El grupo de ransomware como servicio (RaaS) Black Basta, ha acumulado casi 50 víctimas en Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda en los dos meses posteriores a su aparición en la naturaleza, lo que lo convierte en una amenaza prominente en una corta ventana.

> *«Se ha observado que Black Basta apunta a una variedad de industrias, incluyendo la fabricación, la construcción, el transporte, las empresas de telecomunicaciones, los productos farmacéuticos, los cosméticos, la plomería y la calefacción, los concesionarios de automóviles, los fabricantes de ropa interior y más»*, dijo Cybereason.

Al igual que otras operaciones de ransomware, se sabe que Black Basta emplea la táctica comprobada de doble extorsión para robar información confidencial de los objetivos y amenazar con publicar los datos robados a menos que se realice un pago digital.

Un nuevo participante en este panorama de ransomware, las intrusiones que involucran la amenaza han aprovechado QBot, también conocido como Qakbot, como un conducto para mantener la persistencia en los hosts comprometidos y recolectar credenciales, antes de moverse lateralmente a través de la red e implementar el malware de cifrado de archivos.

Además, los atacantes detrás de Black Basta han desarrollado una variante de Linux diseñada para atacar las máquinas virtuales VMware ESXi que se ejecutan en servidores empresariales, poniéndolo a la par con otros grupos como LockBit, Hive y Cheerscrypt.

Los hallazgos se producen cuando el grupo de hackers agregó Elbit Systems of America, un fabricante de soluciones de defensa, aeroespaciales y de seguridad, a la lista de sus víctima durante el fin de semana, según el investigador de seguridad Ido Cohen.

Se cree que Black Basta está compuesto por miembros que pertenecen al grupo Conti, luego de que este último cerrara sus operaciones en respuesta a un mayor escrutinio policial y una filtración importante que vio sus herramientas y tácticas pasar al dominio público luego de

ponerse del lado de Rusia.

La semana pasada, el equipo de Conti desmanteló su infraestructura pública restante, incluyendo dos servidores Tor utilizados para filtrar datos y negociar con las víctimas, lo que marca el final oficial de su organización criminal.

Mientras tanto, el grupo siguió manteniendo la fachada de una operación activa apuntando al gobierno de Costa Rica, mientras que algunos miembros hicieron la transición a otros equipos de ransomware y la marca experimentó una renovación organizacional que la ha llevado a dividirse en subgrupos más pequeños con diferentes motivaciones y modelos de negocio que van desde el robo de datos hasta el trabajo como afiliados independientes.

Según un informe completo de Group-IB que detalla sus actividades, se cree que el grupo Conti ha victimizado a más de 850 entidades desde que se observó por primera vez en febrero de 2020, comprometiendo a más de 40 organizaciones en todo el mundo como parte de una ola de piratería *«rápida como un rayo»* que duró del 17 de noviembre al 20 de diciembre de 2021.

Nombrado como «ARMattack» por la compañía con sede en Singapur, las intrusiones se dirigieron principalmente contra organizaciones estadounidenses (37%), seguidas de Alemania (3%), Suiza (2%), Emiratos Árabes Unidos (2%), Países Bajos, España, Francia, República Checa, Suecia, Dinamarca e India (1% cada uno).

Los cinco principales sectores a los que históricamente se ha dirigido Conti, han sido la fabricación (14%), el sector inmobiliario (11%), logística (8.2%), servicios profesionales (7.1%), y el comercio (5.5%), y los operadores destacan específicamente a las empresas en Estados Unidos (58.4%), Canadá (7%), Reino Unido (6.6%), Alemania (5.8%), Francia (3.9%) e Italia (3.1%).

> *«El aumento de la actividad de Conti y la fuga de datos sugieren que el ransomware ya no es un juego entre desarrolladores de malware promedio, sino una industria*

> *RaaS ilícita que da trabajo a cientos de ciberdelincuentes en todo el mundo con diversas especializaciones*», dijo Ivan Pisarev, de Group-IB.

> *«En esta industria, Conti es un jugador notorio que de hecho ha creado una 'compañía de TI' cuyo objetivo es extorsionar grandes sumas. Está claro que el grupo seguirá sus operaciones, ya sea solo o con la ayuda de sus proyectos 'subsidiarios'».*