Oktoboot

Your Eyes on the underground world

Threat Intelligence Report

example.com

Report Metadata

Version: v1.0
Generated By: Ala Kaddechi
Generated At: 2025-04-28 20:11

Executive Summary

Overview: This is a simulated overview of the attack surface.

Subdomains

12

Exposed Assets

8

Leaked Credentials

3

Methodology

Discovery

Subdomain Enumeration Status: complete Discovered subdomains using multiple tools

Leak Detection

Search Leaks (CRITICAL) Status: complete Found 3 leak sources

Domain & DNS Intelligence

Domains

Total Domains Identified: 5

DNS Records

NS Records

NAME	IP
ns1.example.com	192.168.1.1

NS note goes here

MX Records

NAME	IP
mail.example.com	192.168.1.2

MX note goes here

WHOIS Records

DOMAIN	REGISTRAR	CREATED	UPDATED	EXPIRES
example.com	RegistrarX	2020-01-01	2021-01-01	2023-01-01

WHOIS notes...

Network Infrastructure

AS Number Overview

Total ASNs Identified: 2

Shared Hosting Exposure

DOMAIN	SHARED WITH
example.com	• shared1.com • shared2.com

Shared hosting note

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: 12

ROOT DOMAIN	SUBDOMAIN
example.com	dev.example.com
	admin.example.com
	api.staging.example.com

Only showing sample subdomains

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
example.com	2024-01-01	2025-01-01 (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These exposed assets may pose risk due to open ports, outdated services, or certificate leaks.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.

192.168.0.1

Domain: dev.example.com **ISP:** ISP Inc. **Risk:** High

Open Ports

PORT	MODULE	VERSION	SSL
443	nginx	1.18	dev.example.com Let's Encrypt | TLS 1.2

Top Vulnerabilities

CVE-2023-1234

High severity — CVSS: 8.1

Remote code execution

Recommended Mitigation

Update server and rotate credentials.

Only one asset shown as sample.

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
http://malicious.site	john@example.com	123456	2022

Sensitive leaks detected

Public Breach Leaks

LEAK SOURCE	EMAIL	PASSWORD	YEAR
SomeSource	jane@example.com	password	2021

Public leak info

Combo List Leaks

DOMAIN	EMAIL	PASSWORD	YEAR
admin123	example.com	admin@example.com	2020

Combo list leak info

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

Cybersecurity Analyst

Bob Johnson

Pentester

Sample employee data

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
report.pdf	http://example.com/report.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

- Exposed credentials in public breaches

Medium Risks

- Outdated server software

Informational

- Wildcard subdomain detected

Recommendations

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

Critical Recommendations

Area: Credential Security

Rotate exposed passwords immediately.

Important Recommendations

Area: Server Maintenance

Upgrade nginx to latest version.

Best Practice Recommendations

Area: Employee Awareness

Conduct security training quarterly.