CLIENT-SPECIFIC DARK WEB MONITORING REPORT

Dark Web Monitoring

Dark Web / Cyber Threat Monitoring

ISSUE MONITORING CYCLE 00
CADENCE MONTHLY
HANDLING CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

Two marketplace vendors are now advertising access and data tied to the client's logistics unit, and an encrypted channel shared a staff directory this cycle. No evidence of core network compromise was found, but the directory supports targeted phishing and fraud.

14
MARKETPLACES UNDER WATCH

212
CLIENT MENTIONS REVIEWED

3
VENDORS PROFILED THIS CYCLE

CLIENT EXPOSURE LEVEL

3 / 5

ELEVATED

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method. Up one level after the vendor listings surfaced.

01 Key findings

MARKETPLACE — HIGH

Vendor lists logistics portal access

A vendor trading as [redacted] is offering VPN access to a logistics portal matching the client's naming format for $2,400. Seller feedback suggests prior sales of verified corporate access in the sector.

SOURCE · DARK WEB MARKET

ENCRYPTED CHAT — ELEVATED

Staff directory shared in a channel

A 600-member channel posted a spreadsheet with 380 client staff names, roles and work numbers. The file metadata points to an export from a [redacted] HR platform used by a former contractor.

SOURCE · TELEGRAM CHANNEL

FORUM CHATTER — MODERATE

Sector fraud thread names the client

A [redacted] forum thread on invoice fraud lists the client among sector firms with weak supplier verification. Posters request contacts in accounts payable; no successful attempt has been claimed so far.

SOURCE · DEEP WEB FORUM

02 Client mention watch

INDICATOR	TREND	EXPOSURE
Access listings naming client systems	▲ Rising	HIGH
Staff PII shared on encrypted platforms	▲ Rising	ELEVATED
Brand use in fraud and phishing threads	■ Steady	MODERATE
Stolen card data tied to client customers	▼ Easing	MODERATE

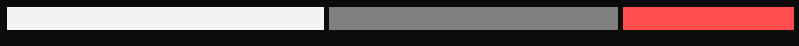
03 Analyst recommendations

01 Rotate VPN credentials for the logistics portal and review recent remote login activity.

02 Brief listed staff on targeted phishing and voice fraud using their directory details.

03 Add callback verification for supplier bank detail changes in accounts payable.

COLLECTION MIX THIS CYCLE



Marketplaces 41% · Encrypted 37% · Forums 22%

WHAT CLIENTS RECEIVE

→ Client-specific monitoring report
→ Vendor and seller profiles
→ Encrypted platform coverage
→ Immediate alerts on critical finds

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

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068