Dos nuevos malware de ransomware-ad-servide (RaaS), aparecieron en el radar de amenazas este mes, con un grupo que profesa ser el sucesor de DarkSide y REvil, los dos grandes sindicatos de ransomware que salieron de la red después de importantes ataques a Colonial Pipeline y Kaseya en los últimos meses.

«El proyecto ha incorporado en sí mismo las mejores características de DarkSide, REvil y LockBit», dijeron los operadores detrás del nuevo grupo BlackMatter en su blog público darknet, haciendo promesas de no atacar organizaciones en varias industrias, incluida la salud, infraestructura crítica, petróleo, y sectores de gas, defensa, organizaciones sin fines de lucro y gobierno.

Según Flashpoint, el actor de amenazas BlackMatter registró una cuenta en los foros en idioma ruso XSS y Exploit el 19 de julio, y después lo siguió rápidamente con una publicación que indica que están buscando comprar acceso a redes corporativas infectadas que comprenden entre 500 y 15,000 hosts en Estados Unidos, Canadá, Australia y el Reino Unido, y con ingresos de más de 100 millones de dólares al año, lo que podría indicar una operación de ransomware a gran escala.

> *«El actor depositó 4 BTC (aproximadamente 150 mil dólares) en su cuenta de depósito en garantía. Los grandes*
> *depósitos en el foro indican la seriedad del actor de la amenaza. BlackMatter no declara abiertamente que es un operador colectivo de ransomware, lo que técnicamente no infringe las reglas de los foro, aunque el lenguaje de su publicación, así como objetivos, indican claramente que son un operador colectivo de ransomware»,* dijeron los investigadores de Flashpoint.

El 27 de julio, se dice que el grupo comenzó a reclutar activamente socios y afiliados utilizando el servidor Jabber del foro Exploit, para difundir su mensaje de reclutamiento, en el que afirman estar buscando probadores de penetración experimentados con conocimiento en sistemas Windows y Linux, así como proveedores de acceso inicial, que vendería su acceso o

trabajaría por un porcentaje de las ganancias.

El mes pasado, la firma de seguridad empresarial Proofpoint, reveló cómo las bandas de ransomware compran cada vez más el acceso de grupos de ciberdelincuentes independientes que se infiltran en los principales objetivos y luego les proporcionan un punto de entrada para implementar operaciones de robo de datos y cifrado a cambio de una parte de las ganancias robadas.

La aparición de BlackMatter coincide con la desaparición de DarkSide y REvil a raíz de incidentes de ransomware altamente publicitados de Colonial Pipeline, JBS y Kaseya, lo que genera especulaciones de que los grupos eventualmente pueden cambiar de marca y resurgir bajo una nueva identidad.

Aunque la evidencia concreta que conecta a BlackMatter y los grupos ahora desaparecidos es escasa, las *«reglas similares sobre la focalización»* y el hecho de que REvil previamente etiquetó su clave del Registro de Windows como *«BlackLivesMatter»* dan crédito a las teorías de que REvil puede haber tomado una pausa temporal y desaparecido después de una ola de ataques de alto perfil.

> *«Es posible que los imitadores estén imitando de forma intencional el comportamiento de REvil para ganar credibilidad inmediata por ser supuestamente la reencarnación de REvil»*, dijo Flashpoint.

Sin embargo, BlackMatter no es el único que ha llegado recientemente. La semana pasada, la compañía de seguridad surcoreana S2W Labs, informó sobre Haron, otro de los últimos participantes en el ecosistema del ciberdelito que lanzó su aparición este mes y toma prestado en gran medida de variantes de ransomware anteriores como Thanos y Avaddon, ahora descontinuado.