EL ESPÍA
En la pública luz de las batallas otros dan su vida a la patria y los recuerda el mármol. Yo he errado oscuro por ciudades que odio. Le di otras cosas. Abjuré de mi honor, traicioné a quienes me creyeron su amigo, compré conciencias, abominé del nombre de la patria, me resigné a la infamia.

Jorge Luis Borges
Quince Monedas

Madrid, 2 de julio de 2013

CRIPTORETO RSA

Resuelto por Alfredo Beaumont, a las 3 horas y 19 minutos de ser publicado
Mensaje secreto: Save Edward Snowden!
Ver resultados y comentarios en página 3

En la cumbre anual del G8 un grupo de agentes de inteligencia del servicio GCHQ interceptan las comunicaciones privadas del presidente ruso Vladimir Putin realizadas a través de su dispositivo móvil. Una información de un agente doble permite a los analistas del GCHQ conocer las características del dispositivo de comunicación. Entre estas características es conocido que dispone de dos algoritmos/protocolos criptográficos, uno el que se utiliza habitualmente, diseñado por el FSB y desconocido, y otro el algoritmo RSA (deshabilitado) que solo se utilizó en pruebas de compatibilidad/conexión cuando se probó el dispositivo en Rusia (por defecto, con un módulo clave de 300 bits). Por suerte, el agente doble mediante la red de espionaje desplegada en Rusia ha conseguido la clave pública RSA del dispositivo:

e = 010001

n = CD942ACE3C9390EC39AA4433E505B47E59DB5D2ADB5ABEE1F5E8A1FE7372D00B2A1A91D40B9

Los analistas de GCHQ conocedores de un fallo hardware del dispositivo consiguen inyectar código ejecutable pudiendo habilitar exclusivamente el uso del algoritmo RSA. Seguidamente, se consigue denegar el servicio al algoritmo/protocolo por defecto (el desconocido y diseñado por el FSB) de forma que el dispositivo cifre/descifre mediante el algoritmo RSA. Por suerte, los servidores del FSB no deshabilitaron el uso del RSA inseguro, mientras que en los terminales sí lo hicieron.

En esta situación y mientras se pueda forzar al uso del algoritmo RSA, se podrán criptoanalizar los datos capturados, como por ejemplo este mensaje secreto:

C = C033F149B9D4455597F3502AA9015819C05EA31D3084E216801F44C7CA52E2DBE63226C04D5

¿Qué dijo el presidente? El tiempo corre en su contra…

Contacto: cryptoreto@gmail.com

Reconocimientos:

1. El ganador/a del reto será la primera persona que obtenga el mensaje en claro y documente brevemente el procedimiento seguido.

2. El ganador/a del reto obtendrá un ejemplar gratuito del libro “Cifrado de las comunicaciones digitales. De la cifra clásica al algoritmo RSA” publicado por la editorial 0xWORD, gastos de envío por cuenta de los autores del libro. Será además considerado/a para futuros proyectos de la red Criptored.

http://0xword.com/libros/36-libro-cifrado-comunicaciones-rsa.html

Resultados y Comentarios del Primer Criptoreto

El presente texto recoge las soluciones al criptoreto de julio de 2013, lanzado en Internet por la Red Temática Criptored el martes 2 de julio de 2013.

En primer lugar, agradecer la acogida del reto que a las pocas horas de su publicación contaba ya con más de 500 descargas.

Los objetivos de este primer reto fueron los siguientes:

1. Habilitar un reto que pudiera ser resuelto entre unos pocos minutos hasta un máximo de 33 horas, en función del conocimiento de herramientas por el atacante y de la capacidad de cálculo disponible.

2. El reto tenía un objetivo de "honeypot": ver la acogida de este tipo de retos e incentivar a la gente a formarse en este aspecto en verano, si lo desea. Entre los objetivos del reto, residía medir el interés y la rapidez de respuesta; por esto se publicó entre semana y en dos tandas, no como sería lo habitual, es decir un viernes y en una única tanda para que así para todo el mundo tuviera las mismas oportunidades, independientemente de su situación laboral/personal. En septiembre de 2013 se publicará un reto más difícil.

3. El reto se podía resolver de varias formas: con software educativo publicado en Crypt4you (donde no era necesario tener conocimientos de programación) con un coste temporal mayor, por ejemplo si se utilizó el programa factor.exe y luego genrsa, o mezcla con otro tipo de software disponible y programas a medida. Diferentes tipos de soluciones han alcanzado el mismo resultado de la factorización con mejor tiempo de respuesta: msieve, yufu, etc. Además. la gente que estudió el curso RSA de Crypt4you o el curso de Criptografía de Coursera-Stanford tenían claramente ventaja sobre el resto.

4. El ranking de las cinco primeras personas que, en ese orden, obtuvieron el resultado y documentaron adecuadamente la solución durante las primeras 24 horas del reto, es el siguiente. No se incluyen tiempos del segundo al quinto puesto por las diferentes horas de publicación del reto, como se indicaba en el apartado 2.
    1. Alfredo Beaumont (GANADOR)
       Tiempo: 3 horas y 19 minutos
       Ver la solución en el siguiente archivo: writeup-alfredo-beaumont.pdf
    2. Ignacio Sánchez
    3. Abel Valero
    4. Michel Ruiz Tejada
    5. Manuel Mollar

De nuevo agradecer la acogida, cordiales saludos y hasta el próximo criptoreto.

Madrid, 4 de julio de 2013

Dr. Alfonso Muñoz
Dr. Jorge Ramió
Editores de Criptored