
netskope
Cloud and Threat Report:
Tendencias mundiales de malware en la nube y la web
EN COLABORACIÓN CON
netskope
THREAT LABS

RESUMEN EJECUTIVO

En esta edición del Informe sobre amenazas en la nube examinamos los últimos doce meses de descargas de malware de la nube y la web. El tipo de malware que se ha descargado mucho más que otros ha sido el troyano, ya que los ciberdelincuentes usan diferentes familias de troyanos y técnicas de ingeniería social para escoger a sus víctimas. En cuanto a los tipos de archivos, los más afectados han sido los archivos EXE/DLL de Windows o los documentos de Microsoft Office, pues los ciberdelincuentes siguen teniendo como objetivo principal Microsoft Windows, el sistema operativo de escritorio más popular en el ámbito empresarial.

También analizamos las fuentes de las descargas de malware y observamos que el 53 % proviene de sitios web tradicionales y el 47 % de aplicaciones en la nube. Las descargas de la web se hacen en diferentes categorías de sitios, y las principales son sitios de tecnología y servidores de contenido. Las descargas de la nube proceden de cientos de aplicaciones, con las aplicaciones de almacenamiento en la nube a la cabeza. Tanto las descargas de malware de la web como de la nube suelen provenir de servidores ubicados en las mismas zonas geográficas de las víctimas.

Por último, conoceremos algunas de las técnicas que usan los ciberdelincuentes para distribuir malware, analizando en detalle los orígenes de referencia más populares de las descargas. Entre los principales se incluyen los motores de búsqueda, ya que los ciberdelincuentes usan técnicas de SEO para conseguir un buen posicionamiento en los buscadores. Los sitios web afectados y los sitios web maliciosos diseñados para imitar sitios web seguros también son orígenes de referencia frecuentes.

PUNTOS DESTACADOS

- **Los troyanos representan el 77 % de todas las descargas de malware de la nube y la web.** Se usan para conseguir un punto de apoyo inicial y para distribuir diferentes cargas que se ejecutan en fases siguientes, como puertas traseras, ladrones de información (infostealers) y ransomware.
- **El 47 % de las descargas de malware proviene de aplicaciones en la nube** y el 53 % de sitios web tradicionales, puesto que los ciberdelincuentes combinan la nube y la web para captar a sus víctimas.
- **Las descargas que involucran phishing están en auge, ya que los ciberdelincuentes usan técnicas de SEO** para conseguir que los archivos PDF maliciosos tengan un buen posicionamiento en los motores de búsqueda más populares, como Google y Bing.
- **Los archivos EXE y DLL representan casi la mitad de todas las descargas de malware,** pues los ciberdelincuentes se siguen centrando en Microsoft Windows, mientras que los archivos de Microsoft Office maliciosos han disminuido y regresado a niveles anteriores a Emotet.
- **Casi todas las descargas de malware provienen de servidores ubicados en las mismas regiones de sus víctimas,** ya que los ciberdelincuentes distribuyen el malware por todo el mundo para evitar las geovallas.

ACERCA DE ESTE INFORME

Netskope ofrece protección de datos y frente a amenazas a millones de usuarios en todo el mundo. La información incluida en este documento se basa en datos de uso anónimos recopilados en la plataforma Netskope Security Cloud relacionados con un subgrupo de clientes de Netskope a quienes les hemos solicitado su autorización previa. En estas páginas, encontrará información sobre detecciones de la solución Next Generation Secure Web Gateway (Next Gen SWG) de Netskope, sin contemplar la magnitud de la incidencia de cada amenaza individual. Las estadísticas de este informe se basan en un periodo de doce meses, del 1 de abril de 2021 al 31 de marzo de 2022.

Netskope Threat Labs

El equipo de Netskope Threat Labs está integrado por los investigadores de malware y amenazas en la nube más destacados del sector, quienes descubren, analizan y diseñan defensas frente a las amenazas de datos y en la nube más recientes que acechan a las empresas. Nuestros investigadores son oradores y voluntarios asiduos de las principales conferencias de seguridad, como DefCon, BlackHat y RSA.

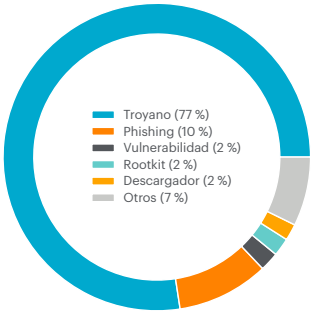
DESCARGAS DE MALWARE

Categorías y familias de malware

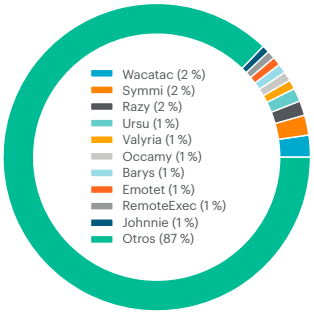
La amplia mayoría (77 %) de todas las descargas de malware de la nube y la web son troyanos. Los troyanos suelen ser la primera etapa de un ciberataque en la que el objetivo es engañar a la víctima para que descargue y ejecute un programa que le permitirá al ciberdelincuente dar el paso inicial. Por lo general, los troyanos se camuflan como software legítimo y se usan para sacar provecho de acontecimientos importantes. Durante la pandemia, por ejemplo, ha circulado una gran variedad de troyanos relacionados con la COVID-19. Los ciberdelincuentes usan troyanos para distribuir cargas que se ejecutan en fases siguientes, como puertas traseras, ladrones de información (infostealers) y ransomware. Si bien la gran mayoría de las descargas de malware son troyanos, no hay una familia de troyanos en concreto que predomine en el mundo. Las diez familias de troyanos más importantes representan solo el 13 % de todas las descargas, y el 87 % restante proviene de una larga lista de familias menos comunes.

Los troyanos representaron la pluralidad de descargas de malware en todas las regiones y la mayoría en cada región menos en Oriente Medio, que tuvo una incidencia más alta de vulnerabilidades que otras regiones. Cuando hablamos de vulnerabilidades, nos referimos a archivos de malware que aprovechan un error o un punto débil cuando la víctima los abre o ejecuta. Las descargas que involucran phishing, también por encima de la media en Oriente Medio, fueron las más altas en África. Las descargas que involucran phishing difieren de los sitios web de phishing tradicionales. Por lo general, son archivos PDF que adoptan la forma de CAPTCHA falsos, solicitudes falsas de intercambio de archivos o facturas falsas, y son parte de una campaña de phishing más amplia. Las descargas que involucran phishing aumentaron en noviembre de 2021 cuando los ciberdelincuentes lograron que figuren en los buscadores populares usando técnicas habituales de SEO (optimización de motores de búsqueda).

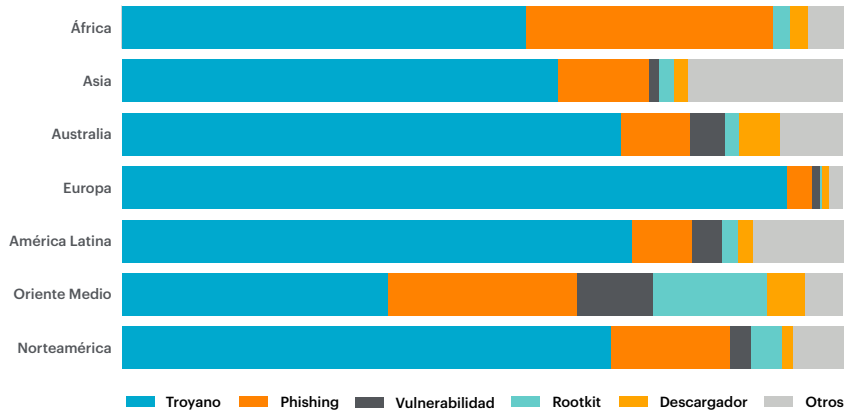
Principales categorías de malware en los últimos 12 meses



Principales familias de troyanos en los últimos 12 meses

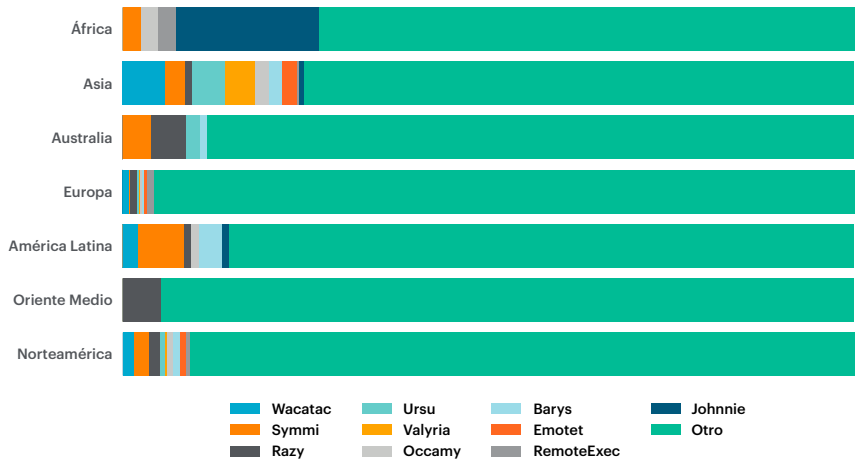


Principales categorías de malware por región



Las principales familias de troyanos varían según la región, ya que las campañas de troyanos suelen apuntar a usuarios que hablan un idioma específico o que viven en un país determinado, o se enmarcan dentro de un acontecimiento de importancia en la región. Algunas familias fueron más predominantes en regiones específicas, como Johnnie en África y Razy en Oriente Medio. En otras regiones, como Norteamérica y Asia, se vieron casi todas las familias principales. En Europa, las familias predominantes representaron un porcentaje menor de todas las descargas de troyanos que en las demás regiones.

Principales familias de malware por región

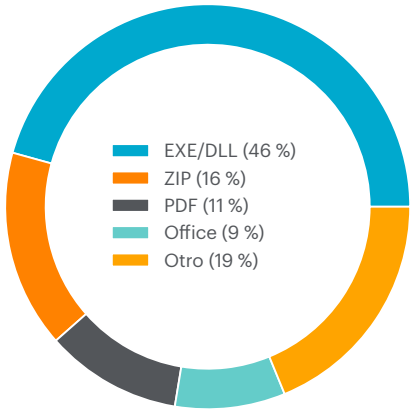


Tipos de archivos de malware

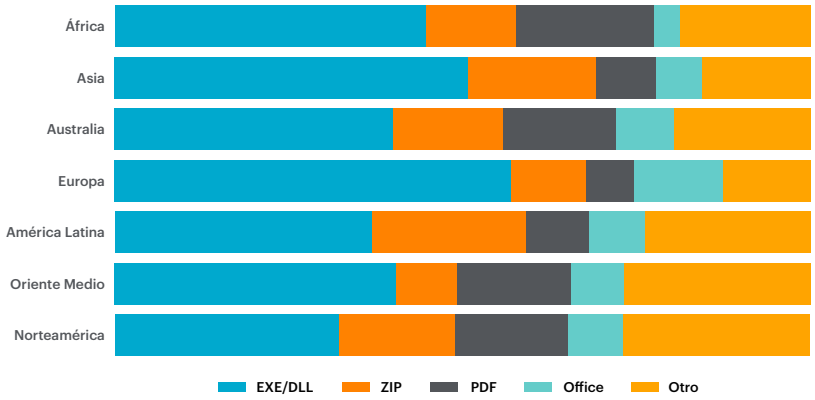
Los archivos portables ejecutables (EXE/DLL), los de Microsoft Office, los PDF y los ZIP representaron el 81 % de todas las descargas de malware en los últimos doce meses. Los documentos de Office maliciosos, que predominaron mucho más en 2020 y principios de 2021 debido a la actividad de Emotet y Dridex, regresaron a los niveles anteriores a Emotet. Es probable que los dos cambios recientes de Microsoft —bloquear las macros de Excel 4.0 y bloquear las macros de VBA de archivos descargados de internet— reduzcan aún más ese porcentaje y obliguen a los ciberdelincuentes a buscar otras estrategias. Además de los PDF de phishing que ya mencionamos en este informe, los ciberdelincuentes también usaron PDF maliciosos para redirigir a los usuarios a sitios de spam, de estafas y de distribución de malware.

En el plano regional, hay muy poca variación en las frecuencias relativas de cada tipo de archivo. Los archivos EXE/DLL siempre representan la pluralidad de descargas de malware, seguidos de archivos PDF, ZIP o de Office. África, que ha tenido el porcentaje más alto de descargas de malware de phishing, también tuvo el porcentaje más alto de descargas de PDF, ya que la mayoría de las descargas de malware de phishing fueron archivos PDF.

Principales tipos de archivos de malware
en los últimos 12 meses



Principales tipos de archivo de malware por región



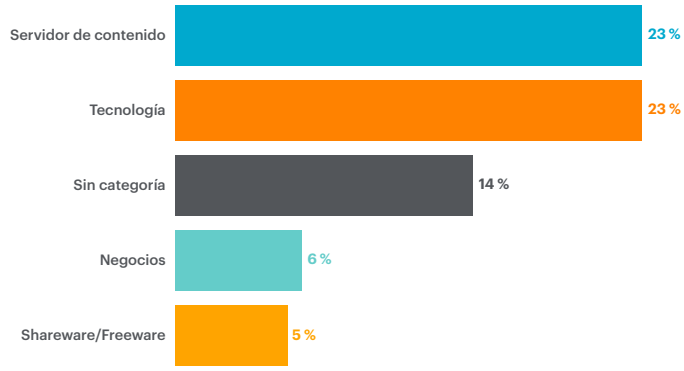
FUENTES DE MALWARE

Descargas de malware de la web

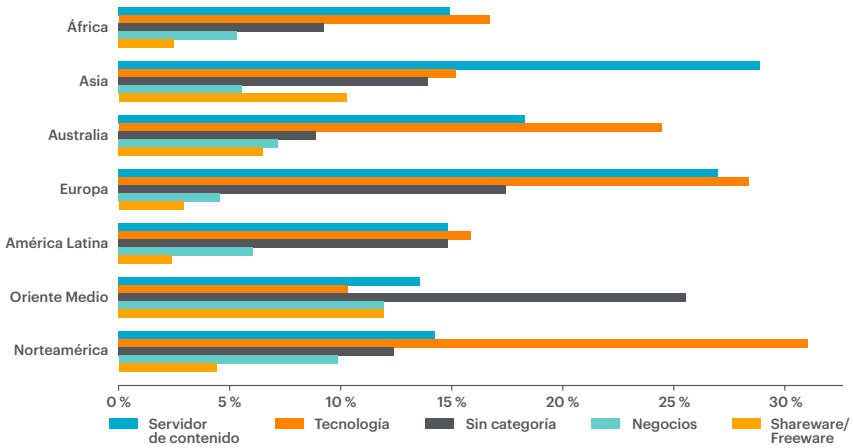
El 53 % de todas las descargas de malware en los últimos doce meses se ha hecho de sitios web tradicionales, en contraste con las aplicaciones en la nube. De las descargas de malware de la web, algunas se iniciaron en sitios que suelen asociarse con malware. Por ejemplo, los sitios «Sin categoría» —aquellos que no son lo suficientemente populares como para asignarles una categoría más específica— representaron el 14 % de las descargas de malware de la web. Asimismo, los sitios «Shareware/Freeware» a veces distribuyen software con spyware y otros programas maliciosos, y representaron el 5 % de las descargas de malware de la web. Las otras categorías principales, como «Tecnología», «Servidor de contenido» y «Negocios», representan una gran parte de la web segura y no se pueden filtrar con facilidad.

En el plano regional, vemos algunas variaciones en las categorías de sitios web más populares en cuanto a descargas de malware. Si bien los sitios web de tecnología ocuparon el primer lugar en casi todas las regiones, los servidores de contenido encabezan la lista en Asia, y los sitios web sin categoría hacen lo suyo en Oriente Medio. En América Latina, no hubo una categoría dominante: las tres categorías principales representaron un 15 % de todas las descargas de malware.

Principales categorías de sitios web de los que se ha descargado malware en los últimos 12 meses

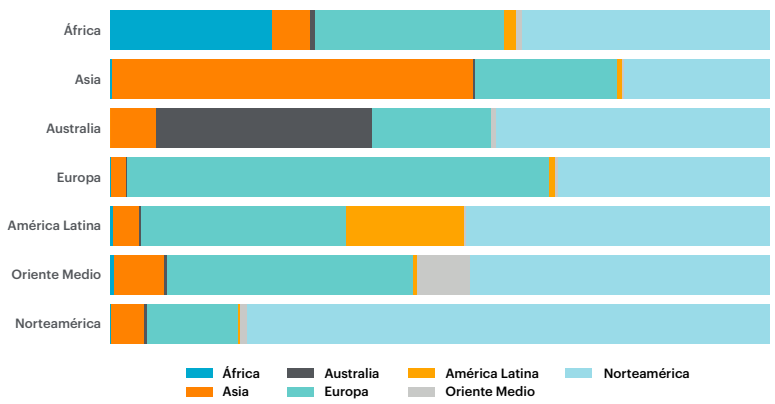


Principales categorías de sitios web de los que se ha descargado malware por región



Los ciberdelincuentes también suelen captar víctimas ubicadas en una región específica con malware alojado en esa misma región. En casi todas las regiones, el mayor número de descargas de malware surgió de la misma región de la víctima. Esto se acentúa más en Norteamérica, donde el 84 % de todas las descargas de malware se hizo de sitios web alojados en Norteamérica. En el lado opuesto está Oriente Medio, donde solo el 7 % de las descargas de malware se originó en la región, ya que muchas provienen de zonas vecinas como Europa y Asia. En promedio entre todas las regiones, el 30 % de las descargas de malware se originó en Europa, y el 42 % en Norteamérica.

Región de origen de descargas de malware

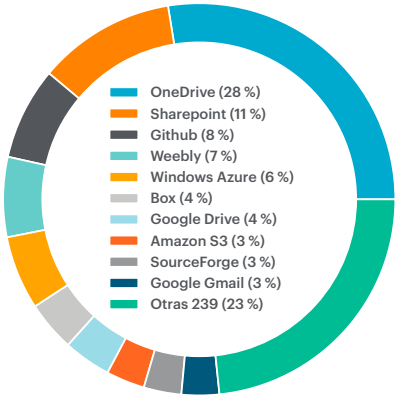


Descargas de malware de la nube

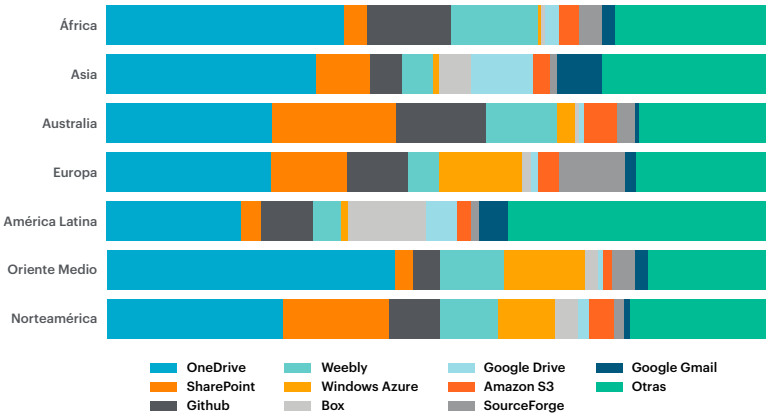
El 47 % de todas las descargas de malware se originó en aplicaciones en la nube con respecto a sitios web tradicionales. En total, se descargó malware de 257 aplicaciones diferentes. Las diez aplicaciones principales representan el 75 % de todas las descargas de malware de la nube. Esto refleja la actividad del ciberdelincuente y la conducta del usuario: los ciberdelincuentes suelen aprovechar aplicaciones populares para llegar a más víctimas, y los usuarios son más propensos a descargar malware de aplicaciones populares que utilizan con frecuencia.

En cada región, las diez aplicaciones principales representaron la mayoría de las descargas de malware de la nube. Microsoft OneDrive fue la más popular en todas las regiones en diferentes niveles. Hubo determinadas aplicaciones que fueron más comunes en una zona geográfica que en las demás: Box en América Latina, Google Drive en Asia y Azure Blob Storage en Oriente Medio. Esto refleja las tácticas del ciberdelincuente y la conducta del usuario en cada región.

Principales aplicaciones de las que
se ha descargado malware en los últimos 12 meses



Principales aplicaciones de las que
se ha descargado malware por región



Origen de las descargas de malware

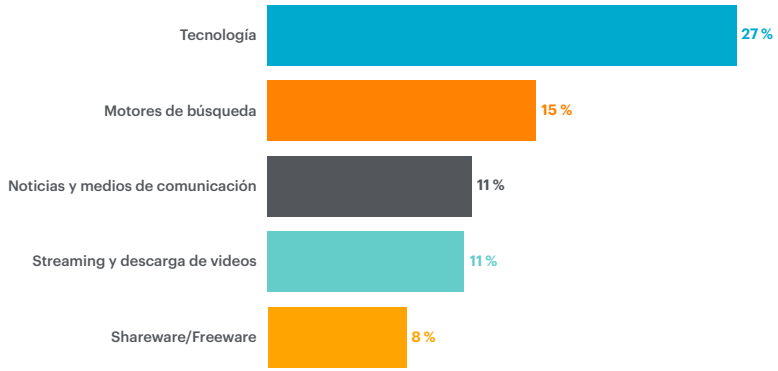
Las descargas de malware de la nube o la web no surgen de forma espontánea. Con los troyanos, los ciberdelincuentes usan la ingeniería social para engañar a sus víctimas para que descarguen malware. Algunas técnicas habituales son diseñar señuelos para sacar provecho de eventos importantes (como la pandemia de COVID-19), crear un clima de urgencia (como una factura que debe abonarse) o hacerse pasar por una aplicación legítima (como una versión gratuita de un videojuego popular). Los ciberdelincuentes también usan métodos técnicos, como vulnerabilidades de software, descargas ocultas o el contrabando de HTML para descargar malware.

El encabezado de solicitud HTTP del «origen de referencia» ofrece algunos datos sobre las técnicas de ingeniería social que usan los ciberdelincuentes para engañar a los usuarios para que descarguen malware. El 14 % fue de aplicaciones en la nube y el 86 % de sitios web tradicionales. Las principales aplicaciones de origen de referencia incluyeron aplicaciones populares de almacenamiento en la nube, colaboración y webmail, es decir, aplicaciones donde los ciberdelincuentes pueden enviar mensajes a sus víctimas de diversas maneras, como correos electrónicos, mensajes directos, comentarios o intercambio de documentos.

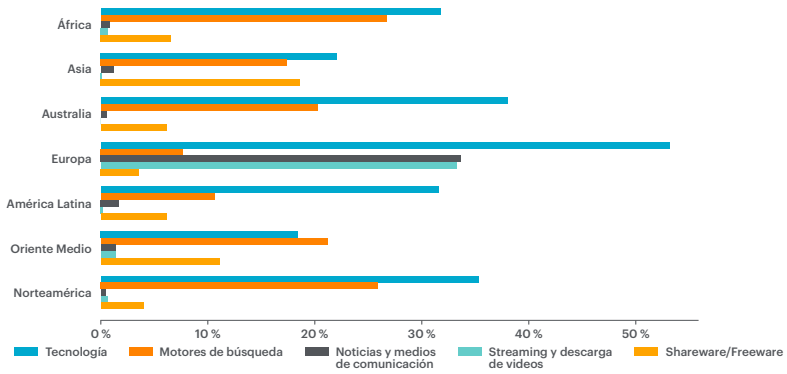
Las principales categorías de origen de referencia web incluyen algunas que suelen asociarse con malware, sobre todo «Shareware/Freeware», aunque predominaron las que, por lo general, no se asocian con programas maliciosos. «Motores de búsqueda» es una entrada particularmente interesante en la lista porque revela lo bien que algunos ciberdelincuentes dominan las técnicas de SEO. Las descargas de malware referidas por motores de búsqueda fueron más que nada archivos PDF maliciosos e incluyen muchos CAPTCHA falsos que redirigieron a los usuarios a sitios de phishing, spam, estafas y malware.

Los sitios de tecnología fueron el principal origen de referencia en todas las regiones, pero hubo diferencias significativas en otras categorías. Europa tuvo el porcentaje más alto en «Noticias y medios de comunicación» y en «Streaming y descarga de videos»; África tuvo el porcentaje más alto en «Motores de búsqueda»; y Asia tuvo el porcentaje más alto en «Shareware/Freeware». Estas diferencias regionales reflejan las técnicas de ingeniería social de los ciberdelincuentes y de la conducta del usuario.

Principales categorías de origen de referencia de descargas de malware en los últimos 12 meses



Principales categorías de origen de referencia de descargas de malware por región



RECOMENDACIONES

El panorama actual de malware está dominado por los troyanos, que se distribuyen a través de categorías de sitios web y aplicaciones en la nube populares, y por lo general desde la misma zona geográfica de la víctima. Para mitigar el riesgo que supone el malware distribuido a través de la nube y la web, Netskope le recomienda aplicar los siguientes controles en su empresa:

1. Analice todo, incluido el tráfico de usuarios en la web, SaaS gestionado y no gestionado, shadow IT, IaaS e instancias corporativas y personales. No eluda paquetes de aplicaciones con almacenamiento en la nube donde las descargas de malware son más habituales. Evite la omisión o el bloqueo por categorías y adopte una estrategia más minuciosa.

2. Implemente protección frente a amenazas inline en diferentes niveles para todo el tráfico en la nube y web, como análisis de aprendizaje automático inline de archivos PE (en lugar de sandboxing en segundo plano) para detectar y evitar que el malware llegue a los endpoints, además de bloquear las comunicaciones salientes de malware.

3. Realice detección de malware en segundo plano usando análisis previos a la ejecución, sandboxing, análisis de aprendizaje automático, alertas de paciente cero en nuevas amenazas, análisis retrospectivos usando indicadores de riesgo (IOC) y análisis MITRE ATT&CK para mejorar la mitigación de respuesta.

4. Aproveche Netskope Cloud Threat Exchange (CTE) para automatizar las actualizaciones de indicadores de riesgo (IOC) de inteligencia de amenazas bidireccional entre defensas, gestione indicadores de riesgo obsoletos e integre su estrategia de seguridad para SSE, endpoints, seguridad de correo electrónico, SIEM, XDR y SOAR.

5. Detecte y desestabilice amenazas bloqueando sitios web peligrosos, y use aislamiento de navegador remoto (RBI) para sitios no categorizados, dominios recién registrados y alias de dominios. Use firewalls en la nube (FWaaS) para filtrar tráfico de salida en todos los puertos y protocolos.

6. Reduzca el riesgo en sus aplicaciones recomendando alternativas más seguras y supervise y enseñe a los usuarios a evitar aplicaciones deficientes y mal valoradas.

7. Unifique el inicio de sesión único (SSO) y la autenticación multifactor (MFA) en sus aplicaciones y servicios en la nube. Además, aproveche el acceso a red Zero Trust (ZTNA) en aplicaciones y recursos privados. Use la autenticación por pasos en políticas adaptativas en función del riesgo de la aplicación, del usuario, del dispositivo, y de la confidencialidad de los datos para habilitar principios Zero Trust.

8. Use el análisis del comportamiento para detectar amenazas internas, exfiltración de datos, dispositivos afectados y credenciales afectadas en todos los carriles del tráfico de usuario hacia aplicaciones privadas y aplicaciones gestionadas mediante introspección de API.

9. Automatice procesos de respuestas en alertas seleccionadas usando Netskope Cloud Ticket Orchestrator para investigaciones y respuesta. Además, aproveche Netskope Cloud Log Shipper para enviar registros de la web, la nube y del firewall a plataformas XDR o SIEM y a data lakes.

10. Utilice análisis para supervisar continuamente movimientos de datos desconocidos, conductas irregulares, riesgos en aplicaciones, duplicación de aplicaciones, perfiles internos y usuarios de riesgo, y aproveche paneles comunes, incluida la evaluación de riesgos de la nube.

MÁS INFORMACIÓN

Para obtener más información acerca de las amenazas en la nube y los estudios realizados en los Netskope Threat Labs, visite **NETSKOPE.COM/ES/NETSKOPE-THREAT-LABS**

Para obtener más información sobre cómo mitigar el riesgo, contáctenos hoy mismo: **WWW.NETSKOPE.COM/ES/REQUEST-DEMO**

EN COLABORACIÓN CON

netskope
THREAT LABS