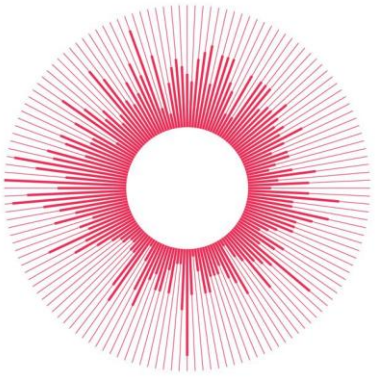

Dark Web Monitoring

PRELIMINARY REPORT OF THE DARK WEB EXPOSURE CHECK

SPAN CYBER THREAT INTELLIGENCE

Span d.d.
Koturaška cesta 47
10000 Zagreb
Tel. +385 1 6690 200
Fax. +385 1 6690 299
OIB: 19680551758
IBAN: OTP banka d.d.
HR4324070001100472815

Datum: <Date>

This report is given for information only.

The results showed serve only as a preliminary assessment of the exposure of your organization or personal data on dark web.

Detailed information (e.g. passwords, hashes), as well as the context and recommendations are available upon the activation of the complete Dark Web Monitoring service.

Search date: 11. November 2025
Total number of reported references: 9

#	identity	Password	Source
1	user12@corp.hr	**********	Stealer Logs
2	user123@corp.hr	**********	Stealer Logs
3	user34@corp.hr	**********	Stealer Logs
4	user345@corp.hr	**********	Stealer Logs
5	user67@corp.hr	**********	Stealer Logs
6	user_29@corp.hr	**********	Stealer Logs
7	user1999@corp.hr	**********	Stealer Logs
8	user19878@corp.hr	**********	Combolist
9	user13@corp.hr	**********	Stealer Logs

For thorough analysis, continuous dark web monitoring and advisory support—our analysts are at your disposal. Get in touch with us at ***info@span.eu***

What is Dark Web Monitoring?

Our Dark Web Monitoring service detects and assesses potential threats from the criminal underground. The service is now available as a one-time risk exposure assessment or a regular, continuous monitoring. It involves searching for any type of references to your company's digital assets on the dark web platforms where stolen data are sold or disclosed. These platforms include forums, illegal marketplaces, web pages where stolen data are disclosed for blackmail, and platforms for anonymous disclosure of documents and data.

All the findings are verified and the level of risk is assessed with clear guidance for taking appropriate steps provided. It enables swift responses such as credential resets, session terminations, and targeted security measures.

How does it work?

- Data collection: We gather potential risk exposure data from curated dark web and clear web sources
- Validation: The authenticity and relevance of each finding is identified
- Priority setting: We analyse risks and rank findings by urgency and potential impact on the business
- Advising: We timely provide you with clear guidance to mitigate adverse effects

User benefits

- Early detection of threats that could affect your organization
- Clear tactical guidance for prompt and effective response
- Accurate and relevant results validated by analysts
- Comprehensive analysis that can extend beyond dark web sources
- Reports intended for security teams and management
- Optional extension to monitor key vendors and partners

What is delivered with continuous Dark Web Monitoring?

- Continuous search for references to your digital assets
- Timely alerts for new, validated findings (most frequently related to credentials)
- Regular reports with current status and recommendations