Los individuos responsables de un nuevo grupo de ransomware denominado Hunters International han obtenido el código fuente y la infraestructura de la ahora desmantelada operación Hive para iniciar sus propias iniciativas en el ámbito de amenazas.

> *«Se percibe que el liderazgo del grupo Hive tomó la decisión estratégica de suspender sus operaciones y transferir sus activos remanentes a otro grupo, Hunters International»,* declaró Martin Zugec, director de soluciones técnicas en Bitdefender, en un informe publicado la semana pasada.

Hive, en su momento una operación prolífica de ransomware como servicio (RaaS), fue desarticulada como parte de una operación coordinada de las fuerzas del orden en enero de 2023.

Aunque es habitual que los actores de ransomware reorganicen, cambien de nombre o disuelvan sus actividades tras incautaciones de este tipo, otra posibilidad es que los desarrolladores principales transfieran el código fuente y demás infraestructura que poseen a otro actor de amenazas.

Informes sobre Hunters International como un posible cambio de marca de Hive surgieron el mes pasado después de identificar varias similitudes de código entre las dos variantes. Hasta la fecha, ha afectado a cinco víctimas.

No obstante, los actores de amenazas detrás de esta operación han intentado desmentir estas especulaciones, indicando que adquirieron el código fuente y el sitio web de Hive de sus desarrolladores.

> *«El grupo parece poner un énfasis mayor en la exfiltración de datos. Cabe destacar que todas las víctimas reportadas tuvieron datos exfiltrados, pero no todas tuvieron sus datos cifrados, convirtiendo a Hunters International en más un grupo de extorsión de datos»,* señaló Zugec.

El análisis de Bitdefender del ejemplar de ransomware revela sus fundamentos basados en Rust, un hecho respaldado por el cambio de Hive a este lenguaje de programación en julio de 2022 debido a su mayor resistencia al análisis inverso.

> *«En términos generales, a medida que el nuevo grupo adopta este código de ransomware, parece que han buscado simplificar las cosas»,* expresó Zugec.

> *«Han reducido el número de parámetros en la línea de comandos, optimizado el proceso de almacenamiento de claves de cifrado y vuelto el malware menos prolijo en comparación con versiones anteriores».*

Además de incorporar una lista de exclusiones de extensiones de archivos, nombres de archivos y directorios para ser excluidos del cifrado, el ransomware ejecuta comandos para prevenir la recuperación de datos y poner fin a diversos procesos que podrían interferir potencialmente con el proceso.

> *«Aunque Hive ha sido uno de los grupos de ransomware más peligrosos, aún está por verse si Hunters International demostrará ser igualmente o incluso más formidable»,* destacó Zugec.

> *«Este grupo surge como un nuevo actor de amenazas que comienza con un conjunto de herramientas maduras y parece ansioso por demostrar sus capacidades, [pero] enfrenta la tarea de demostrar su competencia antes de poder atraer afiliados de alto calibre».*