

Entrevista con un pirata informático anónimo

Antes de comenzar

En la transcripción original de la entrevista, se utilizan muy a menudo las palabras **hacker** y **hacking**, que tienen su traducción al español pero solo como una referencia muy aproximada del concepto que implican estas palabras en inglés, y en su uso habitual.

Para intentar aproximar la traducción al español lo máximo posible al concepto que se quiere expresar en su versión original, respetaremos el uso de dichos vocablos pero con una breve explicación introductoria sobre su significado, incluyendo las traducciones que diversos diccionarios y publicaciones especializadas hacen de estos términos.

Asimismo, hemos incluido notas aclaratorias cuando era necesario, para ayudar a comprender esta particular porción del mundo informático.

- **Hacker**

- Persona que sabe mucho sobre informática.
- Fanático informático.
- Intruso informático
- Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.
- Un programador experto que usa sus conocimientos para romper las restricciones de los sistemas informáticos o redes, por el solo placer de hacerlo o para poner en evidencia la existencia de ciertos riesgos. A diferencia de un **cracker**, un hacker verdadero no desea producir daño a nada ni a nadie.

- **Hacking, hackeo, hackeando**

- ☑ Es habitual utilizar la deformación del vocablo original en inglés, y así lo utilizaremos aquí.
- Intrusión informática.
- Pirateo.
- Acceso ilegal dentro de otros ordenadores o sitios de Internet con fines maliciosos o fraudulentos, o para producir modificaciones no autorizadas, o solo por el placer de hacerlo.

La entrevista

Muchas personas han escuchado hablar acerca de los **hackers** rusos y sus hazañas.

Podríamos mencionar una gran cantidad de ejemplos, desde el enorme robo cibernético al Citibank en 1994, planeado por el programador ruso Vladimir Levi, hasta el reciente secuestro de códigos de identificación personal del banco Nordea, de Suecia. El coste de estos delitos informáticos puede ascender hasta millones de euros.

Ciertamente, como desarrolladores rusos de aplicaciones de seguridad, no nos estamos jactando de nuestros compatriotas. A pesar del talento o las dotes intelectuales del perpetrador, un crimen es siempre un crimen.

Tampoco estamos creando excusas para este tipo de actividades: Rusia difícilmente sea el único país en el mundo con una población técnicamente educada, e inestabilidad financiera en su sociedad. En cambio, sí decidimos investigar las motivaciones comunes a todos los criminales cibernéticos del mundo, incluyendo a los rusos.

Somos vecinos de los **hackers**, y conocemos bien sus hábitos. Entonces, hicimos una breve incursión en la comunidad local de **hackers**, y logramos concertar una entrevista con un ex miembro de los criminales cibernéticos, que asegura que ahora pertenece al bando de los **White hats** (Sombreros blancos), y se preparó para compartir su experiencia con entusiasmo.

📌 **White hat**

Un miembro de la comunidad **White hat** es considerado un hacker "ético" que se opone por cuestiones morales al abuso sobre los sistemas informáticos.

Generalmente, un **White hat** hace centro en la seguridad de los sistemas informáticos y su protección, que a diferencia de un **Black hat** (Sombrero negro) intenta perpetrar una intrusión sobre estos.

El hecho de que ambos efectúen "tareas" similares y planteen similares y altruistas razones para sus actividades, hace que la diferencia conceptual entre estos sea motivo de permanente discusión.

Su nombre es **Víctor**, pero su apellido será mantenido en secreto. Tiene 30 años de edad, y vive en San Petersburgo, en Rusia. Desde que abandonó sus actividades de **hacking**, ha encontrado un trabajo legal en una empresa familiar de desarrollo de aplicaciones, y parece disfrutarlo. No nos comentó mucho acerca de su transformación en una "buena" persona, pero sí quiso exhibirse acerca de sus habilidades.

Cuando escuchó que Agnitum estaba buscando información directa sobre asuntos de seguridad informática, Víctor se acercó a hablar con nosotros acerca del denominado **código malicioso personalizado** y las herramientas utilizadas en su compilación.

• ¿Cuánto tiempo has pasado escribiendo código malicioso y *hackeando*?

Hacking, en fin, no estoy seguro. Alrededor de diez años, aproximadamente.

Todo comenzó cuando era estudiante de colegio. Recuerdo que un día necesitaba acceder al servidor, entonces inicié mi ordenador desde un disquete Linux, y borré todas las contraseñas de Windows con él. Todavía puedo sentir la frustración del administrador. Así es como fue, gracioso, creo.

En mis comienzos, también hice otro tipo de cosas malas, como escribir virus específicos y enviar mensajes electrónicos falsificando sitios para probar cuán fácilmente podía lograr que la gente me brindara información y dinero.

• Si era tan beneficioso, ¿por qué has decidido abandonar la actividad?

Bueno, tal vez porque crecí un poco, y decidí que las perspectivas a largo plazo, buscando errores y vulnerabilidades en diversas aplicaciones por un salario legítimo, eran un poco mejores que cometiendo delitos. Tal vez porque finalmente me di cuenta de que escribir *exploits* ya no era tan divertido.

Creo que ahora realmente disfruto haciendo contribuciones legítimas al movimiento del código abierto.

📌 *Exploit*: código que se aprovecha de las vulnerabilidades o errores de programación de una aplicación para realizar diversas actividades potencialmente peligrosas.

• ¿Cuán difícil es crear tu propio código malicioso?

Existen herramientas disponibles en línea, en el mercado clandestino (si sabes dónde buscar) que permiten generar fácilmente una versión nueva de un troyano, por ejemplo, a partir del código binario original.

Si bien permite alguna modificación rudimentaria o elemental, lo cierto es que hay posibilidades de que logre atravesar algunos productos de seguridad que no se actualizan tan seguido como deberían. Todo lo que se necesita es un poco de experiencia programando en C++.

Yo solía hacerlo en pocos minutos.

• ¿Podrías mencionar algún ejemplo de dichas herramientas de generación de código malicioso?

Seguro, aunque no querría alentar a la gente a que vaya por ellas.

De todos modos, la mayoría de estas herramientas están al alcance del público.

Pinch Builder es un conocido troyano basado en lenguaje Assembler. Cualquiera puede descargar la muestra, y adaptarla a sus propias necesidades.

El código binario original pretende acceder un área conocida como *Windows Protected Storage* (Almacén protegido de Windows), que es el lugar donde se guardan las contraseñas de usuario "seguras", y extraer la información. El resultado obtenido es directo: los datos del usuario quedan expuestos.

Además, puede extenderse su funcionalidad para hacerlo trabajar como un registrador de pulsaciones (*keylogger*), o un robot de envío de correo masivo, o incluso actuar como un anfitrión para código malicioso adicional. El programa original, está diseñado para multiplicarse mientras el ordenador inicia el proceso de apagado, eludiendo los sistemas de seguridad, pues estos generalmente se cierran también en ese momento.

• Aparentemente, es de gran ayuda para los "hombres malos". ¿Tiene algún coste?

Bueno, no lo he verificado por un tiempo, y desconozco la información exacta, pero creo que su precio ronda los € 22. Es una cifra relativamente accesible, para un experimento de este tipo.

Seguramente, también sea bastante fácil encontrar un par de herramientas similares, gratuitas, en la Red.

- **¿Pueden los productos de seguridad habituales, desafiar eficazmente a Pinch y las aplicaciones similares?**

Si te refieres a los productos basados en el análisis de firmas, la respuesta es que es arduo encontrar una solución consistente y a prueba de balas. Estas amenazas camaleónicas son difíciles de detectar. A veces son visibles, en otras oportunidades y con diferentes variaciones de Pinch, sin tener en cuenta otros tipos de código malicioso, estarán completamente ocultas.

Pinch puede ser muy evasivo. Es posible que algunas herramientas de defensa proactiva, que monitorizan el sistema y las interacciones entre los programas, puedan brindar una detección mejor, pero nada está 100% garantizado.

- **¿Entonces no existe la solución mágica?**

Bueno, el programa *System Safety Monitor* (Monitor de seguridad del sistema) verifica la actividad de Windows en tiempo real, y es un buen punto de partida para combatir el código malicioso del tipo de Pinch. Y, por supuesto, estarás orgulloso de escuchar que es muy probable que Outpost haga un trabajo decente también.

- **Pasemos a la siguiente pregunta.**

- **¿Qué opinas del código personalizado que apunta a una determinada actividad o a un tipo de usuario específico?**

Ya existe un mercado bien definido para los virus especializados, *exploits* y vulnerabilidades no informadas. Pero, debido al ritmo y la sofisticación de los creadores de código malicioso actuales, no se puede asegurar si los delincuentes, o los desarrolladores de seguridad ganarán el juego.

Después de haber trabajado para ambos lados de la cerca, diría que los **hackers** están disfrutando de una ventaja saludable.

El surgimiento de tecnologías como los *rootkits*, y servicios basados en Internet, representan un enorme potencial para el aprovechamiento de vulnerabilidades.

- **¿Quién ganará al final?**

Nadie lo sabe a ciencia cierta.

Pero hay algo que puedo afirmar: los desarrolladores de soluciones de seguridad siempre irán detrás, si trabajan de manera reactiva; tanto en sus decisiones estratégicas como en la metodología de sus productos. Y, los usuarios comunes siempre tendrán sus ordenadores infectados, si continúan ignorando las medidas de seguridad básicas.

El ganador será quien trabaje del modo más inteligente, tanto en el ataque como en la defensa.

Supongo que ustedes podrán decir que me pasé del lado de los sombreros blancos, porque, después de todo, me gustaría ver que los buenos ganen.

Traducción y adaptación al español: Ontinet.com, S.L.