EXTERNAL EXPOSURE — EXECUTIVE SUMMARY

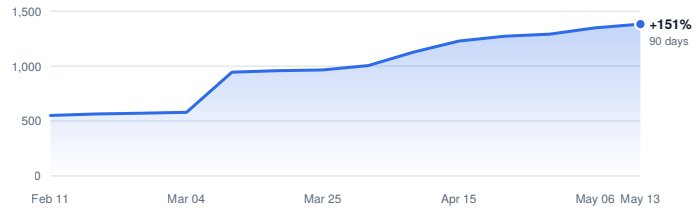
OPEN EXPOSURES	DEVICES INFECTED	LOOKALIKE DOMAINS	ATTACK-SURFACE VULNERABILITIES
1,383	**201**	**154**	**23**
visible to attackers today	with active session cookies — MFA bypass risk	registered against your brand	13 web-app + 10 DNS, externally exploitable

3 ways an attacker could breach you this week

1. **201 infected devices** with valid session cookies → MFA bypass into corporate apps.
2. **163 leaked credential pairs** → credential stuffing against VPN / SSO.
3. **13 exploitable web vulnerabilities** → direct compromise of external infrastructure.

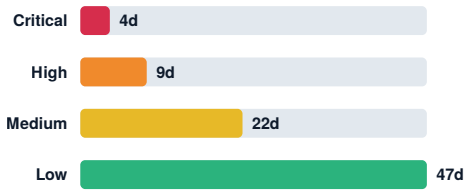
FINDINGS VOLUME — LAST 90 DAYS

Cumulative discovered threat events across all surveillance feeds



MEAN AGE OF OPEN ISSUES

Average days unresolved, by severity



Your organization's exposure

EXPOSURE CATEGORY	OPEN FINDINGS	WHAT THIS MEANS FOR YOUR ORGANIZATION
Accounts found in third-party breaches	842	Employee email addresses appearing in known breach datasets and combo lists — fuel for credential-stuffing attacks against SSO, VPN, and email.
Leaked corporate credentials	163	Active **email + password pairs** tied to your domains, circulating in dedicated credential dumps.
Info-stealer malware infections	201	Devices with active RedLine, Vidar, Lumma, or similar stealer logs containing domain credentials + **session cookies that bypass MFA**.
Lookalike domains	154	Domains registered against your brand, potentially used for phishing your customers and staff.
Attack-surface vulnerabilities	23	**13 web-application + 10 DNS** issues on your external infrastructure — exploitable without credentials.

ESTIMATED FINANCIAL EXPOSURE IF LEFT UNREMEDIATED

LOW	EXPECTED	HIGH
$12M	**$20M**	**$32M**

Based on **1,383 exposures** × 0.3–0.6% breach conversion rate (Verizon DBIR 2025) × $4.67M average credential-vector breach cost (IBM Cost of a Data Breach 2025).