Demo data

This report was built from a demo project: hosts, findings and data leaks are fictional and do not belong to your infrastructure.

intruforce

// EASM · External Attack Surface Management

Full technical report

// Results of automated external checks by SeguriScan

CLIENT

DEMO · Fintech

DATE

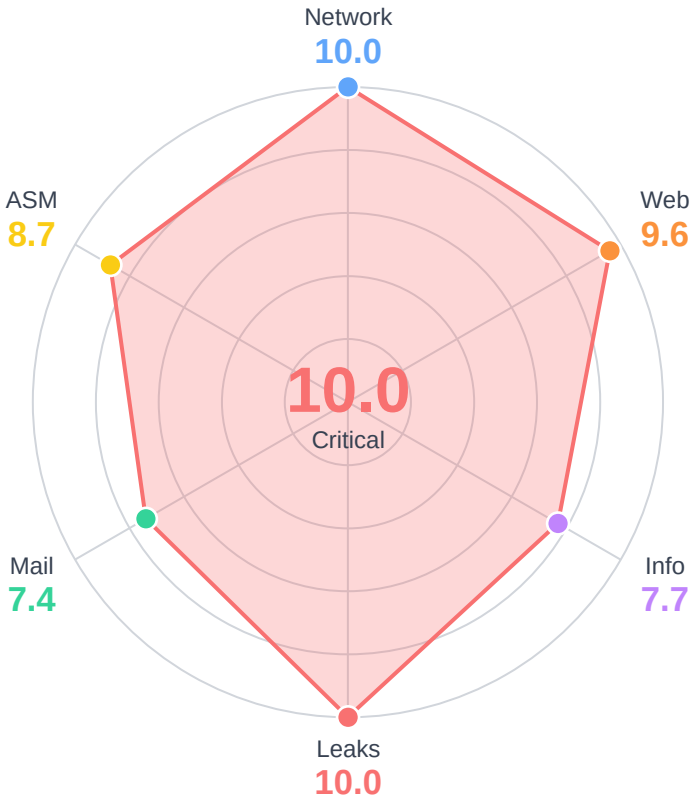
05.11.2026

Cycle period: from 03.11.2026

Threat severity

Critical

10.0 of 10



Cyber threat level: 10.0 / 10 (Critical)

	Category	Risk	Level
●	1. Network security	10.0 / 10	Critical
●	2. Web application security	9.6 / 10	Critical
●	3. Information disclosure	7.7 / 10	High
●	4. Data leaks	10.0 / 10	Critical
●	5. Email and DNS	7.4 / 10	High
●	6. Attack surface management	8.7 / 10	High

Risk scale 0–10 (0 = no threats identified, 10 = critical risk). Levels: "Low" (<4.0), "Moderate" (4.0–6.9), "High" (7.0–8.9), "Critical" (≥9.0). "—" — no data.

1. Most likely attack vectors

Credential brute-forcing against web panels CVSS 5.3

Guessing login/password pairs against web authentication panels that have no lockout or CAPTCHA.
The least likely scenario when strong passwords are used.

- Unauthorized access to web management interfaces and administration panels.

Confirmed by tests:

- [8] Web — resistance of authentication panels to brute force

Identification and authentication failures

Using leaked data, the attacker gains access to the portal and admin panel (Credential Stuffing). Gains access to confidential information. Achieves full access to the vulnerable device by executing PHP code on the server. Utilizes obtained data for further attack development. May encrypt data with ransom intent.

- Unauthorized access to the system, data compromise, ability to encrypt data for ransom.

Confirmed by data:

- Data leaks with passwords — detected: 46

Social engineering and phishing

Obtaining employee email addresses through OSINT or social engineering.
Registering a phishing domain.
Preparing the phishing email.
Sending it out.
Utilizing obtained data for further attack development.

- Compromise of employee credentials, enabling further penetration into the infrastructure.

Confirmed by data:

- Data leaks with email — detected: 52

During the project, the following issues were identified:

Risk	Finding	Asset	Status
Critical	Leaks — Employees: Stealer logs from corporate hosts (with passwords)	mail.example.com	**New**
Critical	Authorization bypass in an internal API method	https://api.example.com:8443	**New**
Critical	Cluster node service accepts anonymous requests	192.0.2.26	**New**
Critical	Key-value store is exposed to the internet without authentication	192.0.2.25	**New**
Critical	SQL injection in the customer account search form	https://lk.example.com	**New**
Critical	Database server accepts an administrator login without a password	192.0.2.25	**New**
Critical	Edge gateway accepts a default account over SSH	198.51.100.11	**New**
Critical	Build server script console is available without login	192.0.2.24	**New**
Critical	Insecure deserialization in the web portal	https://lk.example.com	**New**
Critical	Server-side request forgery in the mail web interface	https://mail.example.com	**New**

Risk	Finding	Asset	Status
Critical	Stealer logs with credentials — 23 records	Project domains	New
High	The name is served by an external node.	portal.example.com 192.0.2.24	New New
High	Similar domains: 12 with high risk	fintech-cards.example fintech-bank.example fintech-pay.example	New
High	Leaks — Customers: Corporate database breach (with passwords)	mail.example.com	New
High	Leaks — Customers: Stealer logs from corporate hosts (with passwords)	mail.example.com	New
High	Leaks — Employees: Corporate database breach (with passwords)	mail.example.com	New
High	Leaks — Employees: Corporate database breach (without passwords)	mail.example.com	New
High	Leaks — Employees: Stealer logs from third-party hosts (password reuse) (with passwords)	mail.example.com	New
High	Monitoring dashboard accepts a weak administrator password	192.0.2.24	New
High	Directory traversal in the application file handler	https:// api.example.com:8443	New
High	Stored script injection in the feedback form	https:// portal.example.com	New
High	A subdomain points to a released provider resource	cdn.example.com	New
High	Version control directory is accessible over HTTP	https:// portal.example.com	New
High	Access to other users' records by identifier substitution in the API	https:// api.example.com:8443	New
High	Gateway management panel is reachable from the internet	198.51.100.11	New
Medium	Leaks — Customers: Stealer logs from third-party hosts (password reuse) (with passwords)	mail.example.com	New
Medium	Leaks — Employees: Third-party database breach (work email in a public breach) (with passwords)	mail.example.com	New
Medium	Leaks — Unclassified subjects: Corporate database breach (with passwords)	mail.example.com	New
Medium	No DMARC policy is set for the domain	mail.example.com	Not Fixed
Medium	API allows requests from any site together with credentials	https:// api.example.com:8443	New
Medium	Email address change bypasses account confirmation	192.0.2.24	Not Fixed
Medium	Security response headers are missing	https:// portal.example.com	New
Medium	Redirect to an arbitrary address through a link parameter	https:// portal.example.com	New
Medium	Session identifier does not change after login	https://lk.example.com	New
Medium	Mail server confirms whether addresses exist	192.0.2.23	New
Medium	User name enumeration through the remote access service	192.0.2.21	Not Fixed
Medium	Test environment returns verbose error messages	http://test.example.com	New
Medium	The login form does not limit the rate of guessing attempts	https://lk.example.com	Not Fixed

**The risk level reflects the likelihood and impact of exploitation: Critical > High > Medium > Low > Info.*

Recommendations

Main recommendations are:

- Change the default passwords, enable a second factor and a progressive delay.

Table of Contents

Table of contents will be built automatically upon opening in Word (right-click → "Update Field").

2. General information

2.1. Infrastructure information

Using information from open sources and specialized utilities, the specialists conducted a collection of information about IP addresses, domains, and subdomains belonging to the Customer.

List of assets to check:

Domains:

api.example.com
app1.example.com
app2.example.com
app3.example.com
docs1.example.com
docs2.example.com
events1.example.com
events2.example.com
events3.example.com
help1.example.com
help2.example.com
lk.example.com
mail.example.com
media1.example.com
media2.example.com
partners1.example.com
partners2.example.com
partners3.example.com
portal.example.com
reports1.example.com
reports2.example.com
reports3.example.com
reports4.example.com
static1.example.com
static2.example.com
status1.example.com
status2.example.com
vpn.example.com
wiki1.example.com
wiki2.example.com
wiki3.example.com

History of changes

No changes detected compared to the previous check.

3. Performed checks

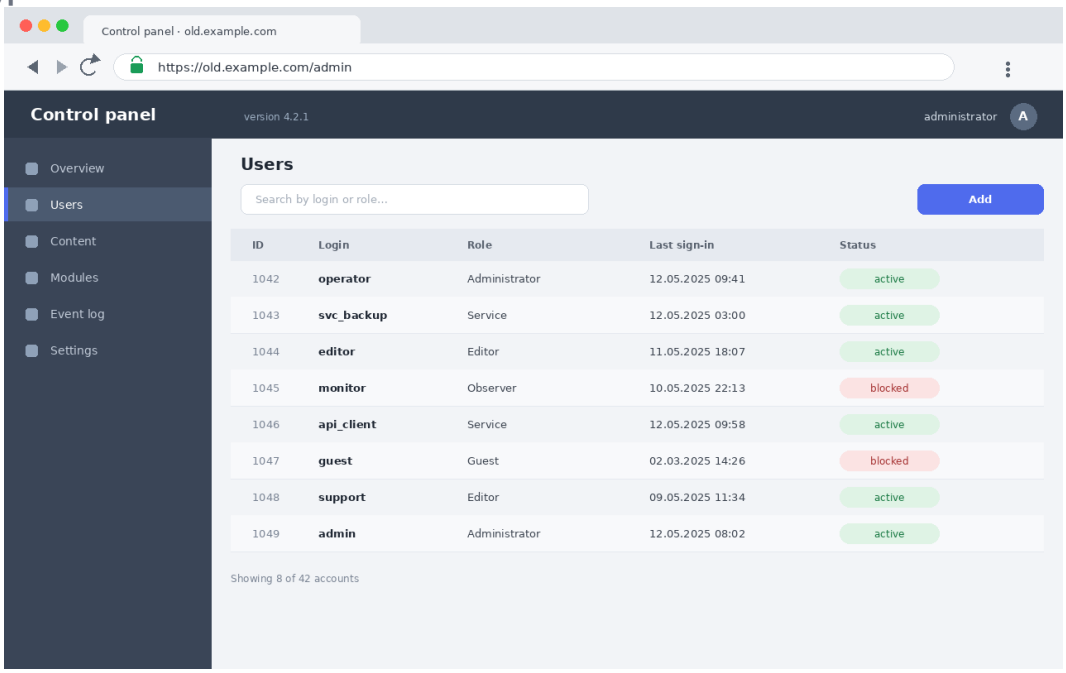
Details of the checks performed. For checks that revealed deficiencies, the codes of the corresponding vulnerabilities from section 4 are given below.

3.1. Web — resistance of authentication panels to brute force

Asset	Result
https://lk.example.com	**Found**
https://portal.example.com	**Found**

Description:
Checking login forms for attempt rate limiting and for acceptance of typical credentials.

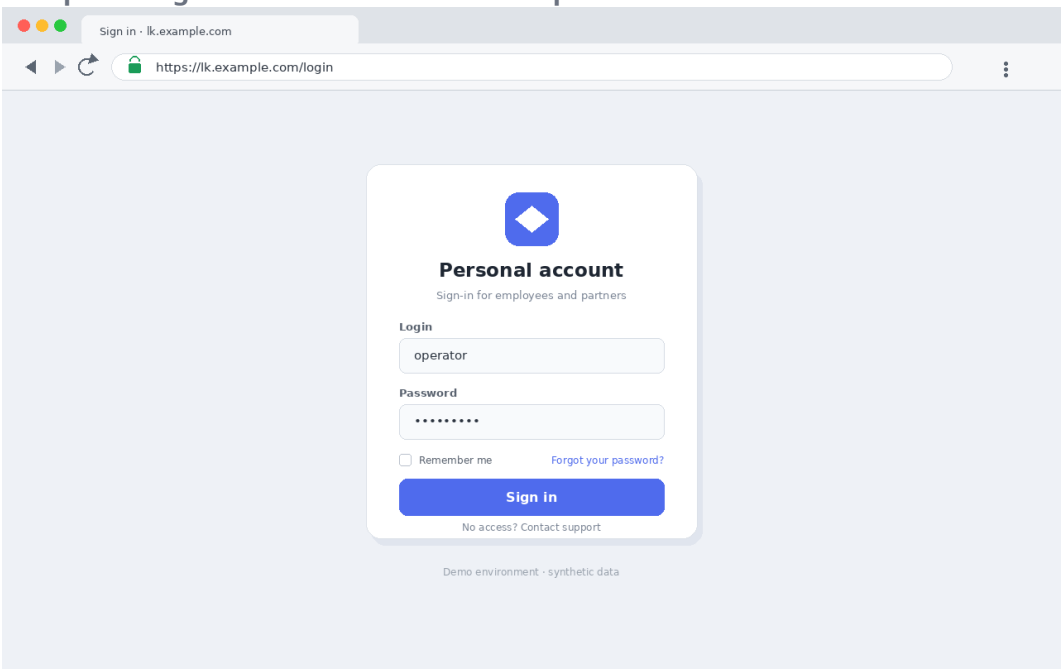
Site control panel on portal.example.com: an administrator session was obtained with a typical account



Sign-in attempt log
attempt=1 status=401
attempt=25 status=401
attempt=26 status=302 (successful sign-in)

Details:
https://lk.example.com
Lockout after a series of failures did not trigger.

Client portal sign-in form found on lk.example.com



https://portal.example.com
Login succeeded with a typical username and password pair.

Discovered:
The login form does not limit the rate of guessing attempts

Recommendations:
Change the default passwords, enable a second factor and a progressive delay.

3.2. External perimeter — inventory of reachable services

Asset	Result
portal.example.com	**Found**
192.0.2.24	**Found**

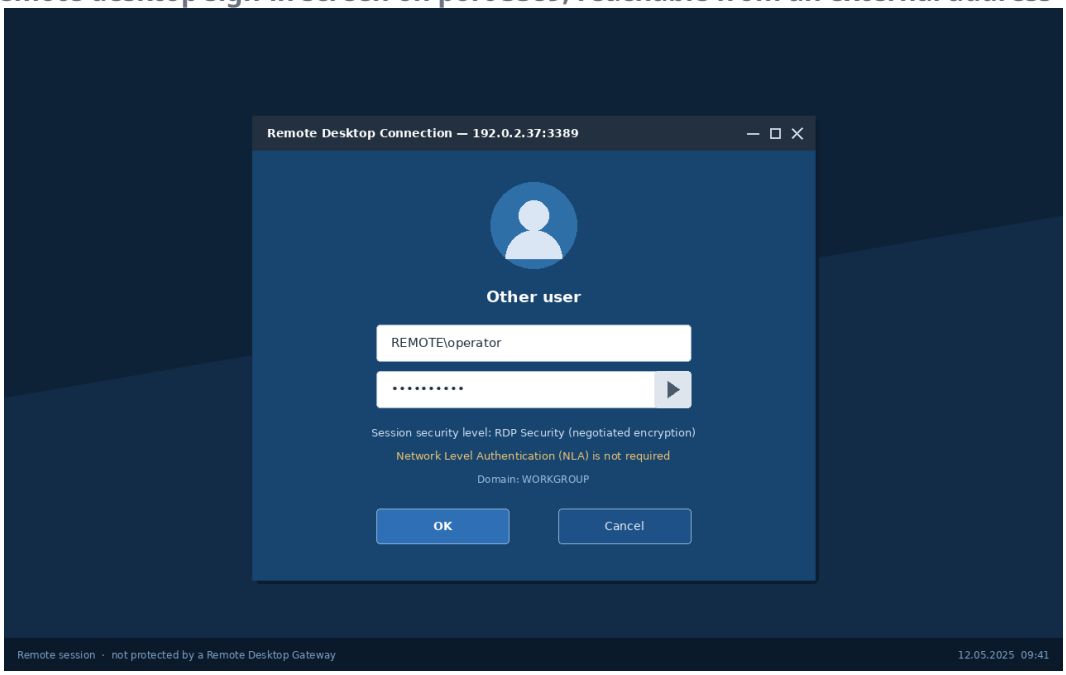
Description:
Building the list of services that respond on the project's external addresses and comparing it with the approved list.

Port scanner output

```
PORT     STATE SERVICE
443/tcp  open  https
3389/tcp open  ms-wbt-server
```

Service list export (CSV)

Remote desktop sign-in screen on port 3389, reachable from an external address

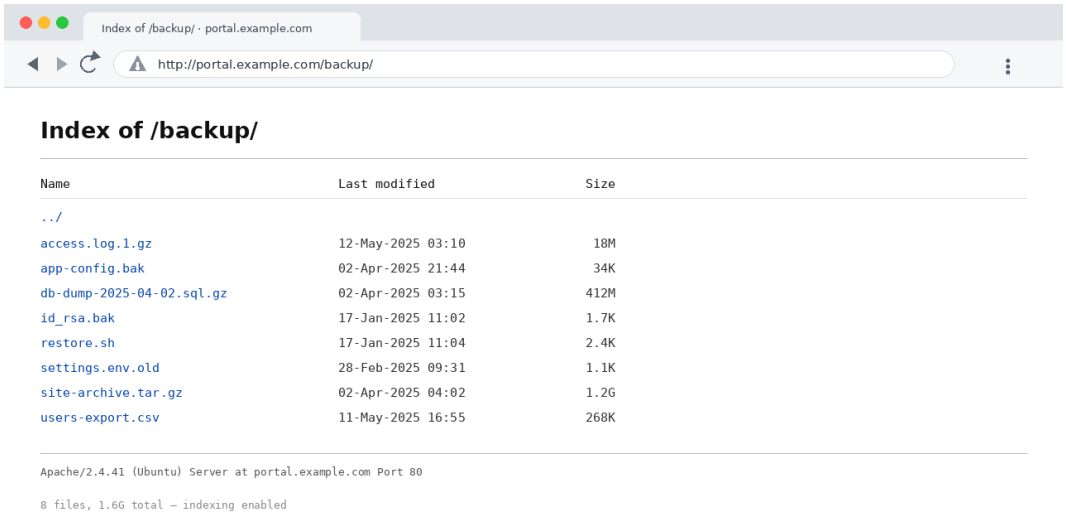


Details:

portal.example.com

The name is served by an external node.

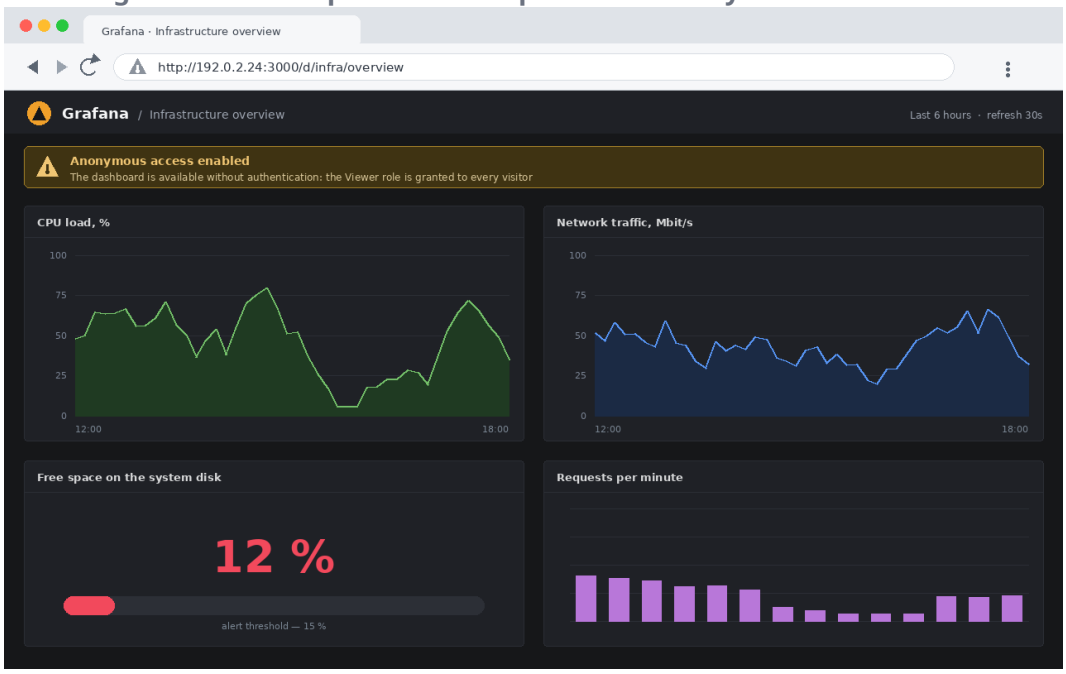
Directory listing of /backup/ on portal.example.com: backups are served without authorization



192.0.2.24

The monitoring panel responds from an external address without authentication.

Monitoring dashboard on port 3000 is exposed externally without authentication



Recommendations:
Agree on the list of external services and close the extra ones.

3.3. Mail and DNS — sender policy check

Object: mail.example.com

Description:
Comparison of sender policy records and mail signatures.

Name service response
_dmarc: record missing
spf: v=spf1 include:example.net ~all

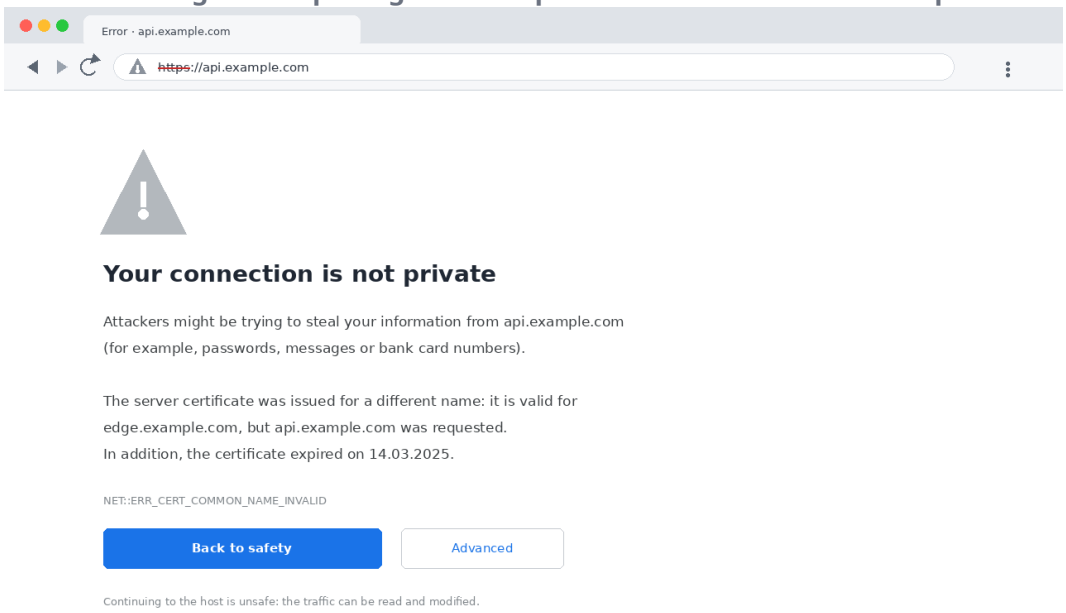
Details:
No handling policy record was found; the analysis continues.

3.4. TLS — configuration audit of endpoints

Object: 192.0.2.22

Description:
Collecting protocol versions, cipher suites and certificate parameters.

Browser warning when opening old.example.com: the certificate has expired



4. Findings register

A consolidated register of the deficiencies found, grouped by type of weakness: vulnerabilities (exploitable defects with CVE/RCE), perimeter exposure (management, database and remote-access services published to the outside — access configuration errors, not flaws in the code), information disclosure, certificates/TLS, data leaks and mail/DNS. Deficiencies with confirmation (a screenshot, a completed check or a problem confirmed by an active probe) are shown as cards; unconfirmed ones are rows of a compact table. High/Critical deficiencies are included in the register regardless of their source and of any link to a check (including those from scanners and imports); technical defects of medium/low level are included by checkbox or in the optional appendix.

Trend by perimeter category

Section	Open now	Before the cycle	Change	New in cycle	Fixed in cycle
Network security	12	3	+9	9	0
Web application security	16	2	+14	14	0
Information disclosure	2	0	+2	2	0
Data leaks	18	0	+18	18	0
Email and DNS security	1	1	0	0	0

4.1 Vulnerabilities

4.1.1. Unconfirmed (summary table)

Code	Name	Severity	CVSS	Asset
DEMO-54	Build server script console is available without login	Critical	9.8	192.0.2.24
DEMO-52	Database server accepts an administrator login without a password	Critical	9.8	192.0.2.25
DEMO-55	Edge gateway accepts a default account over SSH	Critical	9.8	198.51.100.11
DEMO-51	Key-value store is exposed to the internet without authentication	Critical	9.8	192.0.2.25
DEMO-56	SQL injection in the customer account search form	Critical	9.4	https://lk.example.com
DEMO-57	Authorization bypass in an internal API method	Critical	9.1	https://api.example.com:8443
DEMO-53	Cluster node service accepts anonymous requests	Critical	9.1	192.0.2.26
DEMO-58	Server-side request forgery in the mail web interface	Critical	9	https://mail.example.com
DEMO-02	Insecure deserialization in the web portal	Critical	8.8	https://lk.example.com
DEMO-61	Monitoring dashboard accepts a weak administrator password	High	8.6	192.0.2.24
DEMO-23	A subdomain points to a released provider resource	High	8.1	cdn.example.com
DEMO-60	Access to other users' records by identifier substitution in the API	High	8.1	https://api.example.com:8443

Code	Name	Severity	CVSS	Asset
DEMO-62	Gateway management panel is reachable from the internet	High	7.5	198.51.100.11
DEMO-59	Stored script injection in the feedback form	High	7.4	https://portal.example.com
DEMO-04	Directory traversal in the application file handler	High	7.1	https://api.example.com:8443

4.2 Information disclosure

4.2.1. DEMO-12 — Version control directory is accessible over HTTP

Threat level: High | CVSS: 7.5
Target: https://portal.example.com
Status: Active
Source: nuclei

Description:
A web path serves the repository's service directory with the source code change history.

Consequences:
Recovery of the source code and internal connection parameters.

Evidence:

Nuclei: vcs-directory-exposure
```
--- HTTP response ---
HTTP/1.1 200 OK
[core]
        repositoryformatversion = 0
```

Recommendations:
Forbid serving service directories on the web server and remove them from the publishing directory.

4.3 Data leaks

4.3.1. Leaks — Employees: Stealer logs from corporate hosts (with passwords)

Threat level: Critical
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:stealer_corp:creds

Description:
Data leaks affecting employees were found (8 records).

Source class: Stealer logs from corporate hosts.

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Stealer: Aurora, Stealer: Lumma, Stealer: Mars, Stealer: RedLine, Stealer: Rhadamanthys, Stealer: StealC, Stealer: Vidar.

Evidence:

Data leaks: employee:stealer_corp:creds

- Group: employee:stealer_corp:creds
- Records: 8

Email	Source	Date	Fields	Password
***@example.com	Stealer: StealC	2026-11-01	email,password,url	d***1
***@example.com	Stealer: Lumma	2026-11-01	email,password,url	S***!
***@example.com	Stealer: Aurora	2026-10-08	email,password,url	d***2
***@example.com	Stealer: Mars	2026-10-01	email,password,url	W***1
***@example.com	Stealer: RedLine	2026-09-14	email,password,url	d***3

- ... (+3 more)

Recommendations:
1. Force a password reset for all affected accounts.
2. Invalidate active sessions and cookies (log out everywhere).
3. Run antivirus cleanup on the affected users' devices.
4. Enforce MFA for the affected accounts.
5. Audit sign-in logs for the period since the leak.

4.3.2. Leaks — Customers: Corporate database breach (with passwords)

Threat level: High
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID client:corp_db_breach:creds

Description:
Data leaks affecting customers were found (3 records).

Source class: Corporate database breach.

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): CRMDemo Backup 2025, DemoCloud Sync 2023, DemoShop Orders 2022.

Evidence:

Data leaks: client:corp_db_breach:creds

- Group: client:corp_db_breach:creds
- Records: 3

Email	Source	Date	Fields	Password
***@example.com	CRMDemo Backup 2025	2026-10-02	email,password,full_name	d***7
***@example.com	DemoShop Orders 2022	2026-09-04	email,password,full_name	d***8
***@example.com	DemoCloud Sync 2023	2026-07-16	email,password,full_name,birth_date	d***6

Recommendations:
1. Force a password reset for all affected accounts (if password hashes are exposed).
2. Enforce MFA for all users.
3. Audit the leak points (web applications, APIs, databases).
4. Notify regulators (GDPR) where required.
5. Protect against phishing — exposed PII enables targeted attacks.

4.3.3. Leaks — Customers: Stealer logs from corporate hosts (with passwords)

Threat level: High
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID client:stealer_corp:creds

Description:
Data leaks affecting customers were found (4 records).

Source class: Stealer logs from corporate hosts.

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Stealer: Lumma, Stealer: RedLine, Stealer: StealC, Stealer: Vidar.

Evidence:

Data leaks: client:stealer_corp:creds

- Group: client:stealer_corp:creds
- Records: 4

Email	Source	Date	Fields	Password
***@example.com	Stealer: Vidar	2026-11-01	email,password,url	P***4
***@example.com	Stealer: StealC	2026-11-01	email,password,url	d***5
***@example.com	Stealer: RedLine	2026-10-09	email,password,url,browser	n***7
***@example.com	Stealer: Lumma	2026-09-08	email,password,url	d***6

Recommendations:
1. Force a password reset for all affected accounts.
2. Invalidate active sessions and cookies (log out everywhere).
3. Run antivirus cleanup on the affected users' devices.
4. Enforce MFA for the affected accounts.
5. Audit sign-in logs for the period since the leak.

4.3.4. Leaks — Employees: Corporate database breach (with passwords)

Threat level: High
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:corp_db_breach:creds

Description:
Data leaks affecting employees were found (8 records).

Source class: Corporate database breach.

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): CRMDemo Backup 2025, DemoCloud Sync 2023, DemoPay Merchant DB 2024, HRDemo Portal Leak 2023, MailDemo Archive 2020.

Evidence:

Data leaks: employee:corp_db_breach:creds

- Group: employee:corp_db_breach:creds
- Records: 8

Email	Source	Date	Fields	Password
***@example.com	HRDemo Portal Leak 2023	2026-11-01	email,password,full_name	S***5
***@example.com	DemoCloud Sync 2023	2026-11-01	email,password,full_name,phone,address	Q***!
***@example.com	DemoPay Merchant DB 2024	2026-10-20	email,password,full_name	d***6
***@example.com	CRMDemo Backup 2025	2026-10-15	email,password,full_name	d***5
***@example.com	DemoCloud Sync 2023	2026-09-21	email,password,full_name	d***7

- ... (+3 more)

Recommendations:
1. Force a password reset for all affected accounts (if password hashes are exposed).
2. Enforce MFA for all users.
3. Audit the leak points (web applications, APIs, databases).
4. Notify regulators (GDPR) where required.
5. Protect against phishing — exposed PII enables targeted attacks.

4.3.5. Leaks — Employees: Corporate database breach (without passwords)

Threat level: High
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:corp_db_breach:nocreds

Description:
Data leaks affecting employees were found (1 records).

Source class: Corporate database breach.

The leak contains no passwords — the main threat is targeted phishing, not direct compromise.

Sources (Leak.source): HRDemo Portal Leak 2023.

Evidence:

Data leaks: employee:corp_db_breach:nocreds

- Group: employee:corp_db_breach:nocreds
- Records: 1

Email	Source	Date	Fields	Password
***@example.com	HRDemo Portal Leak 2023	2026-06-01	email,full_name	—

Recommendations:
1. Force a password reset for all affected accounts (if password hashes are exposed).
2. Enforce MFA for all users.
3. Audit the leak points (web applications, APIs, databases).
4. Notify regulators (GDPR) where required.
5. Protect against phishing — exposed PII enables targeted attacks.

4.3.6. Leaks — Employees: Stealer logs from third-party hosts (password reuse) (with passwords)

Threat level: High
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:stealer_external:creds

Description:
Data leaks affecting employees were found (3 records).

Source class: Stealer logs from third-party hosts (password reuse).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Stealer: Mars, Stealer: Raccoon, Stealer: RedLine.

Evidence:

Data leaks: employee:stealer_external:creds

- Group: employee:stealer_external:creds
- Records: 3

Email	Source	Date	Fields	Password
***@example.com	Stealer: Mars	2026-10-11	email,password,url	S***!
***@example.com	Stealer: RedLine	2026-08-05	email,password,url	S***5
***@example.com	Stealer: Raccoon	2026-06-02	email,password,url	d***2

Recommendations:
1. Force a password reset for the affected accounts in our services (even if the host is not corporate, the credentials may have been reused).
2. Enforce MFA for the affected accounts.
3. Inform users about the leak and the need to change their passwords in other services.

4.3.7. Leaks — Customers: Stealer logs from third-party hosts (password reuse) (with passwords)

Threat level: Medium
Target: mail.example.com

Status: Active
Source: leak_aggregate, ID client:stealer_external:creds

Description:
Data leaks affecting customers were found (2 records).

Source class: Stealer logs from third-party hosts (password reuse).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Stealer: Rhadamanthys, Stealer: StealC.

Evidence:

Data leaks: client:stealer_external:creds

- Group: client:stealer_external:creds
- Records: 2

Email	Source	Date	Fields	Password
***@example.com	Stealer: StealC	2026-10-04	email,password,url	d***0
***@example.com	Stealer: Rhadamanthys	2026-09-17	email,password,url	d***2

Recommendations:
1. Force a password reset for the affected accounts in our services (even if the host is not corporate, the credentials may have been reused).
2. Enforce MFA for the affected accounts.
3. Inform users about the leak and the need to change their passwords in other services.

4.3.8. Leaks — Employees: Third-party database breach (work email in a public breach) (with passwords)

Threat level: Medium
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:external_db_breach:creds

Description:
Data leaks affecting employees were found (2 records).

Source class: Third-party database breach (work email in a public breach).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Combo List 2024, Paste Dump 2025.

Evidence:

Data leaks: employee:external_db_breach:creds

- Group: employee:external_db_breach:creds
- Records: 2

Email	Source	Date	Fields	Password
***@example.com	Paste Dump 2025	2026-11-01	email,password,full_name	d***6
***@example.com	Combo List 2024	2026-10-16	email,password	P***4

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.9. Leaks — Unclassified subjects: Corporate database breach (with passwords)

Threat level: Medium
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID unknown:corp_db_breach:creds

Description:
Data leaks affecting unclassified subjects were found (1 records).

Source class: Corporate database breach.

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): DemoCloud Sync 2023.

Evidence:

Data leaks: unknown:corp_db_breach:creds

- Group: unknown:corp_db_breach:creds
- Records: 1

Email	Source	Date	Fields	Password
info	DemoCloud Sync 2023	2026-09-22	username,password	d***8

Recommendations:
1. Force a password reset for all affected accounts (if password hashes are exposed).
2. Enforce MFA for all users.
3. Audit the leak points (web applications, APIs, databases).
4. Notify regulators (GDPR) where required.
5. Protect against phishing — exposed PII enables targeted attacks.

4.3.10. Leaks — Customers: Third-party database breach (work email in a public breach) (with passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID client:external_db_breach:creds

Description:
Data leaks affecting customers were found (3 records).

Source class: Third-party database breach (work email in a public breach).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Combo List 2024, DemoShop Orders 2022, Telegram Combo 2025.

Evidence:

Data leaks: client:external_db_breach:creds

- Group: client:external_db_breach:creds
- Records: 3

Email	Source	Date	Fields	Password
***@example.com	DemoShop Orders 2022	2026-11-01	email,password,full_name	d***4
***@example.com	Telegram Combo 2025	2026-10-16	email,password,full_name	d***7
***@example.com	Combo List 2024	2026-08-16	email,password,full_name	d***3

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.11. Leaks — Customers: Third-party database breach (work email in a public breach) (without passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID client:external_db_breach:nocreds

Description:
Data leaks affecting customers were found (1 records).

Source class: Third-party database breach (work email in a public breach).

The leak contains no passwords — the main threat is targeted phishing, not direct compromise.

Sources (Leak.source): FitDemo App Export.

Evidence:

Data leaks: client:external_db_breach:nocreds

- Group: client:external_db_breach:nocreds
- Records: 1

Email	Source	Date	Fields	Password
***@example.com	FitDemo App Export	2026-11-01	email,full_name	—

Recommendations:

1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.12. Leaks — Employees: Third-party database breach (work email in a public breach) (without passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID employee:external_db_breach:nocreds

Description:
Data leaks affecting employees were found (1 records).

Source class: Third-party database breach (work email in a public breach).

The leak contains no passwords — the main threat is targeted phishing, not direct compromise.

Sources (Leak.source): Unknown.

Evidence:

Data leaks: employee:external_db_breach:nocreds

- Group: employee:external_db_breach:nocreds
- Records: 1

Email	Source	Date	Fields	Password
***@example.com	Unknown	2026-06-22	email,phone,full_name,birth_date,address	—

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.13. Leaks — Third-party users: Stealer logs from third-party hosts (password reuse) (with passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID external:stealer_external:creds

Description:
Data leaks affecting third-party users were found (4 records).

Source class: Stealer logs from third-party hosts (password reuse).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Stealer: Aurora, Stealer: Lumma, Stealer: RedLine, Stealer: Vidar.

Evidence:

Data leaks: external:stealer_external:creds

- Group: external:stealer_external:creds
- Records: 4

Email	Source	Date	Fields	Password
***@example.com	Stealer: Lumma	2026-11-01	email,password,url	d***9
***@example.com	Stealer: RedLine	2026-09-09	email,password,url,browser,ip	d***4
***@example.com	Stealer: Aurora	2026-09-02	email,password,url	d***1
***@example.com	Stealer: Vidar	2026-07-13	email,password,url	d***3

Recommendations:
1. Force a password reset for the affected accounts in our services (even if the host is not corporate, the credentials may have been reused).
2. Enforce MFA for the affected accounts.
3. Inform users about the leak and the need to change their passwords in other services.

4.3.14. Leaks — Third-party users: Third-party database breach (work email in a public breach) (with passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID external:external_db_breach:creds

Description:
Data leaks affecting third-party users were found (4 records).

Source class: Third-party database breach (work email in a public breach).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Combo List 2024, FitDemo App Export, Marketplace Demo Users 2022, TravelDemo Loyalty 2021.

Evidence:

Data leaks: external:external_db_breach:creds

- Group: external:external_db_breach:creds
- Records: 4

Email	Source	Date	Fields	Password
***@example.com	Combo List 2024	2026-11-01	email,password	d***7
***@example.com	FitDemo App Export	2026-10-01	email,password,full_name	d***5
***@example.com	TravelDemo Loyalty 2021	2026-09-06	email,password,full_name	W***1
***@example.com	Marketplace Demo Users 2022	2026-08-07	email,password,full_name	Q***4

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.15. Leaks — Third-party users: Third-party database breach (work email in a public breach) (without passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID external:external_db_breach:nocreds

Description:
Data leaks affecting third-party users were found (1 records).

Source class: Third-party database breach (work email in a public breach).

The leak contains no passwords — the main threat is targeted phishing, not direct compromise.

Sources (Leak.source): Forum Dump.

Evidence:

Data leaks: external:external_db_breach:nocreds

- Group: external:external_db_breach:nocreds
- Records: 1

Email	Source	Date	Fields	Password
***@example.com	Forum Dump	2026-06-16	email	—

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.16. Leaks — Unclassified subjects: Stealer logs from third-party hosts (password reuse) (with passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID unknown:stealer_external:creds

Description:
Data leaks affecting unclassified subjects were found (3 records).

Source class: Stealer logs from third-party hosts (password reuse).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Paste Dump 2025, Stealer: Raccoon, Stealer: RedLine.

Evidence:

Data leaks: unknown:stealer_external:creds

- Group: unknown:stealer_external:creds
- Records: 3

Email	Source	Date	Fields	Password
ca	Paste Dump 2025	2026-08-01	email,password,url	d***0
ad	Stealer: Raccoon	2026-07-09	username,password	d***5
svcbk	Stealer: RedLine	2026-06-09	username,password,url	Q***!

Recommendations:
1. Force a password reset for the affected accounts in our services (even if the host is not corporate, the credentials may have been reused).
2. Enforce MFA for the affected accounts.
3. Inform users about the leak and the need to change their passwords in other services.

4.3.17. Leaks — Unclassified subjects: Third-party database breach (work email in a public breach) (with passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID unknown:external_db_breach:creds

Description:
Data leaks affecting unclassified subjects were found (1 records).

Source class: Third-party database breach (work email in a public breach).

Credentials (passwords / sessions) are affected — a critical credential stuffing or direct compromise scenario.

Sources (Leak.source): Telegram Combo 2025.

Evidence:

Data leaks: unknown:external_db_breach:creds

- Group: unknown:external_db_breach:creds
- Records: 1

Email	Source	Date	Fields	Password
bz	Telegram Combo 2025	2026-10-19	email,password,full_name	d***9

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.3.18. Leaks — Unclassified subjects: Third-party database breach (work email in a public breach) (without passwords)

Threat level: Low
Target: mail.example.com
Status: Active
Source: leak_aggregate, ID unknown:external_db_breach:nocreds

Description:
Data leaks affecting unclassified subjects were found (2 records).

Source class: Third-party database breach (work email in a public breach).

The leak contains no passwords — the main threat is targeted phishing, not direct compromise.

Sources (Leak.source): Marketplace Demo Users 2022, Unknown.

Evidence:

Data leaks: unknown:external_db_breach:nocreds

- Group: unknown:external_db_breach:nocreds
- Records: 2

Email	Source	Date	Fields	Password
nz	Unknown	2026-10-22	username	—
cb	Marketplace Demo Users 2022	2026-07-11	email,full_name	—

Recommendations:
1. Audit whether the affected credentials were actually used in our services (credential stuffing risk).
2. Force a password reset in our services if reuse is suspected.
3. Inform users that their email appears in a third-party breach.

4.4 Email and DNS security

4.4.1. DEMO-25 — No DMARC policy is set for the domain

Threat level: Medium | CVSS: 5.3
Target: mail.example.com
Status: Reopened
Source: mail_dns

Description:
The zone lacks a policy record for handling mail that fails sender authentication.

Consequences:
Spoofed mail sent on behalf of the organization's domain.

Recommendations:
Publish a DMARC record, starting with monitoring mode.

4.5 Other

4.5.1. Similar domains: 12 with high risk

Threat level: High
Similar domains: 12
Status: Active
Source: dnstwist

Description:
Registered look-alike domains similar to your domains were found; the list is below. Such domains can be used for targeted phishing of employees and customers: emails sent on behalf of the organisation and/or a fake website imitating the original.

Evidence:

Dnstwist: fin.tech-pay.example
Base domain: fintech-pay.example
Look-alike: fin.tech-pay.example (fake subdomain)
A: 203.0.113.232
MX: mail.fin.tech-pay.example
Look-alike site: yes

Similar domains:
• fin.tech-pay.example — similar to fintech-pay.example
• fintech-bank-login.example — similar to fintech-bank.example
• fintech-bank-secure.example — similar to fintech-bank.example
• fintech-bannk.example — similar to fintech-bank.example
• fintech-bnak.example — similar to fintech-bank.example
• fintech-cards-bank.example — similar to fintech-cards.example
• fintech-cards-login.example — similar to fintech-cards.example
• fintech-cards-online.test — similar to fintech-cards.example
• fintech-pa.example — similar to fintech-pay.example
• fintech-pay-login.example — similar to fintech-pay.example
... and 2 more similar domains (see /vulnerabilities)

Recommendations:
Put the look-alike domain under monitoring (DNS/MX/web). If there are signs of active phishing, send the registrar and the relevant CERT a request to suspend or block it, block the domain on the corporate mail gateway and warn customers. It makes sense to register close unclaimed variants preventively.

Appendix. Data leaks

The summary table shows the distribution of unresolved leaks along two axes: "who was compromised" (rows) and "through which channel the credentials were captured" (columns). Critical combinations are highlighted in colour.

Who	Project mobile app	Project web resources	Third-party services only	No origin	Breach	Total
Employees	**2**	**6**	**2**	**1**	**12**	**23**
Clients	—	**4**	2	—	7	**13**
External	—	—	**3**	**1**	**5**	**9**
Undetermined	—	—	1	2	4	**7**
Total	**2**	**10**	**8**	**4**	**28**	**52**

Records are grouped by the type of compromised subject and by the channel through which the credentials were captured. Each group states the recommended action for the response team.

Employees: credentials captured through the project's mobile app (2)

Action: Urgent: reset the AD/FreeIPA password, isolate the mobile device and check it for malware.

Date	Leak source	Data found
2026-10	Stealer: Aurora	**email:** af@example.com **password:** d***2 **origin:** android-app:com.example.lk **phone:** +7 900 000-00-33
2026-09	Stealer: RedLine	**email:** ah@example.com **password:** d***3 **origin:** ios-app:com.example.shop

Employees: credentials captured through the project's web resources (6)

Action: Urgent: reset the AD/FreeIPA password, isolate the workstation and run an antivirus scan.

Date	Leak source	Data found
2026-11	Stealer: StealC	**email:** ac@example.com **password:** d***1 **origin:** https://shop.example.com/admin
2026-11	Stealer: Lumma	**email:** ab@example.com **password:** S***! **origin:** https://lk.example.com/login **phone:** +7 900 000-00-30
2026-10	Stealer: Mars	**email:** ae@example.com **password:** W***1 **origin:** https://lk.example.com/login
2026-09	Stealer: Rhadamanthys	**email:** ag@example.com **password:** Q***4 **origin:** https://portal.example.com/
2026-08	Stealer: Lumma	**email:** ak@example.com **password:** d***4 **origin:** https://lk.example.com/login
… and 1 more leak		

Clients: credentials captured through the project's web resources (4)

Action: Urgent: force a password change in the client account and notify the client.

Date	Leak source	Data found
2026-11	Stealer: Vidar	**email:** km@example.com **password:** P***4 **origin:** https://shop.example.com/lk
2026-11	Stealer: StealC	**email:** bu@example.com **password:** d***5 **origin:** https://lk.example.com/login **phone:** +7 900 000-00-66
2026-10	Stealer: RedLine	**email:** dn@example.com **password:** n***7 **origin:** https://shop.example.com/lk, https://portal.example.com/pay (+ 2 more)
2026-09	Stealer: Lumma	**email:** bv@example.com **password:** d***6 **origin:** https://shop.example.com/admin

Employees: credentials captured only on third-party services (2)

Action: Recommend changing the AD password (it could match personal ones) and checking the workstation for malware.

Date	Leak source	Data found
2026-10	Stealer: Mars	**email:** aw@example.com **password:** S***! **origin:** https://example.net/login
2026-06	Stealer: Raccoon	**email:** im@example.com **password:** d***2 **origin:** https://forum.example.net/login, https://shop.example.net/

Employees: stealer log with no identified origin (1)

Action: Recommend changing the AD password and checking the workstation for malware.

Date	Leak source	Data found
2026-08	Stealer: RedLine	**email:** ba@example.com **password:** S***5

Employees: public breaches (12)

Action: Monitor. If the personal password was also used for AD, recommend changing it.

Date	Leak source	Data found
2026-11	DemoCloud Sync 2023	**email:** im@example.com **password:** Q***! **phone:** +7 900 000-00-21
2026-11	Paste Dump 2025	**email:** bg@example.com **password:** d***6
2026-11	HRDemo Portal Leak 2023	**email:** am@example.com **password:** S***5
2026-10	DemoPay	**email:** ao@example.com

Date	Leak source	Data found
	Merchant DB 2024	**password:** d***6
2026-10	Combo List 2024	**email:** pk@example.com **password:** P***4
… and 7 more leaks		

External identifiers: on third-party services (3)

Date	Leak source	Data found
2026-11	Stealer: Lumma	**email:** au@example.com **password:** d***9 **origin:** https://example.net/signin **phone:** +7 900 000-00-45
2026-09	Stealer: RedLine	**email:** mb@example.com **password:** d***4 **origin:** https://forum.example.net/login
2026-07	Stealer: Vidar	**email:** bc@example.com **password:** d***3 **origin:** https://example.net/login **phone:** +7 900 000-00-51

External identifiers: stealer log with no origin (1)

Date	Leak source	Data found
2026-09	Stealer: Aurora	**email:** ax@example.com **password:** d***1 **phone:** +7 900 000-00-48

External identifiers: public breaches (5)

Date	Leak source	Data found
2026-11	Combo List 2024	**email:** oz@example.com **password:** d***7
2026-10	FitDemo App Export	**email:** be@example.com **password:** d***5
2026-09	TravelDemo Loyalty 2021	**email:** bf@example.com **password:** W***1 **phone:** +7 900 000-00-54
2026-08	Marketplace Demo Users 2022	**email:** bj@example.com **password:** Q***4 **phone:** +7 900 000-00-57
2026-06	Forum Dump	**email:** mb@example.com

Identifier not determined: on third-party services (1)

Date	Leak source	Data found
2026-06	Stealer: RedLine	**username:** svcbk **password:** Q***! **origin:** https://shop.example.net/

Identifier not determined: stealer log with no origin (2)

Date	Leak source	Data found
2026-08	Paste Dump 2025	**username:** ca **password:** d***0

Date	Leak source	Data found
2026-07	Stealer: Raccoon	**username:** ad **password:** d***5

Identifier not determined: public breaches (4)

Date	Leak source	Data found
2026-10	Unknown	**username:** nz
2026-10	Telegram Combo 2025	**username:** bz **password:** d***9
2026-09	DemoCloud Sync 2023	**username:** info **password:** d***8
2026-07	Marketplace Demo Users 2022	**username:** cb

Appendix. Methodology

The checks were carried out by SeguriScan, IntruForce's automated platform for monitoring the external attack surface. It looks at the company from the internet, as an outsider would, within the scope agreed in writing. The results come from automated checks; no manual penetration testing was performed.

Stage	Scope of work
Discovery	Finding the company's internet-facing systems from its domains and approved address ranges: subdomains, DNS records, IP addresses, open ports and services. Searching known data leaks for the company's accounts and checking for registered look-alike domains.
Vulnerability detection	Identifying the software and versions each system shows and matching them against publicly known vulnerabilities (CVE), with CVSS, EPSS and CISA KEV data. A version match is recorded as a candidate, not as a confirmed vulnerability. Checks that interact with a system run only within the approved scope.
Prioritisation	Merging the results of all checks, removing duplicates and typical false alarms, and ranking findings by severity and by how likely they are to be exploited.
Report preparation	Documenting findings: the affected system, description, evidence, CVSS score and remediation recommendations.