Redpanda

CASE STUDY

Redpanda Fights Recruitment Job Scams

Protecting Candidates and Brand Reputation

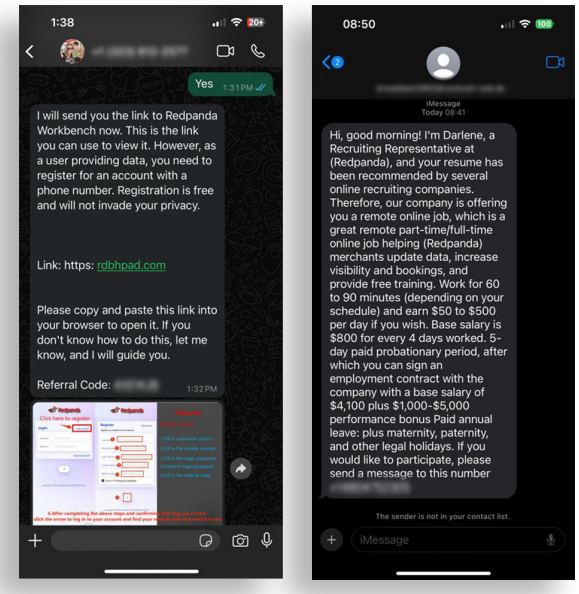
netcraft

Background:

Redpanda is a high-performance, Kafka®-compatible streaming data platform engineered for simplicity, speed, and scalability. Its platform includes tools for seamless data integration and intuitive cluster management, making it a preferred choice for developers aiming to build real-time applications efficiently.

Challenge: Combating Fraudulent Job Scams

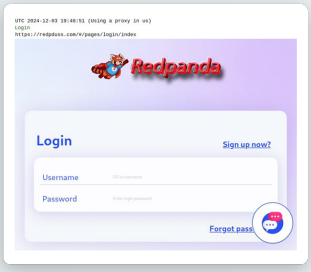
In the latter half of 2024, Redpanda began receiving reports that individuals, pretending to represent the company, were extending fraudulent job offers to targeted victims. These scams amplify appealing opportunities for remote, part-time roles and promise lucrative compensation for minimal tasks—common characteristics of task-based job scams. Despite adding warnings to their careers page and encouraging victims to report such incidents, the number of fraudulent activities continued to grow, and the volume outpaced initial efforts to prevent victimization.

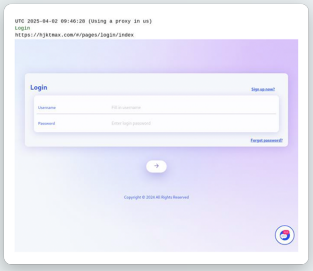


Initial Contact: The scam starts with a direct message containing a callback number (SMS or WhatsApp).

Engagement: When the recipient contacts the number, they're engaged in a conversation about a job opportunity. Once the victim accepts the job offer, they will be asked to attend a webinar and provided with company information and login instructions.

Scam Execution: The victim is directed to the scam website to login where they **are required** to invest their own money to "unlock" further tasks or release virtual earnings in their account.





Evolved Threat Tactics:

Initially this threat actor led customers to a branded login page. Because they were quickly detected and taken down, they evolved to a non-branded page with unconnected phishing URLS. Leveraging Netcraft's pattern matching capabilities coupled with automated searches focused on Redpanda's Terms & Conditions page, our team quickly detected the adversary and had their scam site taken down.

Solution: Efficient Countermeasures with Netcraft

To address this escalating issue, Redpanda worked with Netcraft to deploy 24/7 support and efficient countermeasures against these fraudulent activities. Netcraft's sophisticated technology extracts associated phone numbers, URLs, and emails within screenshots using OCR (Occiptal character recognition) and automatically submits them to relevant infrastructure providers. Additionally, Netcraft's proactive detection capabilities identify and neutralize threats before they are reported by external parties.

Why Netcraft?

> We were able to eliminate the time spent navigating abuse reporting processes for different providers and tracking reporting outcomes reliably. Before onboarding Netcraft, we were unable to pursue takedowns with mobile providers. Netcraft filled that critical gap, allowing us to take robust action earlier in the scam chain"
>
> — Chief of Staff at Redpanda

Impact: Enhanced Brand Protection and Reduced Scam Attempts

- Reduced the time between reporting and takedown from days or weeks to mere minutes or hours, substantially decreasing the reported scam attempts targeting Redpanda.
- Swift and proactive measures not only safeguarded the company's brand integrity but also protected vulnerable job seekers from becoming the victim to fraudulent schemes.
- Reduced the teams' time spent navigating reporting processes and tracking the outcomes' reliability by 95%.
- Initiated takedowns against the domains & emails found within the smishing campaigns with a median 50 hour take down time.

> When fraudulent job scams started targeting our brand, we needed a faster, more scalable solution. Partnering with Netcraft made an immediate difference — hundreds of scam sites and phone numbers were taken down, often within minutes or hours instead of days or weeks. Their proactive detection also caught threats before they reached our team. Thanks to Netcraft, **we've seen a significant drop in scam reports and can better protect our brand and candidates."**
>
> — Chief of Staff at Redpanda

Key Results:

326 cases

326 cases taken down to date (100% resolved, no outstanding threats)

50 hours

Across all attack types: 50 hour Median Takedown Time

55 hours

Fraudulent Phone Numbers Reported: 55 hour Median Takedown Time compared to days and weeks

95% reduction

95% reduction in time spent navigating reporting processes and tracking outcomes

Phishing URLs:

1 hour

Median Takedown Time

netcraft

Connect with Netcraft today for greater speed and global reach at scale.