La plataforma de coordinación de vulnerabilidades y recompensas por errores de HackerOne, reveló el viernes que un ex empleado de la compañía accedió indebidamente a los informes de seguridad que se le enviaron para realizar acciones de su beneficio personal.

> *«La persona reveló de forma anónima esta información de vulnerabilidad fuera de la plataforma HackerOne con el objetivo de reclamar recompensas adicionales. En menos de 24 horas, trabajamos rápidamente para contener el incidente identificando al entonces empleado y cortando el acceso a los datos»,* dijo la compañía.

El empleado, que tuvo acceso a los sistemas de HackerOne entre el 4 de abril y el 23 de junio de 2022, para evaluar las divulgaciones de vulnerabilidades asociadas con diferentes programas de clientes, fue despedido de la compañía con sede en San Francisco el 30 de junio pasado.

Al calificar dicho incidente como una *«clara violación»* de sus valores, cultura, políticas y contratos de trabajo, HackerOne dijo que un cliente no identificado le alertó sobre la violación el 22 de junio y le pidió que *«investigara una revelación de vulnerabilidad sospechosa»* por medio de un comunicado fuera de la plataforma de un individuo identificado como *«rzlr»* utilizando un lenguaje *«agresivo e intimidante».*

Después, el análisis de los datos de registro internos utilizados para monitorear el acceso de los empleados a las revelaciones de los clientes rastreó la exposición a un infiltrado malicioso, cuyo objetivo, dijo, era volver a enviar los informes de vulnerabilidad duplicados a los mismos clientes que usaban la plataforma para recibir pagos monetarios.

«El actor de amenazas creó una cuenta sockpuppet de HackerOne y recibió recompensas en un puñado de divulgaciones», dijo HackerOne en un informe de incidente y agregó que siete de sus clientes recibieron comunicación directa del actor de amenazas.

> *«Siguiendo el rastro del dinero, recibimos la confirmación de que la recompensa del atacante estaba vinculada a una cuenta que beneficiaba financieramente a un empleado de HackerOne en ese momento. El análisis del tráfico de red del actor de amenazas proporcionó evidencia complementaria que conectaba las cuentas principal y sockpuppet del actor de amenazas».*

HackerOne también dijo que notificó de forma individual a los clientes sobre los informes de errores exactos a los que accedió la parte malintencionada junto con el momento del acceso, al mismo tiempo que enfatizó que no encontró evidencia de que los datos de vulnerabilidad hayan sido mal utilizados u otra información del cliente accedida.

Además, la compañía dijo que tiene como objetivo implementar mecanismos de registro adicionales para mejorar la respuesta a incidentes, aislar datos para reducir el *«radio de explosión»* y mejorar los procesos para identificar accesos anómalos y detectar amenazas internas de forma proactiva.