

tecnología

entrevista

El charrúa que acecha al malware

Marcelo Rivero es uno de los referentes de habla hispana en materia de seguridad informática

POR DAVID GÓMEZ*
ESPECIAL PARA EL OBSERVADOR

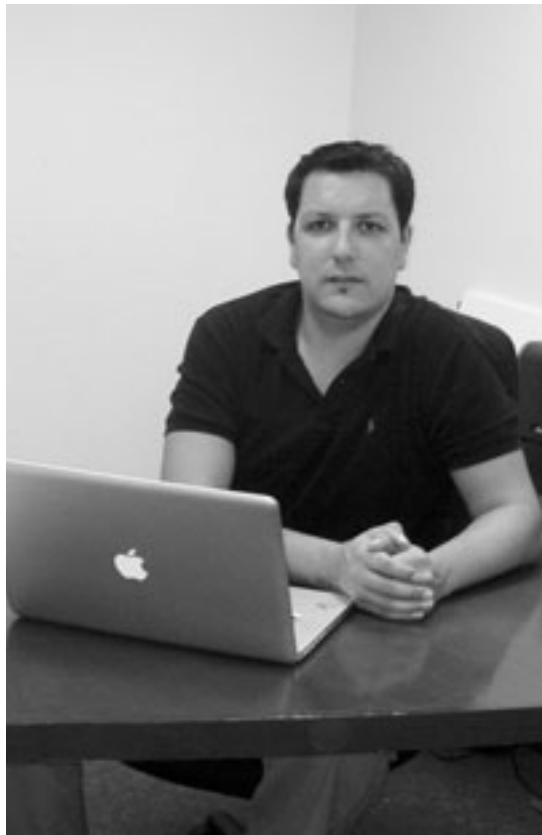
Comenzó a los 12 años con una TK-95 y de ahí no paró hasta ser analista en sistemas. Hoy a sus casi 32 años, Marcelo Rivero es uno de los consultores en seguridad más demandados por las empresas en EEUU. También está al frente de InfoSpyware.com, el blog de habla hispana que lidera en su sector. El uruguayo, al que le huye el malware, habló con *El Observador* acerca de su vida, tendencias en seguridad informática y dejó algunos consejos para los lectores.

¿Cómo ha cambiado el panorama de amenazas?

Anteriormente bastaba con pasar un antivirus en modo seguro en el sistema y este solo era capaz de eliminar cualquier infección. En la actualidad hay técnicas más rebuscadas para evitar ser detectados; van desde el uso de técnicas de *rootkit* para esconderse en el sistema o modificar el archivo HOST para impedir ingresar a páginas web que hablen de seguridad.

A nivel malwares, ¿tienden a desaparecer o su número se acrecienta?

Lejos quedaron aquellos creadores de malwares que programaban desde el garaje de su casa con intereses de investigación o simple ego. Hoy en día solo queda el interés comercial impulsado por cibercriminales muy bien organizados que han visto en esto un negocio muy



rentable que mueve miles de millones de dólares al año, lo que le da la posibilidad de contar con un sinfín de recursos.

Prácticamente han desaparecido aquellos virus que te borraban toda la información de tu disco o que te dejaban el equipo inutilizado y ahora se concentran justamente en tratar de permanecer en el equipo el mayor tiempo posible sin ser identificados convirtiendo este en un equipo Zombie, o sea que pueda ser manejado de forma remota para enviar Spam, robar

datos personales o de cuentas bancarias, alertarnos de falsas infecciones para que terminemos comprando un falso antivirus y similar.

Las redes sociales avanzan a pasos gigantes. ¿Cree que serán objetivo para la transmisión de los virus, como ya ha sucedido en un par de ocasiones?

Las redes sociales han crecido y la tendencia es que seguirán creciendo a nivel mundial, por lo que al seguir siendo tan populares, contar con tantos datos y no tener buen

consejos del experto

- Contar con un programa Antivirus en entorno Windows es fundamental y se puede complementar con un Firewall (Cortafuegos) o ya instalando una "Suite de Seguridad", que proporciona varias herramientas de seguridad como un "todo en uno".

- Mantener el sistema siempre actualizado, no solo Windows sino también todos los programas que tengamos en el PC. Generalmente la gente piensa "si funciona, no lo toques"; esto lo aplica con los nuevos parches y actualizaciones de programas. Pero este punto es muy importante, ya que generalmente son para resolver y tapar agujeros de seguridad explotados por malwares.

- Mantenerse medianamente informado sobre las nuevas amenazas de seguridad que van surgiendo en la red para poder reconocerlas y evitarlas más fácilmente.

- Y lo más importante, usar el "sentido común" a la hora de navegar con especial cuidado en los sitios que visitamos y los archivos que descargamos y ejecutamos en nuestros PCs.

grandes a nivel de usuarios, tienen la principal atención de los cibercriminales. Hay un gusano, que es el más popular de las redes sociales, llamado "Koobface", al cual se le llevan detectadas más de 20 mil variantes diferentes y que sigue en constante evolución por su efectividad a la hora de infectar usuarios utilizando estas redes sociales.

Existe una teoría de que los laboratorios farmacéuticos lanzan enfermedades para luego vender la cura. ¿Esto pasa en la industria de la seguridad informática?

Esto es un mito muy popular que también la mayoría de la gente sigue creyendo, pero que hasta ahora nunca se ha podido demostrar un caso real. Tenemos una encuesta al respecto y 55% cree que esto es así, 35% tiene sus dudas y solo el 10% restante piensa que no. Si esto fuera así, ya se sabría. Las empresas no solo tendrían problemas graves en su reputación, sino que también grandes problemas legales. Por otra parte, los cibercriminales vienen ganándole la batalla a las compañías de antivirus desde hace varios años, y todo demuestra que así seguirá siendo.

¿A qué hay que temer realmente en la web?

Si bien es verdad que puede haber riesgos en Internet, no hay que temerles. Sería lo mismo que decir que no queremos salir de nuestra casa por miedo a engriparnos. Lo importante es ser precavidos y así disfrutar todas las ventajas que la web tiene para ofrecernos.

(*) con la colaboración de Gabriel Fagúndez, un joven blogger de Tacuarembó.

«No me considero un hacker»

Nacido en 1977, a Marcelo se lo conoce en la blogósfera bajo el nic Aka ElPiedra. Hace casi ocho años que vive en Miami, junto a su esposa y su pequeño de tres años y medio de edad. La informática le atrajo desde que le regalaron su primer computadora, a los 12 años. Al principio la usaba solo para jugar, pero luego le em-

pezó a meter mano al código Basic y armó sus primeros programitas. Unos años más tarde hizo un curso de operador PC, cuando se dictaba MS-Dos, Lotus 123, WordPerfect, dBase III y Windows 3.1. Después siguió con cursos de programación, armado y reparación de PCs. Comenzó la carrera de Ingeniería en la ORTY, paralelamente, a trabajar en Movicom. En 2001 migró

a EEUU, y tras pelearla en todo tipo de trabajos, logró encauzarse en lo suyo. Su interés por hallar soluciones contra los recién aparecidos Spywares y Adwares, lo llevó en 2002 a integrarse a CastelCops, uno de los foros pioneros en seguridad informática. A partir de allí se involucró en el desarrollo de los famosos SpyBot y HijackThis. Finalmente en 2004, lanzó su emprendi-

miento personal: InfoSpyware.com, donde ofrece info actualizada sobre seguridad informática, los programas necesarios para su protección, manuales y tutoriales. Luego, ante el caudal de consultas que recibía, inauguró ForoSpyware.com, que a la fecha alberga la mayor comunidad de seguridad informática en español; cuenta con más de 670 mil usuarios, más de

1 millón de mensajes publicados y un tráfico de más de 4 millones de visitantes. InfoSpyware.com es el único sitio en español miembro de ASAP (Alliance of Security Analysis Professionals) del APWG (Anti Phishing Working Group) y colabora en varias compañías de concientización y difusión de la seguridad.