Se trata de un gusano informático que afecta a equipos con sistema operativo Windows, descubierto en junio de 2010 por VirusBlokAda, empresa de seguridad en Bielorrusia.

Es el primer gusano conocido que espía y reprograma sistemas industriales, específicamente, sistemas SCADA de control y monitorización de procesos, con lo que se puede afectar a infraestructuras críticas como centrales nucleares.

Stuxnet puede reprogramar Controladores Lógicos Programables (PLC) y ocultar los cambios que se realizaron. También es el primer gusano conocido que incluye un rootkit para sistemas reprogramables PLC.

Kaspersky Lab describía a Stuxnet en una nota de prensa como “un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial”.

Por otro lado, Kevin Hogan, un ejecutivo de Symantec, dijo que el 60% de las computadoras contaminadas por este gusano se encuentran en Irán, intentando dar a conocer que sus instalaciones industriales podrían ser su objetivo.
Kaspersky afirmó que los ataques sólo pudieron producirse “con el apoyo de una nación soberana”, lo que convierte a Irán en el primer objetivo de una guerra cibernética real.

VirusBlokAda informó de la existencia del gusano a mediados de junio de 2010, y partes de su componente se han fechado desde junio de 2009.

Los países afectados son Irán, con 62,867 ordenadores infectados, Indonesia, con 13,336 ordenadores infectados, India, con 6,552 ordenadores infectados, Estados Unidos, con 2,913 ordenadores infectados y Australia, con 2,346 ordenadores infectados.

Stuxnet ataca equipos funcionando con Windows, aprovechando cuatro vulnerabilidades de día cero de dicho sistema, incluyendo CPLINK, y otra empleada por otro gusano denominado Conficker. Su objetivo son sistemas que emplean programas de monitorización y control industrial (SCADA) WinXX/PCS 7 de Siemens.

El gusano se distribuye por medio de memorias USB infectadas, luego contamina otros equipos con WinXX conectados en red. Cuando ha logrado acceder al sistema, Stuxnet emplea contraseñas por defecto para obtener el control.
Siemens aconseja no cambiar las contraseñas originales ya que “podría tener impacto en el funcionamiento de la planta”.

Algo que llama la atención es que el funcionamiento de Stuxnet es poco habitual en ataques de malware, ya que se requieren conocimientos de procesos industriales y deseos de atacar infraestructuras, lo que no posee cualquier programador de virus informáticos.

Otra característica de Stuxnet es que es demasiado grande, ocupa 500 MB aproximadamente y está escrito en distintos lenguajes de programación, incluyendo C y C++, algo que no siempre se ve en este tipo de ataques.
Además, Stuxnet fue firmado digitalmente con dos certificados auténticos robados de autoridades de certificación. Se puede actualizar mediante P2P, lo que permite que esté actualizado al día, aunque se haya desactivado el servidor remoto de control.

Todas estas capacidades seguramente requirieron de un equipo completo de programadores de distintas áreas, así como verificación en sistemas reales de que el malware no bloquearía los PLCs.

Eric Byres, programador con varios años de experiencia en el mantenimiento y reparación de sistemas Siemens, dijo a Wired que escribir este software podría haber requerido meses o años de trabajo, en caso de haberlo realizado una sola persona.

Siemens ha publicado una herramienta de detección y eliminación de Stuxnet, y recomienda contactar con su soporte técnico en caso de detectar una infección, instalar los parches de

Microsoft que eliminan las vulnerabilidades
del sistema y prohibir en las instalaciones industriales el uso de memorias USB.

También la compañía BitDefender ha desarrollado una herramienta gratuita para eliminar Stuxnet.

ESPECULACIONES

Un portavoz de Siemens dijo que el gusano Stuxnet se encontró en 15 sistemas, de los cuales cinco eran plantas de fabricación en Alemania. Según Siemens, no se han encontrado infecciones activas y no existen informes de daños causados por el gusano.

Ralph Langner, investigador alemán de seguridad informática, afirma que Stuxnet es un arma diseñada para “disparar un solo tiro”, y que el objetivo deseado por sus desarrolladores fue probablemente alcanzado, aunque admite que sólo son especulaciones. El New York Times eliminó todo rumor o especulación cuando confirmó que se trataba de un troyano desarrollado y financiado por Israel y Estados Unidos con el fin de atacar las centrales nucleares iraníes.