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

Hoy acabamos con el Playbook. Tened en cuenta que existen muchas más formas con las que los hackers aprovechan las vulnerabilidades de estos aparatos, pero según San Google y sus resultados, son los escenarios más comunes. Hasta ahora hemos visto escenarios de DDoS, ataque centrado al paciente y robo de información de centros hospitalarios. Hoy vemos el 4º y último escenario:

Mantener como rehenes a hospitales mediante ataques ransomware.

Un tipo de ataque especialmente perjudicial que es cada vez más común el ataque ransom o de rescate. Como en los anteriores, los hackers acceden al sistema mediante un dispositivo para acceder a la red del hospital. Una vez dentro, encriptan datos sensibles y posteriormente demandan dinero a cambio de una contraseña que desencripte esos registros. Los centros médicos que se enfrentan a este tipo de ataques se pueden encontrar de repente con toda la información de sus pacientes encriptada, haciendo imposible el acceso a registros como la prescripción al paciente, informes de patologías, diagnósticos y otras informaciones críticas para atender al paciente. Como el origen de estos ataques tiende a ser internacional y por lo tanto difícil de trazar y enjuiciar, la mayoría de víctimas acaban pagando.

En el año 2012, un grupo de hackers rusos mantuvo "secuestrado" un centro médico en Gold Coast (Australia), el Miami Family Medical Centre, después de que lograran encriptar miles de registros de pacientes en el propio servidor del centro. Los hackers demandaron un rescate de 4000$, unos

3700€, para desencriptar la información. Este precio, que puede parecer bajo, es una estrategia habitual para aumentar la posibilidad de que los afectados paguen, y dadas las dificultades de trazabilidad expertos en seguridad TI reconocieron que quizás su única opción era pagar. ¿Que paso al final? Una compañía de servicios IT, Essential IT Services, consiguió restaurar su sistema. Una de las enseñanzas que deja este caso particular es que los backups nunca deben estar en el mismo servidor ni conectados a internet. El centro tenia backups, pero estos también estaban encriptados. La casualidad hizo que un miembro del staff técnico del centro se llevara a casa uno de los backups de los datos, pero al no tratarse de un backup del sistema completo, esto hizo que la tarea de devolver el funcionamiento del sistema llevara su tiempo.

Por cierto, esto es Gold Coast. Me parecía necesario enseñar y compartir este lugar.

Hasta aquí llega el Playbook del hacker, espero que os haya gustado.