OSINT Report on NAME

Company name
Date

Table of Contents

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Confidentiality Statement

This report is the exclusive property of CyberSudo. It contains sensitive information collected through Open-Source Intelligence (OSINT) methods and is intended solely for the use of authorized personnel. The contents of this report are confidential and must not be disclosed, distributed, or reproduced, in whole or in part, without the explicit written consent of CyberSudo and NAME. Unauthorized access or dissemination of this report is prohibited and may result in legal consequences.

The information provided is for intelligence and investigative purposes only and should not be used for any unlawful activity. By accessing this report, you acknowledge and agree to comply with these confidentiality requirements.

NAME may share this document with auditors who are bound by non-disclosure agreements, solely for the purpose of demonstrating compliance with open-source intelligence investigation requirements.

Disclaimer

This report is based on publicly available open-source information in the public domain as of 29.12.2025 and is provided for informational purposes only. While every effort has been made to ensure accuracy, the information is subject to change. CyberSudo makes no warranties regarding the completeness or reliability of the data.

An OSINT investigation is a snapshot in time. The findings and recommendations are based on the information gathered during the assessment and do not account for any changes or updates made after that period.

This report is not intended to offer legal or professional advice. CyberSudo assumes no liability for any actions taken based on its contents. The report is for internal use only and may not be shared or distributed without proper authorization.

Contact Information

Name	Title	Contact Information
Investigator's name	OSINT investigator	email

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Assessment Overview

Between DATE, and DATE, our OSINT Investigator conducted an Open-Source Intelligence (OSINT) assessment. The findings in this report are based solely on publicly available data, with no unauthorized access to private or confidential information. An OSINT (Open-Source Intelligence) risk assessment is an evaluation of publicly available information to identify potential security risks and exposure of sensitive data. It replicates the methods a threat actor might use to gather intelligence from publicly available sources about an individual, organization, or system.

This OSINT investigation offers a realistic view of the information landscape through the lens of a threat actor, helping organizations and individuals to take proactive measures to enhance their security and resilience.

Open-source intelligence or (OSINT) is the legal collection of free publicly available information on individuals, organizations or websites.

Phases of an OSINT investigation include the following:

- **Planning:** Setting clear objectives, defining the scope, and identifying resources and targets for the intelligence gathering process.
- **Data Collection:** Gathering publicly available information from various sources, such as websites, social media, and public databases.
- **Processing**: Organizing and filtering collected data to make it more manageable and ready for analysis by removing irrelevant information.
- **Analysis**: Interpreting and correlating data to identify patterns, relationships, or insights that address the investigation's goals.
- **Reporting**: Compiling the analyzed information into a clear, actionable report and delivering it to the client.

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Scope

As requested, the OSINT investigation was only carried out on the following targets

Assessment	Target
Investigation's type	NAME

Provided Information

NAME had provided CyberSudo with the following information to start with:

Name: NAME
Emails: johnsmith@gmail.com
Phone Numbers: +1 123 456 7980

Executive Summary

NAME engaged CyberSudo to conduct an open-source intelligence (OSINT) investigation against NAME. The main goal of the investigation was to find publicly available information about NAME.

This report details the scope of the engagement, detailed information about all of the findings. The summary below is intended for non-technical audiences to give an idea of the overall results of the engagement and the key findings. The second section of this report is intended for a technical audience as it lists all of our findings in detail, along with reproduction steps, analysis and recommendations.

Investigation Summary

A comprehensive OSINT investigation across both the clear and dark web identified additional phone numbers previously or currently associated with John. Furthermore, CyberSudo discovered indications that John had attempted to suppress certain search results from public search engines.

Additional research revealed multiple addresses linked to John, as well as the websites where his email address and phone numbers are registered. A hashed password associated with John was also located in a leaked/breached database; no cracking attempts were performed, as this was outside the scope of the investigation.

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Key Findings

Name: NAME

Other Names: Jimmy Smith

DOB: 01.01.1970

Phone Numbers: +1 212-385-2066, +1 917-409-5946

Emails: johnsmith@gmail.com, jimmysmith@gmail.com

Founder of: McDonald's LLC

Works at: McDonald’s

Addresses:
1528 Broadway Times Square, New York, NY 10036, United States
1195 S Colorado Blvd and 5085 N Federal Blvd in Denver

Breached/Leaked Databases:
EatStreet, Jefit, Ledger, Luxottica, MGM Hotels, Parkmobile, Facebook, Acuity.

Password Hashes:
7c6a180b36896a0a8c02787eeafb0e4c
e38ad214943daad1d64c102faec29de4afe9da3d

Plaintext Passwords:
password1

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Discovering Sensitive Personal Data – Data Leak/Breach Lookup

Email Search

Searching for the email address johnsmith@gmail.com across leaked and breached databases indicates that the owner has likely attempted to remove or suppress its appearance from widely used breach-monitoring platforms such as Have I Been Pwned and DeHashed. Despite this, alternative search engines and data sources revealed that the email address appears in the following data leaks and breach incidents:

- **Ledger** — Hardware Wallet
- **Luxottica** — Eyewear Manufacturer
- **Jefit** — Fitness App
- **MGM Hotel** — Hotel Resort

The following lists all sensitive information discovered within each extracted database:

Jefit

- Username: JimmSmith
- IP: 195.50.95.12
- Secret token: 3723260b940aa19a0ccb9eb663e5bd9byjtg`LZVV/?65loUUyT9>N11ASDkS`7

Ledger

- Name: John Smtih
- Phone Number: 917-409-5946
- Address: 1528 Broadway Times Square, New York, NY 10036, United States

Luxottica

- Name: NAME
- Phone Number: +1 917-409-5946
- City: New York City, New York

MGM Hotels

- Name: NAME
- Phone Number: +1 917-409-5946
- Address: 1195 S Colorado Blvd and 5085 N Federal Blvd in Denver

BUSINESS CONFIDENTIAL
Copyright © CyberSudo

Phone Search

Searching for the phone number 917-409-5946 in leaked/breached databases led to finding that the phone is in the following data leaks/breaches:

- **ParkMobile**— Parking App
- **US Voter** — +150 million US voter records by
- **Unknown Consumer DB** — 240+ Million US records
- **Facebook** — +533 million Records

The following lists all sensitive information discovered within each extracted database:

Parkmobile

- Phone number: +1 917-409-5946
- Password hash: e38ad214943daad1d64c102faec29de4afe9da3d
- License plates: 011ABC and ABD4569

Facebook

- Name: NAME
- City: New York
- Phone number: +1 917-409-5946
- Profile ID: 100065365758241
- *Note: The Facebook profile has been deleted*

USA 250 million personally identifiable information

- Name: NAME
- Address: 1195 S Colorado Blvd and 5085 N Federal Blvd in Denver

Acuity

- Name: NAME
- Address: 1195 S Colorado Blvd and 5085 N Federal Blvd in Denver

Name Search

A search for the name "*NAME*" across leaked and breached databases resulted in the identification of a single record with an exact name match in the **"US Voters"** database.

Name: NAME
DOB: 01.01.1970
Address: 1528 Broadway Times Square, New York, NY 10036, United States

A search for the name **"***NAME***"** across leaked and breached databases resulted in the identification of a record with an exact name match in the following databases:

- **EatStreet** — Delivery Platform
- **Bureau van Dijk** — Business Intelligence

BUSINESS CONFIDENTIAL
Copyright © CyberSudo