SECURITY LIFECYCLE REVIEW

Acme

PREPARED BY
Palo Alto Networks
Acme
www.paloaltonetworks.com

Report Period: 8 Days
Tue, Jun 20, 2017 - Tue, Jun 27, 2017

Grupo Smartekh

CPSP

TABLE OF CONTENTS

Grupo Smartekh

paloalto NETWORKS CPSP

Resumen Ejecutivo

Conclusiones principales:

- Se utilizan **204** aplicaciones en total, lo que supone posibles retos para el negocio y la seguridad. Si las funciones más importantes quedan fuera del control de una organización, los empleados utilizan aplicaciones no relacionadas con el trabajo o los ciberatacantes las utilizan para enviar amenazas y robar datos.
- Se observaron **46** aplicaciones de alto riesgo, incluidas aquellas que pueden ocultar o introducir actividad maliciosa, transferir archivos fuera de la red o establecer comunicación no autorizada.
- Se detectaron **376,425** amenazas en total en su red, entre las que se incluyen exploits de vulnerabilidades, malware conocido y desconocido y actividad de mando y control saliente.

En la Revisión del ciclo de vida de la seguridad se resumen los riesgos para el negocio y la seguridad que enfrenta . La información que se utilizó para este análisis fue recopilada por Palo Alto Networks durante el período del informe. El informe proporciona inteligencia práctica respecto de las aplicaciones, el tráfico URL, los tipos de contenido y las amenazas que atraviesan la red e incluye recomendaciones que se pueden aplicar para reducir la exposición general a los riesgos de la organización.

204
APPLICATIONS IN USE

46
HIGH RISK APPLICATIONS

376,425
TOTAL THREATS

366,478
VULNERABILITY EXPLOITS

0
KNOWN MALWARE

Report Period: 8 Days
Start: Thu, Dec 14, 2017
End: Thu, Dec 21, 2017

Información general sobre aplicaciones

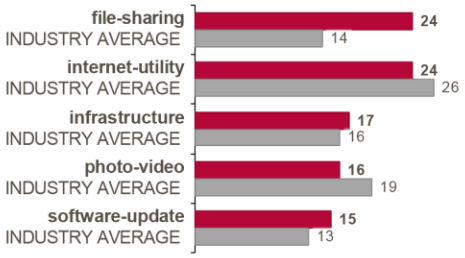
Las aplicaciones pueden introducir riesgos, como enviar amenazas, potencialmente permitir que los datos salgan de la red, permitir acceso no autorizado, reducir la productividad o consumir ancho de banda de la empresa. Esta sección proporciona visibilidad de las aplicaciones en uso, lo que le permite tomar una decisión informada sobre los posibles riesgos frente a las ventajas para el negocio.

Conclusiones principales:

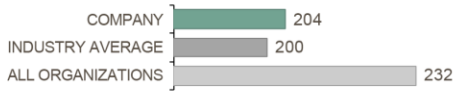
- Se observaron aplicaciones de alto riesgo como **file-sharing, internet-utility y infrastructure** en la red, las cuales deben ser investigadas debido a la posibilidad de abuso.
- Se observaron **204** aplicaciones en total en la red en**27** subcategorías, a diferencia del promedio de **200** aplicaciones en total para el sector que se observaron en otras organizaciones de **Other**.
- Todas las aplicaciones usaron un **244.75GB**, incluido **business-systems** con **104.38GB**, a diferencia del promedio del sector de **320.86GB** en organizaciones similares.

Aplicaciones de alto riesgo

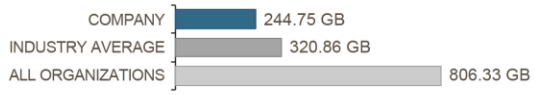
El primer paso para gestionar el nivel de riesgo para el negocio y la seguridad consiste en identificar qué aplicaciones pueden ser usadas para causar el mayor nivel de daño. Recomendamos evaluar detenidamente las aplicaciones que pertenecen a estas categorías para asegurarse de que no estén introduciendo riesgos innecesarios para las operaciones, el cumplimiento de normas o la ciberseguridad



Number of Applications on Network

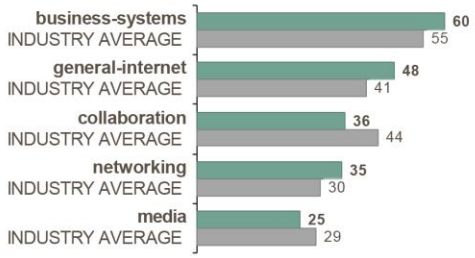


Bandwidth Consumed by Applications



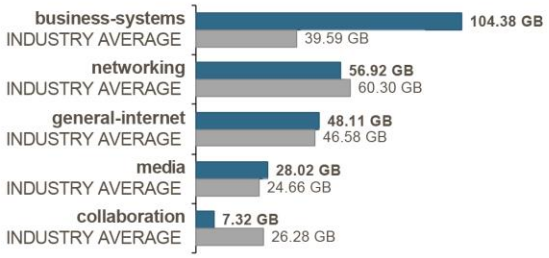
Categorías que incluyen la mayor cantidad de aplicaciones

Las siguientes categorías poseen la mayor cantidad de variantes de aplicaciones y deben ser revisadas para determinar si son relevantes para el negocio.



Categorías que consumen la mayor cantidad de ancho de banda

El ancho de banda consumido por la categoría de aplicaciones demuestra las áreas en las cuales el uso es mayor y aquellas en las que podría reducir los recursos operativos.



Aplicaciones que introducen riesgos

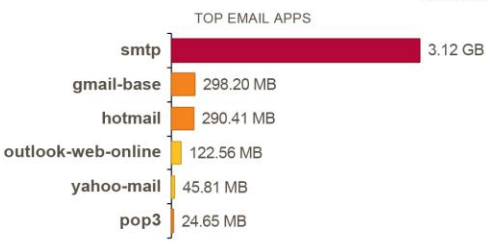
A continuación se muestran las aplicaciones más importantes (ordenadas por el ancho de banda consumido) para las subcategorías de aplicaciones que introducen riesgos, incluidos los puntos de referencia del sector para la cantidad de variantes que existen en otras organizaciones de **Other**. Estos datos se pueden usar para priorizar con mayor eficacia sus esfuerzos para habilitar aplicaciones.

RISK LEVEL

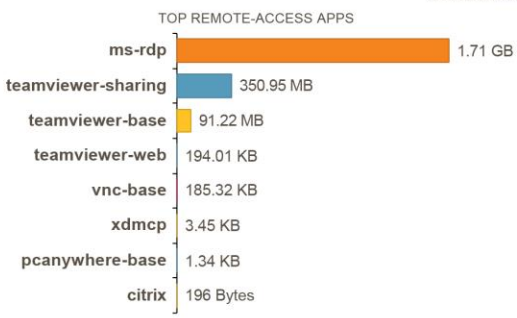
Conclusiones principales:

- En su organización se observaron **204** aplicaciones en total, a diferencia del promedio del sector de **200**en otras organizaciones de **Other**.
- Los tipos de subcategorías de aplicaciones más comunes son: **file-sharing, internet-utility y infrastructure**.
- Las subcategorías de aplicaciones que consumen la mayor cantidad de ancho de banda son: **management, internet-utility y infrastructure**.

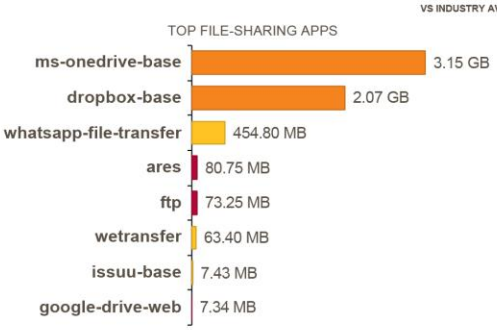
Email - 3.89GB



Remote-Access - 2.14GB



File-Sharing - 5.9GB

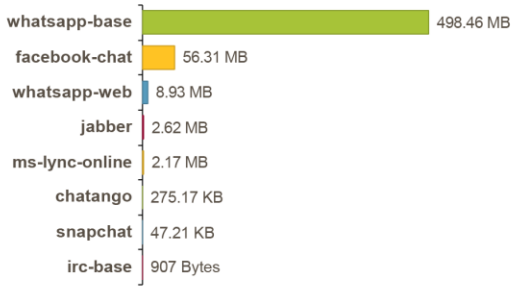


Encrypted-Tunnel - 23.97GB

Instant-Messaging - 568.8MB

8 9
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP INSTANT-MESSAGING APPS



Social-Networking - 2.77GB

12 15
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP SOCIAL-NETWORKING APPS

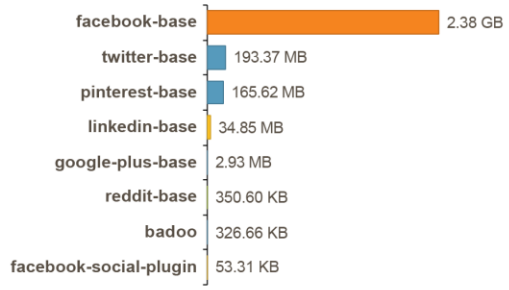
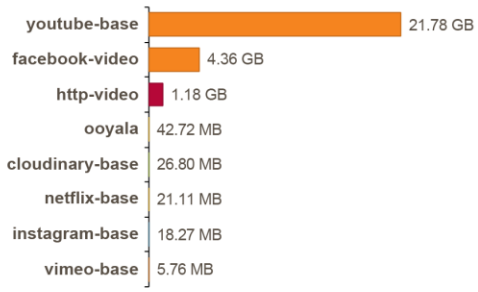


Photo-Video - 27.44GB

16 19
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP PHOTO-VIDEO APPS



Proxy - 313.81KB

1 1
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP PROXY APPS

Aplicaciones que introducen riesgos: detalle

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	3.12GB	14676
4	gmail-base	collaboration	email	browser-based	298.2MB	1684
4	hotmail	collaboration	email	browser-based	290.41MB	1101
3	outlook-web-online	collaboration	email	browser-based	122.56MB	1183
3	yahoo-mail	collaboration	email	browser-based	45.81MB	2558
4	pop3	collaboration	email	client-server	24.65MB	17
4	ssl	networking	encrypted-tunnel	browser-based	23.56GB	1053692
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	262.87MB	15
4	ssh	networking	encrypted-tunnel	client-server	153.16MB	77
2	ike	networking	encrypted-tunnel	client-server	72.71KB	51
2	mobility-xe	networking	encrypted-tunnel	client-server	826Bytes	4
4	ms-onedrive-base	general-internet	file-sharing	client-server	3.15GB	311
4	dropbox-base	general-internet	file-sharing	client-server	2.07GB	5934
3	whatsapp-file-transfer	general-internet	file-sharing	client-server	454.8MB	55
5	ares	general-internet	file-sharing	peer-to-peer	80.75MB	167528
5	ftp	general-internet	file-sharing	client-server	73.25MB	146
3	wetransfer	general-internet	file-sharing	browser-based	63.4MB	142
3	issuu-base	general-internet	file-sharing	browser-based	7.43MB	329
5	google-drive-web	general-internet	file-sharing	browser-based	7.34MB	147
1	whatsapp-base	collaboration	instant-messaging	client-server	498.46MB	387
3	facebook-chat	collaboration	instant-messaging	browser-based	56.31MB	389
2	whatsapp-web	collaboration	instant-messaging	browser-based	8.93MB	172
5	jabber	collaboration	instant-messaging	client-server	2.62MB	35
3	ms-lync-online	collaboration	instant-messaging	client-server	2.17MB	122
1	chatango	collaboration	instant-messaging	client-server	275.17KB	4

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	snapchat	collaboration	instant-messaging	client-server	47.21KB	6
5	irc-base	collaboration	instant-messaging	client-server	907Bytes	1
4	youtube-base	media	photo-video	browser-based	21.78GB	7716
4	facebook-video	media	photo-video	browser-based	4.36GB	2737
5	http-video	media	photo-video	browser-based	1.18GB	423
3	ooyala	media	photo-video	browser-based	42.72MB	90
1	cloudinary-base	media	photo-video	client-server	26.8MB	50
3	netflix-base	media	photo-video	browser-based	21.11MB	1829
2	instagram-base	media	photo-video	client-server	18.27MB	368
4	vimeo-base	media	photo-video	browser-based	5.76MB	164
5	http-proxy	networking	proxy	browser-based	313.81KB	195
4	ms-rdp	networking	remote-access	client-server	1.71GB	464621
2	teamviewer-sharing	networking	remote-access	client-server	350.95MB	14
3	teamviewer-base	networking	remote-access	client-server	91.22MB	2245
2	teamviewer-web	networking	remote-access	browser-based	194.01KB	27
5	vnc-base	networking	remote-access	client-server	185.32KB	271
3	xdmcp	networking	remote-access	client-server	3.45KB	28
2	pcanywhere-base	networking	remote-access	client-server	1.34KB	12
3	citrix	networking	remote-access	client-server	196Bytes	1
4	facebook-base	collaboration	social-networking	browser-based	2.38GB	25064
2	twitter-base	collaboration	social-networking	browser-based	193.37MB	3977
2	pinterest-base	collaboration	social-networking	browser-based	165.62MB	4021
3	linkedin-base	collaboration	social-networking	browser-based	34.85MB	1753
2	google-plus-base	collaboration	social-networking	browser-based	2.93MB	59
1	reddit-base	collaboration	social-networking	browser-based	350.6KB	8

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	badoo	collaboration	social-networking	browser-based	326.66KB	15
3	facebook-social-plugin	collaboration	social-networking	browser-based	53.31KB	20

Notes:

Aplicaciones SaaS

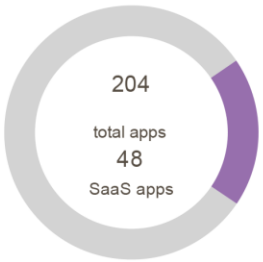
Los servicios de aplicaciones basadas en SaaS continúan redefiniendo el perímetro de la red. Normalmente denominados “shadow IT”, la mayoría de estos servicios son adoptados directamente por usuarios particulares, equipos de negocios o incluso departamentos enteros. Con el objetivo de minimizar los riesgos de seguridad de datos, se debe tener control sobre las aplicaciones SaaS que se usan en la red.

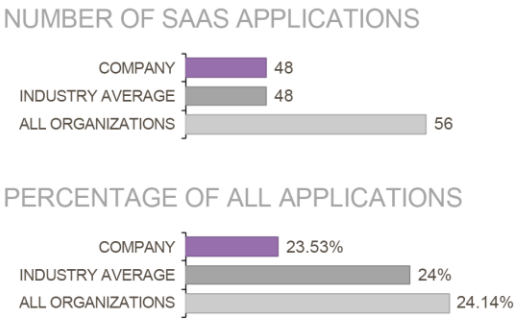
Descubrimientos clave

- **File-Sharing** tiene la mayor cantidad de aplicaciones SaaS exclusivas.
- En términos de movimiento de datos, **ms-onedrive-base** es la aplicación SaaS más usada en su organización.

Aplicaciones SaaS en números

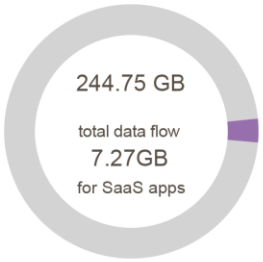
Revise las aplicaciones que se están usando en su organización. Para garantizar el control administrativo, adopte las aplicaciones SaaS que serán gestionadas por su equipo de TI.

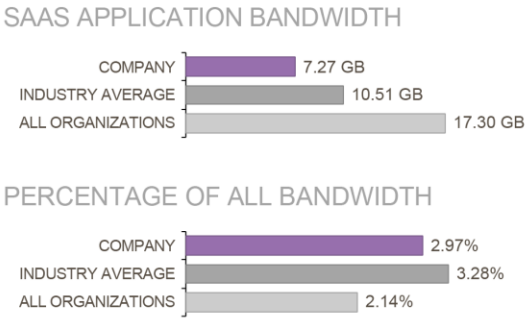




Ancho de banda de las aplicaciones SaaS

Controle el volumen de movimiento de datos hacia y desde las aplicaciones SaaS. Entienda la naturaleza de las aplicaciones y cómo se están usando.

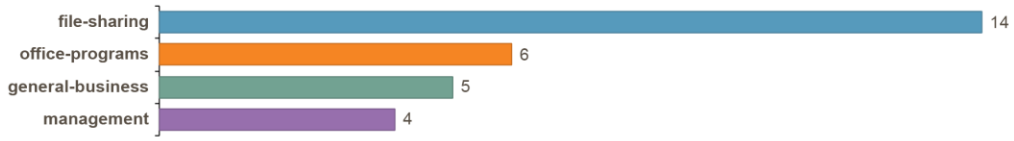




PRINCIPALES SUBCATEGORÍAS DE APLICACIONES SAAS

A continuación se muestra la cantidad de aplicaciones en cada subcategoría de aplicaciones. Esto le permite evaluar las aplicaciones más usadas en la organización. Principales subcategorías de aplicaciones SaaS por cantidad total de aplicaciones. A continuación encontrará las principales aplicaciones usadas para el movimiento de datos en las subcategorías identificadas precedentemente.

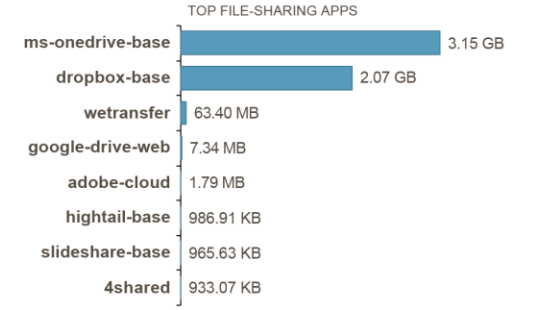
Top SaaS application subcategories by total number of applications



The following shows the top used applications by data movement within the subcategories identified above.

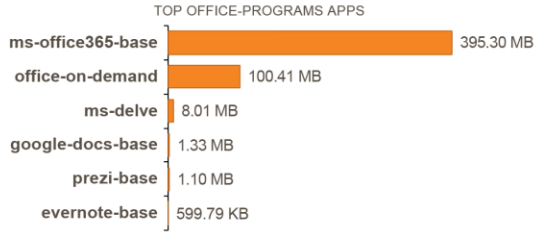
File-Sharing - 5.29GB

14 14
APPLICATION VARIANTS VS INDUSTRY AVERAGE



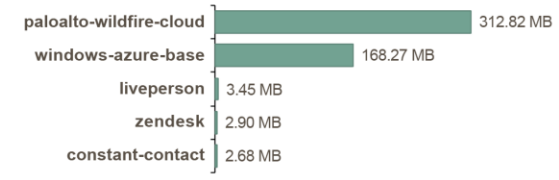
Office-Programs - 506.73MB

6 7
APPLICATION VARIANTS VS INDUSTRY AVERAGE



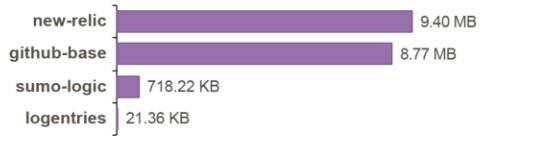
General-Business - 490.12MB

5 9
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Management - 18.89MB

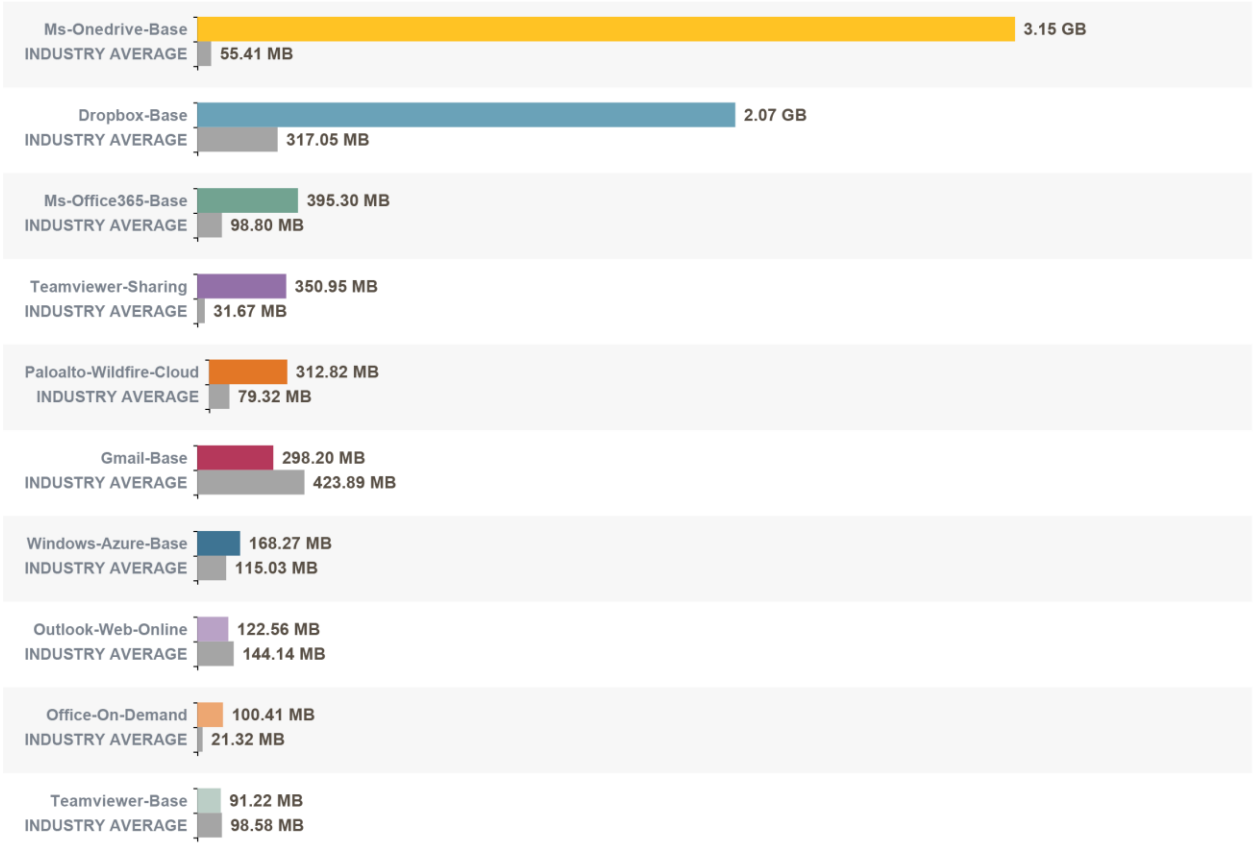
4 11
APPLICATION VARIANTS VS INDUSTRY AVERAGE



PRINCIPALES APLICACIONES SAAS

A continuación se muestran las principales 10 aplicaciones SaaS usadas en su organización y una comparación del uso de aplicaciones con otras empresas del sector y todos los demás clientes de Palo Alto Networks.

Top SaaS Applications by Data Movement

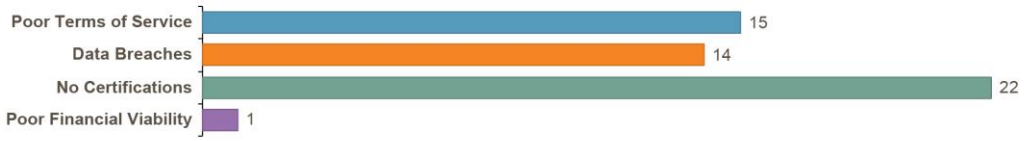


Grupo Smartekh

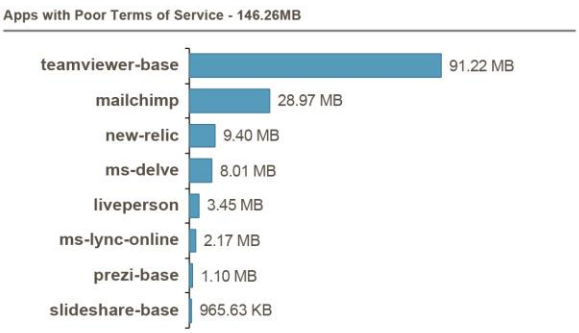
paloalto NETWORKS CPSP

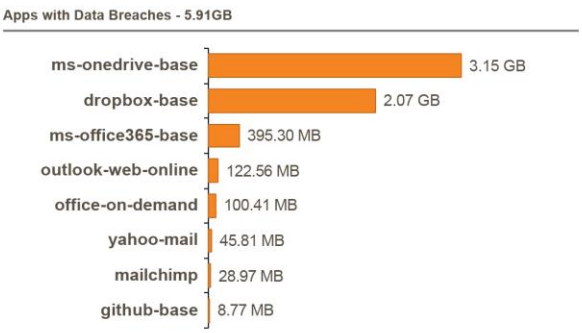
SaaS Applications by Hosting Risk

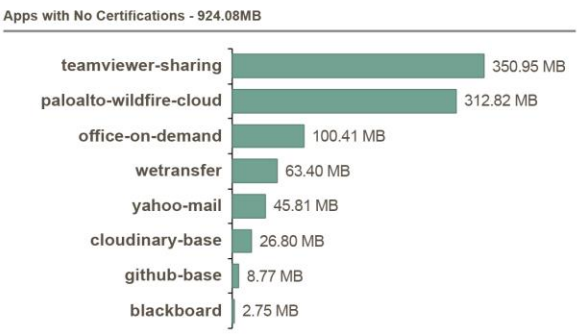
Based on your SaaS usage, it is imperative to regularly review SaaS applications being accessed, who is accessing them, and how they are being used.
The following chart displays the number of applications by each hosting risk characteristic.

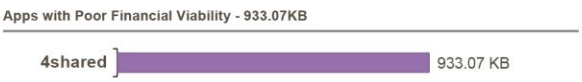


The following charts display the top applications by bandwidth for each hosting risk characteristic.









Actividad de URL

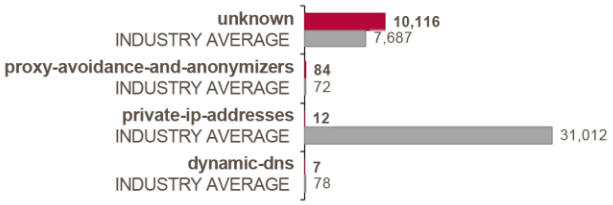
La navegación web sin control expone a las organizaciones a riesgos para la seguridad y el negocio, entre los que se incluyen exposición a la posible propagación de amenazas, pérdida de datos o incumplimiento de la normativa. A continuación se muestran las categorías de URL que los usuarios visitan con mayor frecuencia en la red.

Conclusiones principales

- En la red se observaron categorías de URL de alto riesgo, como **computer-and-internet-info, web-advertisements y business-and-economy**.
- Los usuarios visitaron un total de **1,495,578** URL durante el período del informe, en **55** categorías.
- Se realizaron diferentes actividades web de índole personal y relacionadas con el trabajo, entre las que se incluyen visitas a sitios web potencialmente peligrosos.

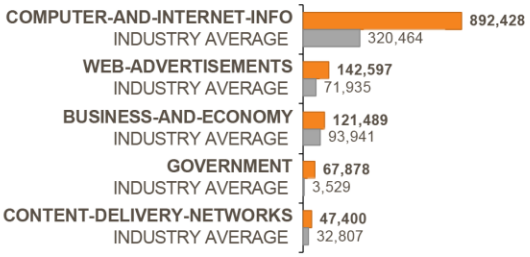
Categorías de URL de alto riesgo

Internet es un vector de infección muy importante para los atacantes, ya que las categorías de URL de alto riesgo representan un riesgo enorme para la organización. Las soluciones deberían permitir bloquear rápidamente los sitios no deseados o maliciosos y realizar una rápida categorización e investigación de sitios desconocidos.



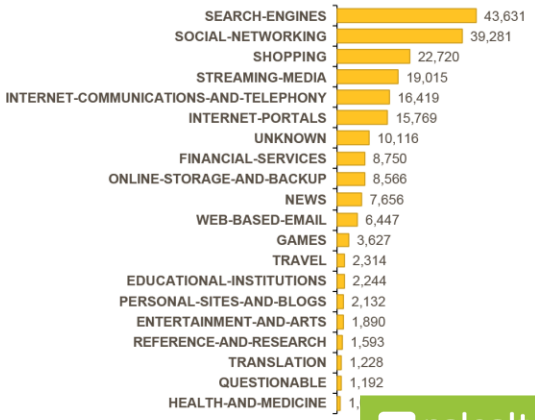
Categorías de URL de alto tráfico

A continuación se muestran las 5 categorías de URL más importantes visitadas con frecuencia, junto con los puntos de referencia del sector para



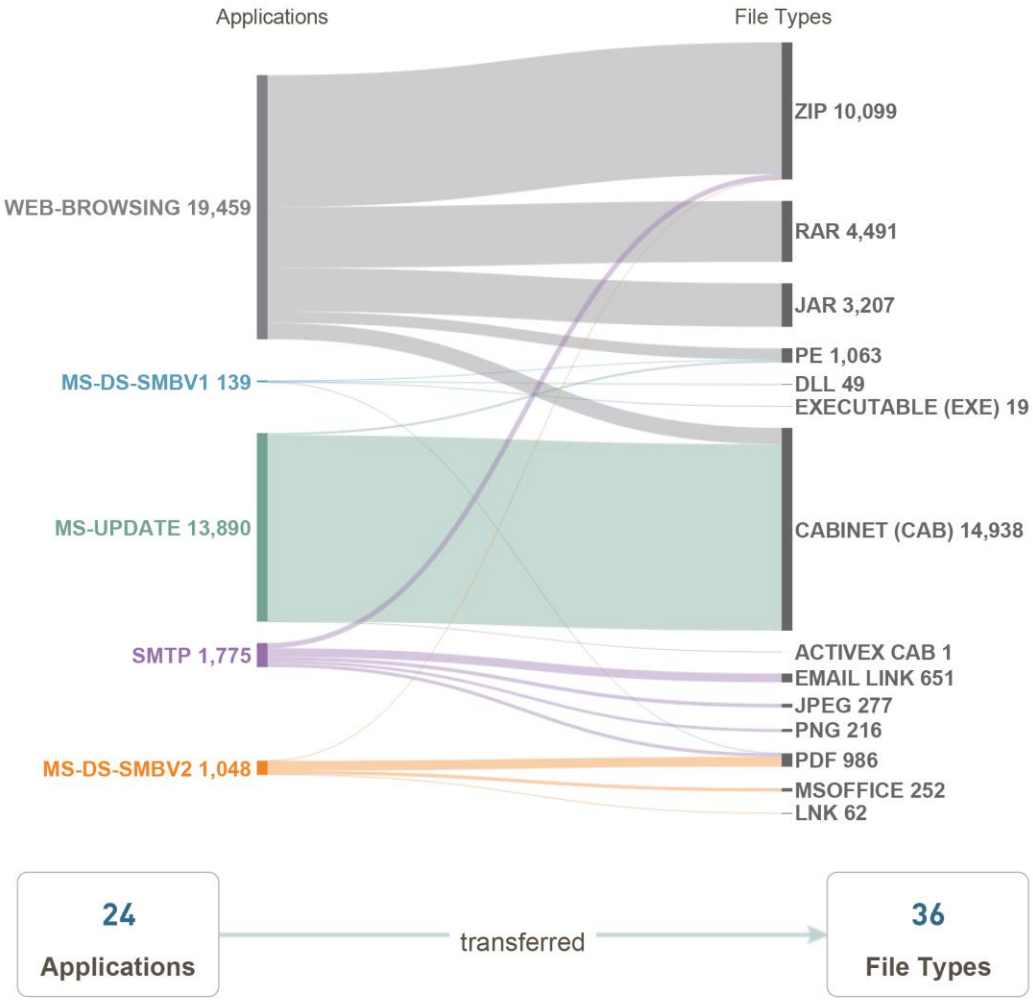
Categorías de URL usadas con frecuencia

A continuación se muestran las 20 categorías de URL más importantes visitadas con mayor frecuencia



Análisis de la transferencia de archivos

Las aplicaciones que pueden transferir archivos desempeñan una función importante para el negocio, pero también pueden permitir que los datos confidenciales salgan de la red o que se envíen ciberamenazas. Dentro de su organización, se observaron **16,391** archivos en total entre **36** tipos de archivos diferentes, que se enviaron a través de un total de **24** aplicaciones en total. En la imagen siguiente se establece una correlación entre las aplicaciones que se utilizan con mayor frecuencia para transferir archivos y los tipos de archivos y contenido que se observaron con mayor frecuencia.

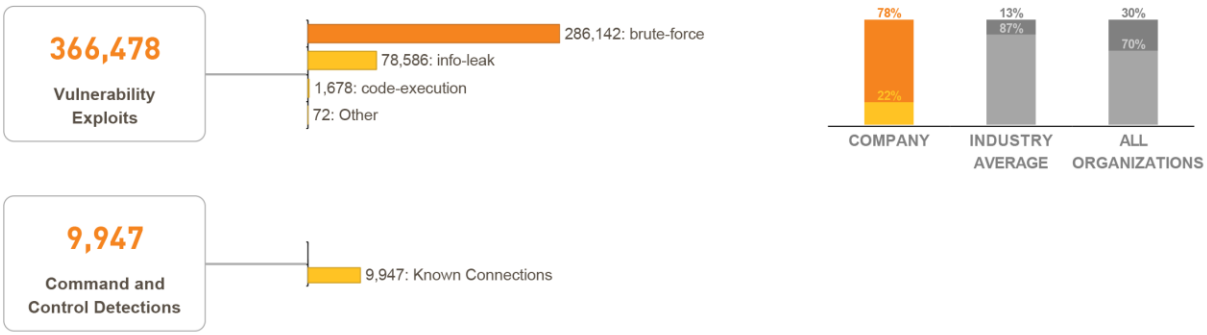


Información general sobre amenazas

Para comprender su exposición a los riesgo y cómo adaptar sus medidas de seguridad para prevenir ataques, debe conocer el tipo y el volumen de amenazas que se utilizan contra su organización. En esta sección se detallan las vulnerabilidades de las aplicaciones, el malware conocido y desconocido y la actividad de mando y control que se observaron en su red.

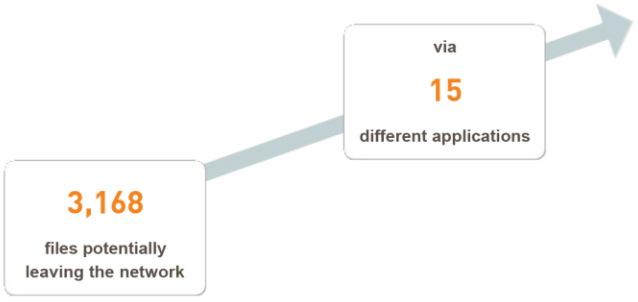
Conclusiones principales:

- En su organización se observaron **366,478** exploits de vulnerabilidades en total, entre los que se incluyen las categorías de vulnerabilidades **brute-force, info-leak y code-execution**.
- Se observaron **0** eventos de malware, frente a un promedio del sector de **278** para su grupo del peer.
- Se identificaron **9,947** solicitudes de mando y control salientes en total, lo que indica que el malware intentó comunicarse con atacantes externos para descargar malware adicional, recibir instrucciones o exfiltrar datos.



Archivos que podrían salir de la red

La transferencia de archivos es una parte necesaria y habitual de las actividades empresariales, pero para poder limitar la exposición de su organización a la pérdida de datos se debe mantener la visibilidad del contenido que sale de la red y de las aplicaciones mediante las cuales lo hace.



Análisis de tipos de archivos de alto riesgo y maliciosos

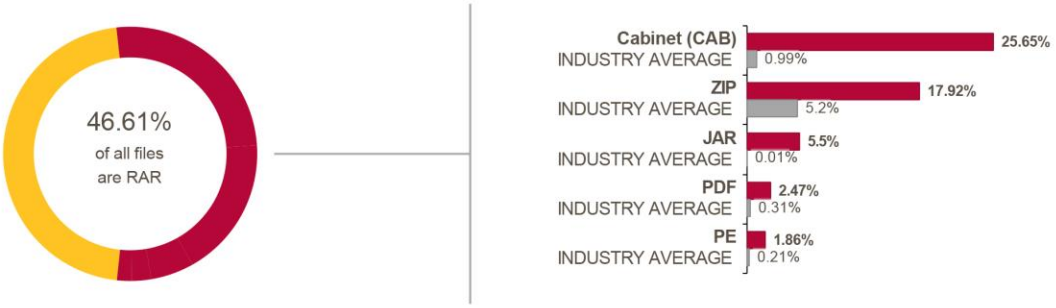
Los ciberatacantes de hoy en día utilizan diversos tipos de archivos para enviar malware y exploits y suelen concentrarse en el contenido de aplicaciones habituales del negocio que se encuentran en la mayoría de las redes empresariales. La mayoría de las amenazas de productos se envía mediante archivos ejecutables y los ataques más específicos y avanzados suelen usar otros contenidos para afectar las redes.

Conclusiones principales:

- Se utilizaron diversos tipos de archivos para enviar amenazas y las estrategias de prevención deberían cubrir todos los tipos de contenido más importantes.
- Para reducir la superficie de ataque, puede bloquear de forma proactiva los tipos de archivos de alto riesgo; por ejemplo, puede bloquear los archivos ejecutables descargados de Internet o no permitir los archivos RTF o LNK que no son necesarios para las operaciones diarias.

Tipos de archivos de alto riesgo

Los tipos de archivos que se muestran representan un mayor riesgo para la organización debido al descubrimiento de una combinación de vulnerabilidades nuevas, a fallos existentes y sin parches y a la frecuencia con la que se usan en ataques.

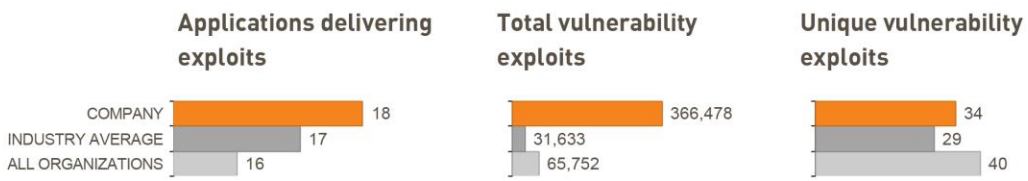


Vulnerabilidades de aplicaciones

Las vulnerabilidades de las aplicaciones permiten que los atacantes aprovechen las aplicaciones vulnerables que suelen no tener parches para infectar los sistemas, lo que generalmente representa uno de los primeros pasos en una infracción. En esta página se detallan las cinco vulnerabilidades de aplicaciones más importantes que los atacantes intentaron aprovechar en su organización, para que pueda determinar cuáles son las aplicaciones que representan la superficie de ataque más importante

Conclusiones principales:

- Se observaron **18** aplicaciones en total que envían exploits a su entorno.
- Se observaron **366,478** exploits de vulnerabilidades en total y las tres categorías más importantes son **mssql-db, eset-update y eset-update**.
- Del total de vulnerabilidades descubiertas, se detectaron **34** vulnerabilidades únicas, lo que significa que los atacantes usaron los mismos exploits de vulnerabilidades una y otra vez.



Vulnerability Exploits per Application (top 5 applications with most detections)

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
130,160	**mssql-db**			
130,160	Microsoft SQL Server User Authentication Brute Force Attempt	High	brute-force	
83,308	**eset-update**			
41,654	HTTP WWW-Authentication Failed	Info	brute-force	
41,654	HTTP Unauthorized Error	Info	brute-force	
64,032	**ssl**			
63,994	POODLE Bites Vulnerability	Info	info-leak	CVE-2014-8730
24	Use of insecure SSLv3.0 Found in Server Response	Info	info-leak	CVE-2014-3566
14	Export RSA cipher suite detected	Info	info-leak	CVE-2015-0204; CVE-2015-1637; CVE-2015-1067; CVE-2015-0138
40,772	**eset-remote-admin**			
20,386	HTTP WWW-Authentication Failed	Info	brute-force	
20,386	HTTP Unauthorized Error	Info	brute-force	
33,204	**web-browsing**			
72	Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	Critical	code-execution	CVE-2017-5638
4	Microsoft Windows HTTP.sys Remote Code Execution Vulnerability	Critical	code-execution	CVE-2015-1635

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
2	Bash Remote Code Execution Vulnerability	Critical	code-execution	CVE-2014-6271; CVE-2014-7169; CVE-2014-6277; CVE-2014-6278
40	Generic HTTP Cross Site Scripting Attempt	High	code-execution	CVE-2017-0068
8	HTTP Unauthorized Brute Force Attack	High	brute-force	
468	ZmEu Scanner Detection	Low	info-leak	
40	HTTP Cross Site Scripting Attempt	Low	code-execution	
30	JavaScript Obfuscation Detected	Low	code-execution	
4	Suspicious Abnormal HTTP Response Found	Low	protocol-anomaly	
15,650	HTTP Unauthorized Error	Info	brute-force	

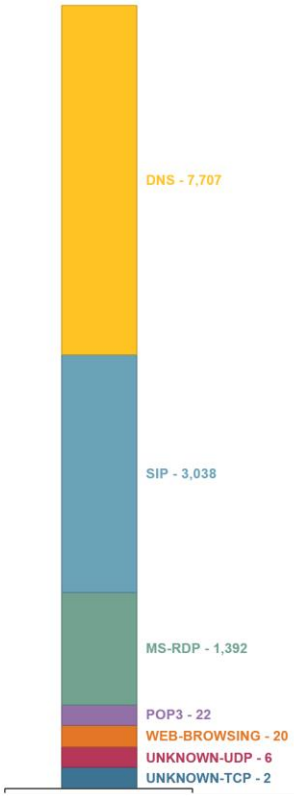
Análisis de mando y control

La actividad de mando y control indica que un host de la red está infectado con malware y está intentando conectarse fuera de la red con actores maliciosos. Es sumamente importante comprender y prevenir esta actividad, ya que los atacantes utilizan la actividad de mando y control para enviar malware adicional, dar instrucciones o exfiltrar datos.

Conclusiones principales:

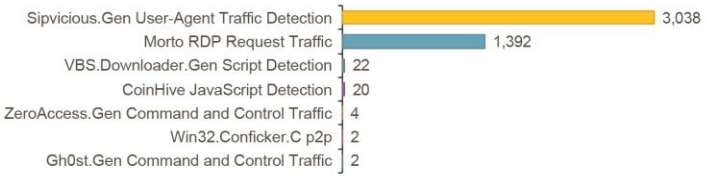
- Se usaron **7** aplicaciones en total para la comunicación de mando y control.
- Se observaron **9,947** solicitudes de mando y control en total que se originan en su red.
- Se observaron **7,707** consultas de DNS sospechosas en total.

COMMAND AND CONTROL ACTIVITY BY APPLICATION



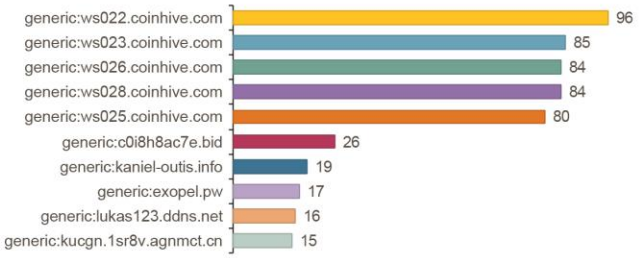
Llamada a casa de spyware 2,240

La imagen a continuación representa los hosts afectados que intentan conectarse con servidores de mando y control maliciosos externos



Consultas de DNS sospechosas 7,707

Si bien DNS es una aplicación frecuente y necesaria, también suele usarse para ocultar comunicación saliente de mando y control, como se muestra en el siguiente gráfico.



Resumen:

El análisis determinó que su red presenta una amplia variedad de aplicaciones y ciberataques. Esta actividad representa posibles riesgos para el negocio y la seguridad de pero también es una oportunidad ideal para implementar políticas de habilitación segura de aplicaciones que no solo le permitan al negocio seguir creciendo, sino que también reduzcan la exposición general a los riesgos de la organización.

204
APPLICATIONS IN USE

46
HIGH RISK APPLICATIONS

376,425
TOTAL THREATS

366,478
VULNERABILITY EXPLOITS

0
KNOWN MALWARE

Aspectos destacados:

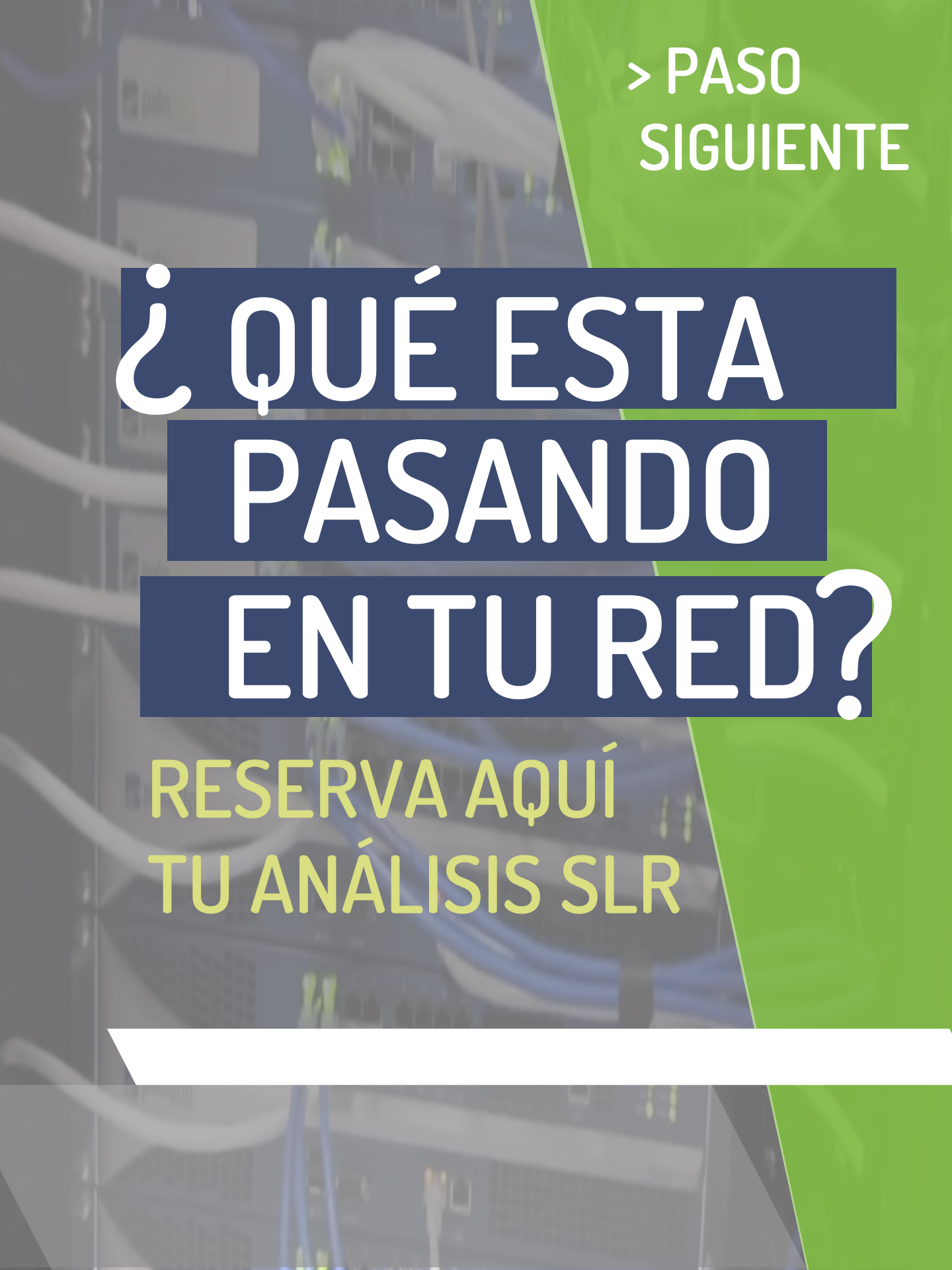
- Se observaron aplicaciones de alto riesgo como **file-sharing, internet-utility y infrastructure** en la red, las cuales deben ser investigadas debido a la posibilidad de abuso.
- Se observaron **204** aplicaciones en total en la red en **27**, a diferencia del promedio de **200** aplicaciones en total para el sector que se observó en otras organizaciones de **Other**.
- Se observaron **366,478** vulnerabilidades en total y las tres categorías más importantes son **mssql-db, eset-update y eset-update**.
- Se observaron **0** eventos de malware, frente a un promedio del sector de **278** para su grupo del peer.
- Se usaron **7** aplicaciones en total para la comunicación de mando y control.

Recomendaciones:

- Implementar políticas de habilitación segura de aplicaciones, permitiendo únicamente las aplicaciones necesarias para el negocio y aplicando un control detallado de todas las demás.
- Abordar las aplicaciones de alto riesgo que presentan posibilidad de abuso, como el acceso remoto, el intercambio de archivos o los túneles cifrados.
- Implementar una solución de seguridad que permita detectar y prevenir amenazas, tanto conocidas como desconocidas, para mitigar el riesgo de los atacantes.
- Usar una solución que pueda reprogramarse automáticamente, que permita crear nuevas protecciones para las amenazas de aparición reciente y que se origine a partir de una comunidad global de otros usuarios empresariales.

Grupo Smartekh

paloalto NETWORKS CPSP



> PASO SIGUIENTE

¿ QUÉ ESTA PASANDO EN TU RED?

RESERVA AQUÍ TU ANÁLISIS SLR

>Conoce más

smartekh.com

Insurgentes Sur 826 P10 Col.Del Valle C.P. 03100 Ciudad de México.

Grupo Smartekh

paloalto NETWORKS®

CPSP