EJEMPLO DE DELITOS EN MÈXICO

\* **30 años de prisión para twitterroristas**

|  |  |
| --- | --- |
| http://www.seguridadydefensa.net/noticias/redimensionar.php?imagen=twitter.jpg&ancho=200&hmax=400  **Foto Ilustrativa** | *Una fallida imitación de La guerra de los mundos, de Orson Welles, generó pánico en la ciudad mexicana de Veracruz al anunciar por Twitter supuestos ataques en escuelas. Hubo una veintena de accidentes de tránsito y colapsaron las líneas de emergencia* |

El profesor Gilberto Martínez Vera y la locutora de radio María de Jesús Bravo Pagola serían los "twitterterroristas" responsables de difundir los supuestos ataques del crimen organizado a escuelas de Veracruz. Por ello, enfrentarían penas de hasta 30 años de prisión por violaciones a las leyes antiterroristas mexicanas.

Los tweets aseguraban que varios colegios de la ciudad mexicana habían recibido amenazas de bomba. Rápidamente, el pánico se apoderó de la ciudad: se generaron unos 26 accidentes automovilísticos protagonizados por padres que acudieron a salvar a sus hijos y colapsaron las líneas telefónicas de emergencia.

Ahora, pesa sobre los bromistas una acusación de la Fiscalía local por mal uso de la red social de microblogging, mientras que sus abogados aseguran que sus defendidos sólo repetían rumores que habían visto en Internet y que no los iniciaron.

Las autoridades sostienen que ambos acusados -que se encuentran detenidos- crearon un rumor a través de Twitter bajo los hashtags #verfolow y #Veracruz. Además, cuentan con otro elemento especialmente curioso: según afirman medios mexicanos, la propia acusada se describe a sí misma en su perfil de Facebook como "TwitTerrorista".

El caso repercutió al punto de que la ONG Amnistía Internacional manifestó que existe "una violación a la libertad de expresión" y culpó a la guerra contra el narcotráfico por esta clase de sucesos: "La inseguridad crea un clima de desconfianza, en el cual los rumores que circulan por las redes sociales son parte del intento de las personas por protegerse a sí mismas, ya que existe muy poca información fidedigna".

Además, en los últimos días surgió el movimiento autodenominado "Yo también soy TwitTerrorista", que exige la liberación de los supuestos iniciadores de la psicosis en Veracruz y denuncia que su detención fue mediante coacción y tortura.

\* **El Narcotráfico recluta hackers**

|  |  |
| --- | --- |
| http://www.seguridadydefensa.net/noticias/redimensionar.php?imagen=clonar%20tarj.jpg&ancho=200&hmax=400  **Foto Ilustrativa** | *Los carteles de droga mexicanos tienen en jaque a los 'hackers', a los que secuestran con el objeto de clonar tarjetas de crédito y robar datos personales de internet, según Dmitri Bestúzhev, director para América Latina del Equipo Global de Investigación y Análisis (GReAT) de Kaspersky Lab.* |

Comparta esta nota!

Los carteles de droga mexicanos tienen en jaque a los 'hackers', a los que secuestran con el objeto de clonar tarjetas de crédito y robar datos personales de internet, según Dmitri Bestúzhev, director para América Latina del Equipo Global de Investigación y Análisis (GReAT) de Kaspersky Lab.

Bestúzhev denunció que los carteles de droga mexicanos están apostando por el negocio delictivo de la clonación de tarjetas de crédito. Gracias a esta práctica ofrecen productos tecnológicos adquiridos mediante tarjetas falsas, a cambio de poco dinero. En otras palabras, al falsificar la tarjeta, se meten a sitios de subastas web, donde ofrecen, por ejemplo, un iPad a un precio ridículo. Ajeno al engaño el comprador le manda el dinero al mafioso que, a su vez, hace la compra con la tarjeta clonada, y entrega la mercancía a la vivienda del comprador.

“Básicamente tú recibes algo legítimo, pero que fue comprado con dinero robado. Le mandaste al criminal tu dinero real, que fue bien, bien lavado”, dice Bestúzhev.

"Lo que estamos viendo es que los criminales, bien organizados, están probando este negocio, reclutando y controlando a la gente. Esto nace en América Latina, pero estoy seguro de que se va a expandir pronto a todos los países. En Colombia y México, esto ya es una realidad", señala Dmitri Bestúzhev.

Esta práctica se está traduciendo en un aumento de los secuestros de hackers en México, donde los carteles de droga reclutaron a unos jóvenes pasantes de la carrera de Computación del DF. El especialista de Kasperksy asegura que los hackers latinoamericanos han sido alertados y tienen miedo a ser reclutados por los mafiosos.

"Ninguno de los 'hackers' que se dedican a robar tarjetas de crédito quisiera trabajar para los cárteles porque saben que es peligroso para su vida. Pero ahora mismo los cárteles están buscando reclutamiento de este tipo. Esto sucede porque cada año crece el negocio del crimen cibernético y está moviendo mucho dinero en esta esfera. En mi opinión, al unirse el crimen cibernético con el clásico van a aparecer leyes nuevas mixtas adecuadas para la realidad nueva. Ahora la policía local de cada país tiene que proteger a los informáticos de que los recluten los cárteles con fines criminales", comentó Bestúzhev.

\* **10 millones de virus**

|  |  |
| --- | --- |
| http://www.seguridadydefensa.net/noticias/redimensionar.php?imagen=virus.jpg&ancho=200&hmax=400  **Foto Ilustrativa** | *Hace poco aprendieron a una banda dedicada a proporcionar información de cuentas de Facebook por una cuota y anteayer Microsoft reconoció que la información de unas 100 mil cuentas de Hotmail fue dada a conocer en una página ilegal. La empresa de seguridad electrónica rusa Kaspersky, en 2009 espera tener en la base de datos dea casi 10 millones de virus distintos cuando en 2004 esta cifra no superaba el millón.* |

Comparta esta nota!

Hace unos meses, uno de los fundadores de la red social Twitter, Biz Stone, escribía en su blog `La mañana del jueves, Twitter fue blanco de un ataque DoS. Este tipo de ataques tiene el objetivo de interrumpir y hacer inaccesible los servicios que ofrece la empresa. Nos estamos defendiendo del ataque y continuaremos actualizando a nuestros usuarios sobre el estado de la red´.

Las técnicas se han hecho cada vez más sofisticadas. Si antes los gusanos cibernéticos servían sólo para destruir el sistema operativo de una computadora, ahora los "hackers" buscan tirar sistemas completos de compañías o llenar de basura los correos electrónicos de millones de usuarios.

Quizá a muchos no les llame la atención el uso de las palabras `defendiendo´ y `ataque´, sin embargo, es un vocabulario de guerra, una batalla que libran las empresas contra el mundo de los `hackers´.

Uno de los aspectos que ha producido este crecimiento es el cambio de enfoque que tuvo la creación de estos programas. Según explica Justin Priestley, vicepresidente de ventas al consumidor de Kaspersky para América Latina, en 2003 los `hackers´ creaban estos programas sólo para probar cuántas computadoras podían dañar, una actividad ociosa. Pero a partir de ese año esto tomó otro curso, convirtiéndolo en un negocio, lo cual comenzó a elevar las cifras de `malware´ creado y llevando el fenómeno a niveles nunca antes vistos.

Justin contó que otra modalidad de estafa. Cuando uno navega en internet puede aparecer una ventana tipo `pop up" para decirte que tu computadora está infectada. En realidad ellos (quienes sean y donde quiera que estén) infectan tu computadora y luego te ofrecen limpiarla por una cantidad de dinero, y entonces caes en la estafa.

Una modalidad más de estafa funciona así: un servidor entra a tu computadora y detecta las teclas que estás usando al entrar en una página para ingresar datos personales o contraseñas de acceso, como puede ser una cuenta de banco.

Para este tipo de estafa Kaspersky ideó un teclado virtual para evitar este tipo de detección que según la compañía elimina el riesgo de caer en este tipo de trucos.

Las compañías que crean software de protección parecen jugar al gato y al ratón con estos hackers todo el tiempo. Aunque cuando hablamos de una actividad que la gente de Kaspersky considera incluso mayor a los 405 mil millones que representa el mercado de software antivirus, con un valor cercano a los 442 mil millones de dólares, la situación deja de tener esa sensación de simple juego.

EJEMPLO DE DELITOS EN EL MUNDO

# \*[**David Smith**](http://top8delitosinformaticos.blogspot.com/2013/01/david-smith.html)

Smith lanzó su virus en el [alt.sex](https://encyclopediadramatica.se/Masturbation)[Usenet](https://encyclopediadramatica.se/Usenet) grupo en marzo de 1999. A las pocas horas se había extendido a través de Internet. Dentro de una semana se estima que ha infectado a al menos [100.000](https://encyclopediadramatica.se/Over_9000) sistemas en todo el mundo. Las estimaciones finales declaró que cerca de medio millón de personas contrajeron el virus.



En algún momento el virus evolucionó. [script kiddies](https://encyclopediadramatica.se/Script_kiddies) que querían [hacerse famoso](https://encyclopediadramatica.se/Attention_whore) había modificado el virus en varias variantes, extremadamente desagradables, que incluyen:

* Melissa.U
  + Melissa.U vendría irrumpir en su ordenador como un [borracho del pueblo](https://encyclopediadramatica.se/Irish) en busca de una pelea. Entonces sería golpear a sus archivos críticos del sistema como command.com, la eliminación de los archivos y los archivos asociados.
* Melissa.V
  + Este hijo de puta desagradable trataría de [eliminar todo lo jodido](https://encyclopediadramatica.se/Delete_fucking_everything) de una serie de unidades de su equipo y la red. Cuando se hace, entonces se mostrará el mensaje *"*[*Hint*](https://encyclopediadramatica.se/PROTIP)*: Consiga*[*Norton 2000*](https://encyclopediadramatica.se/I_GOT_NORTON!)*no McAfee 4.02 "* .

Las empresas vieron a sus servidores de correo intentan hacer frente a las cargas masivas de tráfico generados por el gusano. Uno por uno, [no](https://encyclopediadramatica.se/Fail), cediendo a la creciente [crapflood](https://encyclopediadramatica.se/Crapflood) . Miles de documentos se corrompieron y se pierde en el proceso. Cientos de empresas se vieron obligadas fuera de línea, perdiendo millones de dólares en ingresos en el proceso. Las empresas afectadas incluido [Microsoft](https://encyclopediadramatica.se/Microsoft) (un hecho agravado que prácticamente todo el mundo en Microsoft utiliza Outlook y Word), Lockheed-Martin, Lucent, e Intel.

# \*[**Robert Morris**](http://top8delitosinformaticos.blogspot.com/2013/01/robert-morris.html)

**Robert Tappan Morris** (también conocido como **rtm**) nació en 1965 y es profesor asociado en el Instituto Tecnológico de Massachussets, en el departamento de Ingeniería Electrónica y Ciencias de la Computación. Es conocido por crear el [Gusano Morris](http://es.wikipedia.org/wiki/Gusano_Morris) en 1988, considerado como el primer gusano de ordenador de la era de Internet. Es hijo de [Robert Morris](http://es.wikipedia.org/wiki/Robert_Morris), ex jefe científico en el Centro Nacional de Seguridad Informática, una división de la[agencia de Seguridad Nacional](http://es.wikipedia.org/wiki/Agencia_de_Seguridad_Nacional) (NSA).  


Morris creó el Gusano cuando era estudiante en la Universidad de Cornell. La intención original, según él, era para medir el tamaño de Internet. Él envió el gusano desde el [Instituto Tecnológico de Massachussets](http://es.wikipedia.org/wiki/Instituto_Tecnol%C3%B3gico_de_Massachussets) ([MIT](http://es.wikipedia.org/wiki/MIT)) para ocultar el hecho de que en realidad procedía de Cornell. Lo hizo a través de [ARPANET](http://es.wikipedia.org/wiki/ARPANET) la cual fue una de las precursoras de Internet.

La tarde del miércoles 2 de noviembre de 1988 ha pasado a la historia de las redes informáticas como una de las fechas más fatídicas... e interesantes. Aproximadamente a las 18:00 horas, tiempo de la Costa Oeste de los E.U, el famoso gusano fue liberado en la antecesora de Internet, [ARPANET](http://es.wikipedia.org/wiki/ARPANET) (Advanced Research Projects Administration Network), nada menos que en el legendario [MIT](http://es.wikipedia.org/wiki/MIT).

El día 3 fue considerado como el "Jueves Negro", usando la terminología reservada para los ["cracks"](http://es.wikipedia.org/w/index.php?title=%22cracks%22&action=edit&redlink=1) bursátiles, porque el gusano se propagó con una rapidez y eficacia extraordinarias. Las computadoras de todos los puntos vitales de los Estados Unidos: la [NASA](http://es.wikipedia.org/wiki/NASA), la[RAND](http://es.wikipedia.org/wiki/RAND), el Pentágono, las Universidades de Berkeley, Stanford y Princeton, el [MIT](http://es.wikipedia.org/wiki/MIT), el Lawrence Livermore National Laboratory, e incluso la [MILNET](http://es.wikipedia.org/wiki/MILNET) -la red de Defensa-, fueron cayendo una tras otra.

Muchos administradores reaccionaron con pánico desconectando sus ordenadores de la Red. [MILNET](http://es.wikipedia.org/wiki/MILNET) cortó su comunicación de correo con [ARPANET](http://es.wikipedia.org/wiki/ARPANET). Todas estas reacciones multiplicaron los efectos como si de un pánico bursátil se tratase.

Rápidamente se iniciaron las tareas para saber qué estaba pasando y cómo ponerle remedio. Tras conseguir aislar el gusano y estudiar su código, identificaron las rutinas de infección y crearon una "vacuna". En una semana volvieron a la normalidad todos los ordenadores.

El gusano sólo afectaba a dos modelos de máquinas que trabajaban con sistemas operativos [UNIX](http://es.wikipedia.org/wiki/UNIX) de la variante BSD (Berkeley...). Realizaba dos tareas: enviarse a otras máquinas y duplicarse en la máquina infectada. Si el gusano hubiera funcionado en otros sistemas además de [UNIX BSD](http://es.wikipedia.org/w/index.php?title=UNIX_BSD&action=edit&redlink=1) sobre máquinas Sun Microsystems Sun 3 y VAX, los resultados hubieran sido de dimensiones "apocalípticas".

El Gusano fue diseñado para comprobar si la máquina ya estaba infectada y si no era así la infectaba. Pero Morris creía que muchos administradores intentarían hacer creer al virus que la máquina ya estaba infectada, para contrarrestar esto el virus siempre infectaba a la máquina tuviera o no el virus anteriormente, lo que provocó que se infectaran 6.000 servidores. Arpanet empleaba [UNIX](http://es.wikipedia.org/wiki/UNIX), como sistema operativo. Se estima que el coste de la reparación de los daños causados por el gusano en cada sistema varía entre $ 200 a más de $ 53000. El virus explota varias vulnerabilidades para acceder a los sistemas orientados, en particular:

* Un agujero en el modo de [depuración](http://es.wikipedia.org/wiki/Depuraci%C3%B3n_de_programas) de Unix el programa sendmail.
* Un buffer overflow fingered, que es un agujero en el servicio de red.
* Rexec / rsh red de acceso sin contraseña.

# \*[**Richard Stallman**](http://top8delitosinformaticos.blogspot.com/2013/01/richard-stallman.html)

Este Neoyorquino con aspecto de hippie es uno de los más activos militantes a favor del software libre desde principios de los 80, cuando era un hacker especializado en inteligencia artificial. Desde el MIT se opuso firmemente a la privatización del software que utilizaban en los laboratorios del instituto, así creó lo que hoy día se conoce como GNU (proyecto que aboga por sistemas operativos libres) y el concepto de CopyLeft. Populares entornos como Linux utilizan el modo GNU y Stallman es actualmente uno de los gurues de la democratización del software.

**CLASIFICACIÓN**

* Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
  + Interceptación ilícita de datos informáticos.
  + Interferencia en el funcionamiento de un sistema informático.
  + Abuso de dispositivos que faciliten la comisión de delitos.
  + Acceso ilícito a sistemas informáticos.
  + Phising y Pharming
  + Delincuencia organizada
* Delitos informáticos
  + Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
  + Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
* Delitos relacionados con el contenido
  + Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
* Delitos relacionados con infracciones de la propiedad intelectual y derechos afines
  + Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.