Microsoft y el proveedor de servicios de autenticación Okta, dijeron que se encuentran investigando las denuncias de una posible violación alegada por el grupo de hackers LAPSUS$.

El desarrollo, que fue informado primero por Vice y Reuters, se produce luego de que el grupo de hackers publicara capturas de pantalla y el código fuente en su canal de Telegram de lo que dijo, eran los proyectos y sistemas internos de las empresas.

El archivo filtrado, de 37 GB, muestra que el grupo pudo haber accedido a los repositorios relacionados con Bing, Bing Maps y Cortana de Microsoft, y las imágenes destacan la suite Atlassian de Okta y los canales internos de Slack.

> *«Para un servicio que impulsa los sistemas de autenticación de muchas de las corporaciones más grandes (y aprobado por FEDRAMP), creo que estas medidas de seguridad son bastante deficientes»,* dijo el grupo de hackers en Telegram.

Además, el grupo dijo que violó la seguridad de LG Electronics (LGE) por «segunda vez» en un año.

Bill Demirkapi, investigador de seguridad independiente, dijo que *«LAPSUS$ parece haber obtenido acceso al inquilino de Cloudflare con la capacidad de restablecer las contraseñas de los empleados y la empresa no reconoció públicamente ninguna infracción durante al menos dos meses».*

Desde entonces, LAPSUS$ declaró que no violó las bases de datos de Okta y que *«nuestro enfoque SOLO estaba en los clientes de Okta».* Esto podría tener serias implicaciones para otras agencias gubernamentales y empresas que confían en Okta para autenticar el acceso de los usuarios a los sistemas internos.

> *«A fines de enero de 2022, Okta detectó un intento de comprometer la cuenta de un ingeniero de atención al cliente externo que trabajaba para uno de nuestros subprocesadores. El subprocesador investigó y contuvo el asunto»,* dijo el director ejecutivo de Okta, Todd McKinnon.

> *«Creemos que las capturas de pantalla compartidas en línea están conectadas con este evento de enero. Según nuestra investigación hasta la fecha, no hay evidencia de actividad maliciosa en curso más allá de la actividad detectada en enero»,* agregó.

CLoudflare, en respuesta, dijo que está restableciendo las credenciales de Okta de los empleados que cambiaron sus contraseñas en los últimos cuatro meses, por precaución.

A diferencia de los grupos de ransomware tradicionales que siguen el libro de jugadas de doble extorsión, de robar datos de una víctima y luego cifrar la información a cambio de un pago, el nuevo participante en el panorama de amenazas se enfoca más en el robo de datos y usarlo para chantajear a los objetivos.

En los meses transcurridos desde que se activó a fines de diciembre de 2021, el grupo del cibercrimen acumuló una larga lista de víctimas de alto perfil, incluidas las empresas NVIDIA, Samsung, Mercado Libre, Vodafone y recientemente, Ubisoft.

> *«Cualquier ataque exitoso contra un proveedor de servicios o un desarrollador de software puede tener un impacto mayor que el alcance de ese ataque inicial. Se debe alertar a los usuarios de los servicios y plataformas sobre el hecho de que existen posibles ataques a la cadena de suministro de los que será necesario defenderse»*, dijo Mike DeNapoli, arquitecto principal de seguridad de Cymulate.