LA MAFIA DIGITAL SECUESTRA MÉXICO

POR **HIROSHI TAKAHASHI**


modulan
modulan

Mafias de Europa del Este han comenzado a contagiar con programas para secuestrar computadoras y teléfonos móviles. Polonia, República Checa y México, en ese orden, son las naciones que más sufren ataques desde que arrancó 2015. Las autoridades mexicanas ya lanzaron una alerta. Un ***hacker*** ruso de 31 años es pieza clave para frenar estos ataques. El problema es que ni el FBI ni la Europol han podido atraparlo.

El inquilino del número 120 de la calle Lermontova, en el balneario ruso de Anapa, en la costa del Mar Negro, no posee ninguna característica extraordinaria, nada que llame poderosamente la atención.

Sus vecinos de esa ciudad antigua, de playas rocosas y frías, de la que poco se habla en las guías turísticas, lo consideran un hombre callado, amable y correcto, pero hasta ahí.

Saben, sí, que le gusta pasear en su yate, pero no mucho más. Hace meses que no lo ven. La última vez él estaba en el *lobby*, junto con su hija de nueve años y su esposa. Habrá sido a fines de mayo del año pasado.

Ni siquiera su viejo Volvo es digno de algo más que una mirada distraída. La calcomanía colocada en la defensa trasera del vehículo ofrece servicios nada inusuales: "Se reparan computadoras".

Ya sabrán meses después que Evgeniy Mikhailovich Bogachev, como se llama el inquilino, es algo más que el dueño de ese departamento de 250 mil dólares.

Sabrán, sí, que es bueno en el negocio de las computadoras.

* * *

La mañana del pasado lunes 19 de enero un alud de llamadas atiborró el celular del argentino Pablo Ramos. Algo inusual ocurría en América Latina. Un mapa electrónico de la región podría haber mostrado cómo se encendían los foquitos correspondientes a muchas ciudades de la región.

En México se prendieron muchas luces. Se detectó un brote masivo de correos electrónicos con archivos disfrazados de facturas. Cuando intentaban abrir la información ya habían perdido, sin saberlo, el control de sus máquinas.

Los archivos de las computadoras comenzaron a experimentar un proceso de cifrado. Un programa de cómputo maligno se había echado a andar; no se detuvo hasta que acabó de encriptar toda la información y, luego, apareció una ventana en la pantalla.

Los usuarios leyeron entonces un mensaje de advertencia que brincó de la nada:

"Tus archivos personales han sido encriptados por CTB-Locker. Tus documentos, fotos, bases de datos y otros importantes archivos han sido encriptados por una fuerte y única llave, generada para esta computadora.

"La llave está guardada en un servidor de internet secreto y nadie puede descifrar tus archivos hasta que pagues para obtener la llave privada.

"Tú solamente tienes 96 horas para depositar el pago. Si no mandas el dinero dentro del plazo límite, todos tus archivos permanecerán encriptados y nadie será capaz de recuperarlos".

En otras palabras: quienes leyeron ese texto el 19 de enero pasado ya no tenían mucho qué hacer: su computadora había sido secuestrada por las mafias digitales. Para liberarla, debían pagar un rescate.

Pablo Ramos y su equipo de la firma ESET, una de las pioneras en la industria de la ciberseguridad, comenzaron entonces a lanzar alertas a los países en los que tenían clientes.

Ya habían detectado la primera oleada de ataques y sabían que eso continuaría. Era algo masivo.

"México, al ser uno de los países más importantes de la región, estaba entre las primeras posiciones de ataque. No es que fuera el más afectado, pero sí en el que ocurría mayor propagación. Bases de datos enteras fueron secuestradas", cuenta Pablo Ramos en conversación telefónica desde Buenos Aires.

Al revisar la información estadística recopilada en su laboratorio, Ramos, quien encabeza en Latinoamérica al equipo de investigación de ESET, empresa con sede en Bratislava, Eslovaquia, famosa por sus sistemas de protección, pudo tener un diagnóstico más preciso.

"Lo que vimos el 19 de enero, cuando saltaron las alertas, fue un gran incremento de ataques con *malware*, como los llamados CryptoLocker o CTB-Locker".

* * *

Luego del mensaje que advierte sobre el secuestro de la computadora, los intrusos dan las indicaciones de cómo hacer el pago del rescate. Aunque el monto varía por región del planeta y

puede cambiar de un día a otro, en esa ocasión pidieron ocho *bitcoins*, cantidad en moneda virtual que equivalía hace unos días a aproximadamente 2 mil 350 dólares.

Los secuestradores indican entonces a qué dirección se debe dirigir el pago e informan que tardarán entre 15 y 30 minutos en confirmar la transacción.

La liberación de los archivos comenzará en automático. Dan instrucciones: no debes desconectar tu computadora, correr el programa antivirus o salirte de la red. Cualquier suspensión afectará accidentalmente tu información almacenada. Si no tienes moneda virtual (*bitcoins*), te indican cómo comprarla.

El ataque con CTB-Locker tuvo un impacto directo en América Latina, pero la magnitud del ataque fue global.

ESET descubrió que México ocupó la tercera posición a escala global por el número de ataques detectados, después de República Checa, quien fue segundo país con más ataques, y Polonia, en primero.

"Es muy difícil cuantificar las víctimas, pero fueron muchas", dice Pablo Ramos.

Hubo miles de ataques ese día en todo el continente. Sólo en Estados Unidos, ESET calcula que entre un cinco y siete por ciento de las víctimas pagaron rescate. "Si cada uno debe pagar 2 mil 350 dólares por persona", las ganancias fueron enormes.

* * *

Más de medio año antes del ataque de enero de 2015, algunas de las agencias de seguridad cibernética de todo el mundo habían cantado victoria antes de tiempo.

El viernes 30 de mayo de 2014, en una acción coordinada por el FBI, organizaciones policiacas especializadas, entre ellas el Centro Europeo contra el Cibercrimen (EC3), anunciaron que desmantelaron una vasta red de computadoras *zombie* y confiscaron servidores con los que operaba el virus CryptoLocker.

"Esta grande y muy exitosa operación ha sido una prueba importante para los Estados miembro de la Unión Europea, para demostrar su habilidad de actuar rápido, decisiva y coordinadamente contra los peligroso criminales de la red que han estado robando dinero e información de sus víctimas en Europa y todo el mundo", dijo Troeis Oerting, la cabeza del EC3.

"Durante muchos días y noches, la ciberpolicía de países europeos en cuartos de operación del EC3 maximizaron el impacto de esta investigación conjunta. Cada vez somos mejores en este tipo de operaciones, y muchas más sin duda se llevarán a cabo", alardeó Oerting.

El lunes 2 de junio dieron por terminada la misión, con conferencias de prensa en La Haya y Washington.

Sin embargo, una pieza faltaba en el rompecabezas del discurso triunfal de las autoridades: el sospechoso de crear la red y los programas para secuestrar computadoras seguía prófugo.

> "Tú solamente tienes 96 horas para depositar el pago. Si no mandas el dinero dentro del plazo límite, todos tus archivos permanecerán encriptados y nadie será capaz de recuperarlos".

* * *

El ataque encabezado por el FBI no tuvo un efecto duradero. Una extraña mutación de CryptoLocker encendió nuevamente las alertas en Washington desde julio del año pasado, apenas un mes después de anunciar la operación.

A principios de ese mes comenzó a circular en las agencias del gobierno estadunidense un documento elaborado por el Statewide Information & Analysis Center y la Cyber Intelligence Network, que advierte de la existencia de un programa que puede tomar bajo su control los datos sensibles de cualquier computadora y servidor.

Los *hackers* del gobierno de Estados Unidos advirtieron que no debía confundirse el virus CryptoWall con el anterior (CryptoLocker), amenazas parecidas, pero diferentes. Una evolución más dañina que daba por sentado que los secuestradores no habían estado descansando.

El cable del gobierno estadunidense explicaba que CryptoWall fue descubierto a finales de abril de 2014. Una vez que entra en acción encripta inmediatamente los archivos del disco duro local y cualquier red o dispositivo de almacenamiento ligado a la máquina.

Cuando toma el control de la información, CryptoWall despliega un mensaje en la pantalla de la víctima y exige 500 dólares, que deben pagarse en *bitcoins*, a cambio de una llave para retirar el candado a los archivos. Al mismo tiempo, un contador en la pantalla comienza a correr en reversa, otorgando 100 horas de plazo para pagar, antes de que el monto de la extorsión aumente al doble.

Entre los afectados, sin entrar en muchos detalles, estaban algunos cuarteles de bomberos y agencias de seguridad. Cientos de computadoras y servidores del gobierno estadunidense estaban bajo ataque.

El gobierno de Estados Unidos dice que perdieron información, pero fueron capaces de rescatar sus sistemas con un respaldo.

"Hasta ahora, la mayoría de las víctimas se localizan en Estados Unidos, numerosas víctimas han sido afec-

tadas entre múltiples sectores", indica el documento. "CryptoWall se enmascara como un programa que pide al usuario desplegar el archivo antes de leerlo. Una vez que el usuario trata de abrir el archivo, CryptoWall se replica a sí mismo a través de múltiples lugares de la máquina y demanda el pago".

Washington advertía que debido al nivel de complejidad de la encriptación es necesaria obtener la llave que ofrecen los *hackers* para recuperar los archivos afectados.

* * *

La aparición del virus malicioso mutante mostró que los esfuerzos de la red internacional de policías cibernéticas habían sido en vano.

Tampoco sirvió de mucho que el gobierno de Estados Unidos hubiese identificado al responsable de la infección de cientos de miles de computadoras en su territorio y la pérdida de más de 100 millones de dólares a causa de los ataques que dirigió.

El FBI llevaba ya varios años tras sus pasos desde que comenzó a investigarlo en septiembre de 2011, luego de rastrear el origen de una versión modificada de un virus conocido como Game Over Zeus (GOZ), responsable de infectar más de un millón de computadoras personales.

Desde entonces ya les provocaba problemas y dolores de cabeza con un complicado código llamado CryptoLocker.

De acuerdo con la demanda que el gobierno de Estados Unidos presentó contra quien usaba los alias "Lucky12345", "Slavik" o "Pollingsoon", GOZ es un *malware* que roba datos bancarios de computadoras que infecta y luego enlista en una *botnet*, una red que controlan remota, ilegalmente y en secreto, para cualquier propósito.

Ese tal Lucky12345 creó así un ejército de máquinas *zombie* que obedecen a un líder y son utilizadas para atacar a gobiernos, robar bancos, tirar páginas de internet, espiar o secuestrar computadoras.

"CryptoLocker es una forma de *malware* conocida como *ransomware*, que infecta computadoras, encripta archivos clave, y luego demanda un rescate de cientos de dólares para regresar los archivos encriptados a un estado de lectura. GOZ es uno de los principales vehículos para infectar computadoras con CryptoLocker", dice la demanda presentada el 27 de mayo de 2014.

* * *

México no podía, como ningún otro país, permanecer inmune a los ataques. Por el contrario. "En las últimas semanas hemos visto que están atacando a la gran empresa mexicana", dice Alberto García, director general de Symantec en México.

Están afectando también a entidades de gobierno y bancos. "Les llega a los ejecutivos, les piden que paguen por el rescate de su información para que se las liberen", explica el directivo de una de las empresas de seguridad más respetadas en el mundo, incluso una de las firmas de seguridad que participa en la cacería global de Lucky12345.

A Pablo Ramos le ha tocado atender casos de ese tipo. "El *malware* no sólo cifra la información, sino que toma todas las carpetas compartidas. Imaginemos que tiene un montón de accesos a la institución financiera y se ve

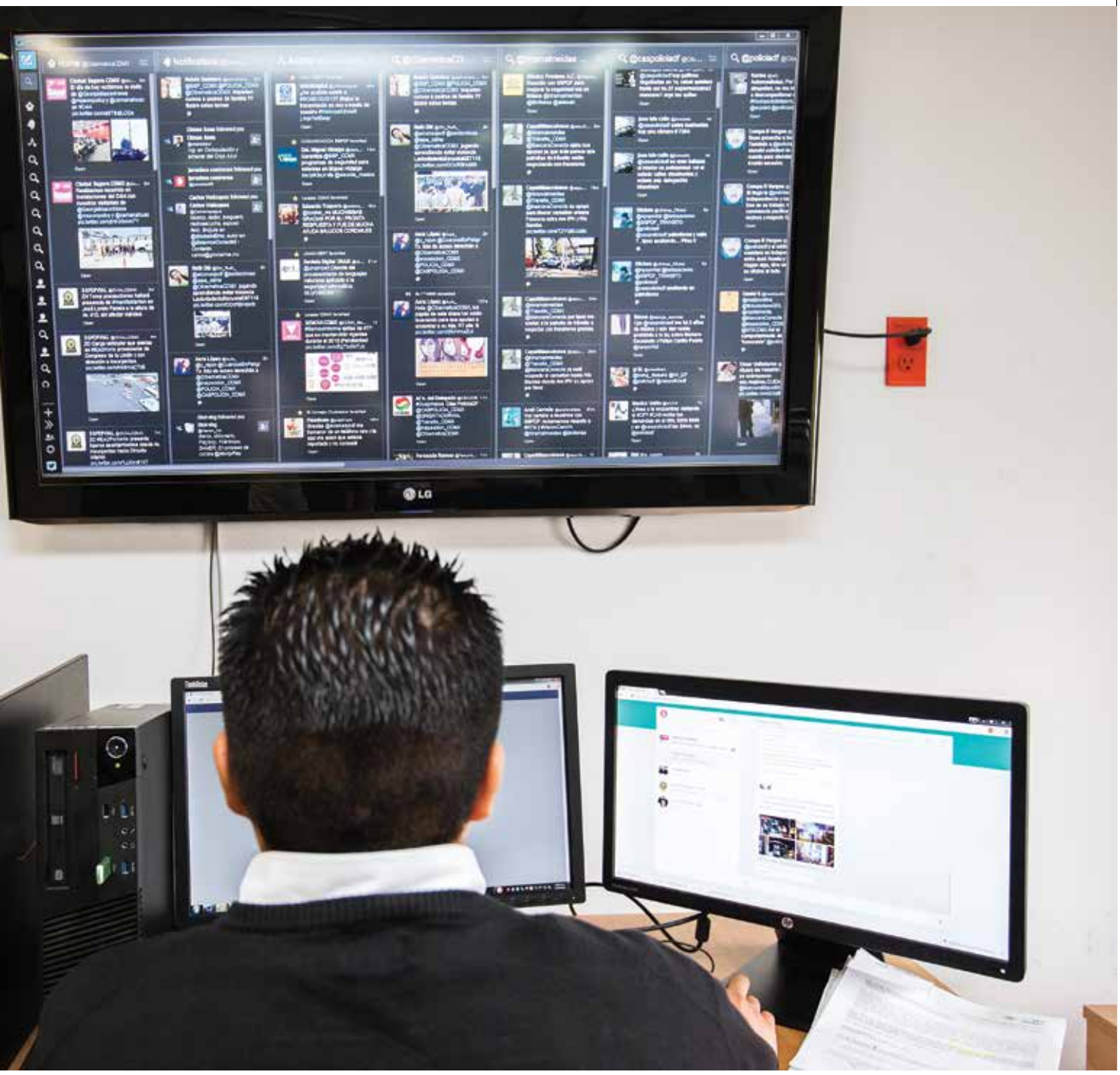
POLICIA CIBERNÉTICA
La policía del DF ha puesto en marcha un cuerpo de especialistas para vigilar delitos en esta plataforma.

afectado. Literalmente toda esa información se ve cifrada. Tardan semanas o meses en recuperar los sistemas, a pesar de tener un respaldo".

Vicente Amozurrutia, director de Check Point Software Technologies en México, coincide en que empresas han sufrido ataques recientemente en este país.

"Hay muchos ataques contra grandes empresas, que no sepamos o que no nos enteremos, es diferente. Pero sí, sí hay. No te puedo dar nombres, pero tenemos conocimiento de empresas que han vivido estas situaciones", cuenta Amozurrutia, representante de una de las firmas más respetadas en seguridad cibernética, cuyo cuartel general se encuentra en Tel Aviv, Israel.

El director de Symantec recuerda que recientemente una entidad financiera en México sufrió un ataque muy fuerte, infectando muchísimas máquinas con *ransomware*. Los expertos de la firma de seguridad llevaron a su equipo de respuesta inmediata y comenzaron a lu-



ENCRIPTADOS Este es el mensaje que se despliega en la pantalla una vez que el *malware* se ha instalado.

char. Hallaron que los atacantes estaban en China. Consiguieron detener el ataque, pero la ofensiva impactó el negocio.

"Escuchamos casos en Europa, Estados Unidos, en Japón; tenemos que aprender de ellos. Punto importante: en México los estamos viviendo, nuestra compañía tiene un tema de éstos todos los días", agrega García.

No sólo es una percerpción de las firmas que brindan servicios de seguridad digital.

El pasado 23 de febrero, la Policía Federal alertó a los usuarios de internet sobre las amenazas de CTB-Locker.

"Esta nueva versión de *software* intruso es operada a distancia por defraudadores, quienes después de obtener información de la computadora extorsionan al propietario para que a cambio de ciertas cantidades de dinero se entregue la contraseña que le permita recuperar sus archivos", advierte en su comunicado.

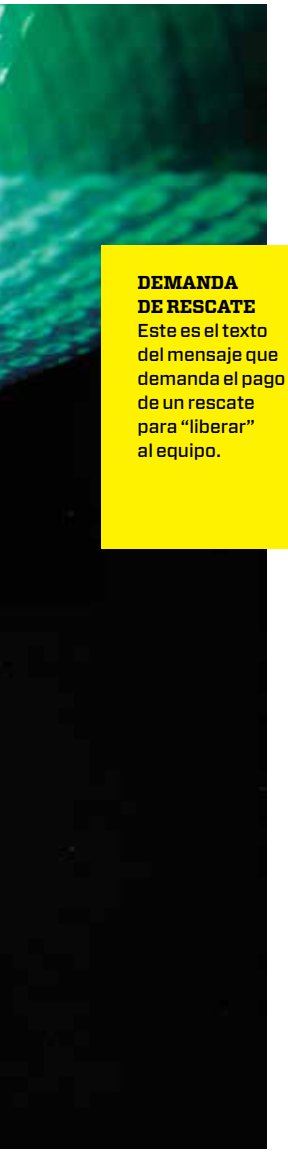
"Las primeras infecciones de este tipo fueron identificadas en países como Inglaterra, Alemania y Rusia. La Policía Federal informa que dado que se está intensificando este comportamiento, es probable que los usuarios de internet de México comiencen a recibir mensajes de correo electrónico que pongan en riesgo sus equipos de cómputo".

* * *

Lucky12345 ha sido identificado por los servicios de inteligencia de Estados Unidos como un joven de 30 años que ha realizado una tarea mayúscula: creó una *botnet* gigante, una colección de computadoras comprometidas y controladas sin el conocimiento de las víctimas.

Una *botnet* puede ser usada para múltiples propósitos comerciales, como mandar *spam*, robar datos o cometer fraudes financieros.

"CryptoLocker es un programa malicioso diseñado para extraer pagos por el rescate de las máquinas de las víctimas. Después de infectar una computadora, encripta los archivos de las máquinas en el disco duro. Una vez que esto ocurre, despliega un aviso en la pantalla de la computadora, demandando el pago de rescate a cambio de la llave para desencriptar los archivos de la víctima", advierte el gobierno estadunidense en su deman-



DEMANDA DE RESCATE
Este es el texto del mensaje que demanda el pago de un rescate para "liberar" al equipo.

da contra el *hacker*, presentada en una corte federal.

"Las víctimas que se rehúsan a pagar el rescate enfrentan una pérdida de datos, pues el algoritmo de encriptado utilizado por los acusados es efectivamente inquebrantable". Sólo tenían 72 horas para cubrir el rescate antes de que los archivos fueran destruidos. Lo mismo ocurriría si alguien intentaba desbloquear el equipo por su cuenta.

Estados Unidos agrega en la demanda que CryptoLocker emergió por primera vez a mediados de 2013 y que infectó 230 mil computadoras en los meses siguientes, más de 120 mil sólo en Estados Unidos.

La demanda revela que el Departamento de Policía de Massachusetts sufrió el secuestro de su servidor principal, que guardaba documentos administrativos, materiales de investigaciones criminales, y las fotos digitales de los detenidos, así como datos confidenciales de los mismos. Para recobrar esos archivos, pagaron 750 dólares de rescate.

Lucky12345 humilló, pues, a la policía del país más poderoso del mundo. Y es un hombre al que ni los *hackers* que trabajan para el gobierno de Barack Obama han podido ubicar.

* * *

¿Quién está detrás de los nuevos ataques? –se pregunta a [redacted] Pablo Ramos, el jefe de investigación de ESET en América Latina.

–La realidad es que las cosas que están pasando van de la mano. Se asume que Europa del Este es una región activa en cibercrimen; allá han sido creados un montón de códigos maliciosos. Claramente estamos hablando de un personaje muy importante al hablar de inseguridad informática.

"Los creadores del CTB-Locker definitivamente hablan ruso", dice por su parte Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para América Latina de Kaspersky Lab.

Desde el norte de Miami, donde tiene sus laboratorios, dice que es correcta la percepción del aumento del *malware* de cifrado de información y de la proliferación de víctimas a las que les piden pagar rescate en la región.

Ellos detectaron las primeras versiones de *ransomware* hace como siete años. Rompieron el protocolo de cifrado y lograron liberar los archivos.

Lo malo es que ahora se utilizan algoritmos de cifrado muy fuertes, de la fuerza militar. Romper esos protocolos es casi imposible. Y mezclan sus ataques.

–¿Por qué vemos que los ataques están repuntando en América Latina?

–Porque el mercado está listo. La gente tiene dinero, información valiosa, y los criminales necesitan expandir sus actividades. Es un negocio garantizado. Comienzan a expandir sus mercados. Y también porque la gente aquí en América Latina es bastante ingenua, da *click* prácticamente en cualquier cosa –responde Dmitry Bestuzhev.

* * *

Ya pasó casi un año desde que las autoridades estadunidenses y europeas anunciaron que golpearon a la banda creadora del virus que secuestra computadoras y presumieron que estaban cerca de capturar a su líder.

Poco éxito también han tenido las autoridades europeas, australianas, canadienses, japonesas y ucranianas, así como Microsoft, Intel, F-Secure, Symantec y Trend Micro, que participaron en la investigación.

La reputación del FBI, por ejemplo, y de los expertos cibernéticos estadunidenses y de sus aliados, lleva un año cuestionada. Anunciaron en grande que habían frenado CryptoLocker, pero lo único que consiguieron fue nuevos ataques, más peligrosos y complejos.

Tanto que se han visto forzados a reportar la acelerada evolución del virus. El pasado 24 de febrero emitieron una nueva alerta:

"El FBI busca desmantelar redes criminales que se dedican a 'secuestrar' computadoras a cambio de dinero. Los ataques, conocidos como estafas de *ransomware*, aumentaron en los últimos años y afectan a computadoras personales, negocios, instituciones financieras y académicas y hasta agencias de gobierno", reiteró la agencia en su página de internet.

La alerta en inglés y en español advierte: "Dichos 'secuestros' ocasionan pérdidas de ganancias, información personal, datos confidenciales e incluso dañan la reputación de compañías e instituciones".

** *

Pablo Ramos recuerda que con esa operación internacional las autoridades trataron de desmantelar la red de quien también se conoce en el mundo como "Pollingsoon", pero lo único que consiguieron fue lo opuesto: atrajo más atención sobre el *hacker* más buscado del mundo.

Y sigue creciendo el virus CryptoLocker. En 2013 Check Point Software Technologies detectó más de

530 mil computadoras secuestradas con éste último *ransomware*.

"Los ataques vienen de todas partes del mundo, de Europa del Este, de Asia, de México", dice Alberto García, director general de Symantec. "Hay un tema: estas personas contratan muchachos universitarios, en cualquier parte del mundo, y les dan unos 200 dólares por *trabajito*".

Pablo Ramos explica que el negocio crece por dos motivos:

"Los cibercriminales venden a diferentes personas los virus. Ellos ganan plata no robando la información, sino a través de lo que venden a otras personas metidas en el cibercrimen. La realidad es que son dos modelos de negocios diferentes. Cuando empieza a vender el *crimepack*, se propaga mucho más".

Dmitry Bestuzhev, uno de los más reconocidos expertos en amenazas cibernéticas y enviado directo del millonario Eugene Kaspersky a vigilar la región, dice que las ofertas están en el mercado negro, principalmente en ruso.

Cuestan alrededor de 3 mil dólares, lo que incluye un mes de soporte técnico gratuito y luego hay que pagar 300 dólares al mes para tener el código malicioso trabajando. "El paquete incluye todo lo necesario para comenzar a lucrar infectando a las víctimas", explica Dmitry.

En América Latina se han creado algunos códigos maliciosos para secuestrar, ha habido intentos de *ransomware* e incluso Dmitry guarda algunas muestras.

"El *ramsomware* de América Latina es bastante fácil de descifrar", explica el enviado de Kaspersky. "Son algoritmos muy sencillos, muchas veces la idea es meter un susto más que cifrar la información".

Vicente Amozurrutia, de Check Point, dice que hoy comenzamos a escuchar mucho acerca del secuestro de computadoras, delito que se está trasladando a los dispositivos móviles. "Me secuestraron mi computadora y este disco duro y este servidor. Lo que sigue es 'me secuestraron mi móvil'", adelanta.

"El crimen existe, no porque ellos estén exitosamente infectando a los usuarios, existe porque la gente paga. Si nadie pagara el rescate, los criminales no harían nada", dice Dmitry Bestuzhev, de Kaspersky.

"La recomendación es no negociar. Un chantaje es para siempre", agrega García, de Symantec.

* * *

A medida que crece el secuestro de computadoras en el mundo, en esa medida los esfuerzos por detener al líder detrás de esa actividad han fracasado.

El Departamento de Estado de EU se vio forzado a ofrecer una recompensa de 3 millones de dólares a quien diera información que ayude a capturarlo.

Pero nada. El diario inglés *The Telegraph* visitó el número 120 de Lermontova, en Anapa, Rusia, y los residentes del edificio de esa ciudad costera se sorprendieron de que la persona que encabeza a *hackers* que infectaron cientos de miles de computadoras con virus capaces de robar datos bancarios y secuestrar la información de las máquinas para después pedir un rescate a sus dueños, era un joven de 30 años llamado Evgeniy Mikhailovich Bogachev.

No podían creer que el líder de los cibercriminales detrás de miles de ataques y secuestros era su vecino, el que conducía un viejo Volvo sedán con una calcomanía en la defensa trasera en la que podía leerse: "Se reparan computadoras". 09