FBI advierte sobre ataques cibernéticos a empresas con software de supplychain

Autor: I. Stepanenko

Fecha: Sunday 24th of January 2021 05:04:30 AM

El FBI envió una alerta de seguridad al sector privado de Estados Unidos acerca de una campaña de piratería en curso que apunta a los proveedores de software de la cadena de suministro.

El FBI asegura que los hackers están intentando infectar a las empresas con el malware Kwampirs, un troyano de acceso remoto (RAT).

> «Se cree que las empresas de la supplychain de software están dirigidas para obtener acceso a los socios estratégicos y/o clientes de la víctima, incluidas las entidades que apoyan los Sistemas de Control Industrial (ICS) para la generación,

> transmisión y distribución de energía a nivel mundial», dijo el FBI en un comunicado.

Además de los ataques contra los proveedores de software de la cadena de suministro, el FBI dijo que el mismo malware también se implementó en ataques contra empresas en los sectores de salud, energía y financiero.

La alerta no identificó a los proveedores de software seleccionados ni a ninguna otra víctima. El FBI compartió los COI (Indicadores de Compromiso) y las reglas de YARA para que las organizaciones puedan escanear las redes internas en busca de signos de la RAT de Kwampirs utilizada en los ataques cibernéticos recientes.

Malware Kwampirs

El malware Kwampirs fue descrito por primera vez en un informe publicado por la compañía estadounidense de seguridad cibernética Symantec en abril de 2018.

En ese momento, Symantec afirmó que un grupo con nombre en código Orangeworm había utilizado el malware Kwampirs para atacar de forma similar a las empresas de la cadena de suministro que proporcionaban software para el sector de la salud.

Symantec asegura que Orangeworm había estado en funcionamiento desde 2015 y se centraba principalmente en la industria de la salud.

> «Los objetivos secundarios de Orangeworm incluyen la fabricación, tecnología de la información, agricultura y logística. Si bien estas industrias pueden parecer no relacionadas, descubrimos que tienen múltiples vínculos con la atención médica, como los grandes fabricantes que producen dispositivos de imágenes médicas que se venden directamente en las empresas de atención médica, las organizaciones de TI que brindan servicios de apoyo a las clínicas médicas y las organizaciones logísticas que ofrecen productos para el cuidado de la salud», dijeron los

> investigadores.

Un informe de Lab52 publicado un año más tarde, en abril de 2019, confirmó los hallazgos de Symantec y el enfoque del grupo en la industria de la salud.

Sin embargo, la alerta del FBI enviada la semana pasada advierte específicamente que los ataques que emplean a Kwampirs ahora evolucionaron para atacar a las compañías en el sector de ICS (Sistemas de Control Industrial), y específicamente en el sector de la energía.

En 2018 y 2019, ni Symantec ni Lab52 hicieron atribuciones al país de origen del grupo. Sin embargo, el FBI afirma que la nueva evidencia del análisis del código sugiere que Kwampirs contienen *«muchas similitudes»* con Shamoon, un malware de limpieza de datos desarrollado por APT33, un grupo de hackers vinculado a Irán.

> «Si bien no se ha observado que el RAT Kwampirs incorpore un componente de limpiaparabrisas, el informe forense comparativo reveló que el RAT tiene muchas similitudes con el malware de destrucción de datos Disttrack», dijo el FBI.

EL malware Shamoon se ha utilizado en muchos ataques de borrado de datos contra empresas del sector energético, y más específicamente, en los campos de petróleo y gas.

El FBI instó a las empresas a escanear redes para poder detectar evidencias de Kwampirs y reportar cualquier infección.