Threat Intelligence Report

Domain A, Domain B, Domain C

Created At
April 24, 2025 16:25

Updated At
April 24, 2025 16:25

Report Metadata

Version:	1.0.0
Generated By:	Security Team
Generated At:	April 24, 2025 16:25

Executive Summary

Overview: This report analyzes potential cyber threats targeting key domains within the organization.

Scope: Domain A, Domain B, Domain C

Methodology

Domain & DNS Intelligence

DNS Record Enumeration

Status: Completed

Enumerating DNS records for the domain.

Leak Detection

Logstealers Search CRITICAL

Status: Ongoing

Searching for logstealers related to the target.

Discovery

Subdomain Enumeration

Status: Completed

Scanning for subdomains in the target network.

Domain & DNS Intelligence

Domains

Total Domains Identified: 5

DNS Records

NS Records

Name	IP
ns1.example.com	192.0.2.1
ns2.example.com	192.0.2.2

MX Records

Name	Priority	Target
example.com	10	mail1.example.com
example.com	20	mail2.example.com

WHOIS Information

Domain	Registrar	Created	Updated	Expires
example.com	Some Registrar	2022-01-01	2022-06-15	2023-01-01
example.net	Another Registrar	2022-02-01	2022-07-20	2023-02-01

WHOIS data collected from public registries

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://example.com	user1@example.com	password123	2021
http://example.org	user2@example.com	password456	2020
http://example.net	user3@example.com	password789	2022

These credentials were exposed by malware targeting user data.

Public Breach Leaks

Leak Source	Email	Password	Year
example_breach.com	breachuser@example.com	breachpassword	2019
anotherbreach.com	anotheruser@example.com	anotherpassword	2018

These credentials were leaked through public breach lists.

Combo List Leaks

Domain	Email	Password	Year
comboleak.com	combo_user@example.com	combo_password	2021

Combo list leaks with combined username and password data.