Deloitte.

Escenario de amenazas en la Industria de Salud y Ciencias de la Vida

Evaluación global de amenazas

Deloitte Threat Intelligence & Analytics

Abreviaturas

Salud y Ciencias de la Vida |**Salud y Ciencias de la Vida**
Información confidencial de salud |**PHI**
Registros Clínico Electrónico de Salud |**EHR**
Servicio Nacional de Salud |**NHS**
Troyanos de acceso remoto |**RAT**
Amenaza persistente avanzada |**APT**
Punto de venta |**POS**
Tácticas, técnicas y procedimientos |**TTP**

Contenido

Resumen ejecutivo

La industria de la **Salud y Ciencias de la Vida** (Life Sciences and Health Care) está expuesta a un amplio espectro de riesgos y ciber-amenazas. Los servicios que las organizaciones de **Salud y Ciencias de la Vida** proveen y los datos que protegen como información confidencial sensible de salud (Protected Health Information), datos de registros electrónicos de datos (Electronic Health Record) y propiedad intelectual farmacéutica o biomédica valiosa, son inherentes a esas amenazas. Esta industria comprende una amplia variedad de servicios que incluye producción de drogas y terapias, dispositivos médicos, distribución, hospitales, clínicas y farmacias, planes de salud, y seguros. Todo lo anterior cuenta con un perfil de riesgo y un escenario de amenazas propios y únicos. No obstante, la industria de **Salud y Ciencias de la Vida** no es inmune a amenazas similares que enfrentan otras industrias. Las amenazas inter-industrias del tipo ransomware, malware de punto de venta (PoS), troyanos de acceso remoto y malware de robo de información también suponen una amenaza para las organizaciones de **Salud y Ciencias de la Vida** .

En este escenario, Deloitte analiza el perfil de riesgos y el escenario de amenazas propios de la industria de **Salud y Ciencias de la Vida** , y las tácticas y los facilitadores claves para hacerles frente. En particular, examina tres amenazas centrales para esta industria:

Dispositivos y aplicaciones médicas vulnerables: Atacantes que apuntan a dispositivos y aplicaciones médicas que funcionan en sistemas operativos desactualizados y no compatibles de Windows, y que sacan provecho de sus vulnerabilidades. Deloitte observó numerosos informes de vulnerabilidad de dispositivos y aplicaciones médicos, donde el código activo de explotación se publicó en menos de 24 horas de revelada la vulnerabilidad.

Violación de datos de PHI/EHR: Atacantes que apunta a información confidencial de salud (PHI) y registros electrónicos de salud (EHR) de pacientes. Estos datos de alto valor convierten a las organizaciones de **Salud y Ciencias de la Vida** en un objetivo principal para el robo de información. Los ciber-criminales atacan datos sensibles de PHI y EHR para convertirlos en dinero en los mercados negros, como através de reclamos fraudulentos a aseguradoras, obtención de medicamentos recetados y robo de identidades.

Los grupos de amenazas persistentes avanzadas (APT) respaldados por estados nación pueden dirigir su ataque a PHI/EHR para identificar objetivos para el reclutamiento de espionaje humano. Por ejemplo, estos datos pueden revelar no solo datos biográficos sino indicaciones de vulnerabilidad ante dificultades médicas que incrementen la probabilidad de que una entidad externa pueda explotar a individuos con acceso a información de seguridad nacional.

Robo de propiedad intelectual a partir de APT:
Los atacantes, particularmente los grupos APT, suelen dirigir su ataque a propiedad intelectual relacionada con dispositivos médicos, datos farmacéuticos o biomédicos. El robo de procesos comerciales privados, tecnologías innovadoras, datos de clientes y otro tipo de propiedad intelectual de organizaciones de **Salud y Ciencias de la Vida** beneficia económicamente a un estado nación adversario al reducir o eliminar los costos de investigación y desarrollo para los negocios domésticos. Los competidores externos pueden utilizar los detalles de logística de la cadena de suministro, de procesos de manufactura y de negocios programáticos para replicar estos procesos o identificar fallas.

El informe finaliza con recomendaciones basadas en cada una de estas categorías de amenazas. El actual escenario de amenazas a **Salud y Ciencias de la Vida** también permitirá que las organizaciones entiendan las amenazas dirigidas a esta industria y ofrezcan la inteligencia necesaria para implementar las medidas que se requieren para gestionar y mitigar los riesgos asociados. Creemos que esta investigación hará que los profesionales de seguridad de la información comprendan aún más, ampliará el conocimiento de los usuarios de negocios generales y ofrecerá una guía práctica para las organizaciones de la industria de **Salud y Ciencias de la Vida** .

Impacto geográfico

Chile

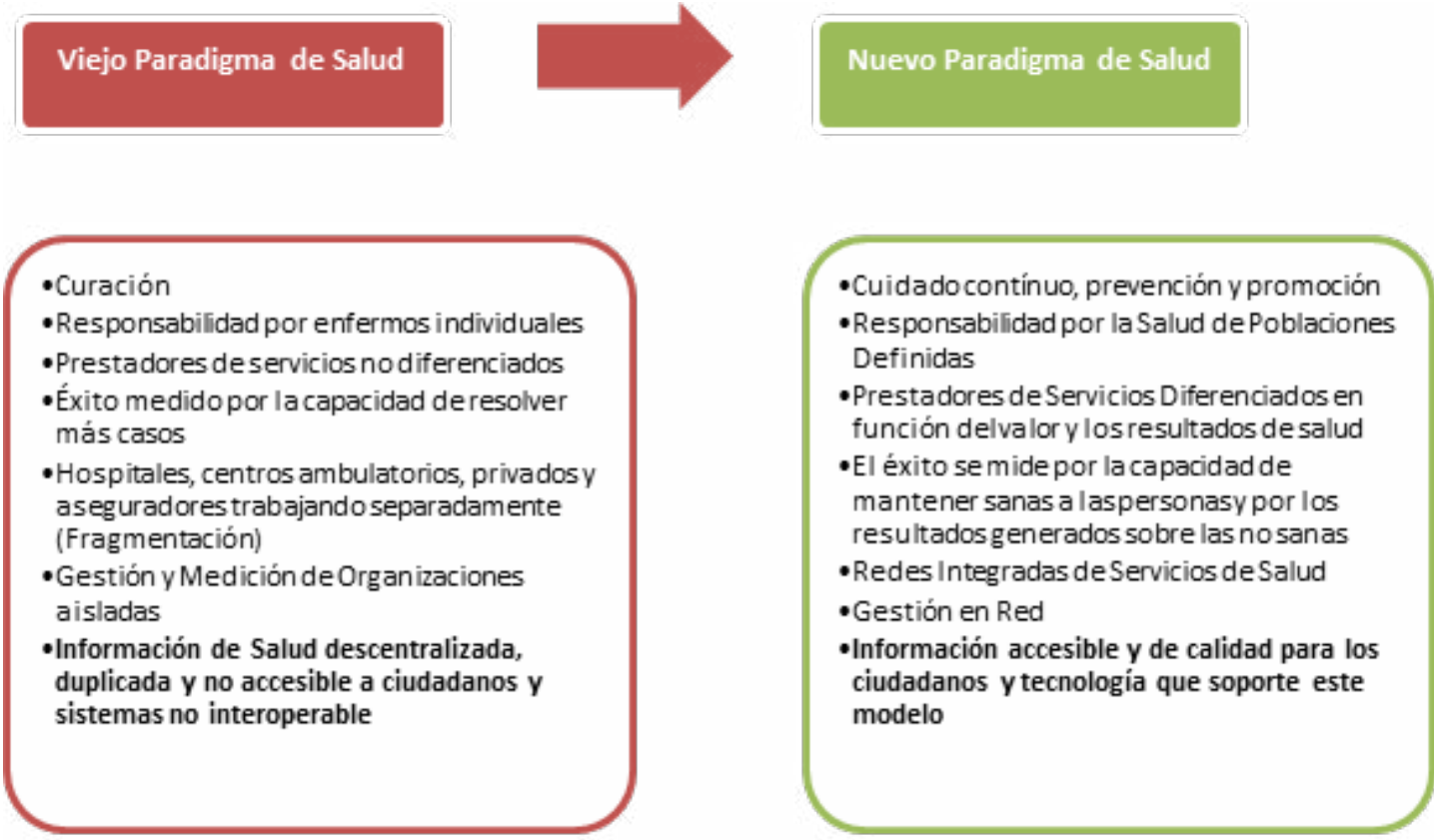
De acuerdo a lo que indica el 24° Informe Anual de Seguridad (ISTR) de Symantec, Chile ocupa el quinto lugar de LATAM de países más propensos a ciberataques y los ataques a nuestro país crecieron entorno al 60% en el 2018. Tanto así que se ubica habitualmente entre las primeras 3-5 posiciones en LATAM y entre las 30 primeras en el mundo en recibir ataques, siendo el Ransomware, Phising y los Ataques Web las amenazas más recurrentes y el network attacks, cryptojacking, ataques por spam y bots y malware los que cierran el ranking.

Es un hecho que el Desarrollo y la Digitalización de Chile, nos hacen un país más expuesto ante las amenazas de ciberseguridad como hemos podido ver en otras industrias como la banca.

¿Cuál ha sido el Desarrollo y la Digitalización de Chile y cuán vulnerables somos?

En los últimos 20-25 años y bajo los diferentes gobiernos, el Ministerio de Salud ha venido trabajando en el Modelo de Gestión de Salud para nuestro país y cómo abordar sus desafíos. Entre los principales desafíos se encontraban: equilibrar los recursos que constituyen la oferta disponible versus la demanda, el acceso a la salud que garantice la equidad sanitaria, el acceso universal a una atención centrada en las personas y lograr comunidades sanas.

Es innegable el avance que hemos tenido en todos estos frentes, observándose en los últimos años una fuerte inversión en infraestructura hospitalaria y la potenciación de la Atención Primaria de Salud, tanto en infraestructura como en recursos para aumentar su capacidad resolutiva, disminuyendo el "Hospitalocentrismo".



Junto a este desarrollo, se ha venido abordando el mayor reto en materia de organización y prestación de Servicios de Salud, la Fragmentación, que es un desafío clave para transitar del viejo paradigma de la Salud al Nuevo:

Una de las áreas de abordaje para resolver la fragmentación ha sido el impulso de iniciativas de Digitalización de la Salud que vienen desarrollándose desde los años 90 y que tuvo su mayor explosión en los últimos 10 años con el desarrollo de iniciativas como SIDRA, que nos han permitido realizar importantes avances en la incorporación de Tecnología y Software para gestionar los Procesos de Atención de Pacientes a través de Registros Clínicos Electrónicos, para gestionar la información de salud de los pacientes.

Si bien el avance de esta iniciativa es claro, sobre todo en Atención Primaria de Salud llegando a niveles entorno al 90% de cobertura, existe aún un espacio de crecimiento en los procesos de Atención Secundaria y Terciaria donde la Implementación de Sistemas de Registro Clínico está entorno al 50%. Estas cifras han llevado a nuestro país a estar entre los más avanzados de LATAM en la implementación de Registros Clínicos Electrónicos y por tanto a ser mirados como referentes desde la región.

Por otro lado, hemos visto un gran impulso en el desarrollo de Sistemas y Soluciones para centralizar información de Salud como el RNI, SIGES, UGCC, DEIS, plataforma NAISS, etc. o el reciente proyecto de Historia Clínica Nacional Compartida, que es el primer Health Information Exchange (HIE) del país. Los servicios de salud tributan información clínica y datos de salud vía carga masiva de datos o interfaces.

En los últimos años, con la proliferación del ecosistema de innovación y emprendimiento, se han desarrollado iniciativas para resolver problemas concretos de salud, mejorar la experiencia del paciente y su bienestar a través de Apps, integración con Wearables, dispositivos IOT, Smartwatch, etc. que universalizan el acceso, aperturando también nuevos canales para la compartición y flujo de los datos de salud.

El plan del Gobierno y del MINSAL y su fuerte apuesta por la inversión en Infraestructura Hospitalaria, así como el fortalecimiento de la Salud Digital con mucho foco en la Telemedicina, dibujan un espacio de crecimiento aún mayor para la incorporación de Tecnología en la gestión de los datos de Salud de nuestros ciudadanos.

Este desarrollo y crecimiento exponencial en la digitalización de la salud, es algo de lo que debemos sentirnos orgullosos y que ha venido para quedarse.

La tan ansiada tecnología 5G nos llevará a la hiperconexión, al aumento de los flujos de datos, las infraestructuras y dispositivos de acceso por los que viajarán los datos de salud, suponiendo un universo de oportunidades para los cibercriminales.

¿Cuánto tiempo tardaremos en enfrentar una situación similar a las sufridas en la banca (caso Banco de Chile, o a la del NHS en Reino Unido y cómo vamos a reaccionar?

Sin ir más lejos, el pasado mes de julio según informó el Servicio de Salud Metropolitano Sur Oriente, dependiente del Ministerio de Salud, se produjo un ataque de un "ransonware" en plena campaña de invierno sobre los sistemas que soportan los procesos de Imagenología, viéndose obligados a implementar un plan de contingencia, pues el servicio estuvo suspendido por algunas horas. Durante esa jornada, sólo se pudieron acceder a imágenes de pacientes de una antigüedad de seis meses, siendo que la empresa proveedora guardaba registros de hace una década. Esto afectó a la operación dado que los médicos tuvieron que solicitar los exámenes manualmente a través de un formulario y no través del mismo sistema. Importantes Hospitales como el Sótero del Río, La Florida, Padre Hurtado, San José de Maipo y el CRS Cordillera fueron afectados por este ataque.

Por tanto, cabe preguntarse..., ¿está preparado nuestro Sistema de Salud para afrontar el crecimiento de amenazas de ciberseguridad que está teniendo el país?

La Estrategia de Ciberseguridad en Salud hasta el momento ha estado más enfocada en la definición de normativas para la seguridad y protección de datos de salud, delegando en gran medida la responsabilidad del cumplimiento de éstas, sobre las empresas proveedoras de tecnología, infraestructura y soluciones. Sin embargo, lo que está en riesgo son los datos de los pacientes, datos que son gestionados e intercambiados por los sistemas e infraestructura que dan soporte a la operación del Sistema Nacional de Salud y a los sistemas centrales para la toma de decisiones. Son los prestadores de salud los últimos responsables sobre los datos de los pacientes, proteger sus derechos y hacer cumplir las obligaciones, y en el caso del sistema público, la Subsecretaría de Redes y el MINSAL en última instancia los que deben velar por esto. Está en juego por tanto la protección de estos datos y la reputación del sistema completo, por lo que se hace necesaria una Estrategia de Ciberseguridad Nacional en Salud, liderada desde el Gobierno, que integre a los responsables de administrar las Infraestructuras Críticas del país, involucre a los diferentes actores del ecosistema y esté sustentada sobre una fuerte inversión, que nos permita protegernos de las amenazas de ciberseguridad, así como también ser resilientes a los ataques que antes o después ocurrirán.

Américas

En la región de las Américas, particularmente en EE. UU., las industrias de **Salud y Ciencias de la Vida** continúan siendo un objetivo lucrativo tanto para los atacantes organizados como para los oportunistas. Esto es atribuible al gran número de importantes organizaciones del sector que operan en EE. UU. y a su rol como un importante núcleo económico, tecnológico e innovador para esta industria a nivel global. De manera acorde, las organizaciones de salud ubicadas en la región son más propensas a asumir un riesgo mayor de ser el objetivo de ciber-ataques. Los autores de los ataques pueden ser oportunistas motivados económicamente y/o sindicatos criminales altamente organizados y grupos APT. Cada uno de ellos ha dirigido su ataque contra organizaciones de **Salud y Ciencias de la Vida** para robar datos confidenciales sensibles de PHI, EHR y propiedad intelectual farmacéutica y biomédica valiosa.

En 2018, los informes de esta industria indicaban que el sector había sufrido alrededor de 351 violaciones informadas de datos, lo que resultó en la exposición de más de 13 millones de registros de atención de salud.[1] Una de las más grandes violaciones de datos de **Salud y Ciencias de la Vida** en 2018 involucró a una compañía de facturación médica llamada AccuDoc Solutions que administra el sistema de pagos en línea utilizado por la red de Atrium Health de 44 hospitales en Carolina del Norte, Carolina del Sur y Georgia. En este ataque, se vieron comprometidas las bases de datos de la compañía y los registros de salud de 2.652.537 pacientes quedaron expuestos. En otro incidente, el objetivo fue una organización llamada UnityPoint Health a la cual dirigieron ataques de phishing que comprometieron a numerosas cuentas comerciales de correo electrónico. Las cuentas comprometidas contenían los datos de PHI de alrededor de 1.421.107 personas.

Asimismo, cabe destacar que a medida que la industria de **Salud y Ciencias de la Vida** aumenta el traspaso de sus transacciones de registros en papel a registros electrónicos de salud (EHR), es casi seguro que habrá una correlación directa con un aumento en las ciber-intrusiones y las violaciones de datos. Estas ciber-intrusiones están aún más exacerbadas por las persistentes vulnerabilidades en las redes de proveedores de atención de salud y los sistemas operativos antiguos usados para alojar dispositivos y aplicaciones médicas, lo cual permitió a los atacantes obtener el acceso inicial a los sistemas de las organizaciones del sector y robar datos de pacientes.

Las amenazas inter-industria también jugaron un rol importante en el escenario de amenazas a numerosas organizaciones de atención de salud en toda la región y en EE. UU. Si bien el ransomware, el malware de punto de venta y los troyanos de acceso remoto no son específicos para atención de salud, hubo múltiples incidentes que los involucraron y que impactaron en esta industria en 2018.

1.- HIPAA, "Largest Healthcare Data Breaches of 2018," HIPAA Journal. [En línea]. Disponible: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018 [consultado el 15 de diciembre de 2018].

Europa y Medio Oriente (EMEA)

La creciente digitalización en la atención de salud sumada a los limitados fondos destinados a la seguridad de TI y la compleja infraestructura de TI constituyen oportunidades para los atacantes de **Salud y Ciencias de la Vida** en todo EMEA. En la Annual European eHealth Survey 2018 (Encuesta anual europea de salud) se evidenció que lo que preocupa a los proveedores de atención de la salud son los inadecuados presupuestos de TI para abordar problemas de ciberseguridad.[2] En febrero de 2018, el Servicio Nacional de Salud (NHS) de Reino Unido, informó que sus 200 servicios de atención integral auditados con posterioridad al ataque Wannacry 2017 no cumplían los estándares de ciberseguridad. Dichos servicios habían tenido dificultades para actualizar los sistemas operativos y softwares vulnerables en sus empresas.[3] Esa desactualización favoreció que Wannacry los afectara.[4]

Gracias a la creciente superficie de ataque y la valiosa naturaleza de la información que contiene, el sector de **Salud y Ciencias de la Vida** en EMEA continuó siendo en 2018 un objetivo atractivo para ciertos atacantes. En Reino Unido, el sector de salud representó la mayor cantidad de informes de violaciones de datos en 2017/18 a la Oficina del Comisionado de Información, que dio cuenta del 43% del total de informes.[5]

En agosto de 2018, la cadena Superdrug de productos de salud y belleza fue objeto de un evidente ataque para obtener detalles de clientes. La cadena advirtió a sus clientes que un grupo afirmaba haber obtenido datos de 20.000 clientes, incluidos nombres, direcciones, fechas de nacimiento y números telefónicos. Si bien la tienda puso en duda el alcance del robo sufrido e insistió en que solo se habían visto comprometidas 38 cuentas, sugirieron que los atacantes reutilizaron credenciales obtenidas de otros robos para acceder a las cuentas de los clientes de Superdrug.[6]

También había indicadores de un ataque patrocinado por el Estado y dirigido a información sensible poder del sector de **Salud y Ciencias de la Vida** en EMEA. La continuidad de las tensiones entre Rusia y los aliados de la OTAN en el norte de Europa pudo haber convertido en objetivo a la información de salud de los participantes de ejercicios de la OTAN. En enero de 2018, las autoridades de Health South-East RHF (Organización regional de salud de Noruega) informaron que había atacantes en una supuesta búsqueda de información relacionada con el apoyo de la autoridad a los ejercicios militares de la OTAN que se realizarían más adelante ese año. Dicha organización es responsable de proveer atención sanitaria a más de la mitad de la población de Noruega. El CERT de atención sanitaria noruego describió a los atacantes como capacitados y profesionales.[7]

Grupos hacktivistas también atacaron al sector de **Salud y Ciencias de la Vida** en 2018. En julio, la rama italiana del grupo hacktivista Anonymous filtró más de 12.000 correos electrónicos, nombres de usuarios y contraseñas de empleados, pacientes y proveedores del hospital Sant'Andrea de Roma. El grupo difundió la información y exigió al Ministro de Salud italiano que proteja mejor los datos de los usuarios.[8]

Se observó que los atacantes, para dirigir el ataque hacia información sensible en manos del sector de **Salud y Ciencias de la Vida** en EMEA, usaban técnicas tales como la ingeniería social. En diciembre de 2018, la organización benéfica de investigación biomédica Wellcome Trust anunció que había sido objeto de dos exitosas campañas de phishing separadas,en una de las cuales los atacantes claramente buscaban información sensible en manos de la alta gerencia.[9]

2.- Health Information and Management Systems Society Europe, "Annual European eHealth Survey 2018." [En línea]. Disponible: https://www.himss.eu/sites/himsseu/files/eHealth-Annual-Survey-Results-2018-v1b.pdf [consultado el 15 de enero de 2019].

3.- UK House of Commons Public Accounts Committee", Oral evidence: Cyber-attack on the NHS, HC 787", 5 de febrero de 2018. [En línea]. Disponible: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/public-accounts- committee/investigation-wannacry-cyber-attack-and-the-nhs/oral/78545.html [consultado el 16 de enero de 2019].

4.- UK National Audit Office", Investigation: WannaCry cyber attack and the NHS", 25 de abril de 2018. [En línea]. Disponible: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the- NHS.pdf [consultado el 16 de enero de 2019].

5.- Kroll, "Data Breach Reports to Information Commissioner Increase by 75%", Comunicados de prensa, 4 de septiembre de 2018. [En línea]. Disponible: https://www.kroll.com/en-us/intelligence-center/press-releases/data-breach-reports-to- information-commissioner [consultado el 15 de enero de 2019].

6.- Angela Monaghan, "Superdrug targeted by hackers who claim to have 20,000 customer details", The Guardian, 22 de agosto de 2019. [En línea]. Disponible: https://www.theguardian.com/business/2018/aug/22/superdrug-targeted-by-hackers-who-claim-to-have-20000-customer-details [consultado el 17 de enero de 2019].

7.- Stormark, Kjetil, "Lette etter pasientjournaler og forsvarsinfo," AldriMer.no, 18 de enero de 2018. [En línea]. Disponible: https://www.aldrimer.no/lette-etter-pasientjournaler-og-forsvarsinfo/: [Consultado el 17 de enero de 2019]. Galaxkey, "Massive Attack On The Norwegian Healthcare Provider, Health South-East RHF", 7 de febrero de 2018. [En línea]. Disponible: https://www.galaxkey.com/massive-attack-on-the-norwegian-healthcare-provider-health-south-east- rhf/: [Consultado el 17 de enero de 2019].

8.- Anonymous Italy, "Privacy all sbando", blog de Anonymous Italia, 14 de julio de 2018. [En línea]. Disponible: https://anon- italy.blogspot.com/2018/07/privacy-allo-sbando.html?m=1, [consultado el 16 de enero de 2019].

Asia Pacífico (APAC)

La mayoría de las ciber-amenazas observadas que impactaron en la región fueron reflejo de las utilizadas a nivel global para atacar al sector de **Salud y Ciencias de la Vida** en conjunto. Esto incluye phishing dirigido, ingeniería social, dispositivos y aplicaciones médicas vulnerables, malware, violación de datos de información confidencial de salud y registros electrónicos de salud (PHI/EHR) y mayores niveles de actividad patrocinada por el Estado. Sin embargo, de acuerdo con los informes e incidentes observados de la industria, el uso de ransomware se limitó comparativamente a la región APAC, a diferencia de lo que se observó que más afectaba al sector de **Salud y Ciencias de la Vida** global.

Dentro de la región APAC, las violaciones de datos de PHI/EHR se consideran una tendencia recurrente que afecta a la industria de **Salud y Ciencias de la Vida** . En el Q2 de 2018, el Australian Notifiable Data Breaches Quarterly Statistics Report (Informe estadístico trimestral australiano de brechas de ciberseguridad) destacó que el 25% de la información personal involucrada en violaciones de datos se trata de información de salud.[10] Esto se ejemplifica a través del incidente SingHealth, la institución más importante de atención sanitaria de Singapore, cuyo ataque comprometió la información personal de 1,5 millones de pacientes y detalles de prescripciones médicas de otros 160.000.[11] Dado el gran espectro de formatos en los que los datos pueden aparecer dentro de una organización de **Salud y Ciencias de la Vida** , ya sean digitales o impresos, esto significa que los riesgos de violaciones de datos se pueden diseminar y generalizar en esta industria.

El sector de **Salud y Ciencias de la Vida** dentro de APAC también se ha plagado de atacantes que sacan ventaja de deficiencias sin resolver para obtener acceso a un sistema. Este sector suele usar dispositivos que están desactualizados y brindan así un vector de ataque más amplio para lograr el acceso inicial, lo cual les permite infectar al sistema con el malware y/o facilitar luego movimientos laterales dentro de la red de las organizaciones.[12] Deloitte estudió al grupo Orangeworm cuyo objetivo fue la industria del sector de Salud en APAC con el uso del malware Kwampirs para atacar a dispositivos médicos como puntos de entrada a las redes de atención sanitaria.[13] También se observó que este vector de ataque estaba siendo comúnmente utilizado a nivel mundial para atacar este sector en conjunto.

El phishing y el phishing dirigido fueron las formas más frecuentes de ingeniería social utilizada para atacar al sector de APAC. Estos tipos de ataque se usaron para infectar con malware o engañar a las víctimas para que brinden a los atacantes datos de PHI/EHR, información de proveedores o miembros.[14] Deloitte informó acerca de STOLEN PENCIL, un grupo de amenazas norcoreano, cuyo objetivo fue la ingeniería biomédica desde por lo menos mayo del año 2018. El vector de infección genera mensajes de correo electrónico de phishing dirigido que contienen enlaces a páginas donde el receptor encuentra indicaciones que lo conducen a la instalación de extensiones maliciosas del navegador Google Chrome .[15]

Se observó que numerosos grupos como Orangeworm, STOLEN PENCIL y Stone Panda dirigen sus ataques a la infraestructura crítica dentro del sector de la Salud . Los criminales y ciber-adversarios patrocinados por el Estado continúan siendo una amenaza persistente para APAC, donde los ataques maliciosos y criminales dan cuenta del 41% de las violaciones de datos del sector de salud en Australia.[16] Estos atacantes patrocinados por el Estado están permanentemente intentando filtrar datos PHI/EHR. Este tipo de información se puede usar de diversas maneras, incluso como forma de cultivar correos electrónicos de phishing dirigido a través del uso de credenciales comprometidas para ingresar a sistemas o alternativamente para monetizar en el mercado negro.[17]

9.- Wellcome Trust, "Statement on data breach", 7 de septiembre de 2018. [En línea]. Disponible: https://wellcome.ac.uk/press-release/statement-data-breach: [Consultado el 16 de enero de 2019]; Wellcome Trust, Annual Report and Financial Statements 2018. [En línea]. Disponible: https://wellcome.ac.uk/sites/default/files/wellcome-trust-annual-report-and-financial-statements-2018.pdf [Consultado el 16 de enero de 2019].

10.- Australian Cyber Security Centre, 2017 Threat Report, 2018, [En línea]. Disponible: https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly- statistics/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018.pdf. [Consultado: 29 de noviembre de 2018].

11.- Personal information of 1.5 million patients compromised in SingHealth data breach, G-TN-EN-01-7310, 23 de julio de 2018.

12.- Several flaws in OpenEMR software can likely expose patient medical records, G-TN-EN-01-7419, 9 de agosto de 2018.

13.- Kwampirs malware operators dubbed Orangeworm targeting Healthcare sector, A-TN-EN-01-6810, 24 de abril de 2018.

14.- 14 myGov phishing campaign stealing bank details through cloned website, 6 de julio de 2018. Beware of fake Medicare email", Staysmartonline.gov.au, 4 de julio de 2018. [En línea]. Disponible: https://www.staysmartonline.gov.au/alert- service/beware-fake-medicare-email. [Consultado: 6 de julio de 2018].

15.- North Korean threat actors target biomedical engineering, G-TR-EN-01-8309, 11 de diciembre de 2018.

16.- 16 Australian Cyber Security Centre, 2017 Threat Report, 2018, [En línea]. Disponible: https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly- statistics/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018.pdf. [Consultado: 29 de noviembre de 2018].

17.- Stone Panda APT campaign leverages new Trojan "ChChes", G-TN-EN-17-00190, 17 de febrero de 2017.

Orangeworm utilizó el malware Kwampirs para atacar a los proveedores de atención de la salud, proveedores de soluciones de TI para atención sanitaria, compañías farmacéuticas y fabricantes de equipos de la industria de atención de la salud en EEUU, Europa y Asia. Este malware, sospechado de estar a favor del ciber-espionaje, obtiene acceso remoto a equipos y sistemas, y fue hallado en dispositivos que controlan máquinas de imágenes de alta tecnología como rayos X y resonancias magnéticas (IRM). Los atacantes intentan acceder a computadoras, información de adaptadores de red, recursos compartidos de red disponibles, unidades de disco vinculadas, y archivos presentes en la computadora comprometida. También muestran interés en máquinas que sirven para asistir a pacientes en el llenado de formularios de consentimiento para procedimientos. Las fuentes internas de Deloitte identificaron que el malware Kwampirs probablemente se origina a partir de otras herramientas para llevar a cabo una campaña de espionaje corporativo.[18]

SingHealth, la institución más importante de atención de salud de Singapur, informó un ataque que comprometió la información personal de 1,5 millones de personas y detalles de prescripciones médicas de otras 160.000.

El análisis forense que realizó la Agencia de Ciberseguridad de Singapur (CAS) determinó que los atacantes habían accedido al sistema de TI de SingHealth a través de una brecha inicial en una determinada estación de trabajo front-end. En consecuencia, fueron capaces de obtener credenciales de cuentas privilegiadas para lograr el acceso privilegiado a la base de datos. El Ministro de Salud del país atribuyó el ataque a autores patrocinados por el Estado. La CAS advirtió que los datos comprometidos podrían ser vendidos en la dark web.

Este ataque resalta el uso del acceso privilegiado de usuarios como un vector de ataque que los atacantes están usando con mayor frecuencia. La infiltración inicial se realiza a través de una estación de trabajo relativamente sin privilegio (es decir, un computador personal) y, desde allí, se obtiene el acceso a una cuenta privilegiada a través de credenciales que operan en la memoria del sistema.[19]

El blanco del grupo norcoreano STOLEN PENCIL se concentró en la ingeniería biomédica desde, por lo menos, mayo de 2018. El vector de infección opera con mensajes de correo electrónico de phishing dirigido con enlaces a páginas que le dan indicaciones a los receptores para instalar extensiones maliciosas del navegador Google Chrome. STOLEN PENCIL expande y mantiene su acceso a través de credenciales comprometidas, software legítimo y el protocolo de escritorio remoto (RDP). Sus objetivos no son claros, pero es posible que estén dirigidos a obtener propiedad intelectual que no esté legalmente disponible en Corea del Norte debido a las sanciones contra ese país.[20]

Esta campaña de reconocimiento de datos beneficia a múltiples implantes, herramientas y variantes de malware asociados con el ciber-grupo Hidden Cobra patrocinado por el Estado. Su objetivo son industrias dedicadas a la salud. Este grupo está vinculado a múltiples campañas de phishing dirigido, operaciones de ciber-espionaje y ataques con motivaciones financieras. Parte del malware utilizado en la campaña Opertion GhostSecret tenía similitudes con los malware conocidos como Bankshot y Destover. La compleja evolución de estos implantes de reunión de datos revela la capacidad avanzada de un atacante que continúa su desarrollo de herramientas.[21]

OpenEMR es un registro médico electrónico de dominio público y una solución de gestión de la práctica médica. De acuerdo con la información que aparece en el sitio web open-emr.org, el software incluye funcionalidades para ofrecer servicios de citas médico/paciente, informes del CMS, facturación médica, prescripción médica electrónica e integración de resultados de laboratorio a los informes del respectivo paciente.[22] Se descubrieron fallas en el software OpenEMR. 15 de las fallas fueron categorizadas como vulnerabilidades de severidad alta. La más llamativa de todas era un desvío simple de la autenticación del portal de pacientes que requería solo una URL modificada para acceder a información confidencial.[23]

18.- Kwampirs malware operators dubbed Orangeworm targeting Healthcare sector, A-TN-EN-01-6810, 24 de abril de 2018.

19.- Personal information of 1.5 million patients compromised in SingHealth data breach, G-TN-EN-01-7310, 23 de julio de 2018.

20.- North Korean threat actors target biomedical engineering, G-TR-EN-01-8309, 11 de diciembre de 2018.

21.- Cyber reconnaissance operation GhostSecret targeting multiple industries, G-TN-EN-01-6821, 25 de abril de 2018.

22.- Several flaws in OpenEMR software can likely expose patient medical records, G-TN-EN-01-7419, 9 de agosto de 2018.

23.- Stone Panda APT campaign leverages new Trojan "ChChes", G-TN-EN-17-00190, 17 de febrero de 2017

La campaña de la APT Stone Panda estaba dirigida a las industrias farmacéuticas japonesas. Además de los troyanos PlugX y Poison Ivy que Stone Panda usó de septiembre a noviembre de 2016, el grupo agregó uno nuevo llamado "ChChes". Stone Panda favorece, fuertemente, el phishing dirigido y toma medidas para diseñar socialmente sus correos electrónicos de phishing para que tengan la apariencia más legítima posible. Esto y su persistencia destaca la necesidad de capacitar y concientizar respecto del phishing dirigido a individuos y organizaciones que sean probables objetivos.

El gobierno australiano publicó una advertencia a través del sitio web Stay Smart Online acerca de la campaña de phishing de myGov. Los atacantes crearon un clon del sitio web myGov para engañar a las víctimas y hacer que compartieran sus datos de inicio de sesión y detalles de cuentas bancarias. El engaño comienza con un correo electrónico de phishing que aparenta ser de Medicare y que pide a los receptores que actualicen los detalles de la transferencia electrónica de fondos (EFT) para que puedan empezar a recibir pagos por los beneficios y reclamos de Medicare. Al hacer clic en el enlace que aparece en el correo, las víctimas son dirigidas a una réplica del sitio web real de myGov. Si un usuario final completa sus detalles de inicio de sesión, se le pide que también ingrese su pregunta secreta de seguridad y la respuesta, y luego es dirigido a un sitio web ficticio de Medicare para completar los datos de su cuenta bancaria. Estos correos electrónicos y estas páginas web imitan el diseño y la marca de myGov y Medicare, lo cual los hace parecer legítimos. El gobierno australiano categorizó este riesgo como una prioridad alta y recomendó que los usuarios actúen siguiendo las recomendaciones dadas para garantizar su seguridad, protección o privacidad.[24]

24.- myGov phishing campaign stealing bank details through cloned website, 6 de julio de 2018. Beware of fake Medicare email", Staysmartonline.gov.au, 4 de julio de 2018. [En línea]. Disponible: https://www.staysmartonline.gov.au/alert- service/beware-fake-medicare-email. [Consultado: 6 de julio de 2018].

Escenario de amenazas a la industria de Salud Y Ciencias De La Vida

SERVICES & ENABLERS

- Underground marketplaces and forums
- Account checking services
- Criminal Proxy and VPN services
- Bullet Proof Hosting
- Maldoc and Downloader kits
- Traffic resellers
- Spam services

Tools & Malware

- Exploit Kits
- Ransomware
- Brute Forcers
- Infostealers
- Self Propagating Malware
- Account Checkers
- POS Malware
- Remote Access Toolkits

Amenazas a la industria

Economía subterránea para monetizar el acceso a registros de salud y a bases de datos de atención médica

Las tendencias claves en el escenario de amenazas que afectan a organizaciones de SALUD Y CIENCIAS DE LA VIDA son ataques que apuntan a datos de EHR/PHI para su venta y el tráfico en el mercado negro de credenciales robadas de portales de pacientes. Deloitte observó que numerosos atacantes demuestran un claro interés en las organizaciones de la industria de SALUD Y CIENCIAS DE LA VIDA y apuntan directamente a ellas. Es probable que esta intención sea de naturaleza estratégica y se relacione directamente con su capacidad para obtener ganancia de estos ataques, ya sea a través de las demandas extorsivas y de dinero que paga la organización, o a través de la venta de EHR/PHI en mercados negros. Una vez vendida, la información de identificación personal (PII) contenida en el EHR se puede usar para presentar reclamos fraudulentos a compañías de seguros, obtener medicamentos bajo prescripción médica y desarrollar el robo de identidades. Deloitte también observó a atacantes que ofrecen acceso libre a las calificaciones del EHR en bases de datos comprometidas de atención sanitaria como información promocional para alentar a que otros atacantes les compren a ellos en el futuro.

En muchas ocasiones, el ataque estratégico al EHR les brindó a los atacantes información sensible de individuos de alto perfil, incluso celebridades, atletas profesionales y funcionarios de gobierno de alto rango. Estos tipos de registro son fácilmente monetizables a través de la venta de los datos a ciber-criminales o gobiernos. Asimismo, el compromiso de propiedad intelectual sensible de las industrias de salud y farmacia, entre otras, también es fácilmente monetizable en el mercado negro a través de su venta a competidores y estados. El tráfico de información de salud robada es una tendencia que probablemente se intensifique debido a la transición continua de registros de papel a registros electrónicos de salud (EHR).

Además de la venta de registros comprometidos y el acceso a EHR, la extorsión monetaria a organizaciones vulneradas con la amenaza de revelar información confidencial comprometida es una de muchas maneras en las que los atacantes pueden monetizar el acceso no autorizado. Si bien esta táctica se puede usar contra organizaciones en cualquier cantidad de industrias, las organizaciones de atención de la salud son especialmente vulnerables debido a la naturaleza, altamente sensible, de información confidencial (PHI) que manejan y a las implicancias legales y normativas que supone su violación.

La información confidencial de salud (PHI) de hospitales y otras organizaciones sanitarias en EEUU son de sumo interés, tanto para atacantes patrocinados por el Estado como para ciber-criminales, pero por diferentes razones. La PHI es particularmente útil para estafadores financieros debido a la gran cantidad de detalles que normalmente contiene, como fechas de nacimiento y números de seguro social, y se vende de manera acorde a precios más altos en los foros criminales. Los delincuentes rusos son los líderes del mercado en este campo, y EEUU sigue siendo su blanco principal

Tácticas, técnicas y procedimientos (TTP)

El monitoreo que hizo Deloitte en foros subterráneos reveló la actividad de numerosos atacantes solicitando PHI en foros criminales, o buscando monetizar PHI robada, o pidiendo acceso a sistemas de PHI que ya estén comprometidos. Estos foros facilitan la monetización al facilitarles a los atacantes un mercado donde comprar, vender y comercializar datos de EHR/PHI. Los atacantes usan una variedad de TTP para comprometer credenciales y robar sus datos.

Se valen de malware de robo de información y correos electrónicos de phishing para sustraer credenciales (nombres de usuario y contraseñas) de víctimas que luego usarán en ataques de repetición de contraseñas o de relleno de credenciales para acceder a las cuentas de sus víctimas y robar datos de EHR/PHI.

Los atacantes apuntan a dispositivos médicos vulnerables en sistemas operativos de Windows antiguos y desactualizados que funcionan como puntos de entrada a hospitales y sirven para robar datos sensibles de EHR/PHI.

Recomendaciones

- Entender el escenario de amenazas – La inteligencia de amenazas permite que las organizaciones de SALUD Y CIENCIAS DE LA VIDA tomen conciencia de la situación y estén al día con los últimos ataques y las TTP dirigidas a la industria de SALUD Y CIENCIAS DE LA VIDA .
- Monitoreo de foros - Monitorear foros subterráneos, volcado de credenciales y otras fuentes de credenciales que le pertenecen a la organización o se originaron en ella.
- Controles de acceso – Asegurar los portales de pacientes con autenticación multifactorial para evitar ataques de repetición de contraseñas.

El mercado negro y el tráfico de credenciales para acceder a portales de pacientes

El interés de los atacantes por obtener y monetizar credenciales robadas de portales de pacientes sigue siendo una tendencia estable. Tras haber realizado el seguimiento correspondiente, Deloitte informó de atacantes que venden credenciales robadas a diversos servicios. Las credenciales para los portales de pacientes, como MyChart, pueden brindar medios para obtener acceso no autorizado a los EHR y habilitar a los atacantes para que realicen otras actividades fraudulentas. Los atacantes también pueden obtener esas credenciales a través de diversos métodos. Estos métodos pueden incluir el uso de malware de robo de información y campañas de phishing. Las credenciales de inicio de sesión se suelen comprar, o se obtienen a partir de "listados combo" [25] que se consiguen sin cargo en foros clandestinos. El éxito de estos ataques puede atribuirse en gran parte a la repetición de contraseñas.

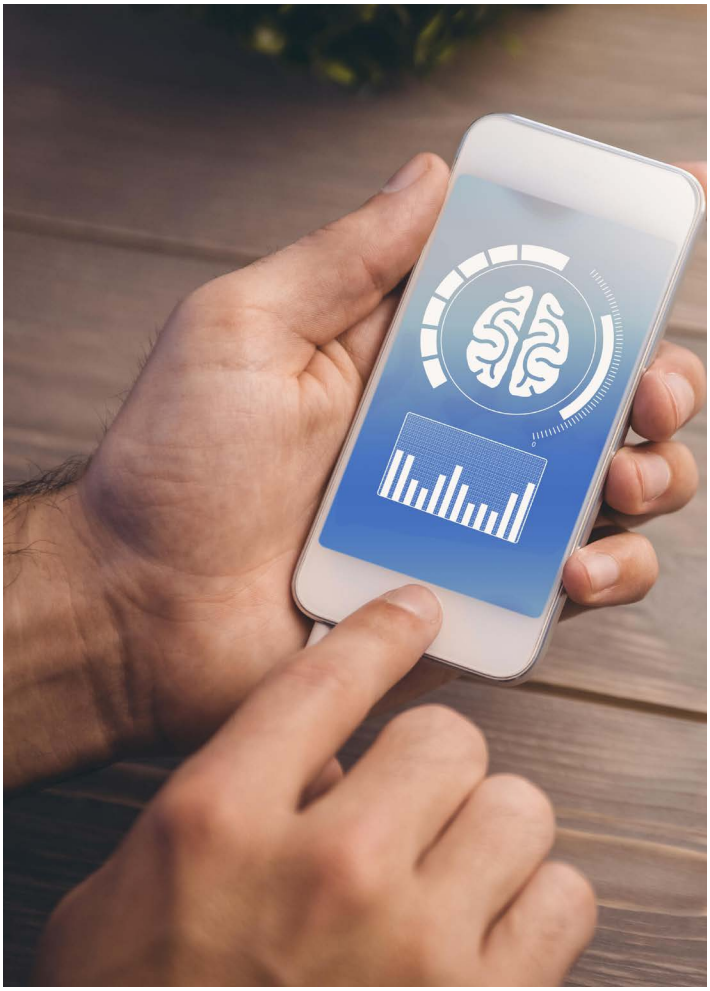
TTP

El monitoreo que hizo Deloitte a foros subterráneos reveló la actividad de numerosos atacantes que fueron observados solicitando PHI en foros criminales o buscando monetizar PHI robada, o pidiendo acceso a sistemas de PHI ya comprometidos. Los foros criminales clandestinos facilitan esta monetización al entregarles a los atacantes un mercado donde comprar, vender y comercializar datos de EHR/PHI.

- Los atacantes se valen de malware de robo de información y correos electrónicos de phishing para robar las credenciales (nombres de usuario y contraseñas) de víctimas.
- Las credenciales robadas se usarán en ataques de repetición de contraseñas o de relleno de credenciales para acceder a las cuentas de sus víctimas.

Recomendaciones

- Usar filtros de correo electrónico para bloquear los adjuntos de Microsoft Office habilitados para macros cuyo origen sea externo a la organización. Estos documentos suelen utilizarse para que descarguen o instalen malware, incluidos los documentos de Word, Excel, PowerPoint y Publisher.
- Uso de una contraseña fuerte: Configurar todas las contraseñas administrativas para que sean largas, complejas y se deban cambiar periódicamente. Antes de implementar cualquier dispositivo nuevo en un entorno de red, es necesario cambiar todas las contraseñas predeterminadas.
- Educar a los usuarios: Las capacitaciones continuas de los usuarios finales ayudan a educarlos. Ellos tomarán más conciencia para detectar intentos de ingeniería social, correos electrónicos de phishing malicioso y páginas web sospechosas, lo que permite tomar medidas a tiempo.



25.- Combo List - Aggregated lists username/password combinations used in account-checking attacks

Amenazas persistentes avanzadas (APT)

El robo de propiedad intelectual y datos sensibles de PII/PHI sigue siendo una tendencia importante en las APT dirigidas a la industria de SALUD Y CIENCIAS DE LA VIDA. Las organizaciones de SALUD Y CIENCIAS DE LA VIDA son blancos permanentes de las amenazas persistentes avanzadas (APT) respaldadas por Gobiernos en operaciones de ciber-espionaje que intentan robar propiedad intelectual valiosa, como datos farmacéuticos o biomédicos, datos de propiedad de dispositivos médicos, o información sensible de PII y PHI de individuos. El interés de las APT en organizaciones de esta industria surge de la motivación de robar propiedad intelectual valiosa para sostener sus negocios domésticos y darles una ventaja competitiva.
El acceso persistente durante largos períodos de tiempo habilita a los atacantes a que roben procesos comerciales privados, tecnologías innovadoras, datos de clientes y otras propiedades intelectuales para permitir que sus socios locales ganen ventaja competitiva en el mercado. La logística de la cadena de suministro, los procesos de manufacturación y los detalles de negocios programáticos pueden todos ser usados por competidores externos para replicar estos procesos o identificar fallas. En 2017, se detectó una APT china que aprovechó el troyano de acceso remoto (RAT) PlugX para apuntar a organizaciones farmacéuticas en Vietnam y robar fórmulas farmacológicas e información comercial sensible.

Otra motivación de las APT para apuntar a las organizaciones de salud es reunir información sensible de PII/PHI, particularmente de individuos del gobierno de EEUU.
Esta información es de sumo interés para las APT ya que les permite identificar objetivos vulnerables para el reclutamiento de espionaje humano debido a las dificultades financieras que pueden resultar de las costosas facturas de atención sanitaria. En particular, les resulta especialmente atractiva la PII y PHI de individuos de diversos países con acceso a información acerca de asuntos gubernamentales y militares.

Su interés en el sector de atención de la salud de EEUU pudo haber motivado en 2014 el ataque del grupo chino APT18 a los sistemas de salud de los Community Health Systems y la violación masiva de datos del grupo chino Deep Panda a la organización de seguros de salud Anthem BSBC, una aseguradora proveedora de la mayoría de los empleados federales estadounidenses que participaban en el programa de beneficios de salud para empleados federales.

TTP

A diferencia de la mayoría de los atacantes, las APT suelen perseguir sus objetivos durante meses o años. Para lograr sus objetivos, las APT también aprovechan malware sofisticado y personalizado, como herramientas de acceso remoto (RAT) o malware de robo de información. La sofisticación de las APT les permite adaptarse a cambios en las ciber-defensas de su objetivo. Además, son persistentes en su ataque contra la misma víctima hasta cumplir su propósito. Al permanecer escondidas en un entorno comprometido por largos períodos, las APT también representan una amenaza importante para la propiedad intelectual y las tecnologías privadas de una organización debido a sus avanzadas capacidades de extracción de datos.

Recomendaciones

- Segmentación de la red: Implementar la segmentación de red y desplegar firewalls para mitigar el riesgo que suponen los autores de amenazas avanzadas.

- Controles de acceso: Implementar controles de acceso según el rol, canales seguros de acceso remoto, monitoreos e inicios de sesión robustos y eficientes en los sistemas para limitar la eficacia de explotaciones, amenazas avanzadas y aumentar la probabilidad de detección.

- Prevención y detección: Implementar contramedidas para mitigar ataques en el perímetro de la red. Esto incluye reglas de firewall utilizadas para bloquear puertos en desuso y denegar pedidos de HTTP para puertos no estándar, filtrado de contenido para permitir que los usuarios solo accedan a sitios confiables, restricción a usuarios para navegar con privilegios de administrador local en las máquinas, y sistemas de prevención de intrusión para detectar tráfico malicioso y bloquearle el ingreso al entorno.

- Sistemas de prevención de intrusión y antivirus - La verificación de los sistemas de prevención de intrusión y antivirus se actualizan automática y periódicamente con los últimos juegos de firmas, y se configuran para bloquear activamente la actividad de los kits de explotación (EK). Utilizar sistemas de prevención de intrusión (IPS) en el canal web saliente para evitar que los EK envíen malware a las máquinas víctima.

- Los IPS también pueden bloquear las comunicaciones que utilizan las instalaciones de malware, así como los sistemas de comando y control y de proxi inverso que usan como canales.

- Los datos reunidos a partir de alertas, como dominios, patrones de URL, direcciones de IP y hashes binarios, se pueden reutilizar e introducir en otros controles.

Ataques contra dispositivos y aplicaciones específicas de atención médica

La cantidad de incidentes que involucran ataques dirigidos a dispositivos médicos vulnerables que funcionan en sistemas operativos antiguos para ganar acceso a redes hospitalarias y robar datos de pacientes continúa siendo una tendencia clave. Las aplicaciones y los dispositivos médicos vulnerables aumentan el umbral de riesgo de las organizaciones de salud , particularmente, proveedores de atención sanitaria. Este riesgo se puede atribuir a aplicaciones y dispositivos médicos antiguos que suelen funcionar en sistemas operativos de Windows desactualizados y no compatibles. Cuando las redes clínicas se segmentan incorrectamente, tienen un mayor riesgo de ser blancos de ataque ya que los sistemas desactualizados e incompatibles que funcionan en ellas las hacen más vulnerables y son más fáciles de explotar que un sistema actualizado y al día. Además, los ataques a aplicaciones y dispositivos médicos también ponen en grave riesgo la disponibilidad de las aplicaciones críticas de la misión de las organizaciones de asistencia de la salud, que son vitales para la seguridad del paciente, y la confidencialidad e integridad de los datos del paciente.

En 2018, Deloitte señaló múltiples informes de vulnerabilidad para aplicaciones y dispositivos médicos, incluidas las vulnerabilidades heredadas de la ejecución de estas aplicaciones en versiones de Windows desactualizadas e incompatibles. En particular, registró varias instancias donde el código de explotación activo para estas vulnerabilidades se publicó en menos de 24 horas de revelada la vulnerabilidad. Los ejemplos de MEDJACK y Siemens Healthineers a continuación brindan una idea más profunda en cuanto a la selección de dispositivos médicos como objetivos de explotaciones y otros agentes de amenazas.

Malware MEDJACK de secuestro de dispositivos médicos ataca redes de atención médica

En febrero de 2017, Deloitte informó acerca de una última versión del malware MEDJACK.3 que se estaba usando para atacar dispositivos médicos como puntos de entrada a las redes de atención de la salud. En estos ataques, el blanco fue un sistema de 10 hospitales y dispositivos médicos vulnerables como el sistema PACS de visualización de imágenes para obtener acceso a las redes más amplias del hospital. Una vez comprometidas las redes, los atacantes robaron rápidamente grandes cantidades de datos de pacientes y continuaron moviéndose lateralmente por las redes de los sistemas del hospital usando un malware autoprogramable altamente personalizado. Este malware fue diseñado para diseminarse a nuevos dispositivos dentro de la red atacada cada tres horas usando una vulnerabilidad no identificada en “svchost.exe” que habilitaba un código de ejecución remoto si se activaba la función para compartir archivos. También se podía diseminar por unidades asignadas o desmontables y por ataques “pass the hash” o contraseñas débiles. El malware intenta dejar una copia de sí mismo en el recurso compartido “admin$” de un dispositivo seleccionado como objetivo usando las credenciales del perfil de usuario activo. Si este intento falla, intentará comprometer las credenciales de otras cuentas de usuario con el uso de tácticas de fuerza bruta y lista codificada de contraseñas.

Los malware como MEDJACK están específicamente diseñados para atacar y sacar provecho de dispositivos médicos vulnerables como monitores cardíacos, tomógrafos y resonadores, bombas de insulina y sistemas de archivo y comunicación de imágenes (PACS) que funcionan en sistemas operativos antiguos o desactualizados como Windows XP y Windows Server 2003. Ignora deliberadamente a los sistemas operativos nuevos.

Las versiones previas del malware MEDJACK como MEDJACK.2 atacaban a los hospitales a través de dispositivos médicos vulnerables, en especial máquinas de rayos X y sistemas de radiología fluoroscópica. Los ataques del MEDJACK.2 explotaron la vulnerabilidad CVE-2008-4250 que afectaba a Windows 2000, Windows XP y Windows Server 2003. Estos ataques evadieron la detección en un hospital afectado a pesar de que tuviera IDS actualizados, firewalls nuevos y dispositivos protegidos porque las soluciones de seguridad no estaban configuradas para emitir alertas en estos sistemas operativos antiguos.

Vulnerabilidades explotables de Windows afectan Molecular Imaging Products de Siemens Healthineers

En julio de 2017, la compañía de tecnología médica Siemens Healthineers publicó dos avisos advirtiendo a sus clientes de que sus productos de imágenes moleculares eran vulnerables a fallas críticas en los sistemas automatizados de Windows XP, Windows 7 y HP usados frecuentemente para alojar el software de Siemens. Las aplicaciones afectadas de obtención de imágenes suelen usarse en entornos clínicos con el fin de obtener imágenes diagnósticas. Los avisos advertían que la explotación exitosa de las vulnerabilidades en estos sistemas podría dar lugar a que los atacantes ejecutaran de manera remota un código binario en el sistema objetivo.

En el primer aviso de vulnerabilidad que publicó Siemens en julio de 2017, se identificaron dos vulnerabilidades críticas como CVE-2008-4250 y CVE-2017-7269. En el caso de CVE-2008-4250, el código de explotación se publicó recién a un mes de que se revelara la vulnerabilidad en octubre de 2008. El código de explotación había estado disponible durante una década en repositorios de código abierto antes de que Siemens publicara su aviso acerca de los efectos cascada de la vulnerabilidad en sus productos de obtención de imágenes moleculares. En los 10 años previos al aviso de Siemens, CVE-2008-4250 fue explotado por múltiples grupos, incluidos los agentes responsables del desarrollo y la distribución del gusano Conficker.

En el caso de CVE-2017-7269, la vulnerabilidad se informó el 26 de marzo de 2017. Su código de explotación se publicó un día después, el 27 de marzo de 2017, y aproximadamente tres meses más tarde, el 13 de junio de 2017, Microsoft publicó un parche para esta vulnerabilidad. Un mes después de la publicación del parche, en julio de 2017, Siemens publicó el aviso antes mencionado para sus clientes. Antes de la publicación del boletín de seguridad de Microsoft con la corrección para CVE-2017-7269, los atacantes aprovecharon esta vulnerabilidad para hacer minería XMRig de la criptomoneda Monero.

TTP

- Los atacantes escanean las redes hospitalarias para identificar dispositivos médicos vulnerables que funcionan en sistemas operativos antiguos y desactualizados como Windows XP, 2008, 2012 y Windows Server 2003; los propagadores de malware se implementan para ignorar a los sistemas operativos más nuevos y que solo apunten a los sistemas operativos viejos.

- Las vulnerabilidades en los sistemas operativos más viejos de Windows se explotan para introducir malware especialmente diseñado, como el MEDJACK que apunta a dispositivos médicos que se utilizan como puntos de entrada a redes hospitalarias.

- Los atacantes roban datos de pacientes aprovechando el malware de autopropagación para moverse lateralmente a través de las redes hospitalarias comprometidas; el malware se disemina a través de unidades asignadas o desmontables mediante ataques "pass the hash" o contraseñas débiles, o a través del compromiso de credenciales de otras cuentas de usuarios con tácticas de fuerza bruta, usando una lista codificada de contraseñas.

Recomendaciones

- Realizar la transición para dejar atrás sistemas operativos antiguos no compatibles y desconectar redes de productos vulnerables hasta que se puedan actualizar a versiones compatibles.

- Aplicar parches apropiados que haya lanzado el fabricante original (OEM) para todas las vulnerabilidades del sistema operativo y del software de aplicación.

- Mantener regularmente una práctica de gestión de vulnerabilidades y ciclos de actualizaciones para todos los sistemas operativos, los softwares de seguridad y otros softwares de aplicación.

- Evitar el movimiento lateral en las redes a través de la implementación del control de acceso (AC) y la gestión de identidad y acceso (IAM) con el fin de evitar que los privilegios de redes y los permisos de unidades compartidas contengan infecciones de dispositivos. Otorgar a los usuarios los privilegios locales mínimos que necesiten para cumplir su función.

Amenazas inter-industria

Ransomware

Los ataques de ransomware a la industria de salud continuaron en aumento. La tendencia detrás de estos ataques con motivación financiera ha sido la interrupción de las redes hospitalarias de misión crítica y el secuestro de datos de pacientes. Las organizaciones de este sector como los grandes hospitales suelen tener redes que dependen en gran parte del EHR y de dispositivos médicos en red. Esto genera la necesidad de mantener la continuidad de red, lo cual convierte a esta industria en un objetivo particularmente atrayente para campañas de ransomware. En 2017, el ataque del ransomware WannaCry al Servicio Nacional de Salud (NHS) del Reino Unido causó una grave interrupción que efectivamente paralizó su red.

Los distribuidores de ransomware saben el enorme impacto, la publicidad y la notoriedad que logran a partir de una interrupción, incluso de corto plazo, en los procesos de misión crítica de una organización de **Salud y Ciencias de la Vida** . En consecuencia, los atacantes creen que estas organizaciones son objetivos valiosos y altamente visibles de los cuales pueden esperar cooperación ante la exigencia de altas sumas de dinero a cambio. Durante el último año, Deloitte informó más de 350 incidentes de ransomware y más de 25 incidentes directamente relacionados con hospitales y organizaciones de la salud. También en 2018 detectó a múltiples atacantes que experimentaron con métodos alternativos de distribución y modelos de negocios al tiempo que simplificaban las interfaces del ransomware. Estos cambios permiten que el desarrollador del ransomware disminuya significativamente el umbral de ingreso para su distribución y abra el mercado a atacantes inexpertos que carecen del conocimiento técnico para desarrollar, adquirir o implementar ransomware. Para incrementar la participación de mercado, los desarrolladores de ransomware modificaron su software para ofrecer capacidades complementarias. Esto permite ofrecer un juego de servicios maliciosos conjuntamente con el ransomware, conocido como Ransomware como servicio (RaaS).

Si bien los métodos de distribución de los correos electrónicos de spam y los kits de explotación siguen siendo efectivos y aún se utilizan, Deloitte también observó un notable incremento en el uso del protocolo de escritorio remoto (RDP) para la distribución de ransomware. Aunque la técnica no es nueva, su popularidad ha crecido a mediados de 2017 y ofrece varias ventajas como vector de infección alternativo. El RDP también se puede aprovechar para que incremente las posibilidades de éxito de ataques más dirigidos.

Muchas familias de ransomware están incorporando capacidades de auto-propagación y procesos de encriptación que no requieren intercambio de claves para encriptar los datos de una víctima. Ambas técnicas hacen que las medidas preventivas tradicionales sean ineficientes, ya que los métodos tradicionales ponen el foco en detectar o bloquear los intercambios de claves, dirigir y controlar (C2) las comunicaciones.

TTP

Los ataques de ransomware están diseñados para interrumpir las operaciones. Sacan ventaja del valor de los datos de la víctima al encriptar archivos importantes de su propiedad y mantienen secuestrada esa información hasta que se realiza el pago del rescate. Suelen estar involucrados las siguientes TTP:

- Los vectores de infección típicos de ransomware incluyen campañas de correos electrónicos spam con enlaces o adjuntos maliciosos; kits de explotación, compromiso de fuerza bruta de servicios de RDP, explotación oculta de web y ataques remotos de servicios.
- Los formatos típicos de estos adjuntos maliciosos incluyen archivos de Microsoft Office habilitados para macros, archivos JavaScript, y archivos .rar o .zip. Algunas familias de ransomware se pueden autopropagar a través de unidades de red o medios extraíbles.
- Los operadores que apuntan a empresas específicas, como los operadores del ransomware SamSam, pueden escanear o sondear dispositivos accesibles, particularmente servidores JBoss, en busca de vulnerabilidades o contraseñas débiles.

Recomendaciones

Una táctica clave para reducir el potencial impacto de un incidente de ransomware es la capacidad de reemplazar con backups los datos afectados. Las organizaciones deben verificar que los backups no estén conectados a los sistemas que pudieran infectarse en el caso de un ataque a nivel de red.

- Educar a los usuarios: Aconsejar a los usuarios que desconfíen de mensajes de correo electrónico inesperados y que los validen con los correspondientes remitentes a través de canales independientes antes de abrir cualquier enlace o adjunto.
- Política de no pago de rescate: No pagar rescates a operadores de ransomware ya que ellos podrían no estar dispuestos o capacitados para desencriptar los archivos. Los pagos de rescate pueden incluso fomentar más ataques.
- Plan de backups: Confiar en los backups frecuentes, segmentados y redundantes como la mejor manera de recuperar archivos encriptados en el caso de una infección por ransomware.
- Restricción de servicios no críticos: Deshabilitar el RDP y otros servicios y puertos a menos que los usuarios los necesiten para tareas específicas.

Troyanos de acceso remoto y malware de robo de información

Deloitte observó una creciente tendencia en el malware de robo de información (info-stealing) combinado con otros módulos de malware para atacar y robar datos valiosos de PHI/EHR propios de organizaciones de **Salud y Ciencias de la Vida** .
Los troyanos de acceso remoto y los malware de robo de información están entre los más usados en los ataques a este tipo de organizaciones. Esto se debe a que ambos se pueden usar para lograr múltiples objetivos a la vez que se extrae sigilosamente información sensible de la red atacada. En los foros clandestinos se pueden hallar info-stealers disponibles y listos para comprar a un precio de entre 100 y 400 usd, los cuales brindan un mecanismo simple pero efectivo para lograr ataques tanto a baja como a gran escala.

Deloitte también señaló un aumento de las capacidades del info-stealer incorporadas a otros grupos de malware de mercancías. La amenaza de malware de robo de información y de troyanos de acceso remoto se ve exacerbada por esta creciente tendencia de variantes modularizadas de malware. Las variantes modulares multi-amenaza se están volviendo cada vez más comunes porque permiten que los atacantes realicen una variedad de actividades maliciosas en un sistema comprometido para lograr su

objetivo. Los info-stealers están entre las funcionalidades modularizadas incorporadas con más frecuencia.
Este desarrollo aumenta la amenaza del robo de EHR que enfrentan las organizaciones de salud como los proveedores de atención de la salud.

Algunos de los objetivos que buscan lograr los atacantes al implementar info-stealers incluyen la recolección de contraseñas que sirvan para la elevación de privilegios, el movimiento lateral o la venta en el mercado negro. Asimismo, los atacantes pueden usar este tipo de malware para cargar pulsaciones de teclas, hacer capturas de pantallas de sistemas y atacar a tipos específicos de archivos para el robo de PHI, EHR y otros datos sensibles. En 2017, Deloitte registró múltiples incidentes donde se implementaron malwares de robo de información y troyanos de acceso remoto dentro de la red de una organización de atención de la salud.

TTP

- Info-stealers y RAT son los malware usados con mayor frecuencia para atacar a los proveedores de servicios de la salud debido a la propiedad intelectual sensible y a los procesos comerciales que se almacenan en sus redes.

- Los datos de PHI/EHR que están en manos de las organizaciones de salud, las convierten en un objetivo central para las campañas de malware de robo de información. Para defenderse contra este malware, las organizaciones deben considerar lo siguiente:

Recomendaciones

- Monitoreo y lista negra: El monitoreo y potencial bloqueo de ciertas extensiones de archivos adjuntos en la puerta de enlace del correo electrónico puede limitar la probabilidad de recibir archivos maliciosos a través de campañas de correos electrónicos de spam.

- Educar a los usuarios: Las capacitaciones continuas de los usuarios finales ayudan a educarlos. Los usuarios tomarán más conciencia para detectar intentos de ingeniería social, correos electrónicos de phishing malicioso y páginas web sospechosas, lo que permite tomar medidas a tiempo.

- Implementar fuertes controles de gestión de acceso: Solicitar contraseñas fuertes y complejas y habilitar la autenticación de factor doble para credenciales sensibles.

- Encriptación de datos: Encriptar datos del EHR y cualquier otra información altamente sensible inactiva o en uso.

Malware de punto de venta (POS)

La tendencia de ataques de malware de punto de venta a organizaciones de **Salud y Ciencias de la Vida** siguen creciendo a medida que se incrementan los ataques dirigidos a los sistemas de PoS para el robo de datos sensibles de tarjetas de pago y PHI. Este tipo de malware es una de las principales fuentes de datos robados de tarjetas de pago que los ciber-criminales intercambian en el mercado negro. Quienes dirigen los ataques y comprometen a los sistemas de PoS pueden monetizar fácilmente los datos robados de tarjetas de pago en el mercado negro. Si bien los servicios y kits de malware de PoS han estado disponibles en foros clandestinos desde principios del 2000, diversas violaciones a PoS a gran escala en múltiples organizaciones de venta minorista y cadenas de hoteles han puesto a estas amenazas bajo la lupa.

Los ataques a PoS no se limitan a la industria minorista y hospitalaria. La posibilidad de obtener datos sensibles de tarjetas de pago en combinación con PHI sensible que se alojan en la misma red hace que las organizaciones de atención sanitaria sean un objetivo principal para el malware de PoS. Deloitte informó anteriormente acerca de dos incidentes de PoS que aprovecharon este malware para atacar a organizaciones de la industria de **Salud y Ciencias de la Vida**.

Incidente de PoS "Banner Health" - En agosto de 2016, Deloitte informó acerca de un compromiso del PoS de "Banner Health" que expuso la información de tarjetas de pago de más de 3,7 millones de personas. El proveedor de atención sanitaria con base en Phoenix, Arizona reveló que el acceso no autorizado a la información de salud comenzó con el compromiso de los sistemas de PoS de la organización que residía en sus locales de servicios de comida; los atacantes se movieron lateralmente para comprometer la información sensible de pacientes[26]. El ataque fue descubierto por Banner Health el 7 de julio de 2016, cuando el sistema de procesamiento de tarjetas de pago en uno de los puntos de venta de alimentos y bebidas de la organización expuso información que incluía números de tarjetas de crédito, nombre de titulares de tarjetas, fechas de vencimiento y códigos de verificación. El 13 de julio de 2016, una investigación reveló que los atacantes probablemente habían obtenido acceso no autorizado a información de pacientes, información de beneficiarios y miembros de planes de salud e información acerca de médicos y proveedores de atención sanitaria. De acuerdo con Banner Health, la información de pacientes y planes de salud pudo haber incluido nombres, fechas de nacimiento, direcciones, nombres de médicos, fechas de servicios, información de reclamos y, posiblemente, información de seguros de salud y números de seguridad social.

Troyano bancario Kronos ataca con ScanPOS - En noviembre de 2016, Deloitte informó acerca de diversas campañas de phishing con un nuevo malware de punto de venta (PoS) llamado "ScanPoS" a través del uso del troyano bancario Kronos. Esta campaña atacó principalmente a usuarios en las industrias de atención sanitaria, hospitales, educación y servicios financieros en el Reino Unido y América del Norte[27]. En una de dichas campañas, los correos electrónicos de spam incluían documentos adjuntos de Microsoft Word habilitados para macros o un enlace a un sitio falsificado de Microsoft SharePoint que se usaba para descargar documentos similares. El malware ScanPoS es capaz de extraer datos de tarjetas de pago de la memoria de procesos en ejecución que son más tarde enviados de vuelta a los servidores de Command & Control (C2) vía HTTP.

A pesar de los mejores esfuerzos realizados por la industria de tarjetas de pagos para mejorar las tecnologías y ajustar los estándares de seguridad, aún persisten las vulnerabilidades y las fallas de seguridad en los sistemas de PoS. En consecuencia, las organizaciones que implementan sistemas de PoS quedan expuestas al riesgo debido a estas debilidades además de una infraestructura de TI segmentada de manera inapropiada.

26.- Deloitte Threat Report, Banner Health Suffers Data Breach, G-TR-EN-16-00703, 4 de agosto de 2016.

27.- Deloitte Threat Notification, New PoS malware "ScanPoS" delivered by Kronos banking Trojan, G-TN-EN-16- 01053, 6 de noviembre de 2016.

TTP

- Las familias de malware de PoS suelen distribuirse a través de correos electrónicos de spam malicioso o kits de explotación, y suelen descargarse al host remoto como una carga útil secundaria.

- Las familias de malware de PoS más recientes surgidas en 2018 incluyen PinkKite, con su pequeña carga útil de solo 6 KB; y UDPoS, que usa consultas del DNS (sistema de nombres de dominio) a través del protocolo UDP para sus comunicaciones C2

Recomendaciones

- Segmentación de la red: Ejecutar los servicios de PoS en un host físico o lógico separado.

- Restringir el acceso de sistemas de PoS a Internet: Verificar cualquier servidor que sea visible desde Internet o red sospechosa y, si no es necesario para los fines comerciales, moverlo a un VLAN interno y asignarle una dirección privada.

- Software actualizado: Ejecutar herramientas de escaneo automático de vulnerabilidades en todos los sistemas de la red de forma semanal o con mayor frecuencia. Elaborar listas de las vulnerabilidades más críticas en orden de prioridad y entregárselas al administrador responsable de sistemas.

- Lista blanca de aplicaciones: Implementar una solución de lista blanca de aplicaciones que permita que los sistemas ejecuten un software sólo si está incluido en la lista blanca y que evite la ejecución de cualquier otro software en el sistema.

- Uso de una contraseña fuerte: Configurar todas las contraseñas administrativas para que sean largas, complejas y se deben cambiar periódicamente. Antes de implementar cualquier dispositivo nuevo en un entorno de red, cambiar todas las contraseñas predeterminadas.

- Monitoreo de tráfico: Garantizar que el tráfico entrante/saliente esté logueado para determinar si los puertos de destino son víctimas de un ataque de fuerza bruta o están asociados con tres paquetes mal formados durante un intervalo de 90 a 100 segundos.

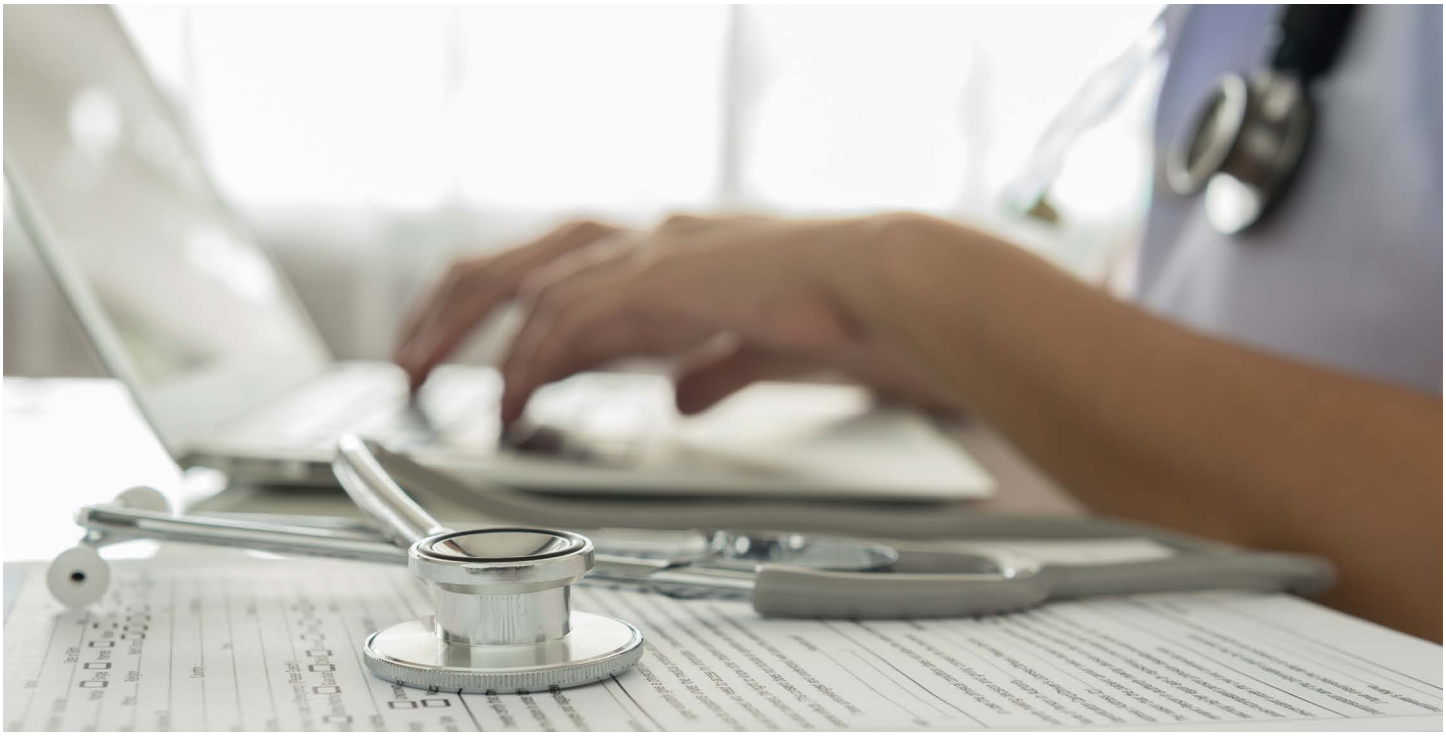
Evaluación

La industria de **Salud y Ciencias de la Vida** enfrenta una variedad de riesgos y amenazas propios de los servicios que proveen y de los datos que guardan. Desde las organizaciones de atención de la salud a las farmacéuticas, de dispositivos médicos y aseguradoras, hasta las de investigación y desarrollo (R&D), cada una de las organizaciones de salud tiene un perfil de riesgo y un escenario de amenazas únicos. Los nuevos desarrollos y las innovaciones en la industria de la salud ofrecen no solo nuevas oportunidades sino también nuevos desafíos. Por ejemplo, si bien los dispositivos médicos portátiles, los análisis de datos en tiempo real y la facilidad del uso de portales electrónicos en línea cada vez más accesibles de pacientes ayudan tanto a consumidores como a organizaciones, también amplían la superficie de ataque.

Muchos atacantes han demostrado tener el conocimiento y el dominio para dirigir ciber-ataques contra organizaciones de Salud u Ciencias de la Vida, incluso la capacidad de explotar vulnerabilidades y robar datos de PHI/EHR sensibles y rentables y propiedad intelectual valiosa. Los desafíos existentes agravan la vulnerabilidad y el riesgo propios de este tipo de organizaciones, como los sistemas operativos antiguos usados para alojar dispositivos y aplicaciones cuyo diseño original no tuvo en cuenta la ciberseguridad.

Tal como se vio en el escenario de amenazas del sector de la salud, las tácticas, técnicas y procedimientos (TTP) que usan los adversarios también están en constante desarrollo y se vuelven cada más más sofisticadas para evadir las defensas tradicionales. Con miras al futuro, las organizaciones en la industria de **Salud y Ciencias de la Vida** continuarán siendo un objetivo atractivo y lucrativo para los atacantes. Su percepción como un objetivo vulnerable y fácil y una fuente altamente rentable de datos de pacientes aumenta significativamente su riesgo y, probablemente, alientan a que los atacantes apunten a ellas con más frecuencia.

La naturaleza altamente dependiente de datos y la creciente transformación de la industria de salud ensalud en tecnologías disruptivas, de innovación como la atención sanitaria virtual, y dependiente de información conducirán casi con certeza a que esta industria sea cada vez más atacada por ciber-criminales y grupos de APT respaldados por Gobiernos. De manera similar, las organizaciones de **Salud y Ciencias de la Vida** seguirán estando en riesgo para atravesar las amenazas a la industria, tales como ransomware, malware de punto de venta (PoS), troyanos de acceso remoto y malware de robo de información, que suponen una amenaza para los servicios que ofrecen y los datos que protegen dichas organizaciones.



Fuentes

Deloitte Threat Report, Breach of hospital system via PACS image viewers, G-TR-EN-17-00188, 17 de febrero de 2017
Deloitte Threat Notification, Windows exploitable flaws affects Molecular Imaging Products from Siemens Healthineers, G-TN-EN-17-02402, 9 de agosto de 2017.

Deloitte Threat Notification, Threat actor "Leak" sells SQLi vulnerabilities targeting multiple healthcare organizations, A-TN-EN-01-6206, 8 de diciembre de 2017.

Deloitte Threat Notification, Threat actor selling scanned copies of 15,000 patient records likely obtained from Texas based healthcare clinic, A-TN-EN-01-5995, 27 de octubre de 2017.

Deloitte Threat Report, Possible Chinese APT sells hospital databases on criminal forum, A-TR- EN-01-5892, 12 de octubre de 2017.

Deloitte Threat Report, Threat Actor Profile: TheDarkOverlord, A-TR-EN-01-5939, 19 de octubre de 2017.

Deloitte Threat Notification, Possible Russian actor managerPR sells PII records of 4,200 US nationals allegedly stolen from Wisconsin hospital, A-TN-EN-01-5942, 20 de diciembre de 2017.

Deloitte Threat Notification, Threat actor "InTheMood" selling database stolen from medical institution, A-TN-EN-17-00154, 10 de febrero de 2017.

Deloitte Threat Notification, Threat actor "Skyscraper" selling pediatric data on criminal forums, G-TN-EN-17-00403, 6 de mayo de 2017.

Deloitte Threat Report, Threat actor tries to extort money from breached healthcare organization, G-TR-EN-16-01021, 8 de noviembre de 2016.

Deloitte Threat Notification, Two new variants of Samsam ransomware discovered, G-TN-EN- 17-02255, 22 de junio de 2017.

Deloitte Threat Study, Ransomware: Holding Your Data Hostage, W-TS-EN-16-00734, 12 de agosto de 2016.

Deloitte Threat Report, Updates to Philadelphia ransomware and possible Brazilian origins of its developer, A-TR-EN-17-00347, 13 de abril de 2017.

Deloitte Threat Notification, Philadelphia ransomware used against US healthcare organization, G-TN-EN-17-00333, 6 de abril de 2017.

Deloitte Threat Notification, Dharma ransomware targeted East Central Kansas Area Agency on Aging, G-TN-EN-01-6035, 6 de noviembre de 2017.

Deloitte Threat Notification, ABCD Pediatrics targeted by Dharma ransomware, G-TN-EN-17- 00328, 5 de abril de 2017.

Deloitte Threat Notification, Backdoor named Dande stealing medication procurement information, G-TN-EN-01-5586, 27 de julio de 2017.

Deloitte Threat Notification, Institute for Women's Health patient data compromised in keylogger infection, G-TN-EN-17-02437, 21 de agosto 2017.

Deloitte Threat Notification, Highly obfuscated infostealer "Retadup" targeting Israeli hospitals, G-TN-EN-17-02275, 29 de junio de 2017.

Deloitte Threat Report, Banner Health Suffers Data Breach, G-TR-EN-16-00703, 4 de agosto de 2016.

Deloitte Threat Notification, New PoS malware "ScanPoS" delivered by Kronos banking Trojan, G-TN-EN-16-01053, 16 de noviembre 2016.

https://www.latercera.com/nacional/noticia/gobierno-alerta-ciberataque-empresa-proveedora-grandes-hospitales/735093/

Contacta a nuestros expertos

Nicolás Corrado
Socio de Cyber de Deloitte
nicorrado@deloitte.com
+56227298665

Antonio Martínez
Líder industrial LSHC en Consulting de Deloitte
amartinezc@deloitte.com
+56227298975

Oficina central

Rosario Norte 407
Las Condes, Santiago
Chile
Fono: +56 227 297 000
Fax: +56 223 749 177
deloittechile@deloitte.com

Regiones

Av. Grecia 860
Piso 3
Antofagasta
Chile
Fono: +56 552 449 660
Fax: +56 552 449 662
antofagasta@deloitte.com

Alvares 646
Oficina 906
Viña del Mar
Chile
Fono: +56 322 882 026
Fax: +56 322 975 625
vregionchile@deloitte.com

Chacabuco 485
Piso 7
Concepción
Chile
Fono: +56 412 914 055
Fax: +56 412 914 066
concepcionchile@deloitte.com

Quillota 175
Oficina 1107
Puerto Montt
Chile
Fono: +56 652 268 600
Fax: +56 652 288 600
puertomontt@deloitte.com

Deloitte.

www.deloitte.cl