Los atacantes detrás del ransomware Conti se han dirigido a no menos de 16 redes de atención médica y primeros auxilios en Estados Unidos durante el año pasado, victimizando por completo a más de 400 organizaciones en todo el mundo, 290 de las cuales están ubicadas en el país.

Eso es según una nueva alerta rápida emitida por la Oficina Federal de Investigaciones (FBI) este jueves.

> *«El FBI identificó al menos 16 ataques de ransomware Conti dirigidos a las redes de primeros auxilios y atención médica de Estados Unidos, incluidas las agencias de aplicación de la ley, los servicios médicos de emergencia, los centros de despacho del 911 y los municipios durante el último año»*, dijo la agencia.

Los ataques de ransomware han empeorado a lo largo de los años, con objetivos recientes tan variados como gobiernos estatales y locales, hospitales, departamentos de policía e infraestructura crítica. Conti es una de las muchas cepas de ransomware que han capitulado en esa tendencia, comenzando sus operaciones en julio de 2020 como un ransomware-as-a-service (RaaS) privado, además de utilizar una técnica de doble extorsión al lanzar un sitio de filtración de datos.

Según un análisis publicado por la firma de recuperación de ransomware Coverware el mes pasado, Conti fue la segunda cepa más prevalente implementada, representando el 10.2% de todos los ataques de ransomware en el primer trimestre de 2021.

Las infecciones que involucran a Conti también violaron las redes del Ejecutivo de Servicios de Salud (HSE) y el Departamento de Salud (DoH) de Irlanda, lo que llevó al Centro Nacional de Seguridad Cibernética (NCSC) a emitir una alerta propia el 16 de mayo, declarando que *«hay graves impactos en las operaciones de salud y algunos procedimientos que no son de emergencia se están posponiendo a medida que los hospitales implementan sus planes de continuidad comercial».*

Los operadores de Conti son conocidos por infiltrarse en redes empresariales y difundirse lateralmente utilizando balizas de Cobalt Strike antes de explotar las credenciales de usuario comprometidas para implementar y ejecutar las cargas útiles de ransomware, y los archivos cifrados se renombran con una extensión *«.FEEDC».*

Los enlaces de correo electrónico maliciosos armados, los archivos adjuntos o las credenciales robadas del Protocolo de Escritorio Remoto (RDP) son algunas de las tácticas que el grupo utilizó para afianzarse inicialmente en la red objetivo, dijo el FBI.

«Los actores son observados dentro de la red de víctimas entre cuatro días y tres semanas en promedio antes de implementar el ransomware Conti», dijo la agencia, y agregó que los montos del rescate se adaptan a cada víctima, con demandas recientes que alcanzan los 25 millones de dólares.

La alerta también se produce en medio de una proliferación de incidentes de ransomware en las últimas semanas, incluso cuando los extorsionadores siguen buscando precios exorbitantes de las empresas con la esperanza de obtener un día de pago enorme y rápido. Se cree que la principal aseguradora CNA Financial pagó 40 millones de dólares, mientras que Colonial Pipeline y Brenntag han desembolsado cada una casi 4.5 millones de dólares para recuperar el acceso a sus sistemas cifrados.