HackNotice

Proactive Infostealer Detection Through Domain Monitoring:

A Fortune 1000 Consumer Goods Success Story

CASE STUDY

Introduction

In a rapidly evolving cybersecurity landscape, HackNotice empowers security teams with real-time, tailored threat intelligence to proactively defend against compromise. With dark web monitoring designed to detect exposures that traditional tools miss, HackNotice delivers unique visibility into emerging threats—allowing organizations to act before incidents escalate. For this Fortune 1000 consumer goods company, HackNotice became a critical layer of defense in detecting infostealer malware activity across its workforce.

The Challenge

A leading consumer goods enterprise needed a way to identify employees who had unknowingly fallen victim to infostealer malware. Despite having endpoint detection and response (EDR) tools in place, the company's cybersecurity team suspected that some infections were evading traditional coverage—particularly on personal or unmanaged devices used for work purposes.

The team needed a solution that could extend visibility beyond their internal infrastructure, detect compromised credentials in real time, and allow them to act quickly to prevent account takeover and internal abuse.

Solution

HackNotice delivered an immediate and effective solution through its **First Party Domain Monitoring** service. By continuously scanning the dark web for data associated with the company's email domain, HackNotice enabled proactive detection of credential exposures from infostealer malware.

Real-Time Credential Exposure Alerts

HackNotice alerted the cybersecurity team whenever employee credentials appeared in trafficked dark web infostealer logs, enabling same-day remediation actions like forced password resets and account lockdowns.

Malware Visibility Beyond EDR

Unlike traditional tools that only monitor company-managed endpoints, HackNotice provided intelligence on malware infections occurring on **any device** where the employee used their business email—whether corporate-issued or personal.

Uncovering Hidden Threats

Several cases of malware were discovered on employee devices that had gone undetected by the company's EDR, validating the need for this complementary dark web monitoring layer.

Results

A Cybersecurity Engineer at a Fortune 1000 consumer goods company noted that HackNotice helped their team uncover employees infected with infostealer malware—insights not surfaced by other tools.

Faster Incident Response

HackNotice alerts allowed the security team to take immediate action, resetting credentials and reducing time-to-containment for exposed accounts.

Malware Detection Coverage Gap Closed

HackNotice filled a blind spot in the company's security stack by identifying infections on unmanaged or personal devices, extending their protection footprint.

Enhanced Threat Visibility

By correlating exposures to specific dark web sources, the team gained context on malware types, breach timing, and user behavior—improving root cause analysis and employee awareness training.

About HackNotice

HackNotice is the leader in dark web intelligence and breach monitoring, helping organizations around the world reduce risk from credential exposure, data leaks, and supply chain threats. Our platform continuously monitors the global dark web—including criminal forums, Telegram, marketplaces, and breach archives—for stolen credentials, infostealer logs, and leaked corporate data.

HackNotice provides real-time alerts for ransomware events, data breaches, and account exposures, empowering security teams to take immediate action. From individual employee protection to comprehensive vendor monitoring, we help enterprises detect and mitigate risk before it becomes a compromise.

Our services include:

Credential and Session Exposure Monitoring
Discover when your employees, customers, or systems appear in infostealer logs or breach dumps.

Third Party and Supply Chain Risk Intelligence
Track vendors and partners for breaches, ransomware attacks, or data leaks that may put your business at risk.

Ransomware & Data Breach Alerts
Get real-time, actionable notifications about new attacks across your ecosystem.

Dark Web Incident Analysis
Receive deep-dive investigations into specific dark web data incidents, including attribution, scope, and remediation guidance.

With HackNotice, your team gains early visibility into attacker data and behavior—enabling you to respond quickly, protect identities, and minimize business disruption. Learn more at hacknotice.com or contact us to schedule a tailored threat briefing.