WEEKLY CYBER THREAT INTELLIGENCE REPORT

ARCTIC

Analytical Review of Cyber Threat Intelligence Concerns

ISSUE	REPORTING WEEK 00
CADENCE	WEEKLY
HANDLING	CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

Ransomware leak-site activity against mid-size financial institutions rose for a third consecutive week, and credentials tied to two regional banks surfaced on public drop sites. Exposure is concentrated in third-party vendors rather than core banking systems.

38
LEAK-SITE POSTINGS REVIEWED

1.2M
EXPOSED RECORDS TRIAGED

6
GROUPS TRACKED THIS WEEK

WEEKLY THREAT LEVEL

3 / 5

ELEVATED

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method. Up one level from the prior week.

01 Key developments

RANSOMWARE — HIGH

Affiliate lists a regional lender

A [redacted] affiliate posted a countdown for a [redacted] regional lender, claiming 400 GB of loan files. Sample documents appear to originate from a document-management vendor.

SOURCE · DARK WEB

HACKING GROUPS — ELEVATED

Hacktivist DDoS campaign announced

A self-described hacktivist collective named [redacted] banks as targets for a 72-hour DDoS window. Prior campaigns by the group caused short outages of online banking portals.

SOURCE · CLEAR WEB

DROP SITES — MODERATE

Employee credentials on a public bin

A paste containing 1,140 email and password pairs for [redacted].com staff appeared on a public drop site. 22% match formats used in prior breaches; resets are recommended.

SOURCE · PASTE AND DROP BINS

02 Financial sector watch

INDICATOR	TREND	EXPOSURE
Phishing kits impersonating online banking	▲ Rising	HIGH
Card data offered on carding markets	▼ Easing	MODERATE
Insider recruitment posts targeting bank staff	▲ Rising	ELEVATED
Initial-access sales for vendor networks	▲ Rising	HIGH

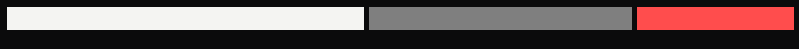
03 Analyst recommendations

01 Force credential resets for the exposed staff accounts and enforce phishing-resistant MFA.

02 Ask document-management and IT vendors to confirm whether they were affected.

03 Pre-stage DDoS mitigation with your provider ahead of the announced window.

COLLECTION MIX THIS WEEK



Dark web 46% · Clear web 34% · Drop bins 20%

WHAT SUBSCRIBERS RECEIVE

→ Analyst-written PDF, every week
→ Dark web and clear web coverage
→ Sector watch tuned to your industry
→ Direct line to the TAM-C cyber team

ILLUSTRATIVE SAMPLE. ORGANIZATIONS, GROUPS AND FIGURES ARE ANONYMIZED OR REDACTED.
FULL ISSUES ARE DISTRIBUTED TO SUBSCRIBERS ONLY.

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068