Threat Intelligence Report

acme-corp.net

Created At: December 01, 2024 at 10:00 AM
Updated At: January 15, 2025 at 04:45 PM

Report Metadata

Version: 1.3.0
Generated By: Automated Scanner
Generated At: January 15, 2025 at 04:30 PM

Executive Summary

Overview: This intelligence report summarizes digital exposure discovered during reconnaissance of acme-corp.net.

Scope: acme-corp.net

Subdomains

12

Exposed Assets

4

Leaked Credentials

3

Methodology

Discovery

Subdomain Enumeration

Status: Completed

Used DNS brute force to identify subdomains.

Leak Detection

Logstealers Search (CRITICAL)

Status: Completed

Cross-referenced log stealer dumps against company emails.

Exposed Assets

Assets Search (CRITICAL)

Status: In Progress

Scanning exposed IPs for open services.

Analysis & Processing

Process Found Files (CRITICAL)

Status: Pending

Parsing public files for metadata leaks.

Domain & DNS Intelligence

Domains

Total Domains Identified: 3

DNS Records

NS Records

Name	IP
ns1.acme-corp.net	192.0.2.1

Legacy DNS servers may not support DNSSEC.

MX Records

Name	IP
mail.acme-corp.net	192.0.2.2

MX server does not enforce SPF.

WHOIS Records

Domain	Registrar	Created	Updated	Expires
acme-corp.net	Namecheap	2020-01-01	2024-01-01	2025-01-01

Contact info is redacted.

Network Infrastructure

AS Number Overview

Total ASNs Identified: 2

Shared Hosting Exposure

Domain	Shared With
vpn.acme-corp.net	• blog.hacktivist.net • torrent.safe.zone • (truncated)

VPN endpoint shares hosting with suspicious domains.

Subdomain Enumeration

This section highlights a sample of the subdomains identified during the reconnaissance process. The full list — along with associated technologies, open ports, and vulnerabilities — is available in the Oktoboot dashboard for deeper investigation and remediation.

Total Unique Subdomains Found: 7

Root Domain	Subdomain
acme-corp.net	api.acme-corp.net
	admin.acme-corp.net
	dev1.acme-corp.net
	internal.acme-corp.net
	login.acme-corp.net
	test-db.acme-corp.net
	backup1.acme-corp.net

High-risk subdomains include admin, login, and internal nodes.

Certificate HTTPS Enumeration

This section summarizes digital certificates discovered during reconnaissance. Certificates may reveal subdomains or exposure timelines. Review carefully — and check Oktoboot Dashboard for full details.

Common Name	Valid From	Valid To
api.acme-corp.net	2024-01-01	2025-01-01 (expired)
admin.acme-corp.net	2022-01-01	2023-01-01 (expired)

Exposed Assets Overview

These exposed assets may pose risk due to open ports, outdated services, or certificate leaks. Risk levels and recommendations are based on observed configurations and known vulnerabilities.

203.0.113.45

Domain: vpn.acme-corp.net | **ISP:** Cloudflare | **Risk:** High

Open Ports

Port	Module	Version	SSL
443	nginx	1.20.1	**vpn.acme-corp.net** Let's Encrypt | TLS 1.2

Top Vulnerabilities

OpenSSH < 8.0 RCE

Critical severity – CVSS: 9.8

Allows unauthenticated remote code execution.

Recommended Mitigation

Upgrade OpenSSH and restrict access to known IPs.

Only high-risk assets are shown in this summary.

Data Leaks & Credential Exposure

These exposed credentials were found across malware logs, public breaches, and combo lists. They may be linked to user accounts or internal access points. Please investigate and rotate impacted credentials immediately. Full dump available in the Oktoboot dashboard.

Logstealer Leaks

URL	Email	Password	Year
vpn.acme-corp.net	ceo@acme-corp.net	hunter2	2023
admin.acme-corp.net	admin@acme-corp.net	qwerty123	2023

Some credentials were reused across services.

Public Breach Leaks

Leak Source	Email	Password	Year
HaveIBeenPwned	user@acme-corp.net	letmein	2019

Combo List Leaks

Domain	Email	Password	Year
acme-corp.net	tech@acme-corp.net	12345678	2022

Employee Enumeration

This section lists publicly accessible employees discovered during reconnaissance. Full role breakdowns and exposure context are available in the Oktoboot dashboard.

Total Identified: 2

Alice Smith

CTO

Bob Jones

Lead Security Analyst

Metadata & Public Files

This section lists publicly accessible files and detected metadata exposures. View complete data in your Oktoboot dashboard.

Discovered Files

File Name	URL
internal-doc.pdf	https://acme-corp.net/files/internal-doc.pdf

Risk Assessment

The following risks were identified during the reconnaissance phase. They are categorized by severity and may require immediate remediation or strategic consideration.

High Risks

- VPN endpoint exposed to internet
- Credentials found in public breach

Medium Risks

- Shared hosting with unknown domains

Informational

- Outdated TLS versions detected

Recommendations

Prioritized guidance based on reconnaissance findings. Grouped by severity for operational clarity.

Critical

> **Area:** Access Control
>
> Disable public access to the admin panel.

Important Recommendations

> **Area:** Encryption
>
> Enforce TLS 1.3 and rotate expired certificates.

Best Practice Recommendations

> **Area:** Subdomain hygiene
>
> Clean up unused subdomains like test-db.

Oktoboot

Your Eyes on the underground world