General Intelligence: Cyber Threat — BrinksHome Breach

Generated: August 19, 2026 **Forreast Score:** 96.9/100 (Critical)

Overview

This report consolidates 1 high-confidence cyber threat signal of critical severity.

Signal Details

HIBP Breach: BrinksHome — 732,162 Accounts

- **Type:** Cyber Incident
- **Source:** Have I Been Pwned (HIBP)
- **Confidence:** 0.95
- **Detected:** August 19, 2026
- **Breached:** July 13, 2026

Summary: Breach of brinkshome.com confirmed. 732,162 accounts compromised. Data classes exposed include: - Dates of birth - Email addresses - Names - Partial credit card data - Phone numbers - Physical addresses

Risk Assessment

Dimension	Score	Rationale
Exposure	9.5	732K+ accounts with PII + partial card data
Velocity	9.0	Breach already occurred; data potentially in circulation
Severity	9.7	Financial fraud + identity theft surface
Confidence	9.5	HIBP-confirmed with specific data classes
Reversibility	2.0	Cannot un-leak data once exposed
Contagion	8.0	Credential reuse across other platforms

Composite Risk Score: 9.7 / 10 — Critical

Recommendations

1. **Immediate:** Force password resets for all brinkshome.com accounts.
2. **Immediate:** Notify affected users of the breach and exposed data classes.
3. **Short-term:** Monitor dark web for credential stuffing attacks using leaked email/password pairs.
4. **Short-term:** Enable MFA for all accounts if not already active.
5. **Medium-term:** Conduct full security audit of web application and database infrastructure.

Falsification Conditions

- If HIBP removes the breach entry, downgrade the assessment.
- If fewer than 100,000 accounts are confirmed affected upon forensic review, downgrade severity.

Forreast Intelligence — Cyber Threat Monitoring. This is intelligence analysis, not investment advice.
