CARI / CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

1

SERIE DE ARTÍCULOS Y TESTIMONIOS Nº 140

FEBRERO 2018

Encriptado extorsivo de Historias Clínicas Electrónicas

Un mejor "negocio" para los hackers que la intrusión en los sistemas financieros

Por Roberto Uzal

En este artículo se presenta el problema relacionado con el ciber robo de información y/o ciber bloqueo extorsivo de historias clínicas electrónicas. Se suministran antecedentes que pueden ser útiles a quienes deseen ampliar y/o profundizar el tema. Se advierte que, para los ciber criminales y/o ciber terroristas, el ciber robo de información y/o ciber bloqueo extorsivo de historias clínicas electrónicas constituyen actividades más "rentables" que las intrusiones a sistemas financieros. Se referencian trabajos anteriores realizados por el Comité sobre Criminalidad Organizada Transnacional y por el Instituto de Seguridad Internacional y Asuntos Estratégicos del Consejo Argentino para las Relaciones Internacionales. Finalmente se enumeran conclusiones y se formulan propuestas sobre el tema tratado

Ciber robo de información y bloqueo extorsivo de Historias Clínicas Electrónicas

Desafortunadamente, para las víctimas reales y potenciales, el robo de la información o el bloqueo extorsivo (ransomware) de historias clínicas electrónicas es, para los ciber criminales y/o ciber terroristas más rentable que el robo de la información o el bloqueo extorsivo de archivos pertenecientes a sistemas financieros [1] [2] [3].

El "Hollywood Presbyterian Medical Center" [4] había denunciado en 2016, ante el FBI, haber sido víctima del secuestro extorsivo de archivos mediante ciber armas (malware) del tipo "ransomware". Desafortunadamente, en ese entonces, la forma más expeditiva encontrada para reanudar la efectiva y plena atención de los pacientes fue pagar el monto exigido por los ciber criminales; los extorsionadores exigieron el pago en criptomonedas lo cual contribuyó a incrementar la complejidad del rastreo de dichos pagos (localización / identificación de los extorsionadores). Inmediatamente los ciber criminales, ante el pago "del rescate", suministraron al citado hospital de Hollywood la clave para concretar el desencriptado (liberación de los archivos).

Adicionalmente, los importantes ataques globales realizados durante el año 2017, utilizando herramientas orientadas al secuestro extorsivo de archivos y bases de datos (ransomware), ratificaron, entre otras cosas, la extrema vulnerabilidad de las instituciones de salud ante este tipo de ciber agresiones [5].

Scientific American [6], específicamente, ha ratificado que, los hospitales en general y los dispositivos comprendidos en "aparatología médica" en particular, son extremadamente vulnerables a las ciber agresiones. Este aspecto ha sido tratado en profundidad y ampliado por la Universidad de Harvard [7].

La historia clínica electrónica [8] ha pasado a ser de uso generalizado. Esto agiliza la labor de los profesionales de la medicina y redunda en el incremento de la calidad de los servicios recibidos

CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

Uruguay 1037, piso 1º
C1016ACA
Buenos Aires
República Argentina

Tel. +5411 4811 0071
Fax +5411 4815 4742

cari@cari.org.ar
cari.org.ar

por los pacientes. Claro que "la otra cara" de la historia clínica electrónica es que la misma ha devenido en un blanco altamente valorado por los ciber criminales y en algunos casos por los ciber terroristas. La extorsión de pacientes individuales, hábilmente seleccionados considerando su solvencia económica, constituye un "negocio muy rentable" para el ciber crimen organizado transnacional.

Los ciber ataques masivos de mayo y junio de 2017 afectaron a más de cien países. Se bloquearon, mediante encriptado, archivos y bases de datos muy sensitivos con fines extorsivos. Algunos de quienes estudiaron el tema llegaron a formular la hipótesis de que se habían utilizado, como niveles de gerenciamiento intermedio de dichos ciber ataques, ciber armas modulares [9][10][11].

En caso de utilizarse un enfoque análogo al de 2017, pero orientado esta vez al bloqueo de decenas de miles o cientos de miles de historias clínicas electrónicas, las consecuencias podrían ser globalmente devastadoras.

Estar preparados para evitar la repetición de agresiones del tipo de las ocurridas en mayo y junio de 2017 es posible y además estrictamente necesario. Este aspecto debe ocupar un lugar prioritario en la ciber estrategia de nuestro país. Se debe evitar el robo o el bloqueo de historias clínicas electrónicas y de toda otra información en formato magnético relacionada con la medicina (resonancias magnéticas nucleares, tomografías computadas, ecografías, etc.). Éste debe ser un tema de gran preocupación, tanto del área Defensa como del área Seguridad. Los orígenes de estos ataques son, en principio, indistinguibles; los estados naciones suelen disimular sus agresiones confiriéndoles características de ciber crímenes transnacionales; un trabajo conjunto Defensa / Seguridad resulta imprescindible.

Conclusiones y propuestas

- En instituciones hospitalarias que atienden a pacientes con alto nivel adquisitivo, la extorsión tipo "ransomware" individual es claramente más rentable que la extorsión a la institución como un todo.
- El ciber robo de información y el bloqueo extorsivo de historias clínicas electrónicas constituyen temas de alta prioridad a ser contemplados en la ciber estrategia de nuestro país.
- El ciber robo de información y el bloqueo extorsivo de historias clínicas electrónicas constituyen actividades que resultan sumamente atractivas tanto a ciber criminales como a ciber terroristas.
- El ciber robo de información y el bloqueo extorsivo de historias clínicas electrónicas constituyen, en principio, típicos ejemplos de acciones del "crimen organizado transnacional".
- No resulta siempre posible distinguir el origen del ataque y la motivación del mismo. Las incumbencias de Defensa y Seguridad en principio están superpuestas. Un contexto cooperativo es necesario para enfrentar situaciones del tipo "ransomware".
- La ciber seguridad en instituciones hospitalarias que utilicen historias clínicas electrónicas deben ser adecuadamente auditadas.
- Esquemas de detección de ciber agresiones del tipo "ransomware" deben estar instalados y puestos a puntos. Esquemas basados en "Análisis de Flujo de Redes" suelen ser efectivos. "Análisis de Flujo de Redes" se basa en la detección de "patrones estadísticos" del comportamiento de los routers de las redes vinculadas, en este caso, al sistema de la historia clínica electrónica.

Referencias

[1] http://www.modernhealthcare.com/article/20170410/NEWS/170419987
[2] http://www.netstandard.com/hackers-want-medical-records/
[3] https://blog.trendmicro.com/why-hackers-are-increasingly-targeting-electronic-health-records/
[4] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[5] http://fortune.com/2017/05/15/ransomware-attack-healthcare/
[6] https://www.scientificamerican.com/article/u-s-hospitals-not-immune-to-crippling-cyber-attacks/
[7] http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf
[8] http://rassalud.com/web/ads/historia-clinica-electronica-ras-salud/
[9] http://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2017/02/170216-Boletin-Triarius-0002.pdf página 14
[10] https://www.youtube.com/watch?v=kEY7r9I2jqQ
[11] http://www.cari.org.ar/organos/comitecot.html

Roberto Uzal / Miembro del Comité sobre Criminalidad Organizada Transnacional y del Instituto de Seguridad Internacional y Asuntos Estratégicos del Consejo Argentino para las Relaciones Internacionales.
Director de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires.
Investigador Categoría I (Programa de Incentivo a la Investigación en Universidades Nacionales de Argentina.