

SUBDIRECCIÓN ADMINISTRATIVA
 Adquisición De Bienes y Servicios

INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

27/12/2024 11:13 a. m. CROSERO

CAJA DE RETIRO DE LAS FF.MM

ASUNTO: REP SUPERV PAGO MC 037-2024
 DESTINATARIO: SANDRA MILENA CHIQUILLO
 DEPENDENCIA: SUBDIRECCION FINANCIERA
 No. COMUNICACIÓN: 019240
 CONSECUTIVO: 2024-19240

I2024019244

[Interno]

Se sugiere la aplicación de este modelo para todas aquellas contrataciones que deben gestionarse y ejecutarse bajo las normas de derecho público (Ley 80 de 1993, Ley 1150/2007 y Decreto 1082 de 2015 y sus normas reglamentarias), así como para contratos y convenios supervisados por las diferentes dependencias en CREMIL.

INFORME No. 1	Porcentaje de cumplimiento	100%	
FECHA DE ELABORACIÓN	26-12-2024		
PERIODO DEL INFORME	Diciembre 2024		

CONTRATO/CONVENIO	MC-037-2024	
VALOR DEL CONTRATO	\$ 113.700.000	
TIPO DE CONTRATACIÓN	Mínima Cuantía	
FECHA DE SUSCRIPCIÓN	05-12-2024	
CONTRATISTA	UT CREMIL 2023	
NIT	9017836132	
REPRESENTANTE LEGAL DEL CONTRATISTA	ANDREA PALACIOS VILLAMIZAR	
CÉDULA	1.018.408.058	
CONTACTO DEL CONTRATISTA	Daniel Hernandez Jiménez daniel.hernandez@datamotion.online	
RÉGIMEN TRIBUTARIO	Responsable IVA <u>X</u>	Régimen Simple _____

SUBDIRECCIÓN ADMINISTRATIVA
 Adquisición De Bienes y Servicios

INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

	No Responsables de IVA —	
SUPERVISOR	Coronel (R) VICTOR AUGUSTO PATIÑO PEÑUELA Coordinador Grupo de TI	
DATOS DEL CONTACTO CREMIL	crosero@cremil.gov.co 6477777 Grupo de TI – Subdirección Administrativa	
OBJETO DEL CONTRATO/CONVENIO:		
CONTRATAR LOS SERVICIOS DE RENOVACIÓN DE LAS LICENCIAS, SOPORTE DE FÁBRICA DE LOS FIREWALL EN ALTA DISPONIBILIDAD Y EL SERVICIO PARA CUMPLIR CON LOS CRITERIOS DE ADMINISTRACIÓN, GESTIÓN, MANTENIMIENTO Y SOPORTE TÉCNICO DE CANAL LOS CUALES HACEN PARTE DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL DE LA CAJA DE RETIRO DE LAS FF.MM.		

FECHA DE INICIACIÓN		06-12-2024			
FECHA DE TERMINACIÓN		26-12-2024			
FECHA DE APROBACIÓN DE LA PÓLIZA		31-12-2024			
COMPañía DE SEGUROS	PÓLIZA No.	AMPARO	VIGENCIA DESDE	VIGENCIA HASTA	VALOR ASEGURADO
SEGUROS DEL ESTADO SA	42-46-1010320215	Cumplimiento del contrato	04-12-2024	04-07-2025	\$11.370.000
		Calidad del servicio	04-12-2024	04-07-2024	\$11.370.000

OTROSÍ, PRÓRROGA, ADICIÓN U OTRAS MODIFICACIONES		
No.	FECHA	DESCRIPCIÓN DE MODIFICACIONES

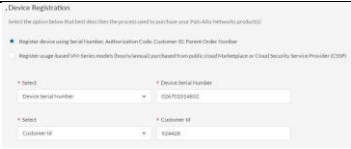
SUBDIRECCIÓN ADMINISTRATIVA
 Adquisición De Bienes y Servicios

INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

DISPONIBILIDAD Y REGISTRO PRESUPUESTAL			
Certificado de disponibilidad presupuestal- CDP y fecha	25024 de 31-10-2024		
Registro presupuestal y fecha	156924 de 06-12-2024		
CUMPLIMIENTO DE LAS OBLIGACIONES DEL CONTRATO/CONVENIO			
OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA	ACTIVIDAD	NOMBRE Y UBICACIÓN DEL (LOS) DOCUMENTO(S) QUE SOPORTA(N) EL CUMPLIMIENTO DE LA OBLIGACIÓN (Ubicación física o digital)	OBSERVACIONES DEL SUPERVISOR
Dar inicio al contrato MC 037-2024	Levantamiento del acta de inicio	Se relaciona evidencia <div></div>	Se firma acta de inicio
Renovación licencia firewall palo alto	Actividad en permanente ejecución según lo establecido contractualmente	Se relaciona evidencia en el informe entregado a la entidad.	100%

SUBDIRECCIÓN ADMINISTRATIVA
 Adquisición De Bienes y Servicios

INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

			
Renovación, del componente de seguridad	Actividad en permanente ejecución según lo establecido contractualmente	Se relaciona evidencia en el informe entregado a la entidad	100%

RELACIÓN DE PAGOS EFECTUADOS

Diligencie el siguiente cuadro cuando se trate de un informe de supervisión final, para su respectivo proceso de liquidación:

FACTURA No.	FECHA	ORDEN DE PAGO N°	FECHA	VALOR
Valor total pagos efectuados				\$ 0
ESTADO FINANCIERO				
DATOS GENERALES		CIFRAS		
Valor inicial del contrato		\$ 113.700.000		
Valor adiciones				
Valor reducciones				
Valor total del contrato		\$ 113.700.000		
Valor total ejecutado		\$ 0		
Saldo por pagar al contratista		\$ 113.700.000		
Saldo por liberar				

CONSTANCIA POR PARTE DEL SUPERVISOR

En el presente informe se deja constancia que el contenido y los documentos anexos a éste, se encuentran debidamente verificados y firmados y como consecuencia se recibe a satisfacción las actividades inherentes a este periodo.

SUBDIRECCIÓN ADMINISTRATIVA
Adquisición De Bienes y Servicios

INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

Se dio inicio al Contrato No. MC 037-2024, mediante acta de inicio firmada el 06 de diciembre de 2024 por el supervisor del contrato y los profesionales de UT CREMIL 2023.

Se aprobó póliza de cumplimiento expedida por Seguros del Estado SA No. 42-46-1010320215 del 04-12-2024.

El plazo de ejecución del contrato es hasta el 31 de diciembre de 2024 y el soporte y mantenimiento local es hasta el 6 de diciembre de 2025.

El valor total del contrato es por **CIENTO TRECE MILLONES SETECIENTOS MIL PESOS M/CTE (\$113.700.000,00) INCLUIDO IVA.**

Se dio cumplimiento a las obligaciones y requerimientos definidos en el contrato MC-037-2024.

Se verificó el valor de la factura No. **FEUT3** por valor de **CIENTO TRECE MILLONES SETECIENTOS MIL PESOS M/CTE (\$113.700.000,00) INCLUIDO IVA.**

Se autoriza el pago de la factura No. **FEUT3** por valor **CIENTO TRECE MILLONES SETECIENTOS MIL PESOS M/CTE (\$113.700.000,00)** incluido IVA, correspondientes al pago total del contrato MC-037-2024. registro presupuestal No. **156924 de 06-12-2024.**

Se adjuntan al presente informe:

- Factura FEUT3
- Certificado para fiscales.pdf
- Planilla SOL.pdf
- Informe.pdf

Nota: Tener en cuenta que la factura física no contiene decimales, al momento de subirla a siifnacion se genera con decimales (,48). Lo anterior para que sea tomada en cuenta y no implique devolución de la misma.

FIRMAS

SUBDIRECCIÓN ADMINISTRATIVA
Adquisición De Bienes y Servicios

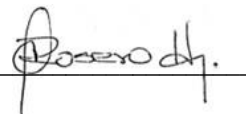
INFORME PERIÓDICO DE SUPERVISIÓN CONTRATOS/CONVENIOS

Supervisor: Coronel (R) Victor Augusto Patiño Peñuela

Cargo/Rol Coordinador Grupo TI

Nombre: CLAUDIA PATRICIA ROSERO HOYOS

Firma:



UT CREMIL 2023
NIT 901783613-2
Calle 31 13 A 51 To 2 Of 1803, Bogotá, D.C., Bogotá D.C.,
Tel: +573184198842
facturacion@datamotion.online ; www.datamotion.online

FACTURA ELECTRÓNICA DE
VENTA
No. FEUT3
Responsable de IVA

SEÑOR(ES) DIRECCIÓN TELÉFONO	CAJA DE RETIRO DE LAS FUERZAS MILITARES		FECHA DEL DOCUMENTO (DD/MM/AA)
	Carrera 13 # 27 - 00 Edificio Bochica Interior 2 Bogotá D.C., Colombia, Bogotá, D.C., Bogotá D.C.		26/12/2024
	601 222 0950	NIT 899999118-1	FECHA DE VENCIMIENTO 25/01/2025

ID	Ítem	Unidad	Precio	Cantidad	Descuento	Total
1	Renovar el licenciamiento y el soporte de fábrica de los componentes de software y hardware de los Firewall Palo Alto PAN-PA-1410	Unidad	\$87.394.958	1		\$87.394.958
2	Servicio de soporte técnico y mantenimiento	Unidad	\$8.151.261	1		\$8.151.261

Ciento trece millones setecientos mil pesos (COP)



Moneda: COP
Generado: 2024-12-26 10:09:24-05:00
Validación DIAN: 2024-12-26 10:10:25-05:00
Tipo de operación: Estándar Forma de pago: Crédito

CUFE: 75dbe86248d517236e22104a3e357926420ee66bbd3884646c1ba4e9f270b23814e238c41b1a471f295a5dc8959bbcf1

Esta factura se asimila en todos sus efectos a una letra de cambio de conformidad con el Art. 774 del código de comercio. Autorizo que en caso de incumplimiento de esta obligación sea reportado a las centrales de riesgo, se cobraran intereses por mora.

Subtotal	\$95.546.218
IVA (19.00%)	\$18.153.782
Total	\$113.700.000

Total de líneas: 2

mfajar

ELABORADO POR

ACEPTADA, FIRMA Y/O SELLO Y FECHA

Autorización de numeración de facturación N°18764064646981 de 2024-01-30 Modalidad Factura Electrónica Desde N° FEUT1 hasta FEUT100 con vigencia hasta 2025-01-30

Representación gráfica de factura de venta electrónica

Proveedor tecnológico: Soluciones Alegria S.A.S - Software: Alegria - NIT 900.559.088-2

**CERTIFICACION DE PAGOS DE APORTES AL SISTEMA DE
SEGURIDAD SOCIAL Y PARAFISCALES.
PERSONA JURIDICA. ARTÍCULO 50 DE LA LEY 789 DE 2002.**

Yo, Andrea Palacios Villamizar identificado con cédula de ciudadanía 1.018.408.058 en mi condición de Representante Legal de UT CREMIL 2023 identificada con Nit. 901.783.613-2, debidamente inscrito en la Cámara de Comercio de Bogotá certifico el pago de los aportes realizados por la compañía durante los últimos meses desde su inicio de operaciones en diciembre de 2023 legalmente exigibles a la fecha de presentación de nuestra propuesta para el presente proceso de selección, por los conceptos de salud, pensiones, riesgos laborales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar(ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

Nota: Para relacionar el pago de los aportes correspondientes a los Sistemas de Seguridad Social, se deberán tener en cuenta los plazos previstos en el Decreto 1406 de 1999 artículos 19 a 24 y Decreto 2236 de 1999. Así mismo, en el caso correspondiente a los aportes parafiscales: CAJAS DE COMPENSACION FAMILIAR, ICBF y SENA, se deberá tener en cuenta el plazo dispuesto para tal efecto en el Decreto 1464 de 2005.

Dada en Bogotá a los (25) días del mes de noviembre de 2024.



FIRMA

NOMBRE DE QUIEN CERTIFICA: Andrea Palacios Villamizar

CEDULA: 1.018.408.058 de Bogotá

UT CREMIL 2023

Nit: 901.783.613-2

correo electrónico: admin@datamotion.online

Dirección: CL 31 13 A 51 TO 2 OF 1803

PLANILLA INTEGRADA AUTOLIQUIDACIÓN APORTES COMPROBANTE DE PAGO

DATOS GENERALES DEL APORTANTE			
TIPO IDENTIFICACIÓN:	NIT NÚMERO DE IDENTIFICACIÓN:		830110359
NOMBRE Ó RAZÓN SOCIAL:	CAPACITACION Y SERVICIOS ESPECIALIZADOS SAS		
CIUDAD/MUNICIPIO:	BOGOTA DISTRITO CAPITAL DEPARTAMENTO:	BOGOTA - DISTRITO CAPITAL	
DIRECCIÓN:	CARRERA 13 # 46 - 76 OF. 501 TELÉFONO:	3383564	
TIPO APORTANTE:	01-EMPLEADOR CLASE APORTANTE:	B-MENOS DE 200 COTIZANTES	
TIPO EMPRESA:	PRIVADA ACTIVIDAD ECONOMICA:	Actividades reguladoras y	
FORMA DE PRESENTACIÓN:	ÚNICO		
APORTANTE EXONERADO PAGO APORTES SALUD, SENA E ICBF (REFORMA TRIBUTARIA):			SI

DATOS GENERALES DE LA PLANILLA			
NÚMERO PLANILLA:	7952614661	TIPO DE PLANILLA:	E-EMPLEADOS
PERIODO COTIZACIÓN	MES: noviembre	PERIODO COTIZACIÓN	MES: diciembre
OTROS SUBSISTEMAS:	AÑO: 2024	SALUD:	AÑO: 2024
DÍAS DE MORA:	0		
FECHA PAGO (aaaa/mm/dd):	2024/12/11	NÚMERO AUTORIZACIÓN:	1117668668

LIQUIDACIÓN GENERAL				
				TOTALES
				COTIZANTES
				TOTAL PAGADO
PENSIÓN				
ADMINISTRADORA				
NIT	CÓDIGO	NOMBRE		
800229739	230201	230201- PROTECCION		5
900336004	25-14	25-14 COLPENSIONES		6
800227940	231001	231001-COLFONDOS		2
800253055	230901	230901-SKANDIA OBLIGATORIO		1
800224808	230301	230301-PORVENIR		6
SUBTOTAL:				20
SALUD				
ADMINISTRADORA				
NIT	CÓDIGO	NOMBRE		
830003564	EPS017	EPS017-FAMISANAR		3
800251440	EPS005	EPS005-SANITAS S.A.		3
800130907	EPS002	EPS002-SALUD TOTAL		1
900156264	EPS037	EPS037-NUEVA EPS		2
830113831	EPS001	EPS001-ALIANSA SALUD S.A.		5
800088702	EPS010	CIA SURAMERICANA DE SERVICIOS DE SALUD		4
860066942	EPS008	EPS008-COMPENSAR		3
SUBTOTAL:				21
CAJA DE COMPENSACIÓN				
ADMINISTRADORA				
NIT	CÓDIGO	NOMBRE		
860007336	CCF22	CCF22-COLSUBSIDIO		14
890900841	CCF04	CCF04-CCF DE ANTIOQUIA		2
890200106	CCF39	CCF39-CAJASAN		4
SUBTOTAL:				20
RIESGOS PROFESIONALES				
ADMINISTRADORA				
NIT	CÓDIGO	NOMBRE		
860011153	14-23	14-23-POSITIVA COMPAÑIA DE SEGUROS S.A.		20
SUBTOTAL:				20

C
O
N
F
I
D
E
N
C
I
A
L

VALOR SIN MORA:	CONFIDENCIAL
VALOR MORA:	
TOTAL PAGADO:	



DATOS DEL APORTANTE						DATOS DE LA PLANILLA									
TIPO	NÚMERO	NOMBRE RAZÓN SOCIAL		DIRECCIÓN	TELÉFONO	FAX	PERIODO LIQUIDACIÓN				TIPO PLANILLA	FECHA PAGO (DÍA MES AÑO)	NÚMERO RADICACIÓN	EXONERADO PAGO PARAFISCALES Y SALUD	SE ACOGE A LOS BENEFICIOS DE LEY 1429 DE 2010 A CAJAS DE COMPENSACIÓN FAMILIAR
NI	901477680	DATAMOTION SAS		Calle 31 No 13A-51 Torre 2 Oficina 1803	3182394432		SALUD		PENSIÓN, RIESGOS LAB, CAJA, SENA, ICBF						
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		MES	AÑO	MES	AÑO					
U	C	PRINCIPAL	PPAL	BOGOTÁ D. C.	BOGOTÁ, D.C.		12	2024	11	2024	E	20 12 2024	82403981	Si	No

CENTRO DE TRABAJO		Todos		NÚMERO DE EMPLEADOS				3				NIT EMPRESA CONVENIO								Todos															
No	DOCUMENTO	APELLIDOS Y NOMBRES		TIPO COT	SUB COT	EXT	COL EXT	Exon	COD MUN	COD DEP	ING	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRP	EPS	AFP	ARL	CCF	CÓDIGO EPS	CÓDIGO AFP	CÓDIGO ARL	CÓDIGO CCF		
1	CC 1018408058	PALACIOS VILLAMIZAR ANDREA		1	0			Si	001	11																30	30	30	30	EPS005	230301	14-23	CCF22		
2	CC 14398631	HERNANDEZ JIMENEZ JUAN CAMILO		1	0			Si	001	11																30	30	30	30	EPS005	231001	14-23	CCF22		
3	CC 80201964	HERNANDEZ JIMENEZ DANIEL		1	0			Si	001	11																30	30	30	30	EPS005	230301	14-23	CCF22		

INFORME CONTRATO MC-037 DE 2024

CONTRATAR LOS SERVICIOS DE RENOVACIÓN DE LAS LICENCIAS, SOPORTE DE FÁBRICA DE LOS FIREWALL EN ALTA DISPONIBILIDAD Y EL SERVICIO PARA CUMPLIR CON LOS CRITERIOS DE ADMINISTRACIÓN GESTIÓN, MANTENIMIENTO Y SOPORTE TÉCNICO DE CANAL LOS CUALES HACEN PARTE DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL DE LA CAJA DE RETIRO DE LAS FF.MM”.

Preparado por: Pedro Julio Esteban Ríos / Gerente de Implementaciones

Fecha 27/12/2024

Cliente:
CAJA DE RETIRO DE LAS FFMM - CREMIL

UT CREMIL 2023 Bogotá - Colombia

SECURITY LIFECYCLE REVIEW

CREMIL - Caja de Retiro de las Fuerzas Militares



Preparado por:

Cayses SAS

Palo Alto Networks

www.paloaltonetworks.com

Período del informe: 8 DAYS

Fri, Dec 20, 2024 - Fri, Dec 27, 2024

TABLE OF CONTENTS

3 Resumen Ejecutivo

4 Aplicaciones

Información general sobre aplicaciones

Aplicaciones que introducen riesgos

Aplicaciones que introducen riesgos: detalle

APLICACIONES SAAS

13 Análisis de Advanced URL Filtering

Traffic Distribution

PRINCIPALES CATEGORÍAS Y DISTRIBUCIÓN DE DOMINIOS

Solicitudes malintencionadas por ubicación

18 Análisis de seguridad de DNS

Distribución del tráfico

Dominios y distribución de destino

22 Amenazas

Análisis de Advanced Threat Prevention

Vulnerabilidades de aplicaciones

Análisis de mando y control

Análisis de tipos de archivos de alto riesgo y maliciosos

27 Transferencia de archivos

Análisis de la transferencia de archivos

28 Resumen

Resumen ejecutivo CREMIL - Caja de Retiro de las Fuerzas Militares

En la Revisión del ciclo de vida de la seguridad se resumen los riesgos para el negocio y la seguridad que enfrenta **CREMIL - Caja de Retiro de las Fuerzas Militares**. 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.

Información Confidencial: No Redistribuir

CONCLUSIONES CLAVE

185

APLICACIONES EN USO

Se utilizan **185** 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.

28

APLICACIONES DE ALTO RIESGO

Se observaron **28** aplicaciones de alto riesgo, incluidas aquellas que pueden ocultar o introducir actividad maliciosa, transferir archivos fuera de la red o establecer comunicación no autorizada.

61

APLICACIONES SAAS

Se observaron **61** aplicaciones SaaS en su red. Para mantener el control a nivel administrativo, adopte aplicaciones SaaS que serán gestionadas por su equipo de TI.

1,447,039

EXPLOITS DE VULNERABILIDAD

En su organización se observaron **1,447,039** exploits de vulnerabilidades en total, entre los que se incluyen las categorías de vulnerabilidades **Signature detections**.

1,447,043

AMENAZAS TOTALES

Se detectaron **1,447,043** 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.

29

SOLICITUDES MALINTENCIONADAS

El filtrado avanzado de URL ha identificado **29** solicitudes malintencionadas. Estas solicitudes malintencionadas incluyen ransomware, malware, phishing, comando y control, y grayware.

Información general sobre aplicaciones

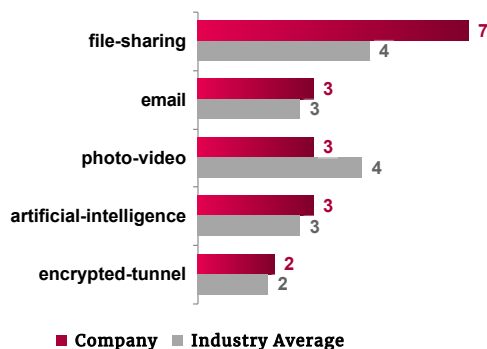
Las aplicaciones pueden introducir riesgos, como enviar amenazas, potencialmente permitir que los datos salgan de la red, permitir acceso no autorizado, reducir la productividad o consumir ancho de banda de la empresa. Esta sección proporciona visibilidad de las aplicaciones en uso, lo que le permite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

CONCLUSIONES CLAVE

- Se observaron aplicaciones de alto riesgo como **file-sharing**, **email**, y **photo-video** en la red, las cuales deben ser investigadas debido a la posibilidad de abuso.
- Se observaron **185** aplicaciones en total en la red en **31** subcategorías, a diferencia del promedio de **154** aplicaciones en total para el sector que se observaron en otras organizaciones de **Government - County**.
- Todas las aplicaciones usaron un **523.84 GB**, incluido **networking** con **305.04 GB**, a diferencia del promedio del sector de **768.43 TB** en organizaciones similares.

APLICACIONES DE ALTO RIESGO

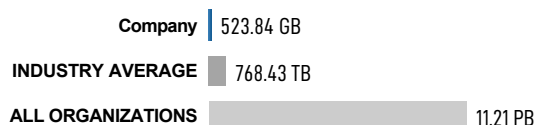
El primer paso para gestionar el nivel de riesgo para el negocio y la seguridad consiste en identificar qué aplicaciones pueden ser usadas para causar el mayor nivel de daño. Recomendamos evaluar detenidamente las aplicaciones que pertenecen a estas categorías para asegurarse de que no estén introduciendo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



NÚMERO DE APLICACIONES EN LA RED

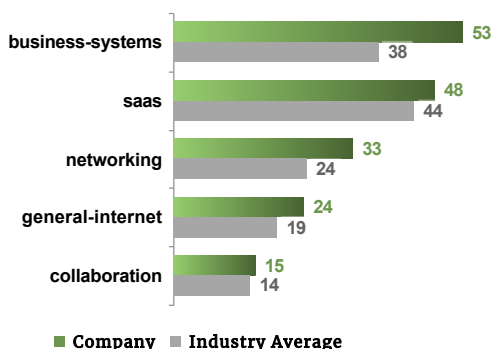


BANDO DE ANCHA CONSUMIDO POR APLICACIONES



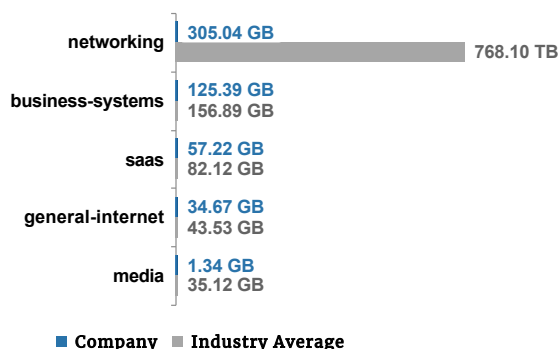
CATEGORÍAS QUE INCLUYEN LA MAYOR CANTIDAD DE APLICACIONES

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 **Government - County**. Estos datos se pueden usar para priorizar con mayor eficacia sus esfuerzos para habilitar aplicaciones.

RISK LEVEL



CONCLUSIONES CLAVE

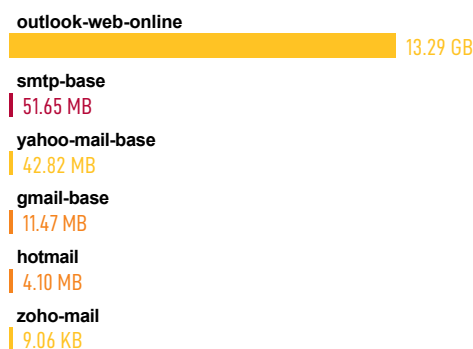
- En su organización se observaron **185** aplicaciones en total, a diferencia del promedio del sector de **154** en otras organizaciones de **Government - County**.
- Los tipos de subcategorías de aplicaciones más comunes son: **internet-utility, infrastructure, y general-business**.
- Las subcategorías de aplicaciones que consumen la mayor cantidad de ancho de banda son: **encrypted-tunnel, storage-backup, y infrastructure**.

■ Number of Applications in the subcategory ■ Industry Average



Email 13.4 GB

TOP EMAIL APPS

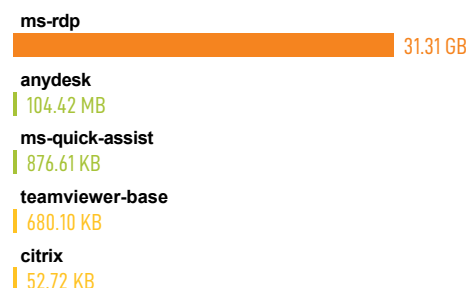


■ Number of Applications in the subcategory ■ Industry Average



Remote-Access 31.41 GB

TOP REMOTE-ACCESS APPS

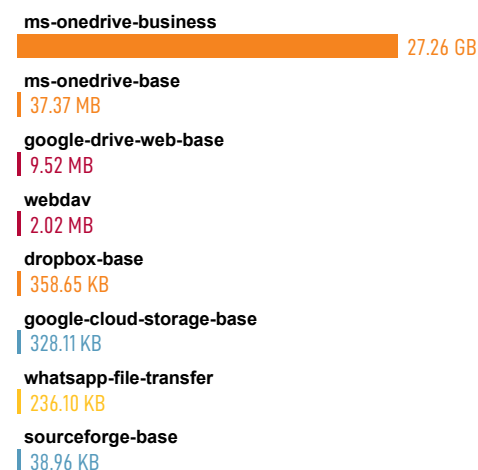


■ Number of Applications in the subcategory ■ Industry Average



File-Sharing 27.31 GB

TOP FILE-SHARING APPS

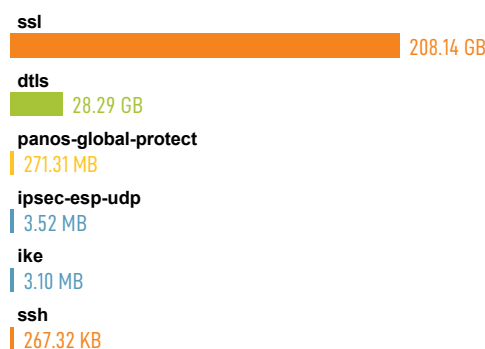


■ Number of Applications in the subcategory ■ Industry Average



Encrypted-Tunnel 236.71 GB

TOP ENCRYPTED-TUNNEL APPS

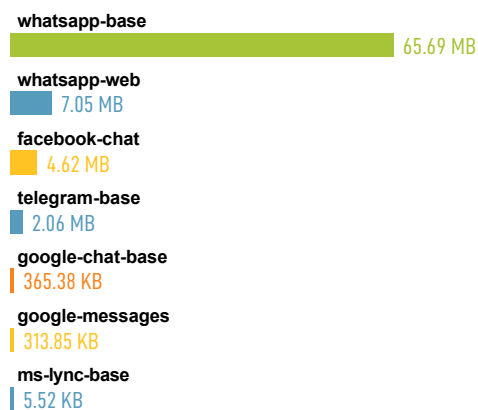


■ Number of Applications in the subcategory ■ Industry Average



Instant-Messaging 80.11 MB

TOP INSTANT-MESSAGING APPS

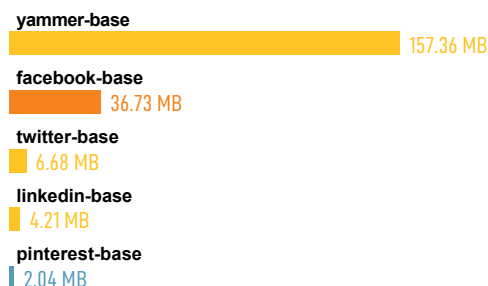


■ Number of Applications in the subcategory ■ Industry Average



Social-Networking 207.01 MB

TOP SOCIAL-NETWORKING APPS

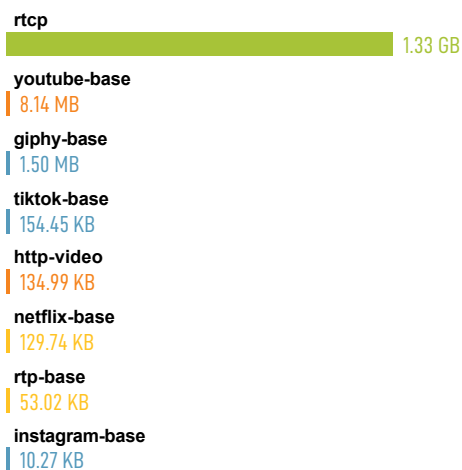


■ Number of Applications in the subcategory ■ Industry Average



Photo-Video 1.34 GB

TOP PHOTO-VIDEO APPS



■ Number of Applications in the subcategory ■ Industry Average



Proxy 18.31 KB

TOP PROXY APPS



Aplicaciones que introducen riesgos: detalle

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
3	outlook-web-online	saas	email	browser-based	13.29 GB	34202
5	smtp-base	collaboration	email	client-server	51.65 MB	41
3	yahoo-mail-base	saas	email	browser-based	42.82 MB	4643
4	gmail-base	saas	email	browser-based	11.47 MB	986
4	hotmail	collaboration	email	browser-based	4.1 MB	502
3	zoho-mail	saas	email	browser-based	9.06 KB	1
4	ssl	networking	encrypted-tunnel	browser-based	208.14 GB	2782379
1	dtls	networking	encrypted-tunnel	client-server	28.29 GB	971
3	panos-global-protect	networking	encrypted-tunnel	client-server	271.31 MB	1141
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	3.52 MB	20
2	ike	networking	encrypted-tunnel	client-server	3.1 MB	5685
4	ssh	networking	encrypted-tunnel	client-server	267.32 KB	14
4	ms-onedrive-business	saas	file-sharing	client-server	27.26 GB	16451
4	ms-onedrive-base	saas	file-sharing	client-server	37.37 MB	2149
5	google-drive-web-base	saas	file-sharing	browser-based	9.52 MB	25
5	webdav	general-internet	file-sharing	browser-based	2.02 MB	977
4	dropbox-base	general-internet	file-sharing	client-server	358.65 KB	22
2	google-cloud-storage-base	saas	file-sharing	browser-based	328.11 KB	57
3	whatsapp-file-transfer	general-internet	file-sharing	client-server	236.1 KB	29
2	sourceforge-base	saas	file-sharing	client-server	38.96 KB	5
1	whatsapp-base	collaboration	instant-messaging	client-server	65.69 MB	2739
2	whatsapp-web	collaboration	instant-messaging	browser-based	7.05 MB	23
3	facebook-chat	saas	instant-messaging	browser-based	4.62 MB	29
2	telegram-base	collaboration	instant-messaging	client-server	2.06 MB	20
4	google-chat-base	saas	instant-messaging	browser-based	365.38 KB	159

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
3	google-messages	collaboration	instant-messaging	browser-based	313.85 KB	17
2	ms-lync-base	collaboration	instant-messaging	client-server	5.52 KB	4
1	rtcp	media	photo-video	client-server	1.33 GB	130
4	youtube-base	media	photo-video	browser-based	8.14 MB	234
2	giphy-base	saas	photo-video	browser-based	1.5 MB	16
2	tiktok-base	media	photo-video	client-server	154.45 KB	7
4	http-video	media	photo-video	browser-based	134.99 KB	1
3	netflix-base	media	photo-video	browser-based	129.74 KB	10
3	rtp-base	media	photo-video	client-server	53.02 KB	1
2	instagram-base	media	photo-video	client-server	10.27 KB	1
5	http-proxy	networking	proxy	browser-based	18.31 KB	13
4	ms-rdp	networking	remote-access	client-server	31.31 GB	821
1	anydesk	networking	remote-access	client-server	104.42 MB	156
1	ms-quick-assist	networking	remote-access	client-server	876.61 KB	2
3	teamviewer-base	saas	remote-access	client-server	680.1 KB	7
3	citrix	networking	remote-access	client-server	52.72 KB	231
3	yammer-base	saas	social-networking	client-server	157.36 MB	1040
4	facebook-base	saas	social-networking	browser-based	36.73 MB	101
3	twitter-base	collaboration	social-networking	browser-based	6.68 MB	11
3	linkedin-base	collaboration	social-networking	browser-based	4.21 MB	117
2	pinterest-base	collaboration	social-networking	browser-based	2.04 MB	46

Notes:

APLICACIONES SAAS

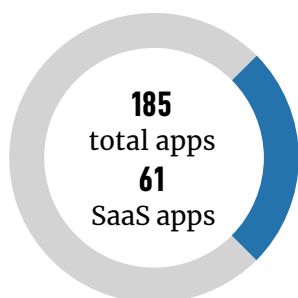
Los servicios de aplicaciones basadas en SaaS continúan redefiniendo el perímetro de la red. Normalmente denominados “shadow IT”, la mayoría de estos servicios son adoptados directamente por usuarios particulares, equipos de negocios o incluso departamentos enteros. Con el objetivo de minimizar los riesgos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

CONCLUSIONES CLAVE

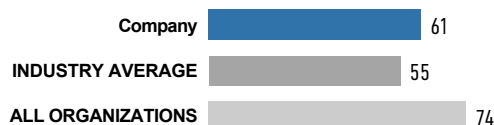
- **Office-Programs** tiene la mayor cantidad de aplicaciones SaaS exclusivas.
- En términos de movimiento de datos, **ms-onedrive-business** es la aplicación SaaS más usada en su organización.

APLICACIONES SAAS EN NÚMEROS

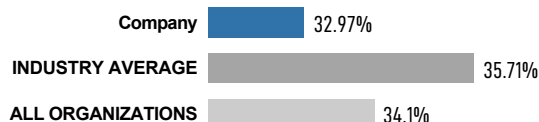
Revise las aplicaciones que se están usando en su organización. Para garantizar el control administrativo, adopte las aplicaciones SaaS que serán gestionadas por su equipo de TI.



NUMBER OF SAAS APPLICATIONS

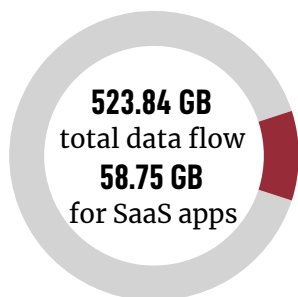


PERCENTAGE OF ALL APPLICATIONS

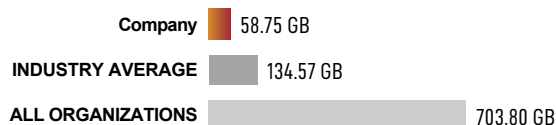


ANCHO DE BANDA DE LAS APLICACIONES SAAS

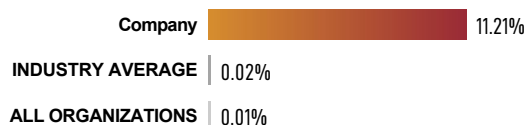
Controle el volumen de movimiento de datos hacia y desde las aplicaciones SaaS. Entienda la naturaleza de las aplicaciones y cómo se están usando.



SAAS APPLICATION BANDWIDTH



PERCENTAGE OF ALL BANDWIDTH



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



■ Number of Applications in the subcategory ■ Industry Average

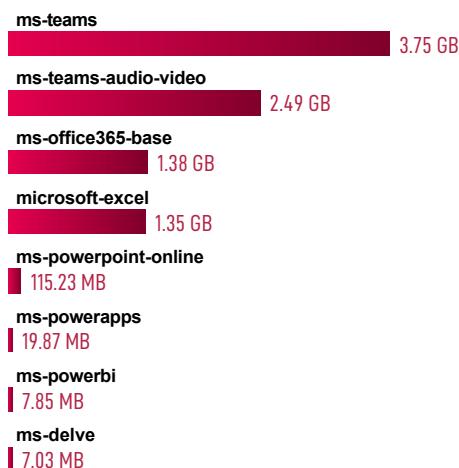
■ Number of Applications in the subcategory ■ Industry Average

10

8

Office-Programs 9.12 GB

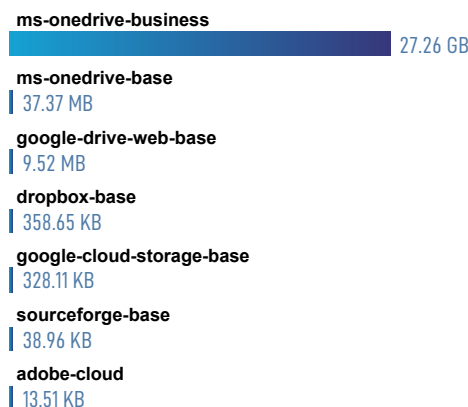
TOP OFFICE-PROGRAMS APPS



■ Number of Applications in the subcategory ■ Industry Average

File-Sharing 27.3 GB

TOP FILE-SHARING APPS



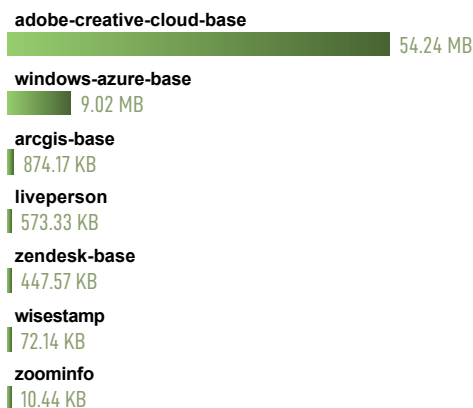
■ Number of Applications in the subcategory ■ Industry Average

7

14

General-Business 65.24 MB

TOP GENERAL-BUSINESS APPS

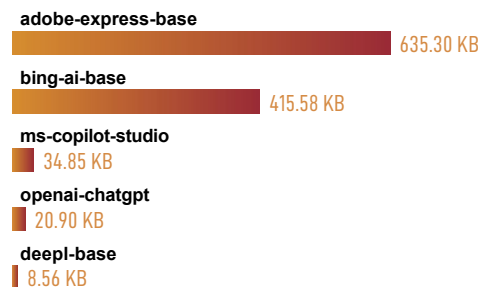


5

4

Artificial-Intelligence 1.12 MB

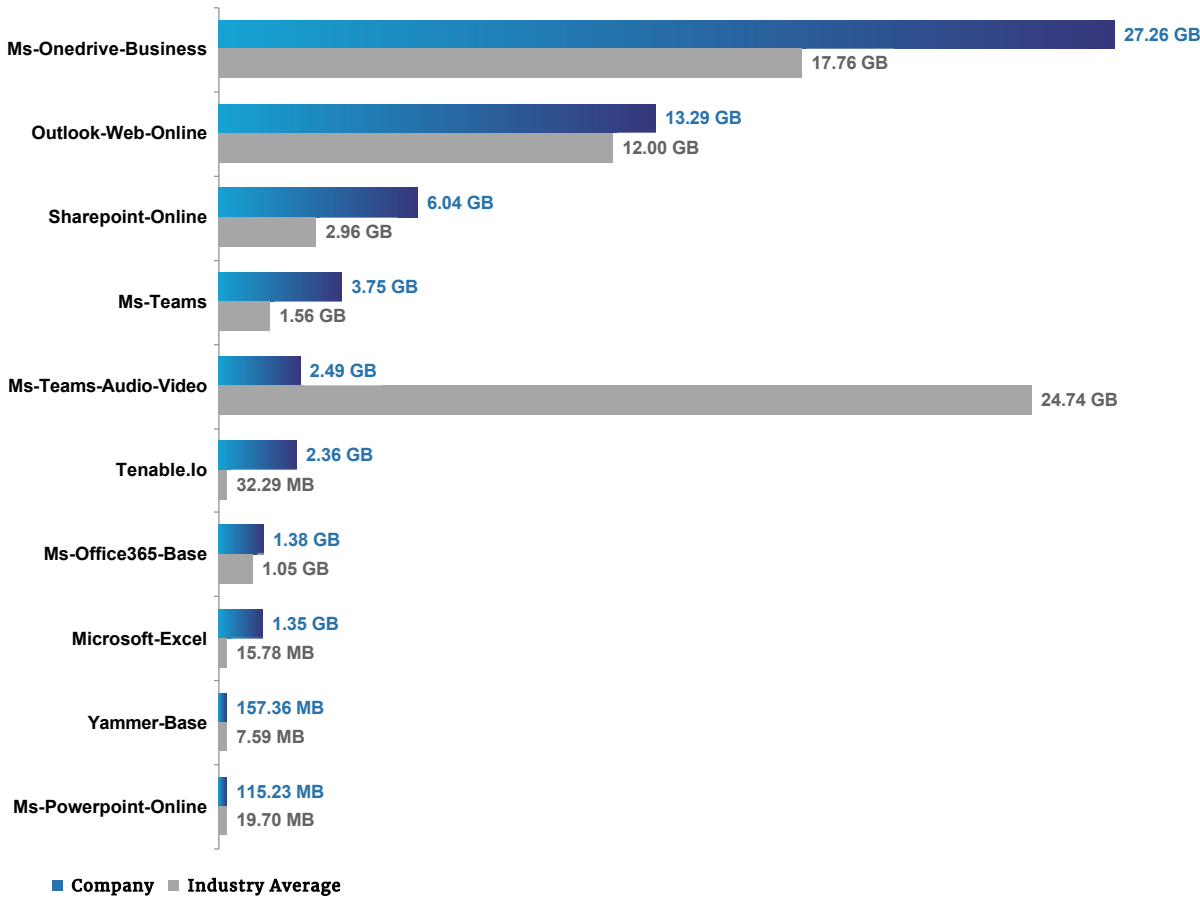
TOP ARTIFICIAL-INTELLIGENCE APPS



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.

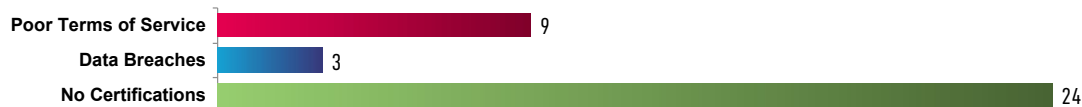
TOP SAAS APPLICATIONS BY DATA MOVEMENT



APLICACIONES SAAS POR RIESGO DE HOSTING

En función del uso que usted haga de SaaS, resulta fundamental revisar en forma regular las aplicaciones SaaS a las que se accede, quién accede a ellas y cómo se las utiliza.

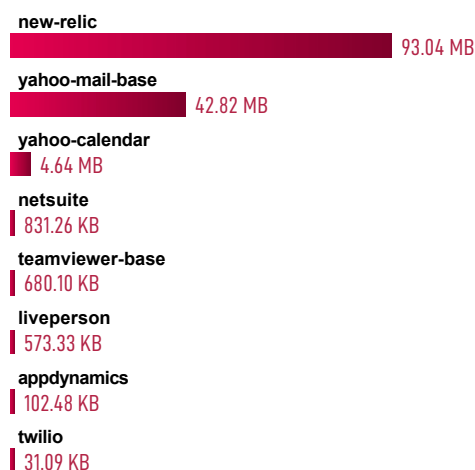
En el siguiente gráfico, se muestra la cantidad de aplicaciones por cada característica de riesgo de hosting.



Los siguientes gráficos muestran las principales aplicaciones por ancho de banda por cada característica de riesgo de hosting.

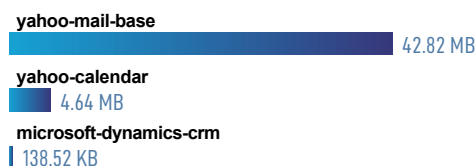
142.74 MB

Apps with Poor Terms of Service



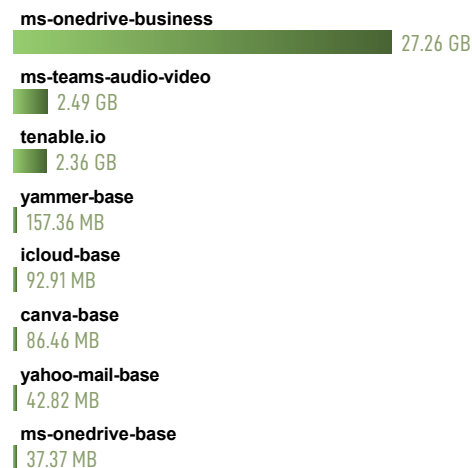
47.6 MB

Apps with Data Breaches



32.61 GB

Apps with No Certifications



Análisis de Advanced URL Filtering

Fri, Dec 20, 2024 - Fri, Dec 27, 2024

A medida que las aplicaciones se trasladan a la nube y las personas trabajan desde cualquier lugar, es cada vez más importante (y más difícil) proteger el tráfico de la web. Los ataques basados en la web, como la suplantación de identidad o phishing, el comando y control, y otros ataques sin archivos, llegan con mayor volumen, mayor velocidad y mayor sofisticación. El servicio de filtrado avanzado de URL de Palo Alto Networks le ofrece una visión profunda del tráfico de la web, le permite controlar el acceso a la web mediante políticas granulares y le permite prevenir las amenazas basadas en la web en tiempo real.

175,833

DE SOLICITUDES DE URL EN TOTAL

El filtrado avanzado de URL ha analizado **175,833** solicitudes de URL en su red. La web se ha convertido en una de las superficies de ataque más utilizadas y las páginas web malintencionadas pueden utilizarse para la entrega de malware o ransomware, comando y control (C2) o exfiltración de datos.

29

SOLICITUDES MALINTENCIONADAS

El filtrado avanzado de URL ha identificado **29** solicitudes malintencionadas. Estas solicitudes malintencionadas incluyen ransomware, malware, phishing, comando y control, y grayware.

12

DIRECCIONES IP MALINTENCIONADAS

El filtrado de URL avanzado ha identificado **12** direcciones IP malintencionadas detrás de estas URL/dominios malintencionados. Estas direcciones IP pueden utilizarse como infraestructura C2 para exfiltrar datos, entregar malware o enviar comandos remotos a un sistema de su red.

9,641

URL ANALIZADAS EN TIEMPO REAL

Se han analizado **9,641** solicitudes de URL en tiempo real. El análisis de las URL en tiempo real protege a los usuarios de ataques malintencionados nuevos o nunca vistos en milisegundos.

TRAFFIC DISTRIBUTION

La navegación por Internet sin control expone a las organizaciones a riesgos para la seguridad y el negocio, como la exposición a posibles ciberamenazas, la pérdida de datos, el robo de credenciales o el incumplimiento de la normativa. Esta sección le proporcionará visibilidad respecto de las solicitudes de URL en su red, lo cual le permitirá tomar decisiones informadas sobre el riesgo potencial frente al beneficio de negocios. Las URL y los dominios malintencionados de su red deben revisarse para comprender quién accede a ellos y el riesgo potencial asociado a ellos.

CONCLUSIONES CLAVE

- Los usuarios visitaron un total de **175,833** URL durante el período de informe en **51** categorías.
- De ese total, **29** solicitudes eran conocidas por ser sitios web malintencionados, incluidos sitios de ransomware, malware, comando y control, phishing y grayware.
- Se visitaron **61** sitios de alto riesgo y **26,718** de riesgo medio.
- Se analizaron en tiempo real **0** solicitudes malintencionadas.

DISTRIBUCIÓN DE SOLICITUDES DE URL



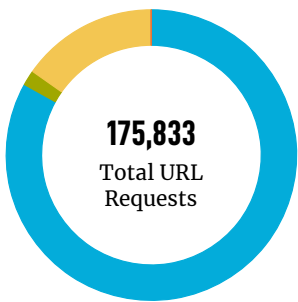
Benign 99.98%
Malicious 0.02%

CATEGORÍAS DE SOLICITUDES DE URL MALINTENCIONADAS



Malware 86.21%
Phishing 6.90%
Grayware 6.90%

NIVELES DE RIESGO DE LAS SOLICITUDES DE URL



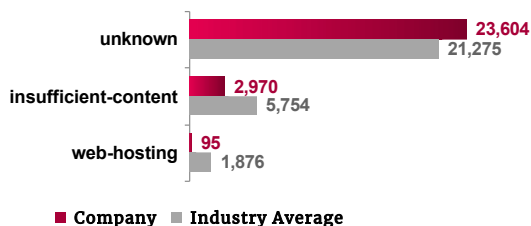
High 0.03%
Medium 15.20%
Low 83.08%

PRINCIPALES CATEGORÍAS Y DISTRIBUCIÓN DE DOMINIOS

Los siguientes gráficos indican las categorías y los dominios más visitados.

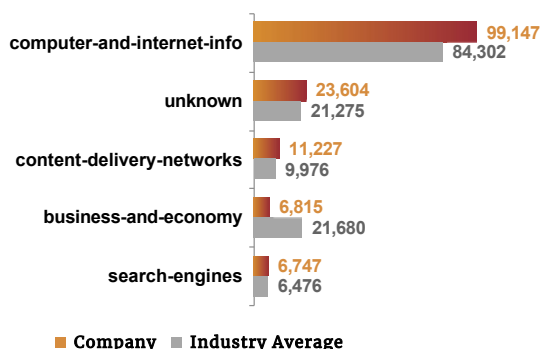
CATEGORÍAS QUE GENERAN UN RIESGO POTENCIAL

Internet es un canal de ataque principal para los actores malintencionados. Las categorías de alto riesgo como desconocido, contenido insuficiente, cuestionable, alto riesgo, detenido, DNS dinámico, alojamiento web y dominios registrados recientemente deben bloquearse o configurarse para que el descifrado de SSL con políticas estrictas de control de amenazas pueda obtener una mejor visibilidad y control.



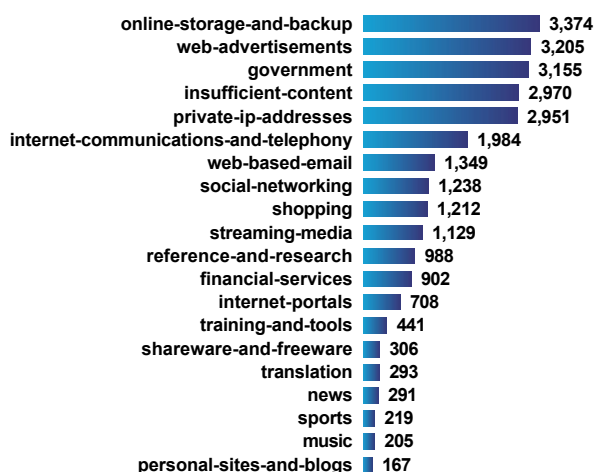
LAS 5 CATEGORÍAS MÁS VISITADAS

A continuación, se muestran las 5 categorías de URL visitadas con mayor frecuencia, junto con los puntos de referencia del sector para su grupo de peers. Comprender la combinación de tráfico web a lo largo del tiempo lo ayudará a identificar anomalías que puedan indicar actividad malintencionada.



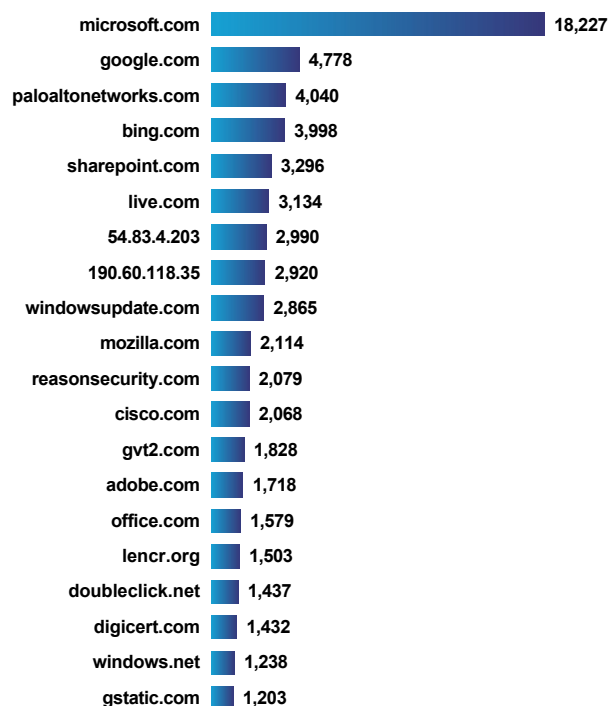
OTRAS CATEGORÍAS MÁS VISITADAS

A continuación, se muestran las siguientes 20 categorías de URL más visitadas. Comprender la combinación de tráfico web a lo largo del tiempo le ayudará a identificar anomalías que puedan indicar actividad malintencionada.



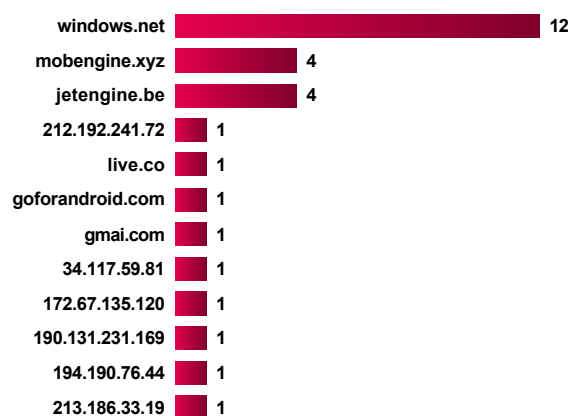
DOMINIOS MÁS VISITADOS

A continuación, se muestran los 20 dominios más visitados en su red. Es importante ver regularmente los dominios más visitados de su red. Comprender el uso de tráfico web a lo largo del tiempo lo ayudará a identificar anomalías que puedan indicar actividad malintencionada.



DOMINIOS MALINTENCIONADOS MÁS VISITADOS

A continuación, se muestran los principales 20 dominios malintencionados visitados en su red. Los dominios malintencionados deben revisarse para comprender el volumen de las solicitudes de dominio, quién accede a esos dominios y qué familias de malware están asociadas a dichos dominios. Las visitas frecuentes a dominios malintencionados desde la misma máquina pueden indicar un endpoint infectado.



URL MALINTENCIONADAS POR NÚMERO DE SERIE DEL DISPOSITIVO

La siguiente tabla muestra el volumen de solicitudes malintencionadas por número de serie del dispositivo. Las URL malintencionadas deben revisarse regularmente para comprender quién accede a esas URL y qué familias de malware están asociadas a esos dominios. Una diferencia considerable en la cantidad de URL malintencionadas entre los números de serie de los dispositivos puede indicar que un sitio en particular puede tener más endpoints infectados.

DEVICE SN	MALICIOUS URLS
026701014833	29

SOLICITUDES MALINTENCIONADAS POR UBICACIÓN

CONCLUSIONES CLAVE

- Se detectaron **12** solicitudes malintencionadas en su red y el **41.67%** de ellas estaban alojadas en **United States of America**.

SOLICITUDES MALINTENCIONADAS POR UBICACIÓN



Análisis de seguridad de DNS

Fri, Dec 20, 2024 - Fri, Dec 27, 2024

166,281

SOLICITUDES DNS ANALIZADAS

El servicio de Seguridad DNS en tiempo real ha analizado **166,281** solicitudes DNS en su red. DNS es una superficie de ataque que, a menudo, se pasa por alto y que puede utilizarse para la distribución de malware, las campañas de phishing/ransomware, las actividades de grayware, el comando y control (C2) o la exfiltración de datos.

34

DOMINIOS MALINTENCIONADOS IDENTIFICADOS

El servicio de seguridad DNS ha identificado **34** dominios malintencionados. Estos dominios fueron utilizados por algoritmos de generación de dominios (DGA), túneles DNS, malware, phishing o grayware.

4

PAÍSES DE DESTINO QUE ALOJAN DOMINIOS MALINTENCIONADOS

El servicio de Seguridad DNS ha identificado **4** países de destino que alojan estos dominios malintencionados.

3,227

SOLICITUDES DNS MALINTENCIONADAS IDENTIFICADAS

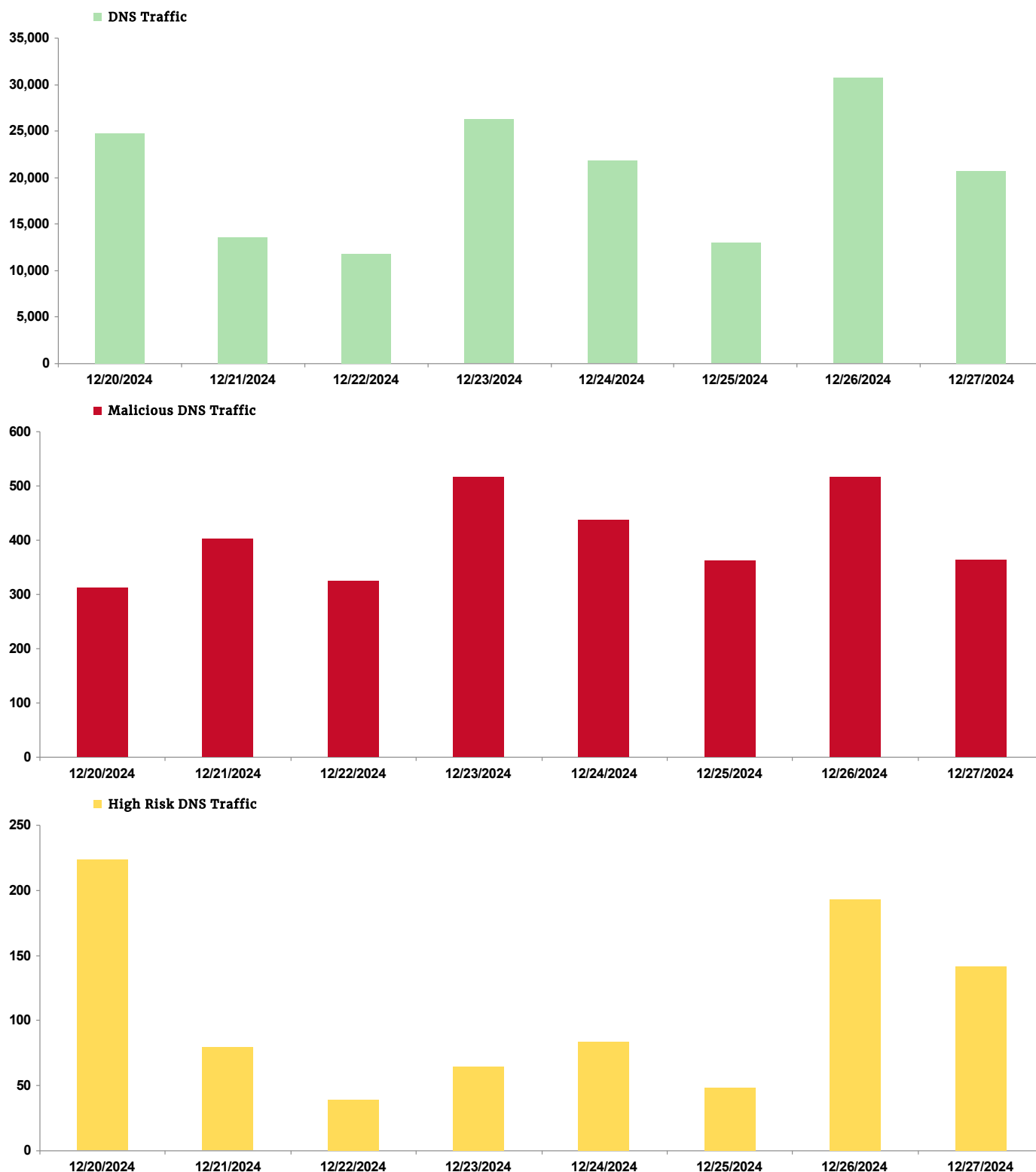
El servicio de Seguridad DNS ha identificado **3,227** solicitudes DNS malintencionadas en su red

DISTRIBUCIÓN DEL TRÁFICO

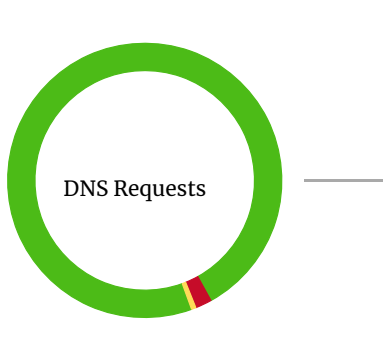
Muchos equipos de seguridad no inspeccionan el tráfico DNS en busca de amenazas porque suponen que las consultas enviadas a través del protocolo DNS y el puerto 53 son benignas. Además de cuán frecuente y fácilmente se abusan los DNS, la velocidad y el volumen de nuevos dominios malintencionados es tan enorme que no se logra crear firmas estáticas con la rapidez suficiente para abordarlos. Si un sistema se ve infectado, los equipos de redes y seguridad se ven desafiados a identificar rápidamente ese sistema y resolver la infección. Para ese entonces, es posible que el malware ya se haya propagado o los datos ya se hayan robado.

CONCLUSIONES CLAVE

- Se observó un total de **166,281** consultas DNS en su red
- Se observaron **34** dominios malintencionados que incluyen C2, DGA, tunelización, malware, grayware y phishing
- Se observaron **870** dominios de alto riesgo, incluidos los detenidos, los dominios registrados recientemente (NRD), la evasión de proxy y los DNS dinámicos

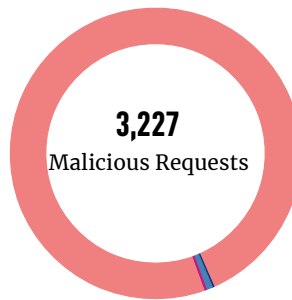


DNS REQUESTS



■ Benign 97.54%
■ Malicious 1.94%
■ High Risk 0.52%

MALICIOUS REQUESTS



■ Malware 98.98%
■ Phishing 0.12%
■ Grayware 0.71%
■ Strategically Aged Domain 0.19%

HIGH RISK REQUESTS

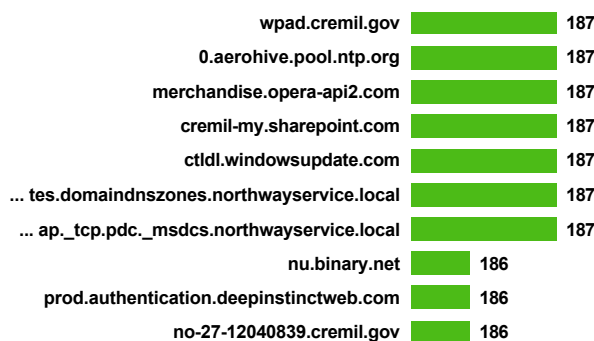


■ Proxy Avoidance 51.61%
■ Parked 47.01%
■ DDNS 0.57%
■ CNAME Cloaking 0.11%

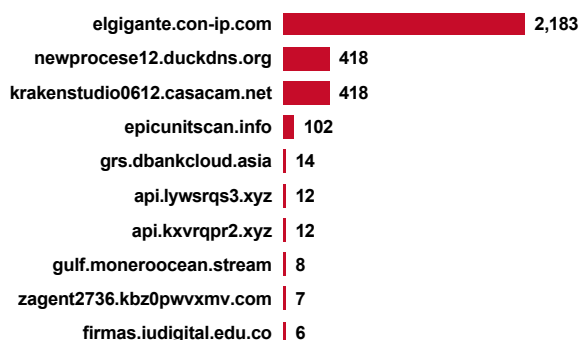
DOMINIOS Y DISTRIBUCIÓN DE DESTINO

En los siguientes gráficos se enumeran los principales dominios y las principales resoluciones con más tráfico en su red.

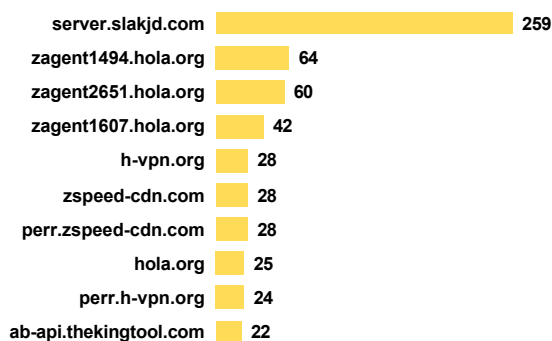
DOMINIOS PRINCIPALES POR TRÁFICO



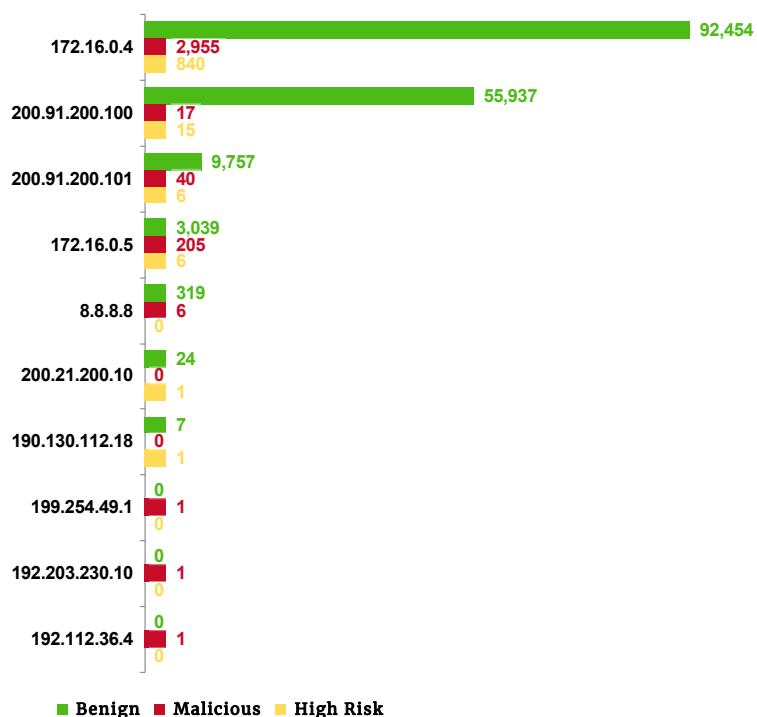
DOMINIOS MALINTENCIONADOS PRINCIPALES POR TRÁFICO



DOMINIOS PRINCIPALES DE ALTO RIESGO POR TRÁFICO



PRINCIPALES RESOLUCIONES DNS POR TRÁFICO



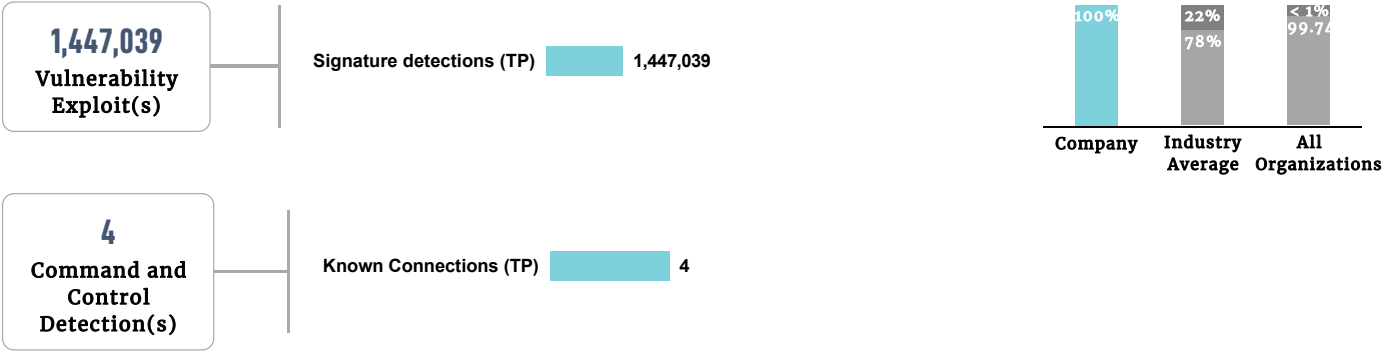
Análisis de Advanced Threat Prevention

Fri, Dec 20, 2024 – Fri, Dec 27, 2024

Para comprender su exposición a los riesgos 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. Esta sección detalla amenazas conocidas, como exploits, malware y actividad de comando y control (C2), además de C2 y exploits desconocidos observados en su red.

CONCLUSIONES CLAVE

- En su organización se observaron **1,447,039** exploits de vulnerabilidades en total, entre los que se incluyen las categorías de vulnerabilidades **Signature detections**.
- Se observaron **0** eventos de malware, frente a un promedio del sector de **3,345** para su grupo del peer.
- Se identificaron **4** 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.



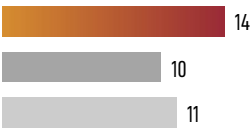
Vulnerabilidades de aplicaciones

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

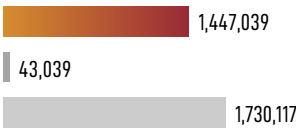
CONCLUSIONES CLAVE

- Se observaron **14** aplicaciones en total que envían exploits a su entorno.
- Se observaron **1,447,039** exploits de vulnerabilidades en total y las tres categorías más importantes son **ssl**, **active-directory-base**, y **ms-ds-smbv3**.
- Del total de vulnerabilidades descubiertas, se detectaron **24** vulnerabilidades únicas, lo que significa que los atacantes usaron los mismos exploits de vulnerabilidades una y otra vez.

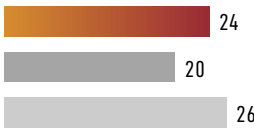
APPLICATIONS DELIVERING EXPLOITS



TOTAL VULNERABILITY EXPLOITS



UNIQUE VULNERABILITY EXPLOITS



Company Industry Average All Organizations

EXPLOITS DE VULNERABILIDAD POR APLICACIÓN

(PRINCIPALES 5 APLICACIONES CON MAYOR DETECCIÓN)

DETECTIONS	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
755,081	Ssl			
8	Nmap Aggressive Option Print Detection	LOW	hacktool	
754,225	TLS Encrypted Client Hello Extension Detection	INFO	info-leak	
225	Non-TLS Traffic On Port 443	INFO	info-leak	
198	Abnormal SSL traffic on port 443	INFO	protocol-anomaly	
191	Non-RFC Compliant SSL Traffic on Port 443	INFO	protocol-anomaly	
169	SSL TLS CBC Cipher Suite Detection	INFO	info-leak	
65	SSL Weak Cipher Suite Selection Vulnerability	INFO	info-leak	CVE-2016-2183
291,276	Active-Directory-Base			
291,276	Microsoft Windows NTLMSSP Detection	INFO	info-leak	
142,285	Ms-Ds-Smbv3			
30,092	Microsoft Windows RPC Encrypted Data Detected	LOW	code-execution	
84,220	Microsoft Windows NTLMSSP Detection	INFO	info-leak	
27,112	Microsoft Windows user enumeration	INFO	info-leak	
590	Microsoft Office File with Macros Detected	INFO	code-execution	
157	Microsoft Windows Server Service NetrServerGetInfo Opnum 21 Access Attempt	INFO	info-leak	
43	Microsoft Windows Server Service NetrShareEnum access	INFO	info-leak	
28	Netbios SMB Tree connect andX Request C\$ access	INFO	info-leak	
15	Microsoft Office Suspicious File Detection	INFO	code-execution	CVE-2023-23397
10	Netbios SMB Tree connect andX Request F\$ access	INFO	info-leak	

EXECUTIVE SUMMARY		APPLICATIONS		SAAS APPLICATIONS		ADV. URL FILTERING		ADV. DNS SECURITY		ADVANCED THREATS		FILE TRANSFER		SUMMARY	
DETECTIONS ▾		EXPLOIT ID ▾		SEVERITY ▾ ▼		THREAT TYPE ▾		CVE ID ▾							
8		Windows SMB Login Attempt		INFO		brute-force									
104,323		Ldap													
104,323		Microsoft Windows NTLMSSP Detection		INFO		info-leak									
56,041		Ms-Teams													
56,041		TLS Encrypted Client Hello Extension Detection		INFO		info-leak									

Análisis de mando y control

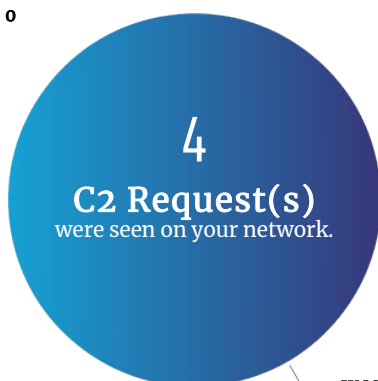
A menudo, la actividad de comando y control (C2) indica que un malware afectó un host de la red y puede estar intentando conectarse fuera de la red con actores malintencionados, intentos de reconocimiento desde el exterior u otras actividades de comando y control. Comprender y prevenir esta actividad resulta fundamental, ya que los atacantes utilizan C2 para entregar malware adicional, dar instrucciones o exfiltrar datos. Los productos de detección y respuesta pueden brindar detalles respecto de la red malintencionada y de la actividad del host que tuvo lugar como consecuencia del malware identificado.

Advanced Threat Prevention es el único IPS que impide ataques nuevos e inéditos basados en el comando y control en tiempo real.

CONCLUSIONES CLAVE

- Se usaron **1** aplicaciones en total para la comunicación de mando y control.
- Se observaron **4** solicitudes de mando y control en total que se originan en su red.
- Se observaron **0** consultas de DNS sospechosas en total.

SUSPICIOUS DNS
QUERIES: 0
EVASIVE COMMAND
& CONTROL: 0



KNOWN COMMAND
& CONTROL: 4



web-browsing: 4



spyware: 4

0 SUSPICIOUS DNS QUERIES

4 KNOWN COMMAND & CONTROL

TOP 10

AndroxGh0st Scanning Traffic Detection

4

0 EVASIVE COMMAND & CONTROL
(Inline Cloud Analysis)

Análisis de tipos de archivos de alto riesgo y maliciosos

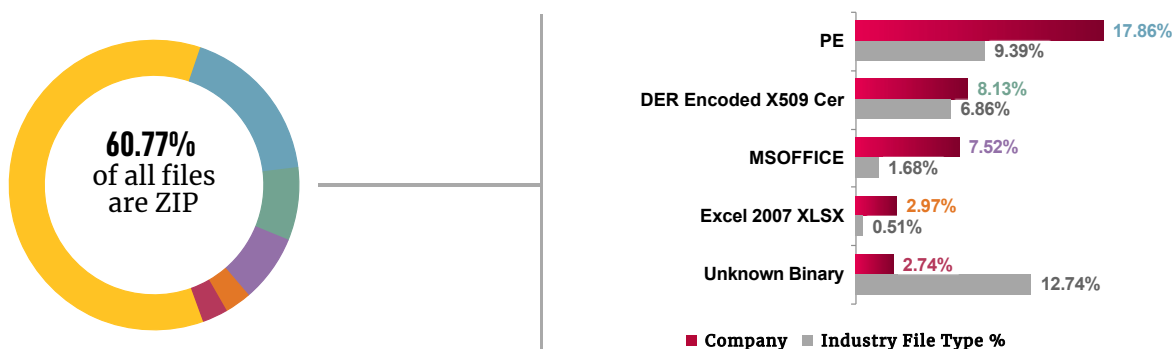
Los ciberatacantes de hoy en día utilizan diversos tipos de archivos para enviar malware y exploits y suelen concentrarse en el contenido de aplicaciones habituales del negocio que se encuentran en la mayoría de las redes empresariales. La mayoría de las amenazas de productos se envía mediante archivos ejecutables y los ataques más específicos y avanzados suelen usar otros contenidos para afectar las redes. Advanced WildFire es el más grande motor de prevención basado en la nube que utiliza el aprendizaje automático y la inteligencia colectiva para proteger a las empresas contra las amenazas desconocidas basadas en archivos, 60 veces más rápido que el competidor más cercano.

CONCLUSIONES CLAVE

- 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. Cuando se garantiza que las soluciones con prevención de host realicen análisis locales y remotos de dichos tipos de archivos se ofrece protección adicional en el endpoint.

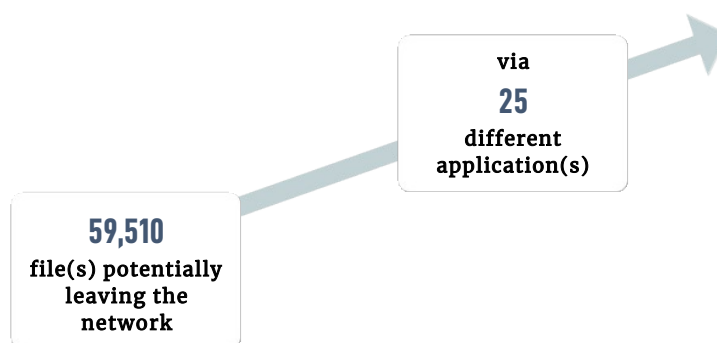
TIPOS DE ARCHIVOS DE ALTO RIESGO

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.



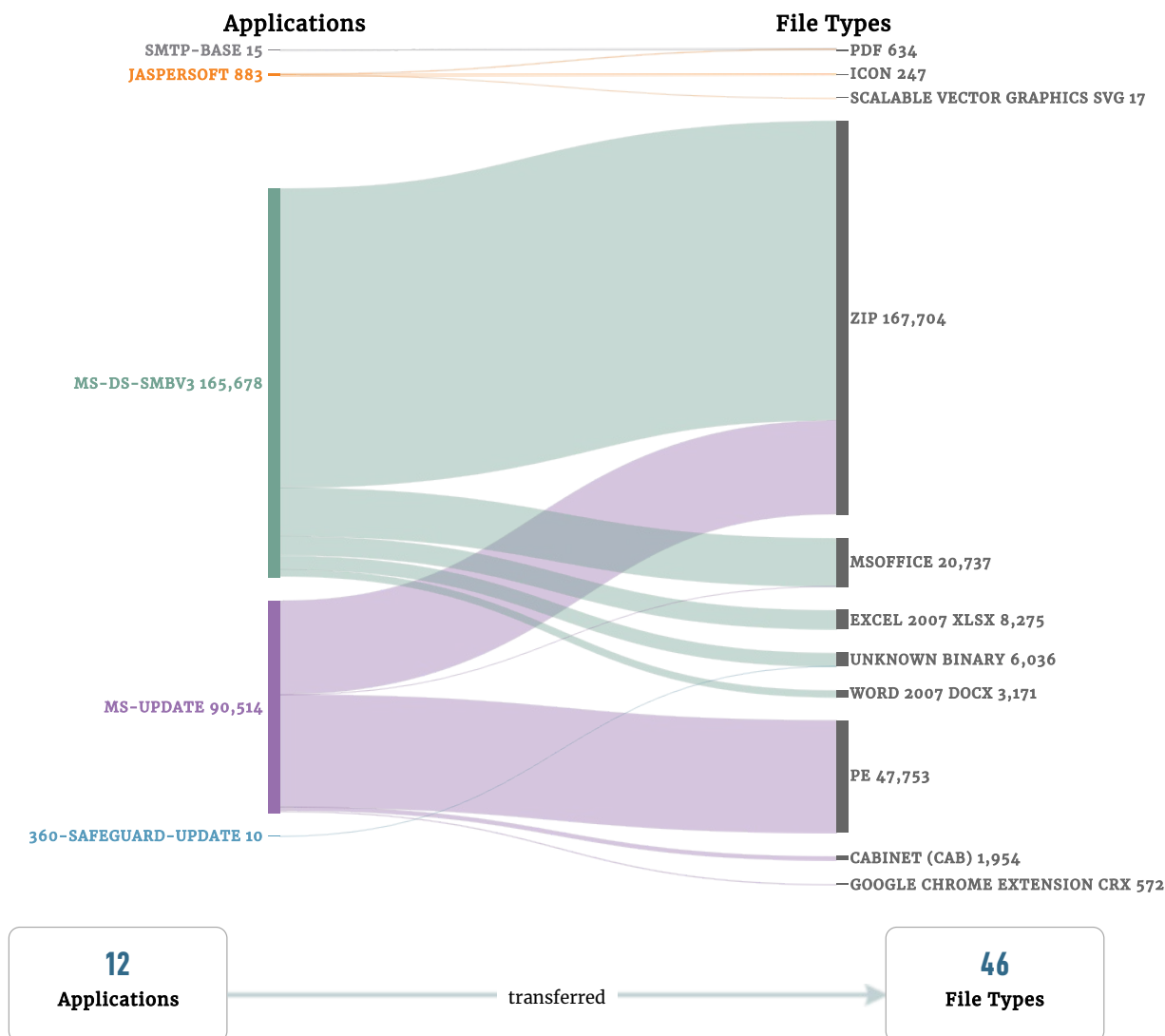
ARCHIVOS QUE PODRÍAN SALIR DE LA RED

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 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 **186** archivos en total entre **46** tipos de archivos diferentes, que se enviaron a través de un total de **12** 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.



Resumen: CREMIL - Caja de Retiro de las Fuerzas Militares

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 **CREMIL - Caja de Retiro de las Fuerzas Militares**, 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.

ASPECTOS DESTACADOS:

- Se observaron aplicaciones de alto riesgo como **file-sharing, email, y photo-video** en la red, las cuales deben ser investigadas debido a la posibilidad de abuso.
- Se observaron **185** aplicaciones en total en la red en **31**, a diferencia del promedio de **154** aplicaciones en total para el sector que se observó en otras organizaciones de **Government - County**.
- Se observaron **1,447,039** vulnerabilidades en total y las tres categorías más importantes son **ssl, active-directory-base, y ms-ds-smbv3**.
- Se observaron **0** eventos de malware, frente a un promedio del sector de **3,345** para su grupo del peer.
- Se usaron **1** aplicaciones en total para la comunicación de mando y control.

CONCLUSIONES CLAVE

185

APLICACIONES EN USO

28

APLICACIONES DE ALTO RIESGO

61

APLICACIONES SAAS

1,447,039

EXPLOITS DE VULNERABILIDAD

1,447,043

AMENAZAS TOTALES

29

SOLICITUDES MALINTENCIONADAS
SOLICITUDES MALINTENCIONADAS: 29

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.
- Ocúpese de la comunicación de comando y control a través del análisis de la red o del origen del host. Las soluciones de detección y respuesta, o las de registros, pueden ofrecer datos sobre lo que pasó.
- 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.