Playbook del hacker: me cuelo en tu dispositivo médico (Parte 3/4)

Previamente, en el Playbook del hacker… En el capitulo 2 vimos como a través de un dispositivo médico se podía interrumpir la actividad de un hospital mediante ataques DDoS. Hoy os publico el tercer escenario:

Robo de datos en red a través de dispositivos médicos.

Los hospitales almacenan miles de registros que contienen información sensible de índole financiera, médica y de identidad, lo que los hace convertirse en un objetivo tentador para los ciberdelincuentes. Estas redes por lo general están fuertemente protegidas, haciéndolas objetivos difíciles de atacar. Pero, ¿qué pasa cuando conectamos un dispositivo inseguro en la robusta red de un hospital? Los hackers buscan estas alternativas inseguras para una vez dentro de ellas pivotar y entrar dentro de la propia red. Con esto se deduce que la motivación principal de hackear un dispositivo médico sea el robo de datos. En la mayoría de casos, los hackers no buscan la información médica que almacenan estos dispositivos, si no una entrada a los registros que contienen información financiera y de identidad que puedan vender en el mercado negro.

TrapX Security, una compañía especializada en ciberseguridad, ha encontrado y analizado 3 incidentes en distintas instituciones médicas que han sido objeto de ciberataques a través de sus dispositivos médicos.

1. En el primer ataque analizado el ataque se hizo por medio de tres analizadores de gas en sangre. Los atacantes usaron estos dispositivos como puerta trasera a la red del hospital
   . Además, instalaron malware adicionalmente, como Zeus y Citadel, y robaron una cantidad indeterminada de datos sin ser detectados. La información robada se llevó a un servidor en Europa.
2. El segundo caso es un ataque al sistema de archivo y comunicación de imágenes (SACI). Este sistema provee imágenes al departamento de radiología

   Máquina de rayos X

   de múltiples dispositivos (como ejemplos: equipos de Rayos X, ultrasonido, resonancia magnética y tomografía computarizada), y por lo tanto está conectado a la red de la organización. Esto hace que sea un objetivo perfecto para ciberataques. Infectando el SACI, los atacantes lograron acceso no autorizado al puesto de trabajo de una enfermera, extrayendo datos de este sin ser detectado. Los datos robados esta vez fueron a parar a un servidor chino. Los investigadores determinaron que los atacantes violaron la seguridad después de que un empleado visitara

una web maliciosa preparada para enviar malware. La amenaza fue eliminada por los sistemas de seguridad del hospital, pero no antes de que infectara el SACI, y como el SACI no podía ser escaneado ni remediado, el sistema se convirtió para los ciberdelincuentes en un punto sobre el que pivotar.

3. El tercer ataque analizado es similar, pero en este caso los cibercriminales se valieron de un sistema de Rayos X exclusivamente.

Considerando que ninguna de estas organizaciones detectaron estas brechas por su cuenta, TrapX cree que una gran mayoría de hospitales están actualmente infectados con malware sin detectar desde hace meses o incluso años.

Como ya he comentado con anterioridad, esta información sustraída acaba en el mercado negro. Rick Kam, presidente de ID Experts, organización que provee servicios y software para gestionar la ciberseguridad, cuenta que los datos médicos completos de un paciente son más valiosos en el mercado negro que las tarjetas de crédito. Según el FBI, se venden por entre 20 y 70 dólares (18 y 63 euros), mientras que una tarjeta puede costar tan solo 5 dólares (4,5 euros).

¿El motivo? Una cuenta bancaria es fácil de cancelar, pero hospitales y aseguradoras no suelen tener un procedimiento claro para ayudar a los pacientes si les roban su información médica. Además, los departamentos de tecnología en sanidad no están equipados como la banca y las finanzas para hacer frente a estas situaciones, por lo que se están encontrando debilidades que pueden ser explotadas.

Los ciberdelincuentes pueden crear una identidad falsa completa y operar con ella o estafar a las aseguradoras gracias a esos datos. Por ejemplo, pueden aprovechar esa identidad para adquirir medicamentos y venderlos posteriormente en la deep web.

Mañana último capitulo de la serie de blogs dedicados al Playbook.