RANSOM AND CYBER ATTACK INCIDENT WATCH

Ransom Monitoring

Ransom & Cyber Attack Monitoring

ISSUE	INCIDENT WATCH 00
CADENCE	24/7 CONTINUOUS
HANDLING	CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

A ransomware crew posted the client's name on its leak site with a seven-day countdown, claiming 120 GB of finance data. Sample files match a supplier's file share, not client systems. In parallel, a brand-targeted DDoS threat against the client's ordering platform was announced.

7d
COUNTDOWN ON LEAK SITE

120G
DATA CLAIMED BY ATTACKERS

2
ACTIVE INCIDENTS TRACKED

INCIDENT SEVERITY

4 / 5

HIGH

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method. Active countdown and a public DDoS threat this week.

01 Incident timeline

RANSOM DEMAND — HIGH

Client named with leak countdown

The [redacted] leak site listed the client with a $1.8M demand and a seven-day timer. Posted samples include invoices and payroll files stored on a shared drive run by a [redacted] payroll provider.

SOURCE · LEAK SITE

DDOS THREAT — ELEVATED

Ordering platform named for DDoS

A hacktivist channel, [redacted], named the client's online ordering platform among targets for a weekend DDoS campaign. The group's prior attacks peaked at moderate volume and lasted under six hours.

SOURCE · TELEGRAM CHANNEL

BRAND ABUSE — MODERATE

Fake support accounts spread claims

Four new social accounts posing as [redacted] support are spreading the leak claim and asking customers to confirm payment details. Accounts were reported and two have already been suspended.

SOURCE · SOCIAL MEDIA

02 Incident watch

INCIDENT	TREND	SEVERITY
Leak-site countdown and data samples	▲ Rising	HIGH
DDoS threat against ordering platform	▲ Rising	ELEVATED
Fake support accounts using the brand	▼ Easing	MODERATE
Threats naming executives or staff	■ Steady	MODERATE

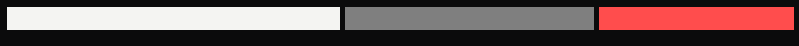
03 Immediate actions

01 Confirm scope with the payroll provider and engage incident response counsel today.

02 Activate DDoS mitigation for the ordering platform ahead of the weekend window.

03 Warn customers through official channels that support will never request card details.

MONITORING COVERAGE



Leak sites 43% · Channels 32% · Social 25%

WHAT THE CLIENT RECEIVES

→ 24/7 ransom and attack monitoring
→ Immediate alerts on new incidents
→ Brand abuse and impersonation watch
→ Incident updates until resolution

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

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068