Más bueno que un hacker

Por: FACUNDO IGLESIA. 04/07/2021

En nuestra existencia digital no hacemos otra cosa que ingresar usuarios y contraseñas alfanuméricas, responder preguntas de seguridad, confiados en que todas esas galerías infinitas de bytes son invulnerables. Pero algunas comunidades con conocimientos informáticos piensan lo contrario: desconfían de todo y meten mano para probarlo. Cuatro casos ocurridos recientemente en la Argentina revelan la fragilidad del sistema y cómo son los hackers quienes pagan las consecuencias por denunciarlo.

“Rodrigo, ayudame, un amigo acaba de hackear un banco”, ruega Iván Barrera Oro en octubre de 2019 al abogado Rodrigo Iglesias, habitual defensor de la comunidad hacker. El amigo es Ariel Ortmann (AO), líder de proyectos de Despegar.com, de 26 años entonces.

Un año antes, AO detecta en el Home Banking del Banco Nación (BN) ciertos números que no deberían ser visibles. Agudiza la mirada y verifica que se puede hacer clic derecho, luego “Inspeccionar elemento”, cambiar la cotización al valor deseado, tocar “Comprar” y listo. Incrédulo, contacta por todas las redes sociales a Red Link, la empresa proveedora de la seguridad del banco. Luego de que le respondan por Twitter, lo llama el Gerente de Seguridad Informática: “No vuelvas a hacer pruebas de seguridad porque vamos a tomar acciones legales”. Minutos más tarde, el gerente llama al jefe de AO en Despegar.com para pedir que lo echen.

En septiembre de 2019, ante una frenética subida del dólar tras las PASO, que lo hizo saltar de 46 a 57 pesos, el macrismo aplicó una herramienta que siempre defenestró: un cepo cambiario de hasta 10.000 dólares mensuales. En ese momento un compañero de trabajo le preguntó sobre la vulnerabilidad de la que le había hablado alguna vez. AO probó de nuevo, confiado en que ya lo habrían corregido y se quedó mudo frente a la pantalla: cambió el valor del dólar de 56,95 pesos a 5,695 pesos. Acto seguido, compró y lo vendió a 530,50 pesos. En segundos, obtuvo una ganancia de 667.243,80 pesos.

Días después, el entonces titular del Banco Central, Guido Sandleris, publicó la lista de los que se saltaron el cepo y allí figuraba su nombre.

AO presentó espontáneamente a su sucursal del BN un escrito en el que detallaba lo que había detectado. Lo hicieron pasar, lo escucharon atónitos, se lo sellaron y le recomendaron que se buscara un abogado. Él hizo caso.

La denuncia del BN recayó en el fuero penal federal y en primera instancia fue tomada por Claudio Bonadío. Luego de su fallecimiento quedó en manos de Marcelo Martínez de Giorgi. Tras más de un año de incertidumbre, el abogado Rodrigo Iglesias lo llamó: “Ganamos”. La resolución firmada por el juez federal es clara: “La intención no estaba dirigida a causar un perjuicio patrimonial a las arcas del Banco de la Nación Argentina sino a probar las debilidades del sistema informático”.

AO forma parte de una comunidad dispersa que se obstina en descubrir la fragilidad de los sistemas informáticos en los que descansan resortes fundamentales de nuestra democracia. Se los denomina “hackers éticos” o “hackers de sombrero blanco”. Su función es demostrar que con unos pocos clics es posible modificar el precio del dólar, alterar resultados de elecciones, descargar información sobre agentes policiales encubiertos y obtener decenas de miles de números de tarjetas de crédito resguardados por una concesionaria de peaje.

No son teorías conspirativas, son historias que ya ocurrieron en la Argentina.ariel ortmann probó de nuevo, confiado en que ya lo habrían corregido y se quedó mudo frente a la pantalla: con un par de clics cambió el valor del dólar de 56,95 pesos a 5.695 pesos. acto seguido, compró y lo vendió a 530,50 pesos. en segundos, obtuvo una ganancia de 667.243,80 pesos.

barreras bajas

Adrián Ruiz (AR) es cordobés, hace veinte años que trabaja en sistemas y está convencido de que no hackeó a nadie: “Usé dos herramientas: la tecla borrar y la tecla enter”. Está en su naturaleza reportar errores en sitios web, pero no le hicieron falta esos conocimientos para acceder a 20 GB de información sensible que cualquiera podría haber descargado.

En junio de 2020 entra al portal de telepeaje para revisar una factura en el sistema

de Camino de las Sierras, concesionaria de once casillas de peajes en la red de acceso a Córdoba. Desde 2017 la empresa implementa un sistema de “peaje dinámico” que lee la patente del auto, está adherido al débito automático y promete, como suele ocurrir, “velocidad” para el automovilista apurado. Como no encuentra la factura, Ruiz borra parte de la dirección en la barra del navegador creyendo que eso lo llevaría a una página anterior. No fue así: ante sus ojos se abre un directorio cargado de archivos de texto crudo sin encriptar. Son los datos de 54.000 usuarios, incluidos los suyos: nombre, teléfono, modelo de auto, fecha y hora en los que pasó por cada peaje y número de tarjeta de crédito (aunque sin los códigos de seguridad del reverso). “Era peligroso porque podés saber sus movimientos, a qué hora está la casa deshabitada, podés hacer una segmentación y saber quiénes tienen tarjetas premium y autos de alta gama. Con el número de teléfono, podés hacer secuestros virtuales”, advierte AR a ***crisis***.

Preocupado, envía mails, llama, se comunica por redes sociales, pero no obtiene respuesta. Cuatro meses más tarde, vuelve a ingresar al sistema y comprueba que el error sigue allí. Se comunica con la empresa una vez más y nada. Decide ir a la prensa y, frente la incredulidad general, les muestra la información de los propios periodistas y dueños de los medios en los que declara.

Recién allí lo llaman desde Caminos de las Sierras. Lo primero que hacen las diez personas que lo rodean es ofrecerle todo tipo de explicaciones y disculpas. “Yo soy un usuario y quiero que borren mis datos, nada más”, los corta. Le llevan una computadora y les demuestra la vulnerabilidad. Alguien se levanta y vuelve a los cinco minutos: “Probá ahora”. AR pulsa F5 y la información no está más.

Dos semanas después el fiscal Franco Pilnik, de la Fiscalía Especializada en Cibercrimen de Córdoba, ordena un allanamiento en su casa tras una denuncia de Caminos de las Sierras. “La prueba incorporada indicaba que el denunciado, además de reportar la vulnerabilidad, presuntamente habría descargado la base de datos”, afirma Pilnik a ***crisis***. Durante siete horas, peritos informáticos de la Policía de Córdoba revisan todos los dispositivos de Adrián y su familia, incluyendo las conversaciones de Facebook y WhatsApp, mientras él y sus hijos se quedan encerrados en una habitación.

Pero no es el final: meses después de su paso por los medios, varias personas se comunican con él para contarle sobre otras fallas de seguridad. La más grave: alguien le envía por Twitter una captura del sistema interno que usan los

trabajadores de la empresa, indicando una penetración que vuelve a poner la información de los automovilistas en peligro. AR se lo envía al Gerente en Sistemas, que le confirma que efectivamente son usuarios y claves internas. Ante la consulta de ***crisis***, la "respuesta oficial" fue sucinta: "Caminos de las Sierras garantiza a sus usuarios la seguridad de los datos brindados y oportunamente se hizo una denuncia en la Justicia".

Mientras tanto, la investigación contra AR sigue en curso.

seguí leyendo el nuevo número de crisis: *pedilo acá*

vot.ar mal

Ciudad de Buenos Aires, 2015, año electoral. Macri necesita que Horacio Rodríguez Larreta lo releve en la jefatura de gobierno para que su carrera a la Rosada no se termine en la línea de largada. No será el único reemplazo: ahora, en lugar de meter una boleta de papel en una urna, los electores pulsarán sobre sus candidatos en la pantalla táctil de una computadora (llamada Vot.ar) que imprimirá una boleta con un chip de Identificación de Radiofrecuencia (RFID, por sus siglas en inglés) y las autoridades de mesa escanearán y transmitirán a un centro de cómputos. El nombre es poco original: Boleta Única Electrónica (BUE).

El sistema está a cargo del Grupo Magic Software Argentina (MSA), nacido en 1995 como vendedora en Argentina de la empresa israelí Magic Software Enterprises. El sistema Vot.ar ya se usó en elecciones en Salta, Chaco y Santa Fe. Por la instalación y el mantenimiento de más de 9000 máquinas en 7377 mesas, cobrarán esta vez algo más de 218 millones de pesos (25,4 millones de dólares de la época).

La Fundación Vía Libre y otros investigadores informáticos independientes se oponen a la implementación. Pero el gobierno de CABA insiste. La Defensoría del Pueblo da explicaciones calcadas a los eslogans de Sergio Angelini, CEO de MSA: la máquina que se usa para votar "no es una computadora, es una impresora", por lo tanto no puede grabar a qué candidato se vota. Pero una misteriosa cuenta de Twitter llamada @fraudevotar comienza a filtrar datos de MSA a cuentagotas: código fuente, manuales y videos para los técnicos que estarán en los centros de cómputos. Es el comienzo de una catarata.

Joaquín Sorianello (JS) tiene 27 años, es cantante, guitarrista, programador y

fundamentalmente un *nerd*. Nada le da más placer que encontrarles fallas a los sistemas informáticos. Cuando la BUE amenaza con instalarse en CABA, donde vive y donde además votará por primera vez, ese juego se convierte en obsesión. Se suma a una investigación colectiva y, con los datos difundidos por la cuenta @fraudevotar, descubren que el sistema es endeble. Las contraseñas de los técnicos, por ejemplo, son sus direcciones de email.

Faltan diez días para las elecciones y desde algún lugar del mundo la cuenta @fraudevotar da el paso definitivo: muestra las credenciales SSL, es decir, las llaves para entrar al sistema de transmisión desde las escuelas a los centros de cómputos, sin necesidad de una contraseña. Desde su Mac, JS ingresa las credenciales filtradas y el sistema se le abre por completo. Tuitea: “No puedo creer lo que estoy viendo”.

Como cualquier otro usuario con esas credenciales, ahora públicas, JS es capaz de derribar el sistema de recuento rápido e incluso de inventar resultados. Esa certeza lo asusta, por lo que llama a un amigo que trabaja en MSA. Luego acude a la prensa. Horas más tarde escucha en Radio Nacional: “Un experto en seguridad informática denuncia vulnerabilidades en el sistema de voto electrónico”.

JS no reveló su identidad, pero tampoco cuidó su privacidad online. La primera señal llega en forma de mensaje directo desde la cuenta @fraudevotar: “Sabemos dónde vivís”. Para descomprimir la paranoia, se toma un avión a su Bariloche natal. A los pocos días, mientras cena con su familia, recibe una llamada: “Policía Metropolitana. Estamos en la puerta de su departamento. Ábranos o la tiramos abajo”. “Es una cama”, piensa y llama al 911 para chequearlo. Se lo confirman: tiene que abrir la puerta o la derriban. JS llama a su novia para que les lleve la llave y los policías recurren a un cerrajero. Finalmente, su novia logra abrirles y los agentes se llevan cuatro computadoras, incluso el Kindle.

El allanamiento fue ordenado por la jueza María Luisa Escrich en el marco de una denuncia que MSA le hace a JS por “daño informático”. El procedimiento causa una paranoia inédita en la comunidad informática. “Hubo gente que rompió discos y algunos se fueron en barco al medio del río. Era la primera vez que pasaba algo así”, recuerda el abogado Rodrigo Iglesias.

El 6 de agosto de 2016, JS es sobreseído. En el medio del proceso, una inmensa campaña de donación le permite comprar equipos nuevos. En el fallo firmado por el

fiscal Norberto Brotto, se admite que solo quiso alertar que el sistema de seguridad “era vago y podía ser vulnerado con facilidad”.

Pero JS es apenas un miembro de una comunidad mayor. Javier Smaldone es riocuartense, experto en seguridad informática. Meses antes de las elecciones demuestra que cualquier celular puede leer el chip RFID, lo que facilitaría la compra de votos. Después, Iván Barrera Oro desarrolla un *zapper*: un aparatito para quemar los chips que se puede ocultar en un paquete de cigarrillos e invalidar una elección sin que haga falta un visible incendio de urnas. Un año después, a Iván lo acusan de “producción y distribución de pornografía infantil”, causa de la que fue sobreseído.

Otro de ellos, Alfredo Ortega, encuentra el *bug* de multivoto, es decir, un mecanismo que puede cargar múltiples sufragios en una boleta. Para colmo queda demostrada la falacia contenida en “no es computadora, es una impresora” cuando Smaldone hace correr YouTube en una de ellas. Por si fuera poco, en la pericial informática contra JS se constata que también hubo un acceso indebido de una IP de otro imputado que prefiere mantener su anonimato. Desde allí se crearon establecimientos y votos, se cambiaron de lugar las escuelas y se modificó el sistema de contabilidad.

Varios de ellos exponen en los medios y en el Congreso contra la BUE, en 2016, cuando un Macri ya presidente intenta implementarla a nivel nacional. La reforma política de Cambiemos naufraga en buena medida por esas presentaciones y muchos están convencidos de que algunos extraños sucesos posteriores fueron la represalia.el procedimiento causa una paranoia inédita en la comunidad informática. “hubo gente que rompió discos y algunos se fueron en barco al medio del río. era la primera vez que pasaba algo así”, recuerda el abogado rodrigo iglesias.

gorraleaks

Patricia Bullrich está en un acto de ascensos de las fuerzas de seguridad junto al presidente Macri. Su Twitter dispara: “Hago de manera oficial mi renuncia como ministra de seguridad”; “Soy una borracha inútil que le queda grande el cargo igual que a @mauriciomacri el cargo de presidente”; “Macri gato”.

La respuesta no se hace esperar: entre el 17 de febrero y el 27 de abril la Policía Federal detiene a Mirco Milski, Martín Horacio Trabucco y a Emanuel Vélez Cheratto. “En Argentina no hay delito sin sanción”, twitea, esta vez sí, la ministra de

Seguridad. En simultáneo comienzan a brotar en la red capturas de la bandeja de entrada de denuncias@minseg.gov.ar, el correo oficial de la Policía Federal Argentina.

Poco después Javier Smaldone, el riocuartense que colaboró en desenmascarar el voto electrónico en la CABA, twitea sobre las detenciones y recibe un email de alguien que se hace llamar “S” con un archivo *zip*. Cuando lo abre encuentra 70 megas de PDFs, planillas Excel, audios y archivos Word con informes de seguimiento de la policía, nombres de narcotraficantes investigados y de policías infiltrados en las bandas.

Smaldone hace una copia y la presenta ante el juez federal Sebastián Ramos. En el cierre de su declaración, advierte: “Me preocupa la posibilidad de que las cuentas de correo sensibles de las fuerzas de seguridad puedan ser fácilmente accesibles y que la respuesta oficial de los funcionarios sea negar la situación. Tienen detenidas a dos personas que no tienen nada que ver y el que fue está libre”.

El 27 de mayo de 2017 los archivos aparecen en un repositorio público de GitHub con el nombre de “Gorraleaks”. Exactamente un mes antes, cuando los archivos ya daban vueltas por la Deep Web, mataron a Alan Maximiliano Dolz, agente encubierto de la Policía Federal de 21 años. Cuatro atacantes lo emboscaron en Villa Loyola, en San Martín. Algunos miembros de la comunidad informática se preguntan todavía si ese asesinato habrá tenido que ver con la filtración.

La investigación sobre el hackeo a Bullrich se cierra con Mirco Milski y Emanuel Vélez Cheratto procesados y la apertura de una causa para investigar la filtración de Gorraleaks. Sin embargo, en agosto de 2019 hay una revelación informática todavía más grande: 700 GB de archivos de la policía (actas de allanamiento, declaraciones de testigos, expedientes, información de movimientos de drogas, escuchas) son filtrados en Twitter, Telegram y en la Deep Web.

Smaldone twitea aconsejando a los usuarios no descargar la información y teorizando sobre cómo podría haber sucedido el ataque. Pero la policía ya decidió quiénes serán los culpables. El 10 de octubre Smaldone duerme en la casa de su novia en la CABA cuando tocan la puerta. Por la mirilla observa seis gorras azules con las letras “PFA”. Luego de seis horas de allanamiento le comunican que debe acompañarlos. Lo suben a un móvil, lo esposan y lo mantienen con custodia durante otras seis horas. En el operativo la policía se lleva veintitrés dispositivos.

En el expediente consta que un agente principal de la Federal fue enviado a seguir a Smaldone a Córdoba, Río Cuarto y finalmente a la CABA. En Río Cuarto, su ciudad de residencia, pusieron una cámara de seguridad frente a la casa de sus hijos y en Capital instalaron otra frente al domicilio de una persona vagamente parecida a él. Además, hicieron ciberpatrullaje en su Twitter y trazaron su perfil de “experto en programación, opositor al gobierno y al voto electrónico”.

¿Cómo sucedieron los ataques? Según lo señala Sebastián Davidovsky en su libro *Engaños digitales, víctimas reales*, el hackeo a Patricia Bullrich se dio cuando le llegó un mail haciéndose pasar por el embajador boliviano y pidiéndole explicaciones sobre declaraciones xenófobas que había dado hacía unos días. Ese correo la redirigió a una página que le pidió los datos de su correo electrónico y ella ingresó.

Por otro lado, el atacante de la Federal usó como puerta de entrada una vulnerabilidad en el servidor de la Superintendencia de Bienestar de la fuerza: la versión de PHP (un lenguaje de *scripting* para la programación web) del webmail durante las penetraciones de 2017 y 2019 era la 5.6.3 (del 2014), es decir, vieja. No se actualizó ni siquiera tras el primer Gorraleaks, pese a que el juez Ramos ordenó en mayo de 2017 al jefe de la Federal de entonces, Néstor Roncaglia, que adoptara “las máximas medidas de seguridad posibles para resguardar la información sensible”.

¿La seguridad del Ministerio y de la Policía Federal mejoró desde ese momento? No parece. A menos de 24 horas de asumir en 2019, la cuenta de Twitter de la ministra de Seguridad Sabina Frederic publica: “Encontramos cajas de vino en la oficina de Bullrich, las vamos a sortear a nuestros seguidores”.en agosto de 2019 hay una revelación informática todavía más grande: 700 gb de archivos de la policía (actas de allanamiento, declaraciones de testigos, expedientes, información de movimientos de drogas, escuchas) son fi ltrados en twitter, telegram y en la deep

web.

resetear la república

Seis años después del allanamiento, Joaquín Sorianello admite a ***crisis*** que sufre de estrés postraumático: “Hoy no participo tanto de la comunidad, estoy más guardado, ya no soy extrovertido como antes”. También extremó su seguridad informática tras casarse y tener hijos.

Javier Smaldone sigue activo en la comunidad informática y en Twitter, donde comparte detalles de la investigación en su contra por el Gorraleaks. Hace poco cambió de estrategia legal: como todavía no lo imputaron, pidió que lo hicieran “así me puedo defender”.

Adrián Ruiz no buscó abogado porque está convencido de que la Justicia no avanzará. “Yo no soy un hacker”, aclara a ***crisis***.

Ariel Ortmann no volverá a reportar vulnerabilidades en sitios estatales argentinos, porque “uno actúa para que robustezcan sus sistemas y la termina pasando mal. Pero hace poco encontré un error en una plataforma internacional y usé su sistema para reportarlo. Me respondieron en el día con la mejor onda y me premiaron”.

Muchos *hackers buenos* se dejan llevar por la curiosidad a pesar del peligro y siguen señalando fallas. A veces con ánimos de corregir el sistema. Y otras para exponer sus engranajes y exigir un reseteo total.

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografía: PANCHOPEPE

Fecha de creación
2021/07/04