

Early detection of third-party breaches prior to public disclosure

with adversary intelligence and analyst-driven investigations

How a Fortune 5 global e-commerce company monitors 150,000+ supply-chain partners for breaches, ransomware, and escalating vendor incidents.

CASE STUDY CUSTOMER

Fortune 5 global e-commerce company with approximately 150,000+ supply-chain partners

OPERATIONAL OUTCOME

Independent breach intelligence with early adversary-source detection, API delivery, and faster third-party response.

THE CHALLENGE

Disclosure delays left the company unaware of third-party incidents

A Fortune 5 global e-commerce company depends on more than 150,000 supply-chain partners across its global operations.

When a critical vendor is breached, public reporting alone may not reveal the scope, exposed data, or evolving threat-actor activity.

The visibility gap

Existing tools could not reliably monitor the company's entire vendor network for breach and ransomware activity. The company needed independent visibility across disclosed incidents and emerging activity from criminal forums, marketplaces, and ransomware leak sites.

Company policy also prevented the incident response team from navigating the dark web directly, creating a critical investigation gap during high-impact events.

The security team needed to

- Continuously monitor 150,000+ supply-chain partners
- Detect incidents before formal vendor notification
- Escalate high-impact events for analyst investigation
- Give incident responders evidence—not just an alert

**VENDORS
MONITORED**

150K+

ACCESS GAP

**Dark-web access
restricted by policy**

ECOSYSTEM SCALE

**150K+ vendors
monitored**

RFI VALUE

**Analyst-validated
evidence**

Awareness gap

Detect relevant incidents without waiting for vendor disclosure.

THE SOLUTION

Early warning and analyst-led RFIs accelerate incident response

HackNotice continuously monitors 150,000+ supply-chain partners and supports high-impact incidents with analyst-led Requests for Information.

01 Monitor

Continuously monitor 150,000+ vendors for breaches, ransomware, data leaks, and related threat activity.

02 Prioritize

Detect activity on ransomware leak sites, criminal forums, marketplaces, and other dark-web sources.

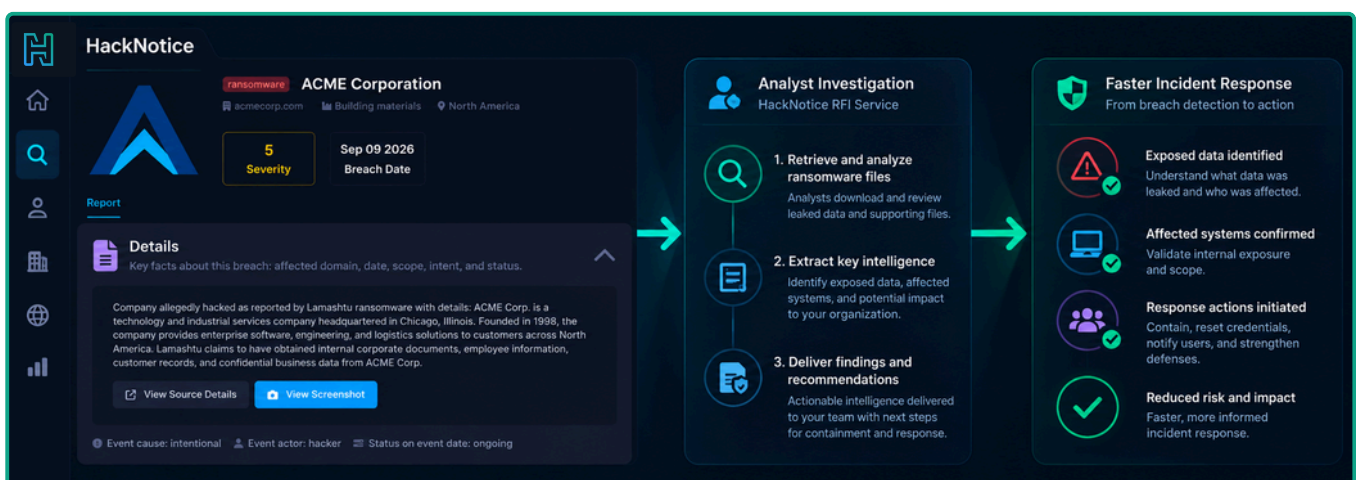
03 Investigate

Combine dark-web findings with company notices, government disclosures, regulatory filings, and news.

04 Respond

Deliver alerts through the API to trigger established TPRM, incident response, and InfoSec workflows.

EARLY WARNING



THE RESULTS

Earlier detection and faster response across a 150,000+ vendor ecosystem

Alerts identify the supply chain incident before public disclosure.

Analyst-led RFIs reveal what was exposed, who is affected, and what incident responders should do next.

RESPOND

with custom analyst-led investigations.

Threat-actor monitoring, breach artifact retrieval & review, and a custom decision-ready report.

WEEKS

earlier awareness of vendor breaches.

Dark-web discovery can precede formal vendor disclosure by weeks or months.

70%

of breaches initially detected from adversary sources.

Ransomware sites, forums, marketplaces, and other criminal communications surface incidents early.

OPERATIONAL IMPACT

From disclosure-dependent monitoring to an active early-warning capability.

API-delivered alerts give TPRM, incident response, and InfoSec teams a shared trigger for investigation.

For high-impact events, HackNotice analysts monitor threat-actor and ransomware posts, capture files and samples as published, and deliver a custom report to support scope, exposure, and response decisions.

Operational adversary intelligence for third-party risk

HackNotice closes the visibility gap between your own environment and your vendor ecosystem. You gain real-time insight into which third parties are under attack or being trafficked, who is likely behind it, and the tactics and attack vectors being used—so your team can prioritize the right controls, focus the right questions, and reduce uncertainty across the supply chain.

Real-time operational risk services for your ecosystem.

Third-Party Monitoring

Continuous vendor breach, ransomware, exposure, actor, TTP, and downstream extended supply chain intelligence.

First-Party Monitoring

Real-time credential, infostealer, and sensitive data exposure to mitigate ATO and identity risk for users and consumers.

Research

Search dark-web files and hacker communications for credentials, leaked data, and relevant threat actor activity.

Information Requests

Analyst-led investigations into source, scope, affected data, attribution, and potential impact.

Raw adversary data transformed into validated, actionable intelligence.

Deep Adversary Sources



1.5+Trillion Records
ingested from source files



260+Ransomware groups
monitored, and growing



1M+ Infostealer records
and credentials reviewed daily



1,000+ Breach sources
verified and monitored

Actionable Outputs



Active threat actor
campaigns



Attack pattern and
TTP trends



Supply chain exposure
and blast-radius clarity



Threats mapped to
controls and risk

Turn vendor uncertainty into operational decisions

hacknotice.com | [Schedule a tailored threat briefing](#)