

nota de tapa

WWW

El lado oscuro de la Web

WWW

Por Darío Laufer
Fotos: Gustavo Fernández

Christian Cámara tiene 20 años, estudia ingeniería informática y se lo acusa de ser un supuesto hacker que vulneró cuentas bancarias y servidores de juegos, con lo que habría podido recaudar hasta US\$ 50.000 por mes. Él dice que es inocente y asegura que todo es un invento de quienes lo denunciaron. INFORMATION TECHNOLOGY habló con él y accedió al expediente de una causa sin resolución en la que se cruzan el submundo de los gamers, las operaciones de prensa y los virus informáticos.

nota de tapa

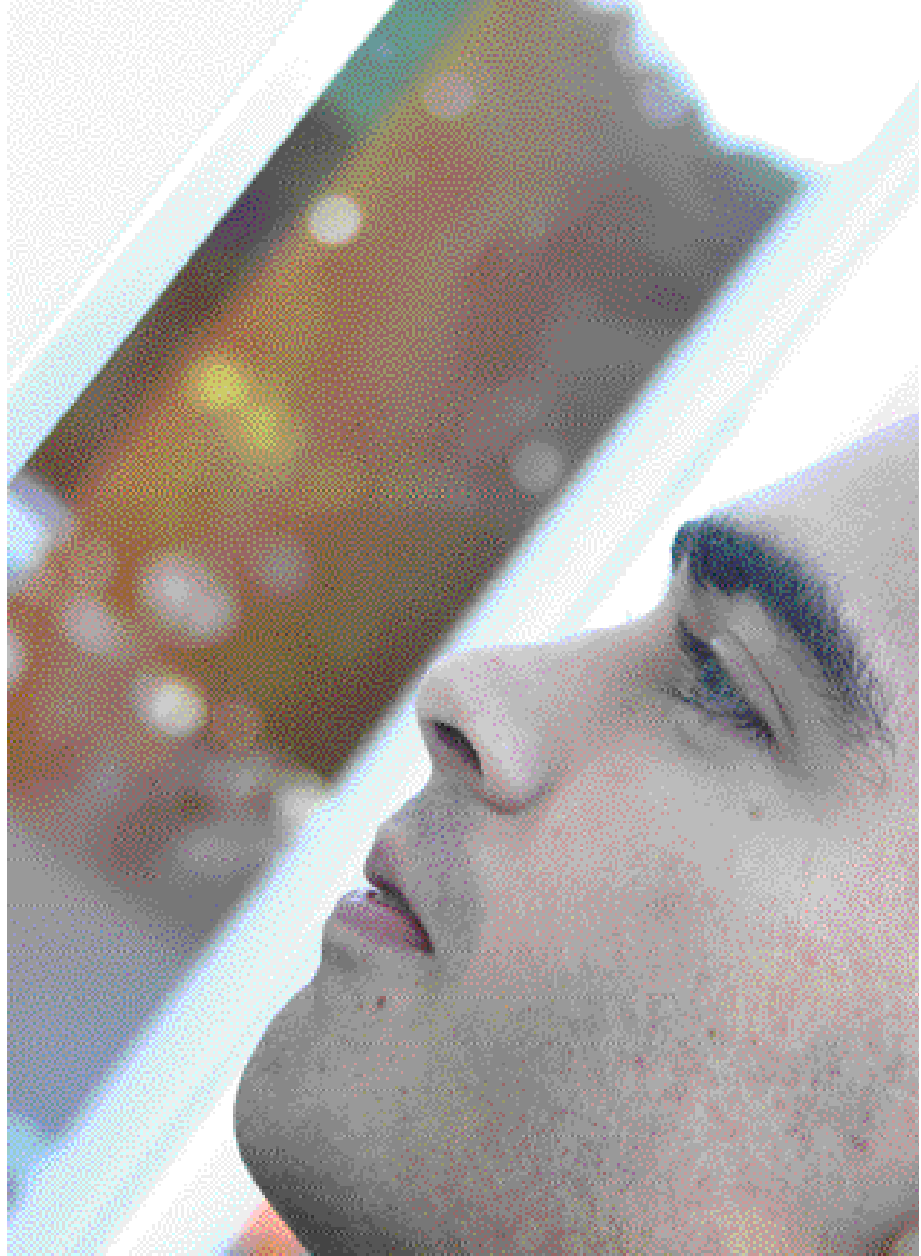
La noche del jueves 12 de septiembre de 2013, cuando Christian Iván Cámara volvía de cursar la materia Aplicaciones Interactivas en la Universidad Argentina de la Empresa (UADE), tuvo un déjà vu: el allanamiento que había acontecido en su domicilio en la Ciudad Autónoma de Buenos Aires, la mañana del 4 de julio de ese año, era contado como la noticia del momento.

Los móviles de C5N, Canal 26 y América Noticias hacían guardia para que explicara a los televidentes cómo había logrado sustraer US\$ 50.000 por mes desde hacía al menos un año, utilizando sus capacidades de súper hacker, como lo bautizó al aire Walter Enrique Bernal, jefe de la División de Delitos Informáticos de la Policía Federal Argentina, durante una entrevista que apareció en Visión 7, el noticiero de la Televisión Pública.

“Esa noche llegaba de cursar y me encontré con la televisión en la puerta de mi casa. No sabía qué hacer. Estaba desesperado”, cuenta Christian Cámara.

El encargado de informar a la televisión fue Manuel Romero Victorica, abogado de Cámara. “Me llamó la madre y fui a su casa. Recuerdo que esa noche llovía mucho. Christian estaba en mi auto, tapado con mi impermeable y lloraba porque no quería salir en televisión. Se cubrió con mi ropa y entró a su casa. Yo me quedé respondiendo las preguntas de los periodistas. Luego entré, me quedé casi una hora viendo lo que salía por televisión. No podíamos creer lo que se decía”, asegura.

Tras responder a las preguntas de los móviles, fue al canal de noticias C5N para explicar el caso. “En la causa no se habla de una estafa de US\$ 50.000 por mes, ni Christian estuvo preso”, dijo esa noche Romero Victorica. Al escuchar las palabras clave por parte del subcomisario Bernal, los medios tuvieron los



“No quiero que hablen más de ese invento que salió en los medios”

Christian Cámara

titulos. La noche del 12 de septiembre, la agencia de noticias Télam envió el cable avisando que “habían detenido a un súper hacker que desviaba grandes sumas por la Web. Y luego informaron que “los peritos trabajan con la hipótesis de que el joven desviaba a su favor cerca de US\$ 50.000 por mes”.

Al día siguiente, la historia fue protagonista de diversos noticieros y repercutió en medios internacionales como BBC Mundo, los diarios El Comercio de Perú y La Tercera de Chile, entre otros.

En televisión desfilaron los especialistas en seguridad informática: “Ellos tenían computadores realmente potentes, en las imágenes se veían unos cuantos servidores rackeables, que se ponen en un rack como si fueran ranuras y tienen gran capacidad de procesamiento”, remarcó esa



noche Gustavo Talaván, consultor informático en t revistado por Eduardo Feinmann, sobre la imagen de un rack vacío en pantalla.

De acuerdo con los medios, Christian Cámara había desarrollado un virus que esparcía en computadoras que se conectaban a su servidor de juegos y que, una vez descargado, convertía a esas máquinas en “zombies” que respondían a sus órdenes. Por ejemplo, la de robar pequeñas cantidades de dinero de cuentas de la red que comandaba y enviarlas a cuentas propias o de conocidos que participaran de la estafa.

La información técnica disponible había sido tomada de unas escuetas palabras dadas el 12 de septiembre, dos meses después del allanamiento. “Según dijeron los voceros de la Policía, en ese lugar, situado en Juan de Garay al 3200, fueron secuestradas computadoras con capacidades de cálculo muy superiores a las corrientes, cables de conexión especiales, servidores, routers y 14 discos rígidos”, dice el cable de Télam sin dar mayores especificaciones.

Un día antes de la aparición en los medios del allanamiento, el experto en seguridad informática Gustavo Presman había sido contactado por los abogados de Cámara para que realizara la pericia de parte. “Al ver la noticia en televisión, p regunté si se trataba del mismo caso y me respondieron que sí”, revela. Finalmente no logró ce nar trato y no participó del caso.

Baticueva tecnológica

Diez meses después del allanamiento televisivo, Christian Cámara está sentado en el bar de la esquina de la UADE, donde cursa el tercer año de la carrera de Ingeniería Informática. Si bien cumplió 20 años dos meses después de su debut estelar en los noticieros como el “súper hacker”, pare-

Izq.: Fotos del allanamiento al domicilio de la familia Cámara que forman parte del expediente. Der. y abajo: La cobertura del caso en diversos medios.

ce un estudiante de los primeros años del secundario.

Es tímido y tiene cierta dificultad para hablar debido a un trastorno neurológico hereditario que también afecta la movilidad de su ojo izquierdo. Algo de lo que prefiere no hablar. Sin embargo, su mirada cobra fuerza cuando habla del caso que lo afecta. “Quiero que todos sepan lo que pasó. No quiero que hablen más de ese invento que salió en los medios”, afirma. Y se defiende: “Un hacker es un delincuente, y eso son los que armaron esta causa. Yo no soy un hacker”. Tras el allanamiento realizado el jueves 4 de julio de 2013, que duró entre las 9 y las 14 horas de ese día, Christian pudo entrar a su casa a reunirse con su madre y su hermano Germán, que en ese momento tenía 16 años. “Mi papá llegó a la noche, cuando salió de trabajar”, cuenta. Alberto Cámara asegura que en esa época no



nota de tapa

tenía celular y que se enteró del allanamiento mucho más tarde. “No tenían forma de comunicarse conmigo”, dice.

En la casa familiar operaban un servicio para gamers llamado FireHosted, que se dedicaba a proveer juegos en red. El emprendimiento había nacido en 2008, cuando Cámara estudiaba en la escuela secundaria y que volvió a retomar en enero de este año.

Cámara usaba su habitación de la casa familiar, ubicada sobre la avenida Juan de Garay, entre 24 de noviembre y Sánchez de Loria, en el barrio de San Cristóbal. Es un típico dúplex de ladrillo a la vista construido en la década del '80, que comparte terreno con otra propiedad en espejo. Su cuarto, en el primer piso, está empapelado de color celeste y tiene una guarda con motivos campestres, un diseño bastante común durante la infancia de Christian, que nació el 9 de noviembre de 1993.

Las fuentes policiales dieron a conocer que antes del allanamiento debieron cortar la energía eléctrica en la manzana para que las cámaras de seguridad que supuestamente había instalado para vigilar la cuadra no pudieran ser usadas. “Desde su domicilio monitoreaba no sólo el frente de su casa, sino también toda la cuadra”, declaró el subcomisario Bernal. Cámara niega esa versión y los citados equipos no forman parte del inventario de la causa, ya que no fueron encontrados.

Durante el procedimiento, Silvina, madre de Christian, y Germán, su hermano menor, vieron cómo la policía secuestraba un rack, seis servidores apilables que habían sido armados por Cámara para brindar el servicio a los gamers, routers, 14 discos rígidos y una placa de red Gigabyte 880gm-UD2H con placa de video incorporada, que forman parte de los elementos de la pericia.

Dos meses más tarde, este hallazgo motivó la denominación de “baticueva tecnológica” por parte de los voceros policiales durante la televisión del allanamiento. “Eran dos usuarios maliciosos, uno de ellos mayor de edad, el otro un



**“Si el hacker
afecta un
servidor con su
'key logger', se
puede instalar
código
malicioso”**

**Camilo Gutiérrez
Amaya,**

especialista de Eset

adolescente”, dijo Bernal al noticiero Visión 7. “Eran dos hermanos, muy avezados en el uso de tecnología informática”, amplió luego ante las cámaras de C5N. De acuerdo con la denuncia, Silvina y Germán Cámara no están involucrados en la causa, aunque sí se acusa a Alberto Cámara, padre de Christian.

“El motherboard encontrado en el allanamiento es un modelo que se vendió mucho por su prestación de precio y calidad, con un precio al público de entre US\$ 115 y US\$ 130. Los que utilizan los gamers hoy en día parten de los US\$ 300 y llegan a US\$ 700”, especifica Gastón Finkelstein, gerente territorial de Gigabyte Argentina. “Hace cuatro años, cuando se lanzó ese producto, los gamers lo usaban para jugar al Crisis porque era relativamente económico, y al tener la placa de video incluida, permitía ver el juego en buena calidad”, amplía.

La denuncia

En 2010, Cámara tuvo los primeros problemas con Pablo Rubén Delgado, también dedicado al negocio de hosting y gaming, que administraba Servilink, un sitio para jugar en red. En la causa 16.490 —a la que tuvo acceso INFORMATION TECHNOLOGY—, radicada en la fiscalía que dirige Graciela Gils Carbó (hermana de la procuradora general de la Nación, Alejandra Gils Carbó) y que motivó el allanamiento en el domicilio de los Cámara, Delgado sostiene que en enero fue víctima de una “transferencia indebida de \$ 4.000 desde su cuenta de Dineromail a un usuario registrado a nombre de cristina@visualbasic6.com.ar”, que pertenecería a la madre de Christian. Seis meses más tarde declaró haber sufrido “varios ataques de denegación de servicio” de su emprendimiento Servilink, por los que culpa a Cámara.

Allí agrega que también sufrió el hackeo de la cuenta de mail pagos@servilink.com.ar por las que cobraba las transacciones con sus clientes. “Ese día —por el 25 de julio de 2012— entre las 20:49 y las 21:07, desde la IP 65.99.247.2, efectuó una transferencia de \$ 2.378 a favor de la cuenta dantemilitello@live.com.ar”, detalla la denuncia.

“Las empresas globales instalan servidores en países con mayor número de usuarios que la Argentina”

Sebastián Di Nardo,

socio gerente de la revista Irrompibles

Dante Militello, propietario de esa casilla de correo electrónico, es otro de los denunciados en la causa. Estudia diseño web, tiene 21 años y su casa en Rosario fue allanada el 4 de julio de 2013, tras la denuncia de Delgado, quien lo responsabiliza por la extracción de dinero de su cuenta de Dineromail. En el escrito, el denunciante asegura que Militello, junto con Christian Cámara, forman un equipo de hackers que arruinaron su negocio.

“Hablé con mi abogado y me pidió que no haga declaraciones. Realmente me gustaría poder contar este tema, pero hasta que la causa no cierre no puedo prestar declaración. Por otro lado, quiero comentar que lo que se dijo en televisión sobre el súper hacker que robaba US\$ 50.000 fue algo bastante gracioso para todos, ya que no es verdad. Cuando hablé con gente de Tribunales que estaban encargados de la causa me dijeron que ellos nunca dijeron algo así. Y de hecho no existe acusación de ese tipo”, explica Militello a INFORMATION TECHNOLOGY desde Rosario.

Más allá de lo publicado en los medios, hoy la causa se encuentra en su primera fase y la Fiscalía espera el resultado del análisis del área de Delitos Informáticos de la Policía Federal para poder avanzar con la investigación. “En este momento se siguen haciendo las pericias sobre los equipos obtenidos durante el allanamiento y por ahora no hay ningún elemento que acredite la denuncia. Para poder tener algo cierto vamos a tener que esperar el avance de la investigación”, explica Sebastián Scarcella, empleado de la Fiscalía 28.

Ante la consulta de INFORMATION TECHNOLOGY, Delgado no respondió a ninguno de los e-mails enviados y llamados realizados. “Luego de la denuncia no apareció más”, asegura Rodolfo Vaccarezza, abogado del estudio que defiende a los Cámara.

Donde sí explicó Delgado su posición frente al caso fue en su perfil de Facebook: “Todo el que pueda vea C5N, por favor, ahí está la casa de Christian Iván Cámara, detenido por todo lo que nos hizo. Gracias”, posteo el 13 de septiembre de 2013. En esa red social, Delgado tiene su perfil abierto y sube fotos de sus prácticas de taekwondo y sus participaciones en competencias de rally en cuatriciclo. También se dedica a subir



nota de tapa

todos los artículos sobre el allanamiento al domicilio de Christian Cámara, que compare con su red de amigos, muchos de ellos al tanto de los problemas que tenía con los Cámara y Militello.

Aunque su abogado le aconsejó no hablar con la prensa hasta que cierre la causa, desde Rosario, Militello se muestra confiado con la evolución del proceso jurídico. “No falta mucho para que la causa se cierre y yo pueda contar en detalle y proporcionar material que seguramente servirá. Voy a esperar a que salga la nota, que hable Christian y luego voy a contar mi verdad”, advierte.

El nombre del padre

La mayor parte de la información sobre los Cámara no se encuentra en la causa ni en la pericia. Está en los foros de gamers de Internet, donde la noticia fue propagada el 13 de septiembre, luego de la televisión del allanamiento.

En esa fecha, usuarios con distintos nombres pero formas similares de redacción e idénticos errores de ortografía, se encargaron de plasmar toda la información existente sobre Christian Cámara y sus familiares cercanos. En más de diez sitios dedicados al gaming subieron links de los videos de los noticieros, la dirección precisa de su domicilio, los documentos de cada uno, números de celular y las fechas de nacimiento, entre otros datos.

Tanto los usuarios que postean como los comentaristas, utilizan apodos para preservar su identidad. En algunos casos, se repiten nombres falsos y direcciones de e-mail, como es el caso de Carola Katerina Costa, quien pide que le envíen información sobre los Cámara a su casilla.

En esos sitios se señala al padre de Christian, Alberto Cámara, como ingeniero informático responsable de los ataques e intentos de hackeo realizados

Empresa en la nube

Para armar un revendedor de juegos online no es necesario abrir una sociedad, estar inscripto en el régimen de autónomos, y ni siquiera ser monotributista. Sólo se necesita contar con un dominio en Internet, una conexión, e invertir en hardware para alojar los juegos. Y una salvedad: si se trata de una dirección web registrada en la Argentina, hasta 2013 el trámite era gratuito. Desde este año, la renovación de los dominios com.ar tiene un valor de \$ 160 al año. Los dominios punto-com, registrados en los Estados Unidos, van desde US\$ 8 el más económico, hasta los miles de dólares los más solicitados. El pago a los servidores se realiza con tarjeta de crédito, depósito bancario o sistemas como Pago mis cuentas, Pay Pal y Western Union, que permiten hacerse del efectivo sin presentar comprobantes fiscales. De la misma forma pueden pagar los usuarios, y el dinero pasa por una cuenta bancaria de la que se puede retirar con tarjeta de débito.

WWW
AAA

por sus hijos. “No se sabe quién hizo los ataques de denegación de servicio que denuncia Delgado. Yo sé que el único profesional de tecnología es él. Yo soy ingeniero civil, trabajo en el Ministerio de Industria (de la Nación) y justamente me anoté en un curso de Office 2010 para poder aprender sobre esta aplicación”, se desentiende Alberto Cámara, padre de Christian.

En la causa, Delgado declara haber sido invitado por el padre de Christian a su domicilio para resolver la situación. “El 7 de julio de 2010, concurrí a casa de los Cámara y vi a Christian sentado frente a una computadora de escritorio instalada en el medio del living conectada a un TV LED de grandes dimensiones, lo que le dio la impresión de que los ataques cibernéticos son la principal actividad de esa familia, impresión que se vio afianzada al enterarse de que José Alberto Cámara asiste a la Facultad de Ingeniería”, figura en el expediente de la causa.

Para Alberto Cámara, sucedió otra cosa. “Él vino a nuestra casa y entró en forma violenta. Hizo todo esto para barrer a la competencia y quedarse con el monopolio de los servidores de juego —argumenta—, porque en ese momento había tres mayoristas y ahora queda él solo.”

En su post que despidió al año 2013 en Facebook, Delgado contó que entre las cosas malas que tuvo que padecer estuvo el cierre de su empresa —en su perfil aparece como CEO de Servilink— aunque podría tratarse de Naiboa Group S.A., una sociedad dedicada a la construcción que lo tiene como director suplente, de acuerdo con la información pública que registra la provincia de Buenos Aires.

El negocio del gaming

Los juegos en red son provistos por los fabricantes globales de videojuegos como Electronic Arts, Nintendo o Activision Blizzard, que crean aventuras online como FIFA World, Super Mario o World WarCraft, entre otros títulos que son consumidos por millones de personas en todo el mundo.

nota de tapa

Desde la década del '90, la modalidad de gaming cambió con la aparición de Internet. Los juegos dejaron de ser para usuarios únicos y se convirtieron en juegos de red. Esta transformación modificó los hábitos de los gamers. “El concepto de audiencia activa, tan controvertido hace dos décadas, se da hoy por sentado en todo el mundo de la industria mediática. Las nuevas tecnologías están permitiendo a los consumidores medios archivar, comentar, apropiarse de los contenidos mediáticos y volver a ponerlos en circulación”, señala Henry Jenkins en su libro “Fans, bloggers y videojuegos: La cultura de la colaboración”.

En la jerga gamer se denomina mayoristas a los usuarios que poseen servidores físicos en un centro de datos y ofrecen servidores virtuales a los jugadores (ver “Empresa en la nube”). “Esto pasa porque las empresas globales instalan servidores en países con mayor número de usuarios que la Argentina, como es el caso de Electronic Arts en Brasil, ya que ofrecen mejor relación cambiaria. Las personas que quieren jugar desde la Argentina lo hacen a un ritmo más lento. Si un gamer le dispara a otro que se mueve más rápido porque tiene mejor acceso al servidor, y cuando llega la bala tiene a su enemigo clavándole un cuchillo por la espalda, seguramente elegirá un servidor local de juegos”, explica Sebastián Di Nardo, socio gerente de la revista de juegos Irrompibles.

A nivel local, esta limitación de la oferta para gamers propició un negocio de baja escala que pudo ser capitalizado por aquellos que vieron una oportunidad para tener su propio emprendimiento. Al cierre de esta edición, el costo mensual de contratar un servidor virtual propio con 500 GB de almacenamiento equipado con procesadores Xeon o Core i7 de Intel, ronda de \$ 1.200 a \$ 1.600 al mes.

Así, las empresas de hosting ofrecen soluciones para los revendedores que operan online. Un plan de \$ 200 al mes les permite ofrecer un servidor virtualizado dentro de uno físico alojado en un centro de datos, contar con hard-



“Era un chico muy entusiasta con las matemáticas y la tecnología”

Eduardo Stamato,
director del Cangallo Schule

ware actualizado periódicamente y, de esa forma, correr los últimos títulos. En cada servidor pueden entrar más de 50 gamers en forma concurrente, con lo cual los mayoristas pueden recaudar ocho veces más de lo que pagan el servicio de hosting.

Fi rHosted, la empresa creada por Christian Cámara, se mantiene operativa, de acuerdo con lo que figura en su sitio web. Su contacto sigue siendo él y hasta el momento del allana-

nota de tapa

Radiografía de la Deep Web

Por Matías Katz, consultor en seguridad informática

Más allá de la Internet que todos conocemos, hay un submundo de contenidos no indexados por los buscadores. Allí se pueden encontrar desde "key loggers" hasta toda clase de drogas.

Usuarios:

Los principales usuarios de esta red son personas de entre 15 y 50 años, que buscan contenido que normalmente no pueden encontrar en Internet, debido a su ilegalidad o por tener un nivel de sensibilidad alto. En la DeepWeb no existe filtrado, por lo que no hay límites éticos ni legales de lo que se puede encontrar.

Cómo llegar a la Internet profunda:

Se puede acceder descargando el navegador Tor (<https://www.torproject.org/index.html.en>). Su instalación es similar a la de un browser normal. Utilizando ese navegador, el usuario va a poder visitar los dominios .onion, el dominio más común en la DeepWeb, ya que está configurado para acceder a la red privada y anónima y llegar a los servidores .onion, que son invisibles a la superficie de Internet.

Actividades más comunes: tráfico de drogas, software malicioso, pornografía

El servicio más común es el de entrega a domicilio de drogas. Se puede comprar cannabis, éxtasis, opios, estimulantes. Para descarga de software ilegal, The pirate bay tiene su propio sitio .onion. Allí se encuentra todo el software de este popular sitio, que están protegidos por la red Tor. Otro contenido muy buscado es el de pornografía infantil. Ya que en esta red no hay filtros, se encuentran sitios que publican fotos de este delito.

Trazabilidad: por qué no se puede encontrar

Para asegurar el anonimato y la falta de trazabilidad, la red Tor separa las comunicaciones en paquetes y envía cada paquete por rutas diferentes, a través de otros usuarios conectados a la red. El tráfico es imposible de rastrear: para llegar a destino una conexión atraviesa al menos 20 países diferentes, en menos de 10 segundos.

Infografía: Javier Furer

miento contrataba su servicio de hosting a dos empresas: iPlan y Dattatec. La primera no quiso hablar para la nota. La segunda es una empresa de Rosario que hoy se llama Don Web. Consultado para hablar del caso, Guillermo Tomatore, CEO de la empresa, prefirió no hablar de los Cámara.

Aunque FireHosted sigue funcionando, la confiscación de las máquinas para realizar las pericias hizo que los Cámara se vieran económicamente afectados. "Esto generó \$ 40.000 de pérdidas para nosotros porque cada cliente pagaba \$ 1.200 para jugar en FireHosted y tuvimos que conseguir otros servidores y comprar nuevo hardware, porque el nuestro lo tiene la policía. Antes había tres mayoristas y ahora sólo queda uno: Pablo Rubén Delgado", se queja Alberto Cámara, padre de Christian. "Dattatec sacó a todos los servidores de juego a partir del allanamiento y ahora solamente usamos su sistema de pagos, porque es muy confiable", agrega Cámara.

Los ingresos que le da FireHosted le permiten a Christian pagar la mensualidad a sus abogados defensores. "Mi papá maneja el tema de los abogados, a los que les pagamos \$ 5.000 por mes. Ellos le pusieron un valor a la defensa y les vamos pagando en cuotas", detalla Christian.

Su padre admite que la cifra es correcta y agrega que los ingresos de Christian hoy no son altos y que les cuesta pagar los gastos derivados de la causa. "También hay que pagarle a los peritos, entonces hay meses en los cuales se va mucho dinero", alega.

Autopsia informática

Como la causa se encuentra en su instancia de indagatoria y los equipos secuestrados en el allanamiento a la familia Cámara están en poder de la división de Delitos Informáticos de la Policía Federal, todavía no se sabe qué pruebas contra los Cámara tendrá la jueza Wilma López, que está a cargo del Juzgado Nacional en lo Criminal de Insrucción N° 11, responsable de la causa, y que ordenó la investigación liderada por la Fiscalía 28.

“Para entender qué pasó hay que analizar los equipos y ver si plantó un ‘key logger’ a través de su servidor y con eso construyó una red de máquinas zombies —analiza Boketero, un ex hacker devenido en desarrollador de tecnología y director de una productora digital que pidió no ser identificado— pero es difícil que haya logrado robar US\$ 50.000 por mes, especialmente en la Argentina, que está muy devaluada.”

“El hacker tenía un servidor. Si lo afecta con su ‘key logger’ para que una persona ingrese a jugar una partida online, con una descarga del archivo y sin que el usuario se dé cuenta, se puede instalar ese código malicioso y registrar lo que se tecléa en la computadora. Si luego el usuario ingresa su tarjeta de crédito y código, podría hacerse del número”, advierte Camilo Gutiérrez Amaya, especialista en Investigación y Concientización de la firma de seguridad Eset en América latina.

Aunque en la comunicación oficial sobre el allanamiento las fuentes de la investigación aseguran haber secuestrado “computadoras con capacidades de cálculo muy superiores a las corrientes”, lo cierto es que en el análisis de pruebas que realiza la policía, los expertos deberán hallar al código malicioso en los servidores secuestrados.

Desarrollar un ‘key logger’ que tome información de las máquinas es tarea para expertos (ver “Cómo se lleva a cabo un fraude bancario”). Pero existen otras formas de obtenerlo. Una de ellas es en el mercado negro de aplicaciones. “Esto es posible desde 2004, cuando la tecnología de botnet y troyanos se expandió. En 2013 se utilizaba uno llamado Zeus, que se vende en foros rusos, y fue uno de los troyanos bancarios más importantes que se autopropaga en forma automática. No estamos hablando de que tiene que ser un súper hacker. Puede ser alguien que pudo haber comprado una tecnología que cuesta US\$ 200 en un sitio ruso como zakepy.ru, que significa hacker en ese idioma”, apunta Christian Russo, un ex hacker que ahora trabaja como consultor de seguridad en su empresa Calcium Sec.

En todo caso, para los expertos entrevistados el tema en cuestión no responde al de una persona con grandes conocimientos de tecnología sino a un principiante. “Parecen acciones

Qué es la Deep Web

Los expertos llaman Deep Web a los sitios que no son accesibles a través de Internet sino mediante el navegador Tor, que oculta los pasos de los navegantes transfiriendo las comunicaciones a través de una docena de países en menos de diez segundos. Eso hace que la posibilidad de rastrear los clicks sea muy remota.

La Deep Web se compone de sitios creados con combinaciones de letras y números que son dadas a conocer por sus creadores a su red de confianza. Estos sitios no son indexados por los buscadores tradicionales como Google, Yahoo o Bing, de Microsoft. “Para poder entrar a los sitios de la Deep Web hay que conocer al dueño del contenido y tiene que invitarte dándote la dirección. Lo que se ve ahí va desde tráfico de drogas hasta software malicioso, pasando por trata de mujeres y sitios de odio a las minorías. Se trata de redes privadas administradas por gente que no quiere ser encontrada pero que necesita darse a conocer en un circuito negro”, explica Christian Russo, ex hacker y director de la consultora Calcium Sec.

típicas de alguien que aprende a meterles un troyano a sus compañeros de colegio o a los miembros despistados de un foro, acciones que en este caso resultan graves porque están organizadas de modo criminal para estafar a los clientes de un servicio”, observa Frankie, un ex hacker que hoy trabaja desarrollando aplicaciones de comercio electrónico.

Un espacio para hallar esta clase de códigos maliciosos se encuentra en lo que los expertos denominan Deep Web. “Es una red similar a la World Wide Web, con servidores y sitios. Sin embargo, existe una gran diferencia: esos servidores no se encuentran directamente conectados a Internet y su contenido no es indexado por los buscadores. No se puede acceder directamente usando un navegador común y corriente, sino que se debe usar un navegador especial. El más conocido es Tor, que se puede descargar libre y gratuitamente desde Internet”, explica Matías Katz, director de Mkit, una consultora en seguridad informática (ver “Qué es la Deep Web”).

Esto no quiere decir que Tor sea una aplicación pirata. Lo que hace es establecer conexiones con equipos de varios países en pocos segundos, para que la comunicación no pueda ser rastreada. “En la Deep Web los sitios tienen dominios .onion y para encontrarlos hay que conocer la extensa combinación exacta de letras y números que lo conforman, y son difíciles de recordar. Allí se maneja información turbia, como tráfico de drogas, armas y pornografía infantil”, revela Gutiérrez Amaya, de Eset Latinoamérica.

Días de escuela

Cuando los datos de Christian Cámara fueron publicados en los foros de gamers, comenzó a recibir llamados y amenazas. Pero lo que realmente cambió la vida de Christian fue su aparición en los medios. “Todos me empezaron a mirar de una forma distinta. Un amigo de la facultad escuchó que el profesor de Programación no iba a aprobarme por lo que supuestamente había hecho”, señala Christian. Consultados sobre este tema por INFORMATION TECHNOLOGY,

nota de tapa

la dirección de la UADE prefirió no responder los requerimientos de esta nota.

Dos semanas después de la televisación del allanamiento, Christian sentía que debía contar su verdad. Por esos días volvió al Cangallo Schule, donde había cursado la escuela primaria y secundaria. “Como ex alumno, siempre fue una persona maravillosa, su familia siempre estuvo presente en la escuela y él particularmente era un chico muy entusiasta con las matemáticas y la tecnología”, recuerda Eduardo Stamato, director del Cangallo Schule, institución que en agosto cumplirá 116 años. Según Alberto Cámara, el rendimiento académico de Christian bajó un poco en la universidad. “En la escuela era muy bueno, pero en la facultad le cuesta un poco más. De hecho, todavía debe rendir el final de Programación porque le fue mal, justo cuando se inició la causa en su contra”, apunta.

Cuando habla de su historia escolar, Christian nombra solamente a tres amigos del colegio: Nazareno, Sebastián y Alejandro. Quizás por eso, en quinto año decidió no viajar a Bariloche. “Preferí quedarme en mi casa descansando”, dice.

El pasado 13 de septiembre, cuando la televisión repetía el allanamiento una y otra vez, los ex compañeros del Cangallo Schule usaron las redes sociales para canalizar su recuerdo sobre Christian. “Siempre dijimos que nos iba a matar a todos algún día... No nos mató pero se la pasó choreando gente. ¡No lo puedo creer!”, escribió @SebaAlbaum en Twitter.

Con algo más de sentido crítico, su compañera @Sofiisola publicó: “Qué loco pensar que un flaco egresado del colegio ahora salga en todos lados como un delincuente”. Un día después, @mavirampa respondió: “@SebaAlbaum Yo lo que no puedo creer es gente del colegio agridándolo en Facebook... Dale, ¿qué te pensás? ¿Qué va a poner algo en fbk?”.

Para Stamato, la aparición de estos comentarios en las redes sociales es parte del juego adolescente que se da en ese ámbito, y que debe

Cómo se lleva a cabo un fraude bancario

Como todo negocio de la era informática, el fraude electrónico es un negocio de escala. “Lo que hace un hacker es plantar un ‘key logger’ en la mayor cantidad de máquinas, para poder explotar el 10 por ciento. Si necesita recaudar US\$ 50.000, lo que deberá hacer es infectar 100.000 máquinas para tratar de conseguir 10.000 dentro de su red botnet, y quitarle US\$ 5 a cada una”, teoriza Matías Katz, director de Mkit, una consultora en seguridad informática. Para el ex hacker Boketero, robar la información de las cuentas requiere un paso adicional al de contar con la información de la cuenta, el usuario y la contraseña. “Muchos bancos operan con tarjeta de coordenadas, y sin esa información no se accede a la cuenta. Además pueden rastrear la IP y, si no la tienen registrada, piden al usuario un código que el banco envía por email o SMS, lo que hace más difícil sacar dinero de la cuenta”, justifica.



“Un hacker es un delincuente, y eso son los que armaron esta causa. Yo no soy un hacker”

Christian Cámara

ser entendido en su contexto. “Quizás puedan verlo como alguien distinto a ellos, y creo que en las redes sociales pusieron cosas que no dirían si lo tuvieran enfrente. Cuando Christian terminó cuarto año, hizo un gran trabajo de apertura y contó qué cosas lo hacían sentir mal y eso hizo que su grupo se uniera más. Al año siguiente, durante la entrega de diplomas, todos lo aplaudieron cuando subió a recibirlo”, cuenta el director de la escuela. Christian Cámara evita hablar sobre lo que decían sus ex compañeros en las redes sociales, aunque sabe lo que se afirma sobre él. Cuando enfoca su mirada para responder, se queda en silencio y revive internamente las escenas del día de la televisación del allanamiento en su casa. Otra vez tiene un déjà vu: las cosas volvieron a ser difíciles, como cuando estaba en el colegio. ■