Al tiempo que Colonial Pipeline restauró todos sus sistemas al estado operativo a raíz de un incidente de ransomware hace una semana, DarkSide, el sindicato de delitos cibernéticos detrás del ataque, afirmó que perdió el control de su infraestructura, citando una incautación por parte de las autoridades.

Todos los sitios web oscuros operados por el grupo de piratas, incluyendo su blog DarkSide Leaks, el sitio de recolección de rescates y los servidores de la red de entrega de contenido de datos (CDN), se han vuelto oscuros y permanecen inaccesibles hasta este momento. Además, los fondos de sus billeteras de criptomonedas fueron supuestamente exfiltrados a una cuenta desconocida, según una nota transmitida por los operadores de DarkSide a sus afiliados.

> *«Por el momento, no se puede acceder a estos servidores a través de SSH, y los paneles de alojamiento han sido bloqueados»*, dice el anuncio obtenido por Intel 471.

El desarrollo se produce cuando DarkSide cerró su programa de afiliados de Ransomware-as-a-Service (RaaS) para siempre *«debido a la presión de Estados Unidos»,* y el grupo afirmó que emitirían descifradores a todos sus afiliados para las empresas que fueron atacadas, junto con la promesa de compensar todas las obligaciones financieras pendientes antes del 23 de mayo.

Aunque los derribos marcan un giro sorpresa en la saga Colonial Pipeline, vale la pena señalar que no hay evidencia para corroborar públicamente estas afirmaciones, lo que genera preocupaciones de que esto pueda ser una estada de salida, una táctica clandestina que ha plagado los mercados ilegales de la red oscura en los últimos años, o que la pandilla está dando la impresión de que se está retirando del centro de atención solo para cambiar la marca y seguir de forma sigilosa sus operaciones en otro formato sin atraer atención no deseada.

Según la compañía de análisis de blockchain Elliptic, la billetera bitcoin utilizada por los

extorsionadores de DarkSide recibió un pago de 75 BTC ($3.2 millones de dólares), realizado por Colonial Pipeline el 8 de mayo, luego de lo cual, la billetera se vació por un total de 5 millones de dólares en bitcoin el 13 de mayo. Se estima que DarkSide tiene al menos 60 millones de dólares desde que surgió en el panorama de amenazas en agosto de 2020.

> *«Se ha especulado que los bitcoins fueron confiscados por el gobierno de Estados Unidos. Si ese es el caso, en realidad no se apoderaron de la mayor parte del pago de rescate de Colonial Pipeline, la mayor parte se sacó de la billetera el 9 de mayo»*, dijo Tom Robinson, cofundador de Elliptic.

Al rastrear las últimas salidas de criptomonedas de la billetera, Elliptic dijo que el 18% del bitcoin se envió a un pequeño grupo de intercambios, con un 4% adicional enviado a Hydra, el bazar de la red oscura más grande del mundo que atiende a clientes en Rusia y Europa del Este. Hydra representa más del 75% de los ingresos del mercado de redes oscuras en todo el mundo en 2020, lo que la posiciona como un jugador importante en el panorama del crimen criptográfico, según Chainalysis.

Los reveses operativos de DarkSide y el mayor escrutinio que siguió al ataque Colonial Pipeline, también pusieron en marcha una ola de prohibiciones de RaaS en foros de ciberdelincuencia ilícitos como XSS, Exploit y RaidForums, lo que representa una importante interrupción a corto plazo de la economía de ransomware.

REvil, de los más prolíficos grupos de ransomware, ha introducido nuevas restricciones que prohíben el uso de su software contra entidades gubernamentales, educativas y de salud que pertenecen a cualquier país.

Visto en este contexto, las acciones de XSS, Exploit y REvil pueden interpretarse como un «efecto dominó» de una serie de incidentes de ransomware de alto perfil en la última semana, incluido el de Babuk en el Departamento de Policía Metropolitana.

> *«No hace falta decir, sin embargo, que es casi seguro que el ransomware seguirá siendo una amenaza persistente en el futuro previsible dada su popularidad entre las comunidades de ciberdelincuentes. En todo caso, es probable que los ataques de ransomware sigan creciendo tanto en escala como en frecuencia. Después del cierre de DarkSide, el panorama del ransomware está dominado por cuatro grandes colectivos: REvil, LockBit, Avaddon y Conti»,* dijo Flashpoint.