El ransomware DarkSide desde los ojos de un equipo de defensa

Por Sean Gallagher, Mark Loman y Peter Mackenzie

CIUDAD DE MÉXICO. 13 de mayo de 2021.- El reciente ataque de *ransomware* a un importante operador de gasoductos en Estados Unidos fue obra de un grupo que utilizó el ransomware DarkSide, conocido por ser responsable de al menos 60 casos de doble extorsión en lo que va del año.

DarkSide ha atacado a varias víctimas de alto perfil en los últimos meses, incluidas empresas que cotizan en la bolsa de valores NASDAQ. Pero el ataque a Colonial Pipeline llevó a la compañía a cerrar también su red de tecnología operativa (OT), cortando la mayor parte del suministro de gasolina al este de la Unión Americana.

Este no es el primer problema crítico de infraestructura provocado por dicho ransomware: en febrero, una instalación de gas natural estadounidense fue cerrada durante dos días por un ataque que se extendió a su red OT. DarkSide también golpeó a una energética brasileña a principios de este año.

Pero el incidente de Colonial Pipeline tiene un impacto potencialmente mayor en el mundo real y aparentemente ha hecho que los operadores de esta red sean más notorios.

- **¿Qué debo saber sobre DarkSide?**

El grupo que propaga el ransomware DarkSide surgió el verano pasado, ganando atención con su supuesto enfoque de “honor entre criminales”: la red de ciberdelincuentes afirmó tener un código de conducta que prohíbe apuntar a industrias y organizaciones sin fines de lucro conectadas con el interés público.

Para cuidar esa ‘honorabilidad’, han utilizado un sitio de filtraciones como plataforma para contrarrestar las malas noticias que salen sobre ellos. Por ejemplo, cuando la empresa de recuperación de ransomware Coveware advirtió sobre el uso de un hosting iraní por parte de DarkSide, publicaron un "comunicado de prensa" en el que negaban haber utilizado algún servicio de TI de ese país. El ataque a Colonial Pipeline nuevamente tiene a la pandilla levantando la voz, ya que indican en una publicación que son "apolíticos" y que su objetivo es "hacer dinero y no crear problemas para la sociedad".

La pandilla prometió “no tocar” a las organizaciones de atención médica, así como a otras personas involucradas en la distribución de vacunas, debido a la atención negativa que tales ataques podrían atraer y a los impactos sociales que generaría.

- **¿Cómo funciona?**

DarkSide sigue los pasos de los operadores de ransomware de doble extorsión como REvil, Maze y LockBit, que filtran datos comerciales antes de cifrarlos y luego amenazan con divulgarlos al público si las víctimas no pagan por un rescate. Del mismo modo, exige grandes cantidades por el descifrado de la información robada. Sophos Rapid Response tiene registro de un caso en el que se exigieron $4 millones de dólares (que no fueron pagados).

DarkSide sigue las mismas tácticas y procedimientos de muchas otras campañas de ransomware dirigidas: una combinación de características nativas de Windows, malware básico (incluido SystemBC) y herramientas de explotación listas para ser ejecutadas (incluido Cobalt). Los creadores de DarkSide subcontratan el proceso de compromiso de los equipos y el despliegue del ransomware criptográfico a especialistas en penetración de redes, quienes entregan la información a los principales operadores del grupo criminal.

Otro detalle importante, desde la experiencia del equipo de defensa de Sophos, es que el acceso inicial a la red del objetivo se produce principalmente como resultado de un ataque de phishing. Desde luego, esa no es la única forma en que los atacantes de esta red se afianzan a sus víctimas, pero parece ser la que más prevalece en los casos en los que se involucra.

A diferencia de otros ransomware, DarkSide es capaz de cifrar computadoras Linux y aquellas que ejecutan Windows, lo que los convierte en una herramienta más deseable para los actores de amenazas que quieren apuntar a grandes empresas.

Si bien algunas operaciones recientes de ransomware dirigidas de otras pandillas han surgido rápidamente, lanzando su ataque en cuestión de días, los actores detrás de las campañas de DarkSide pueden pasar semanas o meses buscando dentro de la red de una organización antes de activar su carga útil.

En ese tiempo, los intrusos extraen la mayor cantidad de datos posible. Las notas de rescate de Darkside afirman el robo de grandes cantidades de archivos, a menudo de varios departamentos dentro de una organización, como contabilidad usando PSExec, conexiones de escritorio remoto y (en el caso de servidores Linux) SSH para moverse lateralmente dentro de la red.

Actualmente, Sophos defiende a todos los equipos de DarkSide de múltiples formas. Existen protecciones dinámicas y de comportamiento que incluyen la función CryptoGuard e InterceptX, además de detecciones de puntos finales convencionales para Windows y Linux, ejecutables contra entes maliciosos.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la

actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/