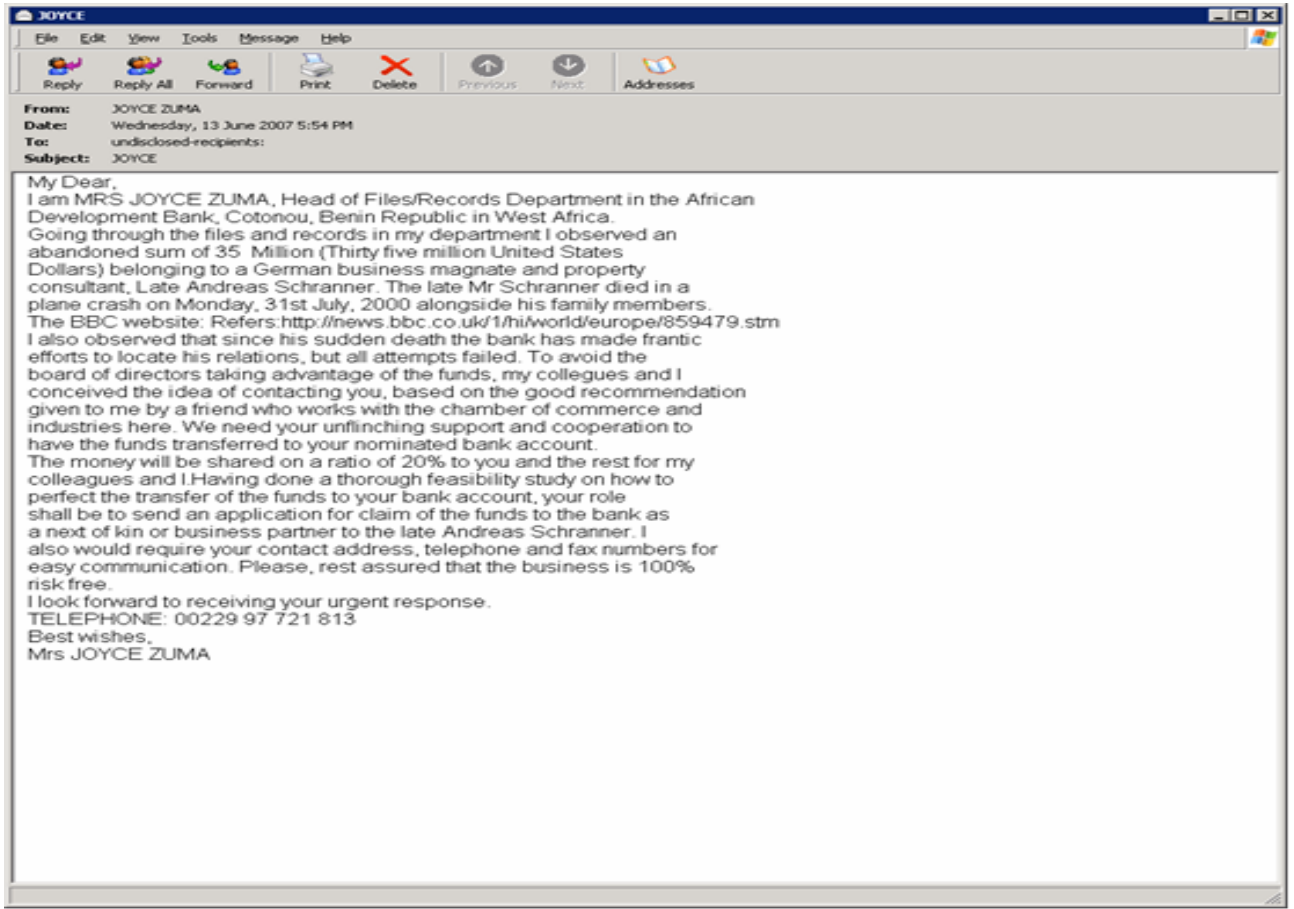
Los datos de las tarjetas de crédito robadas por 2 hackers en Tailandia en el 2007 se vendieron a otras bandar por 6 millones de doláres. La base de datos contaba contaba con unos 10 millones de datos de tarjetahabientes.

Rentabilidad de los cybercrímenes

ParqueTecnologico
Mérida - Venezuela

Rentabilidad de los cybercrímenes

En el 2006 Chatham House, una empresa consultora en el Reino Unido, reportó que apróx. Se perdian anualmente **150 millones** de libras esterlinas en fraudes relacionados a phishings, conocidos como los scam o cartas de Nigeria, en los cuales la víctima recibe un correo electrónico, indicando que la persona había recibido una herencia, que necesitaban sus datos de cuenta para proceder a depositarle el dinero.



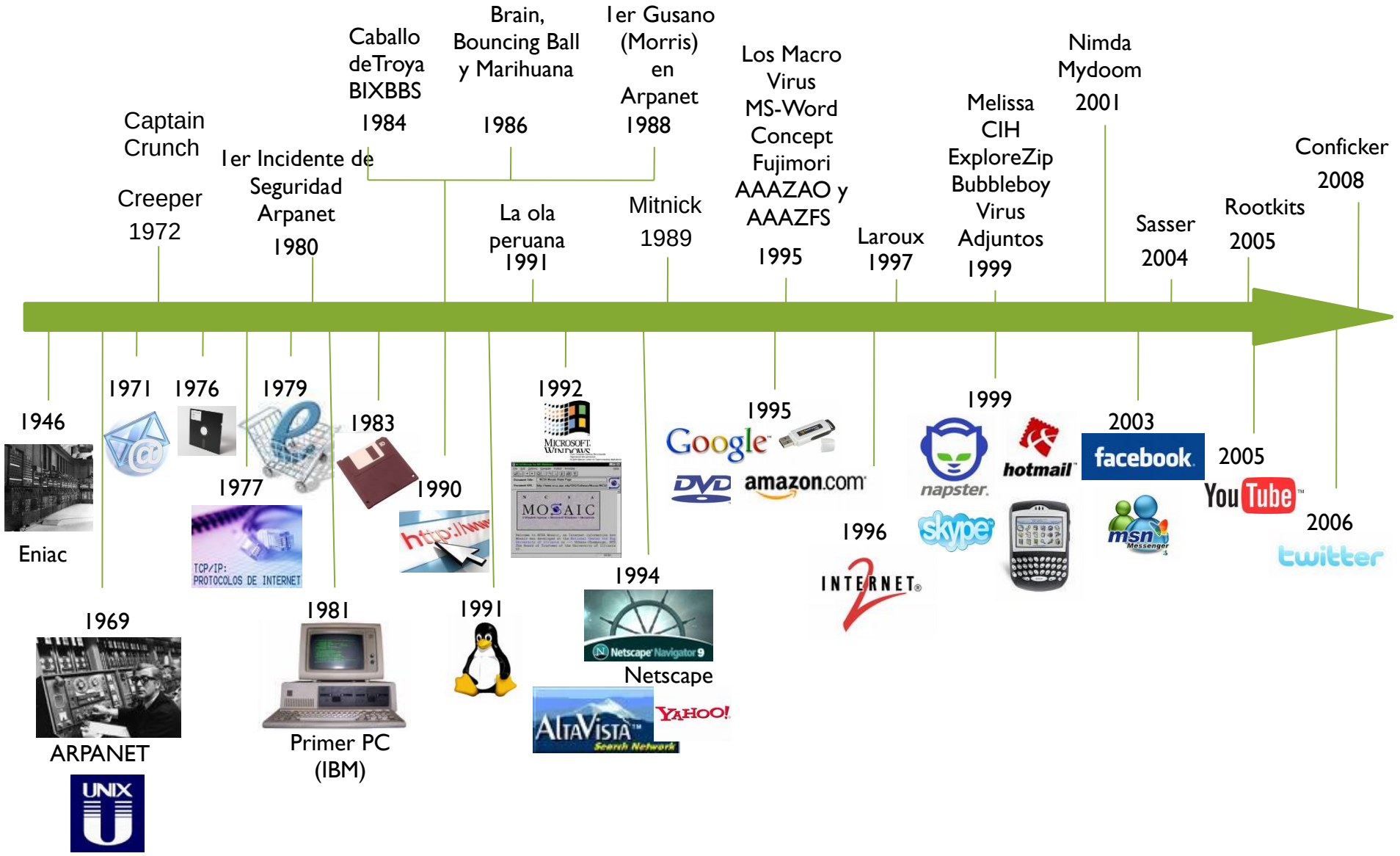
Rentabilidad de los cybercrímenes

En el 2010 Un neo zelándes diagnosticado con el síndrome de asperberg lideró una banda de crackers que tomaron los datos de unos 15 millones de personas, en el momento del arresto no se pudo demostrar que utilizaron los datos, pero se estimó que la pérdida de dinero podría estar en unos 150 millones de libras esterlinas si la base de datos era utilizada.

En el 2011 la empresa Sony ha admitido perder alrededor de 172 millones de dolares debido a los ataques de denegación de servicios a sus consolas de juego X-box en línea! Debido a estos ataques Sony se ha visto obligada en 3 ocasiones a cerrar sus servicios de juego en línea debido a éstos problemas.
El último escándalo fue el robo de más 75.000 códigos para descarga de música y adicionalmente se robaron los datos 3.5 millones de cupones para descargas gratis de música!

Por LulzSec

Línea de Tiempo de algunos virus informáticos



ParqueTecnologico
Mérida - Venezuela

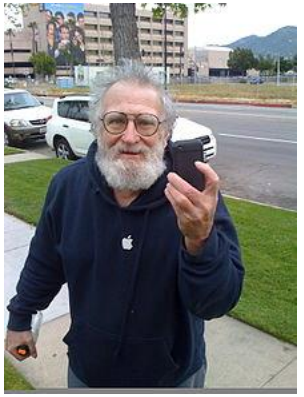
Hackers de ayer y de hoy...

Los de ayer

Kevin Mitnick

Dueño de Mitnick Consulting, que se encarga de realizar, auditorias, hackeo ético, etc.

John Draper



Desarrollador de software como: Easywriter, CrunchBox firewall, Forth 1.7 para Apple, entre muchos otros.

Robert Tappan Morris

Profesor en el departamento de Ciencias de la computación en el MIT

Hackers de ayer y de hoy...

Los de ayer

Kevin Mitnick, Pertenece a las primeras generaciones de hackers, realizó muchas penetraciones, comenzando por las de empresas telefónicas, entre ellas están Cosmos, Pacific Bell, fue procesado en 1981, 1983, 1987, 1995. Finalmente, salió en libertad en el año 2000. Desde entonces, se dedica a la consultoría en seguridad informática.

Fue muy famoso por la persecusión a la que fue sometida, estuvo en las listas de los más buscados, cuando estuvo preso se le aisló e impidió el uso de teléfonos, computadoras, etc.

Sus abogados durante la defensa de su último caso alegaron que Mitnick sufría una adicción al hackeo!! de con el objetivo de que bajaran su condena, cabe destacar que en este último caso robó los datos 20.000 tarjetas de crédito.

Hoy en día dirige una empresa llamada Mitnick consulting, en la que se dedica a la consultoría de seguridad, auditorías, aseguramiento, pruebas de penetración y hackeo ético

Hackers de ayer y de hoy...

Los de ayer

John Draper, es un veterano de la guerra de Vietnam, en el mundo hacker es mejor conocido como Capitán Crunch, un amigo le contó que un pequeño juguete que era distribuido como parte de una promoción del cereal Cap'n Crunch se podía modificar para emitir un tono a 2600 Hz, la misma frecuencia que usaba AT&T para indicar que la línea telefónica estaba lista para rutear una llamada. Al hacer esto, se podía entrar en modo operador, lo que permitía explorar las diversas propiedades del sistema telefónico, y hacer llamadas gratuitas.

Luego de estudiar dichas propiedades, Draper construyó la primera caja azul. Las cajas azules se comercializaron durante algún tiempo, junto con John trabajaron entro otros Steve Wozniak (fundador de Apple).

Estuvo preso por sus incursiones y la comercialización de las "cajas azules" Durante su estadía en la cárcel escribió el programa Easywriter (editor de texto) de Apple.

Posteriormente se dedicó al desarrollo de software

Hackers de ayer y de hoy...

Los de ayer

Robert Morris creó el primer gusano conocido en internet mientras era estudiante en la Universidad de Cornell. Según indicó su intención era conocer el tamaño de Internet. Liberó el gusano desde el MIT para esconder el hecho de que provenia realmente de Cornell.

El gusano que construyó saltaba de equipo en equipo y preguntaba si ya se encontraba allí, cómo pensó que algunos adminsitradores tratarían de eliminarlo, programo al gusano para copiarse no importa su respuesta 14% de las veces. El gusano se distribuyó rápidamente lo que causó denegaciones de servicio por toda la internet. Se estima que causó daños por más de $20.000.

Morris no estuvo preso, pero tuvo que realizar servicio comunitario y pagar una multa por $10.000.

Hoy en día es profesor de ciencias de la computación en el MIT

Hackers de ayer y de hoy...

Los de hoy

Chen Ing-Hau

Chen Ing-Hau, de 25 años, es el autor del virus CIH conocido cómo Chernobyl a pesar de los daños causados por el virus, nunca fue encarcelado!

Chen Inh-Hau es un ciudadano Tailandés, en este país para poder ser procesado una persona local tenía que hacer la denuncia a las autoridades, 1 año y medio después un estudiante reportó a las autoridades que su equipo había sido infectado por el virus CIH. Chen fue citado y "regañado" pero nunca fue procesado ni multado...hoy en día trabaja cómo programador de herramientas linux.

Hackers de ayer y de hoy...

Los de hoy

Sven Jaschan

Sven Jaschan, de 17 años y alemán es el autor de Sasser y Netsky!, fue detenido en Mayo de 2004, tras una denuncia de sus vecinos que perseguian la recompensa propuesta por la empresa Microsoft, ya que el virus afectaba directamente la estabilidad de Windows 2000, 2003 Server y Windows XP.

A pesar de que Sasser ha sido uno de los gusanos más dañinos de la historia, Sophos reportó en el 2004 que un 70% de la infecciones en los equipos eran Sasser!

Sven no estuvo preso, esto se debe a que era menor de edad al momento de su detención y tuvo que ser procesado por la leyes para menores, pasó 3 años de libertad condicional con regimen de presentación y algunas horas de servicio comunitario!

A finales del mismo año lo contrató la empresa alemana Securepoint

Hackers de ayer y de hoy...

Los de hoy

David Smith

David Smith, de 30 años, creador de Melissa, el 26 de marzo de 1999 Melissa atacó a miles de empresas alrededor del mundo.

Melissa es un virus contenido en una macro, específicamente de word, se esparció a través de un grupo de noticias en la red usenet que compartían una lista sobre sus gustos sobre páginas porno!

El virus venía anexo a un correo que cuyo contenido decía "mira esto, es muy dificil de explicar", al abrir el documento el equipo de la víctima se infectaba y comenzaba a enviar correos a todos sus contactos. Los servidores de correo de empresas cómo: Microsoft, Intel, Lockheed Martin colapsaron por el volumen de correos que recibian e intentaban enviar.

Se estima que este virus causó pérdidas de más de 20 millones de dolares, David Smith fue apresado y sentenciado a 20 meses de prisión y una multa 5000 dolares.

Hackers de ayer y de hoy...

Los de hoy

Adrian Lamo

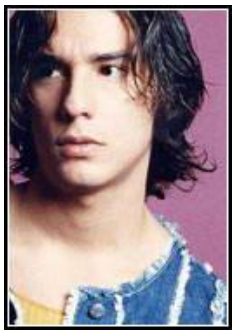
Adrian Lamo, conocido con el "Homeless" hacker, se dedicó a mostrar sus intrusiones en The New York Times y en Microsoft. Es también conocido por tratar de identificar fallas de seguridad en las redes informáticas de Fortune 500 y, a continuación, comunicarles esas fallas encontradas (es ilegal en muchos lugares sin permiso, como una forma de intrusiones no solicitadas).

También es muy conocido por haber delatado a Bradley Manning, el soldado que filtró a WikiLeaks el vídeo que mostraba a soldados estadounidenses asesinando a un fotógrafo de Reuters y a otros civiles en Afganistán, así como otros muchos documentos clasificados del ejército de los EE.UU. que mostraban actitudes delictivas.

Hoy en día es un periodista de tecnología y seguridad informática!!

Hackers de ayer y de hoy...

Los de aquí



Rafael Nuñez

Rafael Nuñez, el Hacker venezolano más famoso fue detenido en Miami, en el 2005

RaFa (su nickname) comenzó en el mundo de la computación a muy temprana edad debido a que su padre es programador y fue mostrándole a su hijo este mundo de la computación.

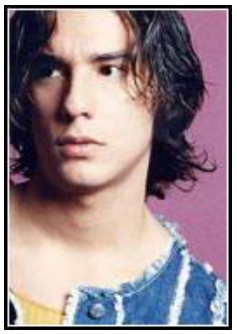
RaFa cuenta que a principios del año 2001 se une a un selecto grupo de hackers conocidos como "World of Hell".

"El grupo duró pocos meses, desde comienzos de 2001 hasta septiembre de ese año. Pero hicimos demasiadas cosas. Violentamos masivamente la seguridad de muchas páginas web como prueba de su vulnerabilidad"

Palabras de Rafael Nuñez en entrevista a El Universal.

Hackers de ayer y de hoy...

Los de aquí



Rafael Nuñez

Entre las páginas que vulneraron estaban páginas de la Fuerzas Armadas de los Estados Unidos, cómo prueba de sus incursiones RaFa toma el diseño de una nave llamada C.O.B.R.A.

RaFa indica que rápidamente el grupo se disolvió y que él decide dejar esas actividades, comienza a trabajar para un empresa de seguridad, posteriormente trabaja para CANTV y comienza a trabajar con la CIPC y CPIUS (una organización para la lucha contra la pedofilia).

Posteriormente, en el 2005 viaja a EUA para asistir a un curso, es detenido en el aeropuerto, luego de permancer casi año detenido enfrentando un juicio que podía desembocar en una setencia de entre 10 a 12 años, RaFa logra demostrar que su incursión en esos sistemas fue un error de su pasado, un acto de inmadurez y que no perseguía el lucro o el fraude, se demostró que Rafael estaba activamente trabajando en contra de la pedofilia en Internet y era pieza clave en las asesorias del CICP en casos de delitos informáticos en su país se le dicta una sentencia de apróx. 1 año que sirvió durante su jucio.

¿Han cambiado los hackers?

Siii dramaticamente!

Un hacker en los años 60 tenía que ser necesariamente un nerd o geek, o un gallo en cristiano

El acceso a las computadoras y el conocimiento necesario era muy restringido a los ambientes universitarios muy avanzados!

En la internet están disponibles miles de códigos para fabricar virus, gusanos, hacker cuentas de gmail, hotmail, facebook, etc.

¿Han cambiado los hackers?

Los hacker de los años 90 y principios del siglo XXI tenían apróx. 18 esa edad va disminuyendo cada día más! El hacker más joven hasta ahora es Tim Rosenbaum con 10 años y un altísimo sentido del oido logro silbar a una frecuencia de 2600 ciclos, el tono le indica a la compañía que la llamada se ha terminado y el niño seguía conversando.

Otro niño hacker, Alex Miller de 12 años, encontró un agujero crítico en Firefox, Mozilla le otorgó la recompensa de $3000 prometida a todo aquel que encontrará vulnerabilidades en su producto.

¿Somos incautos?

Cuando el ser humano pasa del mundo real al virtual le cuesta tomar en cuenta algunos aspectos básicos, uno de ellos es el de la seguridad!!!!

Un venezolano jamás dejaría su casa la con las puertas y ventanas abiertas!! o no le dejaría las llaves a cualquier hijo de vecino!!

Sin embargo, rara vez coloca un password a su equipo bien sea el de la casa o el trabajo y lo dejas conectado a Internet. Por ejemplo, gran cantidad de los equipos ULA se comparten carpetas sin ningún password!!!

¿Somos incautos?

La frase, "En mi computadora no hay nada que robar"

Piénsalo 2 veces un hacker/cracker puede no necesitar los datos de tu computadora pero si estará interesado en utilizar tu computadora para realizar sus ataques, un botnet estudiado por el MIT estaba compuesto por más de 1.5 millones de equipos zombie!

Adicionalmente, muchos ataques no van dirigidos a tí pero te causarán problemas si tu equipo está abierto para ser atacado! Y seguramente está conectado a red, y muy probablemente está encendido aunque nadie lo esté utilizando.

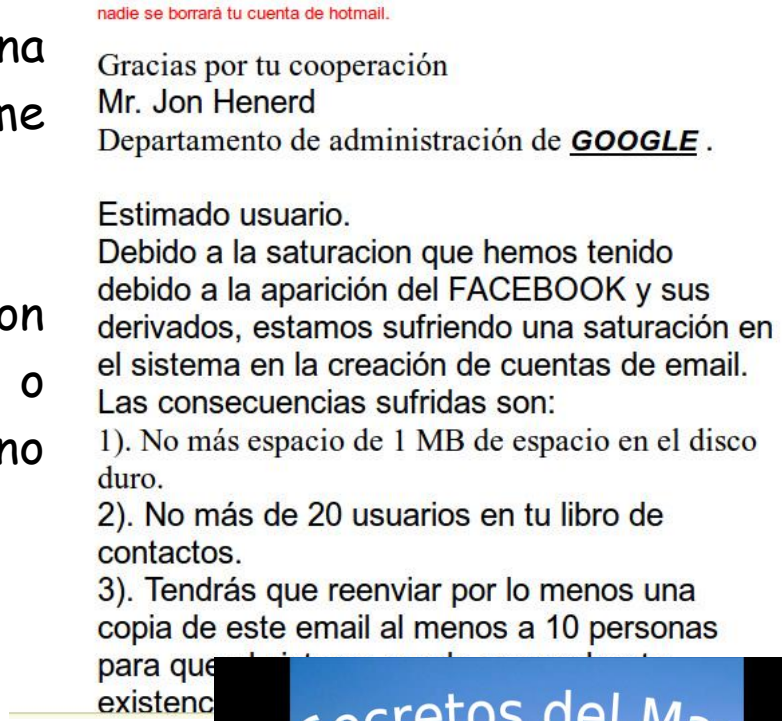
¿Somos incautos?

Si un desconocido llega a tu casa para ofrecerte una gran oferta sobre un producto al estilo llame ya...¿Le abres la puerta y lo invitas a un café?

Todos los días nuestros usuarios abren correos con documentos anexos de personas desconocidas, o conocidas sobre temas de los cuales ellos no manejan cómo:

- Las diez bendiciones de la virgen x, y o z
- Las mejores fotos de todos los tiempos
- Ahora si gmail va a cobrar por sus servicios
- Si no abres este documento te caeran las 7 plagas
- Las fotos nunca vistas del matrimonio de Edward y Kate
- Las fotos "originales" de la muerte de Osama!

Se estiman que más del 80% de éstos documentos tienen algún tipo de malware anexo.


nadie se borrará tu cuenta de hotmail.

Gracias por tu cooperación
Mr. Jon Henerd
Departamento de administración de ***GOOGLE*** .

Estimado usuario.
Debido a la saturacion que hemos tenido debido a la aparición del FACEBOOK y sus derivados, estamos sufriendo una saturación en el sistema en la creación de cuentas de email.
Las consecuencias sufridas son:
1). No más espacio de 1 MB de espacio en el disco duro.
2). No más de 20 usuarios en tu libro de contactos.
3). Tendrás que reenviar por lo menos una copia de este email al menos a 10 personas para que
existenc


ORACIÓN:

Oh Dios, que quisiste que en este día fuese presentada en el templo la Santísima Virgen María, morada del Espíritu Santo: suplicámoste por su intercesión nos concedas merecer ser presentados en el templo de tu gloria. Por nuestro Señor Jesucristo.

Amén.

ParqueTecnologico
Mérida - Venezuela

¿Cuántos de nosotros utilizamos estas técnicas?

Aléjense espiritus!!!!!

A pesar de que tengo que admitir que sus técnicas son un poco radicales, ella es la mejor técnico que hemos tenido para deshacerse de los virus!!!!

OJO: ni tan calvo ni con 2 pelucas

Para mejorar nuestra seguridad! Nadie puede tener acceso a su equipo hasta que completen un sudoku, responda una pregunta de matemáticas y explique brevemente cómo se maneja un DVD player