El 59% del malware de las empresas en América Latina proviene de apps en la nube: Netskope

Ciudad de México, 10 de julio de 2024. El uso de aplicaciones en la nube en América Latina se incrementa de manera sustancial mes con mes. Herramientas como One Drive y Google Drive se han vuelto parte esencial de las operaciones de millones de empresas; pero también se han posicionado como blancos predilectos de los cibercriminales quienes buscan constantemente nuevos métodos para propagar sus amenazas.

El Reporte de Amenazas de Netskope Labs recién publicado destaca que el 59% de todas las descargas de malware de la región provienen de las aplicaciones nube, como las antes mencionadas. En un contexto donde la adopción de la nube sigue en aumento, las organizaciones deben redoblar sus esfuerzos para proteger sus datos y sistemas.

- Apps en la nube, parte de las operaciones cotidianas en Latam

Los usuarios empresariales en América Latina interactúan con un promedio de 25 aplicaciones en la nube cada mes. Aunque esto incluye suites para el ámbito corporativo y laboral, como Microsoft OneDrive y Google Drive, también destaca la prevalencia de otras plataformas como WhatsApp, que es utilizada con fines empresariales por casi una cuarta parte de todos los usuarios en la región, quienes comparten en ella información y datos sobre sus organizaciones.

OneDrive es la aplicación en la nube más utilizada en el ámbito empresarial en América Latina, con un 48% de uso, seguida de Google Drive con un 30%, Microsoft Teams con un 25%, WhatsApp con un 23% y Outlook Mail con un 22%. La popularidad de estas aplicaciones resalta la necesidad de políticas robustas para el manejo seguro de datos sensibles dentro de las organizaciones.

- El abuso de las apps en la nube por los entes maliciosos

A nivel global, aproximadamente la mitad de todas las descargas de malware HTTP/HTTPS provienen de aplicaciones en la nube populares, y América Latina no es una excepción. Las principales aplicaciones utilizadas para descargar malware en la región incluyen Outlook.com, que representa el 18% de todas las descargas de malware en la nube, seguido de OneDrive con un 17%, Azure Blob Storage con un 13%, GitHub con un 12% y SharePoint con un 5.8%.

En particular, las descargas de malware desde Outlook.com provienen tanto de cuentas personales de Outlook como de instancias organizacionales de Microsoft 365. Las cuentas de correo personal representan dos tercios de todas las descargas de malware desde Outlook.com. Los tipos de malware más comunes descargados desde Outlook.com son documentos PDF maliciosos utilizados en campañas de phishing, que dirigen a las víctimas a sitios web fraudulentos o a números de teléfono maliciosos.

Entre las familias de malware más prevalentes que afectan a los usuarios en América Latina se encuentra el troyano bancario Grandoreiro, el cual es típicamente distribuido como parte de una campaña de phishing. Este troyano se encuentra entre los cinco principales tipos de malware detectados por Netskope en la región en los últimos 12 meses, junto con Downloader.BanLoad, Infostealer.AgentTesla, Phishing.PhishingX y Trojan.Ramnit.

Grandoreiro es un troyano bancario de múltiples componentes que opera bajo un modelo de malware como servicio (MaaS). Los atacantes suelen desplegar Grandoreiro en campañas de phishing para controlar las cuentas bancarias de sus víctimas, vaciando las cuentas y lavando los fondos robados.

El informe de Netskope destaca la urgente necesidad de que las organizaciones en América Latina implementen controles de seguridad sólidos para protegerse contra las amenazas que provienen del uso generalizado de aplicaciones en la nube. La combinación de políticas organizacionales, educación sobre seguridad y tecnologías avanzadas es crucial para mitigar los riesgos y salvaguardar los datos sensibles en un entorno digital cada vez más complejo.

Este informe es un llamado a la acción para las empresas en América Latina, recordándoles que, a medida que adoptan la nube y otras tecnologías avanzadas, también deben estar preparadas para enfrentar los desafíos de seguridad que estas conllevan.

Paolo Passeri, director de ciberinteligencia de Netskope, dijo:

"LATAM continúa siendo afectada por varias familias de malware bancario específicamente diseñadas para esta región. Estas operaciones no solo parecen sobrevivir a los intentos de eliminación (Grandoreiro), sino que también continúan evolucionando con nuevas características que las hacen más evasivas, incluido la explotación de servicios legítimos en la nube en varias etapas de la cadena de ataque".

Sobre Netskope

Netskope, empresa líder global en SASE, ayuda a las organizaciones a aplicar principios de confianza cero (Zero Trust) e innovaciones en Inteligencia Artificial/Machine Learning para proteger datos y defenderse contra amenazas cibernéticas. Rápida y fácil de usar, la plataforma Netskope One y su motor de confianza cero patentado proporcionan acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos en cualquier lugar donde se encuentren. Miles de clientes confían en Netskope y en su poderosa red NewEdge para reducir riesgos y obtener una visibilidad sin igual en cualquier actividad en la nube, la web y aplicaciones privadas, proporcionando seguridad y acelerando el rendimiento de los sistemas. Obtén más información en https://www.netskope.com/