Informe

Alerta sanitaria

El sector de la asistencia sanitaria en el punto de mira de la ciberdelincuencia

intel Security

Índice

En la investigación
y redacción de este
informe han participado:

Advanced Programs Group
Christiaan Beek
Charles McFarland
Raj Samani

Introducción

Todos conocemos la naturaleza imperecedera de los datos médicos. Ya sean nuestras historias médicas o la propiedad intelectual del próximo fármaco milagroso, una vez que los ciberdelincuentes se apoderan de este tipo de datos, no resulta fácil recuperarlos. ¿Por qué se roban los datos médicos? ¿Son realmente el objetivo de los ataques o simplemente daños colaterales? Si son el objetivo, significa que hay demanda; y si hay demanda, es porque son rentables. ¿Cuál es la situación?

Este informe trata sobre el robo de datos en el sector de la asistencia sanitaria. Concretamente, describiremos el mercado de los datos sanitarios robados y examinaremos las motivaciones de los ladrones.

En el informe de McAfee Labs *El comercio clandestino de datos*, analizábamos las fugas de datos relacionadas con el robo de información financiera, y concretamente la información de tarjetas de pago. En ese informe, no encontramos datos médicos a la venta. Aunque sabíamos que los robos de datos médicos eran una realidad, no los habíamos detectado en los mercados clandestinos. Tras llevar a cabo una investigación más profunda, podemos exponer nuestras conclusiones.

—Raj Samani, CTO de Intel Security para Europa, Oriente Medio y África

@Raj_Samani
@McAfee_Labs

Ocultos a plena vista

El informe *El comercio clandestino de datos* desveló que existe un mercado de datos robados, y que el negocio va viento en popa. Efectivamente, el aumento de empresas atacadas y de datos robados ha provocado una caída tan pronunciada de los precios de dichos datos que nos preguntamos cuándo tocará fondo. De hecho, el gran volumen de datos de tarjetas de pago ha dado lugar a la aparición de atractivos modelos de negocio en un intento de los vendedores por atraer compradores.

Lo sorprendente de nuestra investigación fue la sospechosa ausencia de datos médicos entre la multitud de datos robados que había a la venta. No es que buscáramos específicamente este tipo de datos, pero suponíamos que los íbamos a encontrar, ya que sabemos que efectivamente se están robando. El hecho de que no halláramos datos médicos en el mercado fue lo que nos llevó a realizar esta investigación.

En lugar de limitarnos a conseguir capturas de pantalla de datos médicos personales robados en venta (suponiendo que pudiéramos encontrarlos), decidimos ir más allá e identificar qué otros afectados hay en el sector de la asistencia sanitaria. Por ejemplo, ¿reciben ataques las empresas farmacéuticas?

En febrero, publicamos el blog "Ransomware Targets Health Care Sector" (El ransomware se dirige al sector sanitario), en el que analizábamos un incidente de ransomware contra un hospital de EE. UU. En el blog se afirma que en la actualidad los ciberdelincuentes centran sus ataques de ransomware en las empresas (frente al enfoque más disperso del pasado) y, en concreto, en el sector sanitario. Por lo tanto, aunque este informe analiza únicamente los datos médicos robados que se ponen a la venta, las empresas del sector sanitario han sufrido otros tipos de ataques.

Antes de entrar en detalle en los resultados de nuestra investigación, queremos dejar algo bien claro: no pretendemos en absoluto generar miedo. Nuestra única intención es documentar el panorama de amenazas para que las empresas relacionadas con el sector sanitario tomen las medidas oportunas. Y es imprescindible que lo hagan, ya que, a diferencia del caso de las tarjetas de pago, las historias clínicas sencillamente no se pueden cambiar. Sin duda, esta naturaleza imperecedera les confiere un valor especial. Por lo tanto, visto que la capacidad para reducir el impacto de una fuga de datos médicos es mínima, debemos hacer todo lo que esté en nuestras manos para reducir la probabilidad de que los ataques consigan su objetivo. El primer paso en este proceso pasa por comprender la amenaza.

¿Existe un mercado de datos médicos?

Lo primero que debemos determinar es si realmente hay datos médicos robados a la venta. Partimos de la premisa de que en nuestra investigación anterior sencillamente no buscamos en los lugares adecuados. Ahora sabemos que estábamos en lo cierto. No tardamos mucho en descubrir a proveedores de la Internet profunda que ofrecían enormes cantidades de datos médicos robados a cambio de dinero. En algunos casos, la venta se había publicitado ampliamente. La Figura 1 muestra cómo se puso a la venta una base de datos con datos médicos personales de 397 000 pacientes. En la Figura 2 el vendedor detalla el contenido del volcado de datos.

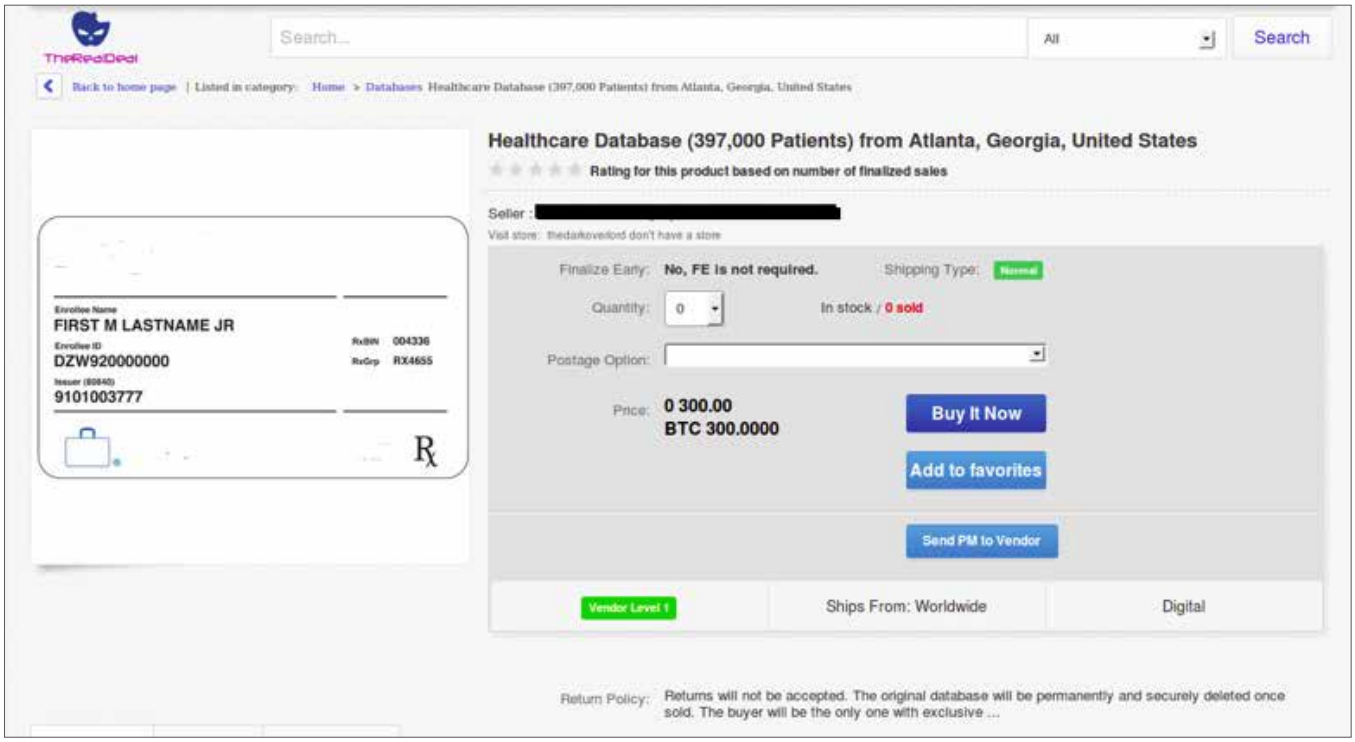


Figura 1: Una base de datos sanitarios a la venta.

Figura 2: Campos de datos de un volcado de datos sanitarios.

En el ejemplo anterior, no solo se incluían los nombres y direcciones de los pacientes, sino también datos sobre sus aseguradoras, además de otra información que puede ser de interés para posibles compradores. El valor de dichos registros es extraordinario; en comparación con otros volcados de datos, el precio de los datos médicos es considerablemente mayor. Ofrecemos detalles más adelante en este informe.

Hay multitud de volcados de datos que podemos analizar. La Figura 3 contiene una oferta de venta de datos médicos robados de una empresa de servicios sanitarios ubicada en Farmington, Missouri. Esta oferta procede del mismo vendedor que aparece en las Figuras 1 y 2.

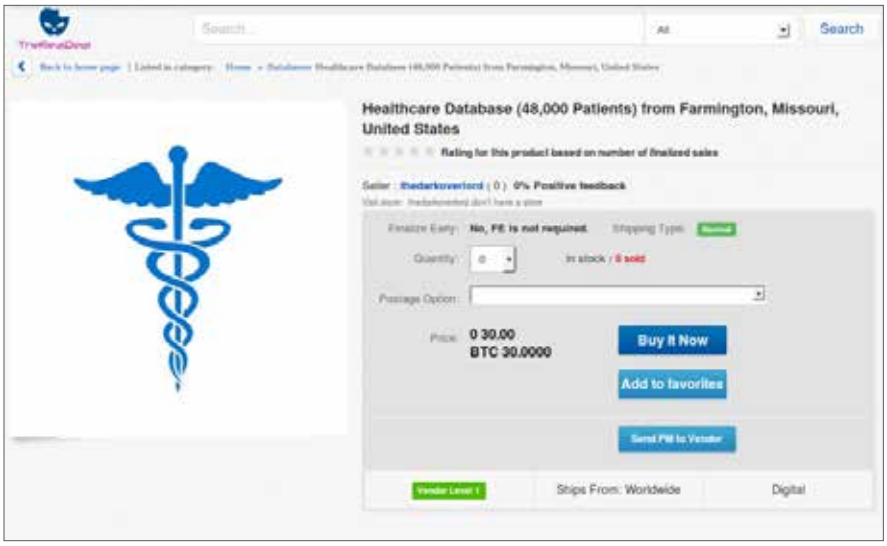


Figura 3: Detalles de un segundo ataque.

Pero la cosa no queda ahí; este vendedor ofrece una tercera base de datos de historias clínicas personales sustraída a otra empresa de servicios sanitarios, como se muestra en la Figura 4.

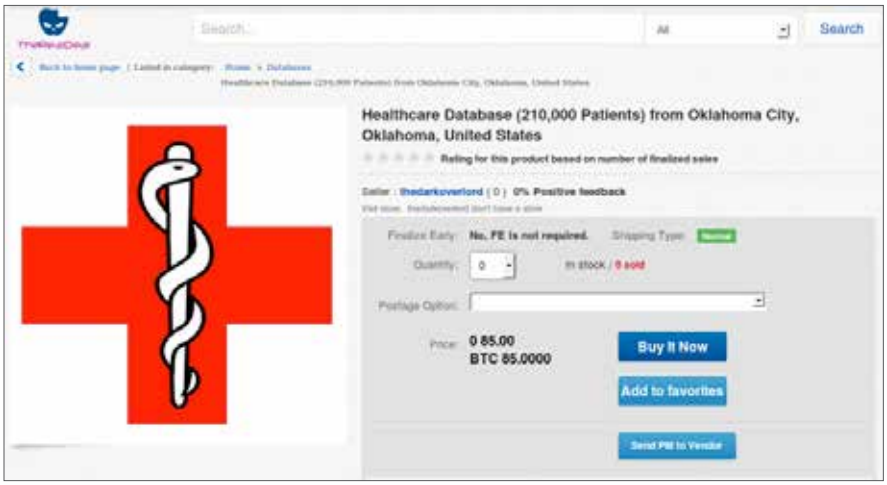


Figura 4: Detalles de un tercer ataque.

Puede que se pregunte por qué dejamos claro que el vendedor robó los datos. Descubrimos que proporcionó pruebas del acceso a las empresas atacadas. En una entrevista a Deepdotweb.com, se incluyeron una serie de capturas de pantalla, una de las cuales se muestra en la Figura 5.

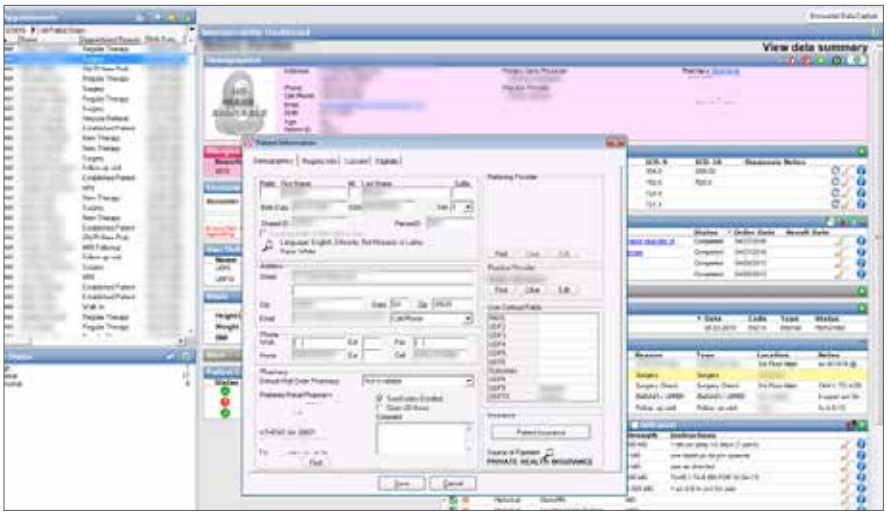


Figura 5: Datos de una empresa de servicios sanitarios atacada.

Todo indica que el vendedor aprovechó una vulnerabilidad en el protocolo de escritorio remoto para llevar a cabo el ataque.

El robo de datos médicos es solo parte de la historia. Aunque en las películas parece que para ser hacker basta con pasar unos minutos tecleando caracteres aleatorios, la realidad es bien distinta, ya que la actividad requiere mucho más tiempo y esfuerzo. Además, los ciberdelincuentes piensan en términos de rentabilidad. Para este vendedor, la posibilidad de rentabilizar la inversión en cuanto a tiempo (y posiblemente a herramientas necesarias) es probablemente la principal motivación. Según una entrevista concedida por este vendedor a Motherboard, parece que esta persona sacó buen provecho del tiempo invertido. En ella afirma: "Alguien quería comprar específicamente todas las historias clínicas [de la aseguradora]". Además, añadió que, por el momento, el esfuerzo le había reportado 100 000 dólares.

Este episodio sugiere dos cosas. En primer lugar, efectivamente los datos médicos se venden (tal y como esperábamos) y, en segundo lugar, existe demanda de esos datos. Esta conclusión no se basa en un solo vendedor. No tuvimos que ir demasiado lejos para encontrar más pruebas.

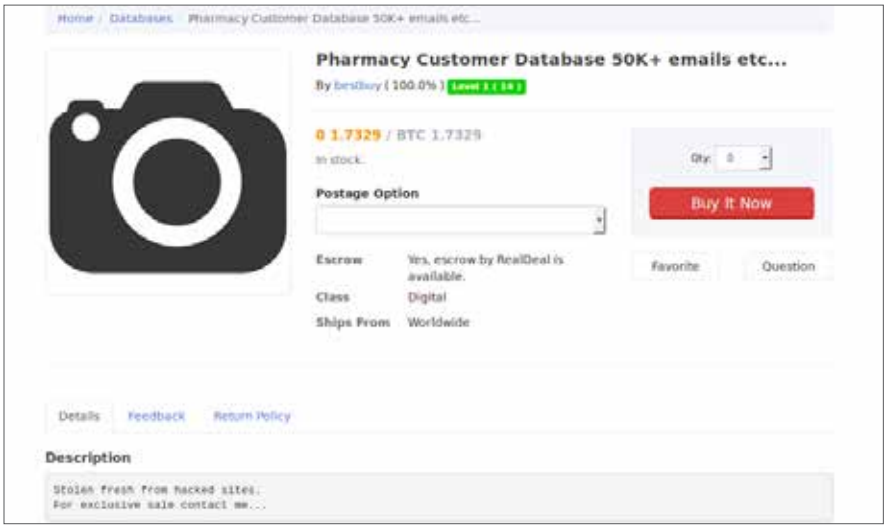


Figura 6: Más datos a la venta.

El vendedor del volcado de datos anterior no es el mismo que el de los ejemplos precedentes, aunque la oferta se encuentra en el mismo mercado. Todo indica que está activo, ya que cuenta con un 100 % de opiniones positivas de 15 interacciones hasta la fecha. La reseña más reciente deja claro que las opiniones positivas se refieren a su actividad como vendedor.

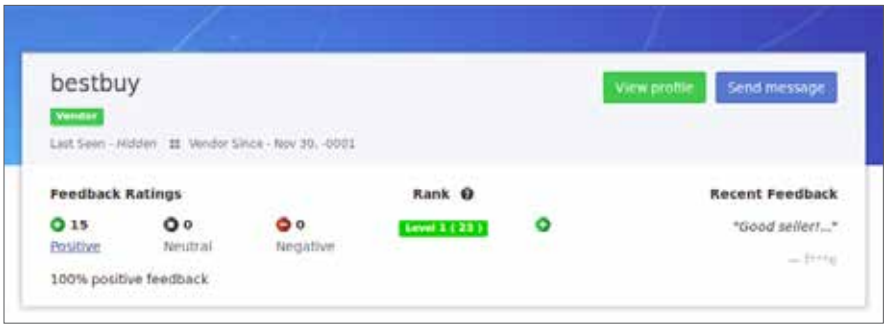


Figura 7: Comentarios positivos sobre este vendedor.

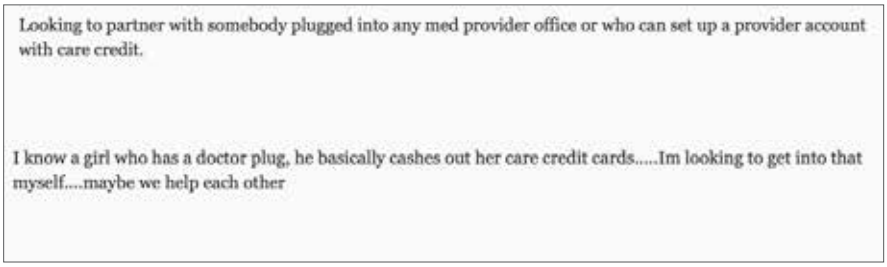
Podemos concluir que en la actualidad se roban y se venden datos en el sector de la asistencia sanitaria. Y no solo se venden, sino que se publicitan abiertamente. En determinados casos, el vendedor incluso alardea del ataque en las redes sociales.

En el momento de la redacción del presente documento, la cuenta en Twitter del usuario anterior ya no estaba activa. Sin embargo, hay informes que indican que la persona (o personas) detrás de la cuenta ha aparecido de nuevo, con un volcado de datos de otra empresa de servicios sanitarios que ha sido atacada. O puede que se trate de un imitador. A mediados de septiembre nos enteramos de que otra empresa de servicios sanitarios estaba siendo extorsionada bajo la amenaza de hacer públicas historias clínicas robadas. Todo indica que este vendedor se comunica en primer lugar con una empresa afectada, y luego la amenaza con publicar datos médicos robados a menos que pague una cantidad de dinero.

Sabemos por otras fuentes que hay muchos ejemplos de datos médicos robados a empresas de servicios sanitarios que están a la venta. No cabe duda de que existe un mercado de datos médicos robados.

El colaborador interno

En algunos foros de la Internet profunda encontramos pruebas de que los ciberdelincuentes buscan a personas con información privilegiada dentro de empresas de servicios sanitarios. En el siguiente ejemplo, mostramos cómo se busca personal interno para crear una cuenta con CareCredit, una empresa de tarjetas de crédito que financia servicios sanitarios. En este caso no se trata estrictamente de datos médicos; este ejemplo se parece más a los fraudes relacionados con las tarjetas de pago que analizamos en nuestro informe *El comercio clandestino de datos.*


Looking to partner with somebody plugged into any med provider office or who can set up a provider account with care credit.

I know a girl who has a doctor plug, he basically cashes out her care credit cards.....Im looking to get into that myself....maybe we help each other

¿Valen más los datos médicos?

Al igual que ocurre con la información de tarjetas de pago, para los datos financieros ya existen mercados consolidados. El precio actual de un solo registro de información "fullz" —paquetes completos de información de identificación personal de individuos, con nombres, números de identificación, fechas de nacimiento y números de cuenta— es de 14 a 25 dólares. Los vendedores menos consolidados tienen precios de lanzamiento bajos; recientemente hemos visto precios en torno a los 20 dólares por registro para compras a pequeña escala. Los precios al por mayor pueden ser incluso más bajos: hasta 3 dólares por tarjeta. Por otro lado, el precio de las historias clínicas parece variar enormemente; desde una fracción de céntimo a 2,42 dólares por unidad. Este precio es significativamente inferior al de las tarjetas de pago individuales, pero no lo es tanto cuando se compara con la venta de dichas tarjetas al por mayor.

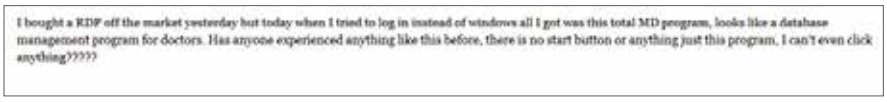
¿Significan estos precios que los datos médicos no valen tanto como los financieros? Es posible, pero es que los mercados son distintos. Algunos vendedores aprovechan mercados paralelos para aumentar sus beneficios. En el foro del mercado clandestino AlphaBay, el usuario Oldgollum vendió 40 000 historias clínicas por 500 dólares, pero eliminó específicamente los datos financieros, que se vendieron por separado. Lo que hace Oldgollum es diversificar para obtener el máximo rendimiento de ambos mercados. Los datos financieros también se pueden vender como registros individuales o en grandes cantidades. Sin embargo, parece que actualmente los datos médicos solo se venden en grandes cantidades, lo que reduce el precio por historia a una cantidad similar al de las tarjetas vendidas al por mayor. Sin duda los datos médicos aumentan el valor de la transacción. El objetivo de los vendedores es sacar el máximo beneficio de ambos mercados, y no confían en vender a un precio alto en los dos.

Los datos financieros no son el único tipo de información que podemos utilizar para comparar la dinámica del mercado. Tomemos por ejemplo dos recientes volcados de cuentas de redes sociales. Los dos venden al por mayor entre 65 y 167 millones de cuentas, pero generan un beneficio muy pequeño por registro vendido. Incluso tras fugas más recientes relacionadas con foros de Bitcoin se ofrecen precios similares por registro. Respecto a los datos médicos, hemos descubierto que la cantidad es algo mayor, pero todavía no se venden al precio de mercados consolidados como el de las tarjetas de pago. El mercado de datos médicos robados parece estar aún tomando forma, pero en el ecosistema actual ya se ofrece un valor por historia superior al de los mercados de datos de cuentas no financieras. ¿Valen más los datos médicos? Parece que su valor oscila entre los volcados de bases de datos tradicionales y los datos de tarjetas de pago. Si los datos médicos contienen información financiera, su venta por separado parece ser más rentable que de manera conjunta.

Ciberdelincuencia como servicio en el sector de la asistencia sanitaria

Cuando McAfee Labs publicó el informe *Cybercrime Exposed* (Análisis de la ciberdelincuencia), el concepto de ciberdelincuencia como servicio estaba relativamente en ciernes. No se tenía constancia de que los componentes de un ciberataques pudieran subcontratarse. En la actualidad ya se sabe, y la ciberdelincuencia como servicio es un modelo de negocio bien conocido. Este modelo de negocio se aplica de igual forma al sector de la asistencia sanitaria.

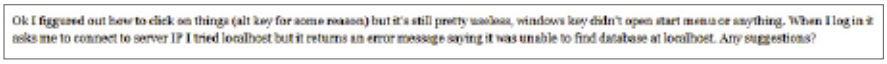
Hoy día observamos cómo la ciberdelincuencia como servicio se emplea en el sector de la asistencia sanitaria, y tenemos la certeza de que las vulnerabilidades se venden y que los ataques como servicio dirigidos a empresas son una realidad. Examinemos algunos mensajes que se han intercambiado online y que, aunque parecen básicos, hablan del robo de un enorme volumen de datos médicos de pacientes que ignoran que su información ha sido robada por un ciberdelicuente "como servicio".


I bought a RDP off the market yesterday but today when I tried to log in instead of windows all I got was this total MD program, looks like a database management program for doctors. Has anyone experienced anything like this before, there is no start button or anything just this program, I can't even click anything?????

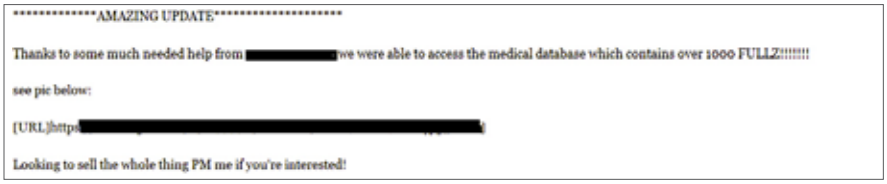
La vulnerabilidad RDP del primer comentario se refiere al mismo fallo del protocolo de escritorio remoto que aprovechó nuestro vendedor de la primera sección. Alguien contestó a la persona o personas que buscaban ayuda:


export the DB and sell it for profit obv

Se trata de una instrucción bastante sencilla. Sin embargo, parece que la pregunta era mucho más táctica:


Ok I figgured out how to click on things (alt key for some reason) but it's still pretty useless, windows key didn't open start menu or anything. When I log in it asks me to connect to server IP I tried localhost but it returns an error message saying it was unable to find database at localhost. Any suggestions?

La conversación continuó y tras algunos intercambios de información, la persona que pedía ayuda pudo solucionar el problema:


**********AMAZING UPDATE**********

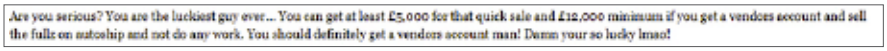
Thanks to some much needed help from [redacted] we were able to access the medical database which contains over 1000 FULLZ!!!!!!!

see pic below:

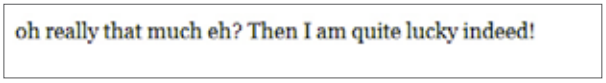
[URL]http[redacted]

Looking to sell the whole thing PM me if you're interested!

La respuesta a este mensaje pone de manifiesto algo que ilustramos en la primera sección: la existencia de demanda en el mercado.


Are you serious? You are the luckiest guy ever... You can get at least £5,000 for that quick sale and £12,000 minimum if you get a vendors account and sell the fullz on autoship and not do any work. You should definitely get a vendors account man! Damn your so lucky lmao!

Para poder apreciar la dimensión del caso, se trata de lo siguiente: un ciberdelincuente con poca experiencia técnica compra herramientas para atacar a una empresa vulnerable, para utilizarlas se sirve de algo de asistencia técnica gratuita, y así consigue extraer 1000 registros que podrían reportarle unos beneficios aproximados de12 000 libras esterlinas (sobre 13 475 euros). Si queríamos pruebas de que la ciberdelincuencia como servicio está en pleno auge dentro del sector de la asistencia sanitaria, estos mensajes no dejan lugar a dudas. Tras algunos mensajes más de felicitación, el ciberdelincuente se muestra un tanto sorprendido del beneficio que podría generarle la venta de los datos médicos robados:


oh really that much eh? Then I am quite lucky indeed!

En este ejemplo, es posible que el proceso haya sido todavía más sencillo. En lugar de "comprar la vulnerabilidad RDP", el ciberdelincuente puede simplemente haber adquirido una cuenta que pertenece a la empresa de servicios sanitarios.

Como destacábamos en el informe *Cybercrime Exposed* (Análisis de la ciberdelincuencia), en la actualidad, los ciberdelincuentes precisan de muy pocos conocimientos técnicos, y solo necesitan disponer de los medios para pagar por la ayuda de alguien con la experiencia necesaria. De hecho, hay una gran cantidad de vendedores que ofrecen datos robados a compradores que no necesitan participar en ataques directos a las empresas:


Almost every week I have FRESH breaches in USA Healthcare/Insurance sector.
No specific requests (like specific clinic/hospital), no pieces selling, no timewasters, ONLY BULK, ETC.

Hemos podido constatar las quejas de innumerables compradores por no haber recibido las mercancías que habían adquirido de los vendedores. En una publicación en un foro de habla rusa, Exploit, un vendedor que parece creíble habla de información obtenida de la red de un hospital. El tema de la conversación, traducido del ruso, es "acceso RDP a la red de un hospital de EE.UU.". El vendedor vende listas de pacientes, proveedores, mensajes de correo electrónico, números de la Seguridad Social, fechas de nacimiento, historias clínicas y otra información. También ofrece varias bases de datos de información similar. Ha publicado comentarios en foros y en mercados como Altenen, Lampeduza y varios foros de ventas de tarjetas desde 2011 y tiene antecedentes en la venta de información de identificación personal. Por lo tanto, existe un alto grado de confianza de que los datos médicos que ofrece son reales.

A través de estos ejemplos hemos descrito actividades delictivas cuya motivación es obtener ganancias financieras, a través de distintos medios para su monetización. Por supuesto, los compradores de datos robados pueden tener otros motivos, pero desde que se produce la fuga de datos hasta su reventa, la motivación de estos ciberdelincuentes es claramente económica.

Aunque es innegable el gran valor de los datos personales y confidenciales, es probable que la propiedad intelectual u otros tipos de datos de carácter médico sean incluso más valiosos. Podríamos dedicar un informe completo solamente a ese tema, pero por el momento ofreceremos solo una visión general.

La industria biotecnológica/farmacéutica en el punto de mira

Los ataques de ransomware dirigidos a empresas de servicios sanitarios o los robos de los datos personales que guardan son fenómenos relativamente recientes. Sin embargo, los ataques contra empresas de biotecnología o farmacéuticas para robar su propiedad intelectual se producen desde hace bastante tiempo. Los primeros casos se remontan a 2008, y su principal objetivo era obtener "información de fármacos en fase experimental, fórmulas químicas y datos confidenciales de todos los medicamentos que se venden en el mercado estadounidense". No cabe duda de que desde el punto de vista económico el valor de este tipo de información es considerablemente superior al del mercado de historias clínicas identificado en este y en otros informes.

Este tipo de oportunidades parecen justificar el coste de una operación de ciberrobo que "emplea a cientos de personas haciendo uso de un mínimo de 1000 servidores". Estos ataques no se dirigen exclusivamente contra empresas del sector privado. Por ejemplo, la Administración de Medicamentos y Alimentos estadounidenses (FDA, por sus siglas en inglés) "ha sido una de las agencias que ha recibido más ataques debido al papel que juega como punto de partida de la comercialización de nuevos productos". Para entender la escala de los intentos de intrusión, una solicitud de información según la Freedom of Information Act (o Ley de Libertad de Información estadounidense) descubrió que "entre 2013 y 2015 se comunicaron 1036 incidentes. De ellos, la mitad se referían al acceso no autorizado e ilegítimo a los ordenadores de la FDA. Otro 21 % fueron clasificados como sondeos o exploraciones —similares al phishing— y el 19 % eran intrusiones de malware".

Parece que el malware es un vector de ataque habitual a redes de empresas de biotecnología y farmacéuticas, pero en otros casos se ha recurrido a personal interno de las empresas para extraer datos y conseguir un beneficio económico. Por ejemplo, en un caso, el ciberladrón "tenía intención de utilizar la información para crear sus propias empresas competidoras".

Hemos evitado especular sobre la autoría, ya que para atribuir el delito se requeriría una investigación que no puede limitarse a los indicadores técnicos. A pesar de que otros investigadores han afirmado conocer el origen de los ataques basándose en dichos indicadores, nuestra intención es demostrar el valor de estos datos, así como que todo parece indicar que los autores de amenazas que disponen de muchos recursos consiguen sus objetivos.

El uso de malware se discutió en la presentación de un Formulario 8-K por parte de la empresa de servicios de atención hospitalaria Community Health Systems en la Comisión del Mercado de Valores de EE.UU. Esta empresa informó de que

su sistema había sufrido un ataque de "malware sofisticado". En la presentación se afirmaba que el agresor "buscaba propiedad intelectual de gran valor, como por ejemplo, datos de desarrollo de dispositivos y equipos médicos". Según el equipo forense encargado de la investigación,·este grupo suele poner en el punto de mira a empresas de los sectores aeroespacial y de defensa, construcción e ingeniería, tecnología, servicios financieros y asistencia sanitaria".

En la mayoría de los casos, el phishing selectivo es el precursor de la infección, como demostró un ataque contra el Consejo Nacional de Investigaciones Científicas canadiense (National Research Council). En este ejemplo, el ataque "comenzó por la obtención de direcciones de correo electrónico válidas de empleados del consejo de investigaciones", según un estudio realizado por el Centro de Respuesta a Ciberincidentes de Canadá (Canadian Cyber Incident Response Centre). Al ataque siguió la instalación de malware cuando los destinatarios hicieron clic en los enlaces maliciosos. Aunque se trata de un recurso muy simple, el phishing selectivo se utiliza con frecuencia para robar propiedad intelectual, secretos comerciales u otra información confidencial o de derechos de autor.

Nuestra investigación sigue con los ataques al sector sanitario que persiguen el robo de propiedad intelectual. Podemos discrepar sobre las motivaciones y los autores de estos ataques, pero de lo que no cabe duda es de que las empresas de biotecnología y farmacéuticas deben extremar la vigilancia, ya que sus activos más valiosos están en el punto de mira de ciberdelincuentes con objetivos claros. Como manifestó un vicepresidente de Reliance Life Sciences, los "hackers están interesadísimos en las compañías farmacéuticas, ya que nosotros tenemos activos críticos de gran valor, como la fórmula (protegida por derechos de propiedad) de varios medicamentos. Además, el hecho de pertenecer a un sector tan grande contribuye también a que seamos un objetivo codiciado".

Conclusión

Los ejemplos de comercio clandestino de datos médicos robados son solo la punta del iceberg. Hemos omitido muchas otras categorías y servicios, pero esperamos que estos ejemplos dejen clara la amenaza. En este informe hemos hablado de la venta de datos robados relacionados con la asistencia sanitaria. Hemos demostrado que los ciberdelincuentes también compran productos que facilitan los ataques. Esto incluye la compra y alquiler de exploits y kits de exploits que generan un enorme número de infecciones en todo el mundo.

Cuando leemos sobre fugas de datos, el mercado de la ciberdelincuencia parece tan alejado de nuestra vida cotidiana que tendemos a ignorar el mensaje. Sin embargo, la ciberdelincuencia no es más que una evolución de la delincuencia tradicional. Debemos superar nuestra apatía y prestar atención a las recomendaciones para luchar contra el malware y otras amenazas. Si no lo hacemos, la información sobre nuestras vidas digitales puede terminar a la venta y a disposición de todo el que tenga una conexión a Internet. Sin embargo, cuando se trata de datos médicos, es mucho más difícil recuperar nuestra información que en el caso de otros datos. Por ejemplo, cuando fue atacada la empresa Target en 2013, se cancelaron las tarjetas de las víctimas y se emitieron nuevas tarjetas de pago. De esta forma se redujo el daño personal, ya que las tarjetas se habían puesto a la venta rápidamente en el mercado clandestino. En el caso de los datos médicos y la información personal, la estrategia de recuperación no es tan sencilla. Por este motivo, es fundamental que tomemos medidas de prevención destinadas a reducir la probabilidad de que se produzcan este tipo de robo de datos.

Uno de los problemas asociados a este tema es la falta de pruebas sobre las motivaciones para adquirir datos médicos robados. En el caso de la información de las tarjetas de pago, hemos documentado que los números de tarjeta se utilizaban para estafar a las víctimas. Durante nuestras investigaciones hemos identificado dónde se buscaban datos específicos para verificar las direcciones de las víctimas. Sin embargo, por el momento no hemos identificado los usos específicos a los que se destinan los datos médicos comprados en grandes cantidades. Seguiremos nuestra investigación sobre este tema, ya que consideramos que merece una atención especial, y publicaremos las novedades cuando descubramos nuevos datos.

Acerca de Intel Security

McAfee forma ahora parte de Intel Security. Con su estrategia Security Connected, su innovador enfoque de seguridad reforzada por hardware y su exclusiva red Global Threat Intelligence, Intel Security trabaja sin descanso para desarrollar soluciones y servicios de seguridad proactivos que protejan los sistemas, las redes y los dispositivos móviles de uso personal y empresarial en todo el mundo. Intel Security combina la experiencia y los conocimientos de McAfee con la innovación y el rendimiento demostrados de Intel para hacer de la seguridad un ingrediente fundamental en todas las arquitecturas y plataformas informáticas. La misión de Intel Security es brindar a todos la tranquilidad para vivir y trabajar de forma segura en el mundo digital. www.intelsecurity.com.

www.intelsecurity.com

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com

OCTUBRE DE 2016