Tres agencias gubernamentales de Estados Unidos publicaron hoy una alerta conjunta sobre Taidoor, una nueva pieza de malware que ha sido utilizada durante las recientes violaciones de seguridad por hackers del gobierno chino.

La alerta fue emitida por la Agencia de Seguridad Cibernética e Infraestructura del Departamento de Seguridad Nacional (DHS CISA), el Comando Cibernético del Departamento de Defensa (CyberCom) y la Oficina Federal de Investigaciones (FBI).

Las tres agencias comenzaron recientemente a colaborar en la publicación de informes conjuntos acerca de nuevas amenazas de malware. La primera alerta conjunta se envió en febrero, cuando las agencias advirtieron sobre seis nuevas cepas de malware desarrolladas por hackers patrocinados por Corea del Norte.

Taidoor: Troyano chino de acceso remoto

Según las tres agencias, Taidoor tiene versiones para sistemas de 32 y 64 bits, y generalmente se instala en los sistemas de la víctima como una biblioteca de enlaces dinámicos (DLL) de servicio.

La DLL contiene otros dos archivos. *«El primer archivo es un cargador, que se inicia como un servicio. El cargador descifra el segundo archivo y lo ejecuta en la memoria, que es el principal troyano de acceso remoto (RAT)»*.

El RAT Taidoor se utiliza para que los piratas informáticos chinos puedan acceder a los sistemas infectados y extraigan datos o implementen otro malware.

El FBI informó que Taidoor normalmente se implementa junto con servidores proxy para ocultar el verdadero punto de origen del operador del malware.

Aunque la alerta especifica se trata de una nueva amenaza para la seguridad cibernética, el Twitter, el Comando Cibernético de Estados Unidos, dijo que el malware ha estado presente y desplegado en silencio en las redes de víctimas durante al menos 12 años, desde 2008.

Las tres agencias presentaron el Informe Conjunto de Análisis de Malware (MAR), que contiene técnicas de mitigación recomendadas y acciones de respuesta sugeridas para organizaciones que desean mejorar la detección, prevenir infecciones o que ya se han infectado y necesitan eliminar el malware de sus sistemas.

Además, el Comando Cibernético de Estados Unidos subió cuatro muestras del malware Taidoor al portal VirusTotal [1, 2, 3, 4], para que las empresas de seguridad cibernética y los analistas independientes de malware puedan descargar los archivos para su análisis.