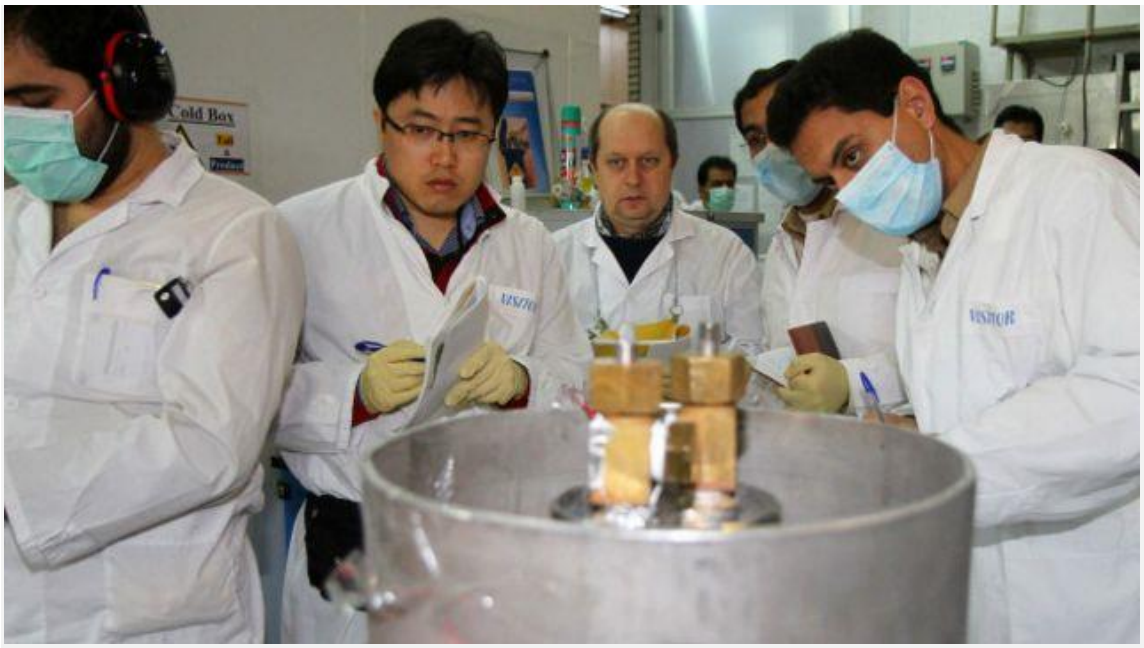
El virus que tomó control de mil máquinas y les ordenó autodestruirse

11 octubre 2015



FUENTE DE LA IMAGEN,GETTY

Pie de foto,
El ataque del gusano Stuxnet destruyó 1000 máquinas en la central nuclear de Natanz, Irán

En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que reemplazaban las máquinas también parecían asombrados.

El fenómeno se repitió cinco meses después en el país, pero esta vez los expertos pudieron detectar la causa: un malicioso virus informático.

El "gusano" - ahora conocido como Stuxnet - tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real".

Durante el análisis del gusano, los analistas hicieron un descubrimiento sorprendente, señala Gordon Corera, corresponsal de temas de seguridad de la BBC. El código altamente avanzado de Stuxnet había sido diseñado con una mentalidad bélica.

¿Cómo un gusano informático logró dañar físicamente 1.000 máquinas en una planta nuclear? Te lo explicamos en cuatro pasos:

FUENTE DE LA IMAGEN,THINKSTOCK

Pie de foto,

El gusano aprovechó brechas en el sistema informático

1- Stuxnet penetró en la red

Según la firma de seguridad cibernética Symantec, Stuxnet probablemente llegó al programa nuclear de Natanz de Irán en una memoria USB infectada. Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta.

2- El gusano se propagó a través de las computadoras

Una vez dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras.

Las centrífugas giran a altas velocidades para separar componentes. En la planta de Natanz, las centrifugadoras estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares.

3- Stuxnet reprogramó las centrifugadoras

El gusano encontró el software que controla las centrifigudoras y se insertó en él, tomando el control de las máquinas.

Stuxnet llevó a cabo dos ataques diferentes. En primer lugar, hizo que las centrífugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses.

4- Destrucción de las máquinas

Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1000, se desintegraran.

Durante el ataque cibernético, alrededor del 20 por ciento de las centrifugadoras en la planta de Natanz quedaron fuera de servicio.

¿Cómo logró Stuxnet infiltrarse en la central iraní?

FUENTE DE LA IMAGEN,GETTY

Pie de foto,

El sofisticado ataque cibernético sorprendió a los técnicos de la central de Natanz

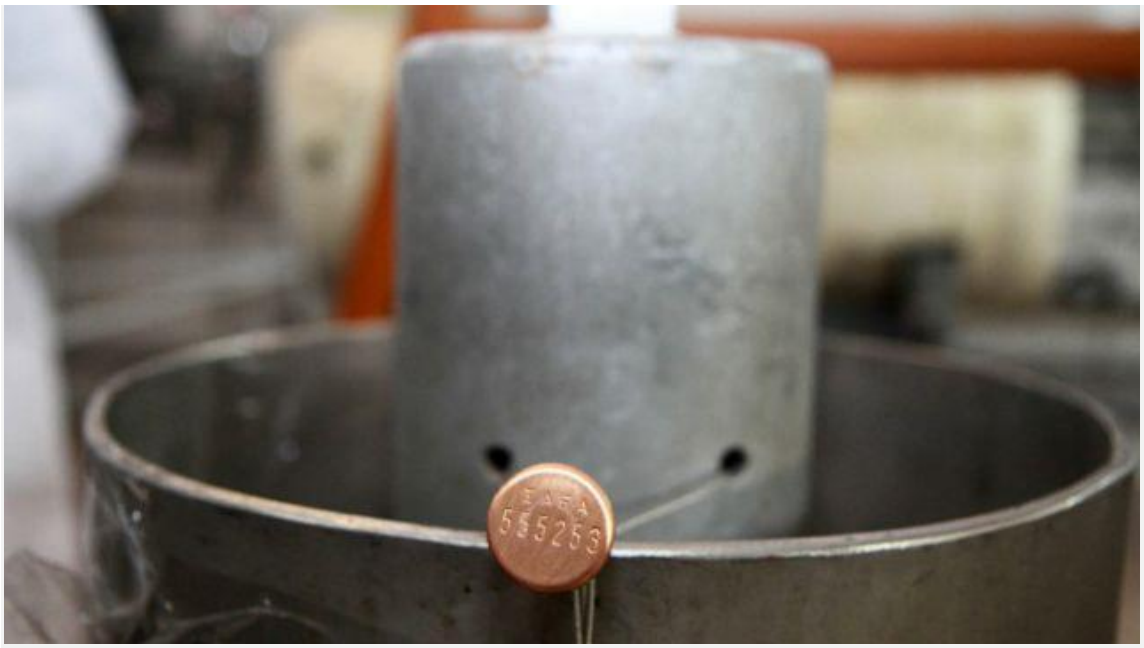
El gusano aprovechó cuatro debilidades previamente desconocidas en el sistema operativo Windows de Microsoft. Una ayudó a Stuxnet a llegar a la red a través de una memoria USB y otra usó impresoras compartidas para penetrar más profundamente. Las dos restantes le permitieron a Stuxnet controlar otras partes menos seguras de la red.

El gusano fue programado específicamente para apuntar y destruir las centrifugadoras.

Una vez dentro del sistema de Natanz, Stuxnet escaneó todas las computadoras con sistema operativo Windows que estaban conectadas a la red, en busca de un determinado tipo de circuito llamado Programmable Logic Controller (Controlador Lógico Programable) o PLC, que controla las máquinas. En este caso, el PLC que fue blanco del ataque controlaba la velocidad específica de las centrifugadoras.

A diferencia de la mayoría de los gusanos informáticos, Stuxnet no hizo nada en las computadoras que no cumplían con requisitos específicos. Pero una vez que encontró lo que estaba buscando, se insertó en los PLC, listo para tomar el control de las centrifugadoras.

Con sigilo de espía



FUENTE DE LA IMAGEN,GETTY

Pie de foto,

Stuxnet penetró en las computadoras y esperó el momento preciso para atacar

Para infiltrarse en el sistema sin ser detectado, el gusano utiliza una "firma digital" - una clave larga, cifrada, robada de piezas genuinas de software- para parecer legítimo. Windows suele comprobar esas claves cuando se instalan nuevos programas. Usando ese modo de acceso, Stuxnet se deslizó sin generar sospechas.

El gusano permaneció latente durante casi un mes después de infectar el PLC de las máquinas.

En ese tiempo observó cómo opera el sistema normalmente y registró los datos generados.

Una vez las centrifugadoras en Natanz quedaron fuera de control, el gusano reprodujo los datos grabados cuando todo estaba funcionando normalmente.

Esto permitió que permaneciera indetectado por los operadores humanos de la fábrica, mientras las centrifugadoras quedaban destruidas.

FUENTE DE LA IMAGEN,GETTY

Pie de foto,

Stuxnet impidió que los técnicos apagaran las máquinas

Stuxnet fue incluso capaz de anular los interruptores de apagado de emergencia.

Incluso cuando los operadores de las centrifugadoras se percataron de que las cosas estaban fuera de control, Stuxnet contenía un código que impidió el apagado de las máquinas.

Todavía se desconoce con seguridad quién o quiénes fueron responsables de la creación de Stuxnet.
Symantec considera que se necesitaron entre 5 y 10 expertos en software, que trabajaron hasta 6 meses para crear el sofisticado gusano cibernético.
En 2011, el reconocido experto Ralph Langner dijo que el gusano fue creado en laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán, pero las autoridades no han confirmado esa afirmación.