**Telecom, la industria más afectada por el malware originado en la nube: Netskope Threat Labs**

CIUDAD DE MÉXICO. 20 de junio de 2024.- Existe un incremento notable en la incidencia de ciberataques en contra de aplicaciones empresariales del sector de telecomunicaciones, enfocados en propagar malware entre los usuarios de esas empresas, de acuerdo con el reciente informe de amenazas de Netskope Threat Labs.   
  
En el reporte, la firma indica que se trata de una tendencia en aumento debido a la adopción continua de aplicaciones en la nube en esta industria, donde los usuarios interactúan con una pequeña selección de aplicaciones populares, incluidas las de Microsoft.

En ese contexto, las empresas de telecomunicaciones son las mayores víctimas del malware originado en la nube, con un margen 7% más alto en comparación con otras industrias.

* Los hallazgos clave incluyen de este reporte, incluyen:

**Adopción de aplicaciones en la nube:** Los usuarios en la industria de telecomunicaciones suben y descargan archivos a aplicaciones en la nube a una tasa similar a otras industrias, pero tienden a interactuar con menos aplicaciones en promedio. El usuario promedio en telecomunicaciones interactúa con 24 aplicaciones en la nube por mes, con una fuerte preferencia por Microsoft OneDrive, Teams y Outlook como las tres aplicaciones más populares en la industria.

Microsoft OneDrive también es la aplicación más popular para subir datos, con el 30% de los usuarios de la industria de telecomunicaciones subiendo datos a OneDrive diariamente, un 50% más que el promedio en todas las industrias. Del mismo modo, Microsoft OneDrive es la aplicación más popular para descargas en la industria de telecomunicaciones, con el 35% de los usuarios descargando de ella.

**Abuso de apps en la nube:** El porcentaje de descargas de malware de los usuarios de la industria de telecomunicaciones cayó en línea con la tendencia global, tocando fondo en la segunda mitad de 2023 y comenzando a aumentar nuevamente a principios de 2024.

Las organizaciones en la industria de telecomunicaciones son las mayores víctimas del malware originado en la nube por un considerable margen del 7% en comparación con otras industrias. Microsoft OneDrive y GitHub tuvieron la mayor cantidad de descargas de malware, seguidas por Outlook.

Las otras aplicaciones en el top 10 son similares a las de otras industrias con sólo diferencias menores, incluyendo más descargas de malware desde SourceForge, el sitio web de desarrollo de software de código abierto, y Google Cloud Storage.

**Malware y ransomware:** Entre las familias de malware más prevalentes que atacan a las organizaciones en la industria de telecomunicaciones se encuentran el troyano de acceso remoto Remcos, el descargador Guloader y el ladrón de información AgentTesla.

Sobre los hallazgos, Paolo Passeri, jefe de Inteligencia Cibernética en Netskope, dijo;

*“Los usuarios en la industria de telecomunicaciones tienden a interactuar con menos aplicaciones en la nube en comparación con otros sectores, pero el porcentaje de malware entregado desde la nube es 7 puntos porcentuales más alto que en otros sectores. Esto indica que los empleados dentro del sector tienen una actitud más abierta hacia los servicios en la nube y esto inevitablemente se refleja en una mayor exposición a amenazas. Están más familiarizados con herramientas en línea como aplicaciones en la nube y esta cifra muestra que los actores de amenazas tienden a explotar esta familiaridad*", indicó.

*“Esta actitud abierta hacia los servicios en línea también es visible en las familias de malware que apuntan a los usuarios de telecomunicaciones. En comparación con otros sectores, hay muchas más familias de malware que atacan a este sector, con una amplia gama de amenazas que abarcan desde IoT (el omnipresente Mirai) hasta descargadores (BanLoad y Guloader), troyanos bancarios (Grandoreiro), ladrones de información (como AgentTesla y Redline) y documentos PDF que fungen como anzuelo de phishing*", agrega.

*“Es interesante que muchas de estas amenazas se caracterizan por la explotación de servicios en la nube auténticos y bien reputados a lo largo de diferentes etapas de la cadena de ataque: Guloader almacena la carga útil cifrada en servicios en la nube legítimos como Microsoft OneDrive o Google Drive, Grandoreiro a menudo ataca a Microsoft Azure (pero también de AWS y Google) para entregar la carga útil final, e incluso los documentos PDF anzuelo de phishing a menudo se alojan en servicios de almacenamiento en la nube legítimos para parecer más realistas y legítimos”,* concluye.

*El informe se basa en datos recopilados sobre un subconjunto de los más de 2,500 clientes de Netskope, quienes dieron autorización previa para que sus datos fueran analizados de esta manera.*

**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/>