DARKNETSEARCH
BY KADUU

Informe de Superficie de Ataque

acmesample.com

Superficie de ataque observada: 2026-09-02 21:04 UTC

Informe generado: 2026-09-17 07:29 UTC

INFORME DE MUESTRA — IDENTIFICADORES ANONIMIZADOS

Resumen Ejecutivo

Perfil objetivo

Dominio	acmesample.com
Organización	Acme Sample GmbH
Tipo	Empresa Privada
Industria	Manufactura industrial
Tamaño	501-1000 empleados
Sede	Ciudad Muestra, Estados Unidos
Operando En	Estados Unidos, Canadá

Acme Sample GmbH, una empresa privada de América del Norte en la industria de Fabricación Industrial, enfrenta una presión moderada de targeting cibernético. El sector de fabricación industrial es cada vez más objetivo de amenazas cibernéticas, particularmente ransomware y ataques a la cadena de suministro, debido a su dependencia de la tecnología y cadenas de suministro complejas. Operar en Canadá y los Estados Unidos, ambos objetivos frecuentes del cibercrimen, aumenta aún más el riesgo. Con un tamaño de empresa de 501-1,000 empleados, Acme Sample GmbH es un objetivo viable para los cibercriminales que buscan ganancias financieras a través de ransomware y otras amenazas cibernéticas.

Acerca de este informe

Este informe proporciona una visión desde la perspectiva de un hacker de la superficie de ataque de su organización, basada en métodos de reconocimiento pasivo. Al agregar datos de múltiples fuentes de inteligencia, refleja cómo un atacante podría identificar activos expuestos, servicios y riesgos potenciales — sin realizar ningún escaneo intrusivo.

El dominio del sitio web escaneado **acmesample.com** utiliza un dominio diferente para el correo electrónico de los empleados: **acmesample.com, acmesample.net**. Las búsquedas de filtraciones de credenciales cubrieron todos los dominios de correo electrónico identificados.

Comparación de Huella de Infraestructura

DOMINIO	EST. SUBDOMINIOS
acmesample.com (dominio de entrada inicial)	~54
acmesample.net	~1

Estructura del informe

Este informe está organizado en cinco capítulos principales, cada uno cubriendo una dimensión distinta de la superficie de ataque:

CAPÍTULO	ENFOQUE	PÁGINA
Network	Rangos de IP, vecinos de red, alojamiento, distribución geográfica	**15**
Aplicaciones	Stack tecnológico, seguridad de DNS y correo electrónico, vulnerabilidades, TLS, seguridad de aplicaciones web	**53**
Infraestructura	Puertos, subdominios, superficie de autenticación, riesgo de software, paneles de administración, exposición	**75**
People	Credenciales, contenido de filtración, enumeración de correos electrónicos, huella digital VIP	**19**
Paisaje de Amenazas	reputación IP, exposición de código, Telegram/Discord/paste, redes sociales, typosquatting	**91**

RESUMEN DE PUNTUACIONES DE SEGURIDAD CLAVE

55 / 100

POSTURA DE SEGURIDAD

ACEPTABLE

Composición en 12 áreas de evaluación. Más alto es mejor.

5.8 / 10

RIESGO OPERACIONAL

ELEVADO

Sensible a hallazgos críticos activos. Impulsado por hosts en el peor de los casos y condiciones urgentes.

Este informe de Monitoreo de Superficie de Ataque para Acme Sample GmbH abarca un análisis exhaustivo de la huella digital de la organización, centrándose en un total de 54 hosts y un puntaje de postura de riesgo de **55/100** (ACEPTABLE) con un nivel de Riesgo Operacional de **5.8/10** (ELEVADO). La metodología empleada consistió en escanear en busca de vulnerabilidades, filtraciones de credenciales y exposiciones en diversas plataformas, incluidos servicios en la nube y redes sociales.

Los hallazgos clave revelan riesgos significativos, incluyendo **26 filtraciones de credenciales** y **11 archivos expuestos en la nube**, que representan una amenaza para datos sensibles. Además, se ha identificado a la organización con **372 dominios de typosquatting** con registros DNS activos, y el puntaje de postura de seguridad de la aplicación web se sitúa en **74**, con **3 problemas de alta gravedad** detectados.

Para mitigar estos riesgos, se recomienda que Acme Sample GmbH realice una revisión exhaustiva de sus configuraciones en la nube e implemente controles de acceso más robustos para abordar las filtraciones de credenciales identificadas. Además, se aconseja un escaneo dedicado del dominio de correo electrónico **acmesample.net** debido a la discrepancia con el dominio del sitio web principal. Las acciones inmediatas también deben incluir el fortalecimiento de las medidas de seguridad de la aplicación web para rectificar las vulnerabilidades de alta gravedad.

Hallazgos Clave

- Se identificaron **26 filtraciones de credenciales** en diversas plataformas.
- Se detectaron **11 archivos expuestos en la nube** que requieren atención inmediata.
- Se encontraron **372 dominios de typosquatting** con registros DNS activos que representan amenazas potenciales de phishing.
- Puntaje de seguridad de la aplicación web de **74** con **3 vulnerabilidades de alta gravedad** registradas.
- Nivel de Riesgo Operacional categorizado como **5.8/10** (ELEVADO), lo que requiere acciones de gestión de riesgos inmediatas.

DETALLES DE PUNTUACIONES DE SEGURIDAD

Escala: **0 = máxima exposición / peor**, **100 = mejor postura** — mayor es mejor para cada categoría a continuación (por ejemplo, una puntuación de Exposición de Personas de 0/100 significa que la organización está maximamente expuesta, no que no se encontró nada).

0 — **EXPOSICIÓN DE PERSONAS** — CRÍTICO
1 empleado con exposición de registro de ladrón
Peso: 10%

50 — **PROTECCIÓN DE MARCA** — POBRE
362 typosquats con servidores web activos
Peso: 4%

53 — **VULNERABILIDADES** — POBRE
67 CVEs críticos/altos no verificados (coincidencia de producto)
Peso: 20%

64 — **RED** — ACEPTABLE
3 hosts con servicios de alto riesgo, 5 hosts de puerto inusual
Peso: 11%

70 — **CREDENCIALES** — ACEPTABLE
9 buzones de riesgo crítico
Peso: 20%

74 — **SEGURIDAD DE APLICACIONES WEB** — ACEPTABLE
3 problemas de seguridad web de alta gravedad
Peso: 10%

76 — **DNS Y CORREO ELECTRÓNICO** — BUENO
No hay problemas críticos de DNS/ correo electrónico
Peso: 10%

79 — **EXPOSICIÓN DEL ACTOR DE AMENAZA** — BUENO
Presión moderada de targeting sectorial
Peso: 5%

80 — **REDES SOCIALES** — BUENO
1 riesgo de suplantación encontrado
Peso: 3%

82 — **INFRAESTRUCTURA** — BUENO
1 punto final de autenticación detectado
Peso: 5%

90 — **EXPOSICIÓN EN CANALES DE HACKERS** — EXCELENTE
No se detectaron menciones de canales de hackers / sitios de paste
Peso: 5%

91 — **TLS / SSL** — EXCELENTE
2 hosts de protocolo débil
Peso: 10%

GUARDRAILS DE PUNTUACIÓN DE POSTURA ACTIVOS

55 **Riesgo Compuesto:** 8 hosts con riesgo compuesto ≥ 8.0

CÓMO SE CALCULA ESTA PUNTUACIÓN

CATEGORÍA	PESO	PUNTUACIÓN	CONTRIBUCIÓN
DNS y correo electrónico	10%	76 / 100	7.6 pts
TLS / SSL	10%	91 / 100	9.1 pts
Vulnerabilidades	20%	53 / 100	10.6 pts
Credenciales	20%	70 / 100	14.0 pts
Red	11%	64 / 100	7.0 pts
Infraestructura	5%	82 / 100	4,1 pts
Protección de marca	4%	50 / 100	2,0 pts
Exposición de Personas	10%	0 / 100	0,0 pts
Redes Sociales	3%	80 / 100	2.4 pts
Exposición en canales de hackers	5%	90 / 100	4.5 pts
Seguridad de Aplicaciones Web	10%	74 / 100	7,4 pts
Exposición del actor de amenaza	5%	79 / 100	4.0 pts

Metodología de puntuación: Cada categoría utiliza escalado logarítmico (no conteos brutos) con multiplicadores de prevalencia: los problemas generalizados en muchos hosts se penalizan más que los hallazgos aislados. El modelo de vulnerabilidad heredado separa los hallazgos verificados de los indicadores pasivos/ajustados al producto, pero no aplica los multiplicadores de contribución de nivel de evidencia DS-90. Los multiplicadores de prevalencia de hasta 1.75× aún se aplican donde se admite. Los hosts críticos para el negocio (puntos finales de autenticación, paneles de administración) amplifican el riesgo a través de la correlación entre módulos. La Puntuación de Postura es un promedio ponderado con límites de guardia que evitan una puntuación general engañosamente buena cuando cualquier área única está críticamente comprometida. La Puntuación de Riesgo Operacional se basa en el riesgo compuesto de los hosts: hosts donde múltiples factores de riesgo se superponen (por ejemplo, panel de administración + TLS débil + credenciales filtradas). (Modelo de puntuación: heredado.)

HALLAZGOS MÁS IMPORTANTES

6

MAYOR RIESGO DE ACTIVO

6 / 10

Peor host único en este escaneo (0 = más bajo).

INSTANCIAS DE CVE

245

De Shodan, Netlas, ZoomEye y CVEDB

HALLAZGOS DE VERIFICACIÓN

2

Accionable · +397 informativo

POSTURA DE SEGURIDAD (DE UN VISTAZO)

CVE references are derived from **análisis de banners de servicio** (Shodan, Netlas, ZoomEye) and **coincidencia de versión del producto** (CVEDB). These are indicators based on detected software versions — not confirmed exploits. Prioritize by severity, exposure, and business context; see the full Vulnerability Assessment section for confidence tiers.

ALCANCE Y HUELLA

SUBDOMINIOS ENCONTRADOS
54
FQDNs únicos descubiertos

HOSTS ACTIVOS
25
Resuelto a una IP

RANGOS DE IP
0
Bloques de red propiedad (RIR)

PUERTOS ABIERTOS (HOSTS)
22
Pasivo + Nmap confirmado

NOMBRES DE HOST SENSIBLES
9
Subdominios señalados

HOSTS CON SEÑALES DE VULNERABILIDAD
10
Cualquier señal relacionada con CVE

DURACIÓN DEL ESCANEO
91 min
Tiempo de espera de pipeline

HOSTS LIMPIOS
6
Hosts activos, puntuación de riesgo 0

INTELIGENCIA DE AMENAZAS

CREDENCIALES FILTRADAS
26
Cuentas de empleados en servicios externos

REGISTROS DE BRECHA DB
2,038
Menciones de dominio (coincidencia de subcadena)

EXPOSICIONES EN LA NUBE
11
7 archivos sensibles

URLS ACORTADAS
3,000
0 recursos internos

REDES SOCIALES
192
1 riesgo de suplantación

EXPOSICIÓN DE CORREO ELECTRÓNICO
498
14 críticas, 61 alto riesgo

EXPOSICIÓN DE CÓDIGO
26
0 alto riesgo en GitHub/ Gists

TG / DISCORD / PASTE
0
0 crítico, 0 alto riesgo

SISTEMAS CRÍTICOS DE NEGOCIO
12
Funciones críticas expuestas a Internet

RUTAS DE ATAQUE
1
1 rutas de pivote total

SEGURIDAD DE INFRAESTRUCTURA Y APLICACIONES

PANELES DE ADMINISTRACIÓN
0
Interfaces de gestión expuestas

PROBLEMAS DE TLS
2
Cert / protocolo / cifrado

SEGURIDAD DE APLICACIONES WEB
74/100
3 alto, 3 medio

DOMINIOS DE TYPOSQUATTING
372
0 phishing detectado

PUNTOS FINALES DE AUTENTICACIÓN
1
SSO, VPN, paneles de firewall

ACTIVOS MÁS RIESGOSOS

Los siguientes sistemas representan el mayor riesgo compuesto basado en la correlación entre módulos. Cada host fue puntuado combinando factores de riesgo individuales — como paneles de administración expuestos, TLS débiles, credenciales filtradas y señales de vulnerabilidad — con multiplicadores de criticidad empresarial. Los sistemas donde múltiples factores de riesgo se superponen reciben puntuaciones exponencialmente más altas, ya que los atacantes pueden encadenar estas debilidades para un impacto máximo.

HOST	RIESGO	IMPACTO EN EL NEGOCIO	FACTORES DE RIESGO
asset-062.acmesample.com +1 alias en 192.0.2.178	10.0	Sistema de correo electrónico	13 CVEs críticos/altos, IP señalada, punto final de autenticación, 13 puertos abiertos
asset-166.acmesample.com	10.0	Sitio web / Expuesto al público	37 CVEs altos/críticos, IP marcada, punto final de autenticación
asset-143.acmesample.com +1 alias en 192.0.2.27	10.0	Sitio web / Público — debilidades de seguridad en el punto final de autenticación	32 CVEs críticos/altos, TLS débil, Aplicación web ALTA, Punto final de autenticación
www.acmesample.com +1 alias en 192.0.2.11	10.0	Sitio web / Público — debilidades de seguridad en el punto final de autenticación	5 CVEs críticos/altos, Aplicación web ALTA, Punto final de autenticación
asset-071.acmesample.com	8.8	Sitio web / Expuesto al público	13 CVEs de alta/crítica, IP señalada, 13 puertos abiertos
asset-141.acmesample.com	7.5	Infraestructura API	2 CVEs alto/crítico, subdominio sensible
portal.acmesample.com	6.0	Portal del Cliente	Punto final de autenticación
asset-142.acmesample.com	5.0	Infraestructura API	2 CVEs altos/críticos
asset-064.acmesample.com	1.8	CRM / ERP	Punto final de autenticación, Subdominio sensible
asset-055.acmesample.com	1.2	Sistema expuesto a Internet	Subdominio sensible

EMPLEADOS MÁS RIESGOSOS

Personal de gestión de alto valor con la mayor exposición basada en inteligencia VIP (registros de filtración, contraseñas filtradas, detecciones de cuentas) y datos de enumeración de correos electrónicos. Estos individuos representan objetivos prioritarios para ataques de spear-phishing y basados en credenciales.

NOMBRE	POSICIÓN	RIESGO	FILTRA-CIONES	PWD	FACTORES DE RIESGO
Executive012 Sample012	Vicepresidente de Gestión de Productos	85	177	SÍ	177 filtraciones, Contraseñas filtradas, recuperación de MS, ID de Google encontrado
Executive035 Sample035	Director Senior de Cuentas Estratégicas	80	79	SÍ	79 filtraciones, Contraseñas filtradas, 1 cuentas en línea, recuperación de MS
Executive020 Sample020	Director Senior, Cuentas Nacionales	85	26	SÍ	26 filtraciones, Contraseñas filtradas, 1 cuentas en línea, recuperación de MS
Ejecutivo067 Sample067	Director Financiero	85	10	SÍ	10 filtraciones, Contraseñas filtradas, 4 cuentas en línea, recuperación de MS
Executive040 Sample040	Líder Técnico de TI	80	11	SÍ	11 filtraciones, Contraseñas filtradas, 5 cuentas en línea, recuperación de MS
Ejecutivo041 Sample041	Director Ejecutivo	95	8	—	8 filtraciones, 5 fuentes web
Ejecutivo036 Sample036	Vicepresidente de Distribución	80	8	—	8 filtraciones
Executive131 Sample131	Director de Recursos Humanos	80	7	—	7 filtraciones
Executive005 Sample005	Director de Cultura	80	6	—	6 filtraciones
Ejecutivo078 Sample078	Gerente de Marketing de Producto	70	6	—	6 filtraciones, 4 fuentes web

LAS 10 ACCIONES PRIORITARIAS

#	ACCIÓN	PERÍODO DE TIEMPO	CATEGORÍA
1	**Revisar y parchear CVEs en asset-166.acmesample.com** El Activo-166 tiene 37 CVEs críticos/altos que afectan su punto final de autenticación. Es necesaria una remediación inmediata para prevenir la explotación. **Afectado:** `asset-166.acmesample.com`	**Inmediato**	VULNERABILIDADES
2	**Revisar y parchear CVEs en asset-143.acmesample.com** El Activo-143 está marcado con 32 CVEs críticos/altos y tiene TLS débil en su punto final de autenticación. Se requiere acción inmediata para asegurar este activo. **Afectado:** `asset-143.acmesample.com`	**Inmediato**	VULNERABILIDADES
3	**Revisar y parchear CVEs en www.acmesample.com** El activo www.acmesample.com tiene 5 CVEs críticos/altos que impactan su punto final de autenticación. La remediación inmediata es crítica. **Afectado:** `www.acmesample.com`	**Inmediato**	VULNERABILIDADES
4	**Restringir la exposición del panel de administración en asset-062.acmesample.com** El Activo-062 está expuesto con 13 puertos abiertos y está marcado como un punto final de autenticación. Limite el acceso para reducir el riesgo. **Afectado:** `asset-062.acmesample.com`	**Esta semana**	RED
5	**Restringir puertos abiertos en asset-071.acmesample.com** El Activo-071 tiene 13 puertos abiertos y está marcado con CVEs críticos/altos. Es necesaria una restricción inmediata de puertos para mitigar riesgos. **Afectado:** `asset-071.acmesample.com`	**Esta semana**	RED
6	**Hacer cumplir la política de rechazo DMARC en acmesample.com** Implementar una política de rechazo DMARC ayudará a proteger contra el phishing y mejorar la postura general de seguridad del correo electrónico.	**Dentro de 30 días**	PROTECCIÓN DE MARCA
7	**Revisar 26 filtraciones de credenciales para acmesample.com** Se encontraron 26 buzones de empleados bajo acmesample.com en conjuntos de datos de filtraciones de terceros. Revise y rote las credenciales.	**Dentro de 30 días**	CREDENCIALES
8	**Revisar 372 dominios de typosquatting relacionados con acmesample.com** Hay 372 dominios de typosquat que podrían representar un riesgo para la integridad de la marca. Revise y tome las acciones necesarias.	**Dentro de 90 días**	PROTECCIÓN DE MARCA
9	**Evalúe 7 archivos sensibles en la nube por exposición** 7 archivos sensibles en almacenamiento en la nube pueden representar un riesgo. Realice una evaluación para asegurar controles de acceso adecuados.	**Dentro de 90 días**	INFRAESTRUCTURA
10	**Revise las vulnerabilidades de seguridad de la aplicación web** Aborde los problemas de seguridad de la aplicación web identificados, incluyendo protecciones faltantes como CSP y HSTS para mejorar la seguridad.	**Dentro de 90 días**	APLICACIÓN WEB

Metodología y Cobertura de Escaneo

DarknetSearch La enumeración de la Superficie de Ataque utiliza un **pipeline automatizado de 8 fases** para mapear la huella digital externa de una organización. Comenzando con el dominio objetivo, el sistema descubre, enriquece y analiza progresivamente cada activo accesible externamente, reflejando las mismas técnicas de reconocimiento utilizadas por atacantes del mundo real.

1
Análisis de objetivo
Resolver IP, línea base WHOIS/RDAP.

2
Descubrimiento de subdominios
Hasta 16 módulos pasivos de OSINT.

3
Mapa de infraestructura
rangos de RIR, misma-IP, WHOIS inverso.

4
Inteligencia pasiva
Shodan, Netlas, ZoomEye.

5 OPT-IN
Escaneo activo
Nmap en puertos descubiertos.

6
Análisis y correlación
Puntuaciones de riesgo, vecinos, CVEs.

7 OPT-IN
Verificación activa
Escaneo seguro de plantillas HTTP/SSL.

8
Generación de informes
Análisis, gráficos, renderización en PDF.

Fase 1 — Análisis de Objetivos

La canalización comienza resolviendo la dirección IP principal del dominio objetivo y consultando bases de datos de registro WHOIS/RDAP para identificar al propietario del dominio, registrador e historial de registro. Esto establece la identidad base para búsquedas posteriores.

Fase 2 — Descubrimiento de Subdominios

Hasta 16 módulos pasivos de OSINT se ejecutan en paralelo — consultando registros de transparencia de certificados (crt.sh, Kaduu CT Monitor), índices de motores de búsqueda (Shodan, ZoomEye, Google a través de SERPHouse/ScrapingBee), bases de datos de DNS pasivo (RapidDNS, DNSDumpster, SubdomainCenter, HackerTarget), historial de archivos web (Wayback Machine), filtraciones de credenciales en la darknet (Kaduu), scraping de navegador sin cabeza (Netcraft), y el sitio web objetivo a través de un rastreador web BFS concurrente. Cuando se habilita la enumeración activa de DNS, un módulo de fuerza bruta de DNS prueba 5,000 prefijos de subdominio comunes.

Fase 3 — Mapeo de Infraestructura

Cuatro fuentes de búsqueda inversa de IP identifican dominios que comparten la IP del objetivo. Las API REST de RIR (RIPE, ARIN) descubren todos los rangos de IP registrados a la organización objetivo. Un pipeline mejorado por GPT identifica la empresa, genera nombres de búsqueda normalizados y adjudica qué registros de RIR pertenecen al objetivo. Las búsquedas inversas de WHOIS encuentran todos los dominios registrados por la misma entidad.

Fase 4 — Inteligencia Pasiva

Para cada host descubierto, el sistema consulta Shodan, Netlas y ZoomEye en busca de puertos abiertos, banners de servicio, certificados SSL, identificadores CPE y vulnerabilidades conocidas — sin tocar la infraestructura del objetivo. Los resultados se almacenan en caché durante 7 días por IP para optimizar el uso de la API.

Fase 5 — Escaneo Activo (opt-in)

Cuando está habilitado, Nmap realiza un escaneo TCP dirigido con detección de versión (-sV) y scripts NSE (vulners para búsqueda de CVE, ssl-enum-ciphers para auditoría de TLS) en puertos descubiertos pasivamente. Si no se conocen puertos, se ejecuta un escaneo rápido de los 100 principales puertos TCP en su lugar.

Fase 6 — Análisis y Correlación

El análisis del vecindario de red examina IPs adyacentes en busca de coincidencias de certificados SSL, patrones PTR, comparación de ASN y huellas digitales HTTP. Las CVE se agregan de 5 fuentes y se verifican cruzadamente contra los banners de servicio de Nmap. Los puntajes de riesgo (0–10) se calculan por host en función de vulnerabilidades, puertos inusuales y patrones de nombres de host sensibles.

Fase 7 — Verificación de seguridad activa (opt-in)

Cuando está habilitado, un motor de verificación de seguridad automatizado escanea todos los hosts descubiertos con puntos finales HTTP/HTTPS activos utilizando **4,000+ plantillas de detección seguras curadas**. Estas plantillas utilizan solo solicitudes GET/HEAD (sin explotación ni inyección de carga) para detectar paneles de administración expuestos, configuraciones de seguridad incorrectas, exposiciones de archivos sensibles, software obsoleto y indicadores de CVE conocidos. Además, se realizan verificaciones de SSL/TLS, DNS y nivel de red contra todos los hosts con puertos clasificados. Solo se prueban los hosts con puertos abiertos; el motor primero sondea cada URL para verificar su actividad antes de escanear.

Fase 8 — Generación de Informe

Todos los resultados del escaneo están deduplicados y consolidados. Los contadores de enriquecimiento están materializados, se detectaron entradas DNS comodín y se finalizaron las puntuaciones de riesgo. La tubería de generación de informes luego recopila todos los datos de la base de datos, realiza un análisis determinista (distribución de riesgo, frecuencia de puerto/servicio, pila tecnológica, paisaje CVE, propiedad de red), genera gráficos a través de matplotlib, obtiene un resumen ejecutivo potenciado por GPT, geolocaliza todas las IP resueltas y renderiza el PDF final usando WeasyPrint. La evidencia detallada en CSV se omite de esta muestra pública.

Resumen del módulo

56 módulos completados, **0** fallidos, **5** omitidos. Desglose completo por módulo disponible en `conjunto de datos de evidencia privada` omitido de esta muestra pública.

Módulos no completados

Los siguientes módulos fallaron o fueron omitidos. Sus hallazgos pueden estar ausentes de este informe; un conteo cero no debe interpretarse como un resultado limpio.

MÓDULO	ESTADO	DIAGNÓSTICO
descubrimiento_de_rango_ip	Omitido	domain_mode=default (scoped) — descubrimiento de dominios adicionales desactivado
reverse_dns	Omitido	Deshabilitado por bandera de función
whois inverso	Omitido	domain_mode=default (scoped) — descubrimiento de dominios adicionales desactivado
same_ip_domains	Omitido	domain_mode=default (scoped) — descubrimiento de dominios adicionales desactivado
hackertarget_same_ns	Omitido	domain_mode=default (scoped) — same-NS apex discovery off

Descripción de la Superficie de Ataque

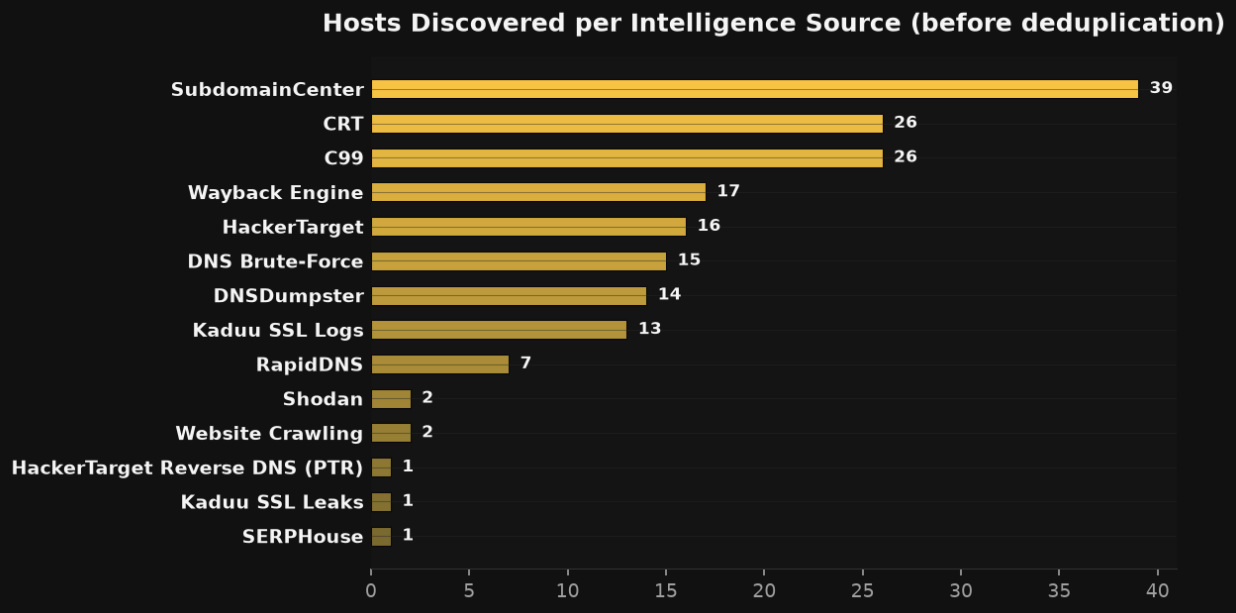
La superficie de ataque representa todos los hosts, servicios y activos digitales accesibles externamente asociados con **acmesample.com**. Los hosts fueron descubiertos a través de fuentes de inteligencia pasiva (transparencia de certificados, bases de datos DNS, motores de búsqueda, credenciales filtradas) y opcionalmente confirmados a través de escaneo activo (Nmap, verificación activa).

Nombres de Host Sensibles son nombres de host que contienen patrones que sugieren sistemas de alto valor o internos — como admin, dev, staging, vpn, jenkins, grafana, o backup. Estos sistemas son a menudo los primeros objetivos en ataques del mundo real. **Puertos Inusuales** son puertos TCP/UDP abiertos fuera del conjunto estándar de servicios comunes de internet (HTTP, HTTPS, SSH, DNS, SMTP, FTP). Su presencia puede indicar servidores de desarrollo, interfaces de gestión, aplicaciones heredadas o servicios mal configurados.

54	54	9	5
SUBDOMINIOS ENCONTRADOS	PROPIEDAD DEL CLIENTE	NOMBRES DE HOST SENSIBLES	PUERTOS INUSUALES

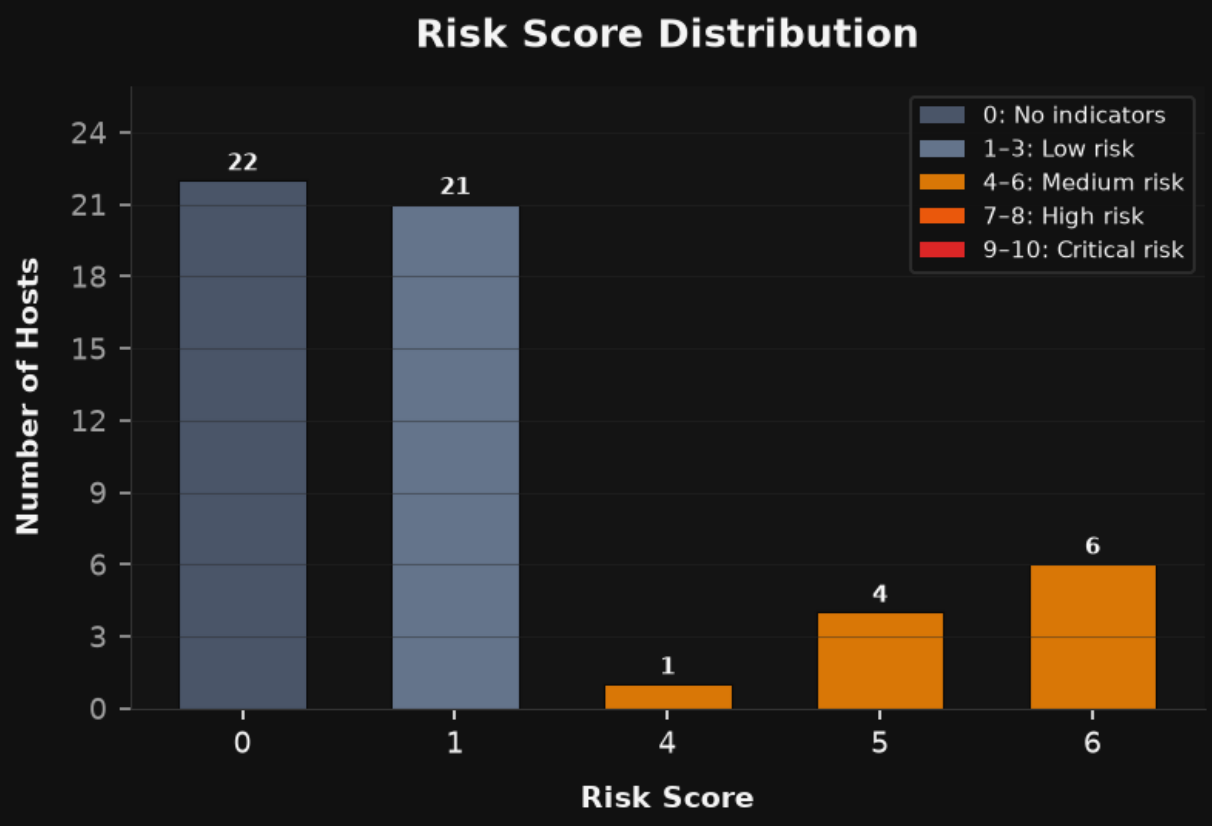
Fuentes de descubrimiento (antes de la deduplicación)

Las barras utilizan una **rampa de oro única** por rango — más fácil de leer que muchos colores no relacionados. Cada barra cuenta los hosts contribuidos por esa fuente (los hosts pueden aparecer en múltiples fuentes).



Distribución de puntuaciones de riesgo

Puntuaciones de 0 a 10 basadas en señales de CVE, puertos inusuales, conteo de puertos y patrones de nombres de host sensibles. La leyenda del gráfico coincide con los colores de las barras.



RED

Rangos de IP Propiedad de la Organización

El descubrimiento de rangos de IP identifica todos los bloques de red registrados a la organización objetivo a través de Registros Regionales de Internet (RIPE para Europa/Medio Oriente, ARIN para América del Norte). Un pipeline mejorado por GPT identifica la empresa detrás del dominio, genera variantes de nombres de búsqueda (incluyendo formas con ASCII doblado y sin sufijos legales) y valida qué registros de RIR pertenecen al objetivo. Los rangos grandes (>/24, 256+ hosts) se enumeran solo como informativos.

Importante: Este análisis identifica qué bloques de red pertenecen a la organización basado en datos de registro de RIR. **No se escanearon, enumeraron ni sondearon hosts dentro de estos rangos.** Los rangos proporcionan contexto sobre el patrimonio de IP registrado de la organización — cualquier evaluación de seguridad de hosts individuales dentro de estos rangos requeriría un escaneo dirigido separado.

No se encontraron rangos de IP registrados

La búsqueda RIR (RIPE, ARIN) no identificó ningún rango de IP directamente registrado a esta organización. Esto generalmente significa que la organización utiliza infraestructura compartida o alojada en la nube (por ejemplo, AWS, Azure, Cloudflare) en lugar de poseer bloques de IP dedicados. Esto es común para organizaciones pequeñas y medianas y no indica un problema de seguridad; sin embargo, significa que no hay patrimonio adicional de IP para auditar más allá de los hosts descubiertos a través de la enumeración de subdominios.

Análisis de Vecinos de Red

Para cada IP descubierta, el sistema examina direcciones vecinas en la misma subred /24. Los vecinos se evalúan a través de la coincidencia de certificados SSL (comparación de CN/SAN), patrones de registros PTR, comparación de ASN y huellas digitales de contenido HTTP. Cada vecino recibe una puntuación de confianza: **CONFIRMADO** (la IP se encuentra dentro de un rango de IP de cliente registrado), **ALTO** (2+ señales fuertes como coincidencia de certificado o ASN), **MEDIO** (1 señal fuerte), **BAJO** (solo señales débiles).

Importante: Las direcciones IP vecinas solo fueron huelladas utilizando técnicas pasivas (inspección de certificados, búsqueda PTR, encabezados HTTP). **No se realizó escaneo activo, pruebas de penetración ni evaluación de vulnerabilidades en ninguna IP vecina.**

Analizados **20** vecindarios IP — **8** coincidencias de certificados SSL, **2** coincidencias de huellas dactilares HTTP, **0** confirmados como propiedad por RDAP. La evidencia completa de vecinos se omite de esta muestra pública.

Hallazgos de muestra

IP OBJETIVO	IP VECINA	CONFIANZA	SEÑALES COINCIDENTES
192.0.2.182	192.0.2.183	MEDIO	Coincidencia de Ptr, misma subred
192.0.2.184	192.0.2.183	MEDIO	Coincidencia de Ptr, misma subred

Por qué importan las IPs vecinas

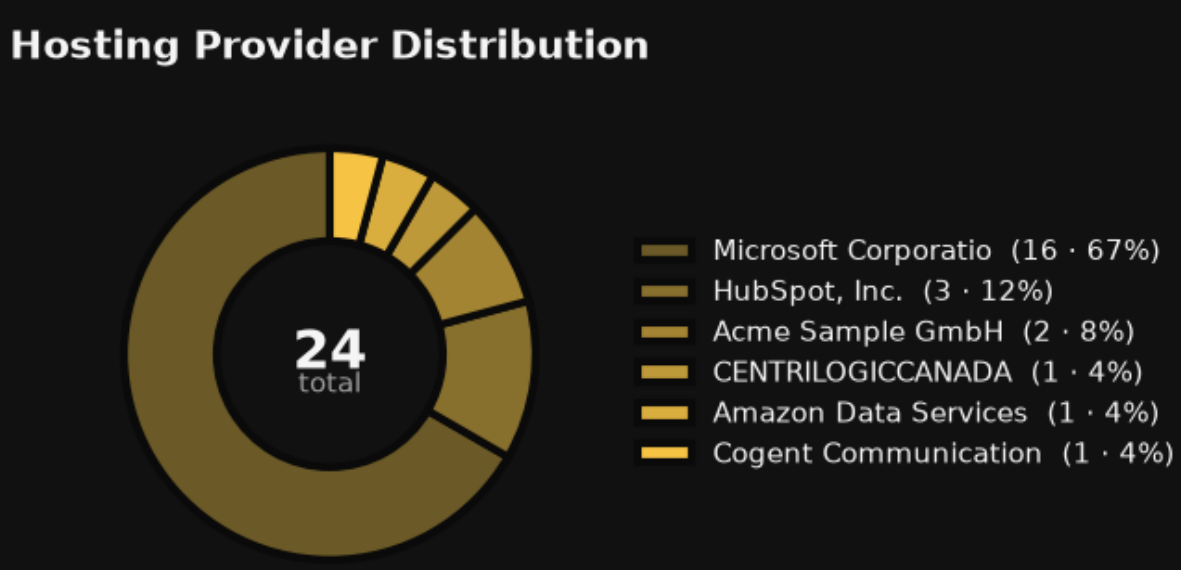
Si el análisis anterior identificó direcciones IP vecinas con **confianza media** o **alta** de pertenecer a su organización, estos hosts no fueron incluidos en el alcance del escaneo activo y no han sido probados en busca de vulnerabilidades. Sin embargo, un atacante que realice reconocimiento también descubriría estos vecinos y podría investigarlos o atacarlos para obtener un punto de apoyo en su red. Recomendamos verificar la propiedad de los vecinos de alta confianza e incluirlos en futuras evaluaciones de seguridad.

Proveedores de Hosting y Distribución

La distribución del proveedor de hosting revela la diversidad de infraestructura de la superficie de ataque de la organización. Una huella de hosting concentrada (pocos proveedores) simplifica la monitorización de seguridad pero crea puntos únicos de fallo. Una huella altamente distribuida aumenta la complejidad de gestión y el riesgo de desviación de configuración entre proveedores.

Evaluación: 6 proveedores — complejidad de gestión moderada.

Distribución



Principales proveedores

Microsoft Corporation	16
HubSpot, Inc.	3
Acme Sample GmbH	2
CENTRILOGICCANADA	1
Amazon Data Services Canada	1
Cogent Communications, LLC	1

Evaluación de Riesgos

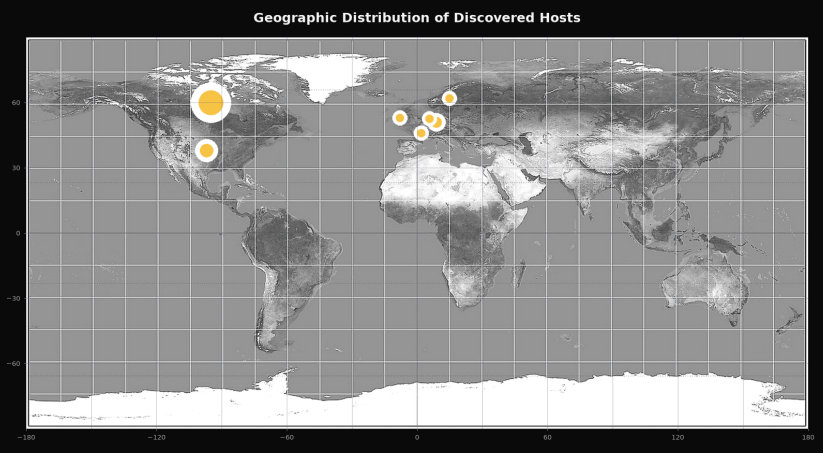
La organización depende en gran medida de la infraestructura de terceros, con un 66.7% de su infraestructura alojada por Microsoft Corporation, lo que indica un riesgo de concentración significativo. Dado que más del 70% de sus hosts están en un único proveedor externo, una única interrupción regional podría afectar gravemente todos los servicios. El veredicto de resiliencia es preocupante debido a esta falta de diversidad de proveedores. La organización debería implementar una estrategia de múltiples proveedores para mitigar los riesgos asociados con la dependencia de un único proveedor, asegurando que los servicios críticos permanezcan operativos durante las interrupciones.

PROVEEDOR	HOSTS
Microsoft Corporation	16
HubSpot, Inc.	3
Acme Sample GmbH	2
CENTRILOGICCANADA	1
Amazon Data Services Canada	1
Cogent Communications, LLC	1

Distribución geográfica

La geolocalización IP muestra dónde están asignados los hosts descubiertos (típicamente con precisión de ciudad/región). Una amplia dispersión puede indicar CDN, nube multi-región o jurisdicciones inesperadas.

Nota: El mapa utiliza una proyección **equirectangular** (WGS-84). La **posición** de la burbuja es el centroide estándar del mapa de cada país (ISO); el **tamaño** refleja el conteo de hosts según la geolocalización. La leyenda enumera cada país con hosts.



CA	Canadá	12
EE. UU.	Estados Uni…	3
DE	Alemania	2
IE	Irlanda	1
SE	Suecia	1
FR	Francia	1
NL	Países Bajos	1

La posición de la burbuja = centroide del país ISO (plano cartesiano); el tamaño de la burbuja ∝ hosts geolocalizados a ese país. Los códigos de país coinciden con la leyenda. Mapa base: proyección equirectangular (Wikimedia Commons, CC BY-SA).

PERSONAS

Exposición de Credenciales Filtradas

70
ACEPTABLE

Análisis de la exposición de credenciales corporativas a través de bases de datos de filtraciones y agregadores de registros de robos. Identifica cuentas de empleados comprometidas en servicios externos.

Validez de Datos de Credenciales Filtradas

Los actores de amenaza a menudo reciclan datos antiguos en lo que se llaman "listas combinadas", y los datos de filtración pueden estar a veces meses o incluso años detrás del incidente original. Basado en nuestra experiencia, menos del ~2% de las credenciales filtradas que indexamos siguen siendo válidas. Dicho esto, incluso un número muy pequeño de credenciales funcionales puede presentar un riesgo real. Prevenir una filtración puede depender de solo una cuenta comprometida de cientos.
También es importante diferenciar entre fuentes de datos: la búsqueda en la base de datos utilizada en este informe se centra en datos filtrados que ya se han compartido públicamente (a menudo de forma gratuita), mientras que los actores de amenaza suelen intentar vender primero datos frescos. Estos datos más recientes y de mayor valor generalmente se encuentran a través de búsquedas en foros de hackers activos (no parte de este informe).
Más allá de la validez de las credenciales, los datos históricos aún proporcionan información de seguridad significativa. Por ejemplo, ayuda a identificar patrones de reutilización de contraseñas en diferentes servicios, un habilitador clave de ataques de relleno de credenciales, o casos donde las cuentas de correo electrónico corporativas se utilizan en plataformas privadas. Estos tipos de hallazgos son particularmente útiles para la capacitación de concienciación dirigida y el fortalecimiento de las prácticas de seguridad internas.

Búsqueda de Credenciales Multi-Dominio

La organización utiliza múltiples dominios de correo electrónico. Se buscaron credenciales en todos los dominios identificados:

DOMINIO	FILTRACIONES DE EMPLEADOS	REGISTROS DE FILTRACIÓN DB	CORREOS ELECTRÓNICOS ÚNICOS
@acmesample.com	26	2,036	15
@acmesample.net	0	2	0

Resumen

Dominio del sitio web buscado (acmesample.com) y dominio(s) de correo electrónico (acmesample.net). @acmesample.com: 26 filtraciones de empleados, 2,036 registros en la base de datos de filtraciones. @acmesample.net: 0 filtraciones de empleados, 2 registros en la base de datos de filtraciones. Se encontraron 2,038 registros de cuentas filtradas en bases de datos de filtraciones. Se detectaron 26 exposiciones de credenciales de empleados en 15 direcciones de correo electrónico únicas. 17 están clasificadas como de alto o crítico riesgo (contraseñas en texto plano presentes en servicios externos).

26
REGISTROS DE CREDENCIALES DE EMPLEADOS
pares de inicio de sesión + contraseña

388
BUZONES DERIVADOS DE FILTRACIONES
unión de filtraciones canónica

2,038
REGISTROS DE FILTRACIÓN DB
menciones de dominio

17
RIESGO ALTO/ CRÍTICO
registros de credenciales

Entendiendo los números

Registros de Credenciales de Empleados cuenta filas de credenciales distintas (login + pares de contraseña/hash) después de que avistamientos idénticos de múltiples fuentes de filtración son colapsados. **Buzones Derivados de Filtraciones** deduplica evidencia de filtración en direcciones distintas y une en cualquier buzón adicional `@acmesample.com` visto a través de la base de datos de filtraciones en vivo (escanado en su totalidad), muestras de contenido de filtración, y fuentes públicas de Hunter.io. Desglose de la fuente (ANTES de la deduplicación): 15 de credenciales, 383 de búsqueda de filtraciones en vivo, 384 de muestras de contenido de filtración, 0 de Hunter.io. **Registros de DB de Filtraciones** cuenta cada documento de filtración (archivos de registro, volcado de bases de datos, contenido pegado) que menciona el dominio en cualquier campo — una medida mucho más amplia que frecuentemente excede el conteo de registros de credenciales por órdenes de magnitud porque un archivo filtrado puede contener miles de líneas mencionando el dominio.

Cómo se relacionan "17 hallazgos críticos" con los 388 buzones derivados de filtraciones: la cantidad de Riesgo Alto/Crítico es el número de registros de credenciales calificados como críticos por la fuente y el modelo de riesgo — típicamente evidencia reciente de stealer-log o en texto plano. La validez de la contraseña no fue probada. El mismo buzón puede tener más de un registro de credencial crítica distinta, por lo que este conteo de registros puede exceder el conteo de buzones.

***Nota sobre la evidencia de la filtración:** Estas cifras reflejan bases de datos históricas de filtraciones y agregadores de registros de robos. Las observaciones idénticas se deduplican, pero diferentes credenciales para un buzón permanecen separadas. La presencia en un feed no establece que una cuenta o contraseña sea actualmente válida.

Registros sin procesar vs. Registros deduplicados

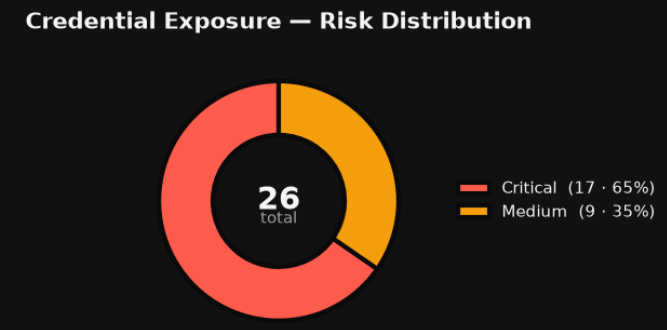
En todas las búsquedas de dominios en alcance, los feeds de filtraciones devolvieron **129** registros de credenciales en bruto. Después de deduplicar el mismo par de buzón/contraseña filtrado que resurgió por búsquedas de dominios superpuestos y múltiples listas combinadas, esto se reduce a **26** registros distintos (103 registros duplicados eliminados). Los resultados y la puntuación utilizan la cifra deduplicada; el subtotal en bruto se muestra aquí para la reconciliación con los conteos de feeds ascendentes. Estos registros abarcan **75** fuentes de filtración distintas.

Ventana de exposición (edad del registro)

Los datos de filtración son históricos: la presencia de un registro no significa que la contraseña siga siendo válida. La distribución a continuación agrupa cada registro fechado según cuánto tiempo ha pasado desde que se vio por primera vez, por lo que el informe muestra una ventana de exposición en lugar de implicar que cada filtración es actual:

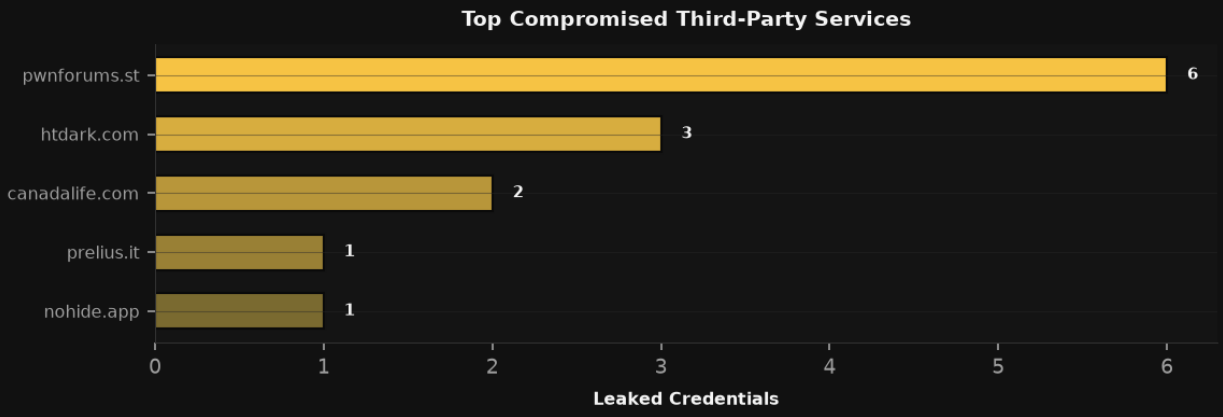
EDAD DE PRIMERA APARICIÓN	REGISTROS
Últimos 90 días	8
90 días – 1 año	18

Este gráfico muestra **registros de credenciales distintos** de la API de búsqueda de contenido de filtración — cada registro representa una combinación distinta de correo electrónico + contraseña redactada sensible a mayúsculas + servidor. El feed devolvió 129 avistamientos en bruto; 103 avistamientos duplicados de fuentes de filtración fueron eliminados antes de graficar.



SERVICIOS DE TERCEROS COMPROMETIDOS PRINCIPALES

Estas son plataformas **de terceros** (no propiedad de la organización) donde se encontraron credenciales de empleados en bases de datos de filtraciones y registros de stealer. Esto no significa que estas plataformas hayan sido comprometidas; más bien, los empleados utilizaron su correo electrónico corporativo para registrarse en estos servicios, y esas credenciales fueron expuestas posteriormente en filtraciones de datos de terceros. Los puntos de inicio de sesión pertenecientes a los propios dominios de la organización se enumeran por separado a continuación.



Detalles de Exposición de Credenciales (Redactados)

Mostrando 20 de 26 registros (balanceado — máximo 3 filas por dirección de correo electrónico para que la tabla muestre usuarios afectados distintos en lugar de repetir un buzón muy comprometido). Datos completos en `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

CORREO ELECTRÓNICO	DOMINIO	SERVICIO	CONTRASEÑA	RIESGO	PRIMERA VEZ VISTO
employee125@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee155@acm...	acmesample.c	htdark.com	S***e (sample)	7.0	2026-01-06

CORREO ELEC-TRÓNICO	DOMINIO	SERVICIO	CONTRASEÑA	RIESGO	PRIMERA VEZ VISTO
employee044@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee088@acm...	acmesample.c	nohide.app	S***e (sample)	7.0	2026-07-31
employee058@acm...	acmesample.com		S***e (sample)	7.0	S***e (sam
employee136@acm...	acmesample.c	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee498@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee192@acm...	acmesample.c	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee158@acm...	acmesample.com	canadalife.com	S***e (sample)	4.0	2026-04-29
employee076@acm...	acmesample.c	canadalife.com	S***e (sample)	4.0	2026-04-29
employee024@acm...	acmesample.com		S***e (sample)	4.0	2026-04-15
employee264@acm...	acmesample.c		S***e (sample)	4.0	2025-12-27
employee341@acm...	acmesample.com		S***e (sample)	4.0	2026-01-05
employee395@acm...	acmesample.c		S***e (sample)	4.0	2026-01-05
employee374@acm...	acmesample.com		S***e (sample)	7.0	2025-12-25
employee125@acm...	acmesample.c	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee155@acm...	acmesample.com	htdark.com	S***e (sample)	7.0	2026-01-06
employee044@acm...	acmesample.c		S***e (sample)	7.0	2026-01-19
employee088@acm...	acmesample.com		S***e (sample)	4.0	2026-04-15
employee058@acm...	acmesample.c			4.0	2025-12-27

CORREO ELEC-TRÓNICO	DOMINIO	SERVICIO	CONTRASEÑA	RIESGO	PRIMERA VEZ VISTO
			S***e (sample)		

Resumen de Filtraciones

El dominio del sitio web que envió es **acmesample.com**, pero los registros MX de la organización se resuelven a un apex registrado diferente utilizado para el correo electrónico de los empleados. La tabla a continuación compara la **huella de la base de datos de filtraciones** de cada uno: el apex del sitio web cubre todo lo indexado contra la marca de cara al público, mientras que el apex del correo electrónico cubre filtraciones de credenciales vinculadas a buzones de empleados reales — frecuentemente una huella mucho más grande y el objetivo de limpieza de mayor prioridad.

El apogeo del correo electrónico alternativo fue consultado en la base de datos de filtraciones leak.center únicamente — su inventario de subdominios, superficie de puertos, vulnerabilidades, etc. NO fueron enumerados por este escaneo. Para realizar un análisis completo de la superficie de ataque en el apogeo del correo electrónico, reenvíelo como el objetivo principal o seleccione `domain_mode=all` en el próximo escaneo.

Fuente: leak.center API distinct-leak. Los conteos son valores resultCount agregados a través de todas las filtraciones donde el dominio aparece en el contenido indexado. La coincidencia de subcadenas por la API de upstream puede inflar los conteos cuando el nombre de dominio registrado es una subcadena del dominio de otra organización (por ejemplo, `acmesample.com` también coincide con `acmesample-group.com`) — los valores deben leerse como indicadores relativos de presión de exposición en lugar de totales exactos de registros únicos.

2
DOMINIOS BUSCADOS

284
TOTAL DISTINTOS FILTRACIONES

2,038
TOTAL DE REGISTROS DE FILTRACIÓN

DOMINIO	FILTRACIONES DISTINTAS	TOTAL DE REGISTROS	STEALER LOGS	COMBOLISTS	FILTRACIONES DE SITIOS WEB	VOLCADOS DE DB	ETIQUETAS PRINCIPALES / RANGO DE FECHAS
acmesample.com OBJETIVO	282	2,036	33	55	48	17	cuenta (222) email (215) contraseña (159) nombre de usuario (122) url (79) 2008-07-01 → 2026-08-15
acmesample.net EMAIL APEX	2	2	—	—	2	—	ip (2) nombre (2) correo electrónico (2) teléfono (2) fecha de nacimiento (1) 2019-03-07 → 2020-01-01

Cómo leer este capítulo

Registros de Stealer indican que el malware infostealer comprometió puntos finales (empleados o terceros) y exfiltró almacenes de credenciales guardadas que hacen referencia a este dominio. **Combolists** son reciclajes de correo electrónico/contraseña agregados: la mayoría de los pares están llenos de credenciales contra este dominio, incluso si no se han visto comprometidos directamente. **Filtraciones de sitios web** significan que el dominio en sí (o un servicio estrechamente relacionado) fue comprometido. **Volcados de bases de datos** son exportaciones completas de SQL/CSV filtradas al público.

Cada capítulo subsiguiente (Evaluación de Riesgo de Contenido de Filtración, Filtraciones Conocidas que Involucran a Esta Organización, Inteligencia de Datos de Filtración) se centra en el **dominio objetivo únicamente** — las cifras por dominio aquí son el único lugar donde cada dominio analizado se compara lado a lado.

Evaluación de Riesgo de Contenido de Filtración

Análisis de Inteligencia de Amenazas en la Darknet

La organización ha sido identificada en **282** fuentes de filtración distintas, con un total de **2036** registros encontrados que mencionan el dominio "acmesample.com". El rango de fechas de exposición abarca desde **1 de julio de 2008** hasta **15 de agosto de 2026**. Este nivel de exposición se considera **elevado** para una organización de este tipo, lo que indica un riesgo significativo para su postura de seguridad.

Las filtraciones se pueden categorizar en varios tipos. Los registros de stealer representan dispositivos infectados por malware que capturan datos sensibles como credenciales y tokens de sesión en tiempo real. Las combolists consisten en pares de nombre de usuario:contraseña agregados de varias filtraciones, a menudo utilizados para ataques de credential stuffing. Las filtraciones de sitios web/bases de datos indican compromisos directos de servicios específicos, exponiendo potencialmente datos de usuarios.

Los riesgos clave para la organización incluyen ataques de credential stuffing utilizando los **222** registros de cuentas encontrados, secuestro de sesión a través de cookies robadas de las **159** entradas de contraseña, y intentos de phishing aprovechando las **215** direcciones de correo electrónico expuestas.

Dado que se identificaron registros de stealer en los últimos **seis meses**, hay una necesidad urgente para que la organización implemente restablecimientos de contraseña inmediatos y haga cumplir la autenticación multifactor para mitigar posibles filtraciones.

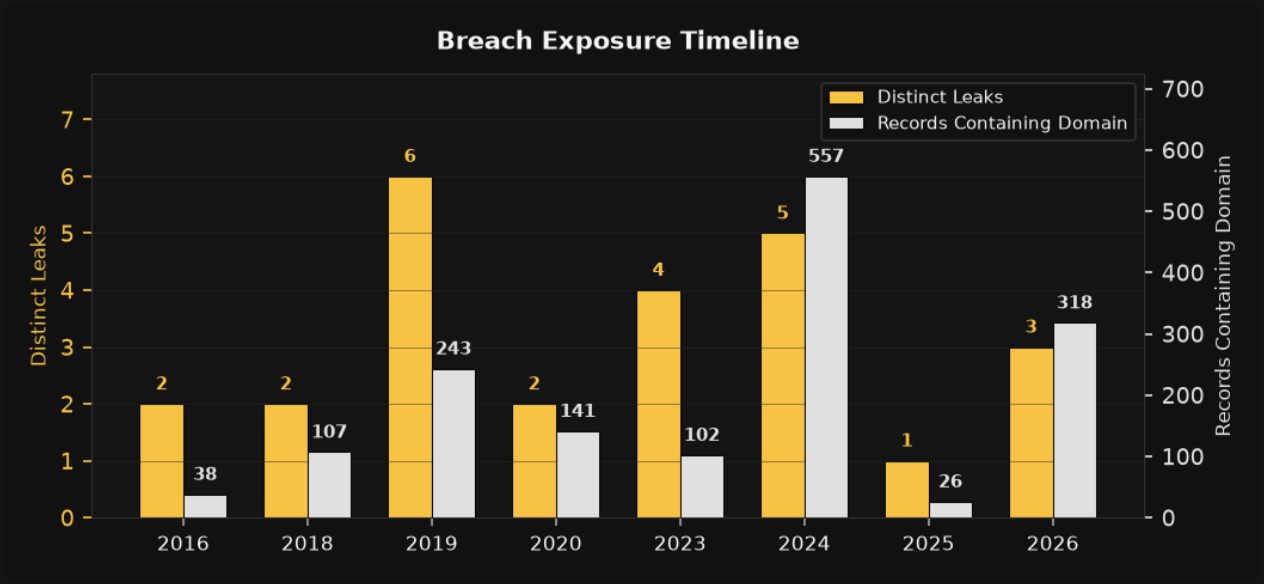
Evaluación de Riesgo de Contenido de Filtración

La organización enfrenta una exposición significativa debido al descubrimiento de **384** direcciones de correo electrónico únicas pertenecientes a su dominio. Esto representa un riesgo directo para su integridad operativa y la privacidad de los empleados. Además, los datos de la filtración revelan una cantidad preocupante de información sensible, incluyendo **376** números de teléfono,

48 direcciones IP y **315** URLs, que podrían facilitar ataques dirigidos. La presencia de **661** perfiles de LinkedIn amplifica aún más el riesgo de tácticas de ingeniería social dirigidas a los empleados.

Los riesgos de ataque específicos derivados de esta filtración son multifacéticos. Las direcciones de correo electrónico filtradas pueden ser explotadas para ataques de credential stuffing, donde los atacantes utilizan estos correos en combinación con contraseñas robadas de otras filtraciones para obtener acceso no autorizado a cuentas. La disponibilidad de números de teléfono aumenta el riesgo de intentos de spear-phishing y de ingeniería social, ya que los atacantes pueden hacerse pasar por contactos de confianza para extraer más información sensible. Además, las direcciones IP y URLs identificadas podrían ser aprovechadas para el mapeo de la red interna, permitiendo a los adversarios planificar ataques más sofisticados contra la infraestructura de la organización.

Los datos de la filtración consisten principalmente en registros de stealer, indicados por la presencia de credenciales en un formato **URL:login:password**, lo que representa un riesgo crítico, ya que estos registros pueden ser utilizados directamente para comprometer cuentas. Esto resalta la urgente necesidad de que la organización implemente medidas de seguridad mejoradas, incluyendo autenticación multifactor y capacitación a los empleados sobre cómo reconocer intentos de phishing, para mitigar los riesgos asociados con esta exposición.



Análisis de Tendencias de Filtraciones

El análisis de los datos de la línea de tiempo de la filtración revela una tendencia fluctuante en la frecuencia de filtraciones de datos distintas asociadas con la organización. A lo largo de los años, el número de filtraciones ha variado, con picos notables en 2019 y 2024, donde la organización registró seis y cinco filtraciones distintas, respectivamente. El volumen de registros expuestos muestra una tendencia más preocupante; 2025 se destaca con un asombroso total de 557 registros, lo que indica un evento de filtración significativo, mientras que 2024 también tuvo un alto conteo de 102 registros. Esto sugiere que, aunque el número de filtraciones puede no aumentar de manera constante, la gravedad de ciertas brechas puede llevar a una exposición sustancial de registros, a menudo indicativa de filtraciones de bases de datos más grandes en lugar de numerosas filtraciones más pequeñas.
Desde una perspectiva de riesgo, la presencia de registros de stealer entre los tipos de filtraciones indica que las amenazas de malware recientes y activas son una preocupación para la organización. Las fechas de exposición varían desde 2008 hasta tan recientemente como agosto de 2026, lo que sugiere que, aunque algunos datos pueden ser históricos, también existe un riesgo de exposición reciente que podría ser explotado. La organización debe priorizar los esfuerzos de remediación inmediata, incluyendo la mejora de las medidas de ciberseguridad para abordar las vulnerabilidades, el monitoreo de signos de explotación de las filtraciones recientes y la implementación de protocolos robustos de respuesta a incidentes. Además, centrarse en la educación de los usuarios sobre phishing y gestión de credenciales será crucial para mitigar los riesgos asociados con los registros de stealer y otras amenazas activas.

Filtraciones conocidas que involucran a esta organización

25 fuentes de filtración distintas que contienen 1,532 registros mencionando el dominio.

FECHA	NOMBRE DE FILTRACIÓN	REGISTROS	TIPOS DE DATOS
2026-08-09	zoominfo.com darkforums.ru 081220…	**155**	privado, dirección, negocio, teléfono, nombre, correo electrónico, url
2026-04-22	Pitney Bowes Inc. (pb.com)_shinyhun…	**46**	privado, dirección, negocio, teléfono, identidad, nombre, correo electrónico, nombre de usuario
2026-02-16	CORPS Combolist_breachforums.as 1…	**117**	contraseña, mezcla, correo electrónico, nombre de usuario
2025-03-13	owcareers.com	**26**	contraseña, privada, dirección, fecha de nacimiento, csv, nombre, correo electrónico, hash, url, cuenta, nombre de usuario
2024-09-23	xiqonline.com	**38**	privado, dirección, negocio, nombre, correo electrónico
2024-09-19	Correos electrónicos únicos de Addka…	**19**	correo electrónico
2024-09-12	pureb2b.co.uk	**128**	contraseña, privada, dirección, negocio, teléfono, csv, ip, nombre, empresa, correo electrónico, hash, cuenta

FECHA	NOMBRE DE FILTRACIÓN	REGISTROS	TIPOS DE DATOS
2024-08-15	demandscience CSV 15 Ago 2024	**342**	contraseña, dirección, negocio, teléfono, ip, nombre, correo electrónico, cuenta
2024-04-07	epa.gov	**30**	privado, dirección, teléfono, csv, nombre, empresa, correo electrónico
2023-06-11	Filtración de registros de stealer y list...	**14**	contraseña, privada, negocio, correo electrónico, hash, cuenta
2023-05-29	"CORP APB" credenciales corporativa...	**18**	contraseña, correo electrónico, cuenta
2023-03-18	Linkedin_darkforumns.su 18 de febrer...	**38**	privado, negocio, teléfono, identidad, csv, nombre, url, nombre de usuario
2023-02-18	LinkedIn 18 de febrero de 2023	**32**	privado, dirección, negocio, teléfono, csv, nombre, empresa, url, nombre de usuario
2020-12-14	Compilación de Filtraciones	**16**	cuenta
2020-01-01	linkedin.com	**125**	contraseña, privada, negocio, nombre, correo electrónico

Mostrando 15 fuentes de filtración distintas más recientes de 25. Datos completos disponibles en `conjunto de datos de evidencia privada`.

Inteligencia de datos de filtración

El análisis de **2,036** registros de filtración de muestra (de un total de **2,038** — Elasticsearch limita las exportaciones por consulta a 2,036) revela los siguientes tipos de datos expuestos más allá de las credenciales:

388 CORREOS ELECTRÓNICOS DE EMPLEADOS	**376** NÚMEROS DE TELÉFONO	**661** PERFILES DE LINKEDIN	**284** NOMBRES PERSONALES
358 DIRECCIONES FÍSICAS	**349** TÍTULOS DE TRABAJO	**315** URLS	**48** DIRECCIONES IP

Por qué esto es importante

Los datos de filtración que contienen nombres personales, direcciones físicas, números de teléfono y títulos de trabajo permiten ataques de phishing y ingeniería social altamente dirigidos. Los atacantes pueden crear pretextos convincentes utilizando detalles reales de empleados, aumentando significativamente la tasa de éxito de las campañas de compromiso de correo electrónico empresarial (BEC).

Muestras de Evidencia de Filtración Cruda

Extractos de registros de filtraciones reales donde se encontró el dominio de la organización. Las coincidencias de dominio están resaltadas.

REGISTRO DE FILTRACIÓN
`[Registro de filtración anonimizado] acmesample.com [valor de credencial eliminado de la muestra pública]`

REGISTRO DE FILTRACIÓN
`[Registro de filtración anonimizado] acmesample.com [valor de credencial eliminado de la muestra pública]`

REGISTRO DE FILTRACIÓN
`[Registro de filtración anonimizado] acmesample.com [valor de credencial eliminado de la muestra pública]`

REGISTRO DE FILTRACIÓN
`[Registro de filtración anonimizado] acmesample.com [valor de credencial eliminado de la muestra pública]`

REGISTRO DE FILTRACIÓN
`[Registro de filtración anonimizado] acmesample.com [valor de credencial eliminado de la muestra pública]`

Enumeración de correo electrónico y análisis de exposición

Buzones pertenecientes a `acmesample.com` descubiertos en cuatro fuentes independientes: bases de datos de filtraciones de datos, enumeración pública de Hunter.io, datos de contacto profesional de RocketReach (solo direcciones corporativas) y el registro de API Central `unique_domain_emails`. El encabezado **Buzones Identificados** a continuación es la unión de descubrimiento más amplia y deduplicada de este capítulo. Los capítulos enfocados en filtraciones utilizan su población de buzones derivada de filtraciones canónicas etiquetadas por separado.

100
EMPLEADOS IDENTIFICADOS
A TRAVÉS DE ROCKETREACH / APOLLO

498
BUZONES IDENTIFICADOS
UNIÓN DEDUPLICADA

390
CON EXPOSICIÓN DE FILTRACIÓN

75
RIESGO ALTO / CRÍTICO

Desglose de Fuente

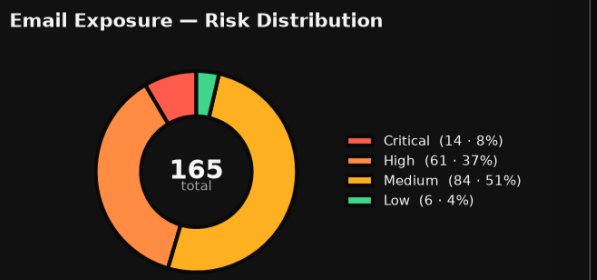
Cada fuente se consulta de manera independiente; el mismo buzón puede ser descubierto por más de un canal. La suma de las filas por fuente es, por lo tanto, típicamente mayor que el total deduplicado de **498** buzones.

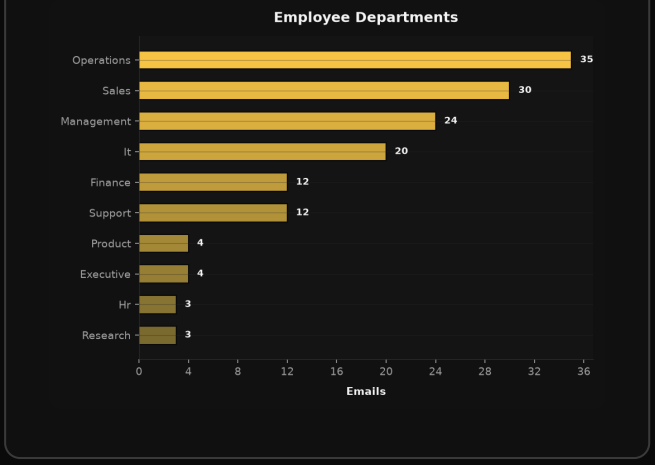
FUENTE	BUZONES	NOTAS
bases de datos_de_filtros	390	Iteración por filtración de leak.center a través de las 100 filtraciones más ricas en datos que contienen `@acmesample.com` (y cualquier dominio de correo electrónico alternativo). Detalle: `conjunto de datos de evidencia privada`.
Hunter.io	165	Descubrimiento de correo electrónico en internet público (Hunter `/v2/domain-search`). Detalle: `conjunto de datos de evidencia privada`.
RocketReach	15	Correos electrónicos de dominio corporativo resueltos a través de la recolección profunda `/person/lookup` sobre el directorio de empleados de RocketReach. Detalle: `conjunto de datos de evidencia privada`.
Registro API central	0	`emails_dominio_unicos` — un registro curado upstream. A menudo vacío para dominios muy cortos (por ejemplo, `tp.com`).
TOTAL (deduplicado)	**498**	Unión de descubrimiento más amplia utilizada por Enumeración de Correo Electrónico (datos de filtración, Hunter.io, RocketReach y el registro de API Central). Los capítulos enfocados en filtraciones utilizan por separado la población de buzones derivada de filtraciones. Consulte `conjunto de datos de evidencia privada` para la auditoría completa.

Cómo se relaciona esto con otros capítulos

Identificamos a **100** personas asociadas con `acmesample.com` a través de datos de red profesional de RocketReach (títulos, empleador, ubicación). El endpoint `/person/search` de RocketReach devuelve solo metadatos — recuperar realmente una dirección de correo electrónico requiere una llamada separada a `/person/lookup` por perfil. El capítulo de Inteligencia de Personas también busca los 15 objetivos de mayor valor (ejecutivos) para el capítulo de Inteligencia VIP; sus direcciones corporativas contribuyen a la fila de RocketReach en el Desglose de Fuentes. El titular de **498** "Buzones Identificados" es la unión de descubrimiento más amplia para este capítulo: direcciones observadas en datos de filtración, Hunter.io, búsquedas de RocketReach, o el registro de la API Central. La Exposición de Credenciales utiliza la población de buzones derivada de filtraciones más estrecha y canónica, por lo que los dos totales no son intencionalmente intercambiables.

De los **498** buzones identificados, **390** fueron observados en al menos una filtración de datos conocida. A través de esos, contamos aproximadamente **26** registros de filtración de credenciales (pares de inicio de sesión + contraseña / hash). El dominio más amplio `acmesample.com` se menciona en **2,038** registros de filtración (cualquier campo — correos electrónicos, URLs, hashes, adjuntos) abarcando **282** bases de datos de filtración distintas.





Exposición dual

62 direcciones de correo electrónico aparecen en ambas bases de datos de filtraciones Y fuentes de internet públicas. Estas personas enfrentan el mayor riesgo: los atacantes pueden combinar credenciales filtradas con detalles personales disponibles públicamente (posición, perfil de LinkedIn) para ataques de phishing altamente dirigidos y compromiso de correo electrónico empresarial (BEC).

Resumen

Se descubrieron 498 correos electrónicos únicos de empleados para acmesample.com. 390 aparecen en bases de datos de filtraciones de datos. 165 son visibles públicamente en internet. 62 correos electrónicos encontrados tanto en filtraciones como en fuentes públicas representan la mayor exposición.

Los 3 Empleados Más Expuestos

Seleccionados en función de la antigüedad organizacional (roles de gestión, director, jefe) combinados con visibilidad pública en línea (número de sitios web donde se encontró la dirección de correo electrónico a través de OSINT)

Estas personas fueron seleccionadas porque su rol senior las convierte en objetivos atractivos para el compromiso de correo electrónico empresarial (BEC) y la ingeniería social, mientras que su alta visibilidad en línea facilita su investigación y suplantación. Las puntuaciones de filtración/datos/acceso a continuación reflejan una exposición adicional por filtraciones de datos.

CRÍTICO Vicepresidente de Gestión de Productos con contraseña filtrada y compromiso del dispositivo

employee058@acmesample.com · Vicepresidente de Gestión de Productos (producto)

PRESENCIA EN LÍNEA	ROL DE LA ORGANIZACIÓN	EXPOSICIÓN DE FILTRACIÓN	EXPOSICIÓN DE DATOS	ACCESO CRÍTICO
3 sitios web públicos	**Ejecutivo** Vicepresidente de Gestión de Productos (producto)	**5**/5 43 filtraciones · registro del ladrón · credencial filtrada	**1**/5 password	**1**/5 sin servicios críticos

Filtración / Datos / Acceso medidos de manera determinista a partir de la evidencia de filtración reconciliada (conteo de registros, presencia de contraseña/stealer filtrada, categorías PII distintas y criticidad del servicio de credenciales).

El correo electrónico Executive012 Sample012 ha aparecido en 43 filtraciones de datos, con una contraseña filtrada y evidencia de compromiso de dispositivo a través de registros de stealer. Esto lo convierte en un objetivo principal para ataques de credential stuffing, lo que podría llevar a la toma de control de la cuenta. Con su posición ejecutiva, también está en riesgo de esquemas de Compromiso de Correo Electrónico Empresarial (BEC), especialmente dado que su correo electrónico es fácilmente encontrable públicamente en 3 sitios web.

CRÍTICO Director Senior, Cuentas Nacionales con contraseña filtrada

employee074@acmesample.com · Director Senior, Cuentas Nacionales (finanzas)

PRESENCIA EN LÍNEA	ROL DE LA ORGANIZACIÓN	EXPOSICIÓN DE FILTRACIÓN	EXPOSICIÓN DE DATOS	ACCESO CRÍTICO
7 sitios web públicos	**Ejecutivo** Director Senior, Cuentas Nacionales (finanzas)	**5**/5 21 filtraciones · contraseña filtrada	**3**/5 contraseña, teléfono, dirección	**1**/5 sin servicios críticos

Filtración / Datos / Acceso medidos de manera determinista a partir de la evidencia de filtración reconciliada (conteo de registros, presencia de contraseña/stealer filtrada, categorías PII distintas y criticidad del servicio de credenciales).

Executive020 Sample020 ha sido expuesto en 21 filtraciones, con una contraseña filtrada que podría facilitar ataques de relleno de credenciales. Además, su información personal de teléfono y dirección está comprometida, haciéndolo vulnerable a ataques de ingeniería social dirigidos. Como director senior, es un objetivo valioso para los atacantes que buscan explotar su acceso, y su correo electrónico es encontrable en 7 sitios web públicos.

CRÍTICO **Director Ejecutivo con exposición de datos personales**

employee158@acmesample.com · Chief Executive Officer (ejecutivo)

PRESENCIA EN LÍNEA	ROL DE LA ORGANIZACIÓN	EXPOSICIÓN DE FILTRACIÓN	EXPOSICIÓN DE DATOS	ACCESO CRÍTICO
5 sitios web públicos	**Ejecutivo** Director Ejecutivo (ejecutivo)	**4**/5 8 filtraciones	**3**/5 teléfono, dirección	**1**/5 sin servicios críticos

Filtración / Datos / Acceso medidos de manera determinista a partir de la evidencia de filtración reconciliada (conteo de registros, presencia de contraseña/stealer filtrada, categorías PII distintas y criticidad del servicio de credenciales).

El correo electrónico de Executive041 Sample041 ha aparecido en 8 filtraciones, pero notablemente carece de una contraseña filtrada. Sin embargo, su teléfono personal y dirección están expuestos, lo que lo hace susceptible a ataques de ingeniería social dirigidos. Como CEO, es un objetivo de alto valor para los atacantes que buscan BEC, y su correo electrónico es localizable en 5 sitios web públicos, aumentando el riesgo de intentos de phishing personalizados.

OBJETIVOS DE ALTO VALOR

Prioridad AI de 100 empleados descubiertos a través de OSINT (RocketReach / Apollo). GPT-4o evalúa la autoridad del rol, el potencial de acceso al sistema y el valor de objetivo para clasificar a los individuos de mayor riesgo.

100
EMPLEADOS DESCUBIERTOS

10
OBJETIVOS DE ALTO VALOR

De **100** empleados identificados a través de OSINT, los siguientes **10** individuos representan los objetivos de mayor valor para el compromiso de correo electrónico empresarial (BEC), ingeniería social y campañas de phishing dirigidas — seleccionados en función de la autoridad organizacional, privilegios de acceso al sistema y visibilidad pública. La lista completa de empleados con todos los 100 registros está disponible en `conjunto de datos de evidencia privada`.

E

MEDIO **Ejecutivo144 Sample144**

Director, Calidad, Inspecciones y Devoluciones · 100 Market Street, Sample City

CORPORATIVO ✉ employee532@acmesample.com [A]

LinkedIn

Como Director, esta persona puede tener acceso a datos y procesos sensibles de control de calidad, lo que la convierte en un objetivo potencial para los atacantes que buscan manipular la calidad del producto o obtener información sobre debilidades operativas.

E

ALTO **Ejecutivo052 Sample052**

Vicepresidente Ejecutivo, Operaciones · 100 Market Street, Ciudad Muestra

CORPORATIVO ✉ employee250@acmesample.com [A]

LinkedIn

En un rol operativo senior, este ejecutivo probablemente tiene una autoridad de toma de decisiones significativa y acceso a sistemas operativos críticos, lo que lo convierte en un objetivo principal para ataques destinados a interrumpir la continuidad del negocio.

E

ALTO **Ejecutivo156 Sample156**

Gerente Senior - Servicios Financieros y Tesorería · 100 Market Street, Sample City

CORPORATIVO ✉ employee565@acmesample.com [A]

LinkedIn

Esta persona tiene acceso a sistemas financieros y operaciones de tesorería, que podrían ser explotados para transacciones fraudulentas o filtraciones de datos, lo que la convierte en un objetivo de alto valor para los atacantes.

E

ALTO **Executive035 Sample035**

Director Senior de Cuentas Estratégicas · 100 Market Street, Sample City

CORPORATIVO ✉ employee148@acmesample.com [A]

PERSONAL ✉ employee480@examplemail.com (proveedor de correo de consumo — no una filtración de dominio objetivo)

LinkedIn Twitter

Con un enfoque en cuentas estratégicas, este director puede tener acceso a datos y contratos sensibles de clientes, lo que lo hace susceptible a ataques de ingeniería social destinados a extraer información confidencial.

E

ALTO **Ejecutivo126 Muestra126**

Director, Ingeniería · 100 Market Street, Ciudad Muestra

CORPORATIVO ✉ employee484@acmesample.com [A]

LinkedIn

Como director de ingeniería, esta persona probablemente posee acceso técnico a sistemas críticos y propiedad intelectual, lo que la convierte en un objetivo para los atacantes que buscan explotar vulnerabilidades o robar información propietaria.

E

CRÍTICO **Executive005 Sample005**

Director de Cultura · 100 Market Street, Sample City

CORPORATIVO ✉ employee009@acmesample.com [A]

LinkedIn

En un rol de C-suite, esta persona tiene una influencia significativa sobre la cultura organizacional y los datos de los empleados, lo que la convierte en un objetivo crítico para los atacantes que buscan manipular dinámicas internas o acceder a información sensible de recursos humanos.

E

CRÍTICO **Executive083 Sample083**

Vicepresidente de Tecnología de la Información · 100 Market Street, Sample City

CORPORATIVO ✉ employee343@acmesample.com [A]

LinkedIn

Como VP de TI, esta persona tiene acceso a infraestructura y sistemas críticos, lo que la convierte en un objetivo de alto valor para los atacantes que buscan explotar vulnerabilidades técnicas o obtener acceso administrativo.

E

ALTO **Executive039 Sample039**

Director de Ventas Cuentas Estratégicas · 100 Market Street, Sample City

CORPORATIVO ✉ employee162@acmesample.com [A]

LinkedIn

El rol de este director implica gestionar cuentas estratégicas, lo que probablemente incluye acceso a información sensible de clientes y datos de ventas, haciéndolo vulnerable a ataques de phishing dirigidos.

E

MEDIO **Executive003 Sample003**

Director de Excelencia Operacional · 100 Market Street, Sample City

CORPORATIVO ✉ employee006@acmesample.com [A]

LinkedIn

Este director se centra en la eficiencia operativa, lo que potencialmente le da acceso a datos de procesos que podrían ser valiosos para competidores o atacantes que buscan interrumpir las operaciones.

E

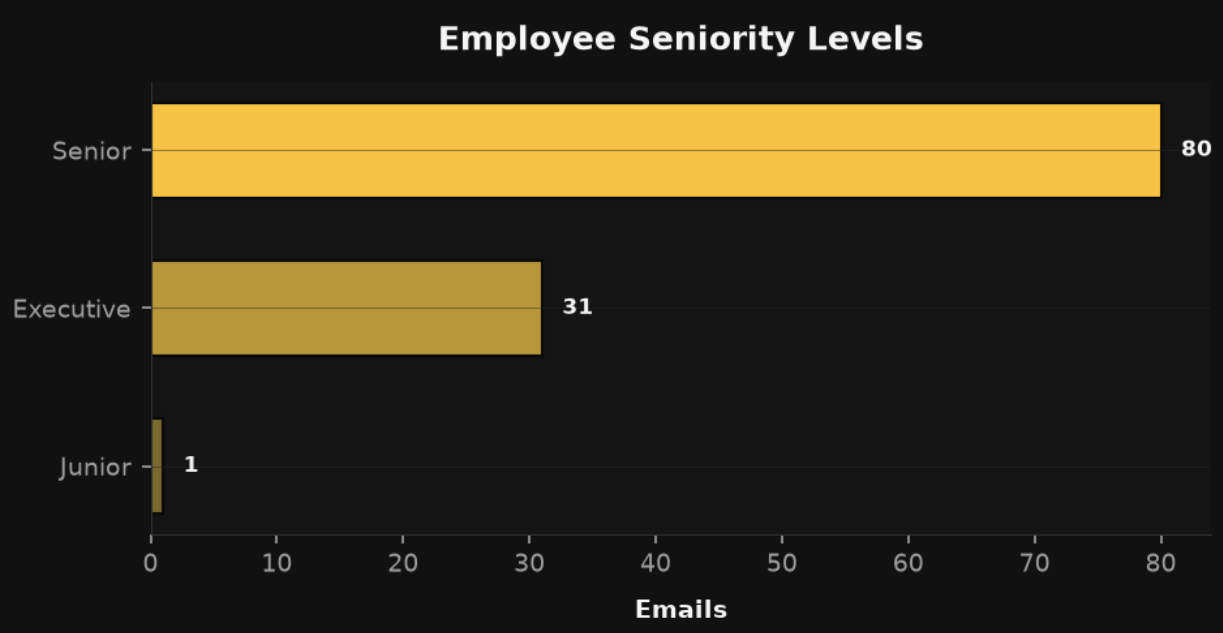
MEDIO **Executive072 Sample072**

Director, Personas y Cultura · 100 Market Street, Ciudad Muestra

CORPORATIVO ✉ employee299@acmesample.com [A]

LinkedIn

Encargado de personas y cultura, este director puede tener acceso a datos sensibles de empleados, lo que lo convierte en un objetivo para los atacantes que buscan explotar información personal para ataques de ingeniería social.



Principales Fuentes de Filtración

FILTRACIÓN / BRECHA	CORREOS ELECTRÓNICOS AFECTADOS
demandscience CSV 15 Ago 2024	41
pureb2b.co.uk	16
demandscience	12
CORPS Combolist_breachforums.as 16.02.2026	10

FILTRACIÓN / BRECHA	CORREOS ELECTRÓNICOS AFECTADOS
zoominfo.com darkforums.ru 08122026 (x)	8
zoominfo.com	7
xiqonline.com	6
Apollo.com	6
CORPS Combolist_breachforums.as	6
zoominfo.com darkforums.ru	6
linkedin.com	4
Pitney Bowes Inc. (pb.com)_shinyhunters	4
Pitney Bowes Inc. (pb.com)_shinyhunters COMPLETO ...	2
canadalife.com_260429	2
UnderArmour_breachforums.bf 15.11.2025	2

Exposición de correo electrónico — Extracto de muestra

Top 20 por puntuación de riesgo. Conjunto de datos completo con todos los 100 registros y desglose de puntuaciones detalladas disponible en `conjunto de datos de evidencia privada`.

CORREO ELECTRÓNICO	NOMBRE	POSICIÓN	RIESGO	FILTRACIONES	PWD	ORIGEN WEB
empleado074@acmesample.com	Executive020 Sample020	Director Senior, Cuentas Nacionales	100	21	1	7
employee158@acmesample.com	Ejecutivo041 Sample041	Director Ejecutivo	95	8	—	5
employee058@acmesample.com	Executive012 Sample012	Vicepresidente de Gestión de Productos	90	43	3	3
employee489@acmesample.com	Executive132 Sample131	Director de Recursos Humanos	80	7	—	1
employee009@acmesample.com	Executive005 Sample005	Director de Cultura	80	6	—	1
employee163@acmesample.com	Ejecutivo036 Sample036	Vicepresidente de Distribución	80	8	—	1
employee425@acmesample.com	Executive124 Sample124	Vicepresidente de Ventas	70	2	—	5
employee220@acmesample.com	Ejecutivo050 Muestra050	Inspector de Control de Calidad	70	3	—	1
employee273@acmesample.com	Ejecutivo067 Sample067	Director Financiero	70	5	—	1

CORREO ELECTRÓNICO	NOMBRE	POSICIÓN	RIESGO	FILTRACIONES	PWD	ORIGEN WEB
employee324@acmesample.com	Executive081 Sample081	Gerente de Distrito	70	4	—	6
employee437@acmesample.com	Executive121 Sample121	Asistente Ejecutivo	70	3	—	1
employee319@acmesample.com	Ejecutivo078 Sample078	Gerente de Marketing de Producto	70	6	—	4
employee533@acmesample.com	Executive146 Sample146	Gerente de ventas regional	65	6	—	1
employee548@acmesample.com	Ejecutivo152 Muestra152	Gerente de Ventas	65	8	—	1
employee526@acmesample.com	Ejecutivo148 Muestra148	Vicepresidente de Ventas	60	0	—	5
employee181@acmesample.com	Executive044 Sample044	Director de Ventas	60	0	—	6
employee148@acmesample.com	Executive035 Sample035	Director Senior de Cuentas Estratégicas	60	0	—	6
employee162@acmesample.com	Executive039 Sample039	Director de Ventas	60	0	—	6
employee484@acmesample.com	Ejecutivo126 Muestra126	Director de Ingeniería	60	2	—	1
employee160@acmesample.com	Executive037 Sample037	Inspector de Control de Calidad	60	2	—	1

Huella Digital VIP

Inteligencia OSINT sobre objetivos de alto valor — cuentas de Google, recuperación de Microsoft, detección de cuentas, exposición de brechas, análisis de contraseñas

En esta evaluación de inteligencia OSINT, evaluamos 20 objetivos corporativos de alto valor, incluidos ejecutivos y alta dirección. Nuestro análisis utilizó múltiples fuentes de datos, incluidas cuentas de Google, información de recuperación de Microsoft, detección de cuentas Holehe y bases de datos de filtraciones. Se probaron un total de 17 direcciones de correo electrónico, revelando 12 ID de Google, 9 cuentas de recuperación de Microsoft y 11 cuentas identificadas a través de Holehe, con un total de 360 hits de filtración en los perfiles analizados. La evaluación descubrió exposiciones significativas, incluidas contraseñas filtradas y correos electrónicos/números de teléfono de recuperación. Notablemente, 10 de los 20 VIPs tenían contraseñas filtradas, lo que podría facilitar ataques de credential stuffing. Además, se obtuvieron datos de ubicación de las reseñas de Google Maps, proporcionando posibles direcciones físicas que podrían ser explotadas para ataques de ingeniería social dirigidos. La presencia de múltiples pruebas de recuperación para varias cuentas aumenta aún más el riesgo de acceso no autorizado. En general, el nivel de riesgo para el liderazgo de la organización es alto. Los atacantes podrían aprovechar esta inteligencia para campañas de phishing dirigidas, utilizando credenciales filtradas para acceder a información o sistemas sensibles. La combinación de datos personales y cuentas comprometidas presenta una vulnerabilidad crítica que requiere atención inmediata para mejorar las medidas de seguridad y mitigar posibles amenazas a la organización.

17	12	9
CORREOS ELECTRÓNICOS PROBADOS	IDS DE GOOGLE	RECUPERACIÓN DE MS

11	360
CUENTAS	REGISTROS DE FILTRACIÓN

ES

Executive012 Sample012

Vicepresidente de Gestión de Productos

employee058@acmesample.com

Executive012 Sample012, Vicepresidente de Gestión de Productos en Acme Sample GmbH, tiene una huella digital significativa con múltiples registros de filtraciones que exponen credenciales corporativas y personales. La reutilización de un patrón de contraseña débil en múltiples sitios y la exposición de datos personales como direcciones físicas y números de teléfono parciales aumentan el riesgo de ataques dirigidos. Esta exposición podría llevar a un acceso no autorizado a sistemas corporativos sensibles y cuentas personales, representando un riesgo CRÍTICO tanto para la seguridad personal como organizacional.

177	0	2	3
REGISTROS DE FILTRACIÓN	PLATAFORMAS	PRUEBAS DE RECUPERACIÓN	FUENTES DE FILTRACIÓN

PUNTUACIÓN DE EXPOSICIÓN **CRÍTICO**

85/100

Potencial de ataque personalizado · mayor = más expuesto

Basado en 177 registros de filtración · 2 pruebas de recuperación · contraseña filtrada · reutilización de contraseñas
Modelo evaluado, limitado por suelos/caps de evidencia determinista

HUELLA DIGITAL

@ Direcciones de correo electrónico

employee058@acmesample.com, employee059@examplemail.com, employee057@examplemail.com

A Dirección física

100 Market Street, Sample City; 100 Market Street, Sample City

T Números de Teléfono

+1 202-555-1013

R Recuperación / Correos electrónicos alternativos

employee057@examplemail.com, email: employee058@acmesample.com, phone: (***) ***-**00

P Ubicaciones observadas

Ciudad de Muestra, Canadá; Ciudad de Muestra, Canadá; Ciudad de Muestra, Canadá; Ciudad de Muestra, Canadá; Ciudad de Muestra, Canadá

G ID de Google confirmado

GAIA sample-45352… · 10 reseñas

ANÁLISIS DE CONTRASEÑAS

6	SÍ	DEBIL	S***E (MUESTRA)
CONTRASEÑAS ÚNICAS	REUTILIZACIÓN	FORTALEZA	PREDECIR.

S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)

- S***e (muestra)
- S***e (muestra)
- S***e (muestra)

Reutilización: S***e (muestra) encontrado en S***e (muestra), S***e (muestra)

Reutilización: S***e (muestra) encontrado en S***e (muestra), S***e (muestra)

S***e (muestra)

CRÍTICO: Misma contraseña utilizada en correo electrónico corporativo Y personal. La contraseña 'S*e (muestra)' se encontró bajo correos electrónicos corporativos (employee058@acmesample.com) y personales (employee057@examplemail.com), lo que indica un uso crítico.**

INTELIGENCIA PERSONAL

Revisado el Lugar de Muestra 01 en Ciudad de Muestra, Canadá el 2026-07-04 — probable viaje de ocio

Revisión de Google Maps · alto

Revisado el Lugar de Muestra 02 en Ciudad de Muestra, Canadá el 2026-05-04 — probable visita frecuente

Revisión de Google Maps · alto

Revisado el Lugar de Muestra 03 en Ciudad de Muestra, Canadá el 2022-09-02 — probable relacionado con el servicio

Revisión de Google Maps · alto

Trabaja en la fabricación industrial de posventa como Vicepresidente de Gestión de Productos en Acme Sample GmbH

Linkedin_darkforumns.su 18 de febrero de 2023 · alto

El código de área telefónica sugiere ubicación: Sample City, Canadá

Linkedin_darkforumns.su 18 de febrero de 2023 · medio

PERSONALIDAD

valores calidad servicio · aprecia personal útil

INTERESES

deportes · comedor

DISPARADORES EMOCIONALES

aprecia el servicio útil · valora experiencias gastronómicas de calidad

ESTILO DE VIDA

viajero frecuente · participa en actividades de ocio

VECTORES DE ATAQUE

Credential Stuffing	ALTO
Spear Phishing - Verificación de credenciales corporativas	ALTO
Spear Phishing - Alerta de Seguridad en Redes Sociales	MEDIO
Ingeniería Social - Estafa de Recompensas de Comida	MEDIO

RIESGO DE CREDENCIALES: Stuffing: **VIABLE** · Spray: **VIABLE**

PRETEXTOS DE SPEAR-PHISHING — UN ESCENARIO POR CADA PUNTO DE DATOS OSINT

Cada fila a continuación empareja UN punto de datos OSINT específico sobre esta persona (un registro de filtración, una cuenta detectada por Holehe, una revisión de Google, un patrón de contraseña, un reutilización de contraseña corporativa↔personal, o un servicio empresarial detectado) con el pretexto de ataque concreto que un adversario podría elaborar a partir de esos datos exactos. La columna “Fuente” es la cita explícita que hace que el pretexto sea creíble — responde a la pregunta “¿por qué es factible este ataque?”. Yield es la estimación de GPT sobre la probabilidad de que un ataque real tenga éxito contra este individuo dado ese señal. Mostrando hasta 6 de 6 pretextos derivados para este perfil (cap: 20).

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	RENDIMIENTO
FILTRACIÓN	**CORP APB** FILTRACIÓN	Filtración de credenciales corporativas de CORP APB mayo 2023	Acme Sample GmbH: Sus credenciales corporativas pueden haber sido comprometidas. Verifique su identidad aquí. filtración reciente + contexto corporativo	ALTO
FILTRACIÓN	**Twitter** FILTRACIÓN	Filtración de datos de Twitter de 1.5M expuso correo electrónico +	Twitter: Se detectó un inicio de sesión inusual. Asegure su cuenta aquí.	MEDIO

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	REND IMI-ENTO
		contraseña para employee057@examplemail.com	filtración de redes sociales + correo electrónico personal	
PATRÓN	**S***e (muestra)** CONTRASEÑA	Se observó el patrón de contraseña 'S***e (muestra)' en 10 filtraciones	Acme Sample GmbH IT: Se detectó un patrón de contraseña débil. Actualice su política de contraseñas aquí. patrón de contraseña común + múltiples filtraciones	MEDIO
REVISAR	**Muestra de Lugar 01** REVISAR	Revisado Muestra de Lugar 01 en Ciudad de Muestra, Canadá el 2026-07-04 (5/5)	Muestra de Lugar 01 Ciudad Muestra: ¡Gracias por su reciente visita! Reclame su recompensa de lealtad aquí. revisión positiva reciente + cena frecuente	MEDIO
REVISAR	**Muestra de Lugar 02** REVISAR	Revisado Muestra de Lugar 02 en Ciudad de Muestra, Canadá el 2026-05-04 (5/5)	Muestra de Lugar 02: ¡Agradecemos su opinión! Disfrute de un 10% de descuento en su próxima compra. revisión positiva + interés en deportes	MEDIO
REVISAR	**Muestra de Lugar 03** REVISIÓN	Revisado Muestra de Lugar 03 en Ciudad de Muestra, Canadá el 2022-09-02 (5/5)	Muestra de Lugar 03: Su satisfacción con el servicio es nuestra prioridad. Reclame su vale de servicio aquí. revisión positiva + satisfacción con el servicio	MEDIO

COMPORTAMIENTO Y PATRONES DE VIAJE — DE 10 RESEÑAS DE GOOGLE

Un atacante puede crear pretextos personalizados (invitaciones a eventos falsos, cebos de proveedor de confianza, phishing en contexto familiar) utilizando las ubicaciones, negocios y tiempos visibles en la actividad pública de Google Maps de esta persona. Cada fila a continuación es una revisión real — la columna “ángulo de explotación” es el gancho de ingeniería social derivado de GPT.

NEGOCIO / LUGAR	UBICACIÓN	CAL-IFIC-ACIÓ N	FECHA	ÁNGULO DE EXPLOTACIÓN
Muestra de Lugar 01	Ciudad de Muestra	5/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 02	Ciudad de Muestra	5/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 03	Ciudad de Muestra	5/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 04	Ciudad de Muestra	4/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 05	Ciudad de Muestra	3/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 06	Ciudad de Muestra	5/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 07	Ciudad de Muestra	3/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 08	Ciudad de Muestra	4/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 09	Ciudad de Muestra	1/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.
Muestra de Lugar 10	Ciudad de Muestra	5/5	—	La actividad de revisión pública apoya un pretexto de lugar rutinario; los detalles del lugar y la ubicación se han eliminado de esta muestra pública.

ES

Executive020 Sample020

Director Senior, Cuentas Nacionales

empleado074@acmesample.com

El Director Executive020 Sample020 de Acme Sample GmbH tiene una exposición de alto riesgo debido a múltiples filtraciones de datos que involucran credenciales filtradas. Estas filtraciones incluyen plataformas significativas como LinkedIn y Trello, con evidencia de patrones de reutilización de contraseñas. La exposición de su dirección física y número de teléfono parcial eleva aún más el riesgo, permitiendo posibles ataques dirigidos. Se recomienda una remediación inmediata para mitigar estos riesgos.

26 REGISTROS DE FILTRACIÓN

1 PLATAFORMAS

2 PRUEBAS DE RECUPERACIÓN

6 FUENTES DE FILTRACIÓN

PUNTUACIÓN DE EXPOSICIÓN — ALTO

85/100

Potencial de ataque personalizado · mayor = más expuesto

Basado en 26 registros de filtración · 1 cuenta · 2 pruebas de recuperación · contraseña filtrada
Modelo evaluado, limitado por suelos/caps de evidencia determinista

HUELLA DIGITAL

@ Direcciones de correo electrónico
empleado074@acmesample.com

A Dirección física
100 Market Street, Sample City

T Números de Teléfono
+1 202-555-1015

R Recuperación / Correos electrónicos alternativos
correo electrónico:
employee074@acmesample.com, teléfono:
********68

W Cuentas detectadas
office365

P Ubicaciones observadas
Sample City, CA

G ID de Google confirmado
GAIA muestra-19499...

ANÁLISIS DE CONTRASEÑAS

5	NO	DEBIL	S***E (MUESTRA)
CONTRASEÑAS ÚNICAS	REUTILIZACIÓN	FORTALEZA	PREDECIR.

S***e (muestra) S***E (MUESTRA) S***e (muestra)
S***e (muestra) S***E (MUESTRA) S***e (muestra)
S***e (muestra) S***E (MUESTRA) S***e (muestra)
S***e (muestra) S***E (MUESTRA) S***e (muestra)

- S***e (muestra)
- S***e (muestra)
- S***e (muestra)

S***e (muestra)

INTELIGENCIA PERSONAL

Trabaja en Transporte como Analista de Negocios en Acme Sample GmbH (100-249 empleados)

DemandScience CSV · alto

Rango de ingresos de $50 - 99 millones

DemandScience CSV · alto

VECTORES DE ATAQUE

Credential Stuffing	ALTO
Spear Phishing	MEDIO
Vishing	MEDIO
Acceso físico	BAJO

RIESGO DE CREDENCIALES: Stuffing: **VIABLE** · Spray: **VIABLE**

PRETEXTOS DE SPEAR-PHISHING — UN ESCENARIO POR CADA PUNTO DE DATOS OSINT

Cada fila a continuación empareja UN punto de datos OSINT específico sobre esta persona (un registro de filtración, una cuenta detectada por Holehe, una revisión de Google, un patrón de contraseña, un reutilización de contraseña corporativa↔personal, o un servicio empresarial detectado) con el pretexto de ataque concreto que un adversario podría elaborar a partir de esos datos exactos. La columna “Fuente” es la cita explícita que hace que el pretexto sea creíble — responde a la pregunta “¿por qué es factible este ataque?”. El rendimiento es la estimación de GPT de cuán probable sería que un ataque real tuviera éxito contra este individuo dado ese señal. Mostrando hasta 5 de 5 pretextos derivados para este perfil (cap: 20).

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	REND IMI-ENTO
FILTRACIÓN	**Zacks.com** FINANZAS	Registro de stealer ULP 21.04.2025 capturó employee074@acmesample.com en Zacks.com usando la contraseña S***e (muestra)	Se detectó actividad inusual en su cuenta de Zacks. Confirme sus transacciones recientes aquí. El registro de stealer proporciona captura directa de credenciales con fecha reciente.	ALTO
SERVICIO	**Office365** PRODUCTIVIDAD	Holehe confirmó que la cuenta existe en office365 para el correo electrónico employee074@acmesample.com	Su cuenta de Office365 requiere verificación inmediata. Haga clic aquí para asegurar su cuenta. Se confirmó la existencia de la cuenta en una plataforma de productividad.	MEDIO
FILTRACIÓN	**Trello.com** PRODUCTIVIDAD	La compilación de filtraciones expuso correo electrónico + contraseña para Trello.com	Cebo dirigido que hace referencia a Trello.com; la redacción original ha sido eliminada de esta muestra pública. Los datos de la filtración incluyen correo electrónico y contraseña para una herramienta de productividad.	MEDIO
FILTRACIÓN	**xiqonline.com** OTRO	La compilación de filtraciones expuso correo electrónico + contraseña para xiqonline.com	Su cuenta de xiqonline ha sido marcada por actividad sospechosa. Verifique los detalles de su cuenta aquí. Los datos de la filtración incluyen correo electrónico y contraseña para un servicio menos conocido.	MEDIO
PATRÓN	**S***e (muestra)** CONTRASEÑA	Patrón de contraseña 'S***e (muestra)' + sufijo numérico observado en múltiples filtraciones	Nuestro sistema detectó una coincidencia de patrón débil contra su contraseña histórica (S***e (muestra)). Actualice su contraseña aquí. Patrón de contraseña débil reutilizado en múltiples filtraciones.	MEDIO

ES

Executive040 Sample040

Líder Técnico de TI

employee157@acmesample.com

El Ejecutivo040 Sample040, un Líder Técnico de TI en Acme Sample GmbH, ha sido expuesto en múltiples filtraciones de datos, incluida una que reveló PII completa. Esta exposición incluye información de correo electrónico, contraseña, teléfono y dirección, que podría ser utilizada para ataques dirigidos. La reutilización de patrones de contraseñas débiles en diferentes plataformas agrava aún más el riesgo, haciendo que tanto las cuentas personales como las corporativas sean vulnerables a compromisos.

11 REGISTROS DE FILTRACIÓN

5 PLATAFORMAS

1 PRUEBAS DE RECUPERACIÓN

2 FUENTES DE FILTRACIÓN

PUNTUACIÓN DE EXPOSICIÓN

ALTO

80/100

Potencial de ataque personalizado · mayor = más expuesto

Basado en 11 registros de filtración · 5 cuentas · 1 prueba de recuperación · contraseña filtrada
Modelo evaluado, limitado por suelos/caps de evidencia determinista

HUELLA DIGITAL

@ Direcciones de correo electrónico
employee157@acmesample.com, employee161@examplemail.com

A Dirección física
100 Market Street, Sample City; 100 Market Street, Sample City

T Números de Teléfono
+1 202-555-1016, +1 202-555-1017

R Recuperación / Correos electrónicos alternativos
teléfono: ********43

W Cuentas detectadas
hubspot, office365, gravatar, spotify

P Ubicaciones observadas
Sample City, Canadá

G ID de Google confirmado
GAIA sample-69845…

ANÁLISIS DE CONTRASEÑAS

1	NO	DEBIL	S***E (MUESTRA)
CONTRASEÑAS ÚNICAS	REUTILIZACIÓN	FORTALEZA	PREDECIR.

S***e (muestra) S***E (MUESTRA) S***e (muestra)

- S***e (muestra)

S***e (muestra)

INTELIGENCIA PERSONAL

Trabaja en la industria de TI como Líder Técnico de TI en Acme Sample GmbH

DemandScience CSV · alto

Navegador/sesión rastreada hasta Sample City, Canadá

Sesión de registro de Stealer · medio

El código de área telefónica sugiere ubicación: Sample City, Canadá

DemandScience CSV · alto

VECTORES DE ATAQUE

Spear Phishing a través de la filtración de Pitney Bowes	ALTO
Credential Stuffing en Office365	MEDIO
Vishing utilizando Números de Teléfono Expuestos	MEDIO

RIESGO DE CREDENCIALES: Stuffing: **VIABLE** · Spray: **VIABLE**

PRETEXTOS DE SPEAR-PHISHING — UN ESCENARIO POR CADA PUNTO DE DATOS OSINT

Cada fila a continuación empareja UN punto de datos OSINT específico sobre esta persona (un registro de filtración, una cuenta detectada por Holehe, una revisión de Google, un patrón de contraseña, un reutilización de contraseña corporativa↔personal, o un servicio empresarial detectado) con el pretexto de ataque concreto que un adversario podría elaborar a partir de esos datos exactos. La columna “Fuente” es la cita explícita que hace que el pretexto sea creíble — responde a la pregunta “¿por qué es factible este ataque?”. Yield es la estimación de GPT sobre cuán probable sería que un ataque real tuviera éxito contra este individuo dado ese señal. Mostrando hasta 3 de 3 pretextos derivados para este perfil (cap: 20).

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	REND IMI-ENTO
FILTRACIÓN	**Pitney Bowes Inc. (pb.com)** FILTRACIÓN	Pitney Bowes Inc. (pb.com)_ shinyhunters FULL 22.04.2026 csv expuso toda la PII (nombre, dirección, teléfono) de employee157@acmesample.com	Alerta de seguridad de Pitney Bowes: Confirme su identidad para asegurar su cuenta. filtración reciente con exposición completa de PII	ALTO
SERVICIO	**Office365** PRODUCTIVIDAD	Holehe confirmó que existe una cuenta en Office365 para el correo electrónico employee157@acmesample.com	Su cuenta de Office365 fue accedida desde un nuevo dispositivo. Haga clic aquí para verificar. confirmación de cuenta corporativa	MEDIO
PATRÓN	**General** CONTRASEÑA	Patrón de contraseña 'S***e (ejemplo)' observado en la filtración de xiqonline.com	Nuestro sistema detectó una coincidencia de patrón débil contra su contraseña histórica. Actualice sus credenciales aquí. patrón de contraseña débil observado	MEDIO

ES

Executive035 Sample035

Director Senior de Cuentas Estratégicas

employee148@acmesample.com

Executive035 Sample035, un Director Senior en Acme Sample GmbH, ha sido identificado con múltiples cuentas comprometidas, incluyendo Luxottica, Houzz y AT&T, con contraseñas expuestas. La reutilización de patrones de contraseñas similares en estas filtraciones representa un riesgo CRÍTICO tanto para la seguridad personal como corporativa. Además, la presencia de correos electrónicos alternativos y números de teléfono parciales aumenta el potencial de ataques de phishing y vishing dirigidos.

79
REGISTROS DE FILTRACIÓN

1
PLATAFORMAS

2
PRUEBAS DE RECUPERACIÓN

4
FUENTES DE FILTRACIÓN

PUNTUACIÓN DE EXPOSICIÓN

ALTO

80/100

Potencial de ataque personalizado · mayor = más expuesto

Basado en 79 registros de filtración · 1 cuenta · 2 pruebas de recuperación · contraseña filtrada · reutilización de contraseñas
Modelo evaluado, limitado por suelos/caps de evidencia determinista

HUELLA DIGITAL

@ **Direcciones de correo electrónico**

employee148@acmesample.com, employee480@examplemail.com, employee481@examplemail.com

T **Números de Teléfono**

+1 202-555-1014

R **Recuperación / Correos electrónicos alternativos**

employee480@examplemail.com, employee481@examplemail.com, correo electrónico: employee480@examplemail.com, teléfono: ***-***-**76

W **Cuentas detectadas**

office365

G **ID de Google confirmado**

GAIA sample-95896...

ANÁLISIS DE CONTRASEÑAS

5
CONTRASEÑAS ÚNICAS

SÍ
REUTILIZACIÓN

DEBIL
FORTALEZA

S*E (MUESTRA)**
PREDECIR.

S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)
S***e (muestra)	S***E (MUESTRA)	S***e (muestra)

- S***e (muestra)
- S***e (muestra)
- S***e (muestra)

Reutilización: S***e (muestra) encontrado en S***e (muestra), S***e (muestra)

Reutilización: S***e (muestra) encontrado en S***e (muestra), S***e (muestra)

S***e (muestra)

CRÍTICO: Misma contraseña utilizada en correo electrónico corporativo Y personal. La contraseña 'S*e (muestra)' se encontró bajo el correo electrónico corporativo (employee148@acmesample.com) y el correo electrónico personal (employee481@examplemail.com), indicando un problema crítico de reutilización.**

INTELIGENCIA PERSONAL

Trabaja en cuentas estratégicas en Acme Sample GmbH

DemandScience CSV · alto

Sesión de navegador rastreada hasta EE. UU.

Sesión de registro de Stealer · medio

El código de área telefónica sugiere ubicación: EE. UU.

Sesión de registro de Stealer · medio

VECTORES DE ATAQUE

Credential Stuffing	ALTO
Spear Phishing	MEDIO
Vishing	MEDIO

RIESGO DE CREDENCIALES: Stuffing: **VIABLE** · Spray: **VIABLE**

PRETEXTOS DE SPEAR-PHISHING — UN ESCENARIO POR CADA PUNTO DE DATOS OSINT

Cada fila a continuación empareja UN punto de datos OSINT específico sobre esta persona (un registro de filtración, una cuenta detectada por Holehe, una revisión de Google, un patrón de contraseña, un reutilización de contraseña corporativa↔personal, o un servicio empresarial detectado) con el pretexto de ataque concreto que un adversario podría elaborar a partir de esos datos exactos. La columna “Fuente” es la cita explícita que hace que el pretexto sea creíble — responde a la pregunta “¿por qué es factible este ataque?”. El rendimiento es la estimación de GPT de cuán probable sería que un ataque real tuviera éxito contra este individuo dado ese señal. Mostrando hasta 5 de 5 pretextos derivados para este perfil (cap: 20).

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	RENDIMIENTO
SERVICIO	**Office 365** PRODUCTIVIDAD	Holehe confirmó que la cuenta existe en office365 para el correo electrónico employee148@acmesample.com	Su cuenta de Office 365 tiene actividad inusual. Verifique su inicio de sesión aquí. contexto corporativo confirmado	ALTO
FILTRACIÓN	**Luxottica.com** FILTRACIÓN	Los datos de la filtración expusieron el correo electrónico + contraseña para Luxottica.com	Cebo dirigido que hace referencia a Luxottica.com; la redacción original ha sido eliminada de esta muestra pública. filtración reciente con exposición de contraseña	MEDIO
FILTRACIÓN	**houzz.com** FILTRACIÓN	Los datos de la filtración expusieron el correo electrónico + contraseña para houzz.com en S***e (muestra)	Alerta de seguridad de Houzz: Su cuenta fue accedida. Asegure su cuenta ahora. filtración histórica con exposición de contraseña	MEDIO
FILTRACIÓN	**AT&T** FILTRACIÓN	Los datos de la filtración expusieron el correo electrónico + contraseña para AT&T en S***e (muestra)	Seguridad de cuenta de AT&T: Se detectó un inicio de sesión inusual. Verifique su identidad. filtración reciente con exposición de contraseña	MEDIO
PATRÓN	**Patrón de Contraseña** PASSWORD	Patrón r2****jf observado en múltiples filtraciones	Nuestro sistema de monitoreo detectó un patrón de contraseña débil en su cuenta. Actualice su contraseña aquí. patrón repetido en filtraciones	MEDIO

ES

Ejecutivo067 Sample067

Director Financiero

employee273@acmesample.com

Executive067 Sample067, el CFO de Acme Sample GmbH, tiene una exposición de alto riesgo debido a múltiples filtraciones que revelan información sensible, incluyendo correo electrónico, contraseña y PII completa. La presencia de patrones de contraseñas débiles y la reutilización en diferentes plataformas aumentan la probabilidad de ataques exitosos a las credenciales. Esta exposición representa un riesgo CRÍTICO tanto para la seguridad personal como corporativa, lo que requiere esfuerzos de remediación inmediatos.

10 REGISTROS DE FILTRACIÓN

4 PLATAFORMAS

2 PRUEBAS DE RECUPERACIÓN

3 FUENTES DE FILTRACIÓN

PUNTUACIÓN DE EXPOSICIÓN — ALTO

85/100

Potencial de ataque personalizado · mayor = más expuesto

Basado en 10 registros de filtración · 4 cuentas · 2 pruebas de recuperación · contraseña filtrada

Modelo evaluado, limitado por suelos/caps de evidencia determinista

HUELLA DIGITAL

@ Direcciones de correo electrónico

employee273@acmesample.com, employee258@examplemail.com

A Dirección física

100 Market Street, Sample City

T Números de Teléfono

+1 202-555-1019

R Recuperación / Correos electrónicos alternativos

autenticador: TOTP, correo electrónico: wi*****@gmail.com

W Cuentas detectadas

office365, spotify, xvideos

G ID de Google confirmado

GAIA muestra-45583...

ANÁLISIS DE CONTRASEÑAS

2	NO	DEBIL	S***E (MUESTRA)
CONTRASEÑAS ÚNICAS	REUTILIZACIÓN	FORTALEZA	PREDECIR.

S***e (muestra) S***E (MUESTRA) S***e (muestra)

S***e (muestra) S***E (MUESTRA) S***e (muestra)

• S***e (muestra)

S***e (muestra)

INTELIGENCIA PERSONAL

Trabaja en Manufactura como Director Financiero en Acme Sample GmbH (500-999 empleados)

DemandScience CSV · alto

Los ingresos de la empresa son de $10-49 millones

DemandScience CSV · alto

VECTORES DE ATAQUE

Credential Stuffing	ALTO
Spear Phishing a través de Office 365	ALTO
Ataque Vishing	MEDIO
Explotación de Acceso Físico	MEDIO

RIESGO DE CREDENCIALES: Stuffing: **VIABLE** · Spray: **VIABLE**

PRETEXTOS DE SPEAR-PHISHING — UN ESCENARIO POR CADA PUNTO DE DATOS OSINT

Cada fila a continuación empareja UN punto de datos OSINT específico sobre esta persona (un registro de filtración, una cuenta detectada por Holehe, una revisión de Google, un patrón de contraseña, un reutilización de contraseña corporativa↔personal, o un servicio empresarial detectado) con el pretexto de ataque concreto que un adversario podría elaborar a partir de esos datos exactos. La columna “Fuente” es la cita explícita que hace que el pretexto sea creíble — responde a la pregunta “¿por qué es factible este ataque?”. El rendimiento es la estimación de GPT de cuán probable sería que un ataque real tuviera éxito contra este individuo dado ese señal. Mostrando hasta 5 de 5 pretextos derivados para este perfil (cap: 20).

TIPO	SERVICIO / TEMA	FUENTE — POR QUÉ ESTE ATAQUE ES FACTIBLE	PRETEXTO Y JUSTIFICACIÓN	REND IMI-ENTO
SERVICIO	**Office 365** PRODUCTIVIDAD	Holehe confirmó que la cuenta existe en Office 365 para el correo electrónico employee273@acmesample.com	Su cuenta de Office 365 requiere verificación debido a actividad inusual. Haga clic aquí para asegurar su cuenta. confirmación de cuenta corporativa + plataforma de productividad de alto valor	ALTO
FILTRACIÓN	**xiqonline.com** FILTRACIÓN	Registro de filtración de xiqonline.com fechado S***e (muestra) expuso el correo electrónico employee273@acmesample.com con la contraseña S***e (muestra)	Detectamos un intento de inicio de sesión en su cuenta de xiqonline.com. Si no fue usted, restablezca su contraseña aquí. filtración reciente + exposición de contraseña	ALTO
FILTRACIÓN	**DemandScience CSV** FILTRACIÓN	La filtración de CSV de DemandScience expuso PII completa (nombre, dirección, teléfono, rol) para employee273@acmesample.com	Cebo dirigido que hace referencia a DemandScience CSV; la redacción original ha sido eliminada de esta muestra pública. exposición completa de PII + contexto corporativo	ALTO
CUENTA	**Spotify** STREAMING	Holehe confirmó que la cuenta existe en Spotify para el correo electrónico employee273@acmesample.com	Su cuenta de Spotify fue accedida desde un nuevo dispositivo. Verifique su identidad aquí. confirmación de cuenta personal + servicio de streaming	MEDIO
PATRÓN	**Patrón de Contraseña** PASSWORD	Patrón 'palabra base + sufijo numérico S***e (muestra)' observado en la filtración de xiqonline.com	Nuestro sistema de monitoreo de credenciales identificó una coincidencia de patrón débil contra su contraseña histórica (S***e (muestra)). Lea la política de contraseña actualizada aquí. patrón de contraseña débil + potencial de reutilización	MEDIO

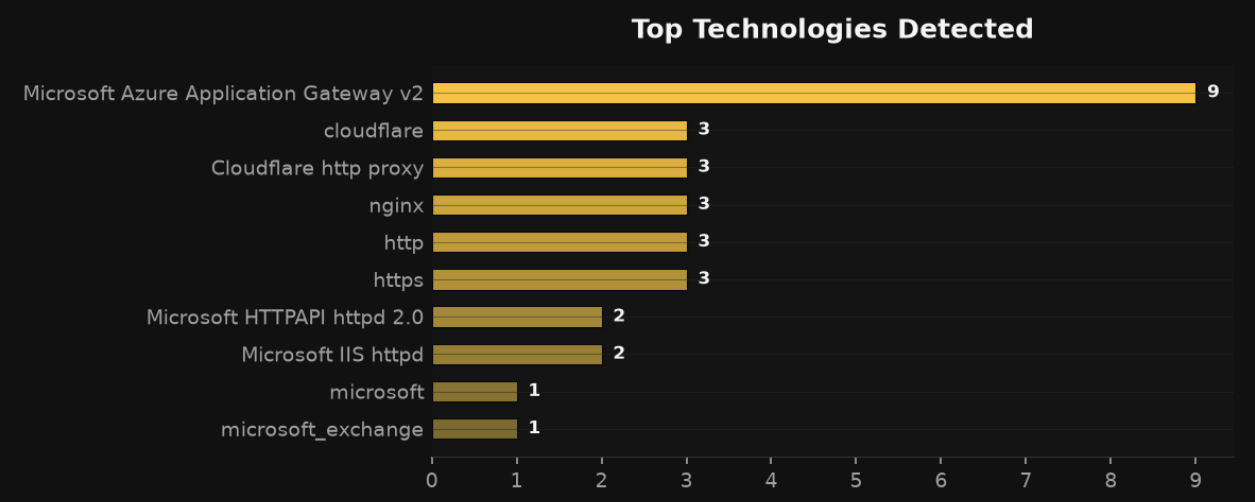
APLICACIONES

Pila Tecnológica

Las tecnologías se detectan a través de inteligencia pasiva: banners de servicio de Shodan, huellas digitales de dominio de Netlas, análisis de host de ZoomEye e identificadores de CPE (Enumeración de Plataforma Común) extraídos de datos de banner. El escaneo de puertos activos (Nmap -sV) proporcionó confirmación adicional de la versión del servicio. La identificación de tecnología permite una investigación de vulnerabilidades dirigida y ayuda a priorizar los esfuerzos de parcheo.

Tecnologías detectadas en **21** de **54** hosts (18 tecnologías únicas). Fuentes de datos: Shodan (banners de servicio, identificadores CPE), Nmap (detección de versión de servicio activa).

Principales tecnologías (rampa de acento único)



Evaluación de Riesgos Tecnológicos

El stack tecnológico de la organización muestra una mezcla de tecnologías, incluyendo Microsoft HTTPAPI httpd 2.0, que está desactualizado y puede representar riesgos de seguridad. Además, la presencia de Microsoft Exchange genera preocupaciones debido a las posibles vulnerabilidades asociadas con versiones más antiguas. Se recomienda que la organización actualice a versiones soportadas de todo el software, enfocándose particularmente en los productos de Microsoft, para mitigar los riesgos de seguridad.

TECNOLOGÍA	DESCRIPCIÓN	HOSTS
Microsoft Azure Application Gateway v2		9
cloudflare	Protección CDN / DDoS	3
proxy http de Cloudflare	CDN / proxy inverso HTTP	3
nginx	Servidor web / proxy inverso	3
http	Protocolo de Transferencia de Hipertexto	3
https	HTTP cifrado por TLS (puerto 443)	3
Microsoft HTTPAPI httpd 2.0		2
Microsoft IIS httpd	Servidor web de Microsoft (IIS)	2
microsoft	Servidor web de Microsoft (IIS)	1
microsoft_exchange	Servidor de correo y colaboración	1
smtp		1
envío		1
microsoft_asp_net		1
kestrel		1
sfdcedge		1

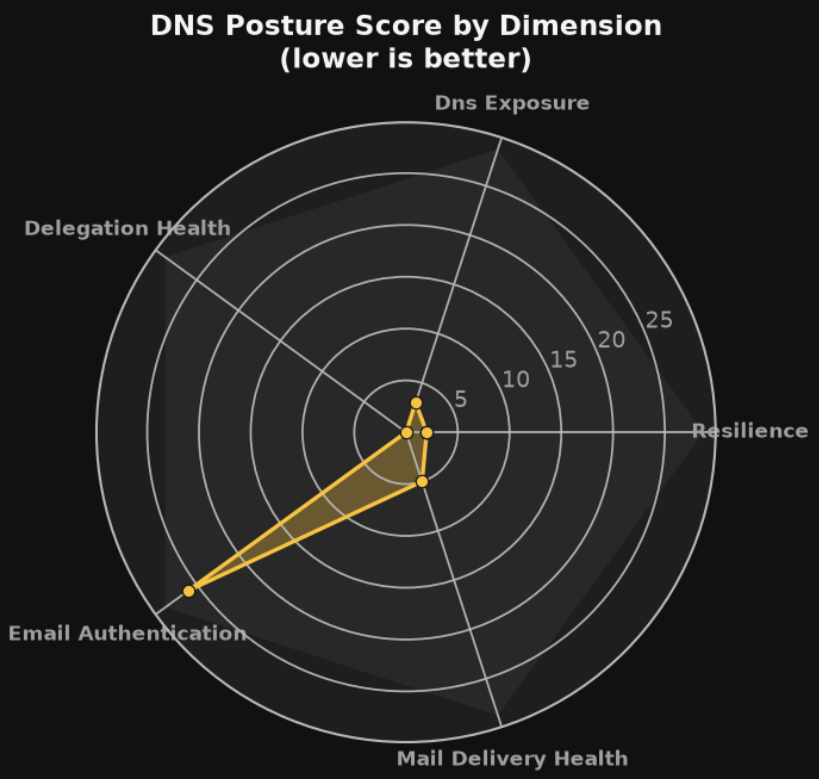
Postura de seguridad de DNS y correo electrónico

76
BUENO

La evaluación de la postura DNS realizó **39 verificaciones automatizadas** en cinco dimensiones de seguridad: salud de delegación (presencia de NS, validez de SOA, delegación débil), exposición DNS (transferencia de zona, recursión abierta, divulgación de versión), autenticación de correo electrónico (SPF, DMARC, DKIM), salud de entrega de correo (resolución de MX, alineación de PTR), y resiliencia (DNSSEC, CAA, diversidad de NS). Se muestran a continuación dos números complementarios: el **puntaje de exposición bruto** (0 = ninguno, 100 = crítico — menor es mejor) y el **puntaje de salud** (100 − exposición, mayor es mejor) que es lo que alimenta el puntaje general de Postura de Seguridad en el resumen ejecutivo.

36/100	64/100	ALTO	39
PUNTUACIÓN DE EXPOSICIÓN (MENOR = MEJOR)	PUNTUACIÓN DE SALUD (MÁS ALTO = MEJOR)	GRAVEDAD GENERAL	VERIFICACIONES REALIZADAS

Dimensiones (menor es mejor)



La postura de DNS tiene brechas: Política de DMARC: Solo monitoreo; No hay registro TXT de MTA-STS. No se encontraron exposiciones críticas.

Hallazgos de Riesgo (2)

GRAVEDAD	VERIFICAR ID	RESULTADO
MEDIO	MAIL_DMARC_POLICY	Política DMARC: Solo Monitoreo
MEDIO	MAIL_MTA_STS_TXT	No hay registro TXT MTA-STS

Resultados de verificación completos (39 en total) disponibles en `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

Perspectivas de DNS inverso (PTR)

Para cada dirección IP descubierta durante el escaneo, realizamos una búsqueda PTR (DNS inverso). Los registros PTR mapean las IPs de vuelta a los nombres de host y revelan convenciones de nomenclatura, detalles de infraestructura y posibles configuraciones incorrectas que los atacantes utilizan durante la exploración.

21	2	19	3
IPS ANALIZADAS	REGISTROS PTR VÁLIDOS	PTR FALTANTE	HALLAZGOS DE RIESGO

Servidores SMTP sin PTR (1)

Los servidores de correo sin registros PTR enfrentan problemas de entregabilidad: muchos servidores receptores rechazan o filtran como spam el correo de IPs que carecen de DNS inverso válido.

IP	NOMBRE DE HOST	PUERTOS SMTP	RIESGO
192.0.2.75	asset-166.acmesample.com	25, 587	ALTO

Desajustes PTR — Fallos de DNS Inverso Confirmados por Adelante (1)

Un desajuste de PTR ocurre cuando el nombre DNS inverso no se resuelve de vuelta a la IP original. Esto es penalizado por los filtros de spam e indica errores de configuración de DNS.

IP	REGISTRO PTR	RESUELVE A	RIESGO
192.0.2.182	bl194.acmesample.com.11.164.207...	NXDOMAIN	MEDIO

Infraestructura de Terceros / Sombra (1)

Los registros PTR que revelan nombres de host de proveedores de nube (por ejemplo, ec2-*.amazonaws.com) pueden indicar activos en la nube no gestionados o IT en la sombra — especialmente cuando el nombre de host hacia adelante pertenece a la organización.

IP	NOMBRE DE HOST	REGISTRO PTR	PROVEEDOR DE NUBE
192.0.2.33	asset-152.acmesample....	ec2-15-156-229-37.ca-central...	AWS

Seguridad de Autenticación de Email

Esta sección evalúa si el dominio puede ser abusado para suplantación de correo electrónico o ataques de phishing basados en configuraciones de SPF, DMARC y DKIM. Los detalles completos del hallazgo, incluidos los dominios afectados, evidencia y pasos de remediación, se omiten de esta muestra pública.

89/100
PUNTUACIÓN DE AUTENTICACIÓN DE CORREO ELECTRÓNICO

MEDIO
RIESGO DE SUPLANTACIÓN

MEDIO
RIESGO DE PHISHING

0
HALLAZGOS CRÍTICOS / ALTOS

Resumen de Configuración

PROTOCOLO	ESTADO	DETALLES
SPF	PRESENTE	Política: `-all` · 3 búsquedas de DNS
DMARC	PRESENTE	Política: p=none
DKIM	1 SELECTOR(ES)	Selectores: selector1
MX	PRESENTE	2 registro(s)

Hallazgos Clave

GRAVEDAD	HALLAZGO	EVIDENCIA
MEDIO	**DMARC Policy: None (Monitoring)** p=none — sin aplicación, solo monitoreo.	Política DMARC: p=none (solo monitoreo).

Hallazgos que requieren atención

RESULTADO	VERIFICAR	DETALLE	RECOMENDACIÓN
ADVERTENCIA	**Incluye Terceros Desconocidos de SPF**	SPF incluye dominios no reconocidos como plataformas de correo electrónico estándar.	Investigar incluir desconocido: dominios y eliminar si no se utilizan.
ADVERTENCIA	**Política DMARC: Ninguna (Monitoreo)**	p=none — sin aplicación, solo monitoreo.	Progresar a p=quarantine luego p=reject después de revisar los informes.
ADVERTENCIA	**DMARC Alineación Relajada**	adkim=r o aspf=r — la alineación relajada puede permitir el spoofing de subdominios.	Establecer adkim=s y aspf=s para alineación estricta.

RESULTADO	VERIFICAR	DETALLE	RECOMENDACIÓN
N/A	**No hay registro BIMI**	BIMI no está configurado.	Publicar un registro TXT de BIMI en default._bimi.dominio.
N/A	**Sin MTA-STS**	MTA-STS no está configurado — el transporte de correo electrónico depende de TLS oportunista.	Publicar el registro TXT _mta-sts y el archivo de política de host.
N/A	**No TLS-RPT**	SMTP TLS Reporting no configurado.	Publicar el registro TXT _smtp._tls con rua= URI de informes.

Evaluación de Vulnerabilidades

53
POBRE

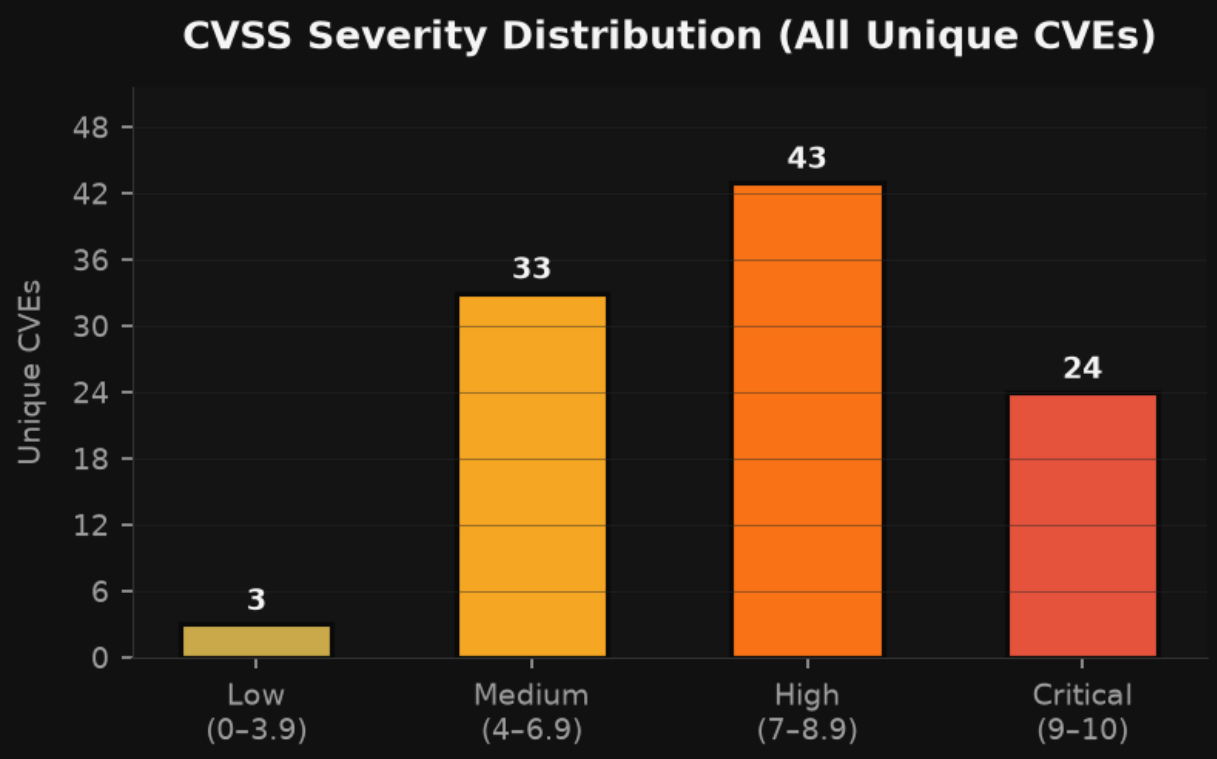
Las vulnerabilidades se agregan de cinco fuentes en orden de prioridad: (1) script de vulnerabilidades de Nmap — mayor confianza, versión coincidente por detección de servicio en vivo, (2) Shodan, (3) Netlas, (4) inteligencia pasiva de ZoomEye, (5) Shodan CVEDB — búsqueda gratuita por nombre/version de producto. Cada CVE se referencia cruzadamente contra los banners de servicio de Nmap; la bandera **version-corroborated** indica que el token del producto y una cadena de versión aparecieron en el banner de servicio detectado (una coincidencia de cadena pasiva, no una verificación de explotación activa).

Descargo de responsabilidad: Todos los hallazgos se basan en **coincidencia de banner de servicio y versión** — no se realizó explotación activa ni inyección de carga útil. Una coincidencia de CVE significa que la versión detectada se sabe que está afectada, no que sea explotable en esta configuración. Los parches, WAF y controles compensatorios pueden mitigar el riesgo.

103	10	0	2
CVES ÚNICOS	HOSTS AFECTADOS	NMAP VERIFICADO	HALLAZGOS DE VERIFICACIÓN
			+397 INFORMATIVOS

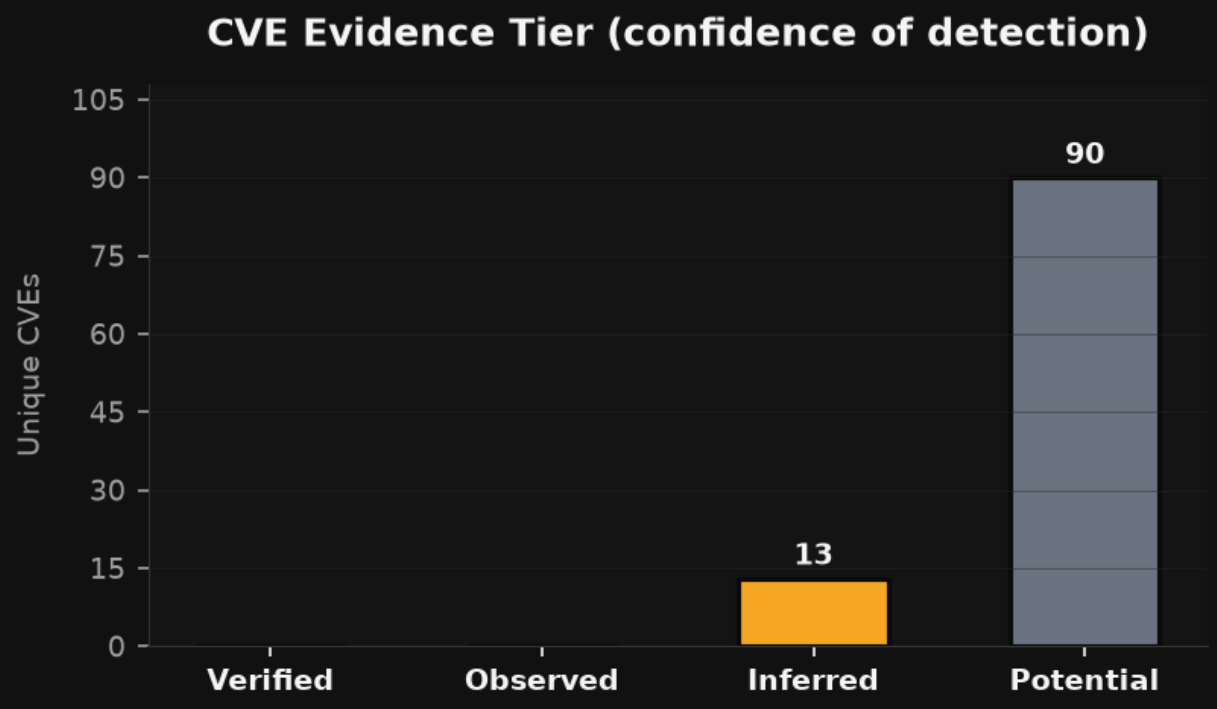
gravedad CVSS (CVE únicos)

Distribución de los 103 CVEs únicos por clasificación de gravedad CVSS v3.

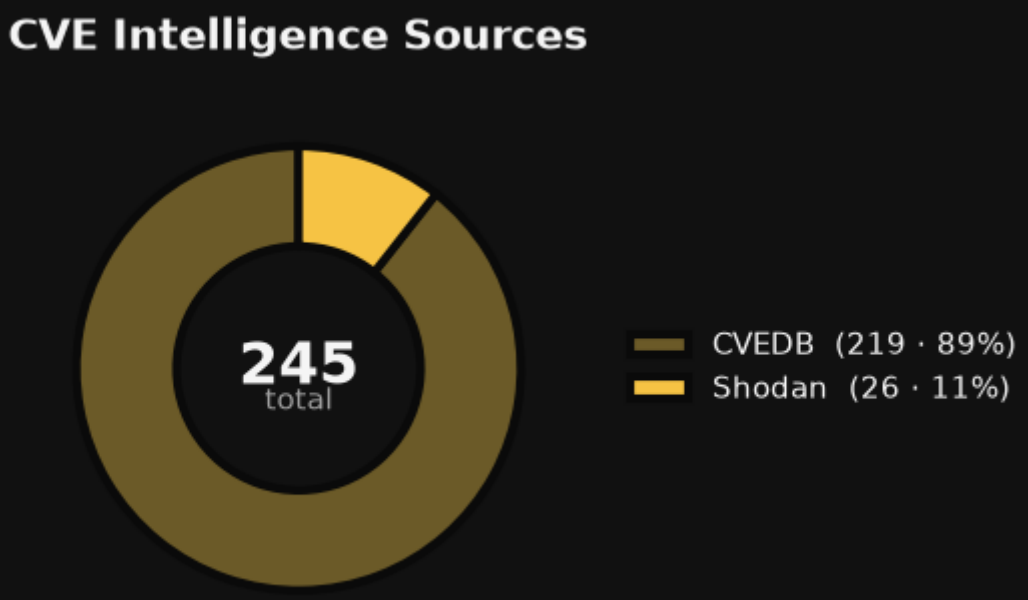


Nivel de evidencia (CVE únicos)

Los mismos CVE clasificados según la fuerza con la que cada uno fue corroborado. **Verificado** = coincidencia exacta de Nuclei host/puerto/CVE o versión confirmada por el operador; **Observado** = banner de servicio Nmap activo; **Inferido** = corroboración de inteligencia pasiva o cadena de versión; **Potencial** = una única señal de producto, aplicabilidad no confirmada.



fuentes de inteligencia CVE



Niveles de confianza

NIVEL	DESCRIPCIÓN	CVE
Producto Coincidente No Verificado	Producto coincidente a través de CPE/banner pero versión no confirmada	**90**
Inteligencia Pasiva	Reportado por plataformas de inteligencia pasiva (Shodan/ Netlas/ZoomEye)	**13**

Niveles de evidencia

Qué tan fuertemente cada CVE fue corroborado, independientemente de su gravedad. Bajo el modelo DS-90 v2, este nivel impulsa la puntuación de vulnerabilidad ponderada por confianza. Los niveles de evidencia se muestran junto a la gravedad en las superficies de CVE y CISA KEV donde la fila subyacente respalda la taxonomía.

NIVEL	SIGNIFICADO	CVE
VERIFICADO	Coincidencia exacta de host/puerto/CVE de Nuclei, o confirmada contra una versión proporcionada por un operador — mayor confianza	0
OBSERVADO	Corroborado por un banner de servicio Nmap activo en el host/puerto afectado	0
INFERIDO	Informe de inteligencia pasiva o corroboración de cadena de versión; no se ha sondeado activamente	13
POTENCIAL	Una señal de producto único; la versión específica y la aplicabilidad no están confirmadas	90

Principales CVEs por gravedad

CVE	CVSS	EVIDENCIA	FUENTES	HOSTS	CONFIANZA
CVE-2004-0847	9.8	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2006-1364	7.5	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2003-0768	6.8	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2005-1664	6.4	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2005-1665	5.0	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2005-2224	5.0	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2005-0452	4.3	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2010-2084	4.3	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2010-2088	4.3	POTENCIAL	CVEDB	4	producto coincidente no verificado
CVE-2015-3105	10.0	POTENCIAL	CVEDB	3	producto coincidente no verificado
CVE-2014-0515	10.0	POTENCIAL	CVEDB	3	producto coincidente no verificado
CVE-2010-0425	10.0	POTENCIAL	CVEDB	3	producto coincidente no verificado

CVE	CVSS	EVIDENCIA	FUENTES	HOSTS	CONFIANZA
CVE-2015-0359	10.0	POTENCIAL	CVEDB	3	producto coincidente no verificado
CVE-2009-3555	9.8	POTENCIAL	CVEDB	3	producto coincidente no verificado
CVE-2024-4577	9.8	POTENCIAL	CVEDB	3	producto coincidente no verificado

Lista completa de vulnerabilidades (103 CVEs) disponible en el Apéndice B y en `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

Orientación sobre Priorización de Explotaciones y Remediación

La siguiente tabla enriquece los componentes de software detectados con inteligencia sobre la madurez de explotación para ayudar a priorizar la remediación más allá de la gravedad CVSS sola. **Madurez de Explotación** indica cuán disponible está el código de explotación funcional — "Arma" significa explotación activa en la naturaleza, mientras que "PoC" indica que existe código de prueba de concepto. Los componentes están ordenados por prioridad de remediación.

SOFTWARE	VERS. DE-TECTADA	VERSIÓN ACTUAL	CVE PRINCIPAL	CVSS	MADUREZ DE EXPLOTACIÓN	PRIORIDAD
windows	unknown	desconocido	CVE-2010-0425	10.0	ARMA	CRÍTICO
Las CVE críticas con exploits conocidos y múltiples hosts afectados requieren una remediación inmediata. cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*						
internet_information_services	10.0	10.0	CVE-2000-0246	10.0	ARMA	BAJO
La versión detectada coincide con la última versión disponible; la CVE listada típicamente requiere una configuración específica o una versión vulnerable — verifique el nivel de parche y la exposición en lugar de realizar una actualización ciega. Las vulnerabilidades críticas con exploits conocidos y un número significativo de hosts requieren atención urgente. cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*						
nginx	unknown	desconocido	CVE-2009-2629	9.8	ARMA	CRÍTICO
Las altas puntuaciones de CVSS y los exploits conocidos en múltiples vulnerabilidades indican un riesgo CRÍTICO. cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*						
asp.net	unknown	desconocido	CVE-2005-1665	9.8	FUNCIONAL	ALTO
Un alto CVSS con exploits públicos confiables sugiere un riesgo significativo, a pesar de no haber explotación conocida. cpe:2.3:a:microsoft:asp.net:*:*:*:*:*:*:*:*						
exchange_server	unknown	desconocido	CVE-2021-26855	9.1	ARMA	CRÍTICO
Las vulnerabilidades CRÍTICAS con exploits conocidos y un solo host afectado requieren acción inmediata. cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*						
cloudflare	unknown	desconocido	CVE-2024-0212	8.1	NO COMPROBADO	MEDIO
Un CVSS moderado sin exploits conocidos y un bajo número de hosts sugiere una menor urgencia para la remediación.						

La madurez de la explotación se evalúa utilizando la gravedad CVSS, la prevalencia del software y la inteligencia de explotación conocida. "Arma" = explotación activa en el entorno; "Funcional" = exploits públicos confiables; "PoC" = existe prueba de concepto; "No probado" = no hay código de explotación conocido.

Verificación de seguridad activa

Escaneados **22/22** IPs únicas (46 puntos finales HTTP activos) en 36.2 minutos utilizando más de 4,000 plantillas seguras curadas (solo GET/HEAD — sin explotación).

¿Por qué 22 IPs en lugar de 54 nombres de host? El motor de verificación opera en direcciones IP únicas (no nombres de host). Se descubrieron 54 nombres de host, de los cuales **25** se resolvieron con éxito a **21** IPs únicas. La mayoría de las IPs en este escaneo están dedicadas a un solo nombre de host — **17** de **21** IPs (81.0%) sirven exactamente un FQDN. Un pequeño número alberga múltiples nombres (IP compartida principal: `192.0.2.178` con 2 FQDNs). Las restantes 22 IPs ingresaron al pipeline y fueron filtradas adicionalmente a través de: (1) una lista blanca de clasificación de puertos (solo web, SSL, DNS y puertos de servicio de red conocidos califican), (2) una verificación de disponibilidad httpx (solo se prueban los puntos finales HTTP/HTTPS que responden con plantillas HTTP), y (3) la caché por IP. Los hosts sin puertos calificativos o sin un punto final HTTP activo aún se cuentan en los totales de despacho pero no producen hallazgos nucleares.

> **2** hallazgos de seguridad accionables (crítico/alto/medio/bajo) y **397** detecciones informativas (huellas tecnológicas, metadatos del entorno — no debilidades por sí mismas).

CATEGORÍA	GRAVEDAD	HALLAZGOS
Accionable	BAJO	**2**
Informativo	INFO	**397**

Hallazgos Accionables Principales por Plantilla

Las plantillas informativas están excluidas de esta tabla (conjunto completo en `conjunto de datos de evidencia privada`).

HALLAZGO	GRAVEDAD	HOSTS	URL DE MUESTRA
Detección de suites de cifrado débiles	BAJO	**2**	asset-188.acmesample.com:443

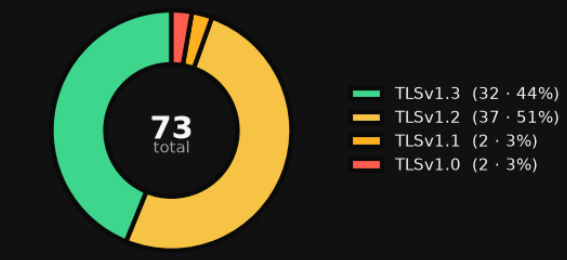
Mostrando las 1 plantillas accionables principales por ocurrencia. Lista completa (incl. informativa) en el Apéndice B y `conjunto de datos de evidencia privada`.

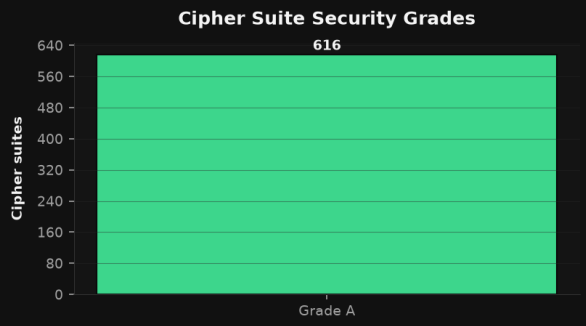
Postura de Seguridad TLS/SSL

91
EXCELENTE

Sintetizado a partir de nmap ssl-enum-ciphers, datos de certificados de Shodan y plantillas SSL de nuclei. Identifica certificados caducados/autofirmados, protocolos obsoletos (TLS 1.0/1.1), suites de cifrado débiles y hosts HTTP-only que faltan HTTPS.

20 HOSTS CON TLS	**0** CERTIFICADOS CADUCADOS	**0** AUTOFIRMADO
2 PROTOCOLOS DÉBILES	**0** CIFRADOS DÉBILES	**90/100** PUNTUACIÓN DE RIESGO · MAYOR = PEOR (CRÍTICO)





Resumen

20 host(s) con TLS detectados a través de la superficie de ataque. 2 host(s) sirven protocolos TLS obsoletos (1.0/1.1). 17 host(s) están en IPs compartidas donde el certificado por defecto pertenece a un dominio diferente (desajuste de CN). 1 host(s) sirven HTTP sin TLS detectado.

Hallazgos de TLS

HOST(S)	IP	HOSTS	PUERTOS AFECTADOS	GRAVEDAD	PROBLEMA
asset-143.acmesample.com (+1 más)	192.0.2.27	**2**	443	ALTO	**TLSv1.0 habilitado**
asset-143.acmesample.com (+1 más)	192.0.2.27	**2**	443	MEDIO	**TLSv1.1 habilitado**
asset-059.acmesample.com	192.0.2.10	**1**	443	MEDIO	**advertencia de cifrado Nmap**
asset-146.acmesample.com	192.0.2.49	**1**	443	MEDIO	**advertencia de cifrado Nmap**
asset-049.acmesample.com	192.0.2.63	**1**	80	INFORMACIÓN	**Host solo HTTP (sin TLS detectado)**

Inventario de Certificados

Mostrando los 15 certificados principales por urgencia de expiración. Inventario completo con los 26 hosts disponibles en `conjunto de datos de evidencia privada`.

HOST	CN	EMISOR	EXPIRA	DÍAS	ESTADO
asset-168.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO

HOST	CN	EMISOR	EXPIRA	DÍAS	ESTADO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VÁLIDO
asset-142.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO
www.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO
asset-141.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO
asset-146.acmesample.com	asset-146.acmesample.com	Let's Encrypt	2026-10-30	**57**	VÁLIDO
asset-169.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO
asset-059.acmesample.com	asset-059.acmesample.com	Let's Encrypt	2026-10-30	**57**	VÁLIDO
asset-170.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VÁLIDO

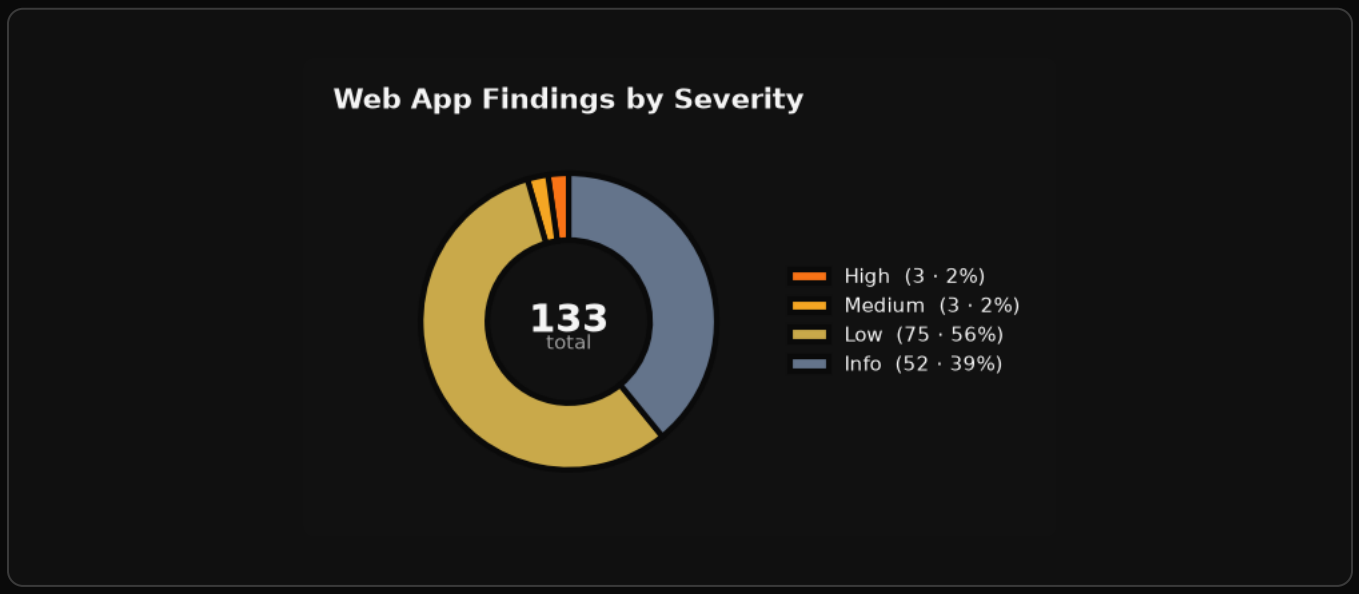
… y 11 certificados más (ver `conjunto de datos de evidencia privada` omitido de esta muestra pública)

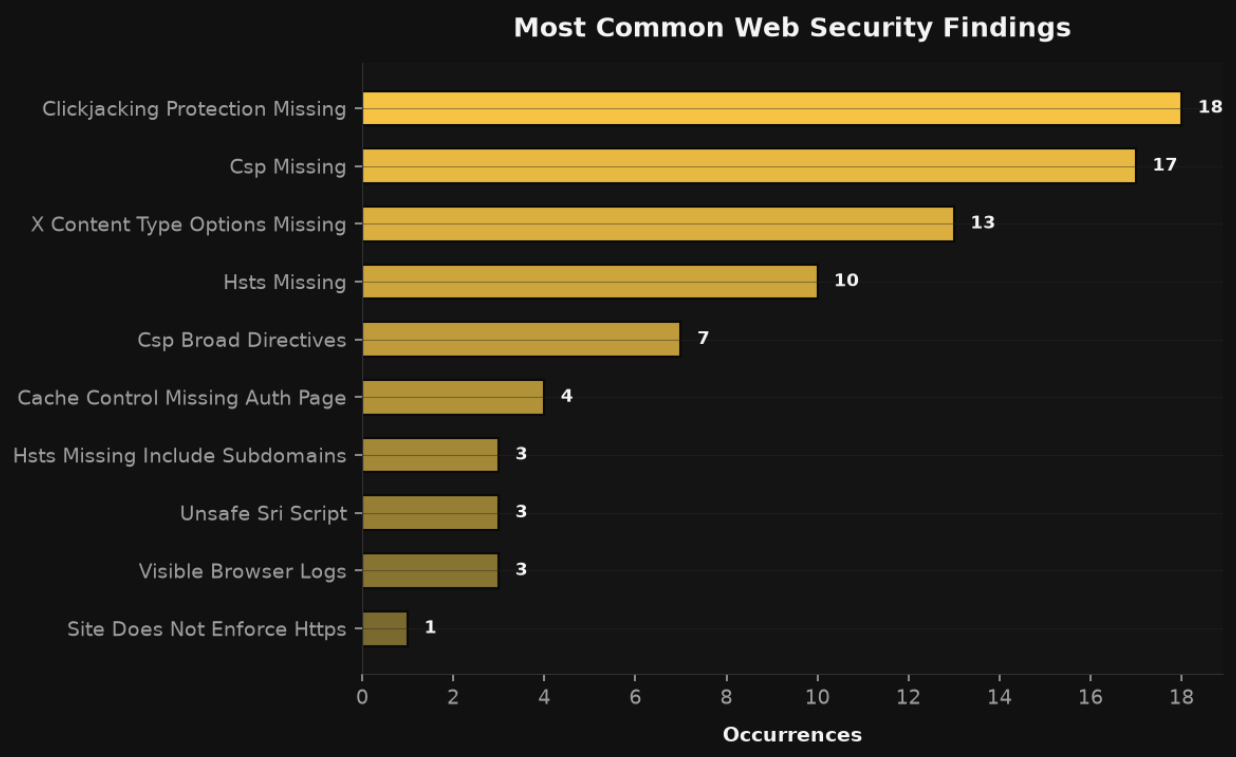
Seguridad de Aplicaciones Web

74
ACEPTABLE

Evalúa los puntos finales web accesibles externamente en busca de debilidades de seguridad HTTP no intrusivas utilizando solicitudes GET seguras, análisis de redirección, inspección de encabezados de respuesta, análisis de Set-Cookie y análisis HTML pasivo. No intenta explotación, inicio de sesión, fuzzing o inyección de payload.

74/100 PUNTUACIÓN DE SEGURIDAD (FAIR)	**48** URLS ESCANEADAS	**33** URLS CON HALLAZGOS
3 ALTA	**3** GRAVEDAD MEDIA	**75** GRAVEDAD BAJA





Resumen

La postura de seguridad de la aplicación web para acmesample.com fue evaluada en 48 URL(s), obteniendo una puntuación general de 74/100 (justa). Se identificaron 3 hallazgos de alta gravedad, incluidos problemas con la seguridad de las cookies de sesión y/o cadenas de redirección inseguras. Se requieren atención 3 problemas de gravedad media. Se notaron 75 debilidades de configuración de baja gravedad (encabezados faltantes, configuraciones débiles de CSP/HSTS).

Puntuaciones de Seguridad de Hosts

HOST	PUNTUACIÓN	ALTO	MEDIO	BAJO	CALIFICACIÓN
asset-064.acmesample.com	**61/100**	0	3	1	JUSTO
www.acmesample.com	**70/100**	1	0	3	JUSTO
asset-188.acmesample.com	**70/100**	1	0	3	JUSTO
asset-143.acmesample.com	**70/100**	1	0	3	JUSTO
192.0.2.68	**78/100**	0	0	8	BUENO

HOST	PUNTUACIÓN	ALTO	MEDIO	BAJO	CALIFICACIÓN
asset-065.acmesample.com	**82/100**	0	0	7	BUENO
asset-134.acmesample.com	**85/100**	0	0	5	BUENO
asset-148.acmesample.com	**88/100**	0	0	4	BUENO
asset-142.acmesample.com	**88/100**	0	0	4	BUENO
asset-168.acmesample.com	**88/100**	0	0	4	BUENO

Hallazgos de seguridad web de alto riesgo

HOST	VERIFICAR	GRAVEDAD	EVIDENCIA
www.acmesample.com	Script Sri inseguro	ALTO	El script externo de hs-scripts.com carece del atributo de integridad SRI
asset-188.acmesample.com	Script Sri inseguro	ALTO	El script externo de hs-scripts.com carece del atributo de integridad SRI
asset-064.acmesample.com	Patrón de Redirección Https Inseguro	MEDIO	Redirección HTTP a dominio externo microsoft.com
asset-064.acmesample.com	Directivas Amplias de Csp	MEDIO	CSP tiene 3 directivas amplias
asset-064.acmesample.com	Directivas Inseguras de Csp	MEDIO	CSP utiliza 1 directiva(s) insegura(s)
asset-143.acmesample.com	Script Sri inseguro	ALTO	El script externo de hs-scripts.com carece del atributo de integridad SRI

Hallazgos Más Comunes

VERIFICAR	OCURRENCIAS
Protección contra Clickjacking faltante	18
Csp Faltante	17
X Content Type Options faltante	13
Hsts Faltante	10
Directivas Amplias de Csp	7
Control de Caché Página de Autenticación Faltante	4
Hsts Faltante Incluir Subdominios	3
Script Sri inseguro	3
Registros de navegador visibles	3
El sitio no aplica Https	1

Metodología. Este capítulo evalúa los puntos finales web accesibles externamente en busca de debilidades de seguridad HTTP no intrusivas utilizando solicitudes GET/HEAD seguras, análisis de redirección, inspección de encabezados de respuesta, análisis de Set-Cookie y análisis pasivo de HTML. No intenta explotación, inicio de sesión, fuzzing o inyección de carga útil. Las verificaciones cubren la seguridad de las cookies de sesión, la aplicación de HTTPS, la Política de Seguridad de Contenidos, HSTS, protección contra clickjacking, integridad de subrecursos y más.

INFRAESTRUCTURA

Análisis de Puertos y Servicios

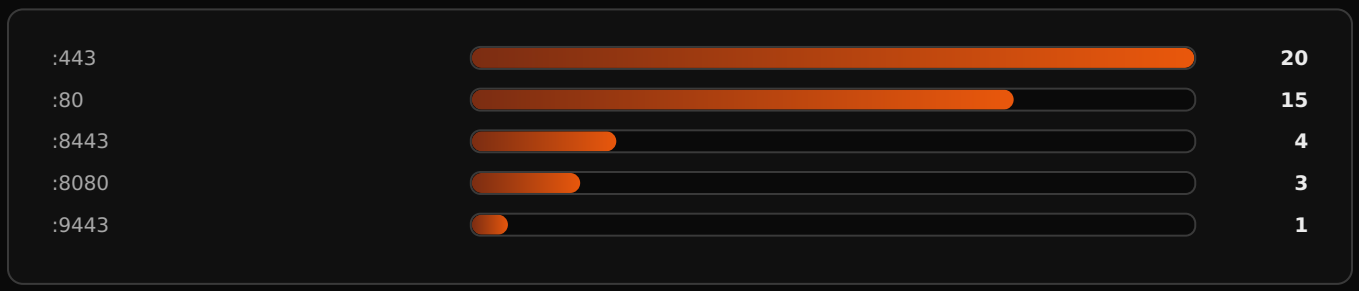
64
ACEPTABLE

Los puertos abiertos se detectan a través de una combinación de **inteligencia pasiva** (Shodan, Netlas y ZoomEye escanean continuamente internet y reportan puertos abiertos sin tocar el objetivo) y **escaneo activo opcional** (Nmap). Las fuentes pasivas proporcionan una cobertura amplia pero pueden reportar datos ligeramente desactualizados; el escaneo activo confirma el estado actual.

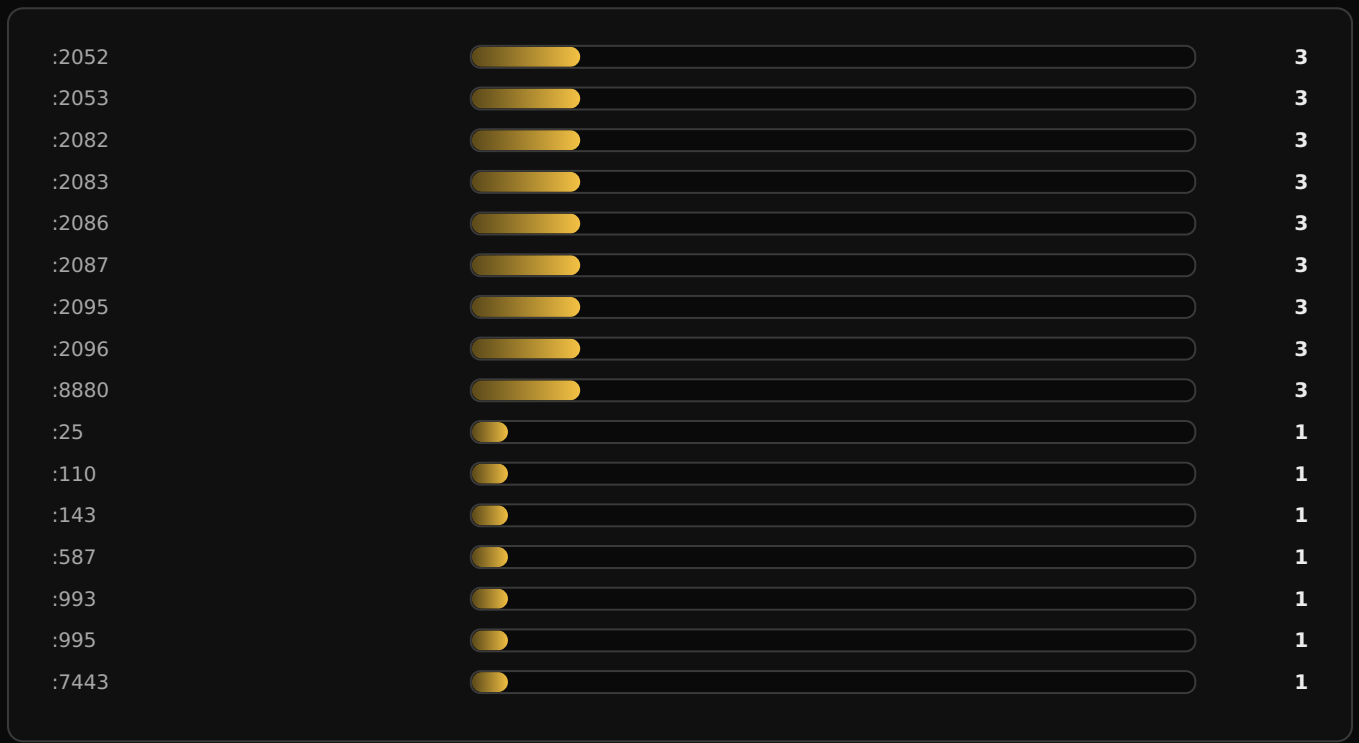
Nota de cobertura: Se habilitó el escaneo activo de puertos. Nmap verificó todos los puertos descubiertos pasivamente con detección de versión de servicio (-sV) y escaneó los 100 principales puertos TCP en hosts sin datos de puertos previos.

23 puertos únicos en **22** hosts.

Frente a la web (típico)

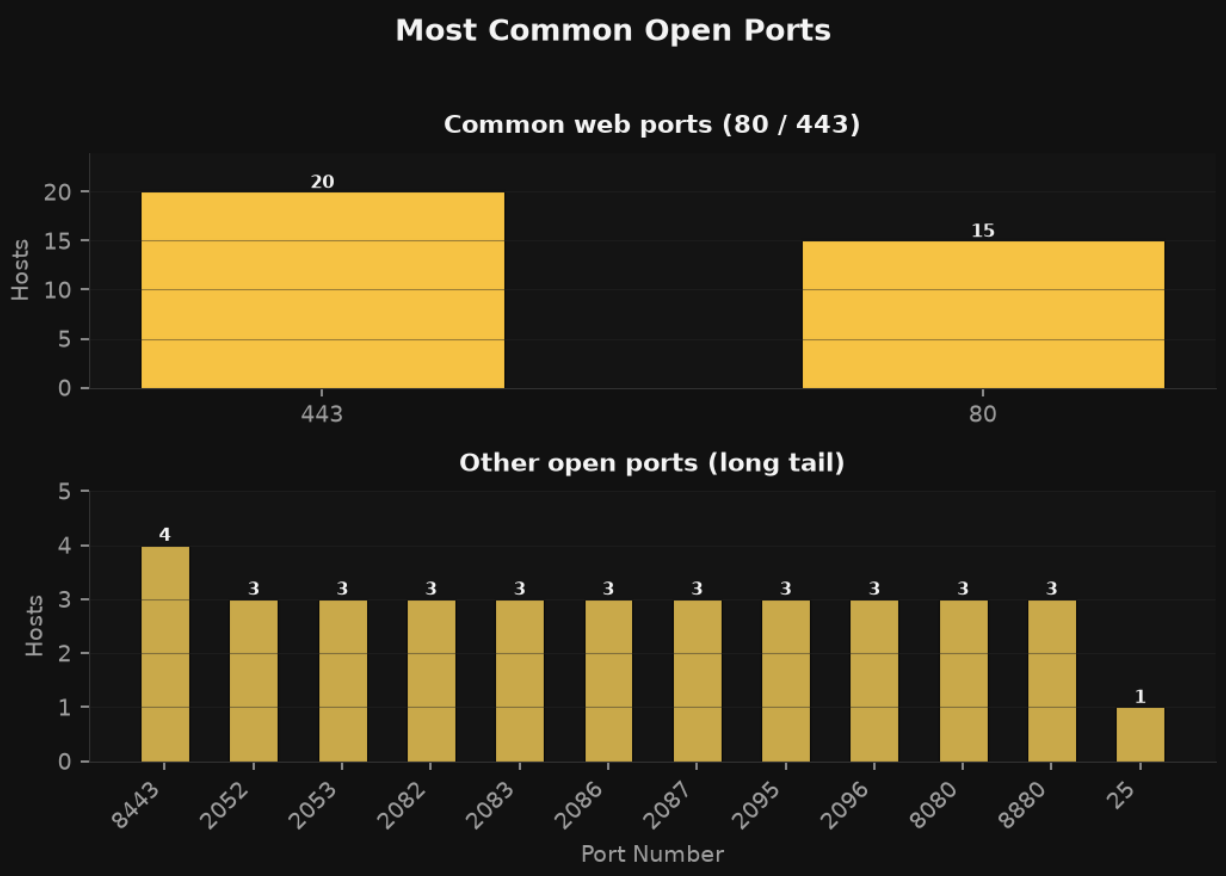


Otros servicios (cola larga)



Las barras comparten una escala (máximo conteo entre ambos grupos).

Todos los puertos — conteos principales (gráfico)



SERVICIO	HOSTS
http/proxy http de Cloudflare	21
http/nginx	12
http/Microsoft Azure Application Gateway	11
upnp/Microsoft IIS httpd	4
https/cloudflare	3
https-alt/cloudflare	3
http	3
https	3
http/Microsoft HTTPAPI httpd	3
smtp	1
envío	1
http/sfdcedge	1

Servicios de backend expuestos a Internet

Los siguientes puertos alojan **servicios de backend** (bases de datos, intermediarios de mensajes, interfaces de gestión) que **no deberían ser accesibles desde internet público**. Estos servicios están diseñados solo para acceso a la red interna; exponerlos aumenta el riesgo de exfiltración de datos, ataques de fuerza bruta y movimiento lateral. Cada uno debe estar detrás de un firewall o VPN. Para un desglose detallado por host, consulte `conjunto de datos de evidencia privada` omitido de esta muestra pública.

PUERTO	SERVICIO	RIESGO	HOSTS	RAZÓN
:8443	Plesk HTTPS	BAJO	4	Panel de administración de hosting (HTTPS)
:2082	cPanel HTTP	MEDIO	3	Panel de administración de hosting — fuerza bruta si no hay restricción de IP
:2083	cPanel HTTPS	MEDIO	3	Panel de administración de hosting — fuerza bruta si no hay restricción de IP
:2086	WHM HTTP	ALTO	3	Panel de gestión del servidor — control total del servidor si se ve comprometido
:2087	WHM HTTPS	ALTO	3	Panel de gestión del servidor — control total del servidor si se ve comprometido
:2095		MEDIO	3	Webmail — vector de fuerza bruta de credenciales

PUERTO	SERVICIO	RIESGO	HOSTS	RAZÓN
	cPanel Webmail			
:8880	Plesk HTTP	MEDIO	3	Panel de administración de hosting

Hosts con Puertos Inusuales

Los puertos inusuales son cualquier puerto TCP/UDP abierto que cae **fuera del conjunto estándar** de servicios comunes de internet (HTTP/80, HTTPS/443, SSH/22, DNS/53, SMTP/25, FTP/21, etc.). La presencia de puertos inusuales puede indicar servidores de desarrollo, interfaces de gestión, aplicaciones heredadas o servicios mal configurados — todos los cuales amplían la superficie de ataque y justifican una investigación.

HOST	IP	PUERTOS INUSUALES	RIESGO
asset-047.acmesample.com	192.0.2.178	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
asset-062.acmesample.com	192.0.2.178	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
asset-071.acmesample.com	192.0.2.179	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
portal.acmesample.com	192.0.2.137	7443, 9443, 10443	4
remote.acmesample.com	192.0.2.182	179	1

Subdominios Sensibles

Los nombres de host se analizan en busca de patrones que sugieran sistemas sensibles o de alto valor. El escáner verifica **9** patrones de nombre de host en 9 categorías: paneles de administración (admin, backend, cpanel), entornos de desarrollo/puesta en escena (dev, staging, qa, sandbox), infraestructura interna (intranet, vpn, gateway), bases de datos (mysql, redis, elastic), sistemas de monitoreo (grafana, prometheus, kibana), infraestructura CI/CD (jenkins, gitlab, docker-registry), servicios de autenticación (auth, sso, oauth), sistemas de almacenamiento/respaldo, y puntos finales de legado/migración. Estos sistemas son frecuentemente los primeros objetivos en pruebas de penetración y ataques del mundo real.

Categorías de Subdominios Sensibles

CATEGORÍA	HOSTS
Desarrollo y Pruebas	3

Hosts Sensibles (Top 9)

NOMBRE DE HOST	IP	CATEGORÍA	PUERTOS	RIESGO
asset-141.acmesample.com	192.0.2.45	Desarrollo y Pruebas	1	6
asset-168.acmesample.com	192.0.2.11	Otro	1	6
asset-059.acmesample.com	192.0.2.10	Desarrollo y Pruebas	2	1
asset-064.acmesample.com	192.0.2.78	Otro	2	1
asset-065.acmesample.com	192.0.2.66	Otro	2	1
asset-148.acmesample.com	192.0.2.43	Desarrollo y Pruebas	2	1
asset-153.acmesample.com	192.0.2.184	Otro	0	1
asset-169.acmesample.com	192.0.2.15	Otro	1	1
asset-170.acmesample.com	192.0.2.15	Otro	1	1

Superficie de Autenticación

Los puntos finales de autenticación — portales SSO, gateways VPN, paneles de firewall y sistemas de acceso remoto — son objetivos de alto valor. Comprometer un solo proveedor de identidad puede otorgar acceso a todos los servicios conectados. Esta sección identifica todos los sistemas relacionados con la autenticación en la superficie de ataque.

1	1	0
PUNTOS FINALES DE AUTENTICACIÓN	TIPOS ÚNICOS	ALTA CONFIANZA

Superficie de Autenticación por Tipo

TIPO DE SUPERFICIE	CONTEO
Puertas de enlace VPN	1

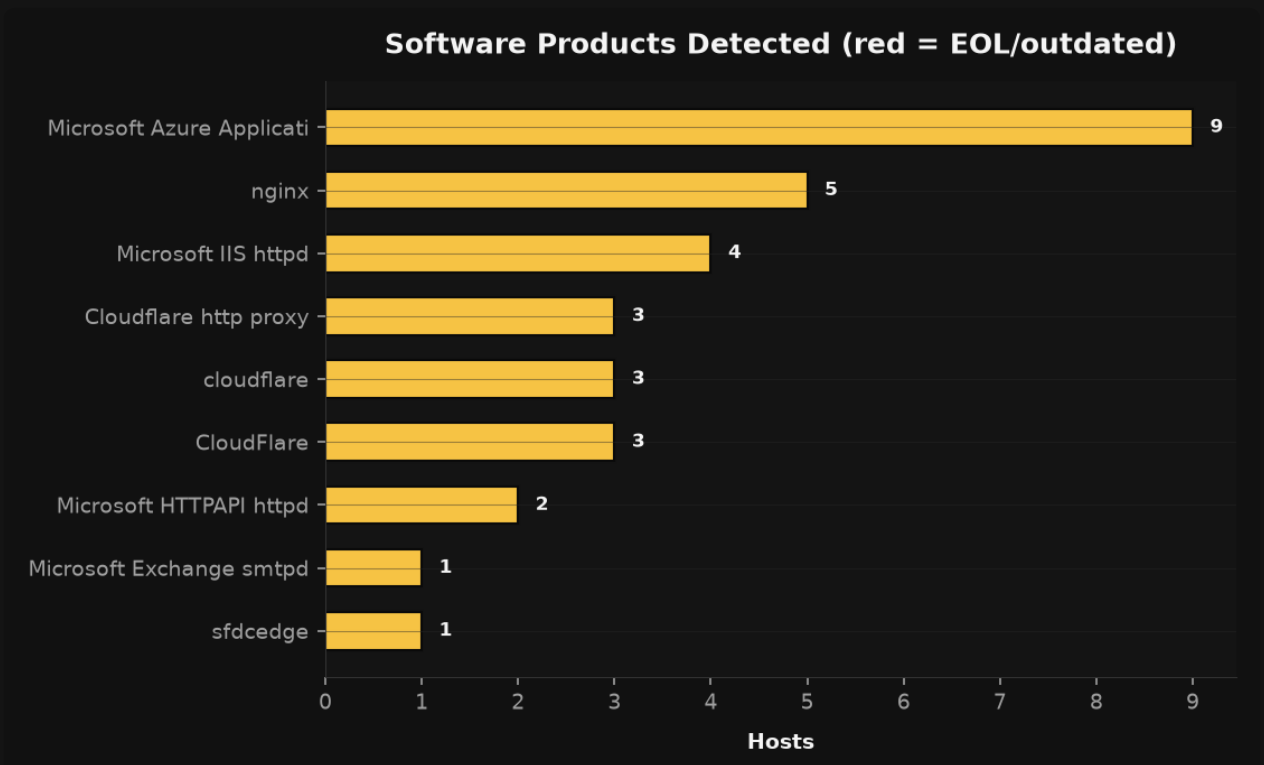
Puntos finales de autenticación detectados

NOMBRE DE HOST	IP	TIPO DE SUPERFICIE	TECNOLOGÍA	CONFIANZA
remote.acmesample.com	192.0.2.182	Puertas de enlace VPN	Patrón de nombre de host	medio

Riesgo de Versión de Software

Las versiones de software detectadas a través del escaneo de servicios de nmap y los datos CPE de Shodan se verifican contra bases de datos conocidas de fin de vida útil (EOL). El software obsoleto con CVEs conocidos representa prioridades inmediatas de parcheo.

9	0	2
PRODUCTOS ÚNICOS	FIN DE VIDA ÚTIL	CON CVES CONOCIDOS



Todos los productos detectados (Top 30)

PRODUCTO	VERSIÓN PRINCIPAL	HOSTS	CVE	ESTADO
Microsoft Azure Application Gateway	v2	9	0	ACTUAL
nginx	—	5	60	SIN VERSIÓN
Microsoft IIS httpd	10.0	4	0	ACTUAL

PRODUCTO	VERSIÓN PRINCIPAL	HOSTS	CVE	ESTADO
proxy http de Cloudflare	—	3	0	SIN VERSIÓN
cloudflare	—	3	3	SIN VERSIÓN
CloudFlare	—	3	0	SIN VERSIÓN
Microsoft HTTPAPI httpd	2.0	2	0	ACTUAL
Microsoft Exchange smtpd	—	1	0	SIN VERSIÓN
sfdcedge	—	1	0	SIN VERSIÓN

Análisis de riesgo de ruta de ataque y pivote

Esta sección identifica posibles caminos de movimiento lateral basados en el análisis de co-localización de red. Cuando los hosts que sirven diferentes funciones comerciales (por ejemplo, desarrollo y producción) comparten la misma dirección IP o subred /24, los atacantes que comprometen el sistema menos seguro pueden pivotar potencialmente al más crítico.

1
RUTAS CRÍTICAS

1
RUTAS TOTALES

0
PUNTOS ÚNICOS DE FALLO

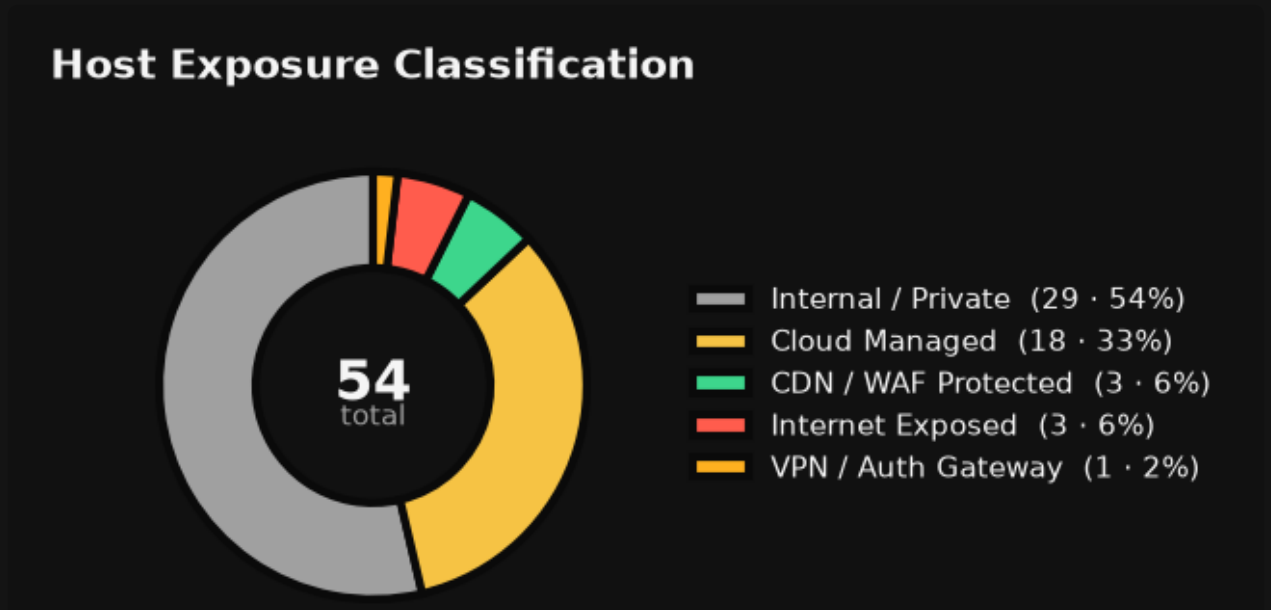
Rutas de ataque identificadas

HOST DE ORIGEN	HOST OBJETIVO	TIPO DE RUTA	PROXIMIDAD	RIESGO
asset-168.acmesample.com	www.acmesample.com	Desarrollo → Producción	MISMA IP	10

Clasificación de exposición

Cada host descubierto se clasifica por tipo de exposición basado en el proveedor de alojamiento, datos RDAP, inteligencia de Shodan y patrones de nombre de host. Esto ayuda a distinguir los sistemas expuestos directamente a Internet de aquellos protegidos por CDN/WAF, gestionados en plataformas en la nube, o servidos por proveedores de SaaS de terceros.

3 EXPUESTO A INTERNET	**3** CDN / WAF PROTEGIDO	**18** GESTIONADO EN LA NUBE
0 SAAS DE TERCEROS	**1** VPN / PUERTA DE AUTENTICACIÓN	**29** INTERNO / PRIVADO



Hosts Expuestos Directamente a Internet (Top 30)

NOMBRE DE HOST	IP	TIPO DE EXPOSICIÓN	EVIDENCIA
asset-153.acmesample.com	192.0.2.184	EXPUESTO A INTERNET	Acme Sample GmbH

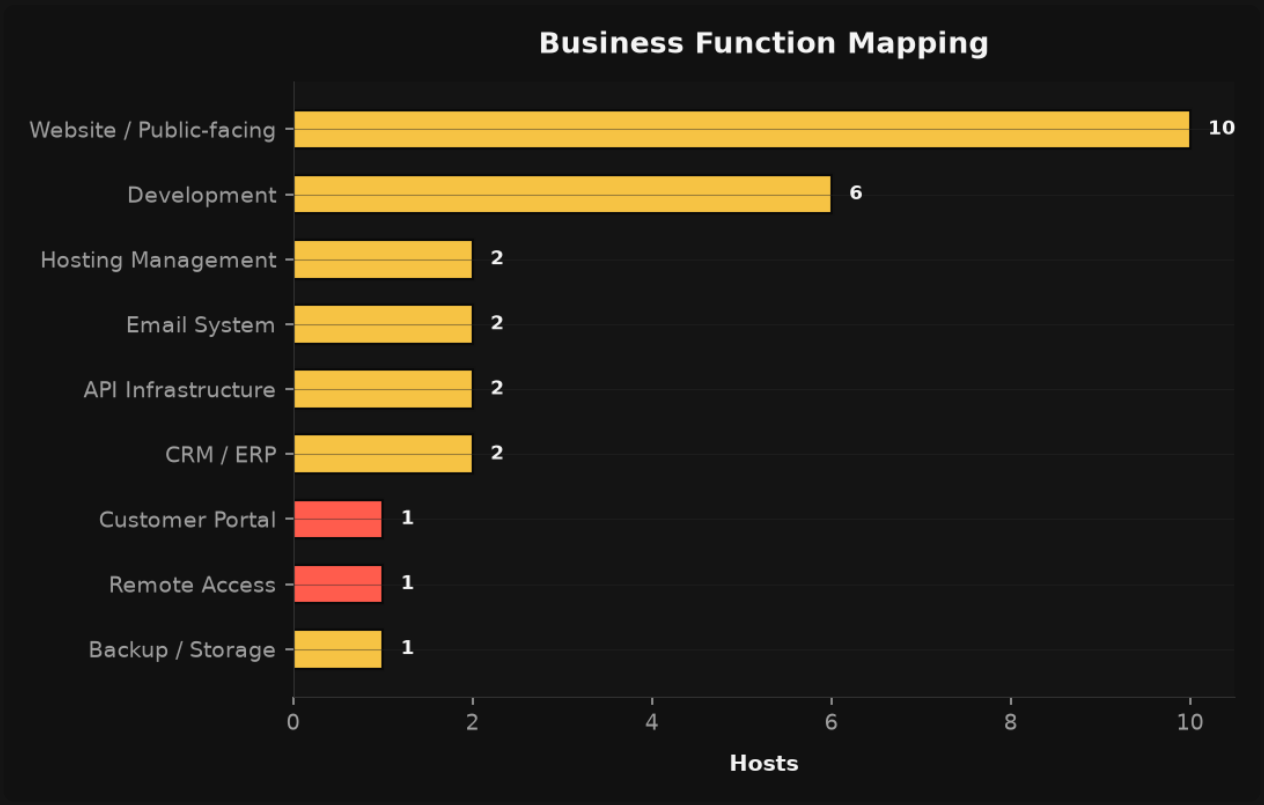
Mapeo del Impacto Empresarial

Los hosts descubiertos se mapean a funciones comerciales basadas en patrones de nombres de host. Esta clasificación ayuda a priorizar la remediación al identificar qué sistemas comerciales críticos están expuestos a Internet.

12
SISTEMAS CRÍTICOS

9
SISTEMAS DE ALTO IMPACTO

6
SISTEMAS DE IMPACTO MEDIO



Hosts críticos para el negocio

NOMBRE DE HOST	IP	FUNCIÓN EMPRESARIAL	GRAVEDAD	PUERTOS	RIESGO
asset-047.acmesample.com	192.0.2.178	Sitio web / Expuesto al público	CRÍTICO	13	6

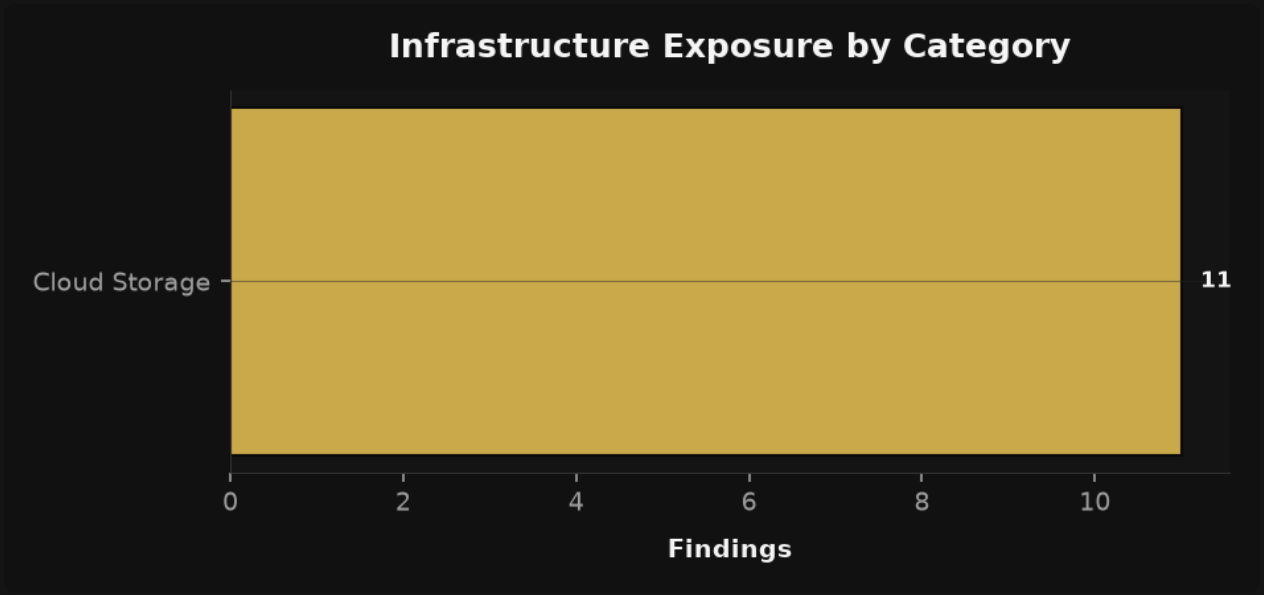
NOMBRE DE HOST	IP	FUNCIÓN EMPRESARIAL	GRAVEDAD	PUERTOS	RIESGO
asset-071.acmesample.com	192.0.2.179	Sitio web / Expuesto al público	CRÍTICO	13	6
asset-166.acmesample.com	192.0.2.75	Sitio web / Expuesto al público	CRÍTICO	8	6
asset-143.acmesample.com	192.0.2.27	Sitio web / Expuesto al público	CRÍTICO	2	5
www.acmesample.com	192.0.2.11	Sitio web / Expuesto al público	CRÍTICO	1	5
asset-188.acmesample.com	192.0.2.27	Sitio web / Expuesto al público	CRÍTICO	2	5
portal.acmesample.com	192.0.2.137	Portal del Cliente	CRÍTICO	6	4
remote.acmesample.com	192.0.2.182	Acceso Remoto	CRÍTICO	1	1
asset-049.acmesample.com	192.0.2.63	Sitio web / Expuesto al público	CRÍTICO	1	0
asset-134.acmesample.com	192.0.2.65	Sitio web / Expuesto al público	CRÍTICO	2	0
asset-146.acmesample.com	192.0.2.49	Sitio web / Expuesto al público	CRÍTICO	2	0
asset-174.acmesample.com	192.0.2.61	Sitio web / Expuesto al público	CRÍTICO	0	0
asset-062.acmesample.com	192.0.2.178	Sistema de correo electrónico	ALTO	13	6
asset-141.acmesample.com	192.0.2.45	Infraestructura API	ALTO	1	6
asset-142.acmesample.com	192.0.2.13	Infraestructura API	ALTO	1	5
asset-064.acmesample.com	192.0.2.78	CRM / ERP	ALTO	2	1
asset-065.acmesample.com	192.0.2.66	CRM / ERP	ALTO	2	1
asset-152.acmesample.com	192.0.2.33	Backup / Storage	ALTO	2	0
asset-168.acmesample.com	192.0.2.11	Desarrollo	MEDIO	1	6
asset-059.acmesample.com	192.0.2.10	Desarrollo	MEDIO	2	1
asset-148.acmesample.com	192.0.2.43	Desarrollo	MEDIO	2	1
asset-169.acmesample.com	192.0.2.15	Desarrollo	MEDIO	1	1

NOMBRE DE HOST	IP	FUNCIÓN EMPRESARIAL	GRAVEDAD	PUERTOS	RIESGO
asset-170.acmesample.com	192.0.2.15	Desarrollo	MEDIO	1	1

Exposición de Nube e Infraestructura

Componentes de infraestructura detectados a través del análisis del panel de administración, verificación de nuclei y escaneo de puertos abiertos. Bases de datos expuestas, orquestación de contenedores, pipelines de CI/CD y sistemas de monitoreo representan objetivos de alto valor para los atacantes.

11
ALMACENAMIENTO EN LA NUBE



Hallazgos de infraestructura

HOST	IP	CATEGORÍA	TIPO	FUENTE	GRAVEDAD
		Almacenamiento en la nube	11 archivos expuestos	Escaneo de Exposición en la Nube	ALTO

Filtraciones que mencionan sus servidores

Nuestra base de datos de filtraciones fue buscada para todos los nombres de host (FQDNs) confirmados descubiertos durante esta evaluación. Cuando un nombre de host de servidor aparece en los datos de filtración, significa que algún registro — como una URL, formulario de inicio de sesión o credencial de usuario — hace referencia a ese servidor. **Esto no significa necesariamente que el servidor en sí fue comprometido.** Explicaciones comunes incluyen:

- Los usuarios cuyos dispositivos fueron infectados con malware de robo tuvieron sus credenciales guardadas en el navegador para estos servidores capturadas y filtradas
- Bases de datos públicas o compilaciones de filtraciones agregadas que indexan URLs y puntos de inicio de sesión
- Servicios de terceros que hacen referencia a su infraestructura en sus datos

Los servidores con un alto número de registros de filtración de tipo credencial merecen atención inmediata, ya que indican que las credenciales de inicio de sesión para esos sistemas están circulando activamente en los canales de actores de amenaza.

Cómo se compara esto con la exposición más amplia de filtraciones: el capítulo a continuación cubre **17** registros de filtración que hacen referencia explícita a uno de sus nombres de host de servidor descubiertos. El capítulo de Exposición de Credenciales Filtradas muestra **2,038** registros de filtración que mencionan su dominio en cualquier campo (URLs, correos electrónicos, hashes, adjuntos) — una medida más amplia de cuán a menudo su organización aparece en corpora de filtraciones. El número específico del servidor es un subconjunto estricto.

1
SERVIDORES EN FILTRACIONES

26
SERVIDORES BUSCADOS

17
REGISTROS DE REFERENCIA DEL SERVIDOR
subconjunto de 2,038 a nivel de dominio

50
FUENTES DE FILTRACIÓN ÚNICAS

www.acmesample.com 192.0.2.11

17 registros **17** filtraciones **1** credenciales **1** correos electrónicos **16** URLs

log (7) url (15) hash (7) nombre (8) correo electrónico (16)

2021-08-18 — 2026-07-15 · CVSS promedio 7.0

Detalles de Filtración del Servidor

NOMBRE DE HOST	IP	REGIS-TROS	FILTRA-CIONES	CREDS	TIPOS DE DATOS PRINCIPALES	RANGO DE FECHAS
www.acmesample.com	192.0.2.11	**17**	**17**	**1**	log, url, hash	2021-08-18 — 2026-07-15

PAISAJE DE AMENAZAS

Reputación de IP e Inteligencia de Amenazas

Cada dirección IP única en la superficie de ataque se verifica contra múltiples fuentes de inteligencia de amenazas: listas de nodos de salida de TOR, la lista DROP de Spamhaus (No Rutees ni Intercambies) de redes controladas por criminales, informes de abuso de AbuseIPDB, pulsos de amenazas de AlienVault OTX y la base de datos de IP maliciosas de C99. Los resultados se almacenan en caché durante 30 días para minimizar las llamadas a la API en escaneos repetidos.

22	0	0
IPS VERIFICADAS	NODOS DE SALIDA DE TOR	EN SPAMHAUS DROP
0	**4**	**0**
INFORMES DE ABUSO	EN FUENTES DE AMENAZAS	C99 MALICIOSO

Resumen

Se revisaron 22 IPs. Marcadas: 4 en feeds de amenazas.

IPs señaladas (Top 30)

DIRECCIÓN IP	NOMBRES DE HOST	TOR	SPAMHAUS DROP	ABUSEIP-DB	OTX PULSES	C99
192.0.2.75	asset-166.acm…	—	Limpio	0	6	Limpio
192.0.2.178	asset-047.acm…	—	Limpio	0	50	Limpio
192.0.2.65	asset-134.acm…	—	Limpio	15	3	Limpio
192.0.2.179	asset-071.acm…	—	Limpio	2	50	Limpio

Análisis de Exposición de Código

82
BUENO

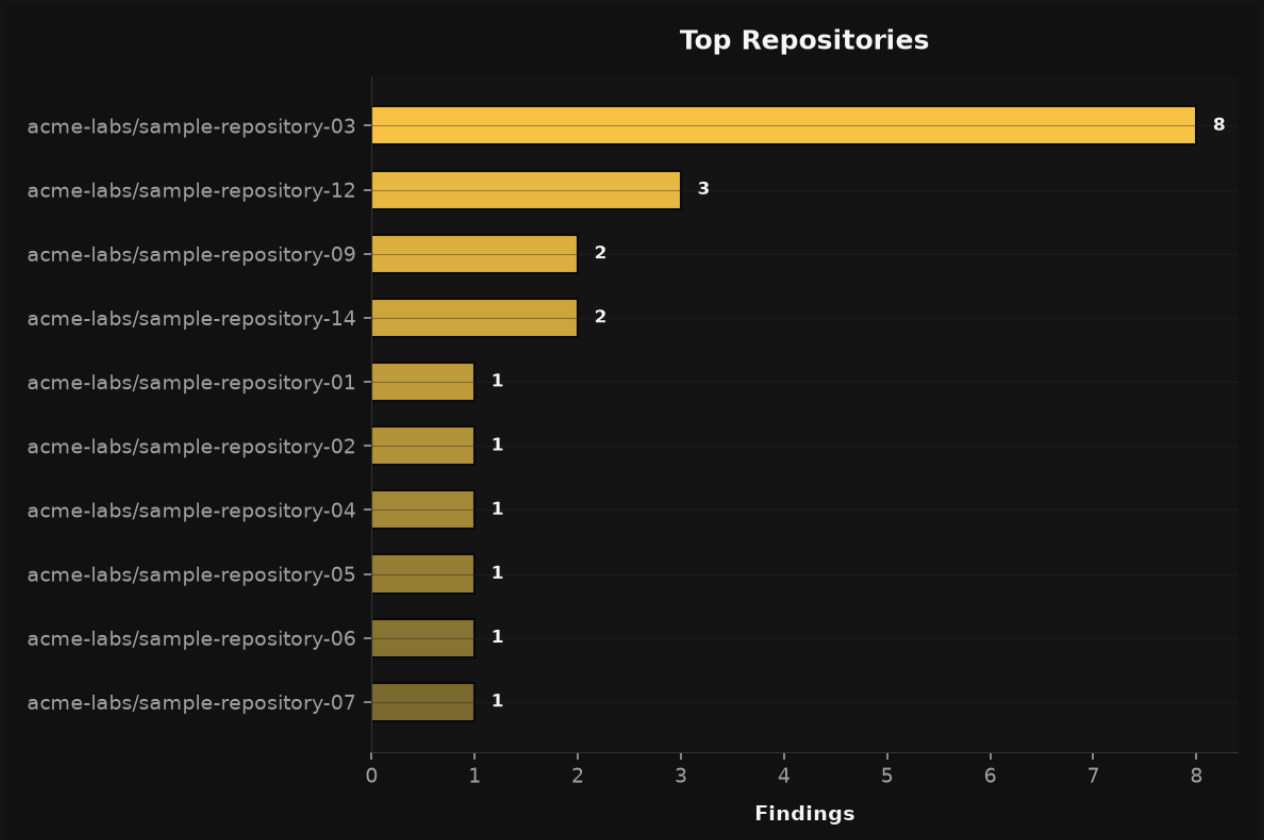
Busca en repositorios y Gists de GitHub código fuente expuesto, secretos, claves API y datos sensibles mencionando **acmesample.com**. Cada hallazgo se puntúa de 0 a 10 por riesgo mediante análisis de IA y se escanea contra más de 150 patrones de detección de secretos.

26	0	0
Total de hallazgos	Riesgo Alto (7-10)	Riesgo Medio (4-6)

26
Bajo / Info

Resumen

Se retuvieron 26 hallazgos de exposición de código anonimizados. Los nombres de los repositorios, las rutas de los archivos, los fragmentos y las identidades de terceros fueron reemplazados para esta muestra pública.



Principales Repositorios por Conteo de Hallazgos

Principales Hallazgos

acme-labs/sample-repository-01 data/conjunto de datos de evidencia privada **3/10**

```
# Extracto de codigo publico anonimizado 01
TARGET_DOMAIN = "acmesample.com"
```

Un repositorio público hizo referencia a la organización de muestra. El extracto original y las identidades de terceros fueron eliminados de este texto publicitario.

acme-labs/sample-repository-02 src/sample-config-02.py **2/10**

```
# Extracto de codigo publico anonimizado 02
TARGET_DOMAIN = "acmesample.com"
```

Un repositorio público hizo referencia a la organización de muestra. El extracto original y las identidades de terceros fueron eliminados de este texto publicitario.

acme-labs/sample-repository-03 data/conjunto de datos de evidencia privada **1/10**

```
# Extracto de codigo publico anonimizado 03
TARGET_DOMAIN = "acmesample.com"
```

Un repositorio público hizo referencia a la organización de muestra. El extracto original y las identidades de terceros fueron eliminados de este texto publicitario.

acme-labs/sample-repository-03 data/conjunto de datos de evidencia privada **1/10**

```
# Extracto de codigo publico anonimizado 04
TARGET_DOMAIN = "acmesample.com"
```

Un repositorio público hizo referencia a la organización de muestra. El extracto original y las identidades de terceros fueron eliminados de este texto publicitario.

acme-labs/sample-repository-04 src/sample-config-05.py **1/10**

```
# Extracto de codigo publico anonimizado 05
TARGET_DOMAIN = "acmesample.com"
```

Un repositorio público hizo referencia a la organización de muestra. El extracto original y las identidades de terceros fueron eliminados de este texto publicitario.

Mostrando los 5 principales de 26 hallazgos. La lista completa se omite de esta muestra pública.

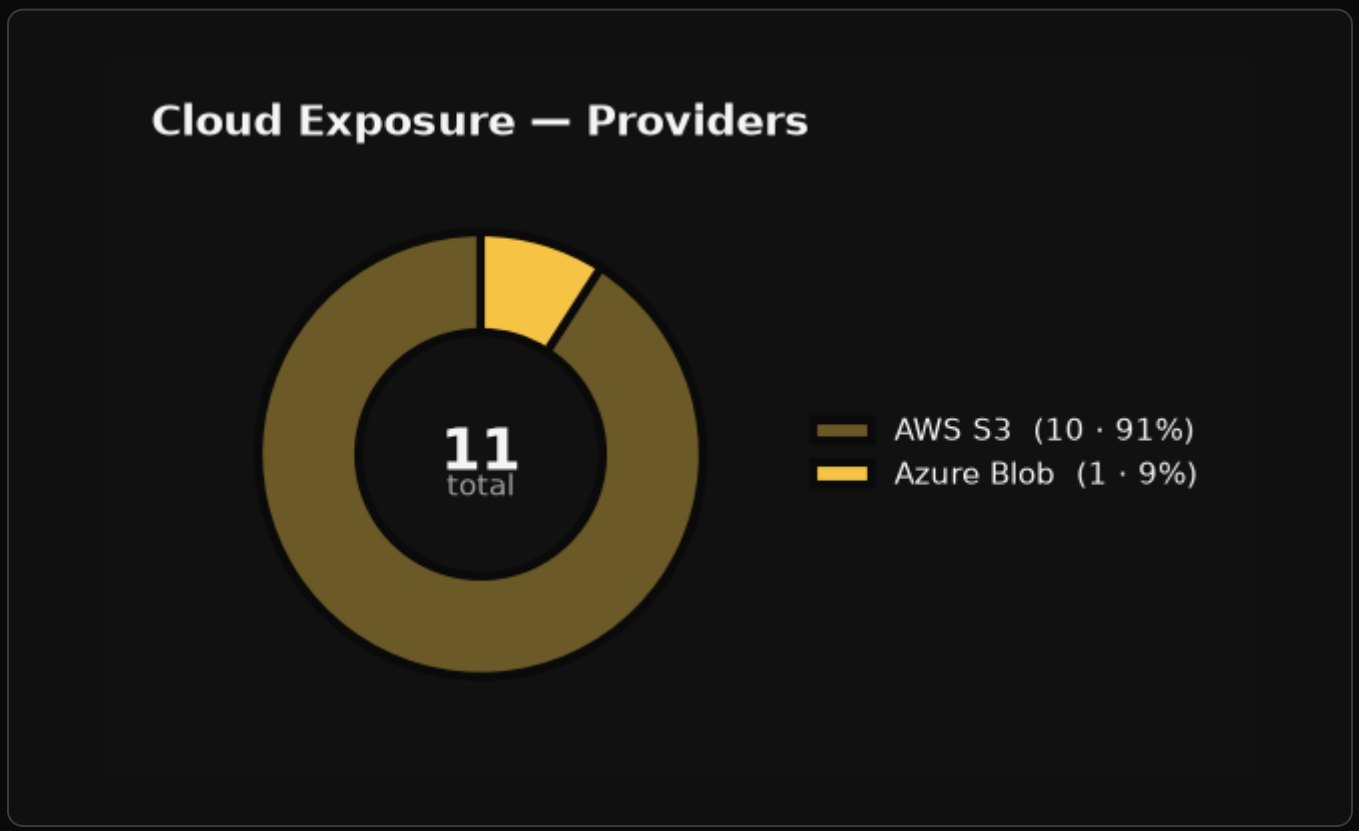
Exposición de Almacenamiento en la Nube

Archivos expuestos descubiertos en buckets de almacenamiento en la nube pública (AWS S3, Azure Blob Storage, Google Cloud Storage) que coinciden con el nombre de la organización.

11	7	2
ARCHIVOS ENCONTRADOS	ARCHIVOS SENSIBLES	PROVEEDORES DE NUBE

Resumen

11 archivos encontrados en buckets de almacenamiento en la nube expuestos. 7 son sensibles a la seguridad (configuraciones, bases de datos, archivos, scripts). Proveedores de nube: AWS S3 (10), Azure Blob (1).



Archivos expuestos

URL DEL ARCHIVO	PROVEEDOR	EXT	TAMAÑO	SENSIBLE
https://sample-storage.invalid/redacted/sample-file-001.dat	AWS S3	pdf	**9214.4 KB**	—
https://sample-storage.invalid/redacted/sample-file-002.dat	AWS S3	pdf	**596.6 KB**	—
https://sample-storage.invalid/redacted/sample-file-003.dat	Azure Blob	pdf	**570.0 KB**	—
https://sample-storage.invalid/redacted/sample-file-004.dat	AWS S3	pdf	**223.1 KB**	—
https://sample-storage.invalid/redacted/sample-file-005.dat	AWS S3	xml	**0.3 KB**	ARCHIVO DE DATOS/ CONFIGURACIÓN
https://sample-storage.invalid/redacted/sample-file-006.dat	AWS S3	xml	**0.3 KB**	ARCHIVO DE DATOS/ CONFIGURACIÓN
https://sample-storage.invalid/redacted/sample-file-007.dat	AWS S3	xml	**0.3 KB**	ARCHIVO DE DATOS/ CONFIGURACIÓN
https://sample-storage.invalid/redacted/sample-file-008.dat	AWS S3	emb	**85.5 KB**	
https://sample-storage.invalid/redacted/sample-file-009.dat	AWS S3	emb	**84.5 KB**	
https://sample-storage.invalid/redacted/sample-file-010.dat	AWS S3		**81,1 KB**	
https://sample-storage.invalid/redacted/sample-file-011.dat	AWS S3	info	**0.2 KB**	

Exposición de URL acortada

URLs acortadas (goo.gl, bit.ly, tinyurl, ow.ly, etc.) que apuntan o hacen referencia al dominio escaneado. Estos enlaces revelan recursos internos compartidos externamente, documentos sensibles y posibles dominios de suplantación de marca.

3,000	0	1	0
TOTAL DE ENLACES	RECURSOS INTERNOS	ARCHIVOS NO HTML	DOMINIOS DE PHISHING

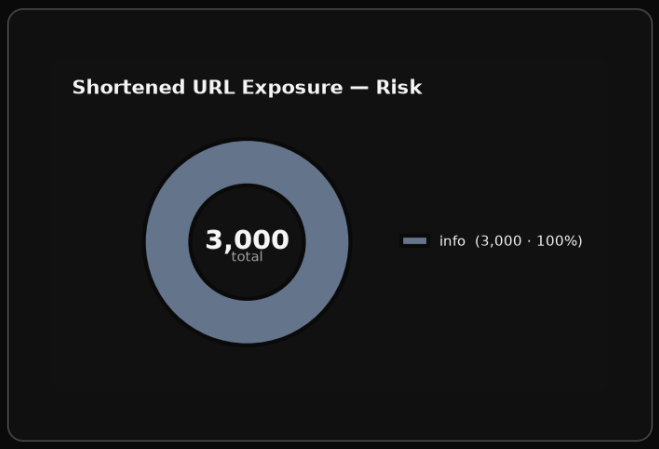
Los contadores de encabezado resumen cada enlace válido devuelto y clasificado por el escaneo. Los registros detallados de hallazgos se persisten para un máximo de **5,000 enlaces**. Las tablas PDF son muestras de presentación más pequeñas, y `conjunto de datos de evidencia privada` contiene solo los hallazgos persistentes que permanecen después de cualquier exclusión de informe; las filas más allá del límite de persistencia no están disponibles como evidencia detallada.

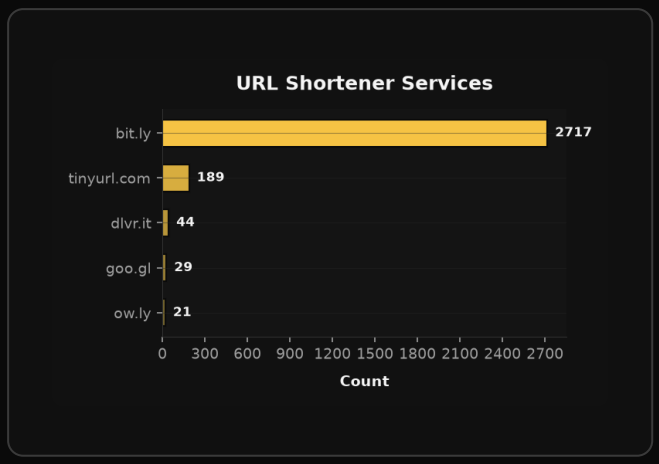
Resumen

Se encontraron 3000 URLs acortadas que apuntan o hacen referencia a acmesample.com. 1 apunta directamente a recursos del dominio propio. 1 enlace a archivos no HTML (PDFs, documentos, archivos).

Por qué las URL acortadas son importantes para la seguridad
Los acortadores de URL ocultan el verdadero destino, lo que los hace populares para compartir recursos internos (SharePoint, Google Drive, Dropbox). Cuando los empleados comparten enlaces acortados públicamente, estos recursos internos se vuelven descubribles. Los tokens de acceso incrustados en las URL acortadas pueden seguir siendo válidos, otorgando acceso directo a archivos corporativos. Las campañas de phishing también utilizan URL acortadas con dominios similares a marcas para eludir los filtros de correo electrónico.

1	2,999
ENLACES DE DOMINIO PROPIO	REFERENCIAS DE TERCEROS


Shortened URL Exposure — Risk
3,000
total
info (3,000 · 100%)


URL Shortener Services
bit.ly
tinyurl.com
dlvr.it
goo.gl
ow.ly
2717
189
44
29
21
0 300 600 900 1200 1500 1800 2100 2400 2700
Count

Exposición en redes sociales

80
BUENO

Análisis de exposición de marca en YouTube, Twitter/X, Facebook, LinkedIn, Reddit y plataformas sociales indexadas por Google. Los hallazgos incluyen detección de suplantación de marca, perfiles falsos y menciones de phishing.

192
TOTAL DE HALLAZGOS

3
PERFILES OFICIALES

1
RIESGOS DE SUPLANTACIÓN

0
MENCIONES DE PHISHING

192 menciones en redes sociales analizadas en **7** plataformas. **3** clasificadas como riesgos accionables, **112** como coincidencias de marcas no relacionadas, **80** como oficiales o benignas.

Canales oficiales verificados

Perfiles oficiales de redes sociales identificados a partir de los metadatos del sitio web de la empresa, registros DNS, datos estructurados y escaneo de redes sociales. Estos están **excluidos** de los hallazgos de suplantación a continuación.

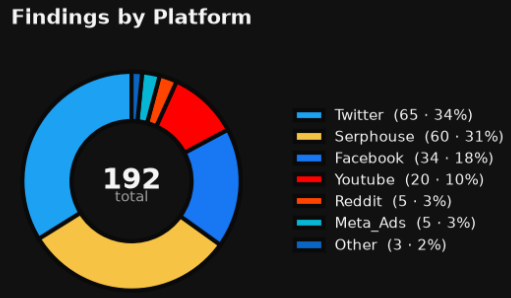
PLATA-FORMA	MANEJAR / NOMBRE	URL	FUENTE
Twitter	Acme Sample GmbH	https://x.com/Acme Sample GmbH	Metadatos de la empresa
Facebook	Acme Sample GmbH	https://facebook.com/Acme Sample G...	Metadatos de la empresa
Linkedin	empresa/Acme Sample GmbH	https://linkedin.com/company/Acme S...	Metadatos de la empresa
Youtube	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account-...	Escaneo de redes sociales

Resumen

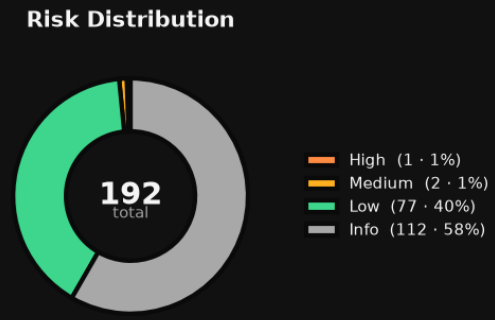
Se encontraron 192 menciones en redes sociales para acmesample.com en 7 plataformas. Se encontraron 3 perfiles oficiales confirmados. Se detectaron 1 riesgos potenciales de suplantación de marca.

Evaluación de Riesgo de IA

Los hallazgos consisten principalmente en menciones benignas y discusiones sobre productos de Acme Sample GmbH en varias plataformas. No hay indicios de suplantación crítica o de alto riesgo o actividad fraudulenta relacionada con la marca.



Hallazgos por plataforma



Distribución de riesgo

Publicidad Potencialmente Fraudulenta

Análisis de anuncios pagados en LinkedIn Ad Library, Meta Ad Library y TikTok Ad Library que mencionan la marca. Los anuncios se clasifican por nivel de amenaza: anuncios de phishing/estafa que suplantan la marca, anuncios de competidores que explotan el nombre de la marca y anuncios legítimos/neutros. La confianza en la clasificación indica cuán seguro está el AI sobre la categoría asignada.

> Clasificación retenida de la evaluación de origen; se eliminaron los detalles de la cuenta identificables.

Los 5 anuncios parecen ser legítimos u oficiales. No se detectaron anuncios fraudulentos.

PLATAFORMA	ANUNCIANTE	CONTENIDO DEL ANUNCIO	RIESGO	CERTEZA	CLASIFICACIÓN
Meta	Cuenta de Muestra 670	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas. — Mención pública de muestra de Acme Sample GmbH; cuenta original y...	BAJO	85%	Clasificación retenida de la evaluación de origen;...
Meta	Cuenta de Muestra 670	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas. — Mención pública de muestra de Acme Sample GmbH; cuenta original y...	BAJO	85%	Clasificación retenida de la evaluación de origen;...
Meta	Cuenta de Muestra 304	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas. — Mención pública de muestra de Acme Sample GmbH; cuenta original y...	BAJO	85%	Clasificación retenida de la evaluación de origen;...
Meta	Cuenta de Muestra 011	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas. — Mención pública de muestra de Acme Sample GmbH; cuenta original y...	INFO	—	Clasificación retenida de la evaluación de origen;...
Meta	Cuenta de muestra 789	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas. — Mención pública de muestra de Acme Sample GmbH; cuenta original y...	INFO	—	Clasificación retenida de la evaluación de origen;...

Twitter — 65 hallazgos (2 medio, 55 bajo, 8 info)

RIESGO	TÍTULO	URL	RAZÓN
MEDIO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
MEDIO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...

Mostrando los 5 principales de 65. Se omitieron pruebas completas de esta muestra pública.

Serphouse — 60 hallazgos (60 info)

RIESGO	TÍTULO	URL	RAZÓN
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...

Mostrando los 5 principales de 60. Se omitieron pruebas completas de esta muestra pública.

Facebook — 34 hallazgos (1 alto, 33 info)

Todos los enlaces son relativos a `https://social.invalid/`

RIESGO	TÍTULO	URL	RAZÓN
ALTO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0008	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0241	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0243	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0245	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0247	Clasificación retenida de la evaluación de origen; se eliminaron los...

Mostrando los 5 principales de 34. Se omitieron pruebas completas de esta muestra pública.

Youtube — 20 hallazgos (19 bajo, 1 info)

Todos los enlaces son relativos a `https://social.invalid/`

RIESGO	TÍTULO	URL	RAZÓN
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0016	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0020	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0024	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0028	Clasificación retenida de la evaluación de origen; se eliminaron los...
BAJO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0032	Clasificación retenida de la evaluación de origen; se eliminaron los...

Mostrando los 5 principales de 20. Evidencia completa omitida de esta muestra pública.

Reddit — 5 hallazgos (5 info)

RIESGO	TÍTULO	URL	RAZÓN
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	https://social.invalid/sample-account...	Clasificación retenida de la evaluación de origen; se eliminaron los...

Linkedin — 3 hallazgos (3 info)

Todos los enlaces son relativos a `https://social.invalid/`

RIESGO	TÍTULO	URL	RAZÓN
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0307	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0309	Clasificación retenida de la evaluación de origen; se eliminaron los...
INFO	Mención pública de muestra de Acme Sample GmbH; cuenta original y copia anonimizadas.	../sample-account-0313	Clasificación retenida de la evaluación de origen; se eliminaron los...

Análisis de Typosquatting de dominio

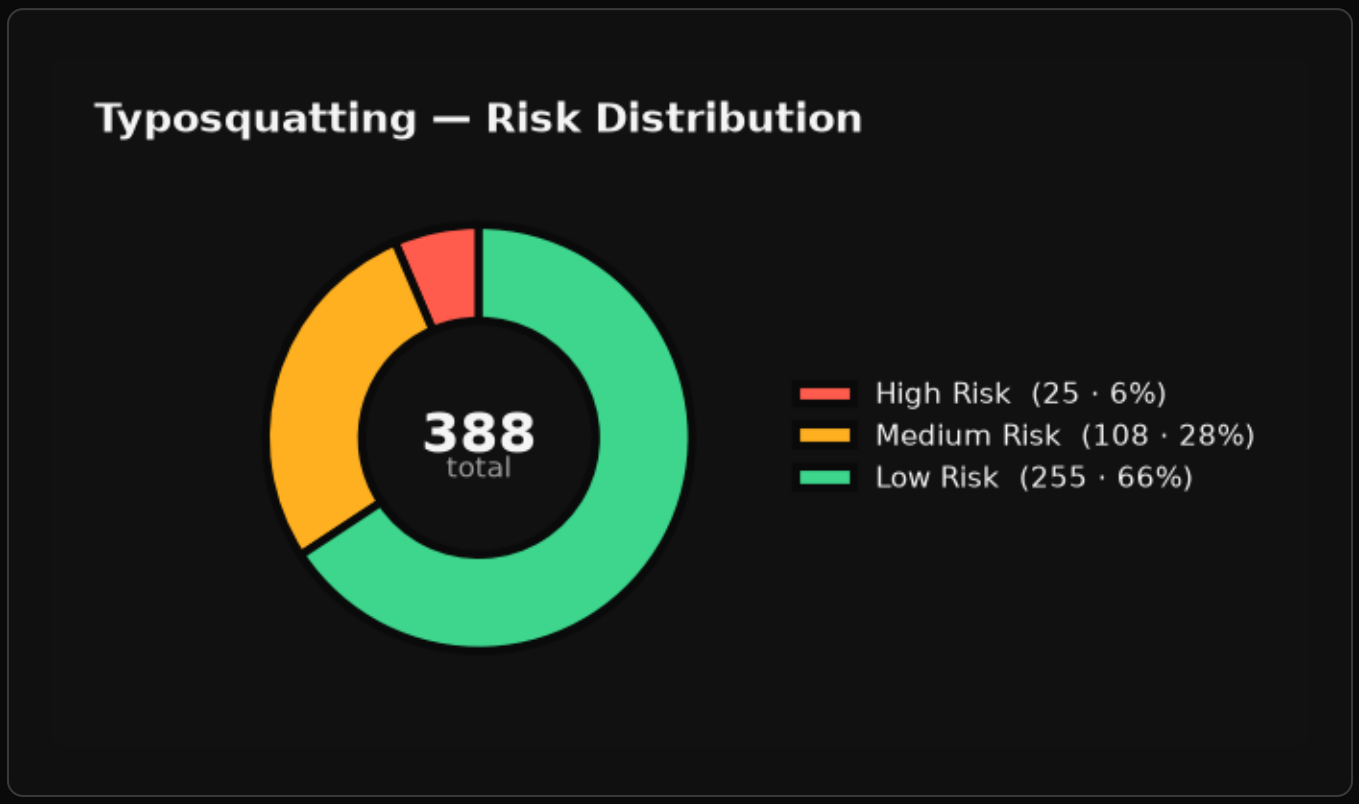
50
POBRE

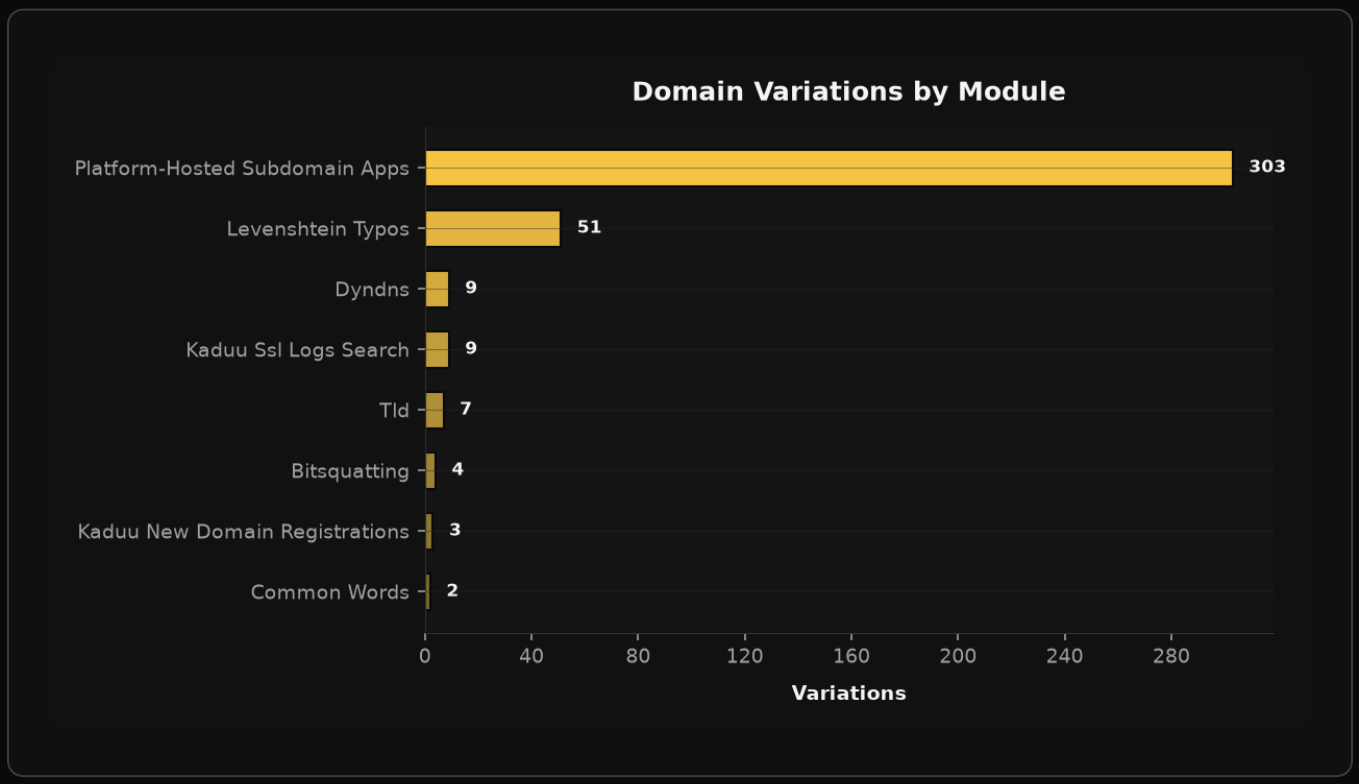
Análisis de variación de dominio impulsado por SpoofGuard. Genera typosquats, homoglyphs, bit-squatting, intercambios de TLD y otros dominios similares, luego verifica cada uno por registros DNS, servidores web activos e indicadores de phishing.

96,461	372	362	0
VARIACIONES TOTALES	CON REGISTROS DNS	SERVIDORES WEB ACTIVOS	PHISHING DETECTADO

Resumen

SpoofGuard generó 96,461 variaciones similares para acmesample.com. 372 se resuelven en DNS; después de verificaciones de actividad, 59 realmente sirven contenido activo (el resto son subdominios de plataforma aparcados, no reclamados, o devuelven errores). 26 están clasificados como alto riesgo — confirmación de suplantación de marca/visual, un golpe de phishing, o un veredicto malicioso de visión GPT. 109 más son de riesgo medio (similares activos aún no confirmados como maliciosos).





Variaciones de dominio — Riesgo alto y medio

Mostrando los 30 principales de 100 entradas. Datos completos en `conjunto de datos de evidencia privada` omitido de esta muestra pública.

DOMINIO	MÓDULO	REGISTRO A	WEB	RELEVAN-CIA	RIESGO
acmesampl3.com	Errores tipográficos de Levenshtein	192.0.2.114	–	ALTO	ALTO
acme-sample-login.net	Errores tipográficos de Levenshtein	192.0.2.187	–	ALTO	ALTO
acmesample.dnsdyn.net	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.now-dns.org	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.dynserv.org	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.tcp4.me	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.dnsup.net	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.mypi.co	Dyndns	192.0.2.1	–	ALTO	ALTO
acmesample.cn	Tld	–	–	ALTO	ALTO
acmesample-alert-010.inv…	Errores tipográficos de Levenshtein	–	–	ALTO	ALTO
acmesample-alert-011.inv…	Errores tipográficos de Levenshtein	–	–	ALTO	ALTO
acmesample-alert-012.inv…	Errores tipográficos de Levenshtein	–	–	ALTO	ALTO
acmesample-alert-013.inv…	Errores tipográficos de Levenshtein	–	–	ALTO	ALTO
acmesample-alert-014.inv…	Errores tipográficos de Levenshtein	–	–	ALTO	ALTO
acmesamplelp.com	Kaduu Nuevas Registraciones de Dominio	–	–	ALTO	ALTO
acmesample.biz	Tld	–	–	MEDIO	ALTO
teaacmesample.com	Kaduu Nuevas Registraciones de Dominio	–	–	MEDIO	ALTO

DOMINIO	MÓDULO	REGISTRO A	WEB	RELEVAN-CIA	RIESGO
acmesamplestore.com	Palabras comunes	–	–	MEDIO	ALTO
sample-redirect-01.invalid	Tld	192.0.2.93	HTTPS	ALTO	MEDIO
sample-redirect-02.invalid	Tld	192.0.2.93	HTTPS	ALTO	MEDIO
sample-redirect-03.invalid	Tld	192.0.2.93	HTTPS	ALTO	MEDIO
sample-redirect-04.invalid	Errores tipográficos de Levenshtein	192.0.2.69	HTTPS	ALTO	MEDIO
sample-redirect-05.invalid	Dyndns	192.0.2.55	HTTPS	ALTO	MEDIO
sample-redirect-06.invalid	Búsqueda de Registros Ssl de Kaduu	192.0.2.71	HTTPS	ALTO	MEDIO
sample-redirect-07.invalid	Búsqueda de Registros Ssl de Kaduu	192.0.2.168	HTTPS	ALTO	MEDIO
sample-redirect-08.invalid	Búsqueda de Registros Ssl de Kaduu	192.0.2.77	HTTPS	ALTO	MEDIO
sample-redirect-09.invalid	Búsqueda de Registros Ssl de Kaduu	192.0.2.79	HTTPS	ALTO	MEDIO
sample-redirect-10.invalid	Kaduu Nuevas Registraciones de Dominio	192.0.2.93	HTTPS	ALTO	MEDIO
sample-redirect-11.invalid	Búsqueda de Registros Ssl de Kaduu	192.0.2.149	HTTPS	ALTO	MEDIO
sample-redirect-12.invalid	Palabras comunes	192.0.2.167	HTTP	ALTO	MEDIO

Visual Verdict — Los 2 Look-Alikes Más Sospechosos

Se abrió un verdadero navegador sin cabeza en cada parecido para renderizar la página (capturando redirecciones impulsadas por JS a páginas de estacionamiento, redes publicitarias o sitios de suplantación que las simples sondas HTTP no detectan). GPT-4o analizó cada captura de pantalla junto con la cadena de redirección y el contexto de la organización objetivo para producir un veredicto.

Mostrando los 2 imitadores de mayor prioridad. **Veredictos, URLs finales, cadenas de redirección y enlaces de captura de pantalla para TODOS los 10 imitadores enriquecidos están en `conjunto de datos de evidencia privada`** (columnas: `Final URL`, `Verdict Category`, `Verdict Severity`, `Verdict One-Liner`, `Verdict Evidence`, `Local Screenshot URL`).



l-acmesample.art.pl

RIESGO MEDIO **REDIRIGIR A NO RELACIONADO** **MEDIO**

Redirige a un subdominio no relacionado, lo que plantea un riesgo de desviar a los usuarios del sitio previsto.

Redirección JS → https://sample-redirect-13.invalid/

- La URL final es sample-redirect-13.invalid, no relacionada con Acme Sample GmbH.
- Se detectó una redirección entre hosts impulsada por JS.



acmesample-alert-043.invalid

RIESGO MEDIO **REDIRIGIR A NO RELACIONADO** **BAJO**

El dominio redirige a un negocio legítimo no relacionado, sin representar una amenaza para Acme Sample GmbH.

Redirección JS → https://sample-redirect-17.invalid/

- La URL final es sample-redirect-17.invalid, no relacionada con Acme Sample GmbH.
- El título de la página indica una industria diferente: Fabricación de tarjetas.

Exposición Cibernética del Actor de Amenaza

79
BUENO

Los actores de amenaza — más notablemente **grupos de ransomware** — son operaciones cibernéticas organizadas que comprometen organizaciones, encriptan sus datos y extorsionan pagos por su liberación. Muchos operan bajo un modelo de “Ransomware-as-a-Service” (RaaS) y mantienen sitios de filtración públicos donde enumeran a las víctimas que se niegan a pagar. Estos grupos escanean continuamente Internet en busca de objetivos vulnerables, haciendo que cada servicio expuesto sea un posible punto de entrada.

Este capítulo evalúa la exposición de su organización a estos actores de amenaza en función de la industria, geografía, tamaño de la organización y datos de inteligencia de ransomware disponibles públicamente.

PRESIÓN DE OBJETIVO
MEDIO
Exposición general a amenazas

EXPOSICIÓN POR SECTOR
MEDIO
riesgo impulsado por la industria

MODIFICADOR DE PAÍS
Aumenta el riesgo
Modificador basado en geografía

SU ORGANIZACIÓN
Riesgo Alto
País (#1) e industria (#20) ambos en el top 20 de objetivos

Amenazas Más Relevantes

Ransomware	ALTO	El ransomware es una amenaza significativa para los sectores manufactureros debido a posibles interrupciones operativas.
Ataques a la Cadena de Suministro	MEDIO	La dependencia de cadenas de suministro complejas en la fabricación industrial la hace vulnerable a ataques de la cadena de suministro.
Filtraciones de Datos	MEDIO	Las filtraciones de datos pueden exponer información sensible, impactando las operaciones comerciales y la reputación.

Costos estimados de un ataque exitoso de ransomware

Basado en el tamaño de la organización identificado de **501-1000 empleados** (Mercado Medio Superior), la investigación de la industria estima el siguiente impacto financiero si la organización fuera golpeada por un ataque de ransomware:

MÉTRICA	VALOR ESTIMADO
Costo Total Promedio	**$1,300,000**
Costo Promedio de Recuperación	$1,300,000
Ransom Promedio Pagado	$300,000
Tasa de pago estimada	40%

Basado en bandas de 251–1,000 empleados de Sophos; el rescate varía según la gravedad del impacto en lugar del tamaño de la organización por sí solo.

Fuentes: Sophos State of Ransomware 2025; Coveware Quarterly Report; Verizon DBIR

Por qué la monitorización de la superficie de ataque puede prevenir ataques de ransomware

Los atacantes a menudo explotan primero las superficies de ataque expuestas.

Los ciberdelincuentes escanean continuamente internet en busca de servicios abiertos, contraseñas débiles y credenciales filtradas. Si algo está expuesto, será encontrado — a menudo automáticamente.

Dos ejemplos típicos:

- **RDP/VPN Expuestos:** los atacantes encuentran un servicio de acceso remoto abierto e inician sesión utilizando fuerza bruta o credenciales robadas.
- **Reutilización de contraseñas:** las credenciales filtradas se reutilizan para acceder a sistemas corporativos a través de stuffing de contraseñas.

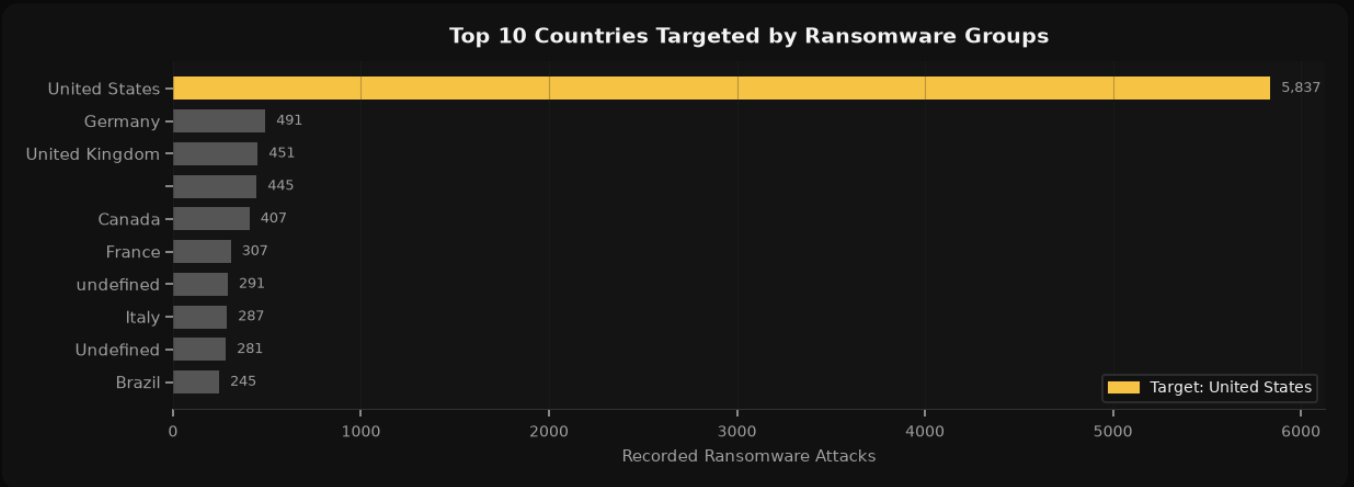
El monitoreo de la superficie de ataque es crítico porque te muestra lo que los atacantes ya pueden ver y explotar. Si reduces esa visibilidad — cerrando puertos, asegurando el acceso y detectando credenciales comprometidas — reduces significativamente el riesgo de ransomware antes de que comience.

¿Está su organización listada en un sitio web de actores de amenaza?

Los grupos de ransomware operan sitios de “filtración” públicos en la dark web donde enumeran organizaciones que han sido comprometidas y se han negado a pagar. Estar listado en un sitio así es un fuerte indicador de que la organización ha sufrido una filtración y que datos sensibles pueden haber sido exfiltrados. Nuestra base de datos monitorea continuamente estos sitios y actualmente rastrea **12,989** registros de víctimas en todos los grupos de ransomware conocidos.

No se encontraron coincidencias. Después de analizar **12,989** registros de víctimas de ransomware, su organización no aparece en ningún sitio de filtración de actores de amenaza conocidos. Este es un indicador positivo, pero no garantiza que la organización nunca haya sido objetivo — no todos los incidentes son divulgados públicamente.

Panorama de Amenazas de Ransomware



PAÍSES ATACADOS

179

Con incidentes de ransomware registrados

MÁS ATACADOS

Estados Unidos

5,837 ataques registrados

INDUSTRIA PRINCIPAL

Manufactura industrial

1.744 ataques

Estados Unidos ocupa el **#1** a nivel mundial por ataques de ransomware con **5,837** incidentes registrados. El sector de **Manufactura Industrial** ocupa el **#20** entre las industrias objetivo con **158** ataques. Como uno de los cinco países más atacados, las organizaciones con sede en Estados Unidos enfrentan una exposición significativamente elevada al ransomware.

Vulnerabilidades Explotadas por Ransomware

La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) mantiene el catálogo de **Vulnerabilidades Conocidas Explotadas (KEV)** — una lista curada de vulnerabilidades que han sido utilizadas activamente en ataques del mundo real. Muchas entradas están explícitamente etiquetadas como utilizadas en campañas de ransomware. Cruzamos cada CVE detectada en sus activos y cada producto / proveedor en su pila tecnológica contra el catálogo actual (1,709 entradas). Cuando existe una coincidencia, su entorno está ejecutando software con un camino de explotación conocido y armado que se documenta que los operadores de ransomware explotan.

⚠ **3 coincidencias contra el catálogo de Vulnerabilidades Conocidas Explotadas de CISA.**

3 co-ocurrencias de producto / proveedor (su stack ejecuta el producto; la exposición específica de la versión debe ser verificada).

Productos en Su Stack con Vulnerabilidades Listadas en KEV

Estos productos aparecen en su pila tecnológica detectada y tienen una o más entradas de CISA-KEV. Si su versión específica desplegada está expuesta depende del nivel de parche; trate cada fila como “verifique su versión”.

PROVEEDOR / PRODUCTO	HOSTS	CVE DE KEV	PRINCIPALES CVES	EVIDENCIA	¿RANSOMWARE?
Microsoft — Exchange	1	1	CVE-2021-42321	POTENCIAL	CONOCIDO · VERSIÓN NO CONFIRMADA
Microsoft — Microsoft	16	1	CVE-2026-42897	POTENCIAL	DESCONOCIDO
Microsoft — Word	2	4	CVE-2006-2492, CVE-2012-2539, CVE-2014-1761 …	POTENCIAL	DESCONOCIDO

Apéndice — Otros Dominios Descubiertos (No Escaneados)

Este escaneo fue configurado en modo **SOLO DOMINIO**, por lo que solo se evaluó el objetivo enviado **acmesample.com**. Durante la exploración observamos el 1 dominio registrado adicional a continuación — co-alojado en la misma infraestructura, compartiendo servidores de nombres, o surgido a través de WHOIS inverso. No fueron **escanados**. Para incluir ellos, vuelva a ejecutar el escaneo con un modo de dominio más amplio.

DOMINIO	HOSTS VISTOS	MÉTODO DE DESCUBRIMIENTO
192.0.2.68	**1**	Enumeración de subdominios

Apéndice A — Inventario Completo de Activos

54 hosts ordenados por puntuación de riesgo (se muestran los 200 principales). Datos completos para todos los hosts están disponibles en `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

FQDN	IP	RIESGO	PUERTOS	FUENTE	CVE
asset-047.acmesample.com	192.0.2.178	6	80, 443, 2052, 2053, 2082…	crt	21
asset-062.acmesample.com	192.0.2.178	6	80, 443, 2052, 2053, 2082…	crt	21
asset-071.acmesample.com	192.0.2.179	6	80, 443, 2052, 2053, 2082…	crt	21
asset-141.acmesample.com	192.0.2.45	6	443	crt	9
asset-166.acmesample.com	192.0.2.75	6	25, 80, 110, 143, 443…	crt	40
asset-168.acmesample.com	192.0.2.11	6	443	crt	13
asset-142.acmesample.com	192.0.2.13	5	443	crt	9
asset-143.acmesample.com	192.0.2.27	5	80, 443	centrodesubdominios	49
www.acmesample.com	192.0.2.11	5	443	crt	13
asset-188.acmesample.com	192.0.2.27	5	80, 443	centrodesubdominios	49
portal.acmesample.com	192.0.2.137	4	80, 443, 7443, 8443, 9443…	dns_bruteforce	0
asset-055.acmesample.com	–	1	—	crt	0
asset-059.acmesample.com	192.0.2.10	1	80, 443	crt	0
asset-060.acmesample.com	–	1	—	centrodesubdominios	0
asset-064.acmesample.com	192.0.2.78	1	80, 443	dns_bruteforce	0
asset-065.acmesample.com	192.0.2.66	1	80, 443	dns_bruteforce	0
asset-148.acmesample.com	192.0.2.43	1	80, 443	crt	0
remote.acmesample.com	192.0.2.182	1	179	crt	0
asset-153.acmesample.com	192.0.2.184	1	—	centrodesubdominios	0

FQDN	IP	RIESGO	PUERTOS	FUENTE	CVE
asset-158.acmesample.com	–	1	—	crt	0
asset-157.acmesample.com	–	1	—	crt	0
asset-156.acmesample.com	–	1	—	crt	0
asset-169.acmesample.com	192.0.2.15	1	443	crt	0
asset-170.acmesample.com	192.0.2.15	1	443	crt	0
asset-175.acmesample.com	–	1	—	waybackengine	0
asset-183.acmesample.com	–	1	—	centrodesubdominios	0
asset-186.acmesample.com	–	1	—	centrodesubdominios	0
asset-190.acmesample.com	–	1	—	centrodesubdominios	0
asset-192.acmesample.com	–	1	—	centrodesubdominios	0
asset-193.acmesample.com	–	1	—	centrodesubdominios	0
asset-194.acmesample.com	–	1	—	centrodesubdominios	0
asset-195.acmesample.com	–	1	—	centrodesubdominios	0
asset-048.acmesample.com	–	0	—	centrodesubdominios	0
asset-049.acmesample.com	192.0.2.63	0	80	crt	0
asset-050.acmesample.com	192.0.2.154	0	—	crt	0
asset-051.acmesample.com	–	0	—	centrodesubdominios	0
asset-056.acmesample.com	–	0	—	crt	0
asset-057.acmesample.com	–	0	—	crt	0
asset-063.acmesample.com	–	0	—	centrodesubdominios	0
mail.acmesample.com	–	0	—	crt	0
asset-134.acmesample.com	192.0.2.65	0	80, 443	dns_bruteforce	0
asset-144.acmesample.com	–	0	—	waybackengine	0
asset-146.acmesample.com	192.0.2.49	0	80, 443	crt	0
asset-152.acmesample.com	192.0.2.33	0	80, 443	dns_bruteforce	0
asset-165.acmesample.com	–	0	—	crt	0

FQDN	IP	RIESGO	PUERTOS	FUENTE	CVE
asset-174.acmesample.com	192.0.2.61	0	—	dns_bruteforce	0
asset-180.acmesample.com	–	0	—	centrodesubdominios	0
asset-181.acmesample.com	–	0	—	crt	0
asset-182.acmesample.com	–	0	—	centrodesubdominios	0
asset-184.acmesample.com	–	0	—	centrodesubdominios	0
asset-185.acmesample.com	–	0	—	centrodesubdominios	0
asset-187.acmesample.com	–	0	—	centrodesubdominios	0
asset-189.acmesample.com	–	0	—	centrodesubdominios	0
www.remote.acmesample.com	–	0	—	crt	0

Todos los 39 chequeos de DNS están disponibles en `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

Apéndice B — Lista Completa de Vulnerabilidades

Todos los 103 CVEs únicos y 399 hallazgos de verificación. Los datos completos están disponibles en `conjunto de datos de evidencia privada`, `conjunto de datos de evidencia privada`, y `conjunto de datos de evidencia privada` omitidos de esta muestra pública.

Todos los CVEs (103)

CVE	CVSS	FUENTES	HOSTS	CONFIANZA
CVE-2004-0847	9.8	CVEDB	4	producto coincidente no verificado
CVE-2006-1364	7.5	CVEDB	4	producto coincidente no verificado
CVE-2003-0768	6.8	CVEDB	4	producto coincidente no verificado
CVE-2005-1664	6.4	CVEDB	4	producto coincidente no verificado
CVE-2005-1665	5.0	CVEDB	4	producto coincidente no verificado
CVE-2005-2224	5.0	CVEDB	4	producto coincidente no verificado
CVE-2005-0452	4.3	CVEDB	4	producto coincidente no verificado
CVE-2010-2084	4.3	CVEDB	4	producto coincidente no verificado
CVE-2010-2088	4.3	CVEDB	4	producto coincidente no verificado
CVE-2015-3105	10.0	CVEDB	3	producto coincidente no verificado
CVE-2014-0515	10.0	CVEDB	3	producto coincidente no verificado
CVE-2010-0425	10.0	CVEDB	3	producto coincidente no verificado
CVE-2015-0359	10.0	CVEDB	3	producto coincidente no verificado
CVE-2009-3555	9.8	CVEDB	3	producto coincidente no verificado
CVE-2024-4577	9.8	CVEDB	3	producto coincidente no verificado
CVE-2022-47986	9.8	CVEDB	3	producto coincidente no verificado
CVE-2015-3113	9.8	CVEDB	3	producto coincidente no verificado
CVE-2014-0497	9.8	CVEDB	3	producto coincidente no verificado
CVE-2015-5119	9.8	CVEDB	3	producto coincidente no verificado

CVE	CVSS	FUENTES	HOSTS	CONFIANZA
CVE-2015-0313	9.8	CVEDB	3	producto coincidente no verificado
CVE-2013-0625	9.8	CVEDB	3	producto coincidente no verificado
CVE-2015-5122	9.8	CVEDB	3	producto coincidente no verificado
CVE-2025-34028	9.3	CVEDB	3	producto coincidente no verificado
CVE-2014-0569	9.3	CVEDB	3	producto coincidente no verificado
CVE-2011-0611	8.8	CVEDB	3	producto coincidente no verificado
CVE-2025-8088	8.4	CVEDB	3	producto coincidente no verificado
CVE-2024-0212	8.1	CVEDB	3	producto coincidente no verificado
CVE-2019-0232	8.1	CVEDB	3	producto coincidente no verificado
CVE-2017-12615	8.1	CVEDB	3	producto coincidente no verificado
CVE-2012-0754	8.1	CVEDB	3	producto coincidente no verificado
CVE-2021-34833	7.8	CVEDB	3	producto coincidente no verificado
CVE-2021-23017	7.7	CVEDB	3	producto coincidente no verificado
CVE-2023-44487	7.5	CVEDB	3	producto coincidente no verificado
CVE-2013-2028	7.5	CVEDB	3	producto coincidente no verificado
CVE-2016-0742	7.5	CVEDB	3	producto coincidente no verificado
CVE-2019-9513	7.5	CVEDB	3	producto coincidente no verificado
CVE-2009-2629	7.5	CVEDB	3	producto coincidente no verificado
CVE-2013-4547	7.5	CVEDB	3	producto coincidente no verificado
CVE-2017-7529	7.5	CVEDB	3	producto coincidente no verificado
CVE-2019-9511	7.5	CVEDB	3	producto coincidente no verificado
CVE-2019-9516	7.5	CVEDB	3	producto coincidente no verificado
CVE-2016-4450	7.5	CVEDB	3	producto coincidente no verificado
CVE-2009-4487	6.8	CVEDB	3	producto coincidente no verificado
CVE-2013-2070	5.8	CVEDB	3	producto coincidente no verificado
CVE-2018-16843	5.3	CVEDB	3	producto coincidente no verificado

CVE	CVSS	FUENTES	HOSTS	CONFIANZA
CVE-2019-20372	5.3	CVEDB	3	producto coincidente no verificado
CVE-2018-16844	5.3	CVEDB	3	producto coincidente no verificado
CVE-2010-2263	5.0	CVEDB	3	producto coincidente no verificado
CVE-2010-2266	5.0	CVEDB	3	producto coincidente no verificado
CVE-2009-3898	4.9	CVEDB	3	producto coincidente no verificado
CVE-2010-3972	10.0	CVEDB	2	producto coincidente no verificado
CVE-2007-2815	10.0	CVEDB	2	producto coincidente no verificado
CVE-2017-7269	9.8	CVEDB	2	producto coincidente no verificado
CVE-2005-4360	7.8	CVEDB	2	producto coincidente no verificado
CVE-2009-1122	7.5	CVEDB	2	producto coincidente no verificado
CVE-2009-1535	7.5	CVEDB	2	producto coincidente no verificado
CVE-2002-0079	7.5	CVEDB	2	producto coincidente no verificado
CVE-2000-0884	7.5	CVEDB	2	producto coincidente no verificado
CVE-2000-0886	7.5	CVEDB	2	producto coincidente no verificado
CVE-2001-0506	7.2	CVEDB	2	producto coincidente no verificado
CVE-2006-0026	6.5	CVEDB	2	producto coincidente no verificado
CVE-2010-3332	6.4	CVEDB	2	producto coincidente no verificado
CVE-2003-0718	5.0	CVEDB	2	producto coincidente no verificado
CVE-2000-0778	5.0	CVEDB	2	producto coincidente no verificado
CVE-2009-2521	5.0	CVEDB	2	producto coincidente no verificado
CVE-2000-0246	5.0	CVEDB	2	producto coincidente no verificado
CVE-2001-1243	5.0	CVEDB	2	producto coincidente no verificado
CVE-2000-0630	5.0	CVEDB	2	producto coincidente no verificado
CVE-2001-0151	5.0	CVEDB	2	producto coincidente no verificado
CVE-2000-0649	2.6	CVEDB	2	producto coincidente no verificado
CVE-2021-34473	9.1	CVEDB	1	producto coincidente no verificado

CVE	CVSS	FUENTES	HOSTS	CONFIANZA
CVE-2021-26855	9.1	CVEDB	1	producto coincidente no verificado
CVE-2020-17132	9.1	CVEDB	1	producto coincidente no verificado
CVE-2021-34523	9.0	CVEDB	1	producto coincidente no verificado
CVE-2020-0688	8.8	CVEDB	1	producto coincidente no verificado
CVE-2022-41040	8.8	CVEDB	1	producto coincidente no verificado
CVE-2021-42321	8.8	CVEDB	1	producto coincidente no verificado
CVE-2021-28482	8.8	CVEDB	1	producto coincidente no verificado
CVE-2023-21707	8.8	CVEDB	1	producto coincidente no verificado
CVE-2023-32031	8.8	CVEDB	1	producto coincidente no verificado
CVE-2022-41082	8.0	CVEDB	1	producto coincidente no verificado
CVE-2023-36035	8.0	CVEDB	1	producto coincidente no verificado
CVE-2023-36744	8.0	CVEDB	1	producto coincidente no verificado
CVE-2021-27065	7.8	CVEDB	1	producto coincidente no verificado
CVE-2021-26857	7.8	CVEDB	1	producto coincidente no verificado
CVE-2021-26858	7.8	CVEDB	1	producto coincidente no verificado
CVE-2021-33766	7.3	CVEDB	1	producto coincidente no verificado
CVE-2021-31207	6.6	CVEDB	1	producto coincidente no verificado
CVE-2021-41349	6.5	CVEDB	1	producto coincidente no verificado
CVE-2023-36777	5.7	CVEDB	1	producto coincidente no verificado
CVE-2026-6722	9.5	Shodan	2	inteligencia pasiva
CVE-2026-17543	8.1	Shodan	2	inteligencia pasiva
CVE-2013-2220	7.5	Shodan	2	inteligencia pasiva
CVE-2025-14179	7.4	Shodan	2	inteligencia pasiva
CVE-2026-6735	7.3	Shodan	2	inteligencia pasiva
CVE-2026-7258	6.3	Shodan	2	inteligencia pasiva
CVE-2026-7261	6.3	Shodan	2	inteligencia pasiva

CVE	CVSS	FUENTES	HOSTS	CONFIANZA
CVE-2026-7568	6.3	Shodan	2	inteligencia pasiva
CVE-2026-14355	5.6	Shodan	2	inteligencia pasiva
CVE-2026-7260	5.4	Shodan	2	inteligencia pasiva

... y 3 CVEs más (ver conjunto de datos de evidencia privada omitido de esta muestra pública)

Todos los Hallazgos de Nuclei por Plantilla

PLANTILLA	GRAVEDAD	CONTEO
Detección de suites de cifrado débiles	BAJO	2
Divulgación de versión de AspNet - Detectar	INFO	2
Política de Seguridad de Contenidos "script-src" Wildcard Detectado	INFO	2
Detección de TLS Obsoleto	INFO	1
Encabezados de seguridad HTTP faltantes	INFO	215
Configuración OpenID de Keycloak - Detectar	INFO	2
Detección de versión de Microsoft IIS	INFO	2
Certificado SSL no coincidente	INFO	5
Falta Cookie SameSite Strict	INFO	27
Falta de integridad de subrecursos	INFO	2
Microsoft Exchange Autodiscover - Exposición de Dominio Local	INFO	1
Detectar proveedor OpenID Connect	INFO	2
Protocolo POP3 - Detectar	INFO	1
Detección SMTP	INFO	2
Nombres DNS SSL	INFO	28
Detectar Emisor de Certificado SSL	INFO	28
Versión de TLS - Detectar	INFO	28
Detección de WAF	INFO	31

PLANTILLA	GRAVEDAD	CONTEO
Política de Seguridad de Contenido Débil - Detectar	INFO	4
Certificado TLS Wildcard	INFO	14

Apéndice D — Metodología y Definiciones

Puntuación de Riesgo (0–10)

PUNTUACIÓN	NIVEL	DESCRIPCIÓN
0	NINGUNO	No se resolvió IP, no hay puertos, no hay indicadores
1–3	BAJO	IP resuelta, puertos web estándar, nombres de subdominio sensibles
4–6	MEDIO	Múltiples puertos abiertos, servicios no estándar, puntos finales de desarrollo
7–8	ALTO	Muchos puertos abiertos, servicios de transferencia de archivos, software conocido como vulnerable
9–10	CRÍTICO	Paneles de administración expuestos, bases de datos no protegidas, vulnerabilidades críticas

Niveles de Inteligencia CVE

FUENTE	MÉTODO	CONFIANZA
Nmap vulners	Detección de versión de servicio activa + búsqueda en vulners.com	ALTO
Shodan / Netlas / ZoomEye	Inteligencia pasiva de escaneos a nivel de internet	MEDIO
CVEDB	Coincidencia de nombre de producto a través de la API gratuita CVEDB de Shodan	BAJO

Fases del Pipeline

FASE	DESCRIPCIÓN
Análisis de Objetivos	Resolver la IP del dominio objetivo y recopilar datos de registro WHOIS.
Descubrimiento de Subdominio	Descubra todos los subdominios utilizando 17 fuentes de OSINT: transparencia de certificados, motores de búsqueda, bases de datos DNS, credenciales filtradas, DNS inverso (PTR) y rastreo web.
Mapeo de Infraestructura	Identificar alojamiento compartido, rangos de IP propiedad del objetivo y dominios registrados por la misma entidad. Utiliza APIs REST de RIR (RIPE, ARIN) y identificación de empresas mejorada por GPT.
Inteligencia Pasiva	Recopilar datos de puertos, servicios, tecnología y vulnerabilidades de Shodan, ZoomEye, Netlas y CVEDB sin tocar el objetivo.
Escaneo Activo	Confirme los puertos abiertos e identifique las versiones exactas de los servicios utilizando Nmap. Los puertos descubiertos de forma pasiva se verifican primero.
Análisis y Correlación	Analizar vecindarios de red, comparar certificados SSL, verificar CVEs contra versiones de servicio y calcular puntuaciones de riesgo.
Verificación de Nuclei	Ejecutar más de 4,000 plantillas de núcleos curados contra los hosts descubiertos para detectar paneles expuestos, configuraciones incorrectas, huellas tecnológicas y verificaciones de CVE seguras. Solo se activa cuando active_vuln_scan=true.
Inteligencia de Amenazas	Consulta automatizada de bases de datos de filtraciones, motores de búsqueda de almacenamiento en la nube y análisis de banners pasivos para identificar filtraciones de credenciales, archivos en la nube expuestos e interfaces de gestión.
Finalización	Finalizar resultados, deduplicar hallazgos, materializar contadores de enriquecimiento y hacer el informe completo disponible.

Descripciones de módulos

Explicación detallada de cada módulo que se ejecutó durante este escaneo.

MÓDULO	DESCRIPCIÓN
paneles_admin	Detecta paneles de administración e interfaces de gestión a partir de datos de banner existentes de Shodan, Netlas y nmap. Más de 55 firmas incluyendo WordPress, Jenkins, Grafana, phpMyAdmin, Fortinet y más. Cero solicitudes HTTP adicionales.

MÓDULO	DESCRIPCIÓN
exposición_nube	Busca archivos expuestos en almacenamiento en la nube pública (AWS S3, Azure Blob, GCS) que coincidan con el nombre de la organización. Filtra el ruido (imágenes, fuentes) y clasifica archivos sensibles (configs, bases de datos, archivos, scripts, claves).
exposición_código	Busca en repositorios y Gists de GitHub código fuente expuesto, secretos, claves API y datos sensibles que mencionan el dominio objetivo. Utiliza la API de Codewatcher con coincidencia de frase exacta. Cada hallazgo es puntuado de 0 a 10 por GPT según el riesgo y escaneado contra más de 150 patrones regex de detección de secretos (reglas de gitleaks).
exposición_credenciales	Consulta bases de datos de filtraciones y agregadores de registros de robos para credenciales de correo electrónico corporativo encontradas en servicios externos. Devuelve registros con puntuación de riesgo, deduplicados y con contraseñas redactadas.
dns_asm	Evaluación integral de la superficie de ataque DNS: 37 verificaciones que cubren la salud de la delegación (presencia de NS, SOA, delegación débil, consistencia), exposición DNS (transferencia de zona AXFR, recursión abierta, divulgación de versión CHAOS), autenticación de correo electrónico (SPF, DMARC, DKIM), salud de entrega de correo (resolución MX, alineación PTR) y resiliencia (diversidad de NS, DNSSEC, CAA, TCP/53, EDNS, IPv6). Prueba el dominio raíz, cada NS autoritativo y cada host MX. Produce calificaciones de gravedad por hallazgo y puntajes de postura en 5 dimensiones.
exposición_dominio	Descubrimiento de dominios por Reverse-IP a través de C99 ip2domains para cada IP de cliente con servicios web (puerto 80/443), seguido de verificación de expiración de dominios RDAP para todos los dominios descubiertos. Identifica dominios olvidados, expirados o que están a punto de expirar que podrían ser secuestrados para phishing o suplantación de marca. Los resultados se almacenan en caché durante 30 días por IP para minimizar el uso de la API.
email_auth	Evalúa la postura de seguridad del correo electrónico basada en DNS: análisis del registro SPF (presencia, sintaxis, fuerza de la política, desbordamiento de inclusión, exposición de terceros, riesgo de comodín), evaluación de la política DMARC (presencia, nivel de aplicación, porcentaje, alineación, informes), descubrimiento del selector DKIM con análisis de fuerza de clave (40 selectores comunes) y validación del registro MX (resolución, detección de IP privada, identificación del proveedor). También verifica la presencia de BIMI, MTA-STS y TLS-RPT. Puntuación:

MÓDULO	DESCRIPCIÓN
	basada en 100 con deducciones por penalización y límites para configuraciones críticas incorrectas.
enumeración_de_correo	Descubre correos electrónicos de empleados a través de bases de datos de filtraciones (API Central) y fuentes públicas de internet (Hunter.io). Fusiona ambos conjuntos de datos y puntúa cada correo electrónico en tres dimensiones de riesgo: exposición a filtraciones, riesgo de senioridad/posición y visibilidad pública.
enriquecimiento_dns_resolver	Resuelve cada subdominio descubierto a su dirección IPv4 a través de una búsqueda de registro A de DNS. Los subdominios sin una IP se marcan como no resolubles (probablemente desactivados o solo internos).
enriquecimiento_registro_mx	Descubre registros de intercambio de correo (MX) para cada dominio, revelando la infraestructura de correo electrónico incluyendo proveedores de nube (Google Workspace, Microsoft 365) y servidores de correo autoalojados.
enriquecimiento_netlas	Consulta Netlas para cada IP y dominio de host para identificar tecnologías de software, marcos, detalles del servidor web y puertos abiertos. Realiza 2 llamadas a la API por host (info de IP + info de dominio). Resultados almacenados en caché durante 7 días.
enriquecimiento_descubrimiento_de_red	Analiza IPs vecinas en la misma subred /24. Para cada vecino, verifica certificados SSL (coincidencia de CN/SAN, coincidencia de emisor), registros PTR, comparación de ASN, huellas digitales de contenido HTTP y colocación en subred /24. Asigna puntuaciones de confianza (ALTA/MEDIA/BAJA) basadas en el número y la fuerza de las señales coincidentes.
enriquecimiento_nmap	Escaneo activo de puertos TCP con objetivo inteligente. Cuando fuentes pasivas (Shodan/Netlas/ZoomEye) han identificado puertos, nmap realiza detección de versión dirigida (-sV) con scripts NSE (vulners para búsqueda de CVE, ssl-enum-ciphers para auditoría de TLS). Cuando no se conocen puertos, realiza un escaneo rápido (-F, los 100 puertos principales). El escaneo UDP está deshabilitado (requiere root). Los resultados incluyen nombre del servicio, producto, versión y salida del script por puerto.
enrichment_shodan	Consultas a Shodan para cada IP de host para obtener puertos abiertos, banners de servicio, detalles del certificado SSL, identificadores CPE, detección del sistema operativo e información de la organización. Resultados almacenados en caché durante 7 días por IP.
enriquecimiento_whois	

MÓDULO	DESCRIPCIÓN
	Recupera datos de registro WHOIS para cada subdominio descubierto, incluyendo registrador, fechas de creación/expiración y detalles del registrante.
enrichment_zoomeye	Consulta ZoomEye para cada IP de host para obtener cadenas de certificados SSL, huellas digitales de dispositivos, información de puertos y referencias de vulnerabilidades. Resultados almacenados en caché durante 7 días.
inteligencia_entidad	Utiliza GPT con búsqueda web para identificar la organización detrás del dominio, clasificar su tipo, tamaño, industria y países de operación, luego evaluar la presión de ciberataques basada en el sector y la geografía. También obtiene datos actuales sobre el panorama de amenazas de ransomware.
people_intelligence	Identifica objetivos de alto valor (C-suite, VPs, Directores) a través de RocketReach y enriquece los datos de la empresa (redes sociales oficiales, stack tecnológico) a través de Hunter.io. Produce perfiles de empleados con detalles de contacto, historial laboral y enlaces sociales para el contexto de la superficie de ataque.
exposición_phishing	Busca en bases de datos de inteligencia de phishing (PhishTank, OpenPhish) a través de la API Central para campañas de phishing conocidas que apuntan al nombre de marca de la organización. Identifica URLs de phishing activas e históricas que suplantan al objetivo.
exposición_de_filtración_de_servidor	Busca en la base de datos de filtraciones de Kaduu todos los FQDNs descubiertos para identificar servidores mencionados en filtraciones de credenciales, registros de stealer y filtraciones de datos. Los resultados se atribuyen por host con clasificación de tipo de datos.
exposición_acortador	Busca URLs acortadas (goo.gl, bit.ly, tinyurl, ow.ly, etc.) que apuntan o hacen referencia al dominio escaneado. Detecta recursos corporativos internos compartidos a través de acortadores, archivos sensibles (PDFs, hojas de cálculo) y dominios sospechosos de suplantación de marca.
redes_sociales	Busca en YouTube, Twitter/X, Facebook, LinkedIn, Reddit y plataformas sociales indexadas por Google menciones de suplantación de marca, perfiles falsos y phishing relacionados con el dominio escaneado.
spoofguard	SpoofGuard genera miles de variaciones de dominio (typosquats, homoglyphs, bit-squatting, intercambios de TLD, punycode, proximidad de teclado, etc.), realiza búsquedas DNS en todos ellos, verifica servidores web

MÓDULO	DESCRIPCIÓN
	activos, detecta páginas de phishing a través de múltiples motores de detección y captura capturas de pantalla.
tg_discord_paste	Busca en canales de hackers de Telegram, servidores de ciberseguridad de Discord y sitios de paste (Pastebin, dpaste, ideone, etc.) menciones de la marca o dominio objetivo. Los hallazgos son analizados por GPT-4o-mini para filtrar ruido y evaluar la relevancia de seguridad. Búsqueda en vivo opcional en Google a través de 76 sitios de paste.
tls_posture	Sintetiza la postura de seguridad TLS/SSL a partir de nmap ssl-enum-ciphers, datos de certificados de Shodan y hallazgos SSL de nuclei. Detecta certificados caducados/autofirmados, protocolos débiles (TLS 1.0/1.1), cifrados débiles (grado C-F) y hosts HTTP-only que faltan HTTPS.
inteligencia_vip	Enumera objetivos de alto valor (ejecutivos, directores, gerentes) a través de cuentas de Google, recuperación de cuentas de Microsoft, detección de cuentas Holehe (más de 120 sitios) y bases de datos de filtraciones. Produce perfiles de riesgo impulsados por GPT con evaluación de vectores de ataque por persona.
vuln_nuclei	Ejecuta más de 4,000 plantillas de nuclei curadas contra hosts descubiertos, seleccionadas dinámicamente por tipo de puerto abierto. Las plantillas HTTP (tecnologías, paneles expuestos, configuraciones incorrectas, exposiciones de archivos sensibles, detección segura de CVE) apuntan a puntos finales web activos. Las plantillas SSL verifican la configuración del certificado y del cifrado. Las plantillas DNS prueban la transferencia de zona y problemas de configuración. Las plantillas de red identifican servicios no HTTP (SSH, FTP, SMTP, bases de datos). Todas las plantillas son de solo lectura (solo GET/HEAD) — sin explotación ni inyección de carga útil.
seguridad_aplicación_web	Evalúa los puntos finales web accesibles externamente en busca de debilidades de seguridad HTTP utilizando solicitudes GET seguras, análisis de redirección, inspección de encabezados de respuesta, análisis de Set-Cookie, evaluación de CSP/HSTS y análisis HTML pasivo. Más de 20 verificaciones que cubren la seguridad de las cookies de sesión, la aplicación de HTTPS, encabezados de seguridad, integridad de subrecursos y protección contra clickjacking.
descubrimiento_rango_ip	Identifica rangos de IP propiedad de la organización objetivo a través de las API REST de RIR (RIPE, ARIN, APNIC/AFRINIC RDAP). Utiliza identificación de nombre de

MÓDULO	DESCRIPCIÓN
	empresa mejorada por GPT para consultar registros y descubrir bloques de red asignados al objetivo.
resolver_ip	Resuelve el dominio objetivo a su dirección IPv4 primaria a través de una búsqueda de registro A DNS. Esta IP se convierte en el ancla para el descubrimiento de rangos de IP y búsquedas ARIN/RIPE.
reverse_dns	Realiza búsquedas inversas de DNS a través de ViewDNS para descubrir dominios y nombres de host adicionales asociados con las direcciones IP del objetivo. Revela registros PTR y asignaciones de DNS inverso.
reverse_whois	Encuentra otros dominios registrados por la misma entidad utilizando búsquedas inversas de WHOIS (ViewDNS). Solo se ejecuta cuando el dominio está auto-registrado (no protegido por privacidad o registrado por un proveedor). Descubre dominios sombra y activos relacionados con la marca.
mismos_dominios_ip	Descubre otros dominios alojados en la(s) misma(s) dirección(es) IP que el objetivo utilizando cuatro fuentes de IP inversa (C99, RapidDNS, HackerTarget, ViewDNS). Los vecinos de alojamiento compartido pueden exponer caminos de movimiento lateral.
descubrimiento_de_subdominio	Descubra todos los subdominios utilizando 17 fuentes de OSINT: transparencia de certificados, motores de búsqueda, bases de datos DNS, credenciales filtradas, DNS inverso (PTR) y rastreo web.
verificación_vuln	Ejecuta más de 4,000 plantillas de núcleos curadas contra los hosts descubiertos para detectar paneles expuestos, configuraciones incorrectas, huellas tecnológicas y comprobaciones de CVE seguras. Las plantillas se seleccionan dinámicamente en función de los puertos abiertos.
whois	Recupera datos de registro WHOIS/RDAP para el dominio principal, incluyendo registrador, fecha de creación, fecha de expiración y organización registrante.
c99	Consulta la base de datos DNS pasiva integral de C99 para subdominios conocidos del dominio objetivo.
crt	Busca en los registros de Transparencia de Certificados a través de crt.sh todos los certificados SSL/TLS emitidos a subdominios del objetivo. Utiliza la API JSON como principal, raspado HTML como respaldo para dominios grandes.
dns_bruteforce	Prueba 5,000 prefijos de subdominio comunes (www, mail, ftp, vpn, dev, staging, etc.) contra el dominio

MÓDULO	DESCRIPCIÓN
	objetivo utilizando 12 resolutores DNS públicos en round-robin. Encuentra subdominios no visibles en ninguna fuente pasiva.
dnsdumpster	Herramienta de reconocimiento DNS que mapea la infraestructura del dominio. Devuelve subdominios de registros A, MX, NS y TXT descubiertos a través de la recolección pasiva de DNS.
hackertarget	Busca en la base de datos DNS de HackerTarget registros de host conocidos (registros A) asociados con el dominio objetivo.
hackertarget_ptr	Consulta la API reversedns de HackerTarget para encontrar registros PTR que apuntan de vuelta al dominio objetivo. Descubre nombres de host internos (puertas de enlace de correo, servidores de staging, recolectores de logs) que solo son visibles a través de DNS inverso.
hackertarget_mismo_ns	Resuelve los registros NS del objetivo, luego consulta la API findshareddns de HackerTarget para cada dominio que comparte esos servidores de nombres. Revela dominios relacionados organizacionalmente.
kaduuleaks	Extrae nombres de host de credenciales filtradas en la base de datos de monitoreo de la darknet de Kaduu. Analiza líneas de volcado de credenciales (por ejemplo, user@host:password) para descubrir subdominios que aparecen en los datos de filtración.
kaduulogs	Monitorea los registros de transparencia de certificados SSL a través de la plataforma de inteligencia darknet propietaria de Kaduu. Descubre subdominios de certificados recién emitidos en tiempo real.
netcraft	Consulta la base de datos de encuestas de internet de Netcraft a través de Selenium Chrome sin cabeza para descubrir subdominios de su archivo de encuestas web de 30 años.
rapiddns	Busca en la base de datos DNS pasiva de RapidDNS.io registros DNS históricos y actuales. Pagina a través de los resultados para encontrar todos los subdominios conocidos.
scrapingbee	Utiliza el bypass anti-bot de ScrapingBee para raspar resultados de búsqueda de Google en busca de referencias de subdominio. Ejecuta 3 páginas en paralelo con un límite de 60 segundos en el reloj.
serphouse	Raspa resultados de búsqueda de Google para referencias a subdominios que aparecen en páginas web

MÓDULO	DESCRIPCIÓN
	indexadas. Utiliza la consulta site:{domain} para encontrar subdominios indexados.
shodan	Descubre subdominios a partir de los datos de escaneo a nivel de internet de Shodan. Busca hostname:{domain} y extrae nombres de host de certificados SSL, DNS inverso y banners HTTP.
subdomaincenter	Servicio de meta-agregación que combina datos de subdominios de docenas de fuentes subyacentes en una única consulta.
waybackengine	Consulta la API CDX del Internet Archive para todas las URL históricas que coincidan con *.{domain}/*, extrayendo subdominios únicos de páginas archivadas. HTTPS como principal, HTTP como respaldo.
webcrawl	Rastrea el sitio web objetivo utilizando 5 trabajadores HTTP paralelos (BFS, máximo 200 páginas, profundidad 8, reloj de 10 minutos). Extrae dominios de <a>, <script src>, <link href>, <img src/srcset>, <iframe>, <form action>, <meta refresh>, expresiones regulares de URL de JavaScript en línea, y encabezados HTTP (CSP, Location, CORS, Link).
zoomeye	Motor de búsqueda del ciberespacio chino que indexa dispositivos y servicios conectados a internet. Busca v2 site="{domain}" (subtipo web) y extrae nombres de host de los campos de dominio/rdns/nombre de host.

DarknetSearch es una plataforma de Monitoreo de Superficie de Ataque de Kaduu AG (Suiza). La plataforma utiliza 49 módulos a través de 8 fases de pipeline para descubrir, enumerar y analizar la huella digital externa de una organización. Este informe fue generado automáticamente a partir de datos de escaneo. Para preguntas sobre este informe, contacte a support@kaduu.io.

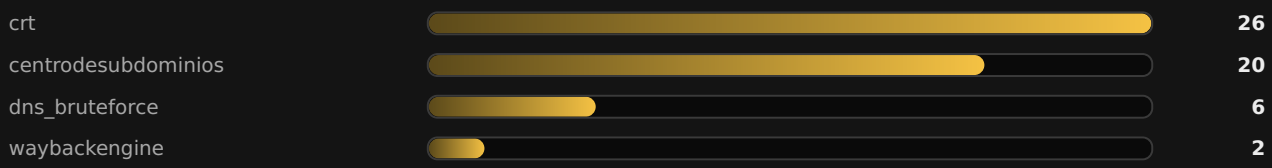
Apéndice E — Contribución de fuente de inteligencia

Contribución de fuente de inteligencia

Cómo cada fuente de inteligencia contribuyó a los tres pilares del descubrimiento de activos: **enumeración de nombres de host** (encontrar subdominios/hosts), **detección de puertos abiertos** (identificación de servicios) y **inteligencia de vulnerabilidades** (referencias CVE).

Descubrimiento de Nombres de Host

Hosts únicos contribuidos por cada módulo OSINT (antes de la deduplicación).



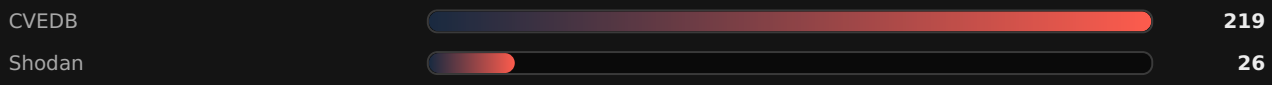
Detección de Puertos Abiertos

Hosts con datos de puertos de cada fuente.



Inteligencia de Vulnerabilidades

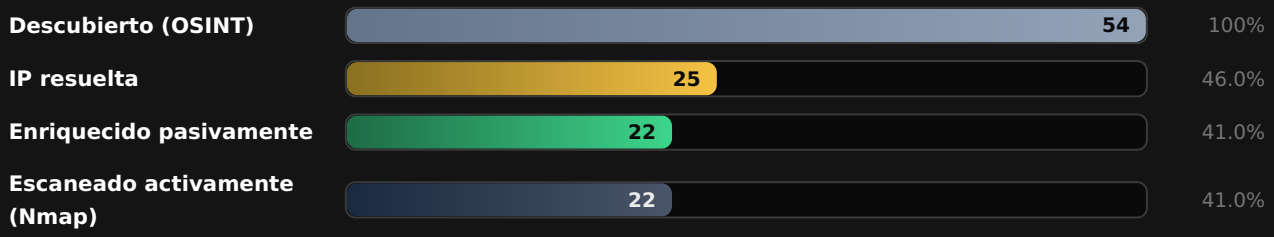
Referencias CVE por fuente de inteligencia.



Inteligencia adicional sobre amenazas: **Exposición de Credenciales** (bases de datos de filtraciones y registros de stealer), **Exposición de Almacenamiento en la Nube** (búsqueda de cubos S3/Azure/GCS), **Exposición de URL Acortadas** (inteligencia de goo.gl, bit.ly, tinyurl), **Detección de Panel de Administración** (análisis pasivo de banners), **Postura de TLS/SSL** (análisis de certificados y cifrados), **Exposición de Dominio y Riesgo de Expiración** (descubrimiento de IP inversa + monitoreo de expiración de RDAP), **Análisis de Exposición de Código** (detección de secretos y código fuente en GitHub/Gist a través de Codewatcher).

Embudo de enriquecimiento

El escaneo funciona en etapas como un embudo. Primero, recopilamos tantos nombres de dominio como sea posible de fuentes OSINT pasivas (registros de certificados, motores de búsqueda, bases de datos de DNS). A continuación, verificamos cuáles de esos dominios realmente resuelven a una dirección IP — muchos pueden ser históricos o inactivos. Para cada host con una IP confirmada, luego realizamos enriquecimiento: consultando Shodan, Netlas y ZoomEye para datos de puerto/servicio, realizando búsquedas WHOIS, verificando registros MX y, opcionalmente, ejecutando escaneos activos de Nmap. Cada etapa naturalmente filtra, por lo que la barra se estrecha en cada paso.



No resuelto: 29 hosts (sin registro DNS A en la ventana de escaneo).