COUNTRY CYBER RISK SCORE CARD

CYRA

Cyber Risk Assessment

ISSUE	COUNTRY FILE 00
CADENCE	QUARTERLY
HANDLING	CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

Brazil scores 4 of 5 on cyber risk. The country is both a major source and a major target of banking malware and phishing, and ransomware against public bodies rose this quarter. Firms with local operations should expect frequent credential theft attempts.

2.4M
ATTACK EVENTS ANALYZED

61%
SHARE TARGETING FINANCE

14
THREAT ACTORS ATTRIBUTED

COUNTRY CYBER SCORE

4 / 5

HIGH

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method using attack data. Up one level from the prior quarter.

01 Key findings

BANKING MALWARE — HIGH

Local banking trojans spread abroad

Banking trojans built in Brazil now target customers in Latin America and Europe. A [redacted] variant abuses instant payment flows to drain accounts within minutes of infection.

SOURCE · THREAT TELEMETRY

RANSOMWARE — ELEVATED

Public bodies hit by ransomware

Several municipal and state agencies reported ransomware incidents this quarter. Entry came through exposed remote access tools at a [redacted] IT contractor serving multiple agencies.

SOURCE · OFFICIAL REPORTS

PHISHING — MODERATE

Phishing kits sold in local forums

Portuguese-language forums sell phishing kits that copy tax and payment portals for under 50 dollars. Kits bundle [redacted] SMS tools that lift click rates on mobile devices.

SOURCE · DARK WEB

02 Cyber indicator watch

INDICATOR	TREND	EXPOSURE
Attacks originating from Brazil	▲ Rising	HIGH
Attacks targeting Brazilian networks	▲ Rising	HIGH
Instant payment fraud schemes	▲ Rising	ELEVATED
DDoS against e-commerce platforms	Steady	MODERATE

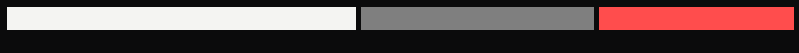
03 Analyst recommendations

01 Enforce phishing-resistant MFA for all staff and vendors with access to local systems.

02 Audit remote access tools used by IT contractors and close unused exposed services.

03 Add transaction limits and alerts on instant payment accounts held in Brazil.

DATA MIX THIS QUARTER



Telemetry 45% · Official 30% · Dark web 25%

WHAT THE CLIENT RECEIVES

- → 1 to 5 cyber score per country
- → Inbound and outbound attack data
- → Sector exposure breakdown
- → Direct line to the TAM-C cyber team

ILLUSTRATIVE SAMPLE. ORGANIZATIONS, GROUPS AND FIGURES ARE ANONYMIZED OR REDACTED.
FULL REPORTS ARE DELIVERED TO CLIENTS ONLY.

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068