DARKNETSEARCH
BY KADUU

Rapport de surface d'attaque

acmesample.com

Surface d'attaque observée : 2026-09-02 21:04 UTC

Rapport généré : 2026-09-24 17:31 UTC

RAPPORT D'ÉCHANTILLON — IDENTIFIANTS ANONYMISÉS

Résumé exécutif

Profil Cible

Domaine	acmesample.com
Organisation	Acme Sample GmbH
Type	Société Privée
Industrie	Fabrication industrielle
Taille	501-1000 employés
Siège	Sample City, États-Unis
Opérant dans	États-Unis, Canada

Acme Sample GmbH, une entreprise privée nord-américaine dans l'industrie de la fabrication industrielle, fait face à une pression de ciblage cybernétique modérée. Le secteur de la fabrication industrielle est de plus en plus ciblé par des menaces cybernétiques, en particulier les rançongiciels et les attaques de la chaîne d'approvisionnement, en raison de sa dépendance à la technologie et de ses chaînes d'approvisionnement complexes. Opérant au Canada et aux États-Unis, deux cibles fréquentes pour la cybercriminalité, augmente encore le risque. Avec une taille d'entreprise de 501 à 1 000 employés, Acme Sample GmbH est une cible viable pour les cybercriminels cherchant un gain financier à travers des rançongiciels et d'autres menaces cybernétiques.

À Propos de Ce Rapport

Ce rapport fournit une vue d'ensemble de la surface d'attaque de votre organisation, basée sur des méthodes de reconnaissance passive. En agrégeant des données provenant de multiples sources d'intelligence, il reflète comment un attaquant pourrait identifier des actifs exposés, des services et des risques potentiels — sans effectuer de scan intrusif.

Le domaine du site web scanné **acmesample.com** utilise un domaine différent pour les emails des employés : **acmesample.com, acmesample.net**. Les recherches de fuite d'identifiants ont couvert tous les domaines email identifiés.

Comparaison de l'empreinte d'infrastructure

DOMAINE	ESTIM. SOUS-DOMAINES
acmesample.com (domaine d'entrée initial)	~54
acmesample.net	~1

Structure du rapport

Ce rapport est organisé en cinq chapitres principaux, chacun couvrant une dimension distincte de la surface d'attaque :

CHAPITRE	FOCUS	PAGE
Network	Plages IP, voisins réseau, hébergement, répartition géographique	**15**
Applications	Technologies, sécurité DNS et email, vulnérabilités, TLS, sécurité des applications web	**53**
Infrastructure	Ports, sous-domaines, surface d'authentification, risque logiciel, panneaux d'administration, exposition	**75**
People	Identifiants, contenu de violation, énumération d'emails, empreinte numérique VIP	**19**
Paysage des menaces	réputation IP, exposition de code, Telegram/Discord/paste, réseaux sociaux, typosquatting	**90**

APERÇU DES SCORES DE SÉCURITÉ CLÉS



POSTURE DE SÉCURITÉ

PASSABLE

Composite à travers 11 domaines d'évaluation. Plus c'est élevé, mieux c'est.



RISQUE OPÉRATIONNEL

ÉLEVÉ

Sensible aux constatations critiques actives. Déterminé par les pires hôtes et les conditions urgentes.

Le rapport de Surveillance de la Surface d'Attaque pour Acme Sample GmbH fournit une analyse complète de la posture de sécurité de l'organisation. Le Score de Posture de Sécurité de l'organisation est de **55/100** (FAIBLE) avec un niveau de Risque Opérationnel de **5.8/10** (ÉLEVÉ). L'évaluation a utilisé une méthodologie de scan structurée, couvrant un total de **54 hôtes** et identifiant des vulnérabilités à travers divers domaines.

Les constatations clés révèlent une exposition significative, y compris **26 fuites d'identifiants** et **11 fichiers exposés dans le cloud**, avec **7 fichiers sensibles** identifiés dans le stockage cloud. Le scan a également détecté **372 domaines de typosquatting** avec des enregistrements DNS actifs, posant une menace potentielle de phishing. De plus, le score de posture de sécurité de l'application web est de **74**, avec **3 constatations de haute gravité** liées aux configurations de sécurité.

Pour atténuer les risques, il est recommandé que l'organisation effectue un examen approfondi de ses pratiques de gestion des identifiants et mette en œuvre des mesures d'authentification plus robustes. De plus, un scan séparé du domaine email **acmesample.net** est conseillé en raison de la divergence identifiée du domaine email. S'attaquer aux vulnérabilités dans le stockage cloud et améliorer la sécurité de l'application web par la remédiation des problèmes de haute gravité renforcera davantage la posture de sécurité globale.

Constatations Clés

- Il y a **26 fuites d'identifiants** associées à l'organisation.
- Un total de **11 fichiers exposés dans le cloud** a été identifié lors du scan.

- Il y a **372 domaines de typosquatting** avec des enregistrements DNS actifs posant des risques potentiels.
- Le score de sécurité de l'application web est de **74**, avec **3 constatations de haute gravité**.
- Le risque opérationnel est évalué à **5.8/10**, indiquant un niveau de risque élevé.

DÉTAILS DES SCORES DE SÉCURITÉ

Échelle : **0 = exposition maximale / pire**, **100 = meilleure posture** — plus élevé est mieux pour chaque catégorie ci-dessous (par exemple, un score d'exposition des personnes de 0/100 signifie que l'organisation est maximement exposée, pas que rien n'a été trouvé).

0 — **EXPOSITION DES PERSONNES** — CRITIQUE
1 employé avec exposition de journal de voleur
Poids : 10%

50 — **PROTECTION DE MARQUE** — MAUVAIS
362 typosquats avec des serveurs web actifs
Poids : 4%

53 — **VULNÉRABILITÉS** — MAUVAIS
69 CVEs critiques/élevés non vérifiés (correspondant au produit)
Poids : 20%

64 — **RÉSEAU** — PASSABLE
3 hôtes avec des services à haut risque, 5 hôtes sur des ports inhabituels
Poids : 11%

70 — **IDENTIFIANTS** — PASSABLE
9 boîtes mail à risque critique
Poids : 20%

74 — **SÉCURITÉ DES APPLICATIONS WEB** — PASSABLE
3 problèmes de sécurité web de gravité ÉLEVÉE
Poids : 10%

76 — **DNS & EMAIL** — BON
Aucun problème critique DNS/email
Poids : 10%

79 — **EXPOSITION DE L'ACTEUR MALVEILLANT** — BON
Pression ciblant le secteur modéré
Poids : 5%

80 — **MÉDIAS SOCIAUX** — BON
1 risque d'imitation trouvé
Poids : 3%

82 — **INFRASTRUCTURE** — BON
1 point de terminaison d'authentification détecté
Poids : 5%

91 — **TLS / SSL** — EXCELLENT
2 hôtes de protocole faibles
Poids : 10%

POSTURE SCORE GUARDRAILS ACTIFS

55 **Risque combiné :** 8 hôtes avec un risque composé ≥ 8.0

COMMENT CE SCORE EST CALCULÉ

CATÉGORIE	POIDS	SCORE	CONTRIBUTION
DNS & Email	10%	76 / 100	7,6 pts
TLS / SSL	10%	91 / 100	9,1 pts

CATÉGORIE	POIDS	SCORE	CONTRIBUTION
Vulnérabilités	20%	53 / 100	10,6 pts
Identifiants	20%	70 / 100	14,0 pts
Réseau	11%	64 / 100	7,0 pts
Infrastructure	5%	82 / 100	4,1 pts
Protection de marque	4%	50 / 100	2,0 pts
Exposition des personnes	10%	0 / 100	0,0 pts
Médias sociaux	3%	80 / 100	2,4 pts
Exposition de canal hacker	5%	Non évalué (module non activé)	
Sécurité des applications web	10%	74 / 100	7,4 pts
Exposition de l'acteur malveillant	5%	79 / 100	4,0 pts

Méthodologie de notation : Chaque catégorie utilise un échelonnement logarithmique (pas de comptes bruts) avec des multiplicateurs de prévalence — les problèmes répandus sur de nombreux hôtes sont pénalisés plus sévèrement que les constatations isolées. Le modèle de vulnérabilité hérité sépare les constatations vérifiées des indicateurs passifs/appariés aux produits mais n'applique pas les multiplicateurs de contribution de niveau de preuve DS-90. Des multiplicateurs de prévalence allant jusqu'à 1,75× s'appliquent toujours là où cela est supporté. Les hôtes critiques pour les affaires (points de terminaison d'authentification, panneaux d'administration) amplifient le risque via la corrélation inter-modules. Le Score de Posture est une moyenne pondérée avec des plafonds de garde-fou qui empêchent un score global trompeusement bon lorsque n'importe quel domaine est gravement compromis. Le Score de Risque Opérationnel est déterminé par le risque d'hôte composé — hôtes où plusieurs facteurs de risque se chevauchent (par exemple, panneau d'administration + TLS faible + identifiants divulgués). (Modèle de notation : hérité.)

CONSTATATIONS LES PLUS IMPORTANTES

6

RISQUE D'ACTIF LE PLUS ÉLEVÉ

6 / 10

Pire hôte unique dans cette analyse (0 = le plus bas).

INSTANCES CVE

249

De Shodan, Netlas, ZoomEye & CVEDB

CONSTATATIONS DE VÉRIFICATION

2

Actionnable · +397 informatif

POSTURE DE SÉCURITÉ (EN UN COUP D'ŒIL)

CVE references are derived from **analyse de l'en-tête de service** (Shodan, Netlas, ZoomEye) and **correspondance de version de produit** (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.

PORTÉE & EMPREINTE

SOUS-DOMAINES TROUVÉS
54
FQDN uniques découverts

HÔTES ACTIFS
25
Résolu vers une IP

PLAGES IP
0
Blocs de réseau possédés (RIR)

PORTS OUVERTS (HÔTES)
22
Passif + Nmap confirmé

NOMS D'HÔTES SENSIBLES
9
Sous-domaines signalés

HÔTES AVEC SIGNAUX DE VULNÉRABILITÉ
10
Tout signal lié aux CVE

DURÉE DU SCAN
91 min
Temps d'attente du pipeline

HÔTES PROPRES
6
Hôtes actifs, score de risque 0

RENSEIGNEMENT SUR LES MENACES

IDENTIFIANTS FUITÉS
26
Comptes d'employés sur des services externes

ENREGISTREMENTS DE LA BASE DE DONNÉES DE VIOLATIONS
2,038
Mentions de domaine (correspondance de sous-chaîne)

EXPOSITIONS CLOUD
11
7 fichiers sensibles

URLS RACCOURCIES
3,000
0 ressources internes

MÉDIAS SOCIAUX
192
1 risque d'usurpation

EXPOSITION DES E-MAILS
498
14 critiques, 61 à haut risque

EXPOSITION DE CODE
26
0 risque élevé sur GitHub/Gists

TG / DISCORD / PASTE
n/a
Non analysé ; 0 mentions brutes conservées

SYSTÈMES CRITIQUES POUR L'ENTREPRISE
12
Fonctions critiques exposées à Internet

CHEMINS D'ATTAQUE
1
1 total pivot paths

SÉCURITÉ DES INFRASTRUCTURES ET DES APPLICATIONS

PANNEAUX D'ADMINISTRATION
0
Interfaces de gestion exposées

PROBLÈMES TLS
2
Certificat / protocole / chiffrement

SÉCURITÉ DES APPLICATIONS WEB
74/100
3 élevés, 3 moyens

DOMAINES DE TYPOSQUATTING
372
0 phishing détecté

POINTS DE TERMINAISON D'AUTHENTIFICATION
1
SSO, VPN, panneaux de pare-feu

ACTIFS LES PLUS RISQUÉS

Les systèmes suivants représentent le risque composé le plus élevé basé sur la corrélation inter-modules. Chaque hôte a été noté en combinant des facteurs de risque individuels — tels que des panneaux d'administration exposés, un TLS faible, des identifiants fuités et des signaux de vulnérabilité — avec des multiplicateurs de criticité commerciale. Les systèmes où plusieurs facteurs de risque se chevauchent reçoivent des scores exponentiellement plus élevés, car les attaquants peuvent enchaîner ces faiblesses pour un impact maximal.

HÔTE	RISQUE	IMPACT COMMERCIAL	FACTEURS DE RISQUE
asset-062.acmesample.com +1 alias sur 192.0.2.178	10.0	Système de messagerie	13 CVE-IDs critiques/élevés, IP signalée, Point de terminaison d'authentification, 13 ports ouverts
asset-166.acmesample.com	10.0	Site Web / Public	38 CVEs critiques/élevés, IP signalée, point de terminaison d'authentification
asset-143.acmesample.com +1 alias sur 192.0.2.27	10.0	Site Web / Public — faiblesses de sécurité sur le point de terminaison d'authentification	33 CVEs critiques/élevés, TLS faible, Web app ÉLEVÉ, point de terminaison d'authentification
www.acmesample.com +1 alias sur 192.0.2.11	10.0	Site Web / Public — faiblesses de sécurité sur le point de terminaison d'authentification	5 CVEs critiques/élevés, Application web ÉLEVÉE, Point de terminaison d'authentification
asset-071.acmesample.com	8.8	Site Web / Public	13 CVEs élevés/critiques, IP signalée, 13 ports ouverts
asset-141.acmesample.com	7.5	Infrastructure API	2 CVEs élevés/critiques, Sous-domaine sensible
portal.acmesample.com	6.0	Portail client	Point de terminaison d'authentification
asset-142.acmesample.com	5.0	Infrastructure API	2 CVEs élevés/critiques
asset-064.acmesample.com	1.8	CRM / ERP	Point de terminaison d'authentification, Sous-domaine sensible
asset-055.acmesample.com	1.2	Système exposé à Internet	Sous-domaine sensible

EMPLOYÉS LES PLUS À RISQUE

Personnel de direction de grande valeur avec la plus grande exposition basée sur des informations VIP (dossiers de violation, mots de passe divulgués, détections de comptes) et des données d'énumération d'emails. Ces individus représentent des cibles prioritaires pour le phishing ciblé et les attaques basées sur des identifiants.

NOM	POSITION	RISQUE	VIOLA-TIONS	PWD	FACTEURS DE RISQUE
Executive012 Sample012	Vice-président de la gestion des produits	85	177	OUI	177 violations, Mots de passe divulgués, Récupération MS, ID Google trouvé
Executive035 Sample035	Directeur Senior des Comptes Stratégiques	80	79	OUI	79 violations, mots de passe divulgués, 1 comptes en ligne, récupération MS
Executive020 Sample020	Directeur senior, Comptes nationaux	85	26	OUI	26 violations, Mots de passe exposés, 1 comptes en ligne, MS recovery
Executive067 Sample067	Directeur Financier	85	10	OUI	10 violations, Mots de passe exposés, 4 comptes en ligne, MS recovery
Executive040 Sample040	Responsable Technique IT	80	11	OUI	11 violations, mots de passe divulgués, 5 comptes en ligne, récupération MS
Executive041 Sample041	Directeur général	95	8	—	8 violations, 5 sources web
Executive036 Sample036	Vice-président de la distribution	80	8	—	8 violations
Executive131 Sample131	Directeur des ressources humaines	80	7	—	7 violations
Exécutif005 Échantillon005	Directeur de la culture	80	6	—	6 violations
Executive078 Sample078	Responsable marketing produit	70	6	—	6 violations, 4 sources web

TOP 10 DES ACTIONS PRIORITAIRES

#	ACTION	PÉRIODE	CATÉGORIE
1	**Examiner et corriger les CVE sur asset-166.acmesample.com** L'actif-166 a 38 CVE de gravité élevée/critiques. Une remédiation immédiate est requise pour sécuriser le site web accessible au public. **Affected:** `asset-166.acmesample.com`	Immédiat	VULNÉRABILITÉS
2	**Examiner et corriger les CVE sur asset-062.acmesample.com** L'actif-062 a 13 CVE de gravité élevée/critiques. Une action immédiate est nécessaire pour protéger le système de messagerie. **Affected:** `asset-062.acmesample.com`	Immédiat	VULNÉRABILITÉS
3	**Examiner et corriger les CVE sur asset-143.acmesample.com** L'actif-143 a 33 CVE de gravité élevée/critiques et un TLS faible. Une remédiation immédiate est cruciale pour le site web accessible au public. **Affected:** `asset-143.acmesample.com`	Immédiat	VULNÉRABILITÉS
4	**Examiner et corriger les CVE sur www.acmesample.com** www.acmesample.com a 5 CVE de gravité élevée/critiques. Une action immédiate est requise pour sécuriser le point de terminaison d'authentification. **Affected:** `www.acmesample.com`	Immédiat	VULNÉRABILITÉS
5	**Restreindre l'exposition du panneau d'administration sur asset-071.acmesample.com** L'actif-071 a 13 ports ouverts et des CVE élevés. Restreindre l'accès est vital pour réduire le risque. **Affected:** `asset-071.acmesample.com`	Cette semaine	RÉSEAU
6	**Appliquer la politique de rejet DMARC sur acmesample.com** La mise en œuvre de DMARC protégera contre le spoofing d'e-mail et améliorera la sécurité du domaine.	Cette semaine	PROTECTION DE MARQUE
7	**Examiner 26 fuites d'identifiants pour acmesample.com** 26 boîtes mail d'employés sous acmesample.com ont été trouvées dans des ensembles de données de violation tiers. Examiner et faire tourner les identifiants.	Dans les 30 jours	IDENTIFIANTS
8	**Examiner 2 configurations TLS faibles** Deux hôtes utilisent des protocoles TLS faibles. Examiner et mettre à niveau vers des configurations sécurisées.	Dans les 30 jours	TLS/SSL
9	**Examiner 372 domaines de typosquatting pour acmesample.com** Il y a 372 domaines de typosquatting qui pourraient poser un risque. Examiner et prendre les mesures nécessaires.	Dans les 90 jours	PROTECTION DE MARQUE
10	**Évaluer 7 fichiers sensibles dans le cloud pour exposition** Il y a 7 fichiers sensibles dans le cloud qui nécessitent une évaluation pour une exposition potentielle.	Dans les 90 jours	INFRASTRUCTURE

Méthodologie de scan & Couverture

DarknetSearch L'énumération de la surface d'attaque utilise un **pipeline automatisé en 8 phases** pour cartographier l'empreinte numérique externe d'une organisation. En commençant par le domaine cible, le système découvre progressivement, enrichit et analyse chaque actif accessible depuis l'extérieur — reflétant les mêmes techniques de reconnaissance utilisées par les attaquants du monde réel.

1
Analyse de la cible
Résoudre IP, base de référence WHOIS/RDAP.

2
Découverte de sous-domaines
Jusqu'à 16 modules OSINT passifs.

3
Carte d'infrastructure
Plages RIR, même-IP, reverse WHOIS.

4
Intelligence passive
Shodan, Netlas, ZoomEye.

5 OPT-IN
Analyse active
Nmap sur les ports découverts.

6
Analyse et corrélation
Scores de risque, voisins, CVE-IDs.

7 OPT-IN
Vérification active
Scan de modèle HTTP/SSL sécurisé.

8
Génération de rapport
Analyse, graphiques, rendu PDF.

Phase 1 — Analyse de la cible

Le pipeline commence par la résolution de l'adresse IP principale du domaine cible et l'interrogation des bases de données d'enregistrement WHOIS/RDAP pour identifier le propriétaire du domaine, le registraire et l'historique d'enregistrement. Cela établit l'identité de base pour les recherches ultérieures.

Phase 2 — Découverte de sous-domaines

Jusqu'à 16 modules OSINT passifs fonctionnent en parallèle — interrogeant les journaux de transparence des certificats (crt.sh, Kaduu CT Monitor), les index des moteurs de recherche (Shodan, ZoomEye, Google via SERPHouse/ScrapingBee), les bases de données DNS passives (RapidDNS, DNSDumpster, SubdomainCenter, HackerTarget), l'historique des archives web (Wayback Machine), les fuites d'identifiants sur le darknet (Kaduu), le scraping de navigateur sans tête (Netcraft), et le site web cible lui-même via un crawler web BFS concurrent. Lorsque l'énumération DNS active est activée, un module de brute force DNS teste 5 000 préfixes de sous-domaines courants.

Phase 3 — Cartographie de l'infrastructure

Quatre sources de recherche inversée IP identifient les domaines partageant l'IP de la cible. Les API REST RIR (RIPE, ARIN) découvrent toutes les plages IP enregistrées au nom de l'organisation cible. Un pipeline amélioré par GPT identifie l'entreprise, génère des noms de recherche normalisés et détermine quelles inscriptions RIR appartiennent à la cible. Les recherches WHOIS inversées trouvent tous les domaines enregistrés par la même entité.

Phase 4 — Intelligence passive

Pour chaque hôte découvert, le système interroge Shodan, Netlas et ZoomEye pour les ports ouverts, les bannières de service, les certificats SSL, les identifiants CPE et les vulnérabilités connues — sans toucher à l'infrastructure de la cible. Les résultats sont mis en cache pendant 7 jours par IP pour optimiser l'utilisation de l'API.

Phase 5 — Analyse active (opt-in)

Lorsque activé, Nmap effectue un scan TCP ciblé avec détection de version (-sV) et des scripts NSE (vulners pour la recherche de CVE, ssl-enum-ciphers pour l'audit TLS) sur les ports découverts passivement. Si aucun port n'est connu, un scan rapide des 100 premiers ports TCP est effectué à la place.

Phase 6 — Analyse & Corrélation

L'analyse du voisinage réseau examine les IP adjacentes pour des correspondances de certificats SSL, des motifs PTR, des comparaisons ASN et du fingerprinting HTTP. Les CVE sont agrégés à partir de 5 sources et vérifiés croisés avec les bannières de service Nmap. Les scores de risque (0–10) sont calculés par hôte en fonction des vulnérabilités, des ports inhabituels et des motifs de nom d'hôte sensibles.

Phase 7 — Vérification de Sécurité Active (opt-in)

Lorsque activé, un moteur de vérification de sécurité automatisé analyse tous les hôtes découverts avec des points de terminaison HTTP/HTTPS actifs en utilisant **plus de 4 000 modèles de détection sûrs**. Ces modèles n'utilisent que des requêtes GET/HEAD (pas d'exploitation ni d'injection de charge utile) pour détecter les panneaux d'administration exposés, les erreurs de configuration de sécurité, les expositions de fichiers sensibles, les logiciels obsolètes et les indicateurs CVE connus. De plus, des vérifications SSL/TLS, DNS et au niveau du réseau sont effectuées sur tous les hôtes avec des ports classifiés. Seuls les hôtes avec des ports ouverts sont testés ; le moteur sonde d'abord chaque URL pour vérifier sa disponibilité avant de procéder à l'analyse.

Phase 8 — Génération de rapport

Tous les résultats de scan sont dédupliqués et consolidés. Les compteurs d'enrichissement sont matérialisés, les entrées DNS wildcard détectées, et les scores de risque finalisés. Le pipeline de génération de rapport collecte ensuite toutes les données de la base de données, effectue une analyse déterministe (distribution des risques, fréquence des ports/services, pile technologique, paysage CVE, propriété du réseau), génère des graphiques via matplotlib, obtient un résumé exécutif alimenté par GPT, géolocalise tous les IP résolus, et rend le PDF final en utilisant WeasyPrint. Les preuves CSV détaillées sont omises de cet échantillon public.

Résumé du module

56 modules complétés, **0** échoués, **5** sautés. Détails complets par module disponibles dans `jeu de donnees de preuves prive` omis de cet échantillon public.

Modules non complétés

Les modules suivants ont échoué ou ont été ignorés. Leurs constatations peuvent être absentes de ce rapport ; un compte nul ne doit pas être interprété comme un résultat propre.

MODULE	STATUT	DIAGNOSTIC
ip_range_discovery	Sauté	domain_mode=default (scopé) — découverte de domaine supplémentaire désactivée
reverse_dns	Sauté	Désactivé par un drapeau de fonctionnalité
reverse_whois	Sauté	domain_mode=default (scopé) — découverte de domaine supplémentaire désactivée
mêmes_domaine_ip	Sauté	domain_mode=default (scopé) — découverte de domaine supplémentaire désactivée
hackertarget_same_ns	Sauté	domain_mode=default (scopé) — découverte apex same-NS désactivée

Aperçu de la surface d'attaque

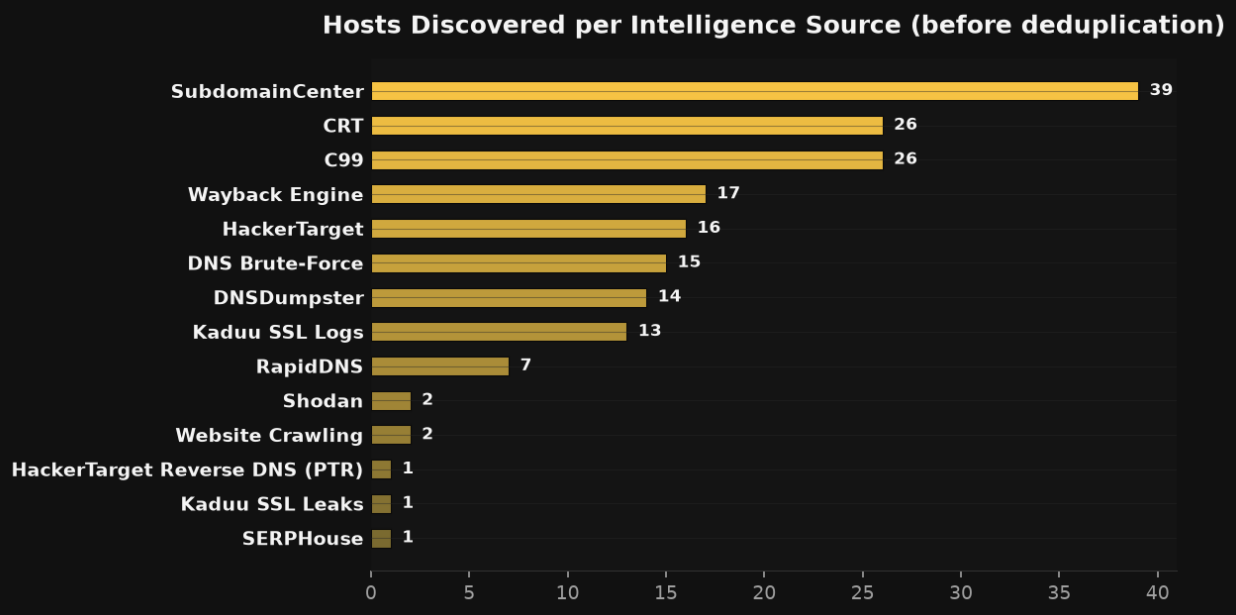
La surface d'attaque représente tous les hôtes, services et actifs numériques accessibles depuis l'extérieur associés à **acmesample.com**. Les hôtes ont été découverts grâce à des sources de renseignement passif (transparence des certificats, bases de données DNS, moteurs de recherche, identifiants divulgués) et confirmés optionnellement par un scan actif (Nmap, vérification active).

Noms d'hôtes sensibles sont des noms d'hôtes contenant des motifs qui suggèrent des systèmes de grande valeur ou internes — tels que admin, dev, staging, vpn, jenkins, grafana, ou backup. Ces systèmes sont souvent les premières cibles lors des attaques réelles. **Ports inhabituels** sont des ports TCP/UDP ouverts en dehors de l'ensemble standard des services Internet courants (HTTP, HTTPS, SSH, DNS, SMTP, FTP). Leur présence peut indiquer des serveurs de développement, des interfaces de gestion, des applications héritées ou des services mal configurés.

54	54	9	5
SOUS-DOMAINES TROUVÉS	PROPRIÉTÉ DU CLIENT	NOMS D'HÔTES SENSIBLES	PORTS INHABITUELS

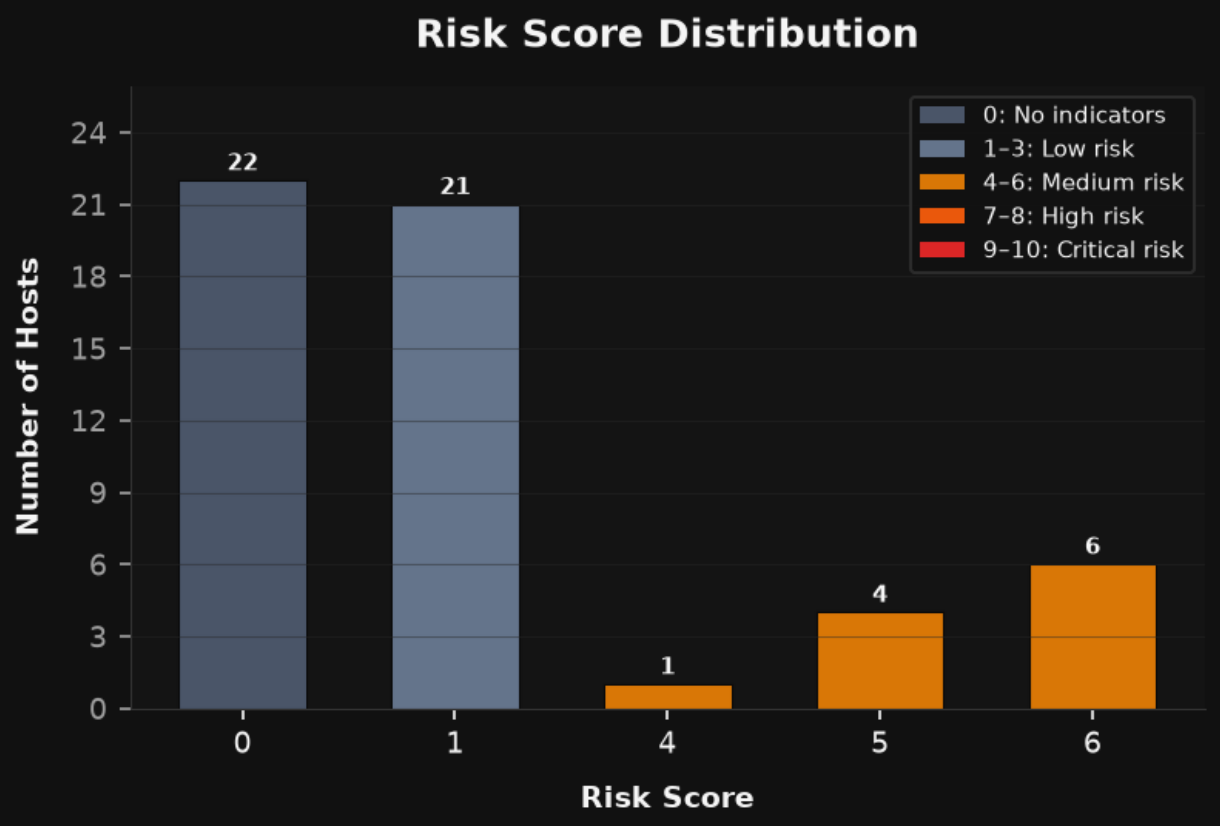
Sources de découverte (avant dé-duplication)

Les barres utilisent une **unique rampe dorée** par rang — plus facile à lire que de nombreuses couleurs non liées. Chaque barre compte les hôtes contribuant à cette source (les hôtes peuvent apparaître dans plusieurs sources).



Distribution des scores de risque

Scores de 0 à 10 basés sur les signaux CVE, les ports inhabituels, le nombre de ports et les modèles de noms d'hôtes sensibles. La légende du graphique correspond aux couleurs des barres.



RÉSEAU

Plages IP possédées par l'organisation

La découverte de plages IP identifie tous les blocs de réseau enregistrés auprès de l'organisation cible via les Registres Internet Régionaux (RIPE pour l'Europe/Moyen-Orient, ARIN pour l'Amérique du Nord). Un pipeline amélioré par GPT identifie l'entreprise derrière le domaine, génère des variantes de noms de recherche (y compris des formes repliées ASCII et dépouillées de suffixes légaux), et valide quelles inscriptions RIR appartiennent à la cible. Les grandes plages (>/24, 256+ hôtes) sont listées à titre informatif uniquement.

Important: Cette analyse identifie quels blocs réseau appartiennent à l'organisation sur la base des données d'enregistrement RIR. **Aucun hôte dans ces plages n'a été scanné, énuméré ou sondé activement.** Les plages fournissent un contexte sur le patrimoine IP enregistré de l'organisation — toute évaluation de sécurité des hôtes individuels dans ces plages nécessiterait un scan ciblé séparé.

Aucune plage IP enregistrée trouvée

La recherche RIR (RIPE, ARIN) n'a identifié aucune plage IP directement enregistrée à cette organisation. Cela signifie généralement que l'organisation utilise une infrastructure hébergée dans le cloud ou partagée (par exemple, AWS, Azure, Cloudflare) plutôt que de posséder des blocs IP dédiés. Cela est courant pour les organisations de petite à moyenne taille et n'indique pas un problème de sécurité — cependant, cela signifie qu'il n'y a pas de patrimoine IP supplémentaire à auditer au-delà des hôtes découverts par l'énumération de sous-domaines.

Analyse des Voisins Réseau

Pour chaque IP découverte, le système examine les adresses voisines dans le même sous-réseau /24. Les voisins sont évalués par correspondance de certificat SSL (comparaison CN/SAN), motifs d'enregistrement PTR, comparaison ASN et empreinte de contenu HTTP. Chaque voisin reçoit un score de confiance : **CONFIRMÉ** (l'IP se trouve dans une plage d'IP client enregistrée), **ÉLEVÉ** (2+ signaux forts tels que correspondance de certificat ou ASN), **MOYEN** (1 signal fort), **FAIBLE** (seuls des signaux faibles).

Important : Les adresses IP voisines ont été uniquement empreintées en utilisant des techniques passives (inspection de certificat, recherche PTR, en-têtes HTTP). **Aucun scan actif, test de pénétration ou évaluation de vulnérabilité n'a été effectué sur aucune adresse IP voisine.**

Analysé **20** quartiers IP — **8** correspondances de certificat SSL, **2** correspondances d'empreinte HTTP, **0** confirmées par RDAP. Les preuves complètes des voisins sont omises de cet échantillon public.

Exemples de constatations

IP CIBLE	IP VOISINE	CONFIANCE	SIGNAUX CORRESPONDANTS
192.0.2.182	192.0.2.183	MOYEN	Correspondance Ptr, Même Sous-réseau
192.0.2.184	192.0.2.183	MOYEN	Correspondance Ptr, Même Sous-réseau

Pourquoi les IP Voisines Comptent

Si l'analyse ci-dessus a identifié des adresses IP voisines avec une **confiance moyenne** ou **élevée** d'appartenir à votre organisation, ces hôtes n'ont pas été inclus dans le périmètre de l'analyse active et n'ont pas été testés pour des vulnérabilités. Cependant, un attaquant effectuant une reconnaissance découvrirait également ces voisins et pourrait les enquêter ou les attaquer pour obtenir un point d'entrée dans votre réseau. Nous recommandons de vérifier la propriété des voisins à haute confiance et de les inclure dans les futures évaluations de sécurité.

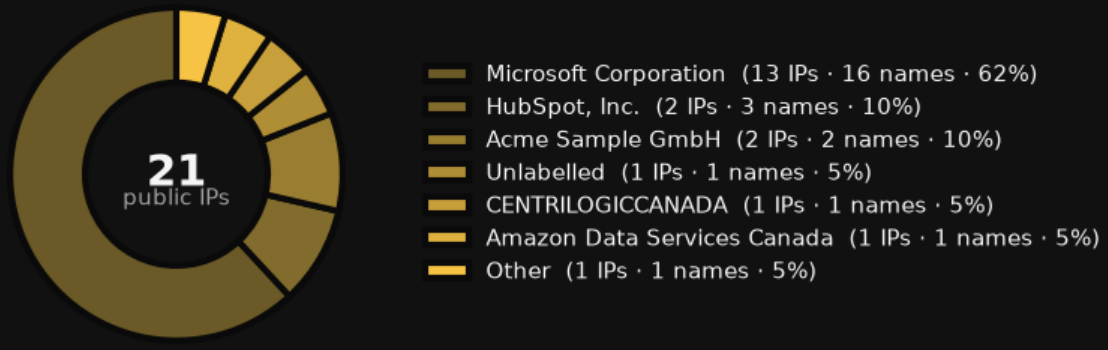
Fournisseurs d'Hébergement & Distribution

Chaque tranche est une étiquette de réseau, dimensionnée par le nombre d'adresses IP publiques portant cette étiquette. De nombreux noms d'hôtes peuvent partager une seule adresse, donc un compte de noms d'hôtes n'est pas la part de l'infrastructure. L'étiquette est une organisation RDAP ou, si cela manque, le propriétaire du réseau. Ce n'est pas une preuve de qui opère le service. Les noms non résolus (29) et les adresses non-routables (0) sont exclus des parts.

Évaluation : 21 adresses publiques à travers 6 réseaux. Les partages sont des adresses, pas des noms d'hôte.

Distribution

Hosting Provider Distribution



Principaux fournisseurs

Microsoft Corporation	**13 IPs · 16 noms**
HubSpot, Inc.	**2 IPs · 3 noms**
Acme Sample GmbH	**2 IPs · 2 noms**
Non étiqueté	**1 IPs · 1 noms**
CENTRILOGICCANADA	**1 IPs · 1 noms**
Amazon Data Services Canada	**1 IPs · 1 noms**
Cogent Communications, LLC	**1 IPs · 1 noms**

Évaluation des risques

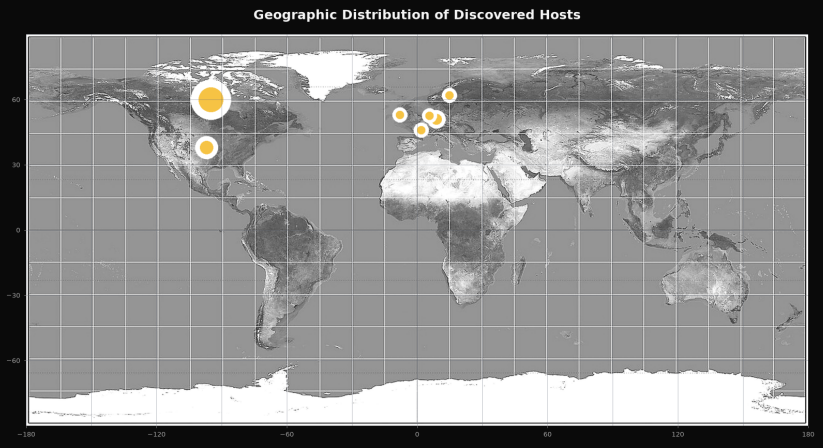
L'organisation s'appuie principalement sur l'hébergement tiers, Microsoft Corporation représentant environ 61,9 % de ses adresses IP publiques. Étant donné que plus de 70 % de l'infrastructure est concentrée auprès d'un seul fournisseur externe, cela présente un risque de concentration traditionnel, où une panne régionale pourrait affecter tous les services. Le verdict de résilience est préoccupant en raison de ce niveau élevé de dépendance. Il est recommandé que l'organisation mette en œuvre une stratégie multi-fournisseur pour atténuer les risques associés à la dépendance à un seul fournisseur, garantissant que les services critiques restent opérationnels pendant les pannes.

FOURNISSEUR	IPS PUBLIQUES	NOMS
Microsoft Corporation	13	16
HubSpot, Inc.	2	3
Acme Sample GmbH	2	2
Non étiqueté	1	1
CENTRILOGICCANADA	1	1
Amazon Data Services Canada	1	1
Cogent Communications, LLC	1	1

Répartition géographique

La géolocalisation IP montre où les hôtes découverts sont alloués (précision typiquement ville/région). Une large répartition peut indiquer un CDN, un cloud multi-région ou des juridictions inattendues.

Note : La carte utilise une projection **équirectangulaire** (WGS-84). La **position** des bulles est le centroïde standard de chaque pays (ISO) ; la **taille** reflète le nombre d'hôtes selon la géolocalisation. La légende liste chaque pays avec des hôtes.



CA	Canada	12
États-Unis	États-Unis	3
DE	Allemagne	2
IE	Irlande	1
SE	Suède	1
FR	France	1
NL	Pays-Bas	1

Position de la bulle = centroïde du pays ISO (plate carrée) ; taille de la bulle ∝ hôtes géolocalisés dans ce pays. Les codes pays correspondent à la légende. Carte de base : projection équidistante (Wikimedia Commons, CC BY-SA).

PERSONNES

Exposition de fuite d'identifiants

70
PASSABLE

Analyse de l'exposition des identifiants d'entreprise à travers les bases de données de violations et les agrégateurs de journaux de voleurs. Identifie les comptes d'employés compromis sur des services externes.

Validité des données d'identifiants compromis

Les acteurs malveillants recyclent souvent des données anciennes dans ce qu'on appelle des "listes combo", et les données de violation peuvent parfois être en retard de plusieurs mois, voire années, par rapport à l'incident original. D'après notre expérience, moins de ~2 % des identifiants divulgués que nous indexons restent valides. Cela dit, même un très petit nombre d'identifiants fonctionnels peut encore représenter un risque réel. Prévenir une violation peut se résumer à un seul compte compromis parmi des centaines.
Il est également important de différencier les sources de données : la recherche dans la base de données utilisée dans ce rapport se concentre sur les données compromises qui ont déjà été partagées publiquement (souvent gratuitement), tandis que les acteurs malveillants tentent généralement de vendre d'abord des données fraîches. Ces données plus récentes et de plus grande valeur se trouvent généralement via des recherches sur des forums de hackers actifs (non inclus dans ce rapport).
Au-delà de la validité des identifiants, les données historiques fournissent toujours des informations de sécurité significatives. Par exemple, elles aident à identifier les modèles de réutilisation de mots de passe à travers les services — un facteur clé des attaques par bourrage d'identifiants — ou des cas où des comptes de messagerie d'entreprise sont utilisés sur des plateformes privées. Ces types de constatations sont particulièrement utiles pour des formations de sensibilisation ciblées et pour renforcer les pratiques de sécurité internes.

Recherche d'identifiants multi-domaines

L'organisation utilise plusieurs domaines email. Les identifiants ont été recherchés sur tous les domaines identifiés :

DOMAINE	FUITES D'EMPLOYÉS	VIOLATIONS DE LA BASE DE DONNÉES	EMAILS UNIQUES
@acmesample.com	26	2,036	15
@acmesample.net	0	2	0

Résumé

Domaine de site web recherché (acmesample.com) et domaine(s) email (acmesample.net). @acmesample.com : 26 fuites d'employés, 2 036 enregistrements dans la base de données des violations. @acmesample.net : 0 fuite d'employés, 2 enregistrements dans la base de données des violations. 2 038 enregistrements de comptes fuités trouvés dans les bases de données des violations. 26 expositions d'identifiants d'employés détectées à travers 15 adresses email uniques. 17 sont classées à risque élevé ou critique (mots de passe en clair présents sur des services externes).

26
DOSSIERS D'IDENTIFIANTS DES EMPLOYÉS
paires login + mot de passe

388
BOÎTES MAIL DÉRIVÉES DE VIOLATIONS
union de violation canonique

2,038
VIOLATIONS DE LA BASE DE DONNÉES
mentions de domaine

17
RISQUE ÉLEVÉ/ CRITIQUE
enregistrements d'identifiants

Comprendre les Nombres

Enregistrements d'identifiants d'employés comptent des lignes d'identifiants distincts (login + mot de passe / paires de hachage) après que les observations identiques provenant de plusieurs sources de fuite ont été fusionnées. **Boîtes mail dérivées de violations** déduplique les preuves de violation en adresses distinctes et s'unit à toute `@acmesample.com` boîte mail supplémentaire vue dans la base de données de violation en direct (scannée dans son intégralité), échantillons de contenu de violation, et sources publiques Hunter.io. Répartition des sources (AVANT dé-duplication) : 15 provenant des identifiants, 383 provenant de la recherche de violation en direct, 384 provenant des échantillons de contenu de violation, 0 provenant de Hunter.io. **Enregistrements de la base de données de violation** comptent chaque document de violation (fichiers journaux, dumps de base de données, contenu de collage) qui mentionne le domaine dans n'importe quel champ — une mesure beaucoup plus large qui dépasse fréquemment le compte d'enregistrements d'identifiants de plusieurs ordres de grandeur car un fichier divulgué peut contenir des milliers de lignes mentionnant le domaine.

Comment "17 constatations critiques" se rapporte aux 388 boîtes mail dérivées de violations : le nombre de risques élevés/critiques est le nombre d'enregistrements d'identifiants évalués critiques par la source et le modèle de risque — généralement des preuves récentes de vol ou de texte en clair. La validité des mots de passe n'a pas été testée. La même boîte mail peut avoir plus d'un enregistrement d'identifiant critique distinct, donc ce nombre d'enregistrements peut dépasser le nombre de boîtes mail.

***Remarque sur les preuves de violation :** Ces chiffres reflètent les bases de données historiques de violations et les agrégateurs de journaux de voleurs. Les observations identiques sont dédupliquées, mais différents identifiants pour une boîte mail restent séparés. La présence dans un flux ne prouve pas qu'un compte ou un mot de passe est actuellement valide.

Enregistrements bruts vs. Enregistrements dédupliqués

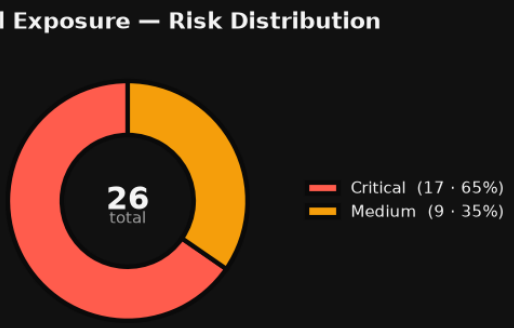
Dans toutes les recherches de domaines concernés, les flux de violation ont renvoyé **129** enregistrements d'identifiants bruts. Après dédupliquer la même paire boîte mail/mot de passe fuitée réapparue par des recherches de domaines chevauchants et plusieurs listes combinées, cela se réduit à **26** enregistrements distincts (103 enregistrements en double supprimés). Le titre et le score utilisent le chiffre dédupliqué ; le sous-total brut est montré ici pour réconciliation avec les comptes de flux en amont. Ces enregistrements couvrent **75** sources de fuite distinctes.

Fenêtre d'exposition (âge de l'enregistrement)

Les données de violation sont historiques — la présence d'un enregistrement ne signifie pas que le mot de passe est encore valide. La distribution ci-dessous regroupe chaque enregistrement daté par la durée écoulée depuis sa première apparition, de sorte que le rapport montre une fenêtre d'exposition plutôt que d'impliquer que chaque fuite est actuelle :

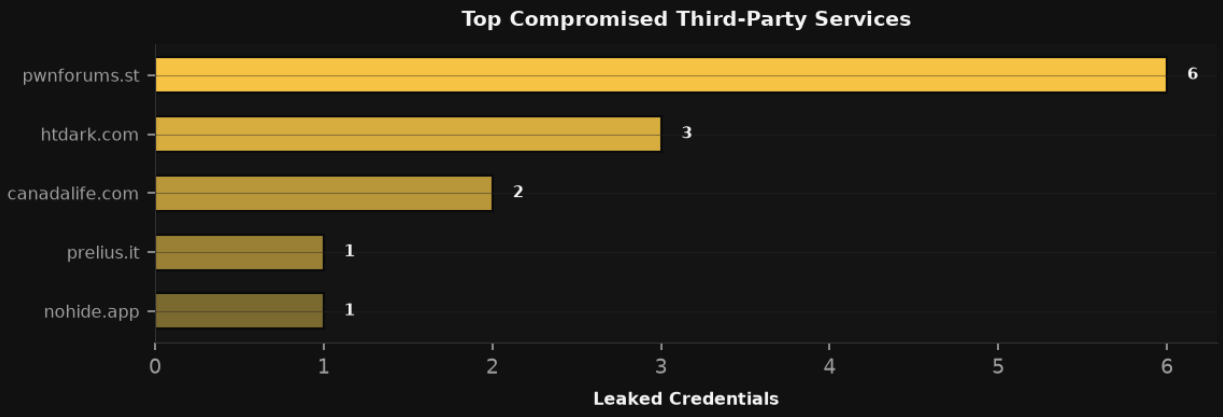
ÂGE DE PREMIÈRE VUE	ENREGISTREMENTS
Derniers 90 jours	8
90 jours – 1 an	18

Ce graphique montre **des enregistrements d'identifiants distincts** provenant de l'API de recherche de contenu de violation — chaque enregistrement représente une combinaison d'email distincte + mot de passe masqué sensible à la casse + serveur. Le flux a retourné 129 observations brutes ; 103 observations en double provenant de sources de fuite ont été supprimées avant le traçage.



Principaux services tiers compromis

Ce sont des plateformes **tiers** (non détenues par l'organisation) où des identifiants d'employés ont été trouvés dans des bases de données de violations et des journaux de voleurs. Cela ne signifie pas que ces plateformes ont été compromises — plutôt, les employés ont utilisé leur email professionnel pour s'inscrire à ces services, et ces identifiants ont ensuite été exposés dans des violations de données tierces. Les points de connexion appartenant aux propres domaines de l'organisation sont listés séparément ci-dessous.



Détails de l'exposition des identifiants (caviardés)

Affichage de 20 des 26 enregistrements (équilibré — max 3 lignes par adresse email afin que le tableau présente des utilisateurs concernés distincts plutôt que de répéter une boîte mail fortement violée). Données complètes dans `jeu de donnees de preuves prive` omises de cet échantillon public.

EMAIL	DOMAINE	SERVICE	MOT DE PASSE	RISQUE	PREMIÈRE VUE
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

EMAIL	DOMAINE	SERVICE	MOT DE PASSE	RISQUE	PREMIÈRE VUE
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

EMAIL	DOMAINE	SERVICE	MOT DE PASSE	RISQUE	PREMIÈRE VUE
			S***e (sample)		

Aperçu des violations

Le domaine du site web que vous avez soumis est **acmesample.com**, mais les enregistrements MX de l'organisation se résolvent à un apex enregistré différent utilisé pour les emails des employés. Le tableau ci-dessous compare l'**empreinte de la base de données de violation** de chacun : l'apex du site web couvre tout ce qui est indexé contre la marque publique, tandis que l'apex des emails couvre les fuites d'identifiants liées aux véritables boîtes mail des employés — souvent une empreinte beaucoup plus grande et la cible de nettoyage de plus haute priorité.

L'apex de l'email alternatif a été recherché uniquement dans la base de données de violation leak.center — son inventaire de sous-domaines, surface de port, vulnérabilités, etc. n'ont PAS été énumérés par cette analyse. Pour effectuer une analyse complète de la surface d'attaque sur l'apex de l'email, soumettez-le à nouveau comme cible principale ou sélectionnez `domain_mode=all` lors de la prochaine analyse.

Source : leak.center distinct-leak API. Les comptes sont agrégés à partir des valeurs resultCount à travers toutes les fuites où le domaine apparaît dans le contenu indexé. La correspondance de sous-chaîne par l'API en amont peut gonfler les comptes lorsque le nom de domaine enregistré est une sous-chaîne du domaine d'une autre organisation (par exemple, `acmesample.com` correspond également à `acmesample-group.com`) — les valeurs doivent être lues comme des indicateurs relatifs de pression d'exposition plutôt que comme des totaux exacts d'enregistrements uniques.

2
DOMAINES RECHERCHÉS

284
FUITES DISTINCTES TOTALES

2,038
TOTAL DES ENREGISTREMENTS DE VIOLATION

DOMAINE	FUITES DISTINCTES	TOTAL DES ENREGISTREMENTS	JOURNAUX DE VOLEUR	LISTES COMBINÉES	VIOLATIONS DE SITES WEB	DUMPS DE DB	ÉTIQUETTES PRINCIPALES / PLAGE DE DATES
acmesample.com CIBLE	282	2,036	33	55	48	17	compte (222) email (215) mot de passe (159) nom d'utilisateur (122) url (79) 2008-07-01 → 2026-08-15
acmesample.net APEX EMAIL	2	2	—	—	2	—	ip (2) nom (2) email (2) téléphone (2) dob (1) 2019-03-07 → 2020-01-01

Comment lire ce chapitre

Les journaux de vol indiquent que des logiciels malveillants infostealer ont compromis des points de terminaison (employé ou tiers) et ont exfiltré des magasins d'identifiants enregistrés faisant référence à ce domaine. **Les combolists** sont des recyclages d'emails/mots de passe agrégés — la plupart des paires sont utilisées pour des attaques par credential stuffing contre ce domaine même si elles n'ont pas été directement compromises. **Les violations de site web** signifient que le domaine lui-même (ou un service étroitement lié) a été compromis. **Les dumps de base de données** sont des exports SQL/CSV complets divulgués au public.

Chaque chapitre suivant (Évaluation des risques de contenu de violation, Violations connues impliquant cette organisation, Intelligence sur les données de violation) se concentre uniquement sur le **domaine cible** — les chiffres par domaine ici sont le seul endroit où chaque domaine analysé est comparé côte à côte.

Évaluation des risques liés au contenu de la violation

Analyse des renseignements sur les menaces du Darknet

L'organisation a été identifiée dans **282** sources de fuite distinctes, avec un total de **2036** enregistrements mentionnant son domaine, acmesample.com. La plage de dates d'exposition s'étend du **1er juillet 2008** à la fuite la plus récente le **15 août 2026**. Ce niveau d'exposition est considéré comme **ÉLEVÉ** pour une organisation de ce type, indiquant un risque significatif pour l'intégrité de ses données et sa posture de sécurité.

Les principales catégories de fuite incluent les journaux de voleurs, qui indiquent la présence de logiciels malveillants sur les appareils des employés ou des clients capturant des données sensibles en temps réel ; les combolists, qui sont des collections de paires nom d'utilisateur et mot de passe utilisées pour des attaques par bourrage d'identifiants ; et les violations de sites web/bases de données, représentant des compromissions directes de services spécifiques.

Les principaux risques pour l'organisation incluent des attaques par bourrage d'identifiants utilisant les **222** enregistrements de compte trouvés, le détournement de session via des cookies volés à partir des **159** enregistrements de mot de passe, et des tentatives de phishing utilisant les **215** adresses email exposées.

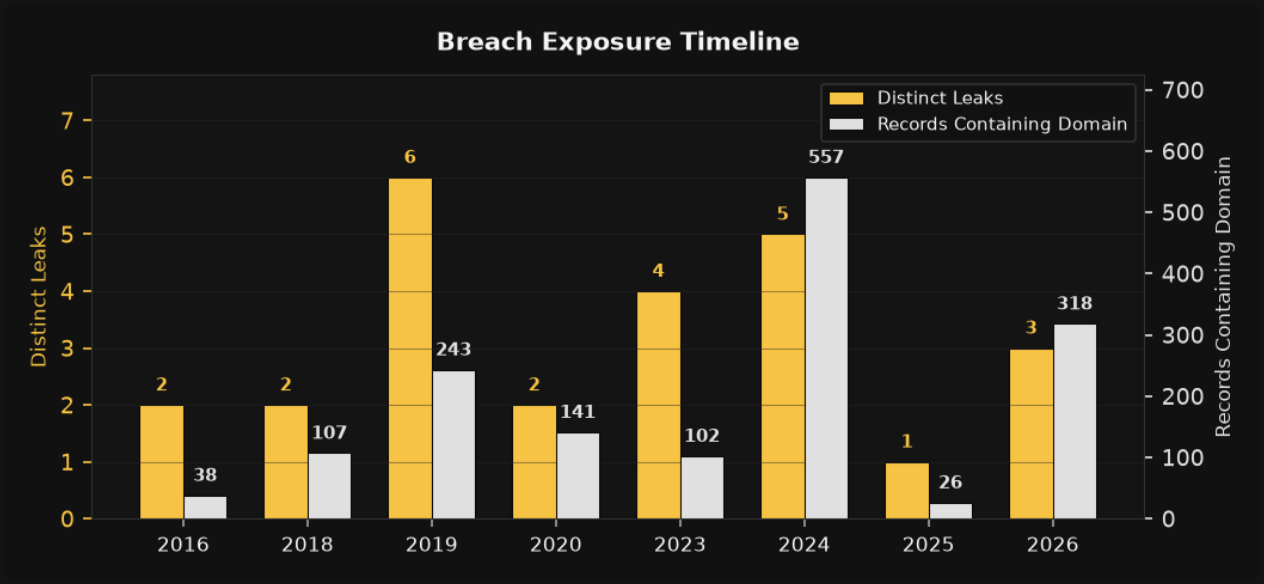
Étant donné que des journaux de voleurs ont été observés au cours des six derniers mois, l'organisation doit agir avec urgence pour réinitialiser les identifiants potentiellement actifs et appliquer l'authentification multi-facteurs afin d'atténuer les menaces immédiates.

Évaluation des risques liés au contenu de la violation

L'organisation présente une exposition significative de données sensibles, avec **384 adresses e-mail uniques** appartenant à son domaine trouvées dans la violation. Cette exposition inclut non seulement des adresses e-mail mais aussi **376 numéros de téléphone**, **48 adresses IP**, et **315 URL**. La présence de ces points de données indique un risque potentiel de vol d'identifiants, d'attaques d'ingénierie sociale et d'accès non autorisé aux systèmes internes.

Les risques d'attaque spécifiques associés à cette violation sont considérables. Les adresses e-mail divulguées peuvent être exploitées pour des attaques de **credential stuffing**, où les attaquants utilisent ces identifiants sur plusieurs plateformes pour obtenir un accès non autorisé. De plus, la présence de numéros de téléphone augmente le risque d'attaques de **spear-phishing** et d'**ingénierie sociale**, car les attaquants peuvent usurper l'identité de contacts de confiance. Les **adresses IP** et les **URL** trouvées dans les données peuvent faciliter la cartographie du réseau interne, permettant aux adversaires d'identifier des points d'entrée potentiels dans l'infrastructure de l'organisation.

Il est important de noter que les données de la violation semblent consister en des **combolists**, qui contiennent généralement un mélange de noms d'utilisateur et de mots de passe, plutôt que des dumps de bases de données complets ou des journaux de voleurs. Cela indique que, bien que l'organisation fasse face à des risques significatifs, les données peuvent ne pas inclure d'informations complètes sur les comptes utilisateurs, ce qui pourrait atténuer certaines menaces immédiates. Cependant, le volume même des données exposées nécessite une action urgente pour atténuer les risques et renforcer les mesures de sécurité.



Analyse des tendances de violation

L'analyse des données de la chronologie des violations révèle une tendance fluctuante dans la fréquence des nouvelles fuites et le volume des enregistrements associés au domaine de l'organisation. Au fil des ans, le nombre de fuites de données distinctes a varié, avec des pics notables en 2019 (6 fuites) et 2024 (5 fuites). Cependant, les comptes d'enregistrements montrent un pic plus prononcé en 2025, où 557 enregistrements ont été signalés, suggérant un incident significatif, probablement une violation à grande échelle plutôt que plusieurs petites fuites. Cette année se distingue par rapport à une moyenne de 1532 enregistrements à travers l'ensemble des fuites, indiquant qu'une seule violation majeure a pu se produire, impactant un nombre substantiel d'enregistrements.
D'un point de vue des risques, la présence de journaux de voleurs dans la distribution des types de fuites, avec 33 instances enregistrées, indique que des logiciels malveillants actifs pourraient cibler l'organisation. Les dates d'exposition vont de 2008 jusqu'à la plus récente en août 2026, suggérant que certaines fuites peuvent être historiques, tandis que d'autres sont récentes et potentiellement des menaces en cours. Compte tenu de ces constatations, l'organisation devrait prioriser l'amélioration de sa posture de cybersécurité, en se concentrant sur la surveillance des logiciels malveillants actifs et en s'attaquant aux vulnérabilités qui pourraient conduire à une exposition des données. De plus, des actions immédiates devraient être entreprises pour évaluer et atténuer les risques associés au nombre significatif d'enregistrements exposés en 2025.

Violations Connues Impliquant Cette Organisation

25 sources de fuite distinctes contenant 1 532 enregistrements mentionnant le domaine.

DATE	NOM DE LA FUITE	ENREGISTREMENTS	TYPES DE DONNÉES
2026-08-09	zoominfo.com darkforums.ru 081220…	**155**	privé, adresse, entreprise, téléphone, nom, email, url
2026-04-22	Pitney Bowes Inc. (pb.com)_shinyhun…	**46**	privé, adresse, entreprise, téléphone, identité, nom, email, nom d'utilisateur
2026-02-16	CORPS Combolist_breachforums.as 1…	**117**	mot de passe, mélange, email, nom d'utilisateur
2025-03-13	owcareers.com	**26**	mot de passe, privé, adresse, date de naissance, csv, nom, email, hachage, url, compte, nom d'utilisateur
2024-09-23	xiqonline.com	**38**	privé, adresse, entreprise, nom, email
2024-09-19	Emails uniques par Addka72424 et Br…	**19**	email
2024-09-12	pureb2b.co.uk	**128**	mot de passe, privé, adresse, entreprise, téléphone, csv, ip, nom, société, email, hash, compte
2024-08-15	demandscience CSV 15 août 2024	**342**	mot de passe, adresse, entreprise, téléphone, ip, nom, email, compte

DATE	NOM DE LA FUITE	ENREGISTREMENTS	TYPES DE DONNÉES
2024-04-07	epa.gov	**30**	privé, adresse, téléphone, csv, nom, entreprise, email
2023-06-11	Collecte des journaux de voleurs et d...	**14**	mot de passe, privé, entreprise, email, hachage, compte
2023-05-29	"CORP APB" identifiants d'entreprise f...	**18**	mot de passe, email, compte
2023-03-18	Linkedin_darkforumns.su 18 février 2...	**38**	privé, entreprise, téléphone, identité, csv, nom, url, nom d'utilisateur
2023-02-18	LinkedIn 18 février 2023	**32**	privé, adresse, entreprise, téléphone, csv, nom, société, url, nom d'utilisateur
2020-12-14	Compilation de violations	**16**	compte
2020-01-01	linkedin.com	**125**	mot de passe, privé, entreprise, nom, email

Affichage des 15 sources de fuite distinctes les plus récentes sur 25. Données complètes disponibles dans `jeu de donnees de preuves prive`.

Intelligence sur les données de violation

Analyse de **2,036** enregistrements de violation d'échantillon (sur **2,038** au total — Elasticsearch limite les exportations par requête à 2,036) révèle les types de données exposées suivants au-delà des identifiants :

388 EMAILS DES EMPLOYÉS	**376** NUMÉROS DE TÉLÉPHONE	**661** PROFILS LINKEDIN	**284** NOMS PERSONNELS
358 ADRESSES PHYSIQUES	**349** TITRES DE POSTE	**315** URLS	**48** ADRESSES IP

Pourquoi cela importe

Les données de violation contenant des noms personnels, des adresses physiques, des numéros de téléphone et des titres de poste permettent des attaques de phishing ciblées et d'ingénierie sociale. Les attaquants peuvent créer des prétextes convaincants en utilisant de vrais détails d'employés, augmentant considérablement le taux de réussite des campagnes de compromission d'email professionnel (BEC).

Échantillons de preuves de violation brutes

Extraits de véritables enregistrements de violation où le domaine de l'organisation a été trouvé. Les correspondances de domaine sont mises en évidence.

ENREGISTREMENT DE VIOLATION

[Enregistrement de violation anonymisé] **acmesample.com** [valeur d'identifiant retirée de l'échantillon public]

ENREGISTREMENT DE VIOLATION

[Enregistrement de violation anonymisé] **acmesample.com** [valeur d'identifiant retirée de l'échantillon public]

ENREGISTREMENT DE VIOLATION

[Enregistrement de violation anonymisé] **acmesample.com** [valeur d'identifiant retirée de l'échantillon public]

ENREGISTREMENT DE VIOLATION

[Enregistrement de violation anonymisé] **acmesample.com** [valeur d'identifiant retirée de l'échantillon public]

ENREGISTREMENT DE VIOLATION

[Enregistrement de violation anonymisé] **acmesample.com** [valeur d'identifiant retirée de l'échantillon public]

Analyse d'énumération et d'exposition des e-mails

Les boîtes mail appartenant à `acmesample.com` découvertes à travers quatre sources indépendantes : bases de données de violations de données, énumération publique Hunter.io, données de contact professionnelles RocketReach (adresses d'entreprise uniquement), et le registre Central API `unique_domain_emails`. Le titre **Boîtes Mail Identifiées** ci-dessous est l'union de découverte dédupliquée plus large de ce chapitre. Les chapitres axés sur les violations utilisent leur population de boîtes mail dérivée de violation séparément étiquetée.

100
EMPLOYÉS IDENTIFIÉS
VIA ROCKETREACH / APOLLO

498
BOÎTES MAIL IDENTIFIÉES
UNION DÉDUPLIQUÉE

390
AVEC EXPOSITION DE VIOLATION

75
ÉLEVÉ / CRITIQUE

Répartition des sources

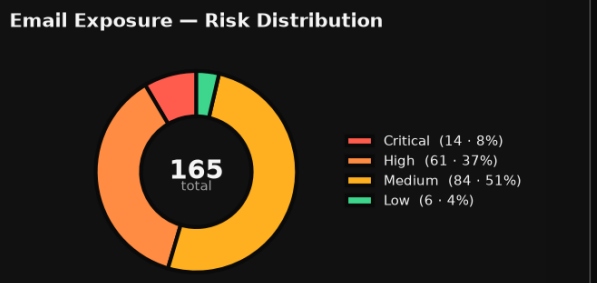
Chaque source est interrogée indépendamment ; la même boîte mail peut être découverte par plus d'un canal. La somme des lignes par source est donc généralement plus grande que le total dédupliqué de **498** boîtes mail.

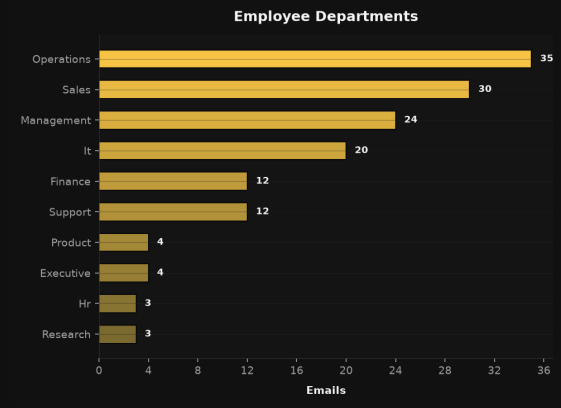
SOURCE	BOÎTES MAIL	NOTES
Bases de données de violations	390	Itération par fuite de leak.center à travers les 100 fuites les plus riches en données contenant `@acmesample.com` (et tous les domaines d'email alternatifs). Détail : `jeu de donnees de preuves prive`.
Hunter.io	165	Découverte d'emails publics sur internet (Hunter `/v2/domain-search`). Détail : `jeu de donnees de preuves prive`.
RocketReach	15	Emails de domaine d'entreprise résolus via une récolte `/person/lookup` dans le répertoire des employés de RocketReach. Détail : `jeu de donnees de preuves prive`.
Registre central des API	0	`unique_domain_emails` — un registre en amont sélectionné. Souvent vide pour des domaines très courts (par exemple, `tp.com`).
TOTAL (dédupliqué)	**498**	Union de découverte plus large utilisée par l'énumération d'emails (données de violation, Hunter.io, RocketReach, et le registre API central). Les chapitres axés sur les violations utilisent séparément la population de boîtes mail dérivée des violations. Voir `jeu de donnees de preuves prive` pour la piste d'audit complète.

Comment cela se rapporte aux autres chapitres

Nous avons identifié **100** personnes associées à `acmesample.com` via les données de réseau professionnel RocketReach (titres, employeur, localisation). L'endpoint `/person/search` de RocketReach renvoie uniquement des métadonnées — récupérer réellement une adresse e-mail nécessite un appel séparé `/person/lookup` par profil. Le chapitre People Intelligence recherche également les 15 cibles de la plus haute valeur (dirigeants) pour le chapitre VIP Intelligence ; leurs adresses professionnelles contribuent à la ligne RocketReach dans la répartition des sources. Le titre **498** "Boîtes Mail Identifiées" est l'union de découverte plus large pour ce chapitre : adresses observées dans les données de violation, Hunter.io, recherches RocketReach, ou le registre de l'API Central. L'Exposition d'Identifiants utilise la population de boîtes mail dérivée de violation plus étroite, donc les deux totaux ne sont intentionnellement pas interchangeables.

Parmi les **498** boîtes mail identifiées, **390** ont été observées dans au moins une violation de données connue. Parmi celles-ci, nous avons compté environ **26** enregistrements de fuite d'identifiants (login + mot de passe / paires de hachage). Le domaine plus large `acmesample.com` est mentionné dans **2,038** enregistrements de violation (tous champs — emails, URLs, hachages, pièces jointes) couvrant **282** bases de données de violation distinctes.





Double exposition

62 adresses email apparaissent dans les deux bases de données de violation ET les sources publiques sur Internet. Ces individus font face au risque le plus élevé — les attaquants peuvent combiner des identifiants divulgués avec des détails personnels disponibles publiquement (poste, profil LinkedIn) pour des attaques de spear-phishing et de compromission d'email professionnel (BEC) très ciblées.

Résumé

498 e-mails d'employés uniques découverts pour acmesample.com. 390 apparaissent dans des bases de données de violations de données. 165 sont visibles publiquement sur Internet. 62 e-mails trouvés à la fois dans des violations et des sources publiques représentent la plus haute exposition.

Top 3 Employés les Plus Exposés

Sélectionné en fonction de la seniorité organisationnelle (gestion, directeur, responsable) combinée avec la visibilité en ligne publique (nombre de sites web où l'adresse e-mail a été trouvée via OSINT)

Ces individus ont été sélectionnés parce que leur rôle élevé les rend attractifs pour les compromissions de courriels professionnels (BEC) et l'ingénierie sociale, tandis que leur forte visibilité en ligne les rend faciles à rechercher et à usurper. Les scores de violation/données/accès ci-dessous reflètent une exposition supplémentaire due à des violations de données.

CRITIQUE Vice-président de la gestion des produits avec mot de passe divulgué et compromission de l'appareil

employee058@acmesample.com · Vice-président de la gestion des produits (produit)

PRÉSENCE EN LIGNE	RÔLE DE L'ORGANISATION	EXPOSITION À LA VIOLATION	EXPOSITION DE DONNÉES	ACCÈS CRITIQUE
3 sites web publics	**Exécutif** Vice-président de la gestion des produits (produit)	**5**/5 43 violations · journal de vol · identifiants fuités	**1**/5 mot de passe	**1**/5 aucuns services critiques

Violation / Données / Accès mesurés de manière déterministe à partir des preuves de violation réconciliées (nombre d'enregistrements, présence de mots de passe/fureteurs divulgués, catégories PII distinctes et criticité du service d'identifiants).

L'email d'Executive012 Sample012 est apparu dans 43 violations de données, avec à la fois un mot de passe exposé et des preuves de compromission de l'appareil à travers des journaux de voleurs. Cela fait de lui une cible privilégiée pour les attaques de credential stuffing, pouvant mener à une prise de contrôle de compte. Avec son poste exécutif, il est également à risque pour des schémas de compromission d'email professionnel (BEC), surtout étant donné que son email est trouvable publiquement sur 3 sites web.

CRITIQUE Directeur Senior, Comptes Nationaux avec mot de passe divulgué

employee074@acmesample.com · Directeur Senior, Comptes Nationaux (finance)

PRÉSENCE EN LIGNE	RÔLE DE L'ORGANISATION	EXPOSITION À LA VIOLATION	EXPOSITION DE DONNÉES	ACCÈS CRITIQUE
7 sites web publics	**Exécutif** Directeur Senior, Comptes Nationaux (finance)	**5**/5 21 violations · identifiant compromis	**3**/5 mot de passe, téléphone, adresse	**1**/5 aucuns services critiques

Violation / Données / Accès mesurés de manière déterministe à partir des preuves de violation réconciliées (nombre d'enregistrements, présence de mots de passe/fureteurs divulgués, catégories PII distinctes et criticité du service d'identifiants).

L'Exécutif020 Sample020 a été exposé dans 21 violations, avec un mot de passe divulgué qui pourrait faciliter des attaques de stuffing d'identifiants. De plus, ses informations personnelles de téléphone et d'adresse sont compromises, le rendant vulnérable à des attaques d'ingénierie sociale ciblées. En tant que directeur senior, il est une cible précieuse pour les attaquants cherchant à exploiter son accès, et son email est trouvable sur 7 sites web publics.

CRITIQUE **Directeur Général avec exposition de données personnelles**

employee158@acmesample.com · Directeur Général (exécutif)

PRÉSENCE EN LIGNE	RÔLE DE L'ORGANISATION	EXPOSITION À LA VIOLATION	EXPOSITION DE DONNÉES	ACCÈS CRITIQUE
5 sites web publics	**Exécutif** Directeur général (exécutif)	**4**/5 8 violations	**3**/5 téléphone, adresse	**1**/5 aucuns services critiques

Violation / Données / Accès mesurés de manière déterministe à partir des preuves de violation réconciliées (nombre d'enregistrements, présence de mots de passe/fureteurs divulgués, catégories PII distinctes et criticité du service d'identifiants).

L'email d'Executive041 Sample041 est apparu dans 8 violations, mais manque notablement d'un mot de passe divulgué. Cependant, son téléphone personnel et son adresse sont exposés, le rendant susceptible à des attaques d'ingénierie sociale ciblées. En tant que PDG, il est une cible de grande valeur pour les attaquants visant le BEC, et son email est trouvable sur 5 sites web publics, augmentant le risque de tentatives de phishing sur mesure.

Cibles de grande valeur

AI-priorisé parmi 100 employés découverts via OSINT (RocketReach / Apollo). GPT-4o évalue l'autorité de rôle, le potentiel d'accès système et la valeur de ciblage pour classer les individus à risque le plus élevé.

100
EMPLOYÉS DÉCOUVERTS

10
CIBLES DE GRANDE VALEUR

Sur **100** employés identifiés via OSINT, les **10** individus suivants représentent les cibles de la plus haute valeur pour le compromis d'email professionnel (BEC), l'ingénierie sociale et les campagnes de phishing ciblées — sélectionnés en fonction de l'autorité organisationnelle, des privilèges d'accès au système et de la visibilité publique. La liste complète des employés avec tous les 100 enregistrements est disponible dans `jeu de donnees de preuves prive`.

E

MOYEN **Executive144 Sample144**

Directeur, Qualité, Inspections et Retours · 100 Market Street, Sample City

CORPORATE ✉ employee532@acmesample.com [A]

LinkedIn

En tant que Directeur, cette personne peut avoir accès à des données opérationnelles sensibles et à des processus de contrôle de la qualité, ce qui en fait une cible pour les attaquants cherchant à perturber les opérations ou à obtenir des informations sur la qualité des produits.

E

ÉLEVÉ **Exécutif052 Échantillon052**

Vice-président exécutif, opérations · 100 Market Street, Sample City

CORPORATE ✉ employee250@acmesample.com [A]

LinkedIn

Dans le rôle de Vice-Président Exécutif, cet individu a probablement une autorité décisionnelle significative sur les processus opérationnels et les relations avec les fournisseurs, ce qui pourrait être exploité à des fins de gain financier ou de perturbation opérationnelle.

E

ÉLEVÉ **Executive156 Sample156**

Senior Manager - Finance Services and Treasury · 100 Market Street, Sample City

CORPORATE ✉ employee565@acmesample.com [A]

LinkedIn

Le rôle de cet individu dans les finances et la trésorerie lui donne accès à des données financières sensibles et une autorité potentielle sur les transactions financières, faisant de lui une cible privilégiée pour les attaquants cherchant à manipuler les systèmes financiers.

E

ÉLEVÉ **Executive035 Sample035**

Directeur senior des comptes stratégiques · 100 Market Street, Sample City

CORPORATE ✉ employee148@acmesample.com [A]

PERSONNEL ✉ employee480@examplemail.com (fournisseur de mail grand public — pas de fuite de domaine cible)

LinkedIn Twitter

En tant que Directeur Senior supervisant des comptes stratégiques, cette personne peut avoir accès à des informations critiques sur les clients et des contrats, ce qui la rend vulnérable aux attaques d'ingénierie sociale visant à extraire des informations commerciales sensibles.

E

ÉLEVÉ **Exécutif126 Sample126**

Directeur, Ingénierie · 100 Market Street, Sample City

CORPORATE ✉ employee484@acmesample.com [A]

LinkedIn

L'expertise technique de ce Directeur et son potentiel accès aux systèmes d'ingénierie pourraient fournir aux attaquants des informations précieuses ou un contrôle sur des infrastructures critiques, ce qui en fait une cible significative.

E

CRITIQUE **Exécutif005 Échantillon005**

Directeur de la culture · 100 Market Street, Sample City

CORPORATE ✉ employee009@acmesample.com [A]

LinkedIn

En tant que cadre de niveau C, cette personne détient un haut niveau d'influence et d'accès à des données sensibles sur la culture organisationnelle et les ressources humaines, ce qui en fait une cible critique pour les attaquants cherchant à exploiter les informations sur les ressources humaines.

E

CRITIQUE **Exécutif083 Sample083**

Vice-président des technologies de l'information · 100 Market Street, Sample City

CORPORATE ✉ employee343@acmesample.com [A]

LinkedIn

Dans le rôle de VP des TI, cette personne possède probablement des identifiants administratifs et un accès à des infrastructures TI critiques, ce qui en fait une cible privilégiée pour les attaquants visant à compromettre la sécurité de l'organisation.

E

ÉLEVÉ **Executive039 Sample039**

Directeur des ventes comptes stratégiques · 100 Market Street, Sample City

CORPORATE ✉ employee162@acmesample.com [A]

LinkedIn

L'accès de ce Directeur des Ventes à des informations stratégiques sur les comptes et aux relations clients pourrait être exploité par des attaquants pour obtenir des informations sur les opérations commerciales ou manipuler les interactions avec les clients.

E

MOYEN **Executive003 Sample003**

Directeur Excellence Opérationnelle · 100 Market Street, Sample City

CORPORATE ✉ employee006@acmesample.com [A]

LinkedIn

En tant que Directeur axé sur l'excellence opérationnelle, cet individu peut avoir accès à des données et processus opérationnels sensibles, faisant de lui une cible pour les attaquants cherchant à perturber l'efficacité ou à obtenir des renseignements concurrentiels.

E

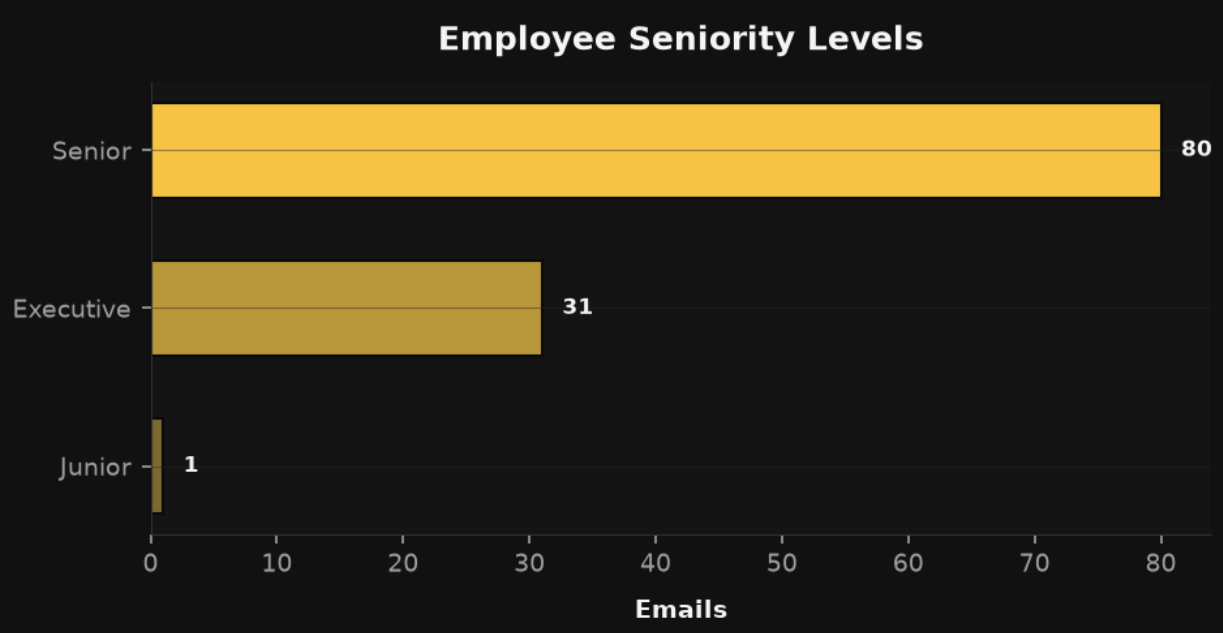
MOYEN **Exécutif072 Échantillon072**

Directeur, People & Culture · 100 Market Street, Sample City

CORPORATE ✉ employee299@acmesample.com [A]

LinkedIn

Le rôle de cet individu dans la gestion des personnes et de la culture peut donner accès à des données sensibles des employés, faisant de lui une cible pour les attaquants cherchant à exploiter des informations personnelles pour des attaques d'ingénierie sociale.



Principales sources de violation

FUITE / VIOLATION	E-MAILS AFFECTÉS
demandscience CSV 15 août 2024	41
pureb2b.co.uk	16
demandscience	12
CORPS Combolist_breachforums.as 16.02.2026	10

FUITE / VIOLATION	E-MAILS AFFECTÉS
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 FULL 22.04.2026 csv	2
canadalife.com_260429	2
UnderArmour_breachforums.bf 15.11.2025	2

Exposition des Emails — Extrait d'Échantillon

Top 20 par score de risque. Ensemble de données complet avec tous les 100 enregistrements et détails des scores disponibles dans `jeu de donnees de preuves prive`.

EMAIL	NOM	POSITION	RISQUE	VIOL-ATIONS	PWD	SRC WEB
employee074@acmesample.com	Executive020 Sample020	Directeur senior, Comptes nationaux	100	21	1	7
employee158@acmesample.com	Executive041 Sample041	Directeur général	95	8	—	5
employee058@acmesample.com	Executive012 Sample012	Vice-président de la gestion des produits	90	43	3	3
employee489@acmesample.com	Executive132 Sample131	Directeur des ressources humaines	80	7	—	1
employee009@acmesample.com	Exécutif005 Échantillon005	Directeur de la culture	80	6	—	1
employee163@acmesample.com	Executive036 Sample036	Vice-président de la distribution	80	8	—	1
employee425@acmesample.com	Executive124 Sample124	Vice-Président des Ventes	70	2	—	5
employee220@acmesample.com	Exécutif050 Échantillon050	Inspecteur de contrôle qualité	70	3	—	1
employee273@acmesample.com	Executive067 Sample067	Directeur Financier	70	5	—	1

EMAIL	NOM	POSITION	RISQUE	VIOL-ATIONS	PWD	SRC WEB
employee324@acmesample.com	Exécutif081 Sample081	Directeur de district	70	4	—	6
employee437@acmesample.com	Exécutif121 Échantillon121	Assistant exécutif	70	3	—	1
employee319@acmesample.com	Executive078 Sample078	Responsable marketing produit	70	6	—	4
employee533@acmesample.com	Executive146 Sample146	Responsable des ventes régionales	65	6	—	1
employee548@acmesample.com	Executive152 Sample152	Responsable des Ventes	65	8	—	1
employee526@acmesample.com	Executive148 Sample148	Vice-Président des Ventes	60	0	—	5
employee181@acmesample.com	Executive044 Sample044	Directeur des Ventes	60	0	—	6
employee148@acmesample.com	Executive035 Sample035	Directeur senior des comptes stratégiques	60	0	—	6
employee162@acmesample.com	Executive039 Sample039	Directeur des Ventes	60	0	—	6
employee484@acmesample.com	Exécutif126 Sample126	Directeur de l'ingénierie	60	2	—	1
employee160@acmesample.com	Executive037 Sample037	Inspecteur de contrôle qualité	60	2	—	1

EMPREINTE NUMÉRIQUE VIP

Renseignement OSINT sur des cibles de grande valeur — comptes Google, récupération Microsoft, détection de compte, exposition de violation, analyse de mot de passe

Cette évaluation a examiné la posture de sécurité en ligne de 20 cadres d'entreprise, directeurs et managers de grande valeur. Les données ont été agrégées à partir de plusieurs sources, y compris des analyses de comptes Google, des vérifications de comptes de récupération Microsoft, la détection de comptes Holehe et diverses bases de données de violations. Un total de 17 comptes email ont été testés, révélant des vulnérabilités significatives dans l'ensemble, avec 12 identifiants Google et 9 comptes de récupération Microsoft identifiés. Les constatations clés indiquent des expositions alarmantes, y compris 360 instances de fuite d'identifiants, plusieurs cadres ayant des mots de passe compromis. Notamment, plusieurs individus avaient des données de localisation accessibles via des avis Google Maps, ce qui pourrait faciliter un ciblage physique. La présence d'adresses email de récupération et de numéros de téléphone augmente encore le risque de campagnes de phishing ciblées et d'attaques par remplissage d'identifiants. Par exemple, 5 cadres ont été trouvés avec plusieurs comptes associés sur Holehe, indiquant une probabilité plus élevée de réutilisation d'identifiants sur différentes plateformes. Le niveau de risque global pour la direction de l'organisation est évalué comme élevé. Un attaquant pourrait tirer parti de ces informations pour un phishing ciblé, en utilisant des mots de passe et des informations personnelles divulgués pour exécuter des attaques d'ingénierie sociale. Le potentiel d'accès non autorisé à des données et systèmes d'entreprise sensibles représente une menace significative pour l'intégrité et la continuité opérationnelle de l'organisation. Une action immédiate est recommandée pour renforcer les protocoles de sécurité et atténuer ces vulnérabilités.

17
EMAILS TESTÉS

12
IDENTIFIANTS GOOGLE

9
RÉCUPÉRATION MS

11
COMPTES

360
CONSTATATIONS DE VIOLATION

ES

Executive012 Sample012

Vice-président de la gestion des produits

employee058@acmesample.com

Executive012 Sample012, Vice-Président de la Gestion des Produits chez Acme Sample GmbH, a une empreinte numérique significative avec plusieurs enregistrements de violation exposant des identifiants d'entreprise et personnels. La réutilisation d'un modèle de mot de passe faible sur plusieurs sites et l'exposition de données personnelles telles que des adresses physiques et des numéros de téléphone partiels augmentent le risque d'attaques ciblées. Cette exposition pourrait conduire à un accès non autorisé à des systèmes d'entreprise sensibles et à des comptes personnels, posant un risque CRITIQUE pour la sécurité personnelle et organisationnelle.

177
CONSTATATIONS DE VIOLATION

0
PLATEFORMES

2
PREUVES DE RÉCUPÉRATION

3
SOURCES DE VIOLATION

SCORE D'EXPOSITION **CRITIQUE**

85/100

Potentiel d'attaque personnalisé · plus élevé = plus exposé

Basé sur 177 enregistrements de violation · 2 preuves de récupération · mot de passe divulgué · réutilisation de mot de passe
Évalué par modèle, limité par des preuves déterministes minimales/maximales

EMPREINTE NUMÉRIQUE

@ Adresses e-mail
employee058@acmesample.com, employee059@examplemail.com, employee057@examplemail.com

A Adresse Physique
100 Market Street, Sample City; 100 Market Street, Sample City

T Numéros de téléphone
+1 202-555-1013

R Emails de récupération / alternatifs
employee057@examplemail.com, email : employee058@acmesample.com, téléphone : (***) ***-**00

P Lieux Observés
Sample City, Canada; Sample City, Canada; Sample City, Canada; Sample City, Canada; Sample City, Canada

G Google ID confirmé
GAIA sample-45352… · 10 avis

ANALYSE DES MOTS DE PASSE

6	OUI	FAIBLE	S***E (SAMPLE)
MOTS DE PASSE UNIQUES	RÉUTILISATION	FORCE	PRÉDIRE.

S***e (échantillon) S***E (SAMPLE) S***e (échantillon)
S***e (échantillon) S***E (SAMPLE) S***e (échantillon)
S***e (échantillon) S***E (SAMPLE) S***e (échantillon)
S***e (échantillon) S***E (SAMPLE) S***e (échantillon)

- S***e (échantillon)
- S***e (échantillon)
- S***e (échantillon)

Réutilisation : S***e (échantillon) trouvé sur S***e (échantillon), S***e (échantillon)

Réutilisation : S***e (échantillon) trouvé sur S***e (échantillon), S***e (échantillon)

S***e (échantillon)

CRITIQUE : Même mot de passe utilisé sur l'email professionnel ET personnel. Le mot de passe 'S*e (échantillon)' a été trouvé sous les emails professionnels (employee058@acmesample.com) et personnels (employee057@examplemail.com), indiquant une réutilisation critique.**

INTELLIGENCE PERSONNELLE

Examen du lieu d'échantillon 01 dans la ville d'échantillon, Canada le 2026-07-04 — probablement un voyage de loisirs

Avis Google Maps · élevé

Examen du lieu d'échantillon 02 dans la ville d'échantillon, Canada le 2026-05-04 — probablement une visite fréquente

Avis Google Maps · élevé

Examen du lieu d'échantillon 03 dans la ville d'échantillon, Canada le 2022-09-02 — probablement lié à un service

Avis Google Maps · élevé

Travaille dans le secteur de la fabrication industrielle après-vente en tant que Vice-Président de la gestion des produits

Linkedin_darkforumns.su 18 février 2023 · élevé

L'indicatif régional suggère l'emplacement : ville d'échantillon, Canada

Linkedin_darkforumns.su 18 février 2023 · moyen

PERSONNALITÉ

valeurs service de qualité · apprécie le personnel serviable

INTÉRÊTS

sports · dining

DÉCLENCHEURS ÉMOTIONNELS

apprécie le service utile · valorise les expériences culinaires de qualité

STYLE DE VIE

voyageur fréquent · s'engage dans des activités de loisirs

VECTEURS D'ATTAQUE

Credential Stuffing	ÉLEVÉ
Spear Phishing - Vérification des Identifiants d'Entreprise	ÉLEVÉ
Spear Phishing - Alerte de sécurité des médias sociaux	MOYEN
Ingénierie sociale - Arnaque aux récompenses de restauration	MOYEN

RISQUE D'IDENTIFIANTS : Stuffing: **VIABLE** · Spray : **VIABLE**

PRÉTEXTES DE PHISHING CIBLÉ — UN SCÉNARIO PAR POINT DE DONNÉES OSINT

Chaque ligne ci-dessous associe UN point de données OSINT spécifique concernant cette personne (un enregistrement de violation, un compte détecté par Holehe, un avis Google, un modèle de mot de passe, un réemploi de mot de passe corporate↔personnel, ou un service d'entreprise détecté) avec le prétexte d'attaque concret qu'un adversaire pourrait élaborer à partir de ces données exactes. La colonne “Source” est la citation explicite qui rend le prétexte crédible — elle répond à la question « pourquoi cette attaque est-elle réalisable ? ». Le rendement est l'estimation de GPT de la probabilité qu'une véritable attaque réussisse contre cet individu compte tenu de ce signal. Affichage de jusqu'à 6 des 6 prétextes dérivés pour ce profil (cap: 20).

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
VIOLATION	**CORP APB** VIOLATION	Fuite d'identifiants d'entreprise CORP APB mai 2023	Acme Sample GmbH : Vos identifiants d'entreprise ont peut-être été compromis. Vérifiez votre identité ici. violation récente + contexte d'entreprise	ÉLEVÉ
VIOLATION	**Twitter** VIOLATION	Fuite de données Twitter de 1,5 M exposant l'email + le mot de passe pour employee057@examplemail.com	Twitter : Connexion inhabituelle détectée. Sécurisez votre compte ici. violation des réseaux sociaux + email personnel	MOYEN

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
MODÈLE	**S***e (sample)** MOT DE PASSE	Modèle de mot de passe 'S***e (exemple)' observé dans 10 violations	Acme Sample GmbH IT : Modèle de mot de passe faible détecté. Mettez à jour votre politique de mot de passe ici. modèle de mot de passe courant + multiples violations	MOYEN
AVIS	**Échantillon de lieu 01** EXAMEN	Avis sur Sample Venue 01 à Sample City, Canada le 2026-07-04 (5/5)	Échantillon de Lieu 01 Échantillon Ville : Merci pour votre récente visite ! Réclamez votre récompense de fidélité ici. avis positif récent + restauration fréquente	MOYEN
AVIS	**Échantillon de lieu 02** EXAMEN	Avis sur Sample Venue 02 à Sample City, Canada le 2026-05-04 (5/5)	Échantillon de Lieu 02 : Nous apprécions vos retours ! Profitez d'une remise de 10 % sur votre prochain achat. avis positif + intérêt pour le sport	MOYEN
AVIS	**Échantillon de lieu 03** EXAMEN	Avis sur Sample Venue 03 à Sample City, Canada le 2022-09-02 (5/5)	Échantillon de lieu 03 : Votre satisfaction de service est notre priorité. Réclamez votre bon de service ici. avis positif + satisfaction de service	MOYEN

COMPORTEMENT & MODÈLES DE VOYAGE — À PARTIR DE 10 AVIS GOOGLE

Un attaquant peut créer des prétextes personnalisés (invitations à de faux événements, leurres de fournisseurs de confiance, phishing en contexte familial) en utilisant les emplacements, les entreprises et le timing visibles dans l'activité publique de Google Maps de cette personne. Chaque ligne ci-dessous est un véritable avis — la colonne « angle d'exploitation » est le crochet d'ingénierie sociale dérivé de GPT.

ENTREPRISE / LIEU	EMPLACEMENT	ÉVALUATION	DATE	ANGLE D'EXPLOITATION
Échantillon de lieu 01	Sample City	5/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de Lieu 02	Sample City	5/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de lieu 03	Sample City	5/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de Lieu 04	Sample City	4/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de lieu 05	Sample City	3/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Sample Venue 06	Sample City	5/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Sample Venue 07	Sample City	3/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de Lieu 08	Sample City	4/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de lieu 09	Sample City	1/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.
Échantillon de lieu 10	Sample City	5/5	—	L'activité de révision publique soutient un prétexte de lieu de routine ; les détails du lieu et de l'emplacement sont supprimés de cet échantillon public.

ES

Executive020 Sample020

Directeur senior, Comptes nationaux

employee074@acmesample.com

L'Exécutif020 Sample020, un Directeur Senior chez Acme Sample GmbH, présente une exposition à haut risque en raison de multiples violations impliquant des fuites d'identifiants. Ces violations concernent des plateformes significatives telles que LinkedIn et Trello, avec des preuves de modèles de réutilisation de mots de passe. L'exposition de son adresse physique et d'un numéro de téléphone partiel augmente encore le risque, permettant des attaques ciblées potentielles. Une remédiation immédiate est recommandée pour atténuer ces risques.

26
CONSTATATIONS DE VIOLATION

1
PLATEFORMES

2
PREUVES DE RÉCUPÉRATION

6
SOURCES DE VIOLATION

SCORE D'EXPOSITION

ÉLEVÉ

85/100

Potentiel d'attaque personnalisé · plus élevé = plus exposé

Basé sur 26 enregistrements de violation · 1 compte · 2 preuves de récupération · mot de passe divulgué

Évalué par modèle, limité par des preuves déterministes minimales/maximales

EMPREINTE NUMÉRIQUE

@ **Adresses e-mail**
employee074@acmesample.com

A **Adresse Physique**
100 Market Street, Sample City

T **Numéros de téléphone**
+1 202-555-1015

R **Emails de récupération / alternatifs**
email: employee074@acmesample.com,
téléphone: ********68

W **Comptes détectés**
office365

P **Lieux Observés**
Sample City, CA

G **Google ID confirmé**
GAIA sample-19499...

ANALYSE DES MOTS DE PASSE

5
MOTS DE PASSE UNIQUES

NON
RÉUTILISATION

FAIBLE
FORCE

S*E (SAMPLE)**
PRÉDIRE.

S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)

- S***e (échantillon)
- S***e (échantillon)
- S***e (échantillon)

S***e (échantillon)

INTELLIGENCE PERSONNELLE

Travaille dans le secteur des transports en tant qu'analyste commercial chez Acme Sample GmbH (100-249 employés)

DemandScience CSV · élevé

Tranche de revenus de 50 à 99 millions $

DemandScience CSV · élevé

VECTEURS D'ATTAQUE

Credential Stuffing	ÉLEVÉ
Phishing ciblé	MOYEN
Vishing	MOYEN
Accès physique	FAIBLE

RISQUE D'IDENTIFIANTS : Stuffing: **VIABLE** · Spray : **VIABLE**

PRÉTEXTES DE PHISHING CIBLÉ — UN SCÉNARIO PAR POINT DE DONNÉES OSINT

Chaque ligne ci-dessous associe UN point de données OSINT spécifique concernant cette personne (un enregistrement de violation, un compte détecté par Holehe, un avis Google, un modèle de mot de passe, un réemploi de mot de passe corporate↔personnel, ou un service d'entreprise détecté) avec le prétexte d'attaque concret qu'un adversaire pourrait élaborer à partir de ces données exactes. La colonne “Source” est la citation explicite qui rend le prétexte crédible — elle répond à la question « pourquoi cette attaque est-elle réalisable ? ». Yield est l'estimation de GPT de la probabilité qu'une véritable attaque réussisse contre cet individu compte tenu de ce signal. Affichage jusqu'à 5 de 5 prétextes dérivés pour ce profil (cap : 20).

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
VIOLATION	**Zacks.com** FINANCE	Journal de vol ULP 21.04.2025 capturé employee074@acmesample.com sur Zacks.com en utilisant le mot de passe S***e (exemple)	Activité inhabituelle détectée sur votre compte Zacks. Confirmez vos transactions récentes ici. Le journal de vol fournit une capture directe des identifiants avec une date récente.	ÉLEVÉ
SERVICE	**Office365** PRODUCTIVITÉ	Holehe a confirmé que le compte existe sur office365 pour l'email employee074@acmesample.com	Votre compte Office365 nécessite une vérification immédiate. Cliquez ici pour sécuriser votre compte. Existence du compte confirmée sur une plateforme de productivité.	MOYEN
VIOLATION	**Trello.com** PRODUCTIVITÉ	Compilation de violations exposée email + mot de passe pour Trello.com	Appât ciblé faisant référence à Trello.com ; le libellé original a été supprimé de cet échantillon public. Les données de violation incluent email et mot de passe pour un outil de productivité.	MOYEN
VIOLATION	**xiqonline.com** AUTRE	Compilation de violations exposée email + mot de passe pour xiqonline.com	Votre compte xiqonline a été signalé pour activité suspecte. Vérifiez les détails de votre compte ici. Les données de violation incluent email et mot de passe pour un service moins connu.	MOYEN
MODÈLE	**S***e (sample)** MOT DE PASSE	Mot de passe motif 'S***e (exemple)' + suffixe numérique observé dans plusieurs violations	Notre système a détecté une correspondance de motif faible par rapport à votre mot de passe historique (S***e (exemple)). Mettez à jour votre mot de passe ici. Mot de passe faible réutilisé à travers plusieurs violations.	MOYEN

ES

Executive040 Sample040

Responsable Technique IT

employee157@acmesample.com

Executive040 Sample040, un Responsable Technique IT chez Acme Sample GmbH, a été exposé dans plusieurs violations de données, y compris une qui a révélé des PII complètes. Cette exposition inclut des informations sur l'email, le mot de passe, le téléphone et l'adresse, qui pourraient être exploitées pour des attaques ciblées. La réutilisation de modèles de mots de passe faibles sur différentes plateformes aggrave encore le risque, rendant à la fois les comptes personnels et professionnels vulnérables à une compromission.

11
CONSTATATIONS DE VIOLATION

5
PLATEFORMES

1
PREUVES DE RÉCUPÉRATION

2
SOURCES DE VIOLATION

SCORE D'EXPOSITION

ÉLEVÉ

80/100

Potentiel d'attaque personnalisé · plus élevé = plus exposé

Basé sur 11 enregistrements de violations · 5 comptes · 1 preuve de récupération · mot de passe divulgué
Évalué par modèle, limité par des preuves déterministes minimales/maximales

EMPREINTE NUMÉRIQUE

@ Adresses e-mail
employee157@acmesample.com,
employee161@examplemail.com

A Adresse Physique
100 Market Street, Sample City; 100 Market Street, Sample City

T Numéros de téléphone
+1 202-555-1016, +1 202-555-1017

R Emails de récupération / alternatifs
téléphone : ********43

W Comptes détectés
hubspot, office365, gravatar, spotify

P Lieux Observés
Sample City, Canada

G Google ID confirmé
GAIA sample-69845...

ANALYSE DES MOTS DE PASSE

1	NON	FAIBLE	S***E (SAMPLE)
MOTS DE PASSE UNIQUES	RÉUTILISATION	FORCE	PRÉDIRE.

S***e (échantillon) S***E (SAMPLE) S***e (échantillon)

- S***e (échantillon)

S***e (échantillon)

INTELLIGENCE PERSONNELLE

Travaille dans l'industrie informatique en tant que Responsable Technique IT chez Acme Sample GmbH

DemandScience CSV · élevé

Navigateur/session tracé à Sample City, Canada

Session de journal de vol · moyen

L'indicatif régional suggère l'emplacement : ville d'échantillon, Canada

DemandScience CSV · élevé

VECTEURS D'ATTAQUE

Phishing ciblé via la violation de Pitney Bowes	ÉLEVÉ
Credential Stuffing sur Office365	MOYEN
Vishing utilisant des numéros de téléphone exposés	MOYEN

RISQUE D'IDENTIFIANTS : Stuffing: **VIABLE** · Spray : **VIABLE**

PRÉTEXTES DE PHISHING CIBLÉ — UN SCÉNARIO PAR POINT DE DONNÉES OSINT

Chaque ligne ci-dessous associe UN point de données OSINT spécifique concernant cette personne (un enregistrement de violation, un compte détecté par Holehe, un avis Google, un modèle de mot de passe, un réemploi de mot de passe corporate↔personnel, ou un service d'entreprise détecté) avec le prétexte d'attaque concret qu'un adversaire pourrait élaborer à partir de ces données exactes. La colonne “Source” est la citation explicite qui rend le prétexte crédible — elle répond à la question « pourquoi cette attaque est-elle réalisable ? ». Le rendement est l'estimation de GPT de la probabilité qu'une véritable attaque réussisse contre cet individu compte tenu de ce signal. Affichage de jusqu'à 3 des 3 prétextes dérivés pour ce profil (cap : 20).

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
VIOLATION	**Pitney Bowes Inc. (pb.com)** VIOLATION	Pitney Bowes Inc. (pb.com)_ shinyhunters FULL 22.04.2026 csv exposé PII complète (nom, adresse, téléphone) pour employee157@acmesample.com	Alerte de sécurité Pitney Bowes : Confirmez votre identité pour sécuriser votre compte. violation récente avec exposition PII complète	ÉLEVÉ
SERVICE	**Office365** PRODUCTIVITÉ	Holehe a confirmé qu'un compte existe à Office365 pour l'email employee157@acmesample.com	Votre compte Office365 a été accédé depuis un nouvel appareil. Cliquez ici pour vérifier. confirmation de compte d'entreprise	MOYEN
MODÈLE	**Général** MOT DE PASSE	Mot de passe motif 'S***e (exemple)' observé dans la violation xiqonline.com	Notre système a détecté une correspondance de motif faible par rapport à votre mot de passe historique. Mettez à jour vos identifiants ici. mot de passe faible observé	MOYEN

ES

Executive035 Sample035

Directeur Senior des Comptes Stratégiques

employee148@acmesample.com

Executive035 Sample035, un directeur senior chez Acme Sample GmbH, a été identifié avec plusieurs comptes violés, y compris Luxottica, Houzz et AT&T, avec des mots de passe exposés. La réutilisation de modèles de mots de passe similaires à travers ces violations représente un risque CRITIQUE pour la sécurité personnelle et d'entreprise. De plus, la présence d'emails alternatifs et de numéros de téléphone partiels augmente le potentiel d'attaques de phishing et de vishing ciblées.

79 CONSTATATIONS DE VIOLATION

1 PLATEFORMES

2 PREUVES DE RÉCUPÉRATION

4 SOURCES DE VIOLATION

SCORE D'EXPOSITION — ÉLEVÉ

80/100

Potentiel d'attaque personnalisé · plus élevé = plus exposé

Basé sur 79 enregistrements de violation · 1 compte · 2 preuves de récupération · mot de passe divulgué · réutilisation de mot de passe

Évalué par modèle, limité par des preuves déterministes minimales/maximales

EMPREINTE NUMÉRIQUE

Adresses e-mail

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

Numéros de téléphone

+1 202-555-1014

Emails de récupération / alternatifs

employee480@examplemail.com,
employee481@examplemail.com, email:
employee480@examplemail.com, téléphone:
--**76

Comptes détectés

office365

Google ID confirmé

GAIA sample-95896...

ANALYSE DES MOTS DE PASSE

5 MOTS DE PASSE UNIQUES

OUI RÉUTILISATION

FAIBLE FORCE

S*E (SAMPLE)** PRÉDIRE.

S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)
S***e (échantillon)	S***E (SAMPLE)	S***e (échantillon)

- S***e (échantillon)
- S***e (échantillon)
- S***e (échantillon)

Réutilisation : S***e (échantillon) trouvé sur S***e (échantillon), S***e (échantillon)

Réutilisation : S***e (échantillon) trouvé sur S***e (échantillon), S***e (échantillon)

S***e (échantillon)

CRITIQUE : Même mot de passe utilisé sur l'email professionnel ET personnel. Le mot de passe 'S*e (sample)' a été trouvé sous l'email professionnel (employee148@acmesample.com) et l'email personnel (employee481@examplemail.com), indiquant un problème critique de réutilisation.**

INTELLIGENCE PERSONNELLE

Travaille dans des comptes stratégiques chez Acme Sample GmbH
DemandScience CSV · élevé

Session de navigateur tracée aux États-Unis
Session de journal de vol · moyen

L'indicatif régional suggère une localisation : États-Unis
Session de journal de vol · moyen

VECTEURS D'ATTAQUE

Credential Stuffing	ÉLEVÉ
Phishing ciblé	MOYEN
Vishing	MOYEN

RISQUE D'IDENTIFIANTS : Stuffing: **VIABLE** · Spray : **VIABLE**

PRÉTEXTES DE PHISHING CIBLÉ — UN SCÉNARIO PAR POINT DE DONNÉES OSINT

Chaque ligne ci-dessous associe UN point de données OSINT spécifique concernant cette personne (un enregistrement de violation, un compte détecté par Holehe, un avis Google, un modèle de mot de passe, un réemploi de mot de passe corporate↔personnel, ou un service d'entreprise détecté) avec le prétexte d'attaque concret qu'un adversaire pourrait élaborer à partir de ces données exactes. La colonne “Source” est la citation explicite qui rend le prétexte crédible — elle répond à la question « pourquoi cette attaque est-elle réalisable ? ». Yield est l'estimation de GPT de la probabilité qu'une véritable attaque réussisse contre cet individu compte tenu de ce signal. Affichage jusqu'à 5 de 5 prétextes dérivés pour ce profil (cap : 20).

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
SERVICE	**Office 365** PRODUCTIVITÉ	Holehe a confirmé que le compte existe sur office365 pour l'email employee148@acmesample.com	Votre compte Office 365 présente une activité inhabituelle. Veuillez vérifier votre connexion ici. contexte d'entreprise confirmé	ÉLEVÉ
VIOLATION	**Luxottica.com** VIOLATION	Les données de violation ont exposé l'email + le mot de passe pour Luxottica.com	Appât ciblé faisant référence à Luxottica.com ; le libellé original a été supprimé de cet échantillon public. violation récente avec exposition de mot de passe	MOYEN
VIOLATION	**houzz.com** VIOLATION	Les données de violation ont exposé l'email + le mot de passe pour houzz.com sur S***e (échantillon)	Alerte de sécurité Houzz : Votre compte a été accédé. Sécurisez votre compte maintenant. violation historique avec exposition de mot de passe	MOYEN
VIOLATION	**AT&T** VIOLATION	Les données de violation ont exposé l'email + le mot de passe pour AT&T sur S***e (échantillon)	Sécurité du compte AT&T : Connexion inhabituelle détectée. Vérifiez votre identité. violation récente avec exposition de mot de passe	MOYEN
MODÈLE	**Modèle de Mot de Passe** MOT DE PASSE	Modèle r2****jf observé à travers plusieurs violations	Notre système de surveillance a détecté un modèle de mot de passe faible dans votre compte. Mettez à jour votre mot de passe ici. modèle répété à travers les violations	MOYEN

ES

Executive067 Sample067

Directeur Financier

employee273@acmesample.com

L'Exécutif067 Sample067, le CFO d'Acme Sample GmbH, présente une exposition à haut risque en raison de multiples violations de données révélant des informations sensibles, y compris des e-mails, des mots de passe et des PII complets. La présence de modèles de mots de passe faibles et de réutilisation sur plusieurs plateformes augmente la probabilité d'attaques réussies sur les identifiants. Cette exposition représente un risque CRITIQUE pour la sécurité personnelle et d'entreprise, nécessitant des efforts de remédiation immédiats.

10
CONSTATATIONS DE VIOLATION

4
PLATEFORMES

2
PREUVES DE RÉCUPÉRATION

3
SOURCES DE VIOLATION

SCORE D'EXPOSITION

ÉLEVÉ

85/100

Potentiel d'attaque personnalisé · plus élevé = plus exposé

Basé sur 10 enregistrements de violation · 4 comptes · 2 preuves de récupération · mot de passe divulgué
Évalué par modèle, limité par des preuves déterministes minimales/maximales

EMPREINTE NUMÉRIQUE

@ **Adresses e-mail**
employee273@acmesample.com,
employee258@examplemail.com

A **Adresse Physique**
100 Market Street, Sample City

T **Numéros de téléphone**
+1 202-555-1019

R **Emails de récupération / alternatifs**
authentificateur : TOTP, email :
wi*****@gmail.com

W **Comptes détectés**
office365, spotify, xvideos

G **Google ID confirmé**
GAIA sample-45583...

ANALYSE DES MOTS DE PASSE

2	NON	FAIBLE	S***E (SAMPLE)
MOTS DE PASSE UNIQUES	RÉUTILISATION	FORCE	PRÉDIRE.

S***e (échantillon) S***E (SAMPLE) S***e (échantillon)

S***e (échantillon) S***E (SAMPLE) S***e (échantillon)

- S***e (échantillon)

S***e (échantillon)

INTELLIGENCE PERSONNELLE

Travaille dans le secteur manufacturier en tant que directeur financier chez Acme Sample GmbH (500-999 employés)

DemandScience CSV · élevé

Le chiffre d'affaires de l'entreprise est de 10-49 millions de dollars

DemandScience CSV · élevé

VECTEURS D'ATTAQUE

Credential Stuffing	ÉLEVÉ
Phishing ciblé via Office 365	ÉLEVÉ
Attaque Vishing	MOYEN
Exploitation de l'accès physique	MOYEN

RISQUE D'IDENTIFIANTS : Stuffing: **VIABLE** · Spray : **VIABLE**

PRÉTEXTES DE PHISHING CIBLÉ — UN SCÉNARIO PAR POINT DE DONNÉES OSINT

Chaque ligne ci-dessous associe UN point de données OSINT spécifique concernant cette personne (un enregistrement de violation, un compte détecté par Holehe, un avis Google, un modèle de mot de passe, un réemploi de mot de passe corporate↔personnel, ou un service d'entreprise détecté) avec le prétexte d'attaque concret qu'un adversaire pourrait élaborer à partir de ces données exactes. La colonne “Source” est la citation explicite qui rend le prétexte crédible — elle répond à la question « pourquoi cette attaque est-elle réalisable ? ». Yield est l'estimation de GPT de la probabilité qu'une véritable attaque réussisse contre cet individu compte tenu de ce signal. Affichage jusqu'à 5 de 5 prétextes dérivés pour ce profil (cap : 20).

TYPE	SERVICE / SUJET	SOURCE — POURQUOI CETTE ATTAQUE EST RÉALISABLE	PRÉTEXTE ET JUSTIFICATION	RENDEMENT
SERVICE	**Office 365** PRODUCTIVITÉ	Holehe a confirmé qu'un compte existe à Office 365 pour l'email employee273@acmesample.com	Votre compte Office 365 nécessite une vérification en raison d'une activité inhabituelle. Cliquez ici pour sécuriser votre compte. confirmation de compte d'entreprise + plateforme de productivité de grande valeur	ÉLEVÉ
VIOLATION	**xiqonline.com** VIOLATION	L'enregistrement de violation de xiqonline.com daté de S***e (exemple) a exposé l'email employee273@acmesample.com avec le mot de passe S***e (exemple)	Nous avons détecté une tentative de connexion sur votre compte xiqonline.com. Si ce n'était pas vous, réinitialisez votre mot de passe ici. violation récente + exposition de mot de passe	ÉLEVÉ
VIOLATION	**DemandScience CSV** VIOLATION	La violation de DemandScience CSV a exposé des PII complètes (nom, adresse, téléphone, rôle) pour employee273@acmesample.com	Appât ciblé faisant référence à DemandScience CSV ; le libellé original a été supprimé de cet exemple public. exposition complète de PII + contexte d'entreprise	ÉLEVÉ
COMPTE	**Spotify** STREAMING	Holehe a confirmé qu'un compte existe à Spotify pour l'email employee273@acmesample.com	Votre compte Spotify a été accédé depuis un nouvel appareil. Vérifiez votre identité ici. confirmation de compte personnel + service de streaming	MOYEN
MODÈLE	**Modèle de Mot de Passe** MOT DE PASSE	Motif 'mot de base + suffixe numérique S***e (exemple)' observé dans la violation de xiqonline.com	Notre système de surveillance des identifiants a identifié une correspondance de motif faible par rapport à votre mot de passe historique (S***e (exemple)). Lisez la politique de mot de passe mise à jour ici. motif de mot de passe faible + potentiel de réutilisation	MOYEN

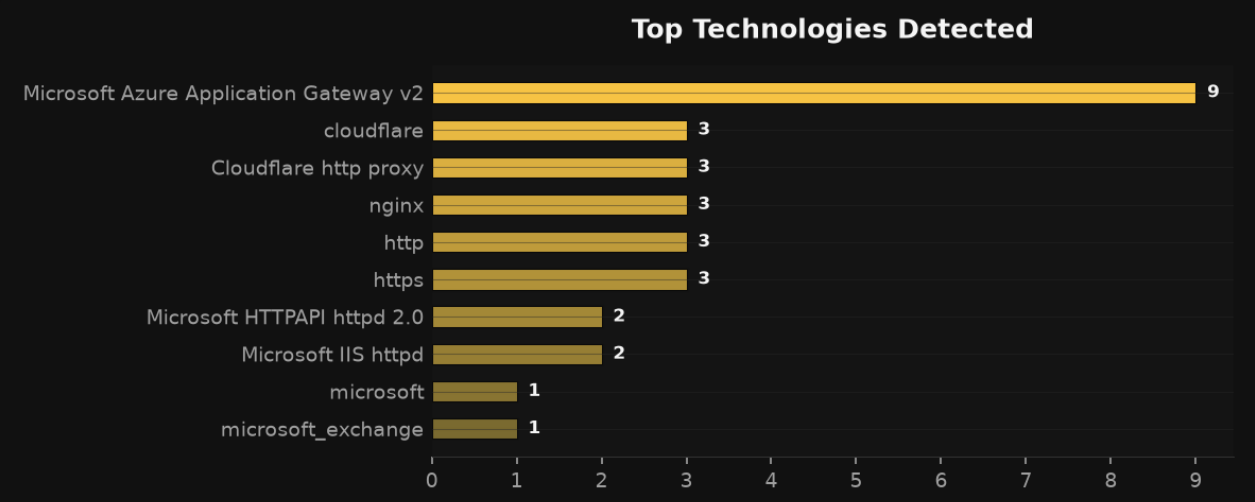
APPLICATIONS

Technologie

Les technologies sont détectées grâce à l'intelligence passive : bannières de service Shodan, empreintes de domaine Netlas, analyse d'hôte ZoomEye et identifiants CPE (Common Platform Enumeration) extraits des données de bannières. Le scan de ports actif (Nmap -sV) a fourni une confirmation supplémentaire des versions de service. L'identification des technologies permet une recherche ciblée de vulnérabilités et aide à prioriser les efforts de patching.

Technologies détectées sur **21** des **54** hôtes (18 technologies uniques). Sources de données : Shodan (bannières de service, identifiants CPE), Nmap (détection de version de service active).

Technologies principales (rampe à accent unique)



Évaluation des risques technologiques

La pile technologique de l'organisation présente une santé mitigée, avec des risques potentiels liés à l'utilisation de Microsoft HTTPAPI httpd 2.0, qui est obsolète et pourrait exposer des vulnérabilités. De plus, la dépendance à Microsoft Exchange et IIS soulève des inquiétudes, car ces produits peuvent avoir des vulnérabilités connues s'ils ne sont pas correctement corrigés. Il est recommandé que l'organisation priorise la mise à jour ou le remplacement des composants logiciels obsolètes, en particulier Microsoft HTTPAPI, afin d'améliorer la posture de sécurité globale.

TECHNOLOGIE	DESCRIPTION	HÔTES
Microsoft Azure Application Gateway v2		9
cloudflare	CDN / protection DDoS	3
Proxy http Cloudflare	CDN / proxy inverse HTTP	3
nginx	Serveur web / proxy inverse	3
http	Protocole de transfert hypertexte	3
https	HTTP chiffré TLS (port 443)	3
Microsoft HTTPAPI httpd 2.0		2
Microsoft IIS httpd	Serveur web Microsoft (IIS)	2
microsoft	Serveur web Microsoft (IIS)	1
microsoft_exchange	Serveur de messagerie et de collaboration	1
smtp		1
soumission		1
microsoft_asp_net		1
kestrel		1
sfdcedge		1

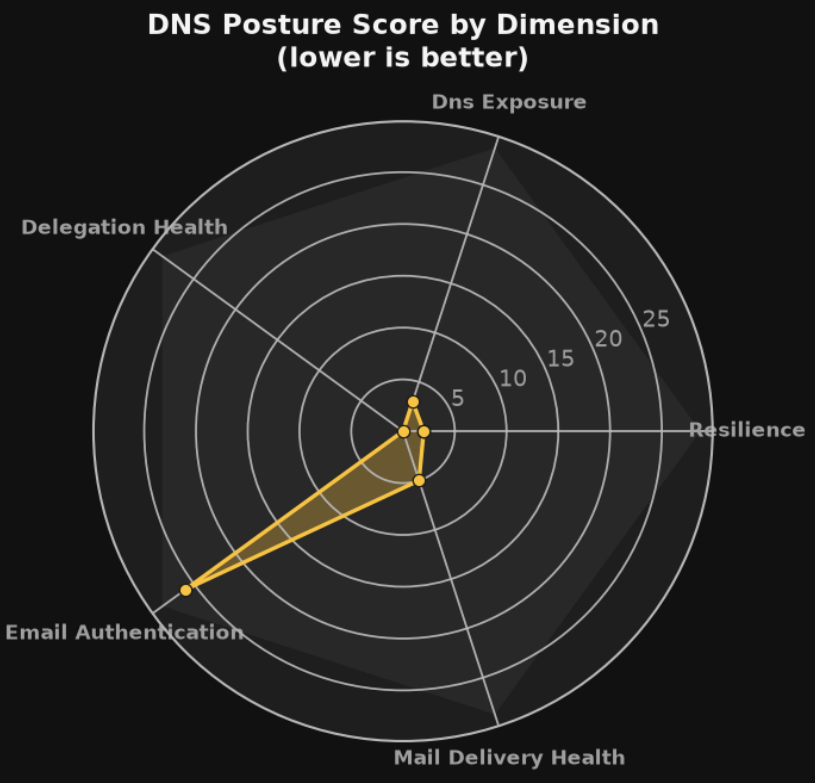
Posture de Sécurité DNS & Email

76
BON

L'évaluation de la posture DNS a effectué **39 vérifications automatisées** à travers cinq dimensions de sécurité : santé de la délégation (présence NS, validité SOA, délégation lâche), exposition DNS (transfert de zone, récursion ouverte, divulgation de version), authentification par e-mail (SPF, DMARC, DKIM), santé de la livraison des e-mails (résolution MX, alignement PTR), et résilience (DNSSEC, CAA, diversité NS). Deux chiffres complémentaires sont affichés ci-dessous : le **score d'exposition brut** (0 = aucun, 100 = critique — plus bas est mieux) et le **score de santé** (100 − exposition, plus haut est mieux) qui alimente le score global de posture de sécurité dans le résumé exécutif.

36/100	64/100	ÉLEVÉ	39
SCORE D'EXPOSITION (PLUS BAS = MIEUX)	SCORE DE SANTÉ (PLUS ÉLEVÉ = MIEUX)	GRAVITÉ GLOBALE	VÉRIFICATIONS EFFECTUÉES

Dimensions (plus bas est mieux)



La posture DNS présente des lacunes : Politique DMARC : Surveillance uniquement ; Aucun enregistrement TXT MTA-STS. Aucune exposition critique trouvée.

Constats de risque (2)

GRAVITÉ	VÉRIFIER L'ID	RÉSULTAT
MOYEN	MAIL_DMARC_POLICY	Politique DMARC : Surveillance uniquement
MOYEN	MAIL_MTA_STS_TXT	Aucun enregistrement TXT MTA-STS

Les résultats de vérification complets (39 au total) sont disponibles dans `jeu de donnees de preuves prive` omis de cet échantillon public.

Informations DNS inverses (PTR)

Pour chaque adresse IP découverte lors du scan, nous effectuons une recherche PTR (DNS inversé). Les enregistrements PTR associent les IPs aux noms d'hôtes et révèlent les conventions de nommage, les détails d'infrastructure et les configurations incorrectes potentielles que les attaquants utilisent lors de la reconnaissance.

21	2	19	3
IPS ANALYSÉS	ENREGISTREMENTS PTR VALIDES	PTR MANQUANT	CONSTATATIONS DE RISQUE

Serveurs SMTP sans PTR (1)

Les serveurs de messagerie sans enregistrements PTR rencontrent des problèmes de délivrabilité — de nombreux serveurs récepteurs rejettent ou filtrent les mails provenant d'IPs dépourvues de DNS inverse valide.

IP	NOM D'HÔTE	PORTS SMTP	RISQUE
192.0.2.75	asset-166.acmesample.com	25, 587	ÉLEVÉ

Mismatches PTR — Échecs de DNS inversé confirmés par l'avant (1)

Un désaccord PTR se produit lorsque le nom DNS inverse ne résout pas l'adresse IP d'origine. Cela est pénalisé par les filtres anti-spam et indique des erreurs de configuration DNS.

IP	ENREGISTREMENT PTR	RÉSOUT VERS	RISQUE
192.0.2.182	bl194.acmesample.com.in-addr.arpa	NXDOMAIN	MOYEN

Infrastructure tierce / Infrastructure fantôme (1)

Les enregistrements PTR révélant des noms d'hôtes de fournisseurs de cloud (par exemple, ec2-*.amazonaws.com) peuvent indiquer des actifs cloud non gérés ou de l'IT fantôme — surtout lorsque le nom d'hôte de destination appartient à l'organisation.

IP	NOM D'HÔTE	ENREGISTREMENT PTR	FOURNISSEUR DE CLOUD
192.0.2.33	asset-152.acmesample....	ec2-192-0-2-33.ca-central-1.c...	AWS

Sécurité de l'authentification par e-mail

Cette section évalue si le domaine peut être abusé pour le spoofing d'email ou des attaques de phishing basées sur les configurations SPF, DMARC et DKIM. Les détails complets des constatations, y compris les domaines affectés, les preuves et les étapes de remédiation sont omis de cet échantillon public.

89/100	MOYEN	MOYEN	0
SCORE D'AUTHENTIFICATION PAR EMAIL	RISQUE DE SPOOFING	RISQUE DE PHISHING	CONSTATATIONS CRITIQUES / ÉLEVÉES

Résumé de la configuration

PROTOCOLE	STATUT	DÉTAILS
SPF	PRÉSENT	Politique : `-all` · 3 recherches DNS
DMARC	PRÉSENT	Politique : p=none
DKIM	1 SÉLECTEUR(S)	Sélecteurs : selector1
MX	PRÉSENT	2 enregistrement(s)

Constats Clés

GRAVITÉ	CONSTAT	PREUVE
MOYEN	**Politique DMARC : Aucune (Surveillance)** p=none — pas d'application, surveillance uniquement.	Politique DMARC : p=none (surveillance uniq…

Constatations nécessitant une attention

RÉSULTAT	VÉRIFIER	DÉTAIL	RECOMMANDATION
AVERTISSEMENT	**SPF Inclusions de tiers inconnus**	SPF inclut des domaines non reconnus comme des plateformes email standard.	Enquêter sur les inclusions inconnues : domaines et supprimer si inutilisés.
AVERTISSEMENT	**Politique DMARC : Aucune (Surveillance)**	p=none — aucune application, surveillance uniquement.	Progression vers p=quarantine puis p=reject après examen des rapports.
AVERTISSEMENT	**DMARC Alignment Relaxed**	adkim=r ou aspf=r — un alignement détendu peut permettre le spoofing de sous-domaines.	Définir adkim=s et aspf=s pour un alignement strict.

RÉSULTAT	VÉRIFIER	DÉTAIL	RECOMMANDATION
N/A	**Aucun enregistrement BIMI**	BIMI n'est pas configuré.	Publiez un enregistrement BIMI TXT à default._bimi.domain.
N/A	**Pas de MTA-STS**	MTA-STS n'est pas configuré — le transport des e-mails repose sur TLS opportuniste.	Publier le fichier TXT _mta-sts et héberger le fichier de politique.
N/A	**Pas de TLS-RPT**	Reporting SMTP TLS non configuré.	Publier l'enregistrement TXT _smtp._tls avec rua= URI de rapport.

Évaluation de vulnérabilité

53
MAUVAIS

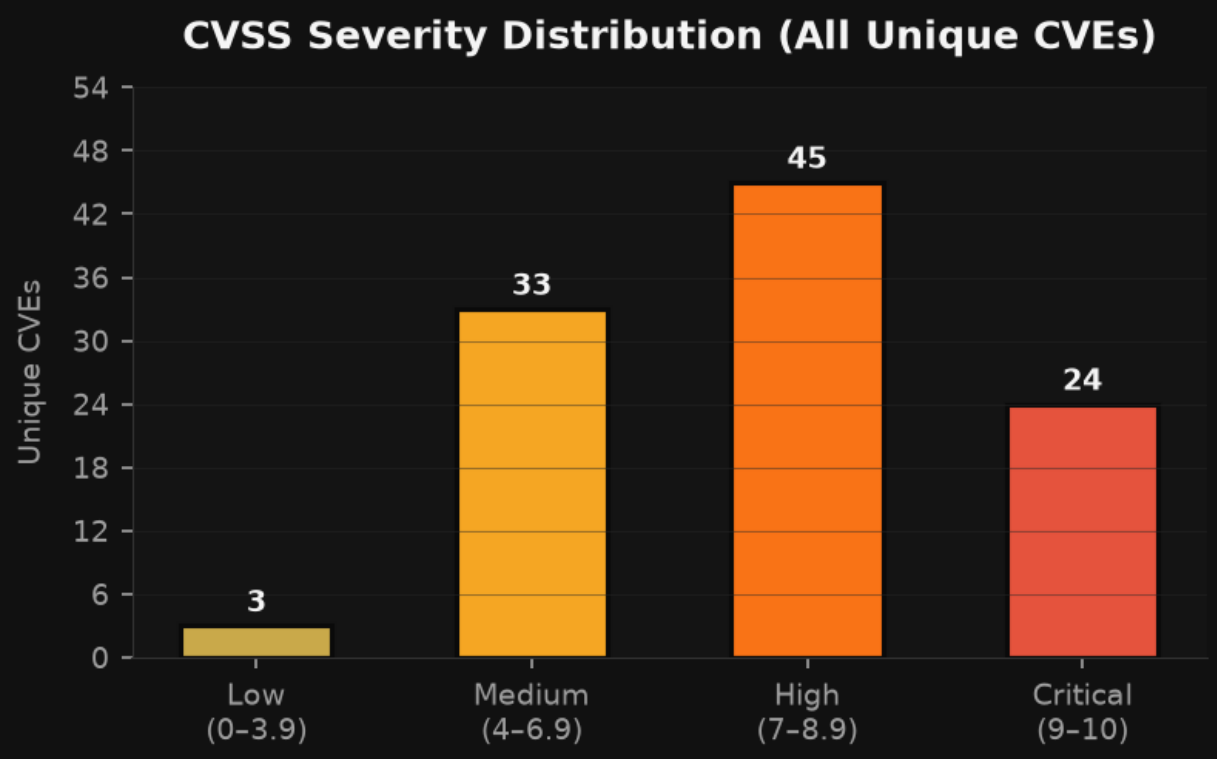
Les vulnérabilités sont agrégées à partir de cinq sources par ordre de priorité : (1) script Nmap vulners — confiance maximale, version correspondante par détection de service actif, (2) Shodan, (3) Netlas, (4) intelligence passive ZoomEye, (5) Shodan CVEDB — recherche gratuite par nom/version de produit. Chaque CVE est croisée avec les bannières de service Nmap ; le drapeau **version-corroborée** indique que le jeton de produit et une chaîne de version sont tous deux apparus dans la bannière de service détectée (une correspondance de chaîne passive, pas une vérification d'exploitation active).

Avertissement : Tous les constats sont basés sur **la correspondance des bannières de service et des versions** — aucune exploitation active ou injection de charge utile n'a été réalisée. Une correspondance CVE signifie que la version détectée est connue pour être affectée, pas qu'elle est exploitable dans cette configuration. Des correctifs, des WAF et des contrôles compensatoires peuvent atténuer le risque.

105	10	0	2
CVES UNIQUES	HÔTES AFFECTÉS	NMAP VÉRIFIÉ	CONSTATATIONS DE VÉRIFICATION
			+397 INFORMATIF

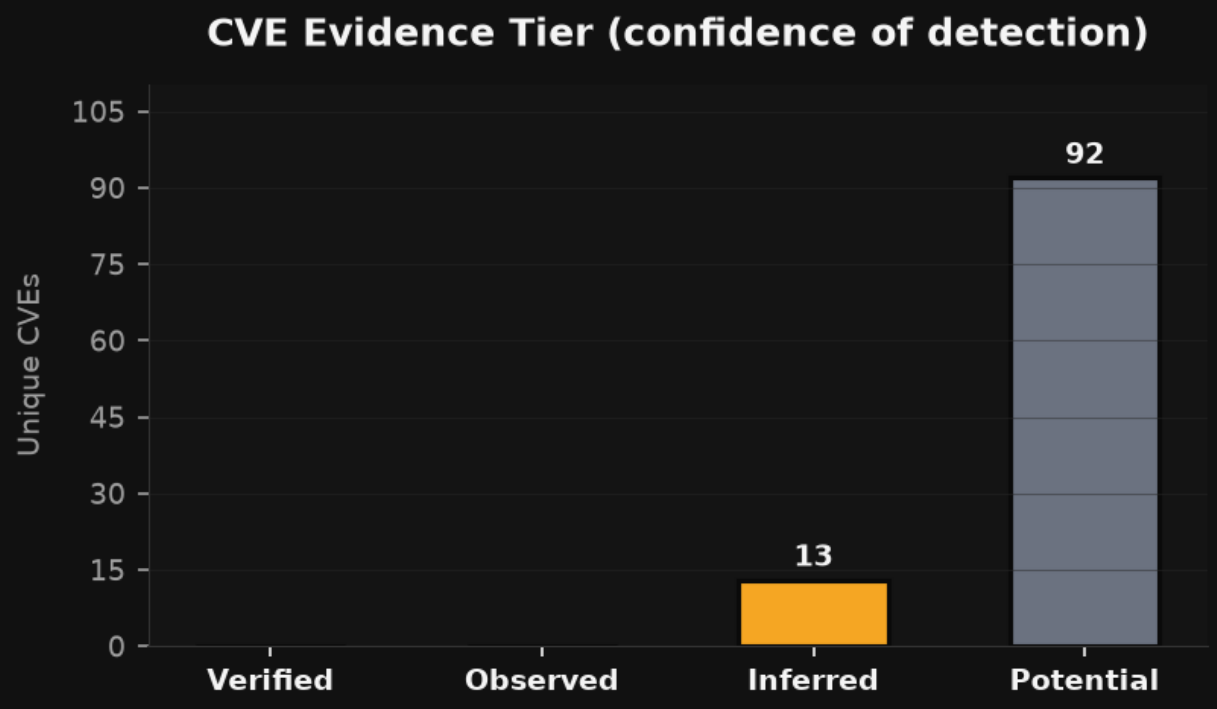
Gravité CVSS (CVE uniques)

Distribution de tous les 105 CVEs uniques par évaluation de gravité CVSS v3.

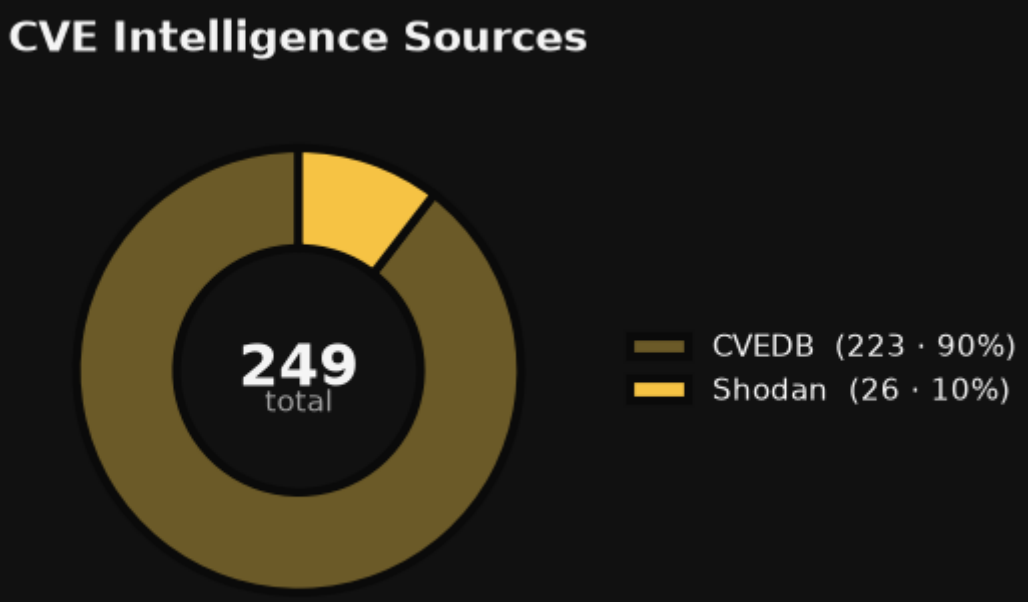


Niveau de preuve (CVE uniques)

Les mêmes CVE classés par la force avec laquelle chacun a été corroboré. **Vérifié** = correspondance exacte hôte/port/CVE Nuclei ou version confirmée par l'opérateur ; **Observé** = bannière de service Nmap en direct ; **Inféré** = corroboration d'intelligence passive ou de chaîne de version ; **Potentiel** = un seul signal de produit, applicabilité non confirmée.



Sources d'intelligence CVE



Niveaux de confiance

NIVEAU	DESCRIPTION	CVE
Produit Correspondant Non Vérifié	Produit correspondant via CPE/bannière mais version non confirmée	**92**
Intelligence passive	Signalé par des plateformes d'intelligence passive (Shodan/ Netlas/ZoomEye)	**13**

Niveaux de preuve

À quel point chaque CVE a été corroboré, indépendamment de sa gravité. Selon le modèle DS-90 v2, ce niveau génère un score de vulnérabilité pondéré par la confiance. Les niveaux de preuve sont affichés à côté de la gravité sur les surfaces CVE et CISA KEV où la ligne sous-jacente soutient la taxonomie.

NIVEAU	SIGNIFICATION	CVE
VÉRIFIÉ	Correspondance exacte hôte/port/CVE, ou confirmée contre une version fournie par un opérateur — confiance maximale	0
OBSERVÉ	Corroboré par une bannière de service Nmap active sur l'hôte/le port affecté	0
DÉDUIT	Rapport d'intelligence passive ou corroboration de version; non sondé activement	13
POTENTIEL	Un seul signal produit uniquement ; la version spécifique et l'applicabilité ne sont pas confirmées	92

Top CVEs par gravité

CVE	CVSS	PREUVE	SOURCES	HÔTES	CONFIANCE
CVE-2004-0847	9.8	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2006-1364	7.5	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2003-0768	6.8	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2005-1664	6.4	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2005-1665	5.0	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2005-2224	5.0	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2005-0452	4.3	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2010-2084	4.3	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2010-2088	4.3	POTENTIEL	CVEDB	4	produit correspondant non vérifié
CVE-2015-3105	10.0	POTENTIEL	CVEDB	3	produit correspondant non vérifié
CVE-2014-0515	10.0	POTENTIEL	CVEDB	3	produit correspondant non vérifié
CVE-2010-0425	10.0	POTENTIEL	CVEDB	3	produit correspondant non vérifié
CVE-2015-0359	10.0	POTENTIEL	CVEDB	3	produit correspondant non vérifié

CVE	CVSS	PREUVE	SOURCES	HÔTES	CONFIANCE
CVE-2009-3555	9.8	POTENTIEL	CVEDB	3	produit correspondant non vérifié
CVE-2024-4577	9.8	POTENTIEL	CVEDB	3	produit correspondant non vérifié

Liste complète des vulnérabilités (105 CVEs) et adresses IP associées dans l'Annexe B et dans `jeu de donnees de preuves prive` / `jeu de donnees de preuves prive` omis de cet échantillon public.

Priorisation des exploits et recommandations de remédiation

Le tableau suivant enrichit les composants logiciels détectés avec des informations sur la maturité des exploits pour aider à prioriser la remédiation au-delà de la gravité CVSS seule. **Maturité de l'Exploit** indique à quel point le code d'exploit fonctionnel est facilement disponible — "Arme" signifie exploitation active dans la nature, tandis que "PoC" indique qu'un code de preuve de concept existe. Les composants sont triés par priorité de remédiation.

LOGICIEL	VERSION DÉTECTÉE	VERSION ACTUELLE.	CVE PRINCIPALE	CVSS	MATURITÉ DE L'EXPLOITATION	PRIORITÉ
windows	unknown	inconnu	CVE-2010-0425	10.0	ARME	CRITIQUE
Les CVE CRITIQUES avec des exploits connus et plusieurs hôtes affectés nécessitent une remédiation immédiate. `cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*`						
internet_information_services	10.0	10.0	CVE-2000-0246	10.0	ARME	FAIBLE
La version détectée correspond à la dernière version disponible ; la CVE listée nécessite généralement une configuration spécifique ou une version vulnérable — vérifiez le niveau de correctif et l'exposition plutôt que de procéder à une mise à niveau aveugle. Les vulnérabilités CRITIQUES avec des exploits connus et un nombre significatif d'hôtes nécessitent une attention urgente. `cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*`						
nginx	unknown	inconnu	CVE-2009-2629	9.8	ARME	CRITIQUE
Des scores CVSS ÉLEVÉS et des exploits connus à travers plusieurs vulnérabilités indiquent un risque CRITIQUE. `cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*`						
asp.net	unknown	inconnu	CVE-2005-1665	9.8	FONCTIONNEL	ÉLEVÉ
Un CVSS ÉLEVÉ avec des exploits publics fiables suggère un risque significatif, malgré l'absence d'exploitation connue. `cpe:2.3:a:microsoft:asp.net:*:*:*:*:*:*:*:*`						
exchange_server	unknown	inconnu	CVE-2021-26855	9.1	ARME	CRITIQUE
Les vulnérabilités CRITIQUES avec des exploits connus et un seul hôte affecté nécessitent une action immédiate. `cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*`						
cloudflare	unknown	inconnu	CVE-2024-0212	8.1	NON PROUVÉ	MOYEN
Un CVSS MOYEN sans exploits connus et un faible nombre d'hôtes suggèrent une urgence de remédiation plus faible.						

La maturité de l'exploitation est évaluée à l'aide de la gravité CVSS, de la prévalence des logiciels et des informations sur les exploits connus. "Arme" = exploitation active dans la nature ; "Fonctionnel" = exploits publics fiables ; "PoC" = preuve de concept existante ; "Non prouvé" = aucun code d'exploitation connu.

Vérification de la sécurité active

Scanné **22/22** IPs uniques (46 points de terminaison HTTP actifs) en 36,2 minutes en utilisant plus de 4 000 modèles sûrs sélectionnés (GET/HEAD uniquement — pas d'exploitation).

Pourquoi 22 IP au lieu de 54 noms d'hôtes ? Le moteur de vérification fonctionne sur des adresses IP uniques (pas des noms d'hôtes). 54 noms d'hôtes ont été découverts, dont **25** ont été résolus avec succès en **21** IP uniques. La plupart des IP dans ce scan sont dédiées à un seul nom d'hôte — **17** des **21** IP (81,0 %) servent exactement un FQDN. Un petit nombre héberge plusieurs noms (IP partagée principale : `192.0.2.178` avec 2 FQDNs). Les 22 IP restantes ont été intégrées dans le pipeline et ont été filtrées davantage par : (1) une liste blanche de classification de port (seuls les ports web, SSL, DNS et de service réseau connus sont qualifiés), (2) un contrôle de vivacité httpx (seuls les points de terminaison HTTP/HTTPS répondants sont testés avec des modèles HTTP), et (3) le cache par IP. Les hôtes sans ports qualifiés ou sans point de terminaison HTTP actif sont toujours comptés dans les totaux d'envoi mais ne produisent aucune constatation de noyau.

> **2** constatations de sécurité exploitables (critique/élevé/moyen/faible) et **397** détections informatives (empreinte technologique, métadonnées d'environnement — pas des faiblesses en soi).

CATÉGORIE	GRAVITÉ	CONSTATATIONS
Actionnable	FAIBLE	**2**
Informationnel	INFO	**397**

Constats actionnables par modèle

Les modèles d'information sont exclus de ce tableau (ensemble complet dans `jeu de donnees de preuves prive`).

CONSTAT	GRAVITÉ	HÔTES	URL D'EXEMPLE
Détection de suites de chiffrement faibles	FAIBLE	**2**	asset-188.acmesample.com:443

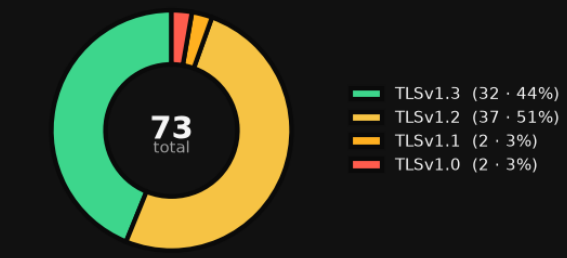
Affichage des 1 modèles actionnables les plus fréquents. Liste complète (incl. informatif) en Annexe B et `jeu de donnees de preuves prive`.

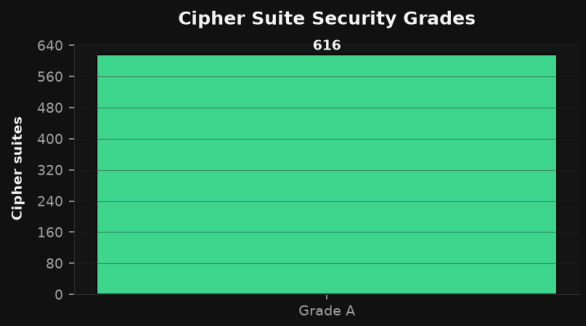
Posture de sécurité TLS/SSL

91
EXCELLENT

Synthétisé à partir de nmap ssl-enum-ciphers, des données de certificats Shodan et des modèles SSL de nuclei. Identifie les certificats expirés/autosignés, les protocoles obsolètes (TLS 1.0/1.1), les suites de chiffrement faibles et les hôtes HTTP uniquement manquant HTTPS.

20 HÔTES AVEC TLS	**0** CERTIFICATS EXPIRÉS	**0** AUTO-SIGNÉ
2 PROTOCOLES FAIBLES	**0** CHIFFRES FAIBLES	**90/100** SCORE DE RISQUE · PLUS ÉLEVÉ = PIRE (CRITIQUE)





Résumé

20 hôte(s) avec TLS détecté(s) sur la surface d'attaque. 2 hôte(s) servent des protocoles TLS obsolètes (1.0/1.1). 17 hôte(s) sont sur des IP partagées où le certificat par défaut appartient à un domaine différent (mismatch CN). 1 hôte(s) sert HTTP sans TLS détecté.

Constatations TLS

HÔTE(S)	IP	HÔTES	PORTS AFFECTÉS	GRAVITÉ	PROBLÈME
asset-143.acmesample.com (+1 de p...	192.0.2.27	**2**	443	ÉLEVÉ	**TLSv1.0 activé**
asset-143.acmesample.com (+1 de p...	192.0.2.27	**2**	443	MOYEN	**TLSv1.1 activé**
asset-059.acmesample.com	192.0.2.10	**1**	443	MOYEN	**Avertissement de chiffrement Nmap**
asset-146.acmesample.com	192.0.2.49	**1**	443	MOYEN	**Avertissement de chiffrement Nmap**
asset-049.acmesample.com	192.0.2.63	**1**	80	INFO	**Hôte HTTP uniquement (aucun TLS détecté)**

Inventaire des certificats

Affichage des 15 certificats les plus urgents par date d'expiration. Inventaire complet avec tous les 26 hôtes disponible dans `jeu de donnees de preuves prive`.

HÔTE	CN	ÉMETTEUR	EXPIRE	JOURS	STATUT
asset-168.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE

HÔTE	CN	ÉMETTEUR	EXPIRE	JOURS	STATUT
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALIDE
asset-142.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE
www.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE
asset-141.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE
asset-146.acmesample.com	asset-146.acmesample.com	Let's Encrypt	2026-10-30	**57**	VALIDE
asset-169.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE
asset-059.acmesample.com	asset-059.acmesample.com	Let's Encrypt	2026-10-30	**57**	VALIDE
asset-170.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALIDE

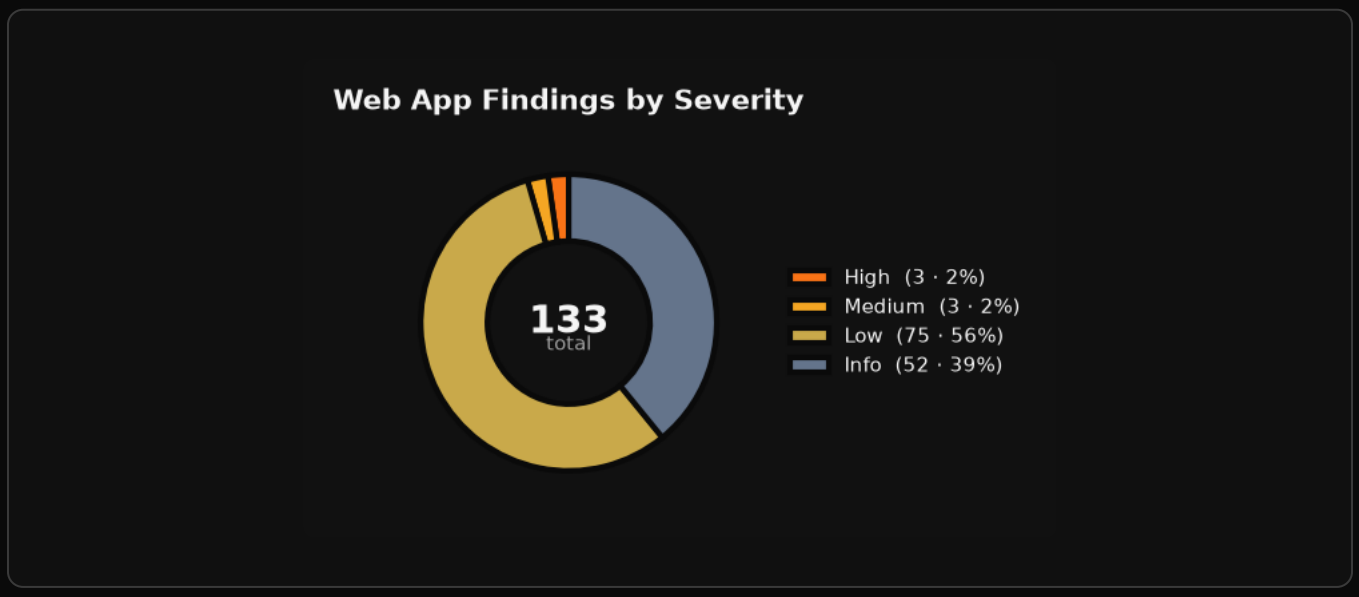
… et 11 autres certificats (voir `jeu de donnees de preuves prive` omis de cet échantillon public)

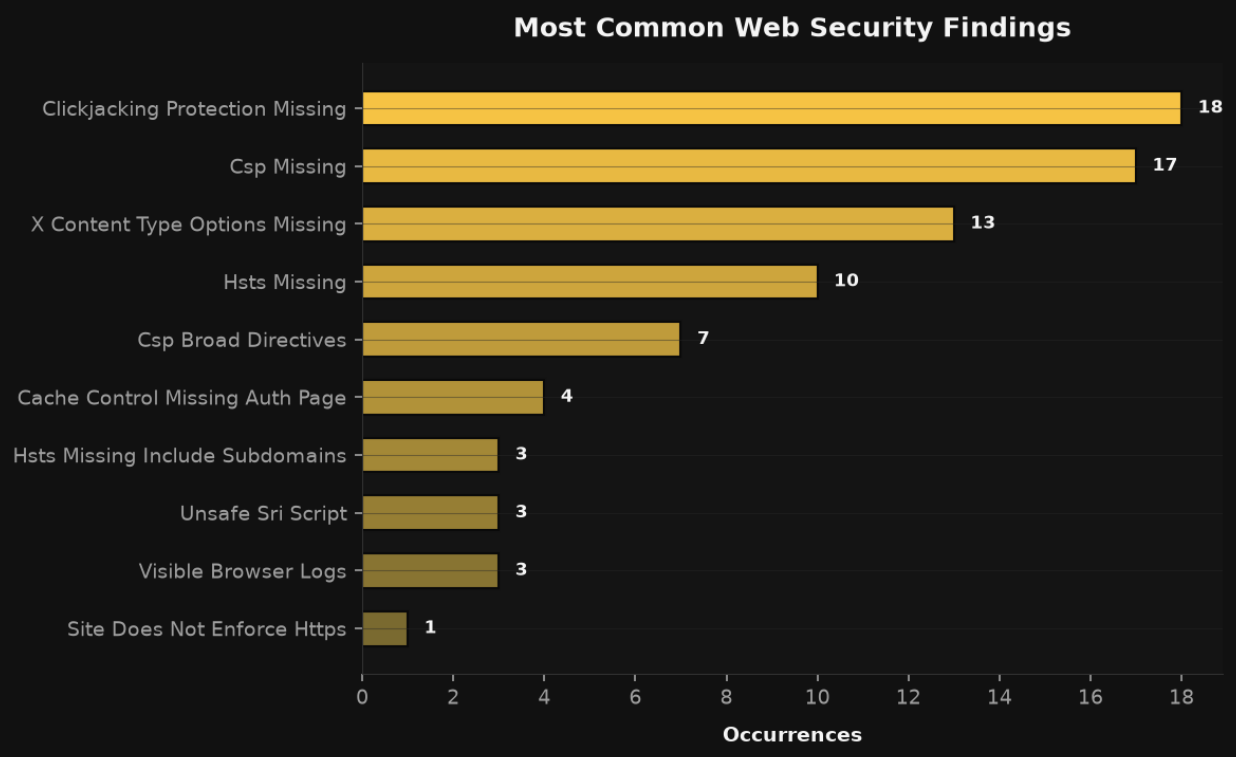
Sécurité des applications web

74
PASSABLE

Évalue les points de terminaison web accessibles depuis l'extérieur pour des faiblesses de sécurité HTTP non intrusives en utilisant des requêtes GET sûres, une analyse des redirections, une inspection des en-têtes de réponse, une analyse des Set-Cookie et un parsing HTML passif. N'essaie pas d'exploiter, de se connecter, de fuzzing ou d'injection de payload.

74/100 SCORE DE SÉCURITÉ (FAIBLE)	**48** URLS ANALYSÉES	**33** URLS AVEC CONSTATATIONS
3 GRAVITÉ ÉLEVÉE	**3** GRAVITÉ MOYENNE	**75** GRAVITÉ FAIBLE





Résumé

La posture de sécurité des applications web pour acmesample.com a été évaluée sur 48 URL(s), donnant un score global de 74/100 (acceptable). 3 constat(s) de haute gravité ont été identifiés, y compris des problèmes de sécurité des cookies de session et/ou des chaînes de redirection non sécurisées. 3 problème(s) de gravité moyenne nécessitent une attention. 75 faiblesses de configuration de faible gravité ont été notées (en-têtes manquants, paramètres CSP/HSTS faibles).

Scores de sécurité des hôtes

HÔTE	SCORE	ÉLEVÉ	MOYEN	FAIBLE	ÉVALUATION
asset-064.acmesample.com	**61/100**	0	3	1	ÉQUITABLE
www.acmesample.com	**70/100**	1	0	3	ÉQUITABLE
asset-188.acmesample.com	**70/100**	1	0	3	ÉQUITABLE
asset-143.acmesample.com	**70/100**	1	0	3	ÉQUITABLE
192.0.2.68	**78/100**	0	0	8	BON
asset-065.acmesample.com	**82/100**	0	0	7	BON

HÔTE	SCORE	ÉLEVÉ	MOYEN	FAIBLE	ÉVALUATION
asset-134.acmesample.com	**85/100**	0	0	5	BON
asset-148.acmesample.com	**88/100**	0	0	4	BON
asset-142.acmesample.com	**88/100**	0	0	4	BON
asset-168.acmesample.com	**88/100**	0	0	4	BON

Constatations de sécurité Web à haut risque

HÔTE	VÉRIFIER	GRAVITÉ	PREUVE
www.acmesample.com	Script Sri non sécurisé	ÉLEVÉ	Le script externe de hs-scripts.com manque de l'attribut d'intégrité SRI
asset-188.acmesample.com	Script Sri non sécurisé	ÉLEVÉ	Le script externe de hs-scripts.com manque de l'attribut d'intégrité SRI
asset-064.acmesample.com	Modèle de redirection Https non sécurisé	MOYEN	Redirection HTTP vers le domaine externe microsoft.com
asset-064.acmesample.com	Directives Csp Broad	MOYEN	La CSP a 3 directive(s) générale(s)
asset-064.acmesample.com	Directives Csp non sécurisées	MOYEN	CSP utilise 1 directive(s) non sécurisée(s)
asset-143.acmesample.com	Script Sri non sécurisé	ÉLEVÉ	Le script externe de hs-scripts.com manque de l'attribut d'intégrité SRI

Constatations les plus courantes

VÉRIFIER	CONSTATATIONS
Protection contre le clickjacking manquante	18
Csp Manquant	17
Options de type de contenu X manquantes	13
Hsts manquant	10
Directives Csp Broad	7
Cache Control Missing Auth Page	4
Hsts manquant inclure les sous-domaines	3
Script Sri non sécurisé	3
Journaux de navigateur visibles	3
Le site n'impose pas Https	1

Méthodologie. Ce chapitre évalue les points de terminaison web accessibles de l'extérieur pour des faiblesses de sécurité HTTP non intrusives en utilisant des requêtes GET/HEAD sûres, une analyse des redirections, une inspection des en-têtes de réponse, une analyse de Set-Cookie et un parsing HTML passif. Il n'essaie pas d'exploiter, de se connecter, de faire du fuzzing ou d'injecter des charges utiles. Les vérifications couvrent la sécurité des cookies de session, l'application de HTTPS, la politique de sécurité de contenu, HSTS, la protection contre le clickjacking, l'intégrité des sous-ressources, et plus encore.

INFRASTRUCTURE

Analyse de port et de service

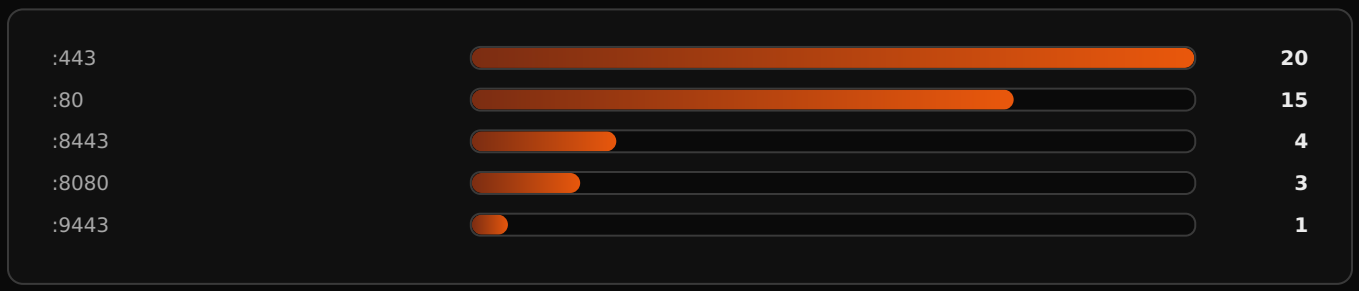
64
PASSABLE

Des ports ouverts sont détectés grâce à une combinaison de **renseignement passif** (Shodan, Netlas et ZoomEye scannent continuellement Internet et rapportent les ports ouverts sans toucher à la cible) et de **scanning actif optionnel** (Nmap). Les sources passives offrent une large couverture mais peuvent rapporter des données légèrement obsolètes ; le scanning actif confirme l'état actuel.

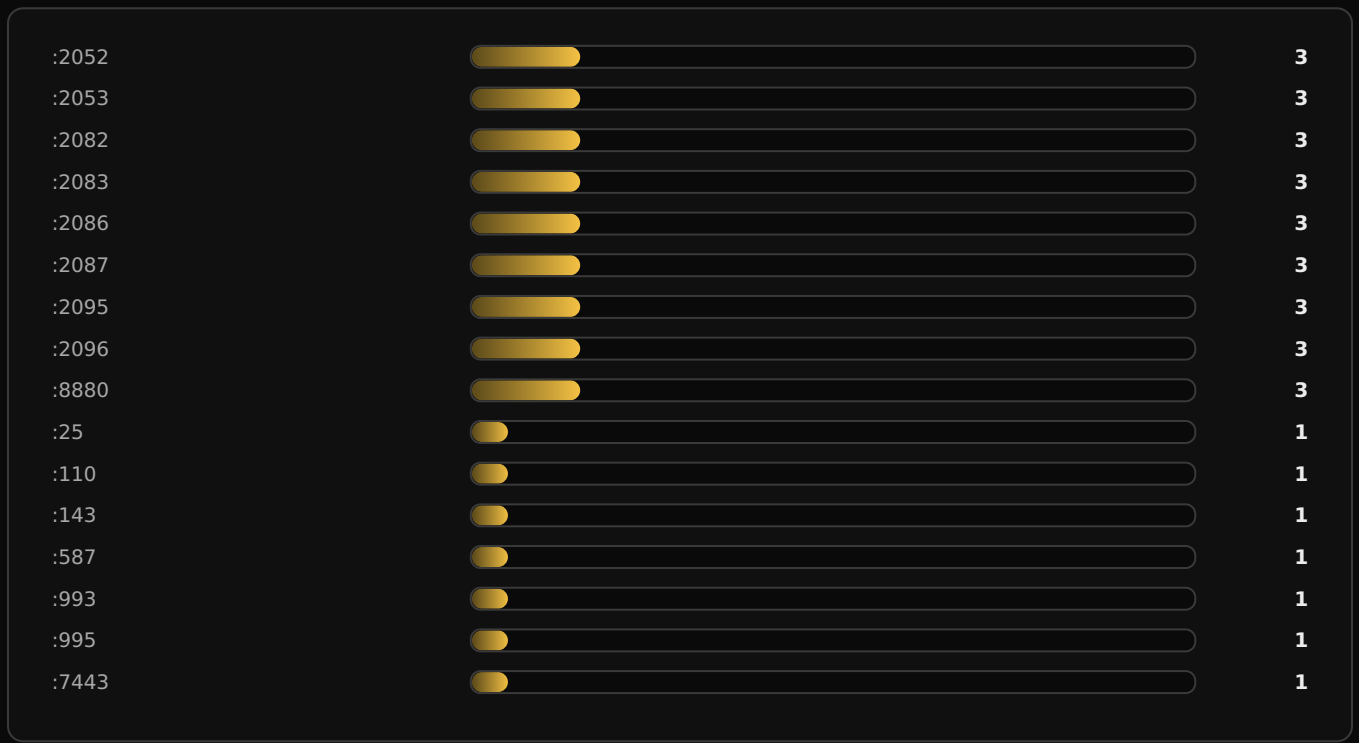
Note de couverture : Le scan de ports actifs a été activé. Nmap a vérifié tous les ports découverts passivement avec détection de version de service (-sV) et a scanné les 100 premiers ports TCP sur les hôtes sans données de port antérieures.

23 ports uniques à travers **22** hôtes.

Web exposé (typique)

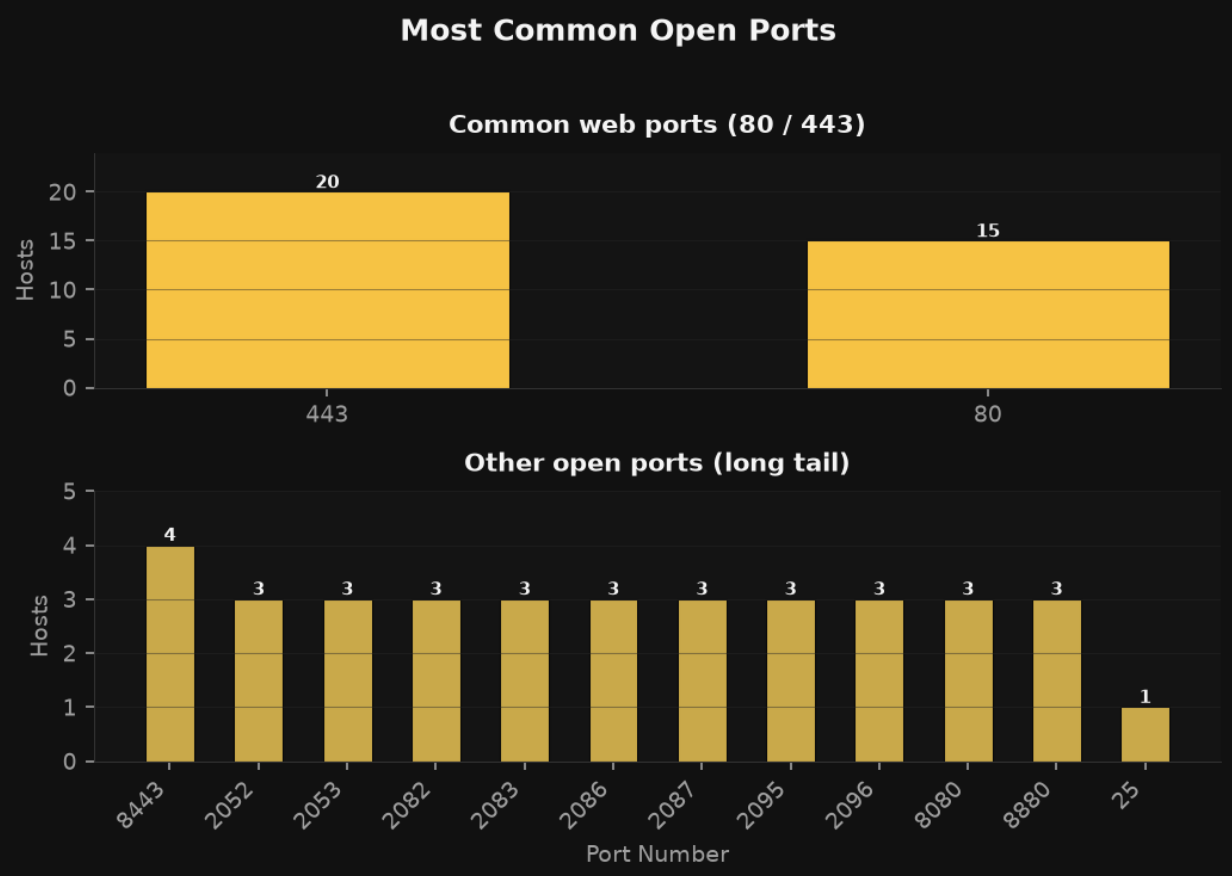


Autres services (longue traîne)



Les barres partagent une échelle (nombre maximum à travers les deux groupes).

Tous les ports — top des comptes (graphique)



SERVICE	HÔTES
http/Cloudflare http proxy	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
soumission	1
http/sfdcedge	1

Services backend exposés à Internet

Les ports suivants hébergent des **services backend** (bases de données, courtiers de messages, interfaces de gestion) qui ne devraient **pas être accessibles depuis Internet public**. Ces services sont conçus pour un accès réseau interne uniquement — les exposer augmente le risque d'exfiltration de données, d'attaques par force brute et de mouvements latéraux. Chacun devrait être placé derrière un pare-feu ou un VPN. Pour une répartition détaillée par hôte, voir `jeu de donnees de preuves prive` omis de cet échantillon public.

PORT	SERVICE	RISQUE	HÔTES	RAISON
:8443	Plesk HTTPS	FAIBLE	**4**	Panneau d'administration d'hébergement (HTTPS)
:2082	cPanel HTTP	MOYEN	**3**	Panneau d'administration d'hébergement — brute-force si aucune restriction IP
:2083	cPanel HTTPS	MOYEN	**3**	Panneau d'administration d'hébergement — brute-force si aucune restriction IP
:2086	WHM HTTP	ÉLEVÉ	**3**	Panneau de gestion de serveur — contrôle total du serveur en cas de compromission
:2087	WHM HTTPS	ÉLEVÉ	**3**	Panneau de gestion de serveur — contrôle total du serveur en cas de compromission
:2095		MOYEN	**3**	Webmail — vecteur de force brute d'identifiants

PORT	SERVICE	RISQUE	HÔTES	RAISON
	Webmail cPanel			
:8880	Plesk HTTP	MOYEN	**3**	Panneau d'administration d'hébergement

Hôtes avec des ports inhabituels

Les ports inhabituels sont tous les ports TCP/UDP ouverts qui se situent **en dehors de l'ensemble standard** des services Internet courants (HTTP/80, HTTPS/443, SSH/22, DNS/53, SMTP/25, FTP/21, etc.). La présence de ports inhabituels peut indiquer des serveurs de développement, des interfaces de gestion, des applications héritées ou des services mal configurés — tous ces éléments élargissent la surface d'attaque et justifient une enquête.

HÔTE	IP	PORTS INHABITUELS	RISQUE
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**

Sous-domaines sensibles

Les noms d'hôte sont analysés pour des motifs qui suggèrent des systèmes sensibles ou de grande valeur. Le scanner vérifie **9** motifs de noms d'hôte à travers 9 catégories : panneaux d'administration (admin, backend, cpanel), environnements de développement/staging (dev, staging, qa, sandbox), infrastructure interne (intranet, vpn, passerelle), bases de données (mysql, redis, elastic), systèmes de surveillance (grafana, prometheus, kibana), infrastructure CI/CD (jenkins, gitlab, docker-registry), services d'authentification (auth, sso, oauth), systèmes de stockage/sauvegarde, et points de terminaison hérités/migration. Ces systèmes sont souvent les premières cibles lors des tests de pénétration et des attaques réelles.

Catégories de Sous-domaines Sensibles

CATÉGORIE	HÔTES
Développement & Staging	3

Hôtes sensibles (Top 9)

NOM D'HÔTE	IP	CATÉGORIE	PORTS	RISQUE
asset-141.acmesample.com	192.0.2.45	Développement & Staging	1	6
asset-168.acmesample.com	192.0.2.11	Autre	1	6
asset-059.acmesample.com	192.0.2.10	Développement & Staging	2	1
asset-064.acmesample.com	192.0.2.78	Autre	2	1
asset-065.acmesample.com	192.0.2.66	Autre	2	1
asset-148.acmesample.com	192.0.2.43	Développement & Staging	2	1
asset-153.acmesample.com	192.0.2.184	Autre	0	1
asset-169.acmesample.com	192.0.2.15	Autre	1	1
asset-170.acmesample.com	192.0.2.15	Autre	1	1

Surface d'authentification

Les points de terminaison d'authentification — portails SSO, passerelles VPN, panneaux de pare-feu et systèmes d'accès à distance — sont des cibles de grande valeur. La compromission d'un seul fournisseur d'identité peut donner accès à tous les services connectés. Cette section identifie tous les systèmes liés à l'authentification dans la surface d'attaque.

1	1	0
POINTS DE TERMINAISON D'AUTHENTIFICATION	TYPES UNIQUES	CONFIANCE ÉLEVÉE

Surface d'authentification par type

TYPE DE SURFACE	NOMBRE
Passerelles VPN	1

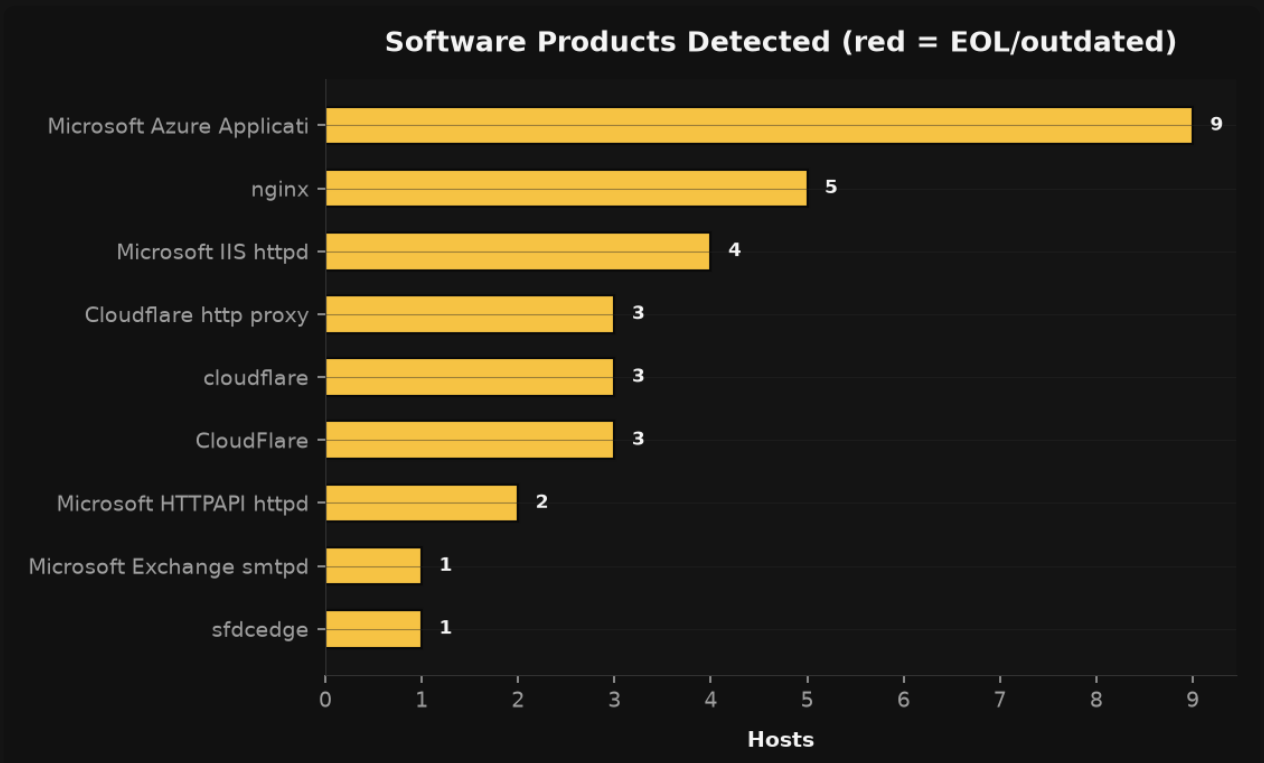
Points de terminaison d'authentification détectés

NOM D'HÔTE	IP	TYPE DE SURFACE	TECHNOLOGIE	CONFIANCE
remote.acmesample.com	192.0.2.182	Passerelles VPN	Modèle de nom d'hôte	moyen

Risque de Version Logicielle

Les versions logicielles détectées via le scan de service nmap et les données CPE de Shodan sont vérifiées par rapport aux bases de données de fin de vie (EOL) connues. Les logiciels obsolètes avec des CVE connus représentent des priorités de correction immédiates.

9	0	2
PRODUITS UNIQUES	FIN DE VIE	AVEC CVE CONNUS



Tous les produits détectés (Top 30)

PRODUIT	VERSION PRINCIPALE	HÔTES	CVE	STATUT
Microsoft Azure Application Gateway	v2	9	0	ACTUEL
nginx	—	5	60	PAS DE VERSION
Microsoft IIS httpd	10.0	4	0	ACTUEL

PRODUIT	VERSION PRINCIPALE	HÔTES	CVE	STATUT
Proxy http Cloudflare	—	3	0	PAS DE VERSION
cloudflare	—	3	3	PAS DE VERSION
CloudFlare	—	3	0	PAS DE VERSION
Microsoft HTTPAPI httpd	2.0	2	0	ACTUEL
Microsoft Exchange smtpd	—	1	0	PAS DE VERSION
sfdcedge	—	1	0	PAS DE VERSION

Analyse des chemins d'attaque et des risques de pivot

Cette section identifie les chemins potentiels de mouvement latéral basés sur l'analyse de la co-localisation réseau. Lorsque des hôtes servant différentes fonctions commerciales (par exemple, développement et production) partagent la même adresse IP ou le même sous-réseau /24, les attaquants qui compromettent le système le moins sécurisé peuvent potentiellement pivoter vers le système plus critique.

1
CHEMINS CRITIQUES

1
TOTAL DES CHEMINS

0
POINTS DE DÉFAILLANCE UNIQUES

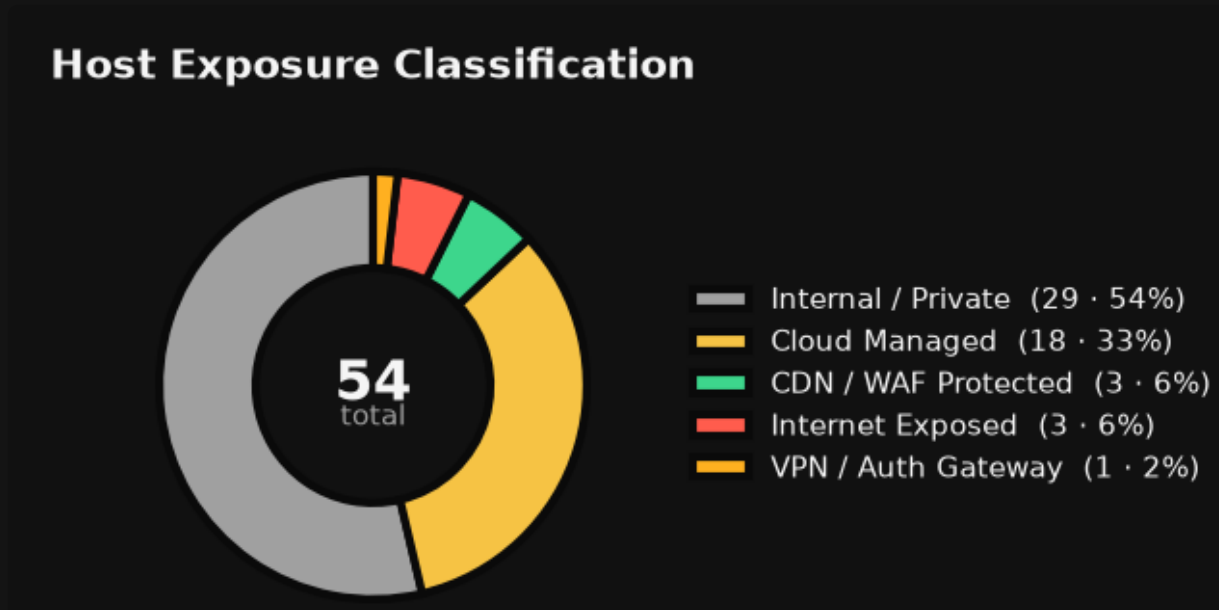
Chemins d'attaque identifiés

HÔTE SOURCE	HÔTE CIBLE	TYPE DE CHEMIN	PROXIM-ITÉ	RISQUE
asset-168.acmesample.com	www.acmesample.com	Développement → Production	MÊME IP	10

Classification de l'exposition

Chaque hôte découvert est classé par type d'exposition en fonction du fournisseur d'hébergement, des données RDAP, de l'intelligence Shodan et des motifs de nom d'hôte. Cela aide à distinguer les systèmes exposés directement à Internet de ceux protégés par CDN/WAF, gérés dans des plateformes cloud ou fournis par des fournisseurs SaaS tiers.

3 EXPOSÉ SUR INTERNET	**3** CDN / WAF PROTÉGÉ	**18** GÉRÉ PAR LE CLOUD
0 SAAS TIERS	**1** VPN / PASSERELLE D'AUTHENTIFICATION	**29** INTERNE / PRIVÉ



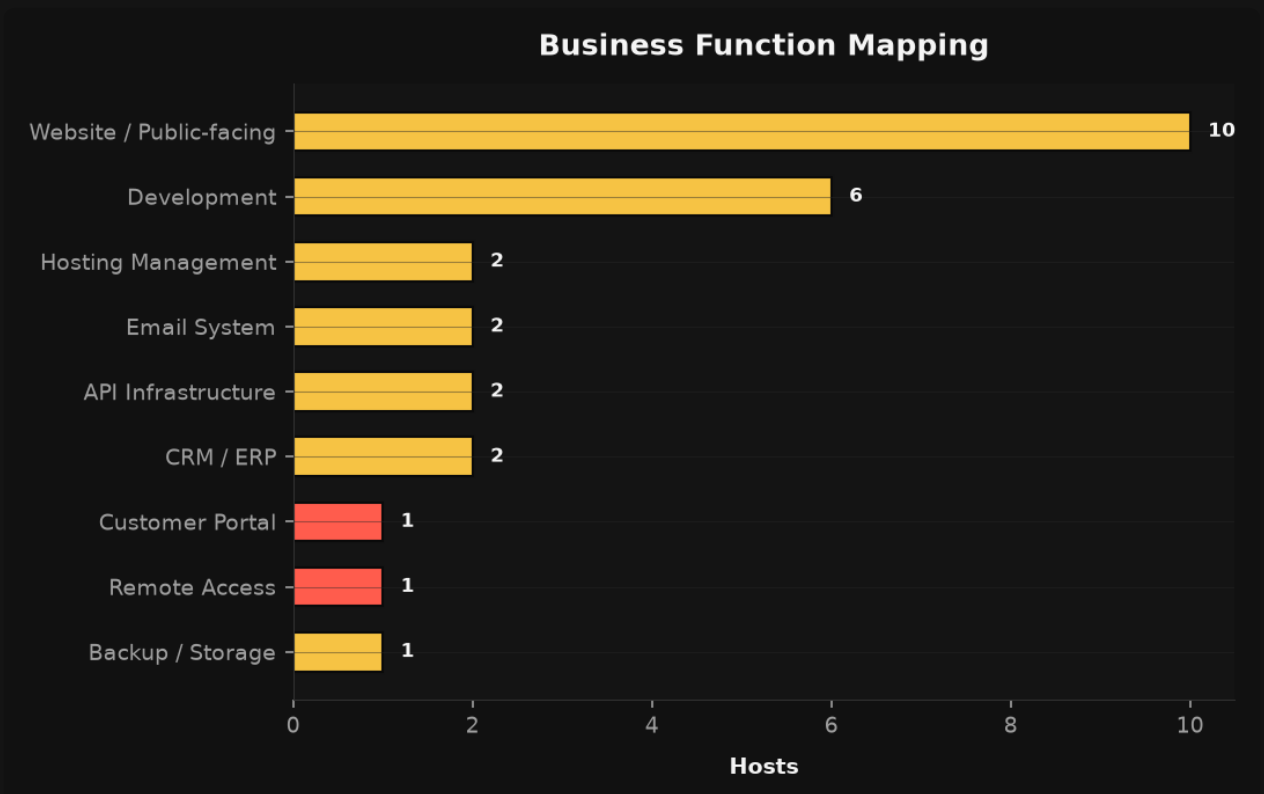
Hôtes exposés directement à Internet (Top 30)

NOM D'HÔTE	IP	TYPE D'EXPOSITION	PREUVE
asset-153.acmesample.com	192.0.2.184	EXPOSÉ SUR INTERNET	Acme Sample GmbH

Cartographie de l'impact commercial

Les hôtes découverts sont mappés aux fonctions commerciales en fonction des modèles de nom d'hôte. Cette classification aide à prioriser la remédiation en identifiant quels systèmes commerciaux critiques sont exposés à Internet.

12	9	6
SYSTÈMES CRITIQUES	SYSTÈMES À FORT IMPACT	SYSTÈMES À IMPACT MOYEN



Hôtes critiques pour l'entreprise

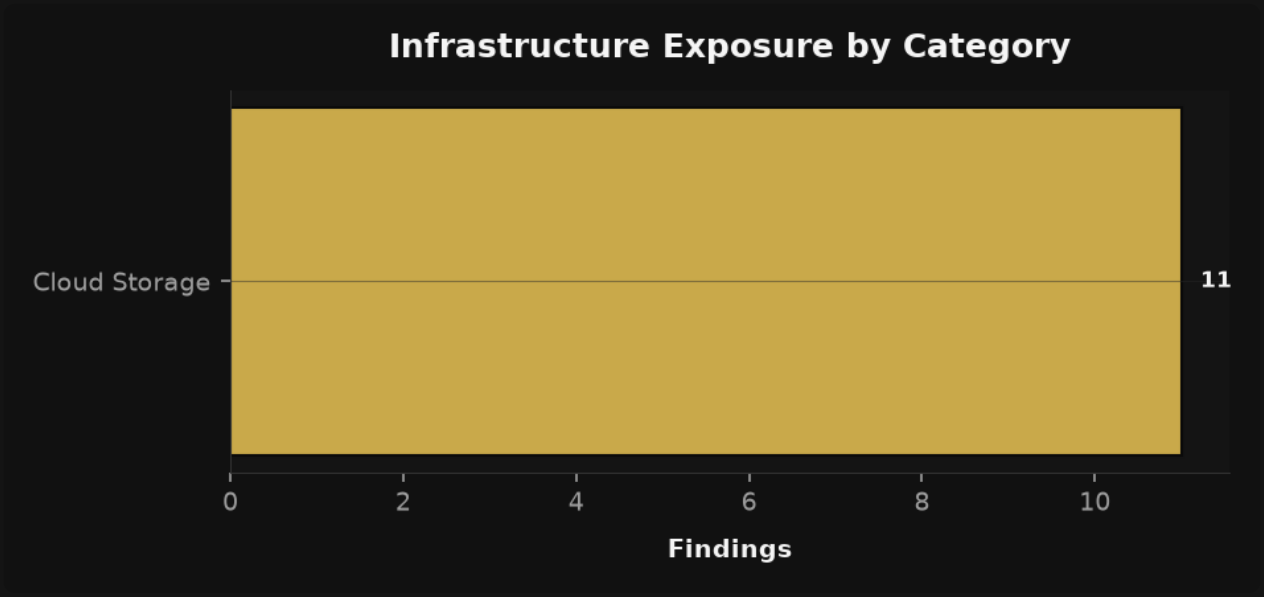
NOM D'HÔTE	IP	FONCTION COMMERCIALE	CRITICITÉ	PORTS	RISQUE
asset-047.acmesample.com	192.0.2.178	Site Web / Public	CRITIQUE	13	6
asset-071.acmesample.com	192.0.2.179	Site Web / Public	CRITIQUE	13	6
asset-166.acmesample.com	192.0.2.75	Site Web / Public	CRITIQUE	8	6

NOM D'HÔTE	IP	FONCTION COMMERCIALE	CRITICITÉ	PORTS	RISQUE
asset-143.acmesample.com	192.0.2.27	Site Web / Public	CRITIQUE	2	5
www.acmesample.com	192.0.2.11	Site Web / Public	CRITIQUE	1	5
asset-188.acmesample.com	192.0.2.27	Site Web / Public	CRITIQUE	2	5
portal.acmesample.com	192.0.2.137	Portail client	CRITIQUE	6	4
remote.acmesample.com	192.0.2.182	Accès à distance	CRITIQUE	1	1
asset-049.acmesample.com	192.0.2.63	Site Web / Public	CRITIQUE	1	0
asset-134.acmesample.com	192.0.2.65	Site Web / Public	CRITIQUE	2	0
asset-146.acmesample.com	192.0.2.49	Site Web / Public	CRITIQUE	2	0
asset-174.acmesample.com	192.0.2.61	Site Web / Public	CRITIQUE	0	0
asset-062.acmesample.com	192.0.2.178	Système de messagerie	ÉLEVÉ	13	6
asset-141.acmesample.com	192.0.2.45	Infrastructure API	ÉLEVÉ	1	6
asset-142.acmesample.com	192.0.2.13	Infrastructure API	ÉLEVÉ	1	5
asset-064.acmesample.com	192.0.2.78	CRM / ERP	ÉLEVÉ	2	1
asset-065.acmesample.com	192.0.2.66	CRM / ERP	ÉLEVÉ	2	1
asset-152.acmesample.com	192.0.2.33	Sauvegarde / Stockage	ÉLEVÉ	2	0
asset-168.acmesample.com	192.0.2.11	Développement	MOYEN	1	6
asset-059.acmesample.com	192.0.2.10	Développement	MOYEN	2	1
asset-148.acmesample.com	192.0.2.43	Développement	MOYEN	2	1
asset-169.acmesample.com	192.0.2.15	Développement	MOYEN	1	1
asset-170.acmesample.com	192.0.2.15	Développement	MOYEN	1	1

Exposition Cloud & Infrastructure

Composants d'infrastructure détectés par analyse du panneau d'administration, vérification des noyaux et analyse des ports ouverts. Bases de données exposées, orchestration de conteneurs, pipelines CI/CD et systèmes de surveillance représentent des cibles de grande valeur pour les attaquants.

11
STOCKAGE CLOUD



Constatations d'infrastructure

HÔTE	IP	CATÉGORIE	TYPE	SOURCE	GRAVITÉ
		Stockage Cloud	11 fichiers exposés	Analyse d'exposition au cloud	ÉLEVÉ

Violations mentionnant vos serveurs

Notre base de données de violations a été recherchée pour tous les noms d'hôtes (FQDN) confirmés découverts lors de cette évaluation. Lorsqu'un nom d'hôte de serveur apparaît dans les données de violation, cela signifie qu'un enregistrement — tel qu'une URL, un formulaire de connexion ou un identifiant utilisateur — fait référence à ce serveur. **Cela ne signifie pas nécessairement que le serveur lui-même a été compromis.** Les explications courantes incluent :

- Les utilisateurs dont les appareils ont été infectés par un logiciel malveillant de vol ont vu leurs identifiants enregistrés dans le navigateur pour ces serveurs capturés et divulgués
- Bases de données publiques ou compilations de violations agrégées qui indexent les URL et les points de terminaison de connexion
- Services tiers qui font référence à votre infrastructure dans leurs données

Les serveurs avec un nombre élevé de dossiers de violation de type identifiant méritent une attention immédiate, car ils indiquent que les identifiants de connexion pour ces systèmes circulent activement dans les canaux des acteurs malveillants.

Comment cela se compare à l'exposition plus large des violations : le chapitre ci-dessous couvre **17** registrements de violation qui font explicitement référence à l'un de vos noms d'hôte de serveur découverts. Le chapitre sur l'Exposition de Credentials Fuités montre **2,038** enregistrements de violation mentionnant votre domaine dans n'importe quel champ (URLs, emails, hachages, pièces jointes) — une mesure plus large de la fréquence à laquelle votre organisation apparaît dans les corpus de violations. Le nombre spécifique au serveur est un sous-ensemble strict.

1
SERVEURS DANS LES VIOLATIONS

26
SERVEURS RECHERCHÉS

17
ENREGISTREMENTS DE RÉFÉRENCE DU SERVEUR
sous-ensemble de 2,038 à l'échelle du domaine

50
SOURCES DE VIOLATION UNIQUES

www.acmesample.com 192.0.2.11

17 enregistrements **17** violations **1** identifiants **1** emails

16 URLs

journal (7) url (15) hash (7) nom (8) email (16)

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

Détails de la violation du serveur

NOM D'HÔTE	IP	ENREGIS-TRE-MENTS	VIOL-ATION S	IDEN-TIFI-ANTS	TYPES DE DON-NÉES PRINCI-PAUX	PLAGE DE DATES
www.acmesample.com	192.0.2.11	**17**	**17**	**1**	log, url, hash	2021-08-18 — 2026-07-15

PAYSAGE DE MENACES

Réputation IP & Renseignement sur les menaces

Chaque adresse IP unique dans la surface d'attaque est vérifiée contre plusieurs flux de renseignement sur les menaces : listes de nœuds de sortie TOR, liste DROP de Spamhaus (Ne pas router ou pairer) des réseaux contrôlés par des criminels, rapports d'abus AbuseIPDB, pulsations de menaces AlienVault OTX, et la base de données IP malveillantes C99. Les résultats sont mis en cache pendant 30 jours pour minimiser les appels API lors des scans répétés.

22 IPS VÉRIFIÉES	**0** NŒUDS DE SORTIE TOR	**0** SUR SPAMHAUS DROP
0 RAPPORTS D'ABUS	**4** DANS LES FLUX DE MENACES	**0** C99 MALVEILLANT

Résumé

Vérifié 22 IPs. Signalé : 4 dans les flux de menaces.

IPs signalées (Top 30)

ADRESSE IP	NOMS D'HÔTE	TOR	SPAMHAUS DROP	ABUSEIP-DB	IMPUL-SIONS OTX	C99
192.0.2.75	asset-166.acm...	—	Propre	0	6	Propre
192.0.2.178	asset-047.acm...	—	Propre	0	50	Propre
192.0.2.65	asset-134.acm...	—	Propre	15	3	Propre
192.0.2.179	asset-071.acm...	—	Propre	2	50	Propre

Analyse de l'exposition du code

82
BON

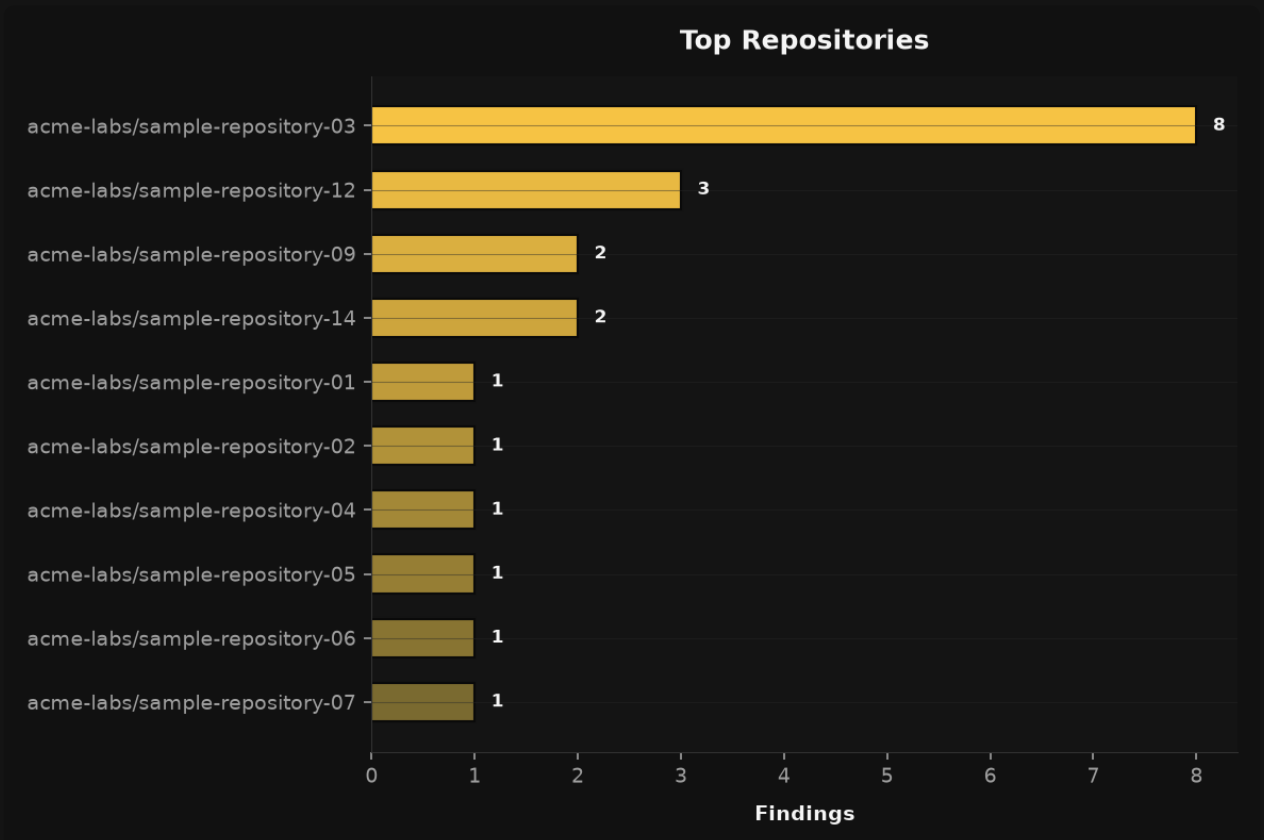
Recherche dans les dépôts et Gists GitHub pour du code source exposé, des secrets, des clés API et des données sensibles mentionnant **acmesample.com**. Chaque constat est noté de 0 à 10 pour le risque par analyse IA et scanné contre plus de 150 modèles de détection de secrets.

26 Total des constatations	0 Risque ÉLEVÉ (7-10)	0 Risque Moyen (4-6)

26
FAIBLE / INFO

Résumé

26 constatations d'exposition de code anonymisées ont été conservées. Les noms de référentiels, les chemins de fichiers, les extraits et les identités tierces ont été remplacés pour cet échantillon public.



Top des dépôts par nombre de constatations

Principales constatations

acme-labs/sample-repository-01 data/jeu de donnees de preuves prive **3/10**

```
# Extrait de code public anonymise 01
TARGET_DOMAIN = "acmesample.com"
```

Un dépôt public a référencé l'organisation échantillon. L'extrait original et les identités tierces ont été supprimés de cette copie marketing.

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

```
# Extrait de code public anonymise 02
TARGET_DOMAIN = "acmesample.com"
```

Un dépôt public a référencé l'organisation échantillon. L'extrait original et les identités tierces ont été supprimés de cette copie marketing.

acme-labs/sample-repository-03 data/jeu de donnees de preuves prive **1/10**

```
# Extrait de code public anonymise 03
TARGET_DOMAIN = "acmesample.com"
```

Un dépôt public a référencé l'organisation échantillon. L'extrait original et les identités tierces ont été supprimés de cette copie marketing.

acme-labs/sample-repository-03 data/jeu de donnees de preuves prive **1/10**

```
# Extrait de code public anonymise 04
TARGET_DOMAIN = "acmesample.com"
```

Un dépôt public a référencé l'organisation échantillon. L'extrait original et les identités tierces ont été supprimés de cette copie marketing.

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

```
# Extrait de code public anonymise 05
TARGET_DOMAIN = "acmesample.com"
```

Un dépôt public a référencé l'organisation échantillon. L'extrait original et les identités tierces ont été supprimés de cette copie marketing.

Affichage des 5 premiers sur 26 constatations. La liste complète est omise de cet échantillon public.

Exposition Telegram, Discord & Paste

Recherche des canaux de hackers Telegram, des serveurs de cybersécurité Discord et des sites de paste pour des mentions de **Acme Sample GmbH** (dérivé de acmesample.com). Les preuves de source brute sont conservées pour audit. Seules les lignes classées de manière déterministe **exact** ou **corroboré** peut recevoir une gravité AI ou affecter le risque client.

Non évalué

Cette population source ou ses lignes pertinentes n'ont pas été entièrement évaluées. Les preuves manquantes, ambiguës ou non analysées ne sont pas interprétées comme un zéro propre.

Source coverage: No source_coverage_v1 evidence was persisted.

0 Mentions brutes	0 Exact / Corroboré	0 Analysé
0 Affiché	0 Critique + Élevé	Non analysé Score de risque

Totaux de source brute — Telegram : 0, Discord : 0, Paste : 0. Les lignes pertinentes sont traitées par lots équitables de jusqu'à 80 ; il s'agit d'une taille de lot, pas d'une limite de lignes totales. Cette évaluation est partielle.

Évaluation limitée par des preuves

0 mention(s) de source brute ont été conservées pour audit. La pertinence déterministe a conservé 0 ligne(s) exacte(s) ou corroborée(s). Aucun score de risque soutenu n'a été produit. L'évaluation est partielle ; les preuves non analysées ou indisponibles ne sont pas présentées comme un zéro propre.

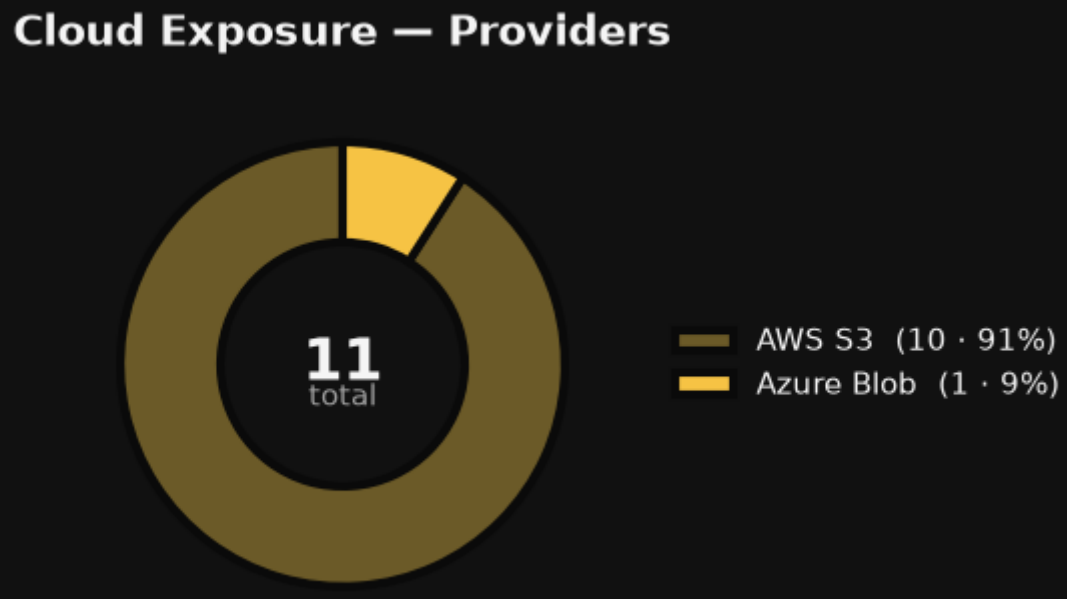
Exposition de stockage cloud

Fichiers exposés découverts dans des buckets de stockage cloud public (AWS S3, Azure Blob Storage, Google Cloud Storage) correspondant au nom de l'organisation.

11	7	2
FICHIERS TROUVÉS	FICHIERS SENSIBLES	FOURNISSEURS DE CLOUD

Résumé

11 fichiers trouvés dans des buckets de stockage cloud exposés. 7 sont sensibles à la sécurité (configs, bases de données, archives, scripts). Fournisseurs de cloud : AWS S3 (10), Azure Blob (1).



Fichiers exposés

URL DU FICHIER	FOURNISSEUR	EXT	TAILLE	SENSIBLE
https://sample-storage.invalid/redacted/sample-file-001.dat	AWS S3	pdf	**9214,4 Ko**	—
https://sample-storage.invalid/redacted/sample-file-002.dat	AWS S3	pdf	**596,6 Ko**	—
https://sample-storage.invalid/redacted/sample-file-003.dat	Azure Blob	pdf	**570,0 Ko**	—
https://sample-storage.invalid/redacted/sample-file-004.dat	AWS S3	pdf	**223,1 Ko**	—
https://sample-storage.invalid/redacted/sample-file-005.dat	AWS S3	xml	**0,3 Ko**	FICHIER DE DONNÉES/ CONFIGURATION
https://sample-storage.invalid/redacted/sample-file-006.dat	AWS S3	xml	**0,3 Ko**	FICHIER DE DONNÉES/ CONFIGURATION
https://sample-storage.invalid/redacted/sample-file-007.dat	AWS S3	xml	**0,3 Ko**	FICHIER DE DONNÉES/ CONFIGURATION
https://sample-storage.invalid/redacted/sample-file-008.dat	AWS S3	emb	**85,5 Ko**	
https://sample-storage.invalid/redacted/sample-file-009.dat	AWS S3	emb	**84,5 Ko**	
https://sample-storage.invalid/redacted/sample-file-010.dat	AWS S3		**81,1 Ko**	
https://sample-storage.invalid/redacted/sample-file-011.dat	AWS S3	info	**0,2 Ko**	

Exposition d'URL raccourcie

URLs raccourcies (goo.gl, bit.ly, tinyurl, ow.ly, etc.) qui pointent vers ou référencent le domaine scanné. Ces liens révèlent des ressources internes partagées à l'extérieur, des documents sensibles et des domaines potentiels d'usurpation de marque.

3,000	0	1	0
LIENS TOTAUX	RESSOURCES INTERNES	FICHIERS NON-HTML	DOMAINES DE PHISHING

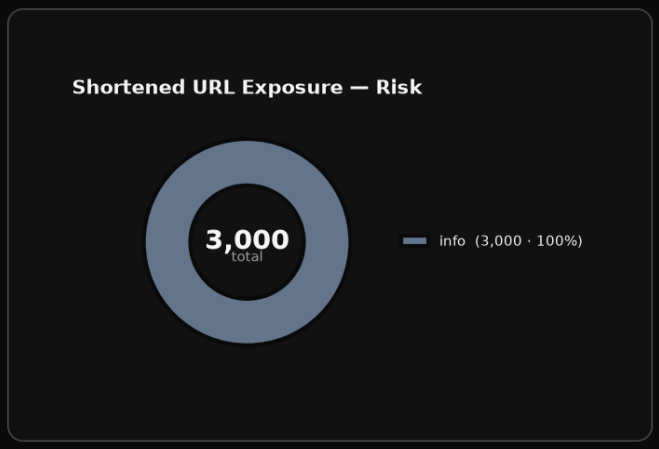
Les compteurs de titres résument chaque lien valide retourné et classé par le scan. Les enregistrements de constat détaillés sont conservés pour au maximum **5 000 liens**. Les tableaux PDF sont des échantillons de présentation plus petits, et `jeu de donnees de preuves prive` contient uniquement les constatations conservées qui restent après toute exclusion de rapport ; les lignes au-delà de la limite de conservation ne sont pas disponibles en tant que preuves détaillées.

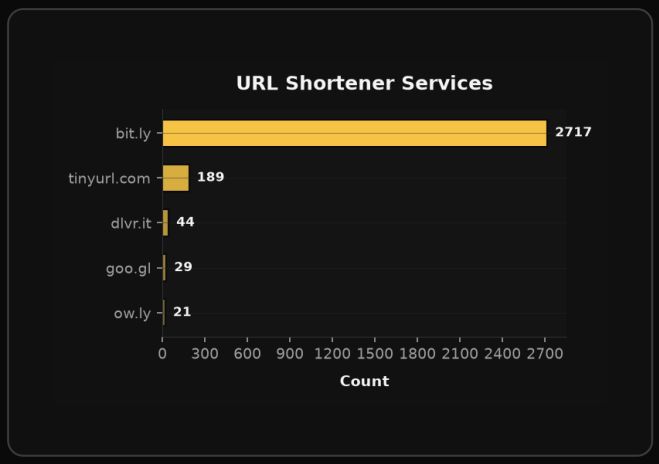
Résumé

3000 URL raccourcies trouvées pointant vers ou référencant acmesample.com. 1 point directement vers des ressources de domaine propre. 1 lien vers des fichiers non-HTML (PDF, documents, archives).

Pourquoi les URL raccourcies sont importantes pour la sécurité
Les raccourcisseurs d'URL cachent la véritable destination, ce qui les rend populaires pour le partage de ressources internes (SharePoint, Google Drive, Dropbox). Lorsque les employés partagent des liens raccourcis publiquement, ces ressources internes deviennent découvrables. Les jetons d'accès intégrés dans les URL raccourcies peuvent encore être valides, accordant un accès direct aux fichiers d'entreprise. Les campagnes de phishing utilisent également des URL raccourcies avec des domaines similaires à des marques pour contourner les filtres de messagerie.

1	2,999
LIENS DE DOMAINE PROPRE	RÉFÉRENCES TIERCES


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

Exposition sur les réseaux sociaux

80
BON

Analyse de l'exposition de la marque sur YouTube, Twitter/X, Facebook, LinkedIn, Reddit et les plateformes sociales indexées par Google. Les constatations incluent la détection d'usurpation de marque, de faux profils et de mentions de phishing.

192
TOTAL DES CONSTATATIONS

3
PROFILS OFFICIELS

1
RISQUES D'USURPATION

0
MENTIONS DE PHISHING

192 mentions sur les réseaux sociaux analysées sur **7** plateformes.**3** classées comme risques exploitables,**112** comme correspondances de noms de marque non pertinentes,**80** comme officielles ou bénignes.

Canaux officiels vérifiés

Profils de médias sociaux officiels identifiés à partir des métadonnées du site web de l'entreprise, des enregistrements DNS, des données structurées et du scanning des médias sociaux. Ceux-ci sont **exclus** des constatations d'imitation ci-dessous.

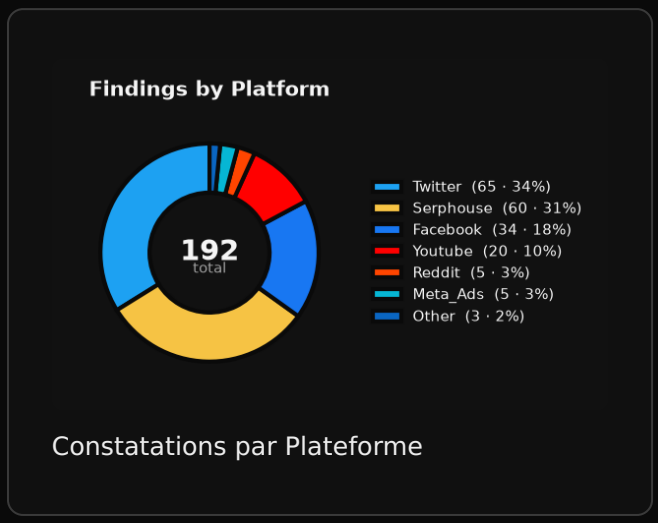
PLATE-FORME	GÉRER / NOM	URL	SOURCE
Twitter	Acme Sample GmbH	https://x.com/Acme Sample GmbH	Métadonnées de l'entreprise
Facebook	Acme Sample GmbH	https://facebook.com/Acme Sample G...	Métadonnées de l'entreprise
Linkedin	company/Acme Sample GmbH	https://linkedin.com/company/Acme S...	Métadonnées de l'entreprise
Youtube	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account-...	Analyse des réseaux sociaux

Résumé

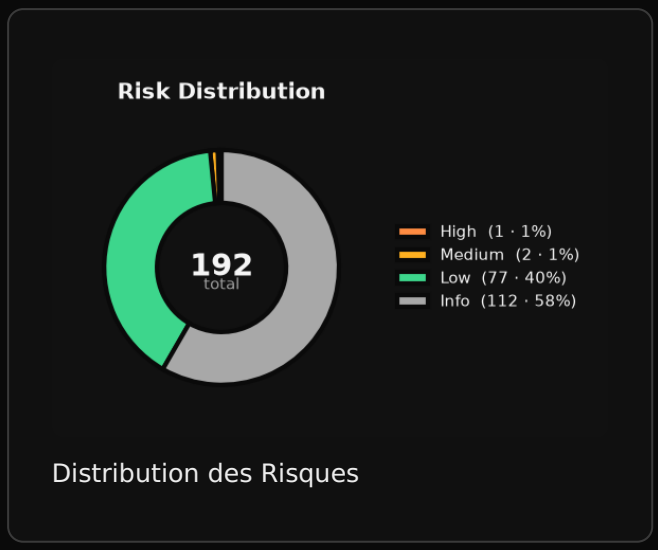
Trouvé 192 mentions sur les réseaux sociaux pour acmesample.com sur 7 plateformes. 3 profils officiels confirmés trouvés. 1 risque potentiel d'imitation de marque détecté.

Évaluation des risques IA

Les constatations consistent principalement en des mentions bénignes et des discussions sur les produits d'Acme Sample GmbH sur diverses plateformes. Il n'y a aucune indication d'usurpation d'identité critique ou à haut risque ou d'activité frauduleuse liée à la marque.



Constatations par Plateforme



Distribution des Risques

Publicité potentiellement frauduleuse

Analyse des publicités payantes sur la bibliothèque d'annonces LinkedIn, la bibliothèque d'annonces Meta et la bibliothèque d'annonces TikTok mentionnant la marque. Les annonces sont classées par niveau de menace : annonces de phishing/hameçonnage qui usurpent la marque, annonces de concurrents exploitant le nom de la marque, et publicités légitimes/neuves. La confiance de classification indique à quel point l'évaluation de l'IA est certaine de la catégorie assignée.

> Classification retenue de l'évaluation de la source; les détails du compte identifiés ont été supprimés.

Les 5 annonces semblent toutes légitimes ou officielles. Aucune annonce frauduleuse n'a été détectée.

PLATEFORME	ANNONCEUR	CONTENU DE L'ANNONCE	RISQUE	CERTITUDE	CLASSIFICATION
Meta	Compte d'échantillon 670	Mention publique de Sample d'Acme Sample GmbH ; compte original et copie anonymisés. — Mention publique de Sample d'Acme Sample GmbH ; compte original et…	FAIBLE	85%	Classification retenue de l'évaluation de la source;…
Meta	Compte d'échantillon 670	Mention publique de Sample d'Acme Sample GmbH ; compte original et copie anonymisés. — Mention publique de Sample d'Acme Sample GmbH ; compte original et…	FAIBLE	85%	Classification retenue de l'évaluation de la source;…
Meta	Compte d'exemple 304	Mention publique de Sample d'Acme Sample GmbH ; compte original et copie anonymisés. — Mention publique de Sample d'Acme Sample GmbH ; compte original et…	FAIBLE	85%	Classification retenue de l'évaluation de la source;…
Meta	Compte Échantillon 011	Mention publique de Sample d'Acme Sample GmbH ; compte original et copie anonymisés. — Mention publique de Sample d'Acme Sample GmbH ; compte original et…	INFO	—	Classification retenue de l'évaluation de la source;…
Meta	Compte d'échantillon 789	Mention publique de Sample d'Acme Sample GmbH ; compte original et copie anonymisés. — Mention publique de Sample d'Acme Sample GmbH ; compte original et…	INFO	—	Classification retenue de l'évaluation de la source;…

Twitter — 65 constatations (2 moyen, 55 faible, 8 info)

RISQUE	TITRE	URL	RAISON
MOYEN	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account…	Classification retenue de l'évaluation de la source; les détails du compte…
MOYEN	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account…	Classification retenue de l'évaluation de la source; les détails du compte…
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account…	Classification retenue de l'évaluation de la source; les détails du compte…
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account…	Classification retenue de l'évaluation de la source; les détails du compte…
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account…	Classification retenue de l'évaluation de la source; les détails du compte…

Affichage des 5 premiers sur 65. Preuves complètes omises de cet échantillon public.

Serphouse — 60 constatations (60 info)

RISQUE	TITRE	URL	RAISON
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...

Affichage des 5 premiers sur 60. Preuves complètes omises de cet échantillon public.

Facebook — 34 constatations (1 élevé, 33 info)

Tous les liens relatifs à `https://social.invalid/`

RISQUE	TITRE	URL	RAISON
ÉLEVÉ	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0008	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0241	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0243	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0245	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0247	Classification retenue de l'évaluation de la source; les détails du compte...

Affichage des 5 premiers sur 34. Preuves complètes omises de cet échantillon public.

Youtube — 20 constatations (19 faible, 1 info)

Tous les liens relatifs à `https://social.invalid/`

RISQUE	TITRE	URL	RAISON
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0016	Classification retenue de l'évaluation de la source; les détails du compte...
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0020	Classification retenue de l'évaluation de la source; les détails du compte...
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0024	Classification retenue de l'évaluation de la source; les détails du compte...
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0028	Classification retenue de l'évaluation de la source; les détails du compte...
FAIBLE	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0032	Classification retenue de l'évaluation de la source; les détails du compte...

Affichage des 5 premiers sur 20. Preuves complètes omises de cet échantillon public.

Reddit — 5 constatations (5 info)

RISQUE	TITRE	URL	RAISON
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	https://social.invalid/sample-account...	Classification retenue de l'évaluation de la source; les détails du compte...

Linkedin — 3 constatations (3 info)

Tous les liens relatifs à `https://social.invalid/`

RISQUE	TITRE	URL	RAISON
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0307	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0309	Classification retenue de l'évaluation de la source; les détails du compte...
INFO	Mention publique d'Acme Sample GmbH ; compte original et copie anonymisés.	../sample-account-0313	Classification retenue de l'évaluation de la source; les détails du compte...

Analyse de Typosquatting de Domaine

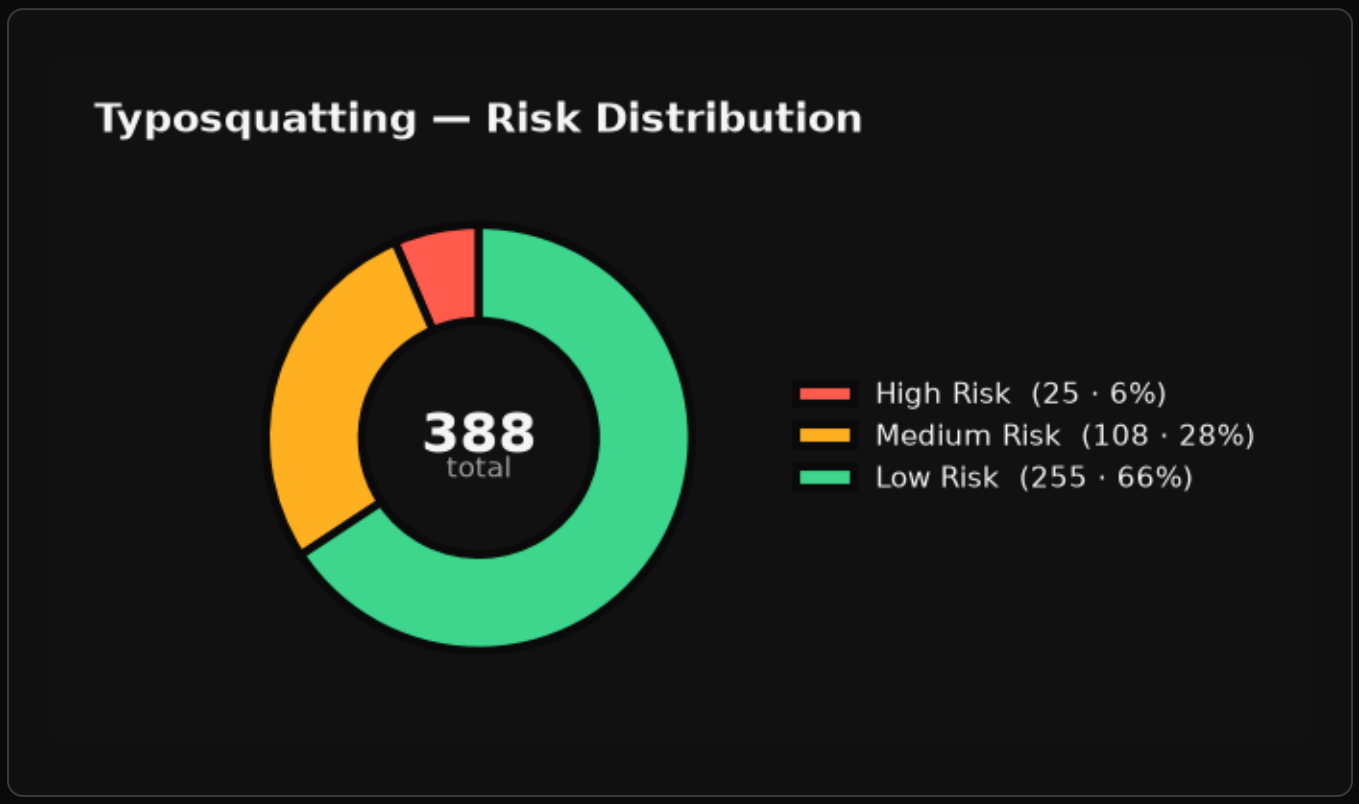
50
MAUVAIS

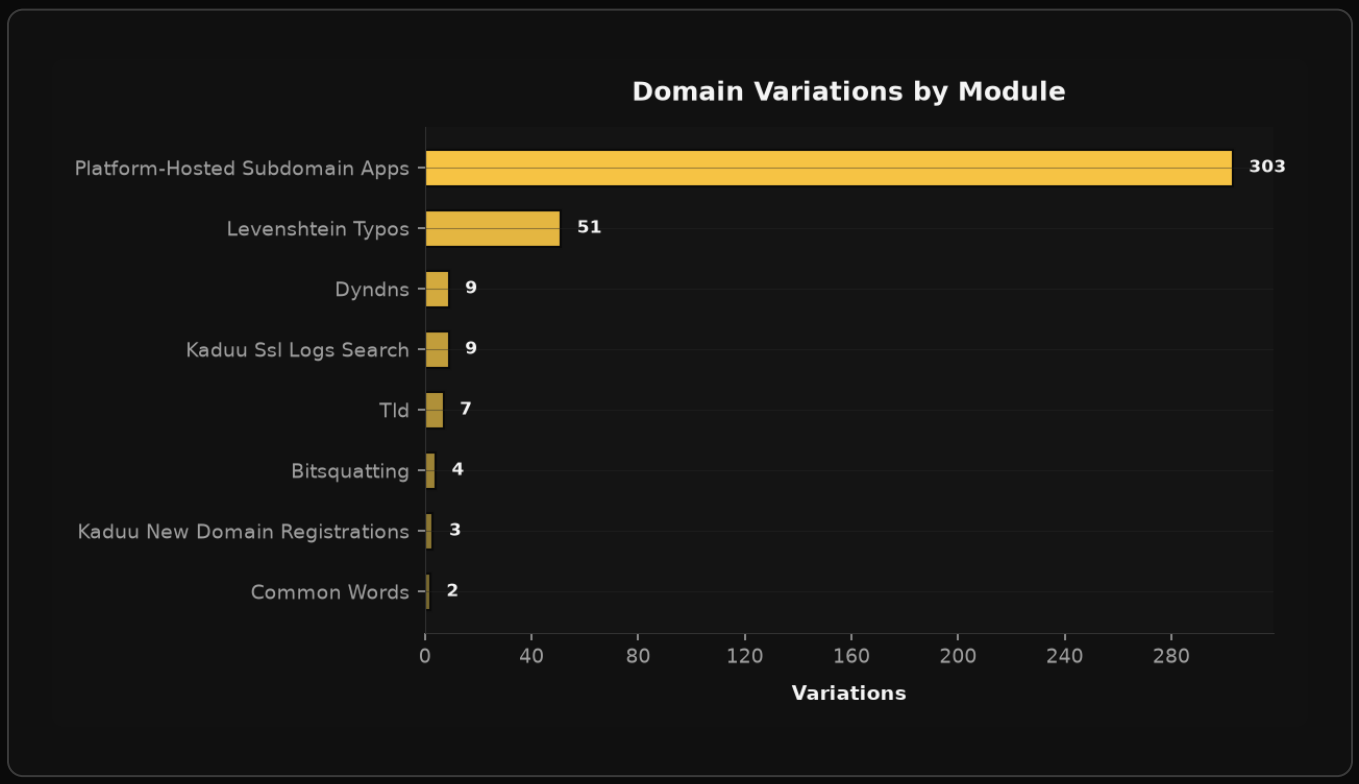
Analyse de variation de domaine alimentée par SpoofGuard. Génère des typosquats, homoglyphes, bit-squatting, échanges de TLD et d'autres domaines similaires, puis vérifie chacun pour les enregistrements DNS, les serveurs web actifs et les indicateurs de phishing.

96,461	372	362	0
VARIATIONS TOTALES	AVEC LES ENREGISTREMENTS DNS	SERVEURS WEB ACTIFS	PHISHING DÉTECTÉ

Résumé

SpoofGuard a généré 96,461 variations ressemblantes pour acmesample.com. 372 se résolvent dans DNS ; après des vérifications de vivacité actives, 59 servent réellement du contenu en direct (le reste est stationné, sous-domaines de plateforme non revendiqués, ou renvoie des erreurs). 26 sont classés à risque ÉLEVÉ — spoofing de marque/visuel confirmé, un hit de phishing-feed, ou un verdict malveillant de vision GPT. 109 de plus sont Moyens (ressemblances actives pas encore confirmées malveillantes).





Variations de domaine — Risque ÉLEVÉ & MOYEN

Affichage des 30 premiers sur 100 entrées. Données complètes dans `jeu de donnees de preuves prive` omis de cet échantillon public.

DOMAINE	MODULE	ENREGIS-TREMENT A	WEB	PERTIN-ENCE	RISQUE
acmesampl3.com	Fautes de Levenshtein	192.0.2.114	–	ÉLEVÉ	ÉLEVÉ
acme-sample-login.net	Fautes de Levenshtein	192.0.2.187	–	ÉLEVÉ	ÉLEVÉ
acmesample.dnsdyn.net	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.now-dns.org	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.dynserv.org	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.tcp4.me	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.dnsup.net	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.mypi.co	Dyndns	192.0.2.1	–	ÉLEVÉ	ÉLEVÉ
acmesample.cn	Tld	–	–	ÉLEVÉ	ÉLEVÉ
acmesample-alert-010.inv…	Fautes de Levenshtein	–	–	ÉLEVÉ	ÉLEVÉ
acmesample-alert-011.inv…	Fautes de Levenshtein	–	–	ÉLEVÉ	ÉLEVÉ
acmesamplelp.com	Kaduu Nouvelles Enregistrements de Domaines	–	–	ÉLEVÉ	ÉLEVÉ
acmesample.com.br	Tld	–	–	MOYEN	ÉLEVÉ
acmesample.biz	Tld	–	–	MOYEN	ÉLEVÉ
teaacmesample.com	Kaduu Nouvelles Enregistrements de Domaines	–	–	MOYEN	ÉLEVÉ
acmesamplestore.com	Mots courants	–	–	MOYEN	ÉLEVÉ
sample-redirect-01.invalid	Tld	192.0.2.93	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-02.invalid	Tld	192.0.2.93	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-03.invalid	Tld	192.0.2.93	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-04.invalid	Fautes de Levenshtein	192.0.2.102	HTTPS	ÉLEVÉ	MOYEN

DOMAINE	MODULE	ENREGIS-TREMENT A	WEB	PERTIN-ENCE	RISQUE
sample-redirect-05.invalid	Dyndns	192.0.2.55	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-06.invalid	Recherche des journaux Ssl de Kaduu	192.0.2.71	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-07.invalid	Recherche des journaux Ssl de Kaduu	192.0.2.168	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-08.invalid	Recherche des journaux Ssl de Kaduu	192.0.2.77	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-09.invalid	Recherche des journaux Ssl de Kaduu	192.0.2.79	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-10.invalid	Kaduu Nouvelles Enregistrements de Domaines	192.0.2.93	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-11.invalid	Recherche des journaux Ssl de Kaduu	192.0.2.149	HTTPS	ÉLEVÉ	MOYEN
sample-redirect-12.invalid	Mots courants	192.0.2.167	HTTP	ÉLEVÉ	MOYEN
l-acmesample.art.pl	Applications de sous-domaine hébergées sur la plateforme	192.0.2.138	HTTPS	ÉLEVÉ	MOYEN
acmesample.aquila.it	Tld	192.0.2.155	HTTPS	MOYEN	MOYEN

Visual Verdict — Top 2 des Look-Alikes les Plus Suspects

Un véritable navigateur sans tête a été ouvert sur chaque site similaire pour rendre la page (capturant les redirections basées sur JS vers des pages de stationnement, des réseaux publicitaires ou des sites d'imitation que de simples sondages HTTP manquent). GPT-4o a analysé chaque capture d'écran avec la chaîne de redirection et le contexte de l'organisation cible pour produire un verdict.

Affichage des 2 ressemblances les plus prioritaires. **Verdicts, URL finales, chaînes de redirection et liens d'écran pour TOUS les 10 ressemblances enrichies sont dans `jeu de donnees de preuves prive`** (colonnes : `URL finale`, `Catégorie de verdict`, `Gravité de verdict`, `Résumé de verdict`, `Preuve de verdict`, `URL d'écran local`).



l-acmesample.art.pl

RISQUE MOYEN · REDIRIGER VERS NON LIÉ · MOYEN

Redirections vers un domaine non lié, posant un risque de tromper les utilisateurs en les éloignant du site prévu.

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

- L'URL final est sample-redirect-13.invalid, sans rapport avec Acme Sample GmbH.
- Redirection inter-hôtes basée sur JS détectée.



acmesample-alert-044.invalid

RISQUE MOYEN · REDIRIGER VERS NON LIÉ · FAIBLE

Le domaine redirige vers une entreprise légitime non liée, ne posant aucune menace pour Acme Sample GmbH.

JS redirection → https://sample-redirect-18.invalid/

- L'URL finale est sample-redirect-18.invalid, sans rapport avec Acme Sample GmbH.
- Le titre de la page indique une industrie différente : Fabrication de cartes.

Exposition cybernétique de l'acteur malveillant

79
BON

Les acteurs malveillants — notamment les **groupes de rançongiciels** — sont des opérations criminelles organisées qui violent des organisations, encryptent leurs données et extorquent un paiement pour leur libération. Beaucoup opèrent sous un modèle de “Ransomware-as-a-Service” (RaaS) et maintiennent des sites de fuite publics où ils listent les victimes qui refusent de payer. Ces groupes scannent en continu Internet à la recherche de cibles vulnérables, rendant chaque service exposé un point d'entrée potentiel.

Ce chapitre évalue l'exposition de votre organisation à ces acteurs malveillants en fonction de l'industrie, de la géographie, de la taille de l'organisation et des données d'intelligence sur les rançongiciels disponibles publiquement.

PRESSION CIBLÉE
Moyen
Exposition globale aux menaces

EXPOSITION SECTORIELLE
Moyen
Risque piloté par l'industrie

MODIFICATEUR DE PAYS
Augmente le risque
Modificateur basé sur la géographie

VOTRE ORGANISATION
Risque ÉLEVÉ
Pays (#1) et secteur d'activité (#20) tous deux dans le top 20 des cibles

Menaces les Plus Pertinentes

Rançongiciel	ÉLEVÉ	Le rançongiciel est une menace significative pour les secteurs de la fabrication en raison des perturbations opérationnelles potentielles.
Attaques de la chaîne d'approvisionnement	Moyen	La dépendance à des chaînes d'approvisionnement complexes dans la fabrication industrielle la rend vulnérable aux attaques de la chaîne d'approvisionnement.
Violations de Données	Moyen	Les violations de données peuvent exposer des informations sensibles, impactant les opérations commerciales et la réputation.

Coûts Estimés d'une Attaque Rançongiciel Réussie

En fonction de la taille de l'organisation identifiée de **501-1000 employés** (Moyenne supérieure), les recherches sectorielles estiment l'impact financier suivant si l'organisation devait être touchée par une attaque par rançongiciel :

MÉTRIQUE	VALEUR ESTIMÉE
Coût Total Moyen	**$1,300,000**
Coût moyen de récupération	$1,300,000
Rançon moyenne payée	$300,000
Taux de paiement estimé	40%

Basé sur Sophos 251–1 000 employés ; la rançon varie en fonction de la gravité de l'impact plutôt que de la taille de l'organisation seule.

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

Pourquoi la surveillance de la surface d'attaque peut prévenir les attaques par rançongiciel

Les attaquants exploitent souvent d'abord les surfaces d'attaque exposées.

Les cybercriminels scannent en continu Internet à la recherche de services ouverts, de mots de passe faibles et d'identifiants divulgués. Si quelque chose est exposé, il sera trouvé — souvent automatiquement.

Deux exemples typiques :

- **RDP/VPN exposé :** les attaquants trouvent un service d'accès à distance ouvert et se connectent en utilisant la force brute ou des identifiants volés.
- **Réutilisation de mot de passe :** des identifiants divulgués sont réutilisés pour accéder aux systèmes d'entreprise via le bourrage de mots de passe.

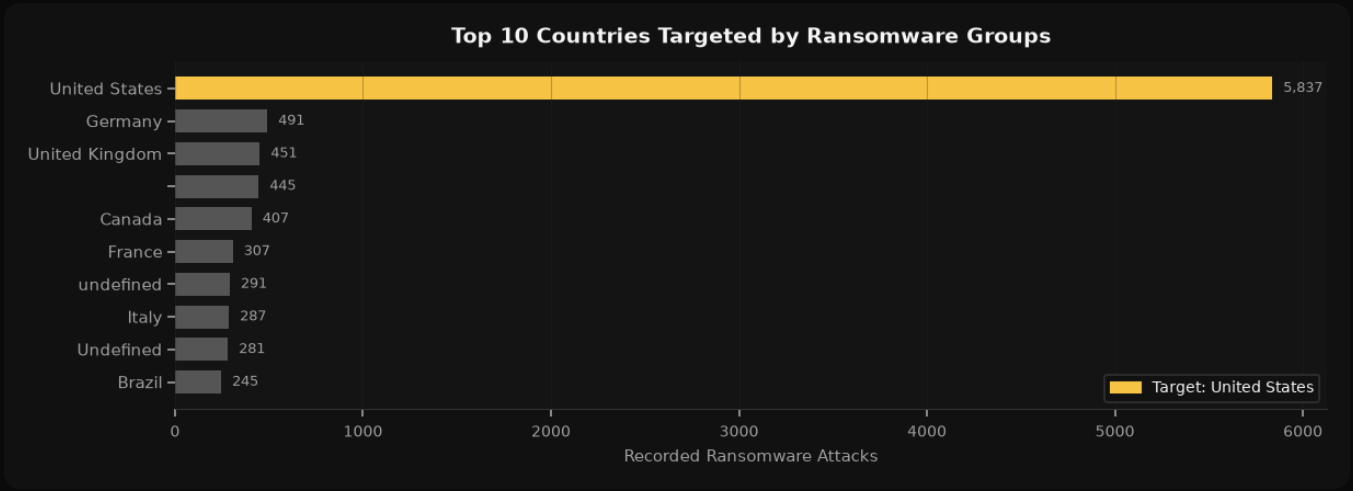
La surveillance de la surface d'attaque est critique car elle vous montre ce que les attaquants peuvent déjà voir et exploiter. Si vous réduisez cette visibilité — en fermant des ports, en sécurisant l'accès et en détectant des identifiants compromis — vous réduisez considérablement le risque de rançongiciel avant même qu'il ne commence.

Votre organisation est-elle répertoriée sur un site d'acteur malveillant ?

Les groupes de rançongiciels exploitent des « sites de fuite » publics sur le dark web où ils listent les organisations qui ont été compromises et ont refusé de payer. Être listé sur un tel site est un fort indicateur que l'organisation a été violée et que des données sensibles ont pu être exfiltrées. Notre base de données surveille en continu ces sites et suit actuellement **13,180** enregistrements de victimes à travers tous les groupes de rançongiciels connus.

Aucun match trouvé. Après avoir analysé **13,180** enregistrements de victimes de rançongiciels, votre organisation n'apparaît sur aucun site de fuite d'acteurs malveillants connu. C'est un indicateur positif, mais cela ne garantit pas que l'organisation n'a jamais été ciblée — tous les incidents ne sont pas divulgués publiquement.

Paysage de menaces de rançongiciels



PAYS ATTAQUÉS

179

Avec des incidents de rançongiciel enregistrés

LES PLUS CIBLÉS

États-Unis

5 837 attaques enregistrées

SECTEUR PRINCIPAL

Fabrication industrielle

1 744 attaques

Les États-Unis se classent **#1** mondialement pour les attaques de rançongiciels avec **5,837** incidents enregistrés. Le secteur **Industrie Manufacturière** se classe **#20** parmi les industries ciblées avec **158** attaques. En tant que pays parmi les 5 les plus ciblés, les organisations dont le siège est aux États-Unis font face à une exposition de rançongiciels considérablement élevée.

Vulnérabilités exploitées par rançongiciels

L'Agence de cybersécurité et de sécurité des infrastructures des États-Unis (CISA) maintient le catalogue des **Vulnérabilités connues exploitées (KEV)** — une liste soigneusement sélectionnée de vulnérabilités qui ont été activement utilisées dans des attaques réelles. De nombreuses entrées sont explicitement étiquetées comme utilisées dans des campagnes de rançongiciels. Nous croisons chaque CVE détecté sur vos actifs et chaque produit / fournisseur dans votre pile technologique avec le catalogue actuel (1 716 entrées). Lorsqu'une correspondance existe, votre environnement exécute un logiciel avec un chemin d'exploitation connu et armé que les opérateurs de rançongiciels sont documentés pour exploiter.

⚠ 3 correspondances avec le catalogue des vulnérabilités exploitées connues de la CISA.

3 co-occurrences de produits / fournisseurs (votre pile utilise le produit ; l'exposition spécifique à la version doit être vérifiée).

Produits dans votre pile avec des vulnérabilités répertoriées dans KEV

Ces produits apparaissent dans votre pile technologique détectée et ont une ou plusieurs entrées CISA-KEV. Que votre version déployée spécifique soit exposée dépend du niveau de correctif ; traitez chaque ligne comme « vérifiez votre version ».

FOURNISSEUR / PRODUIT	HÔTES	CVES KEV	TOP CVES	PREUVE	RANÇONGICIEL ?
Microsoft — Exchange	1	1	CVE-2021-42321	POTENTIEL	CONNU · VERSION NON CONFIRMÉE
Microsoft — Microsoft	16	1	CVE-2026-42897	POTENTIEL	INCONNU
Microsoft — Word	2	4	CVE-2006-2492, CVE-2012-2539, CVE-2014-1761 …	POTENTIEL	INCONNU

Annexe — Autres domaines découverts (non scannés)

Ce scan a été configuré en mode **DOMAIN ONLY**, donc seul le cible soumise **acmesample.com** a été évaluée. Lors de la reconnaissance, nous avons observé le 1 domaine enregistré supplémentaire ci-dessous — co-hébergé sur la même infrastructure, partageant des serveurs de noms, ou révélé via WHOIS inversé. Ils n'ont **pas été scannés**. Pour les inclure, relancez le scan avec un mode de domaine plus large.

DOMAINE	HÔTES VUS	MÉTHODOLOGIE DE DÉCOUVERTE
192.0.2.68	**1**	Énumération de sous-domaines

Annexe A — Inventaire complet des actifs

54 hôtes triés par score de risque (200 premiers affichés). Les données complètes pour tous les hôtes sont disponibles dans `jeu de donnees de preuves prive` omises de cet échantillon public.

FQDN	IP	RISQUE	PORTS	SOURCE	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	subdomaincenter	51
www.acmesample.com	192.0.2.11	5	443	crt	13
asset-188.acmesample.com	192.0.2.27	5	80, 443	subdomaincenter	51
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	—	subdomaincenter	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	—	subdomaincenter	0

FQDN	IP	RISQUE	PORTS	SOURCE	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	—	subdomaincenter	0
asset-186.acmesample.com	–	1	—	subdomaincenter	0
asset-190.acmesample.com	–	1	—	subdomaincenter	0
asset-192.acmesample.com	–	1	—	subdomaincenter	0
asset-193.acmesample.com	–	1	—	subdomaincenter	0
asset-194.acmesample.com	–	1	—	subdomaincenter	0
asset-195.acmesample.com	–	1	—	subdomaincenter	0
asset-048.acmesample.com	–	0	—	subdomaincenter	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	—	subdomaincenter	0
asset-056.acmesample.com	–	0	—	crt	0
asset-057.acmesample.com	–	0	—	crt	0
asset-063.acmesample.com	–	0	—	subdomaincenter	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	RISQUE	PORTS	SOURCE	CVE
asset-174.acmesample.com	192.0.2.61	0	—	dns_bruteforce	0
asset-180.acmesample.com	–	0	—	subdomaincenter	0
asset-181.acmesample.com	–	0	—	crt	0
asset-182.acmesample.com	–	0	—	subdomaincenter	0
asset-184.acmesample.com	–	0	—	subdomaincenter	0
asset-185.acmesample.com	–	0	—	subdomaincenter	0
asset-187.acmesample.com	–	0	—	subdomaincenter	0
asset-189.acmesample.com	–	0	—	subdomaincenter	0
www.remote.acmesample.com	–	0	—	crt	0

Tous les 39 contrôles DNS sont disponibles dans `jeu de donnees de preuves prive` omis de cet échantillon public.

Annexe B — Liste complète des vulnérabilités

Tous les 105 CVEs uniques et 399 constatations de vérification. Les adresses IP associées à chaque CVE sont listées ci-dessous (tronquées lorsque plusieurs adresses sont concernées) et en entier dans `jeu de donnees de preuves prive` et `jeu de donnees de preuves prive` omis de cet échantillon public.

Tous les CVEs (105)

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
CVE-2004-0847	9.8	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2006-1364	7.5	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2003-0768	6.8	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2005-1664	6.4	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2005-1665	5.0	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2005-2224	5.0	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2005-0452	4.3	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2010-2084	4.3	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2010-2088	4.3	CVEDB	4	192.0.2.27, 192.0.2.45 (+1)	produit correspondant non vérifié
CVE-2015-3105	10.0	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2014-0515	10.0	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2010-0425	10.0	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2015-0359	10.0	CVEDB	3	192.0.2.27, 192.0.2.75	

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
					produit correspondant non vérifié
CVE-2009-3555	9.8	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2024-4577	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2022-47986	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2015-3113	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2014-0497	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2015-5119	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2015-0313	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2015-5122	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2013-0625	9.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2025-34028	9.3	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2014-0569	9.3	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2011-0611	8.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2025-8088	8.4	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2024-0212	8.1	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2019-0232	8.1	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2017-12615	8.1	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2012-0754	8.1	CVEDB	3	192.0.2.27, 192.0.2.75	

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
					produit correspondant non vérifié
CVE-2021-34833	7.8	CVEDB	3	192.0.2.27, 192.0.2.75	produit correspondant non vérifié
CVE-2021-23017	7.7	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2023-44487	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2013-2028	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2016-0742	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2019-9513	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2009-2629	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2013-4547	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2017-7529	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2019-9511	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2019-9516	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2016-4450	7.5	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2009-4487	6.8	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2013-2070	5.8	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2018-16843	5.3	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2019-20372	5.3	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2018-16844	5.3	CVEDB	3	192.0.2.178, 192.0.2.179	

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
					produit correspondant non vérifié
CVE-2010-2263	5.0	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2010-2266	5.0	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2009-3898	4.9	CVEDB	3	192.0.2.178, 192.0.2.179	produit correspondant non vérifié
CVE-2010-3972	10.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2007-2815	10.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2017-7269	9.8	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2005-4360	7.8	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2009-1122	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2009-1535	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2002-0079	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2002-0148	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2000-0884	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2000-0886	7.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2001-0506	7.2	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2006-0026	6.5	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2010-3332	6.4	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2003-0718	5.0	CVEDB	2	192.0.2.27	

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
					produit correspondant non vérifié
CVE-2000-0778	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2009-2521	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2000-0246	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2001-1243	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2000-0630	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2001-0151	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2002-1744	5.0	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2000-0649	2.6	CVEDB	2	192.0.2.27	produit correspondant non vérifié
CVE-2021-34473	9.1	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-26855	9.1	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2020-17132	9.1	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-34523	9.0	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2020-0688	8.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2022-41040	8.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-42321	8.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-28482	8.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2023-21707	8.8	CVEDB	1	192.0.2.75	

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE
					produit correspondant non vérifié
CVE-2023-32031	8.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2022-41082	8.0	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2023-36035	8.0	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2023-36745	8.0	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-27065	7.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-26857	7.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-26858	7.8	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2006-0027	7.5	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-33766	7.3	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-31207	6.6	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2021-41349	6.5	CVEDB	1	192.0.2.75	produit correspondant non vérifié
CVE-2026-6722	9.5	Shodan	2	192.0.2.11	intelligence passive
CVE-2026-17543	8.1	Shodan	2	192.0.2.11	intelligence passive
CVE-2013-2220	7.5	Shodan	2	192.0.2.11	intelligence passive
CVE-2025-14179	7.4	Shodan	2	192.0.2.11	intelligence passive
CVE-2026-6735	7.3	Shodan	2	192.0.2.11	intelligence passive
CVE-2026-7258	6.3	Shodan	2	192.0.2.11	intelligence passive
CVE-2026-7261	6.3	Shodan	2	192.0.2.11	intelligence passive
CVE-2026-7568	6.3	Shodan	2	192.0.2.11	intelligence passive

CVE	CVSS	SOURCES	HÔTES	IPS	CONFIANCE

… et 5 autres CVE (voir `jeu de donnees de preuves prive` omis de cet échantillon public)

Toutes les constatations Nuclei par modèle

MODÈLE	GRAVITÉ	NOMBRE
Détection de suites de chiffrement faibles	FAIBLE	2
Divulgation de version AspNet - Détecter	INFO	2
Content-Security-Policy "script-src" Wildcard Détecté	INFO	2
Détection de TLS obsolète	INFO	1
En-têtes de sécurité HTTP manquants	INFO	215
Configuration OpenID Keycloak - Détecter	INFO	2
Détection de la version Microsoft IIS	INFO	2
Certificat SSL non correspondant	INFO	5
Cookie SameSite Strict manquant	INFO	27
Intégrité de sous-ressource manquante	INFO	2
Microsoft Exchange Autodiscover - Exposition de domaine local	INFO	1
Détecter le fournisseur OpenID Connect	INFO	2
Protocole POP3 - Détecter	INFO	1
Détection SMTP	INFO	2
Noms DNS SSL	INFO	28
Détecter l'émetteur du certificat SSL	INFO	28
Version TLS - Détecter	INFO	28
Détection WAF	INFO	31
Politique de sécurité du contenu faible - Détecter	INFO	4
Certificat TLS Wildcard	INFO	14

Annexe D — Méthodologie & Définitions

Score de risque (0–10)

SCORE	NIVEAU	DESCRIPTION
0	AUCUN	Aucune IP résolue, aucun port, aucun indicateur
1–3	FAIBLE	IP résolue, ports web standards, noms de sous-domaines sensibles
4–6	MOYEN	Plusieurs ports ouverts, services non standards, points de terminaison de développement
7–8	ÉLEVÉ	De nombreux ports ouverts, services de transfert de fichiers, logiciels connus comme vulnérables
9–10	CRITIQUE	Panneaux d'administration exposés, bases de données non protégées, vulnérabilités critiques

Niveaux d'intelligence CVE

SOURCE	MÉTHODE	CONFI-ANCE
Nmap vulners	Détection de version de service actif + recherche vulners.com	ÉLEVÉ
Shodan / Netlas / ZoomEye	Renseignement passif provenant d'analyses à l'échelle d'Internet	MOYEN
CVEDB	Correspondance du nom du produit via l'API CVEDB gratuite de Shodan	FAIBLE

Phases de Pipeline

PHASE	DESCRIPTION
Analyse de Cible	Résoudre l'adresse IP du domaine cible et rassembler les données d'enregistrement WHOIS.
Découverte de sous-domaines	Découvrez tous les sous-domaines en utilisant 17 sources OSINT : transparence des certificats, moteurs de recherche, bases de données DNS, identifiants divulgués, DNS inversé (PTR) et exploration web.
Cartographie de l'infrastructure	Identifier l'hébergement partagé, les plages IP possédées par la cible et les domaines enregistrés par la même entité. Utilise les API REST RIR (RIPE, ARIN) et l'identification d'entreprise améliorée par GPT.
Intelligence passive	Rassembler les données sur les ports, services, technologies et vulnérabilités à partir de Shodan, ZoomEye, Netlas et CVEDB sans toucher à la cible.
Analyse Active	Confirmer les ports ouverts et identifier les versions exactes des services en utilisant Nmap. Les ports découverts passivement sont vérifiés en premier.
Analysis & Correlation	Analysez les quartiers réseau, comparez les certificats SSL, vérifiez les CVE par rapport aux versions de service et calculez les scores de risque.
Vérification Nuclei	Exécute plus de 4 000 modèles nuclei sélectionnés contre les hôtes découverts pour détecter les panneaux exposés, les erreurs de configuration, les empreintes technologiques et les vérifications CVE sécurisées. Ne se déclenche que lorsque active_vuln_scan=true.
Renseignement sur les menaces	Interrogation automatisée des bases de données de violation, moteurs de recherche de stockage cloud et analyse passive des bannières pour identifier les fuites d'identifiants, les fichiers cloud exposés et les interfaces de gestion.
Achèvement	Finaliser les résultats, dédupliquer les constatations, matérialiser les compteurs d'enrichissement et rendre le rapport complet disponible.

Descriptions des modules

Explication détaillée de chaque module qui a fonctionné pendant cette analyse.

MODULE	DESCRIPTION
admin_panels	Détecte les panneaux d'administration et les interfaces de gestion à partir des données de bannière existantes de Shodan, Netlas et nmap. Plus de 55 signatures, y compris WordPress, Jenkins, Grafana, phpMyAdmin, Fortinet, et plus encore. Aucune requête HTTP supplémentaire.

MODULE	DESCRIPTION
exposition_cloud	Recherche de fichiers exposés dans le stockage cloud public (AWS S3, Azure Blob, GCS) correspondant au nom de l'organisation. Filtre le bruit (images, polices) et classe les fichiers sensibles (configs, bases de données, archives, scripts, clés).
code_exposure	Recherche dans les dépôts et Gists GitHub pour le code source exposé, les secrets, les clés API et les données sensibles mentionnant le domaine cible. Utilise l'API Codewatcher avec correspondance de phrase exacte. Chaque constat est noté de 0 à 10 par GPT pour le risque et analysé contre plus de 150 modèles regex de détection de secrets (règles gitleaks).
exposition_identifiants	Interroge les bases de données de violation et les agrégateurs de journaux de voleurs pour les identifiants de courriel d'entreprise trouvés sur des services externes. Renvoie des enregistrements notés en fonction du risque, dédupliqués avec des mots de passe expurgés.
dns_asm	Évaluation complète de la surface d'attaque DNS : 37 vérifications couvrant la santé de la délégation (présence NS, SOA, délégation lâche, cohérence), l'exposition DNS (transfert de zone AXFR, récursion ouverte, divulgation de version CHAOS), l'authentification par e-mail (SPF, DMARC, DKIM), la santé de la livraison des e-mails (résolution MX, alignement PTR) et la résilience (diversité NS, DNSSEC, CAA, TCP/53, EDNS, IPv6). Teste le domaine apex, chaque NS autoritaire et chaque hôte MX. Produit des évaluations de gravité par constat et des scores de posture à 5 dimensions.
domain_exposure	Découverte de domaine par Reverse-IP via C99 ip2domains pour chaque IP appartenant au client avec des services web (port 80/443), suivie d'une vérification de l'expiration des domaines RDAP pour tous les domaines découverts. Identifie les domaines oubliés, expirés ou sur le point d'expirer qui pourraient être détournés pour du phishing ou de l'imitation de marque. Les résultats sont mis en cache pendant 30 jours par IP pour minimiser l'utilisation de l'API.
email_auth	Évalue la posture de sécurité des emails basée sur DNS : analyse des enregistrements SPF (présence, syntaxe, force de la politique, débordement d'inclusion, exposition tierce, risque de joker), évaluation de la politique DMARC (présence, niveau d'application, pourcentage, alignement, rapport), découverte de sélecteurs DKIM avec analyse de la force des clés (40 sélecteurs courants), et validation des enregistrements MX (résolution, détection d'IP privée, identification du fournisseur). Vérifie également la présence de BIMI, MTA-STS et TLS-RPT. Score : basé sur 100 avec des déductions de pénalité et des garde-fous pour les erreurs de configuration critiques.
email_enumeration	Découvre les emails des employés via des bases de données de violations (API centrale) et des sources publiques sur

MODULE	DESCRIPTION
	Internet (Hunter.io). Fusionne les deux ensembles de données et évalue chaque email selon trois dimensions de risque : exposition à la violation, risque de séniorité/position et visibilité publique.
enrichment_dns_resolve	Résout chaque sous-domaine découvert à son adresse IPv4 via une recherche d'enregistrement DNS A. Les sous-domaines sans IP sont marqués comme non résolvables (probablement désaffectés ou uniquement internes).
enrichment_mx_record	Découvre les enregistrements de mail exchange (MX) pour chaque domaine, révélant l'infrastructure email y compris les fournisseurs de cloud (Google Workspace, Microsoft 365) et les serveurs de mail auto-hébergés.
enrichment_netlas	Interroge Netlas pour chaque IP et domaine d'hôte afin d'identifier les technologies logicielles, les frameworks, les détails du serveur web et les ports ouverts. Effectue 2 appels API par hôte (info IP + info domaine). Résultats mis en cache pendant 7 jours.
découverte_réseau_enrichissement	Analyse les IP voisines dans le même sous-réseau /24. Pour chaque voisin, vérifie les certificats SSL (correspondance CN/SAN, correspondance de l'émetteur), les enregistrements PTR, la comparaison ASN, le fingerprinting de contenu HTTP et la colocation de sous-réseau /24. Attribue des scores de confiance (ÉLEVÉ/MOYEN/FAIBLE) en fonction du nombre et de la force des signaux correspondants.
enrichment_nmap	Analyse de port TCP active avec ciblage intelligent. Lorsque des sources passives (Shodan/Netlas/ZoomEye) ont identifié des ports, nmap effectue une détection de version ciblée (-sV) avec des scripts NSE (vulners pour la recherche de CVE, ssl-enum-ciphers pour l'audit TLS). Lorsque aucun port n'est connu, exécute un scan rapide (-F, 100 premiers ports). L'analyse UDP est désactivée (nécessite les droits root). Les résultats incluent le nom du service, le produit, la version et la sortie du script par port.
enrichissement_shodan	Interroge Shodan pour chaque IP hôte afin d'obtenir des ports ouverts, des bannières de service, des détails sur les certificats SSL, des identifiants CPE, la détection du système d'exploitation et des informations sur l'organisation. Résultats mis en cache pendant 7 jours par IP.
enrichment_whois	Récupère les données d'enregistrement WHOIS pour chaque sous-domaine découvert, y compris le registraire, les dates de création/expiration et les détails du titulaire.
enrichment_zoomeye	Interroge ZoomEye pour obtenir les chaînes de certificats SSL, les empreintes des appareils, les informations sur les ports et les références de vulnérabilité pour chaque IP hôte. Résultats mis en cache pendant 7 jours.

MODULE	DESCRIPTION
entity_intelligence	Utilise GPT avec recherche web pour identifier l'organisation derrière le domaine, classer son type, sa taille, son secteur et ses pays d'exploitation, puis évaluer la pression de ciblage cybernétique basée sur le secteur et la géographie. Récupère également les données actuelles sur le paysage des menaces de rançongiciels.
people_intelligence	Identifie des cibles de grande valeur (C-suite, VPs, Directeurs) via RocketReach et enrichit les données de l'entreprise (réseaux sociaux officiels, stack technologique) via Hunter.io. Produit des profils d'employés avec des coordonnées, un historique de carrière et des liens sociaux pour le contexte de la surface d'attaque.
phishing_exposure	Recherche dans les bases de données d'intelligence de phishing (PhishTank, OpenPhish) via l'API centrale pour des campagnes de phishing connues ciblant le nom de marque de l'organisation. Identifie les URL de phishing actives et historiques usurpant la cible.
exposition_violation_serveur	Recherche dans la base de données des violations Kaduu pour tous les FQDN découverts afin d'identifier les serveurs mentionnés dans les fuites d'identifiants, les journaux de voleurs et les violations de données. Les résultats sont attribués par hôte avec classification par type de données.
shortener_exposure	Recherches d'URL raccourcies (goo.gl, bit.ly, tinyurl, ow.ly, etc.) qui pointent vers ou font référence au domaine scanné. Détecte les ressources internes de l'entreprise partagées via des raccourcisseurs, des fichiers sensibles (PDF, tableurs) et des domaines suspects d'usurpation de marque.
réseaux_sociaux	Recherche sur YouTube, Twitter/X, Facebook, LinkedIn, Reddit et les plateformes sociales indexées par Google pour l'usurpation de marque, les faux profils et les mentions de phishing liées au domaine scanné.
spoofguard	SpoofGuard génère des milliers de variations de domaine (typosquats, homoglyphes, bit-squatting, échanges de TLD, punycode, proximité de clavier, etc.), effectue des recherches DNS sur tous, vérifie les serveurs web actifs, détecte les pages de phishing via plusieurs moteurs de détection et capture des captures d'écran.
tg_discord_paste	Recherche dans les canaux de hackers Telegram, les serveurs de cybersécurité Discord et les sites de paste (Pastebin, dpaste, ideone, etc.) pour des mentions de la marque ou du domaine cible. Les constatations sont analysées par GPT-4o-mini pour filtrer le bruit et évaluer la pertinence en matière de sécurité. Recherche Google en direct optionnelle sur 76 sites de paste.

MODULE	DESCRIPTION
tls_posture	Synthétise la posture de sécurité TLS/SSL à partir des données nmap ssl-enum-ciphers, des certificats Shodan et des constatations SSL de nuclei. Détecte les certificats expirés/autosignés, les protocoles faibles (TLS 1.0/1.1), les chiffrements faibles (note C-F) et les hôtes HTTP uniquement manquant HTTPS.
vip_intelligence	Énumère les cibles de grande valeur (dirigeants, directeurs, managers) à travers les comptes Google, la récupération de compte Microsoft, la détection de compte Holehe (120+ sites) et les bases de données de violations. Produit des profils de risque alimentés par GPT avec évaluation des vecteurs d'attaque par personne.
vuln_nuclei	Exécute plus de 4 000 modèles de noyaux sélectionnés dynamiquement par type de port ouvert contre les hôtes découverts. Les modèles HTTP (technologies, panneaux exposés, erreurs de configuration, expositions de fichiers sensibles, détection de CVE sécurisés) ciblent les points de terminaison web actifs. Les modèles SSL vérifient la configuration des certificats et des chiffrements. Les modèles DNS testent les problèmes de transfert de zone et de configuration. Les modèles réseau identifient les services non-HTTP (SSH, FTP, SMTP, bases de données). Tous les modèles sont en lecture seule (GET/HEAD uniquement) — aucune exploitation ou injection de charge utile.
web_app_security	Évalue les points de terminaison web accessibles depuis l'extérieur pour des faiblesses de sécurité HTTP en utilisant des requêtes GET sûres, une analyse des redirections, une inspection des en-têtes de réponse, une analyse des Set-Cookie, une évaluation CSP/HSTS et un parsing HTML passif. Plus de 20 vérifications couvrant la sécurité des cookies de session, l'application de HTTPS, les en-têtes de sécurité, l'intégrité des sous-ressources et la protection contre le clickjacking.
ip_range_discovery	Identifie les plages IP possédées par l'organisation cible via les API REST RIR (RIPE, ARIN, APNIC/AFRINIC RDAP). Utilise l'identification de nom d'entreprise améliorée par GPT pour interroger les registres et découvrir les blocs de réseau assignés à la cible.
résoudre_ip	Résout le domaine cible vers son adresse IPv4 principale via une recherche d'enregistrement A DNS. Cette IP devient l'ancre pour la découverte de plages IP et les recherches ARIN/RIPE.
reverse_dns	Effectue des recherches DNS inverses via ViewDNS pour découvrir des domaines et noms d'hôtes supplémentaires associés aux adresses IP de la cible. Révèle les enregistrements PTR et les mappages DNS inverses.

MODULE	DESCRIPTION
reverse_whois	Trouve d'autres domaines enregistrés par la même entité en utilisant des recherches WHOIS inversées (ViewDNS). Ne s'exécute que lorsque le domaine est auto-enregistré (pas protégé par la vie privée ou enregistré par un fournisseur). Découvre des domaines fantômes et des actifs liés à la marque.
same_ip_domains	Découvre d'autres domaines hébergés sur la ou les mêmes adresses IP que la cible en utilisant quatre sources de reverse-IP (C99, RapidDNS, HackerTarget, ViewDNS). Les voisins d'hébergement partagé peuvent exposer des chemins de mouvement latéral.
subdomain_discovery	Découvrez tous les sous-domaines en utilisant 17 sources OSINT : transparence des certificats, moteurs de recherche, bases de données DNS, identifiants divulgués, DNS inversé (PTR) et exploration web.
vuln_verification	Exécute plus de 4 000 modèles de noyaux sélectionnés avec soin contre les hôtes découverts pour détecter les panneaux exposés, les erreurs de configuration, les empreintes technologiques et les vérifications CVE sécurisées. Les modèles sont sélectionnés dynamiquement en fonction des ports ouverts.
whois	Récupère les données d'enregistrement WHOIS/RDAP pour le domaine principal, y compris le registraire, la date de création, la date d'expiration et l'organisation du titulaire.
c99	Interroge la base de données DNS passive complète de C99 pour les sous-domaines connus du domaine cible.
crt	Recherche dans les journaux de transparence des certificats via crt.sh pour tous les certificats SSL/TLS jamais émis aux sous-domaines de la cible. Utilise l'API JSON comme principale, le scraping HTML comme solution de secours pour les grands domaines.
dns_bruteforce	Essaye 5 000 préfixes de sous-domaines courants (www, mail, ftp, vpn, dev, staging, etc.) contre le domaine cible en utilisant 12 résolveurs DNS publics en round-robin. Trouve des sous-domaines non visibles dans aucune source passive.
dnsdumpster	Outil de reconnaissance DNS qui cartographie l'infrastructure de domaine. Retourne les sous-domaines à partir des enregistrements A, MX, NS et TXT découverts grâce à la collecte passive DNS.
hackertarget	Recherche dans la base de données DNS de HackerTarget pour des enregistrements d'hôtes connus (enregistrements A) associés au domaine cible.

MODULE	DESCRIPTION
hackertarget_ptr	Interroge l'API reversedns de HackerTarget pour trouver des enregistrements PTR pointant vers le domaine cible. Découvre des noms d'hôtes internes (passerelles mail, serveurs de staging, collecteurs de logs) qui ne sont visibles que via DNS inversé.
hackertarget_same_ns	Résout les enregistrements NS de la cible, puis interroge l'API findshareddns de HackerTarget pour chaque domaine partageant ces serveurs de noms. Révèle des domaines liés organisationnellement.
kaduuleaks	Extrait les noms d'hôtes des identifiants divulgués dans la base de données de surveillance du darknet de Kaduu. Analyse les lignes de dump d'identifiants (par exemple, user@host:password) pour découvrir des sous-domaines qui apparaissent dans les données de violation.
kaduulogs	Surveille les journaux de transparence des certificats SSL via la plateforme d'intelligence darknet propriétaire de Kaduu. Découvre des sous-domaines à partir de certificats nouvellement émis en temps réel.
netcraft	Interroge la base de données d'enquête Internet de Netcraft via Selenium headless Chrome pour découvrir des sous-domaines à partir de leur archive d'enquête web de 30 ans.
rapiddns	Recherche dans la base de données DNS passive de RapidDNS.io pour les enregistrements DNS historiques et actuels. Pagination à travers les résultats pour trouver tous les sous-domaines connus.
scrapingbee	Utilise le contournement anti-bot de ScrapingBee pour extraire les résultats de recherche Google pour les références de sous-domaines. Exécute 3 pages en parallèle avec une limite de 60 secondes.
serphouse	Extrait les résultats de recherche Google pour les références aux sous-domaines qui apparaissent dans les pages web indexées. Utilise la requête site:{domain} pour trouver des sous-domaines indexés.
shodan	Découvre des sous-domaines à partir des données de scan internet de Shodan. Recherche pour nom d'hôte :{domain} et extrait des noms d'hôtes à partir des certificats SSL, DNS inversé et bannières HTTP.
centre_des_sous-domaines	Service de méta-agrégation qui combine les données de sous-domaines provenant de dizaines de sources sous-jacentes en une seule requête.
waybackengine	Interroge l'API CDX de l'Internet Archive pour toutes les URL historiques correspondant à *.{domain}/*, extrayant des sous-

MODULE	DESCRIPTION
	domaines uniques à partir des pages archivées. HTTPS principal, HTTP de secours.
webcrawl	Exploration du site web cible en utilisant 5 travailleurs HTTP parallèles (BFS, max 200 pages, profondeur 8, horloge de 10 minutes). Extrait des domaines de <a>, <script src>, <link href>, <img src/srcset>, <iframe>, <form action>, <meta refresh>, regex d'URL JavaScript en ligne, et en-têtes HTTP (CSP, Location, CORS, Link).
zoomeye	Moteur de recherche du cyberespace chinois qui indexe les dispositifs et services connectés à Internet. Recherche v2 site="{domain}" (sous-type web) et extrait les noms d'hôte des champs domaine/rdns/nom d'hôte.

DarknetSearch est une plateforme de Surveillance de Surface d'Attaque par Kaduu AG (Suisse). La plateforme utilise 49 modules à travers 8 phases de pipeline pour découvrir, énumérer et analyser l'empreinte numérique externe d'une organisation. Ce rapport a été généré automatiquement à partir des données de scan. Pour des questions concernant ce rapport, contactez support@kaduu.io.

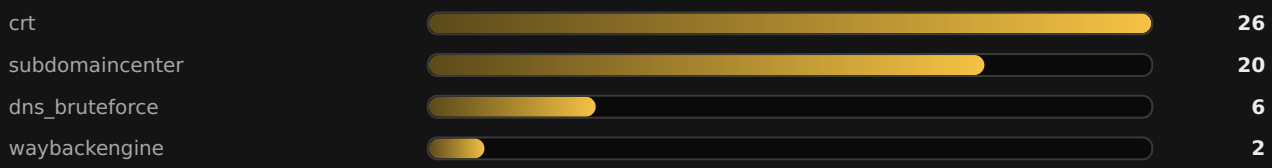
Annexe E — Contribution de la source d'intelligence

Contribution de Source d'Intelligence

Comment chaque source de renseignement a contribué aux trois piliers de la découverte d'actifs : **énumération de noms d'hôtes** (recherche de sous-domaines/hôtes), **detection de ports ouverts** (identification des services), et **renseignement sur les vulnérabilités** (références CVE).

Découverte de nom d'hôte

Hôtes uniques contribuant par chaque module OSINT (avant dé-duplication).



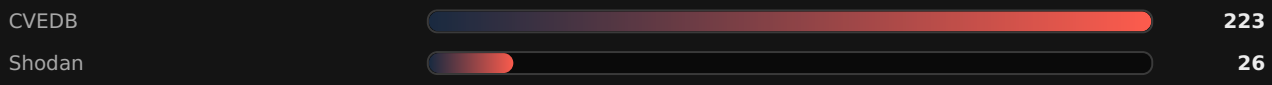
Détection de port ouvert

Hôtes avec des données de port provenant de chaque source.



Intelligence sur les vulnérabilités

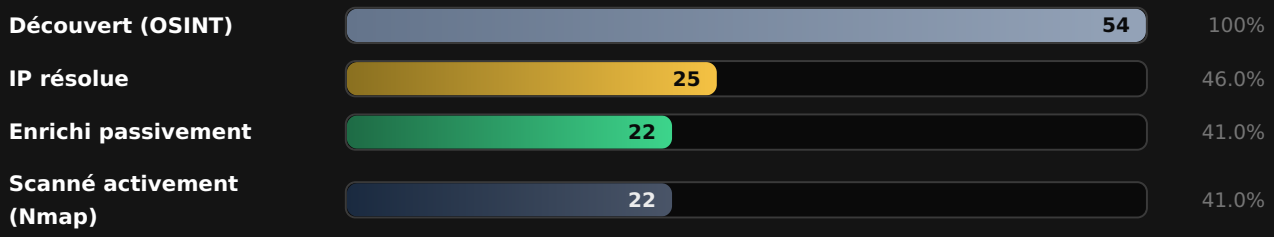
Références CVE par source d'intelligence.



Informations supplémentaires sur les menaces : **Fuite d'identifiants** (bases de données de violations & journaux de voleurs), **Exposition de stockage cloud** (recherche de buckets S3/Azure/GCS), **Exposition d'URL raccourcies** (intelligence goo.gl, bit.ly, tinyurl), **Détection de panneau d'administration** (analyse passive des bannières), **Posture TLS/SSL** (analyse des certificats & des chiffrements), **Exposition de domaine & risque d'expiration** (découverte reverse-IP + surveillance d'expiration RDAP), **Analyse de l'exposition de code** (détection de secrets & de code source GitHub/Gist via Codewatcher).

Entonnoir d'enrichissement

Le scan fonctionne en étapes comme un entonnoir. Tout d'abord, nous collectons autant de noms de domaine que possible à partir de sources OSINT passives (journaux de certificats, moteurs de recherche, bases de données DNS). Ensuite, nous vérifions lesquels de ces domaines se résolvent réellement en une adresse IP — beaucoup peuvent être historiques ou inactifs. Pour chaque hôte avec une IP confirmée, nous effectuons ensuite un enrichissement : interrogeant Shodan, Netlas et ZoomEye pour des données de port/service, effectuant des recherches WHOIS, vérifiant les enregistrements MX, et optionnellement exécutant des scans Nmap actifs. Chaque étape filtre naturellement, c'est pourquoi la barre se rétrécit à chaque étape.



Non résolu : 29 hôtes (aucun enregistrement DNS A dans la fenêtre de scan).