

OPEN SOURCE INTELLIGENCE (OSINT)

# See What Is Already Visible About Your Organisation

Get a free view of the information linked to your organisation across external sources



## GET YOUR FREE OSINT PROFILE CHECK



### See the scale

Understand how much information is out there.



### Spot what matters

Identify credentials, stealer logs, exposed systems and sensitive information.



### Understand the risk

See what may need attention.



### Know what to do next

Identify where further investigation may be worthwhile.



## A clearer view of your digital footprint

*See what's publicly visible, what matters and where action may be needed.*

See what your OSINT profile **could look like**

View an anonymised example overleaf



# Company A

companya.co.uk | Insurance | ~200 employees

## DARK WEB RATING

**LOW**

Limited dark web signal in the initial scan

## ATTACK SURFACE RATING

**LOW**

Limited attack surface signal in the initial scan

**343**

TOTAL RECORDS

**37**

PAST 12 MONTHS

**13**

PAST MONTH

**0**

RECORDS LINKED  
TO STEALER LOGS

**0**

@DOMAIN STEALER  
LOG RECORDS

**7**

ATTACK SURFACE  
RECORDS

**0**

RECORDS LABELLED  
HIGH RISK

### Overview

Company A has a **Low** dark web rating and a **Low** attack surface rating based on this initial scan. The key question is whether the organisation has visibility of this data and a process to determine what is relevant.

### Dark web database records

A search for the organisation's domain returned **343** records, with **37** added in the past 12 months and **13** in the past month. Some of this may be background noise, but without analysis it is not possible to confirm which records may relate to employees, systems, customers, suppliers, or sensitive services.

### Stealer log interpretation

No full stealer log records were identified in this initial view. However not all dark web records will be correctly categorised, and credential exposure could still be apparent in a data set.

### Attack surface interpretation

The passive attack surface scan identified **7** externally visible records, with no higher-risk findings flagged in this initial scan. These records represent infrastructure that would be visible to attackers during reconnaissance.

### What this means

This profile should not be read as confirmation of compromise. External datasets often contain a mixture of background noise, customer activity, third-party exposure, historic records, and potentially relevant organisational data. The value of OSINT analysis is determining which elements matter.

### Recommended next steps

Even if an immediate risk is not illustrated by this data, you should consider a need to understand what external data exists or whether it is reviewed regularly. There are also **other approaches for ongoing OSINT activity** beyond dark web and attack surface, such as public web data, social media, PII and code exposure.

### Questions for consideration

- Do you feel confident you understand the external visibility of your organisation?
- Do you have access to dark web or external intelligence sources?
- How do you currently determine whether externally available data is relevant to your organisation?

# Company B

companyb.com | Higher Education | ~5000 employees

## DARK WEB RATING

**HIGH**

7 @domain stealer record(s) identified

## ATTACK SURFACE RATING

**HIGH**

5 high-risk attack surface finding(s) identified

**701,353**

TOTAL RECORDS

at least **10,000**  
PAST 12 MONTHS

at least **10,000**  
PAST MONTH

**520**

RECORDS LINKED  
TO STEALER LOGS

**7**

@DOMAIN STEALER  
LOG RECORDS

**115**

ATTACK SURFACE  
RECORDS

**5**

RECORDS LABELLED  
HIGH RISK

### Key indicator: Possible corporate credential exposure due to malware

7 stealer-log record(s) contain the organisation's email domain. This is one of the strongest indicators in this initial profile and should be treated as a priority conversation point.

## Overview

Company B has a High dark web rating and a High attack surface rating based on this initial scan. The key question is whether the organisation has visibility of this data and a process to determine what is relevant.

## Dark web database records

A search for the organisation's domain returned 701,353 records, with at least 10,000 added in the past 12 months and at least 10,000 in the past month. Some of this may be background noise, but without analysis it is not possible to confirm which records may relate to employees, systems, customers, suppliers, or sensitive services.

## Stealer log interpretation

520 full stealer log records were identified. Importantly, **7 record(s) contained @companyb.com**. This is a strong indicator that some records may relate to corporate accounts or users. This does not confirm compromise, but it is a clear signal that deeper analysis would be valuable.

## Attack surface interpretation

The passive attack surface scan identified **115** externally visible records, including **5 higher-risk finding(s)**. This does not confirm vulnerability, but it is recommended that assets should be reviewed to confirm whether they are relevant, maintained, and appropriately risk assessed.

## What this means

This profile should not be read as confirmation of compromise. External datasets often contain a mixture of background noise, customer activity, third-party exposure, historic records, and potentially relevant organisational data. The value of OSINT analysis is determining which elements matter.

## Recommended next steps

The focus area should be the presence of 7 @domain stealer record(s). Do you have visibility of exposed credentials and stealer-log data?

## Questions for consideration

- Do you feel confident you understand the external visibility of your organisation?
- Do you have access to dark web or external intelligence sources?
- How do you currently determine whether externally available data is relevant to your organisation?

# Company C

companyc.org | Financial Services | ~88 employees

## DARK WEB RATING

**LOW**

Limited dark web signal in the initial scan

## ATTACK SURFACE RATING

**HIGH**

4 high-risk attack surface finding(s) identified

**8,387**

TOTAL RECORDS

**4,340**

PAST 12 MONTHS

**847**

PAST MONTH

**22**RECORDS LINKED  
TO STEALER LOGS**0**@DOMAIN STEALER  
LOG RECORDS**72**ATTACK SURFACE  
RECORDS**4**RECORDS LABELLED  
HIGH RISK

### Overview

Company C has a **Low** dark web rating and a **High** attack surface rating based on this initial scan. The key question is whether the organisation has visibility of this data and a process to determine what is relevant.

### Dark web database records

A search for the organisation's domain returned **8,387** records, with **4,340** added in the past 12 months and **847** in the past month. Some of this may be background noise, but without analysis it is not possible to confirm which records may relate to employees, systems, customers, suppliers, or sensitive services.

### Stealer log interpretation

**22** full stealer log records were identified. No records were immediately attributable through simple **@domain** filtering, but this does not rule out relevance. Stealer logs often require deeper analysis to determine whether records relate to employees, customers, suppliers, portals, third-party services, or corporate systems.

### Attack surface interpretation

The passive attack surface scan identified **72** externally visible records, including **4 higher-risk finding(s)**. This does not confirm vulnerability, but it is recommended that assets should be reviewed to confirm whether they are relevant, maintained, and appropriately risk assessed.

### What this means

This profile should not be read as confirmation of compromise. External datasets often contain a mixture of background noise, customer activity, third-party exposure, historic records, and potentially relevant organisational data. The value of OSINT analysis is determining which elements matter.

### Recommended next steps

The key focus should be **attack surface visibility**. High-risk attack surface findings provide a clear reason to consider external reconnaissance and whether exposed assets are monitored and reviewed.

### Questions for consideration

- Do you feel confident you understand the external visibility of your organisation?
- Do you have access to dark web or external intelligence sources?
- How do you currently determine whether externally available data is relevant to your organisation?

# Company D

companyd.org.uk | Consumer Services | ~5000 employees

## DARK WEB RATING

**MEDIUM**

14,960 total raw records identified

## ATTACK SURFACE RATING

**HIGH**

3 high-risk attack surface finding(s) identified

**14,960**

TOTAL RECORDS

**7,517**

PAST 12 MONTHS

**1,229**

PAST MONTH

**42**RECORDS LINKED  
TO STEALER LOGS**0**@DOMAIN STEALER  
LOG RECORDS**96**ATTACK SURFACE  
RECORDS**3**RECORDS LABELLED  
HIGH RISK

### Overview

Company D has a **Medium** dark web rating and a **High** attack surface rating based on this initial scan. The key question is whether the organisation has visibility of this data and a process to determine what is relevant.

### Dark web database records

A search for the organisation's domain returned **14,960** records, with **7,517** added in the past 12 months and **1,229** in the past month. Some of this may be background noise, but without analysis it is not possible to confirm which records may relate to employees, systems, customers, suppliers, or sensitive services.

### Stealer log interpretation

**42** full stealer log records were identified. No records were immediately attributable through simple **@domain filtering**, but this does not rule out relevance. Stealer logs often require deeper analysis to determine whether records relate to employees, customers, suppliers, portals, third-party services, or corporate systems.

### Attack surface interpretation

The passive attack surface scan identified **96** externally visible records, including **3 higher-risk finding(s)**. This does not confirm vulnerability, but it is recommended that assets should be reviewed to confirm whether they are relevant, maintained, and appropriately risk assessed.

### What this means

This profile should not be read as confirmation of compromise. External datasets often contain a mixture of background noise, customer activity, third-party exposure, historic records, and potentially relevant organisational data. The value of OSINT analysis is determining which elements matter.

### Recommended next steps

The key focus should be **attack surface visibility**. High-risk attack surface findings provide a clear reason to consider external reconnaissance and whether exposed assets are monitored and reviewed.

### Questions for consideration

- Do you feel confident you understand the external visibility of your organisation?
- Do you have access to dark web or external intelligence sources?
- How do you currently determine whether externally available data is relevant to your organisation?

# Understanding Your OSINT Profile

The value is not finding more data. It is knowing **which findings matter**.

The example profile highlights several types of OSINT findings. Here's what those findings mean and why they could matter to your organisation.

## The question behind every OSINT assessment

What can someone find about your people, credentials, devices and systems, and would you know if any of it created a real risk?

## OSINT in Plain English



Open source intelligence, or OSINT, shows what information about your organisation can be found from the outside.

The aim is simple: find the information that matters, understand the risk and decide what to do next.



Some findings will be old or harmless. Others can reveal stolen credentials, exposed devices, malware-linked data, sensitive documents or information that could make your organisation easier to target.

## What can an OSINT Assessment Uncover?

An OSINT assessment can uncover a range of external information linked to your organisation, people and systems.



**Stealer Logs**



**Exposed Credentials**



**Dark Web Records**



**Attack Surface**



**People and Executive Exposure**



**Sensitive Information, Code & Secrets**

We break down what each of these findings means over the following pages



# What the Main OSINT Findings Actually Mean

A customer-friendly guide to the information we look for and **why it matters in practice**.



## Stealer Logs

A strong indicator that information may have been taken from an infected device.

### WHAT IT MEANS

Data taken by information-stealing malware from an infected device.

### WHAT WE CAN FIND

Corporate email addresses, usernames, passwords, browser data, cookies, session details and other information taken from the device

### WHY IT MATTERS

If a corporate account appears in a stealer log, information linked to an employee may have been stolen. You may need to check whether passwords still work, which device was affected and whether anything else was accessed.

### WHAT IT CAN COST

If a stealer-log finding is ignored, stolen credentials could stay valid and usable by an attacker. That could lead to account takeover, unauthorised access, further compromise and the cost of responding to an incident.



## Exposed Credentials

Authentication information found outside the systems you control.

### WHAT IT MEANS

Usernames, passwords or other login details linked to your organisation that appear in external datasets.

### WHAT WE CAN FIND

Corporate email addresses, passwords, password hashes, reused passwords and other account details.

### WHY IT MATTERS

If the credentials still work, they could give someone access to email, cloud services, applications or other systems. Even old passwords can help an attacker guess how people create new ones.

### WHAT IT CAN COST

The impact could be as small as a password reset, or as serious as unauthorised access, fraud, data loss or a wider security incident.

# What the Main OSINT Findings Actually Mean

A customer-friendly guide to the information we look for and **why it matters in practice**.



## Dark Web Records

External records associated with your organisation, domains or people.

### WHAT IT MEANS

Information linked to your organisation that appears in dark web, breach-related and other external datasets.

### WHAT WE CAN FIND

Employee email addresses, login details, breach records, personal information, historic data and other records linked to your organisation.

### WHY IT MATTERS

A high number of records does not automatically mean high risk. What matters is whether any of the information is current, sensitive or useful to someone targeting you.

### WHAT IT CAN COST

The biggest cost is not knowing what matters. Your team can waste time on old data while a small number of important findings stay hidden in the noise.



## Attack Surface

The systems and technology that can be discovered from the internet.

### WHAT IT MEANS

The systems, services and technologies linked to your organisation that can be seen from the internet.

### WHAT WE CAN FIND

Domains, subdomains, internet-facing systems, open services, software and other technology details, including assets your security team may not know about.

### WHY IT MATTERS

Attackers can use this information to understand where to look. Forgotten or outdated systems matter because they may not be monitored or patched.

### WHAT IT CAN COST

A forgotten internet-facing system can give an attacker another way in. If it is found too late, the result can be urgent fixes, disruption and the cost of responding to an incident.

# What the Main OSINT Findings Actually Mean

A customer-friendly guide to the information we look for and **why it matters in practice**.



## People and Executive Exposure

Information that can make targeting an individual easier and more convincing.

### WHAT IT MEANS

Public information about employees and executives, including their roles, relationships and online activity.

### WHAT WE CAN FIND

Names, job titles, email formats, work history, public profiles, contact details and information about teams or responsibilities.

### WHY IT MATTERS

This information can help an attacker choose who to target and make phishing, impersonation or fraud attempts more believable.

### WHAT IT CAN COST

The result could be successful phishing, fraudulent payments, account compromise or reputational damage, especially for senior leaders and finance teams.



## Sensitive Information, Code and Secrets

Information that may have travelled beyond where the organisation expected it to be.

### WHAT IT MEANS

Files, code or technical information found outside your organisation that may contain internal, confidential or security-sensitive material.

### WHAT WE CAN FIND

Documents, source code, API keys, tokens, configuration details, internal names, technology details and metadata.

### WHY IT MATTERS

One exposed file can reveal far more than expected. It can show how your organisation works, what technology you use, who is involved and, in some cases, information that can be used directly.

### WHAT IT CAN COST

Depending on what is exposed, the impact could include unauthorised access, data loss, fraud, intellectual property loss or regulatory issues.

# What Does This Mean For Your Organisation?

The real value of OSINT is understanding which findings deserve attention.

A large number of records can look worrying, but more data does not always mean more risk. Thousands of old records may matter less than one valid password, one exposed device or one malware-linked finding.

## Finding data is easy. Knowing what matters is harder.

A useful OSINT assessment filters out the noise and highlights the findings that could affect your people, systems or data.

## From Finding to Action

### 1. DISCOVER

#### What is visible?

Find the information visible about your people, devices, infrastructure and wider digital footprint.

### 2. ANALYSE

#### What does it mean?

Check whether the finding is real, current and likely to create a meaningful risk.

### 3. ACT

#### What should happen next?

Fix it, monitor it or accept it based on how serious it is.

## Recommended Next Steps

### ● Investigate significant findings

Start with the findings that could cause real harm, such as stealer-log records, exposed credentials, sensitive information or exposed devices.

### ● Validate what is visible

Check that every internet-facing system and service is known, expected and properly secured.

### ● Separate signal from noise

Filter out old or irrelevant records so your team can focus on the findings that actually matter.

### ● Keep visibility current

Your external footprint changes as people, systems and suppliers change. Make sure new exposure can be spotted after the first assessment.

# The Cost of Not Knowing

Some findings are simply information. Others can be an early warning that something needs attention.

Not every finding needs fixing. Some need no action. Some should be watched. Others may be old or irrelevant. But stolen credentials, exposed devices, malware-linked data or sensitive information should be understood before they are dismissed.

## When a Significant Finding is Left Unexplored

| Finding                  | What Doing Nothing Means                                                             | Potential Consequence                                                                     |
|--------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| A compromised credential | A stolen login may still work.                                                       | Account takeover, unauthorised access, fraud or a wider breach.                           |
| A stealer-log record     | Stolen information may still be usable, and the infected device may still be a risk. | More stolen credentials, account misuse and incident response costs.                      |
| An exposed device        | A public-facing system may stay forgotten, outdated or vulnerable.                   | More time for an attacker to find and exploit it, followed by urgent fixes or disruption. |
| Sensitive information    | Sensitive information may stay available to people outside the organisation.         | Data loss, intellectual property loss, regulatory issues or targeted attacks.             |

### A useful risk question

If this information is already out there, do you know which findings matter and what you would do about them?

### Want to see your own OSINT Profile?



A clearer view of your digital footprint

**GET YOUR FREE OSINT CHECK**



(+44) 121 709 2526



info@omnicybersecurity.com