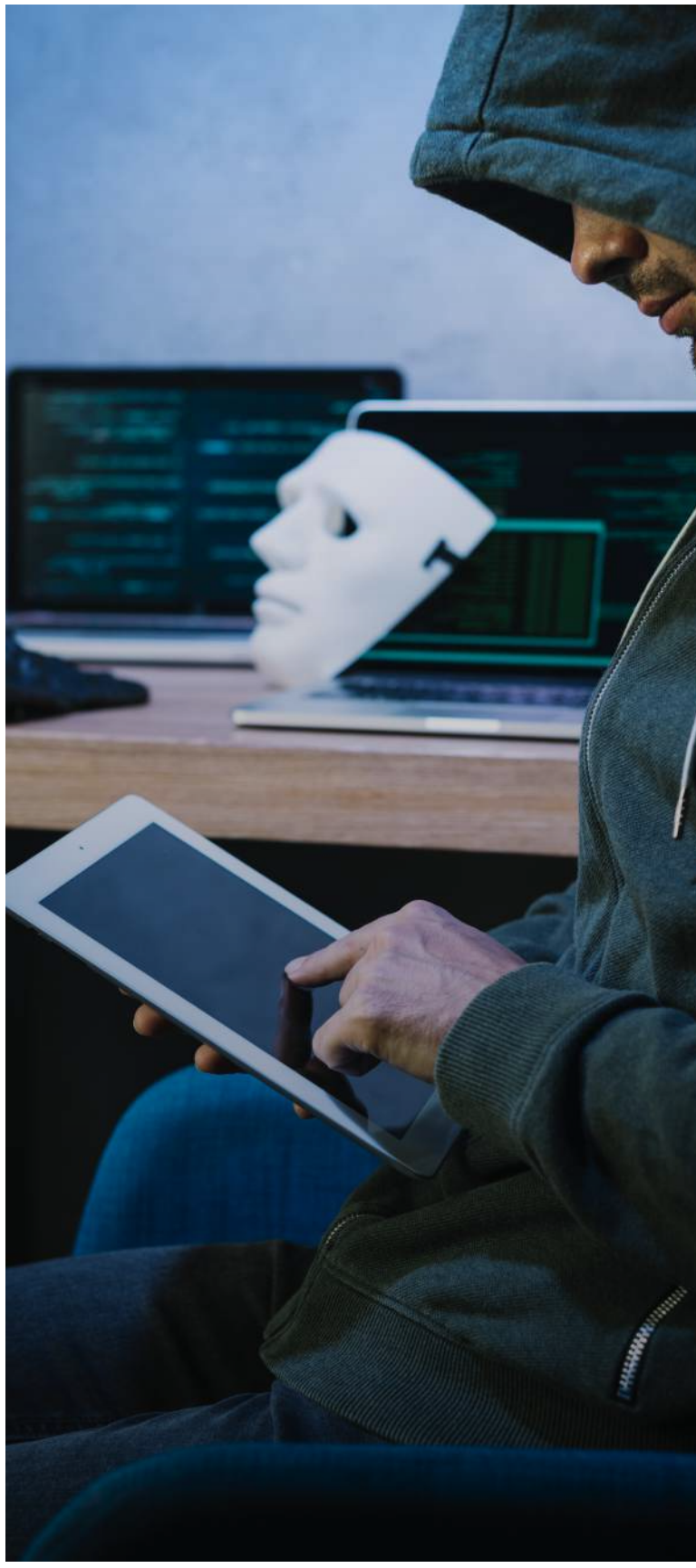
Aplicaciones en la nube, principal vía distribución de Malware

La adopción de aplicaciones en la nube sigue aumentando en América Latina, al permitir a las empresas mejorar su productividad y crear fuerzas de trabajo híbridas.



Al igual que en otras regiones, **en Latinoamérica los usuarios utilizan cada vez más aplicaciones en la nube.** Un informe de Amenazas para LATAM, señala que el número de aplicaciones con las que interactúa un usuario en América Latina ha aumentado de 22 a 25 aplicaciones en los últimos doce meses (julio de 2022 a junio 2023), por delante de otras zonas. La media, 23 aplicaciones, es ligeramente superior a la de otras regiones (22). El 1% de los usuarios de América Latina usó 75 aplicaciones al mes, frente a las 96 de otras regiones.

Al respecto de los ritmos de descarga y carga de datos de aplicaciones en la nube, el informe destaca que, en el primer caso, es similar al de otras zonas: con un 95% de usuarios descargando datos de aplicaciones en la nube cada mes, frente al 93% en otras geografías; y superior en el segundo. De media, el 72% de los usuarios de América Latina cargó datos en aplicaciones en la nube, frente al 64% de los de otros territorios. Asimismo, el número de usuarios que subió información a aplicaciones en la nube aumentó un 4% entre julio de 2022 y junio de 2023, al ritmo de otras regiones.

Distribución de malware en la nube

La popularidad de la entrega de malware en la nube en las organizaciones latinoamericanas ha aumentado significativamente en los últimos 12 meses, pasando del 47% en julio de 2022 al 71% en junio de 2023.

De este modo, la media de descargas de malware durante este periodo es ligeramente superior en comparación con otras regiones, con un 61% de descargas de malware de usuarios en América Latina en comparación con el 57% en otras zonas.

Los atacantes intentan pasar desapercibidos distribuyendo contenido malicioso a través de aplicaciones populares en la nube como OneDrive, que **representó el 21% de todas las descargas de malware en la nube, seguida de Amazon S3 (con un 11% de usuarios en promedio en los últimos 12 meses) y Outlook (que supuso un 7,5% de las descargas).**

Abusar de las aplicaciones en la nube para la distribución de malware permite a los atacantes evadir los controles de seguridad que se basan principalmente en listas de bloqueo de dominios y filtrado de URL, o que no inspeccionan el tráfico en la nube.

En comparación con otras regiones, América Latina tiene una media más alta de descargas de malware desde la nube, con un 61% de media, solo por detrás de Australia. Los tipos más comunes de malware bloqueados en América Latina fueron los troyanos, seguidos de los descargadores y los backdoors. Grandoreiro y Mekotio, que son troyanos bancarios, se encuentran entre las principales familias de malware bloqueadas en América Latina, mientras que LockBit y BlackCat destacan entre los ransomware más habituales bloqueados en el mismo periodo. En cuanto a las puertas traseras, Remcos, Quakbot y NjRAT (también conocido como Bladabindi) fueron los principales programas maliciosos bloqueados.

Principales recomendaciones de seguridad

Se recomienda a las organizaciones en América Latina que revisen su postura de seguridad para asegurarse de que están adecuadamente protegidas, con recomendaciones como:

- **Inspeccionar todas las descargas HTTP y HTTPS**, incluido todo el tráfico web y en la nube, para evitar que el malware se infiltre en la red.
- **Comprobar** que los tipos de archivos de alto riesgo, como los ejecutables y los comprimidos, se inspeccionan minuciosamente mediante una combinación de análisis estáticos y dinámicos antes de ser descargados.
- **Configurar políticas para bloquear descargas de aplicaciones** e instancias que no se utilizan en la organización para reducir la superficie de riesgo a solo aquellas aplicaciones e instancias que son necesarias para el negocio.
- **Establecer políticas para bloquear las cargas a aplicaciones** e instancias que no se utilizan en su organización para reducir el riesgo de exposición accidental o deliberada de datos por parte de personas con acceso a información privilegiada o el abuso por parte de atacantes.
- **Utilizar un Intrusion Prevention System (IPS)** que pueda identificar y bloquear patrones de tráfico malicioso, como el tráfico de comando y control asociado al malware más popular. El bloqueo de este tipo de comunicación puede evitar daños mayores al limitar la capacidad del atacante para realizar acciones adicionales.

Fuente de información: CIO Magazine