El fiscal de este caso ha metido entre rejas a narcotraficantes y pederastas. **Lo suyo sería que ahora anunciase el mayor éxito de su carrera a bombo y platillo, pero Scott Ferber no quiere cometer errores.**

El acusado ha confesado, pero todavía no se ha dictado sentencia; el veredicto se espera para agosto. Ferber ha metido en la cárcel a alguien intocable, a un maestro del cibercrimen. Y lo ha atrapado gracias a la colaboración de la Policía de seis países, la actuación de agentes encubiertos y genios de la informática. El acusado es Alexander Alexandrevich Panin, un ruso de 24 años.

El FBI lo considera un «hacker de categoría mundial», un título que no te ganas siendo un cibercriminal del montón, de esos que vacían únicamente un par de cuentas bancarias. **Lo que hizo Panin fue diseñar unos programas que permitían a sus clientes-criminales cometer delitos a gran escala. Creó un conjunto de herramientas para que los ladrones de este siglo pudieran entrar en cuentas ajenas, romper contraseñas y reventar correos electrónicos con solo un clic de ratón. Panin creó el «pack perfecto para el cibercriminal» y lo convirtió en algo accesible, asequible y comercializable.**

Su paquete de programas llevaba el nombre de SpyEye, una combinación de las palabras 'espía' y 'ojo'. El FBI asegura que con él se infectaron más de 1,4 millones de ordenadores y se accedió a más de diez mil cuentas en 2013. Un cliente de Panin, conocido por el sobrenombre de Soldier, robó con él cerca de tres millones de dólares en seis meses. **Si se multiplica esta cifra por el número de compradores de SpyEye, que habrían sido unos 150, significaría que con el software de Panin se habrían robado 450 millones de dólares en todo el mundo. Quizá muchos más.**

El ladrón moderno no revienta cajas de seguridad ni desactiva alarmas. Recurre a virus informáticos que inyectan su ADN digital en ordenadores ajenos, que a su vez infectan otros que pasan a estar al servicio de los hackers. SpyEye, el programa de Panin, podía hacer todo

esto a la perfección: infectaba ordenadores, robaba contraseñas, vaciaba cuentas... **Para capturar a este superhacker, la Fiscalía ha recurrido a un batallón de colaboradores. Loucif Kharouni es uno de ellos. Como forense de alta tecnología, busca pruebas donde se supone que no las puede haber. Trabaja para Trend Micro, una empresa japonesa de seguridad, que cuenta con otros 24 agentes encubiertos repartidos por el mundo. Se ganan el sueldo reuniendo pruebas contra ciberdelincuentes.**

Kharouni y sus colegas se mueven con falsas identidades en los bajos fondos digitales y comparten sus descubrimientos con el FBI o la Interpol. Analizan discos duros, diseccionan virus y elaboran informes sobre hackers que saltan de repente a escena y hacen carreras fulgurantes, bajo alias como Monstr, MaDaGaSka o mechn1zm. A sus 35 años, Kharouni es todo un veterano. Lleva 14 en el negocio y no es muy optimista sobre el futuro: «El número de delincuentes no deja de crecer.**Sus ataques se hacen más precisos; sus métodos, más sofisticados». Su opinión sobre Panin y sus cómplices desvela una sana confianza en sí mismo: «Son delincuentes con mucho talento, sí, pero no son programadores sobresalientes».**

Kharouni oyó hablar por primera vez de SpyEye en 2009. Empresas y usuarios estaban aterrados: un nuevo programa robaba en un abrir y cerrar de ojos los datos de acceso a los ordenadores. Por esa misma época aparecieron en los foros de delincuentes hackers comentarios elogiosos sobre una nueva herramienta, tan polifacética como una navaja suiza. Estos foros son el verdadero bazar de los bajos fondos digitales. Aquí se reúnen, en círculos abiertos o privados, recomiendan y venden productos, negocian con información, ofrecen servicios y difunden rumores.

Los piratas informáticos compran en los foros lo que no pueden o no quieren crear ellos mismos, y la oferta es variada. **Se ofrecen troyanos: «Roba contraseñas de Opera, Mozilla Firefox, Chrome, Safari. Precio: US$ 8». O acceso a ordenadores que se convierten en bots abreviatura de 'robots' sin que sus usuarios lo sepan y se integran en las llamadas botnets, grandes redes de ordenadores esclavizados: «2000 bots por US$ 200». Se ofrecen ataques coordinados, por ejemplo, para**

bloquear la tienda on-line de una empresa: «Ataque de una hora: US$ 10. Un día: a partir de US$ 30. Una semana: US$ 150. Un mes: US$ 1200». En esta casba digital apareció SpyEye. La versión básica costaba 1000 dólares y la completa, 8500. La posibilidad de conseguir un programa hecho a medida era una de sus grandes ventajas. Los delincuentes solo compraban lo que necesitaban: módulos para entrar en cuentas bancarias de los Estados Unidos, el Reino Unido, España o Suiza.

La clientela de Panin pagaba por transferencia a cuentas de dudosas agencias financieras como Liberty Reserve, mediante ingresos en casas de dinero electrónico como Ukash o por transferencias a profesionales del lavado de dinero, que lo blanqueaban antes de ingresar en el bolsillo de Panin. **SpyEye ofrecía una posibilidad más. Por 30 dólares te ofrecía un módulo llamado Billing Hammer. Este software generaba una tienda virtual a través de la cual el delincuente podía venderse a sí mismo mercancías inexistentes utilizando los datos robados de las tarjetas de crédito. Es decir, Billing Hammer era un programa para el lavado de dinero.**

Panin incluyó otra posibilidad más, una extravagancia que indignó a los hackers de los foros. Si se introducía SpyEye en un ordenador que ya tuviera instalado Zeus, una herramienta similar pero de la competencia, el programa de Panin lo eliminaba. Zeus estaba en el mercado desde 2006, era un producto para hackers acreditados y costaba 5000 dólares. SpyEye, en cambio, permitía robar a cualquiera, incluidos los recién llegados al sector. **Los más estetas atacaron duramente a SpyEye, les desagradaba la forma en la que estaba programado, era poco elegante, decían. Pero estas críticas no impidieron su éxito.Cuando Kharouni se embarcó en la misión de cazar al fantasma que había creado SpyEye, se puso a analizar ordenadores infectados. Buscaba pistas en su código de programación.** Quizá por pereza, quizá por arrogancia, porque estaba seguro de que no lo podrían atrapar, Panin dejó huellas. Kharouni encontró en el programa un breve pasaje encriptado, que logró descifrar, y un alias: bx1.

Los cibercriminales tienen en la Red un número limitado de identidades, básicamente porque quieren que sus potenciales clientes puedan reconocerlos. Así que Kharouni empezó a buscar por los foros especializados a ese bx1. Y no tardó en encontrarlo. **En pocas semanas ya**

había localizado cinco alias y siete direcciones de correo electrónico, que a su vez lo condujeron a 29 sitios web, todos ellos mantenidos por bx1 para vender sus programas ilegales. Kharouni fue conociendo cada vez mejor a bx1. Era fanfarrón, irascible, arrogante. Se vanagloriaba de sus éxitos. A un bloguero norteamericano especializado en la materia le confesó: «Yo hackeé al tío ese que jodió a casi todos los bancos». Kharouni había encontrado el rastro bueno.

Pero cuanto más rastreaba a bx1, más pruebas lo conducían hacia un segundo pirata informático que se movía por Internet con los alias de Harderman y Gribodemon. Y, cuanto más investigaba, más seguro estaba de que Harderman, alias Gribodemon, era el verdadero creador SpyEye y que bx1 solo había aportado algunos de los componentes. **Harderman apareció el 10 de enero de 2010 en un exclusivo foro hacker llamado Darkode. El 6 de junio de 2011, Harderman le vendió la versión completa de su programa, por 8500 dólares, a un agente encubierto del FBI.** El dinero debía ser transferido a una cuenta en Liberty Reserve, mientras que el programa se entregaría a través de Sendspace.com, un servicio que permite el envío de archivos de gran tamaño.

Kharouni y otros investigadores habían conseguido conectar varias de las cuentas usadas con la identidad de Alexander Panin. Además, el FBI confiscó un importante servidor al norte del Estado de Georgia, utilizado por SpyEye y que albergaba cerca de un millar de gigabytes de información con pruebas de que se había atracado a 253 bancos con ayuda de SpyEye. **También encontraron registros que confirmaban que el servidor recibía sus órdenes desde Argelia, el país de origen de bx1. Bx1, alias Airlord, alias Princedelune, fue detenido en enero de 2012 en el aeropuerto de Bangkok. Según el FBI, su verdadero nombre es Hamza Bendelladj. Cuando los policías tailandeses lo esposaron, bx1 mantuvo la sonrisa durante tanto tiempo que se ganó otro alias más: The Happy Hacker (el Hacker Feliz).**

Hoy, Bendelladj sigue negando las acusaciones que pesan sobre él. Panin fue capturado medio año más tarde. Scott Ferber, el fiscal, y Loucif Kharouni, el investigador freelance, necesitaron mucha paciencia. Panin era mucho más precavido que bx1. Viajaba poco y dirigía sus negocios desde Moscú, donde se sentía seguro, ya que no hay un acuerdo de extradición

entre los Estados Unidos y Rusia. Sin embargo, el verano de 2013 Panin rompió sus costumbres y viajó a la República Dominicana. **Quizá necesitaba unas vacaciones. Sus negocios no marchaban del todo bien. Un hacker francés había roto el código de Panin y eliminado la protección anticopia. El criminal se había convertido en víctima. Cada vez que publicaba una actualización de su programa, su rival volvía a romper el código.**

Panin fue detenido por la Policía dominicana en junio del año pasado. Una foto que se publicó tras el arresto muestra a un joven con cara de pocos amigos, pelo corto y barba de tres días. El fiscal Scott Ferber no comenta detalles de la detención, podrían dar pie a un escándalo diplomático entre Washington y Moscú. **Y Ferber no quiere cometer errores, no ahora, cuando el final está tan próximo. Panin ha reconocido su culpabilidad y en agosto escuchará la sentencia de un tribunal de Atlanta. Treinta años de cárcel son una posibilidad más que real.**

Fuente: finanzas