Desde inicios de 2023, se ha detectado que agencias de empleo y empresas minoristas, principalmente ubicadas en la región de Asia-Pacífico (APAC), son objeto de ataques por parte de un actor de amenazas hasta ahora no registrado, conocido como ResumeLooters. Su objetivo principal es robar información sensible.

El Grupo-IB, con sede en Singapur, informó que las actividades de este grupo de piratas informáticos se centran en plataformas de búsqueda de empleo y en el robo de currículums, comprometiendo hasta 65 sitios web entre noviembre de 2023 y diciembre de 2023.

Se estima que los archivos sustraídos contienen 2,188,444 registros de datos de usuarios, de los cuales 510,259 provienen de sitios web de búsqueda de empleo. Dentro de este conjunto de datos se encuentran más de dos millones de direcciones de correo electrónico únicas.

> Nikita Rostovcev, investigador de seguridad, mencionó en un informe que *«mediante ataques de inyección SQL contra sitios web, el actor de amenazas intenta robar bases de datos de usuarios que pueden incluir nombres, números de teléfono, correos electrónicos y fechas de nacimiento, así como información sobre la experiencia laboral, historial de empleo y otros datos personales sensibles de los buscadores de empleo».*
>
> *«El actor de amenazas pone a la venta los datos robados en canales de Telegram».*

Group-IB también identificó evidencia de infecciones de scripting entre sitios (XSS) en al menos cuatro sitios web legítimos de búsqueda de empleo. Estas infecciones están diseñadas para cargar scripts maliciosos que muestran páginas de phishing capaces de recopilar credenciales de administradores.

ResumeLooters es el segundo grupo, después de GambleForce, que se ha encontrado llevando a cabo ataques de inyección SQL en la región de APAC desde finales de diciembre de 2023.

La mayoría de los sitios web comprometidos tienen su base en India, Taiwán, Tailandia, Vietnam, China, Australia y Turquía, aunque también se han reportado compromisos en Brasil, EE. UU., Rusia, México e Italia.

El modus operandi de ResumeLooters implica el uso de la herramienta de código abierto sqlmap para realizar ataques de inyección SQL y ejecutar cargas útiles adicionales, como la herramienta de prueba de penetración BeEF (acrónimo de Browser Exploitation Framework) y código JavaScript malicioso diseñado para recopilar datos sensibles y redirigir a los usuarios a páginas de recolección de credenciales.

El análisis de la infraestructura del actor de amenazas por parte de la empresa de ciberseguridad revela la presencia de otras herramientas como Metasploit, dirsearch y xray, junto con una carpeta que alberga los datos robados.

La campaña parece tener motivaciones financieras, ya que ResumeLooters ha creado dos

canales de Telegram llamados □□□□□□ y □□□□□□ el año pasado para vender la información.

> *«ResumeLooters es otro ejemplo de cuánto daño se puede causar con solo un puñado de herramientas públicamente disponibles. Estos ataques son impulsados por una seguridad deficiente, así como prácticas inadecuadas de gestión de bases de datos y sitios web»,* dijo Rostovcev.
>
> *«Es sorprendente ver cómo algunos de los ataques SQL más antiguos pero notoriamente efectivos siguen siendo prevalentes en la región. No obstante, destaca la persistencia del grupo ResumeLooters, ya que experimentan con diversos métodos para explotar vulnerabilidades, incluyendo ataques XSS».*