Nota de prensa

Ciberseguridad

El Gobierno hace un seguimiento de los ciberataques masivos en EEUU

- **El ataque de denegación de servicio a proveedores de internet en Estados Unidos resulta novedoso por basarse en la infección masiva de dispositivos conectados al Internet de las Cosas (IoT).**

- **El Equipo de Respuesta a Incidentes Cibernéticos de León (CERTSI), gestionado conjuntamente por los ministerios del Interior e Industria, se encuentra monitorizando el incidente, que no ha tenido efectos relevantes en España.**

22.10.16. Desde el 12 de octubre se viene produciendo una serie de ciberataques hacia importantes proveedores de Internet en EEUU, en formatos de ataque de denegación de servicio (Denial of Service –DoS- o Distributed Denial of Service –DdoS-) o ataque a la disponibilidad del mismo, y realizadas en tres oleadas. La más reciente ha sido la sucedida durante el 21 de octubre, que se ha focalizado principalmente en Dyn, una compañía norteamericana que provee servicios de telecomunicaciones a un alto número de empresas como Twitter, Spotify, Reddit, Paypal, WhatsApp o SoundCloud, que se han visto afectadas con la ralentización, e incluso paralización en algunos momentos, de sus comunicaciones y servicios.

Los principales objetivos que persiguen este tipo de ataques son la ralentización de los servicios de DNS o de traducción de las direcciones IP que identifican las máquinas, servidores o servicios que soportan, hacia sus nombres de dominio, de modo que se dificulte o no se puedan acceder a dichos servicios de la forma correcta, y que por lo tanto el funcionamiento de Internet se vea afectado.

Cambio de paradigma: utilizando la Internet de las Cosas

CORREO ELECTRONICO
prensa@minetur.es

PSO DE LA CASTELLANA, 160
28071 - MADRID
TEL: 91 349 48 39 - 40
FAX: 91 349 45 48

La denominada Internet de las Cosas o “IoT, Internet of Things” es la red de objetos cotidianos interconectados con acceso a Internet que incluye routers wifi, impresoras, electrodomésticos, sistemas de calefacción y alumbrado, coches inteligentes y una infinidad de dispositivos que pueden encontrarse en cualquier hogar y al alcance de cualquier ciudadano.

Precisamente los ciberataques producidos en Estados Unidos se han basado en infectar estos objetos que, con una dirección IP o URI, son capaces de recoger información, procesarla y compartirla en las redes de comunicación. Esta característica particular del ataque supone una nueva tendencia en los ciberataques.

Impacto menor en los operadores y usuarios españoles

En España, el impacto de este ciberataque sólo habría producido, de acuerdo con las fuentes de Interior y de Industria, un perjuicio superficial en servicios no esenciales para los operadores. El CERT de Seguridad e Industria (CERTSI_), operado técnicamente por el Instituto Nacional de Ciberseguridad (INCIBE), en coordinación con el Centro para la Protección de Infraestructuras Críticas (CNPIC), ha llevado a cabo una serie de acciones con objeto de disponer de información más detallada acerca del caso y prevenir o mitigar un caso similar en España.

Entre ellas destacan la recopilación y análisis de información disponible tanto en fuentes abiertas como en entornos o foros del ámbito de la ciberseguridad; la monitorización de la resolución de dominios, con objeto de poder identificar de forma temprana un posible impacto a nivel nacional y el contacto con operadores de telecomunicaciones nacionales, con los que se ha valorado el impacto nacional del ataque en tiempo real. Igualmente, el CERTSI_ mantiene estrecho contacto con los operadores españoles con actividad en Estados Unidos y que se han visto afectados por la cadena de pérdida de servicio que se ha dado en dicho país.

A corto plazo el CERTSI_ continuará monitorizando el incidente para recabar más información de interés para la detección y alerta temprana en el ámbito nacional, en permanente coordinación con los operadores nacionales a nivel de CERT Nacional y con el US-CERT, con objeto de disponer de información técnica que permita una mitigación efectiva en caso de producirse un ataque análogo sobre algún operador de telecomunicaciones español.