IOT EXPOSURE AND LOOK-ALIKE DOMAIN SCAN

Vulnerability & IoT

Vulnerability & IoT Monitoring

ISSUE	SCAN CYCLE 00
CADENCE	MONTHLY
HANDLING	CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

The scan found 47 internet-facing devices tied to the client, including nine IP cameras with default credentials and an exposed building management panel. Six newly registered look-alike domains were identified, two already hosting a cloned employee login page.

47
EXPOSED DEVICES IDENTIFIED

9
DEVICES WITH DEFAULT LOGINS

6
LOOK-ALIKE DOMAINS FOUND

EXPOSURE SCORE

4 / 5

HIGH

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method. Live phishing pages and default logins drive the score.

01 Key exposures

IOT DEVICE — HIGH

Building management panel exposed

A [redacted] building management interface controlling HVAC and door access at the client's Dubai office is reachable from the internet. The firmware version has a known remote access flaw.

SOURCE · INTERNET SCAN

LOOK-ALIKE — HIGH

Cloned login page on a typo domain

The domain [redacted]-portal.com, registered 11 days ago, hosts a copy of the client's staff sign-in page. Its mail server is configured, suggesting a phishing campaign is ready to launch.

SOURCE · DOMAIN REGISTRY

IOT DEVICE — ELEVATED

IP cameras on default credentials

Nine [redacted] IP cameras across two warehouses accept factory default logins and stream live video. Camera views cover loading bays and a server room entrance, giving outsiders a view of site routines.

SOURCE · INTERNET SCAN

02 Exposure register

ASSET	TREND	EXPOSURE
Look-alike domains with live content	▲ Rising	HIGH
IoT devices with known firmware flaws	▲ Rising	HIGH
Open remote desktop and admin ports	▼ Easing	ELEVATED
Expired TLS certificates on client hosts	■ Steady	MODERATE

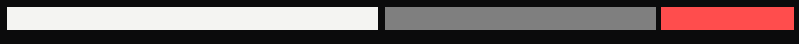
03 Remediation priorities

01 Remove the building management panel from public access and patch its firmware.

02 File takedown requests for the two live phishing domains and block them at the mail gateway.

03 Change default credentials on all cameras and move them to an isolated network.

DETECTION SOURCES



IoT scans 48% · Domains 35% · Web crawl 17%

WHAT THE CLIENT RECEIVES

→ Exposed device register with risk
→ Look-alike domain watchlist
→ Prioritized remediation steps
→ Takedown support for phishing sites

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

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068