

# Help Wanted: Vietnamese Actors Using Fake Job Posting Campaigns to Deliver Malware and Steal Credentials

Google Threat Intelligence Group : : 10/22/2025

---



**Threat  
Intelligence**

## Google Threat Intelligence

Visibility and context on the threats that matter most.

### [Contact Us & Get a Demo](#)

Google Threat Intelligence Group (GTIG) is tracking a cluster of financially motivated threat actors operating from Vietnam that leverages fake job postings on legitimate platforms to target individuals in the digital advertising and marketing sectors. The actor effectively uses social engineering to deliver malware and phishing kits, ultimately aiming to compromise high-value corporate accounts, in order to hijack digital advertising accounts. GTIG tracks parts of this activity as UNC6229.

The activity targets remote digital advertising workers who have contract or part-time positions and may actively look for work while they currently have a job. The attack starts when a target downloads and executes malware or enters credentials into a phishing site. If the target falls victim while logged into a work computer with a personal account, or while using a personal device with access to company ads accounts, threat actors can gain access to those company accounts. Successful compromise of a corporate advertising or social media account allows the threat actor to either sell ads to other actors, or sell the accounts themselves to other actors to monetize, as they see fit. This blog describes the actor's tactics, techniques, and procedures (TTPs).

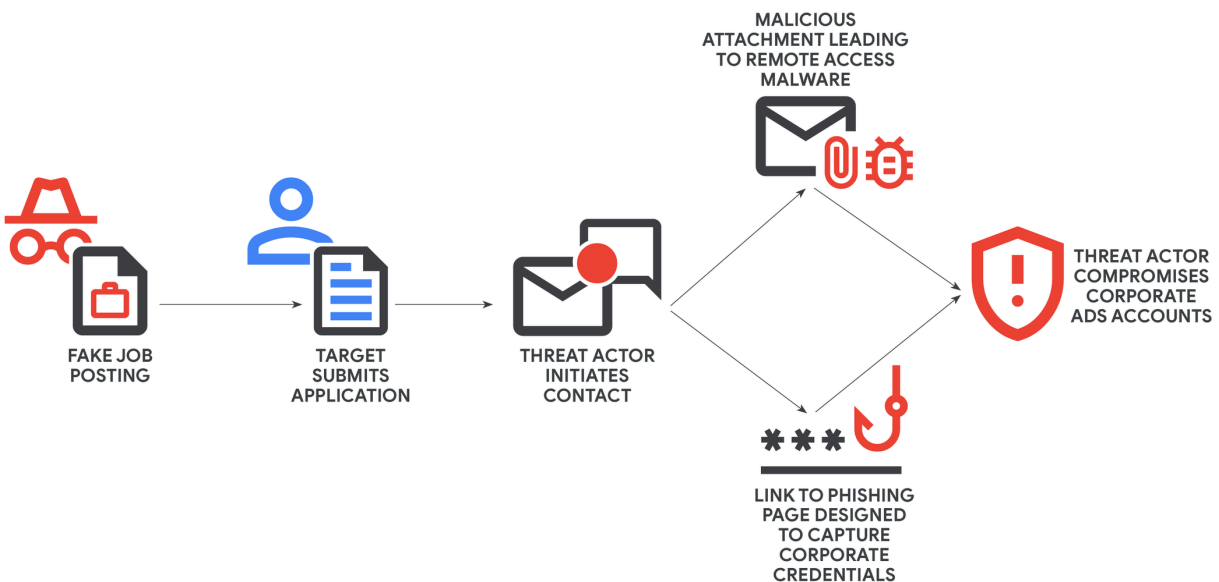
As part of our efforts to combat serious threat actors, GTIG uses the results of our research to improve the safety and security of Google's products and users. Upon discovery, all identified websites, domains and files are added to the [Safe Browsing](#) blocklist in order to protect web users across major browsers. We are committed to sharing our findings with the security community to raise awareness and to disrupt this activity. We hope that improved understanding of tactics and techniques will enhance threat hunting capabilities and lead to stronger user protections across the industry.

## Introduction

GTIG identified a persistent and targeted social engineering campaign operated by UNC6229, a financially motivated threat cluster assessed to be operating from Vietnam. This campaign exploits the trust inherent in the job application process by posting fake career opportunities on popular employment platforms, as well as freelance marketplaces and their own job posting websites. Applicants are lured into a multi-stage process that culminates in the delivery of either malware that allows remote access to the system or highly convincing phishing pages designed to harvest corporate credentials.

The primary targets appear to be individuals working in digital marketing and advertising. By targeting this demographic, UNC6229 increases its chances of compromising individuals who have legitimate access to high-value corporate advertising and social media accounts. The campaign is notable for its patient, victim-initiated social engineering, abuse of legitimate commercial software, and its targeted approach to specific industries.

## Campaign Overview: The "Fake Career" Lure



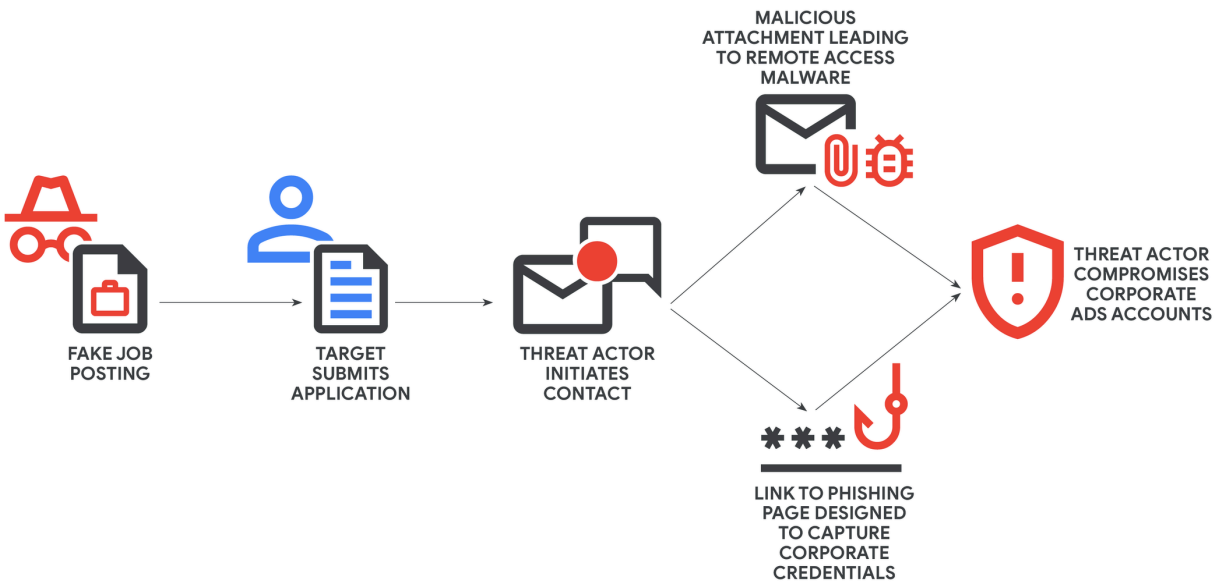


Figure 1: Attack flow

The effectiveness of this campaign hinges on a classic social engineering tactic where the victim initiates the first contact. UNC6229 creates fake company profiles, often masquerading as digital media agencies, on legitimate job platforms. They post attractive, often remote, job openings that appeal to their target demographic.

When an individual applies for one of these fake positions, they provide the actor with their name, contact information, and resume. This self-initiated action establishes a foundation of trust. When UNC6229 later contacts the applicant, the victim is more receptive, believing it to be a legitimate follow-up from a potential employer.

The vulnerability extends beyond the initial job application. The actor can retain the victim's information for future "cold emails" about other fabricated job opportunities or even sell the curated list of active job seekers to other attackers for similar abuse.

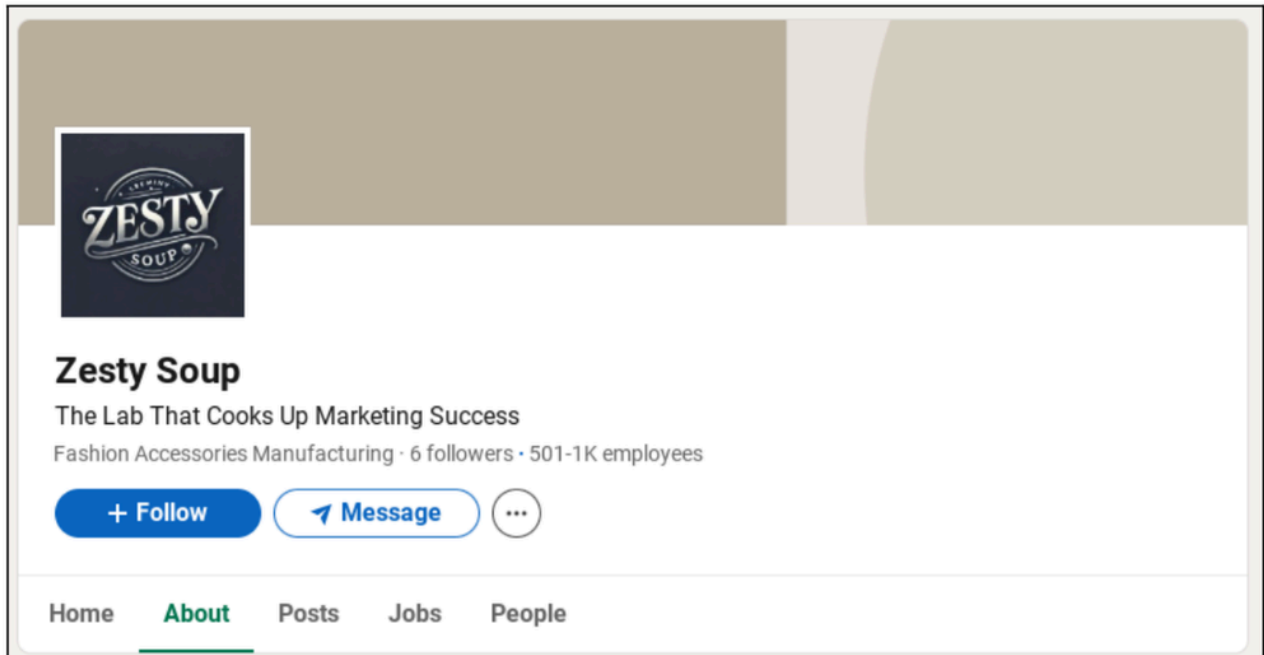
## Technical Analysis: The Attack Chain

Once a victim applies to a job posting, UNC6229 initiates contact, typically via email, but also through direct messaging platforms. In some cases the attackers also use commercial CRM tools that allow sending bulk emails. Depending on the campaign the attacker may send the victim an attachment with malware, a link to a website that hosts malware, or a link to a phishing page to schedule an interview.

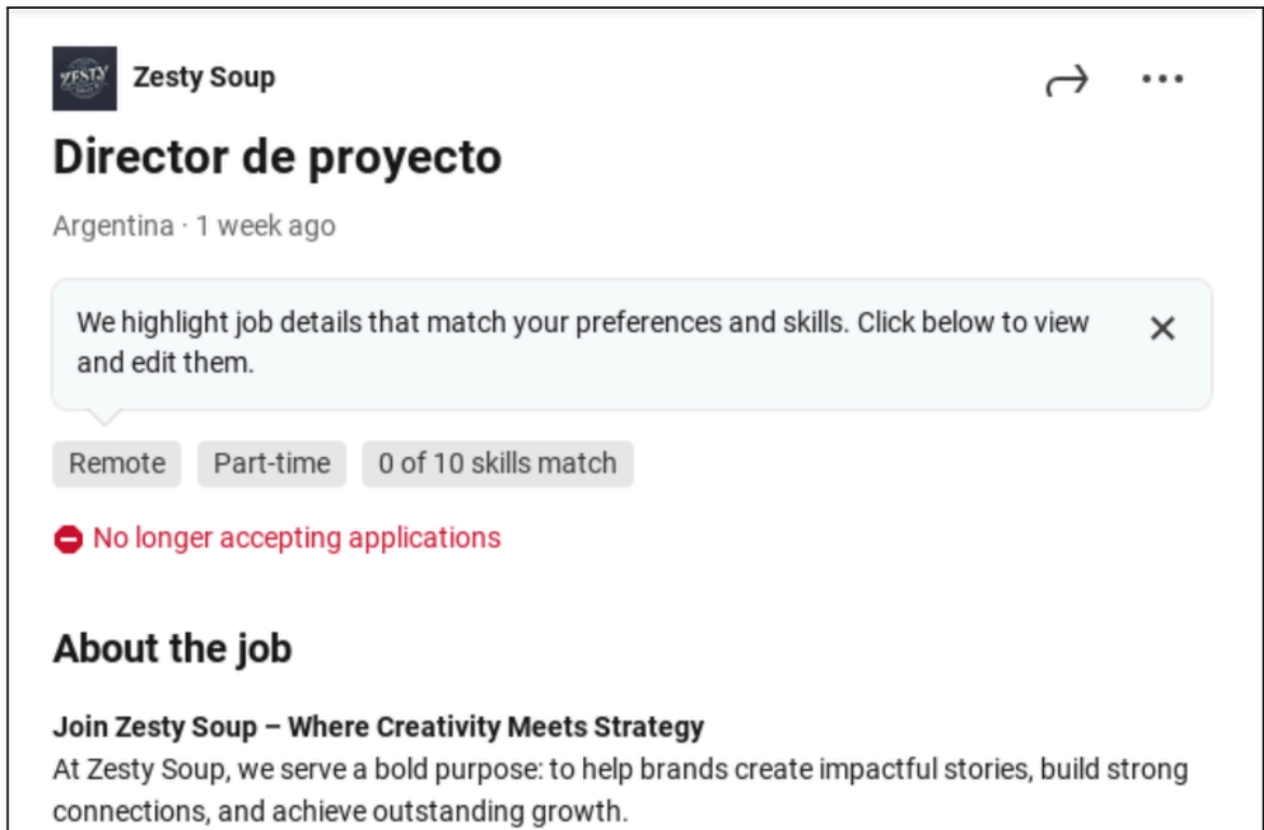
### 1. Fake Job Posting

Using fake job postings the attackers target specific industries and locations, posting jobs relevant to the digital advertising industry in specific regions. This same kind of targeting would work across any industry or

geographic location. The job postings are both on legitimate sites, as well as on websites created by the threat actors.



The screenshot shows the LinkedIn profile for Zesty Soup. The profile picture is a dark blue square with the Zesty Soup logo. The name 'Zesty Soup' is displayed in bold. Below the name is the tagline 'The Lab That Cooks Up Marketing Success' and the industry 'Fashion Accessories Manufacturing'. It also shows '6 followers' and '501-1K employees'. There are three buttons: '+ Follow', 'Message', and a three-dot menu. At the bottom, there are navigation tabs for 'Home', 'About', 'Posts', 'Jobs', and 'People', with 'About' being the active tab.



The screenshot shows a job posting for 'Director de proyecto' by Zesty Soup. The location is 'Argentina' and it was posted '1 week ago'. A light blue notification box states: 'We highlight job details that match your preferences and skills. Click below to view and edit them.' Below this are three tags: 'Remote', 'Part-time', and '0 of 10 skills match'. A red banner with a minus sign icon says 'No longer accepting applications'. The section is titled 'About the job' and contains the text: 'Join Zesty Soup – Where Creativity Meets Strategy' and 'At Zesty Soup, we serve a bold purpose: to help brands create impactful stories, build strong connections, and achieve outstanding growth.'

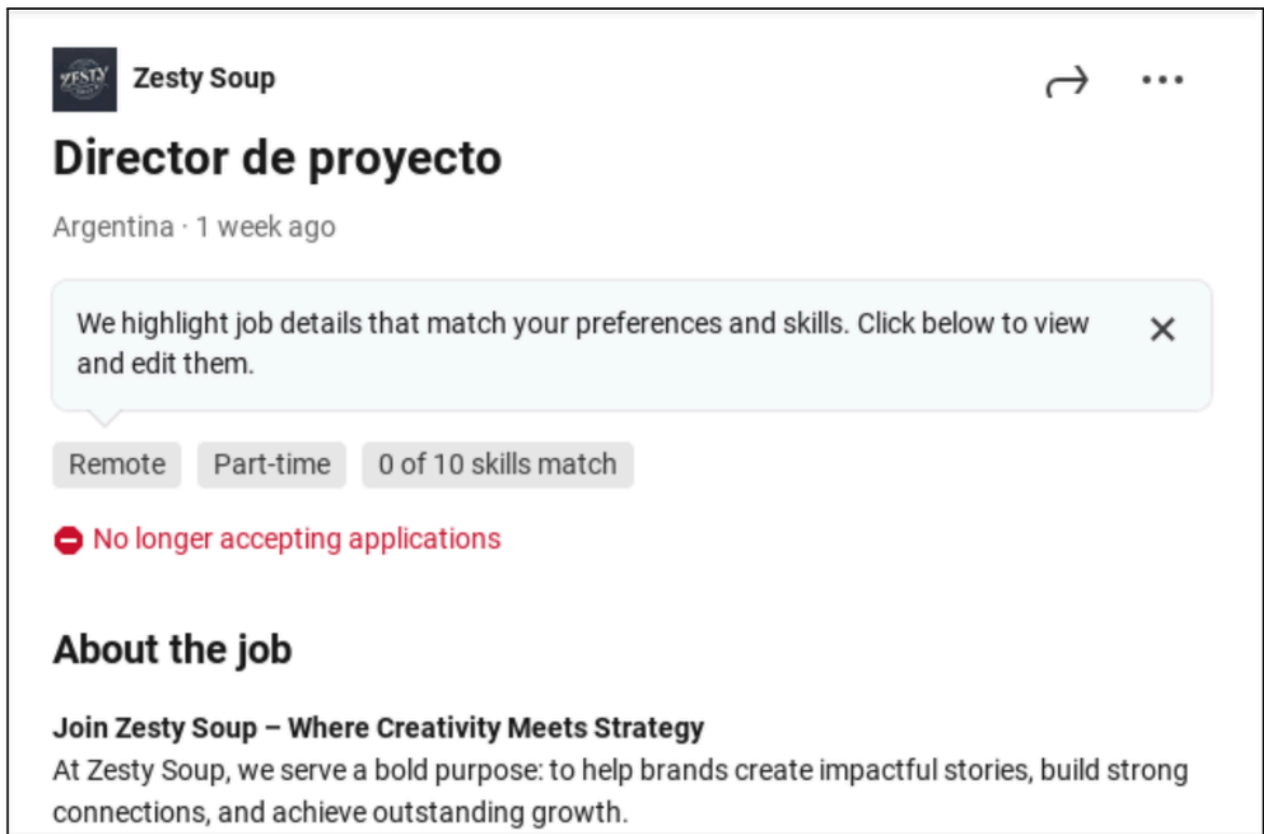
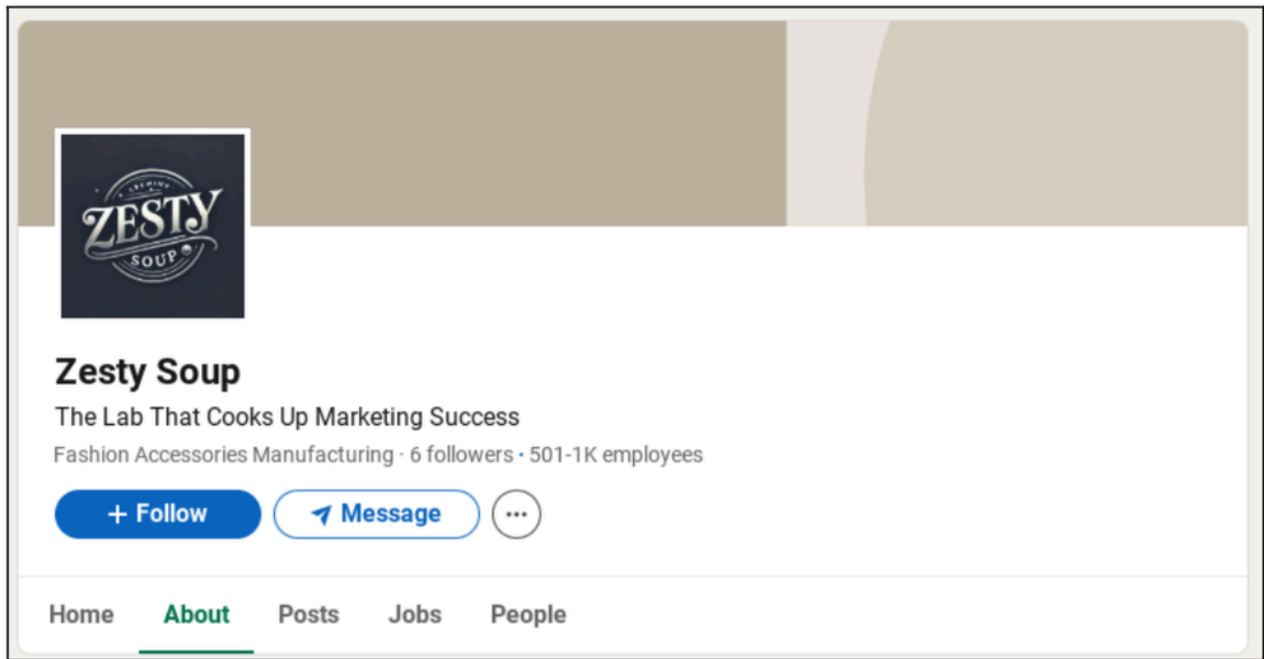


Figure 2: Screenshots of threat actors posting on LinkedIn

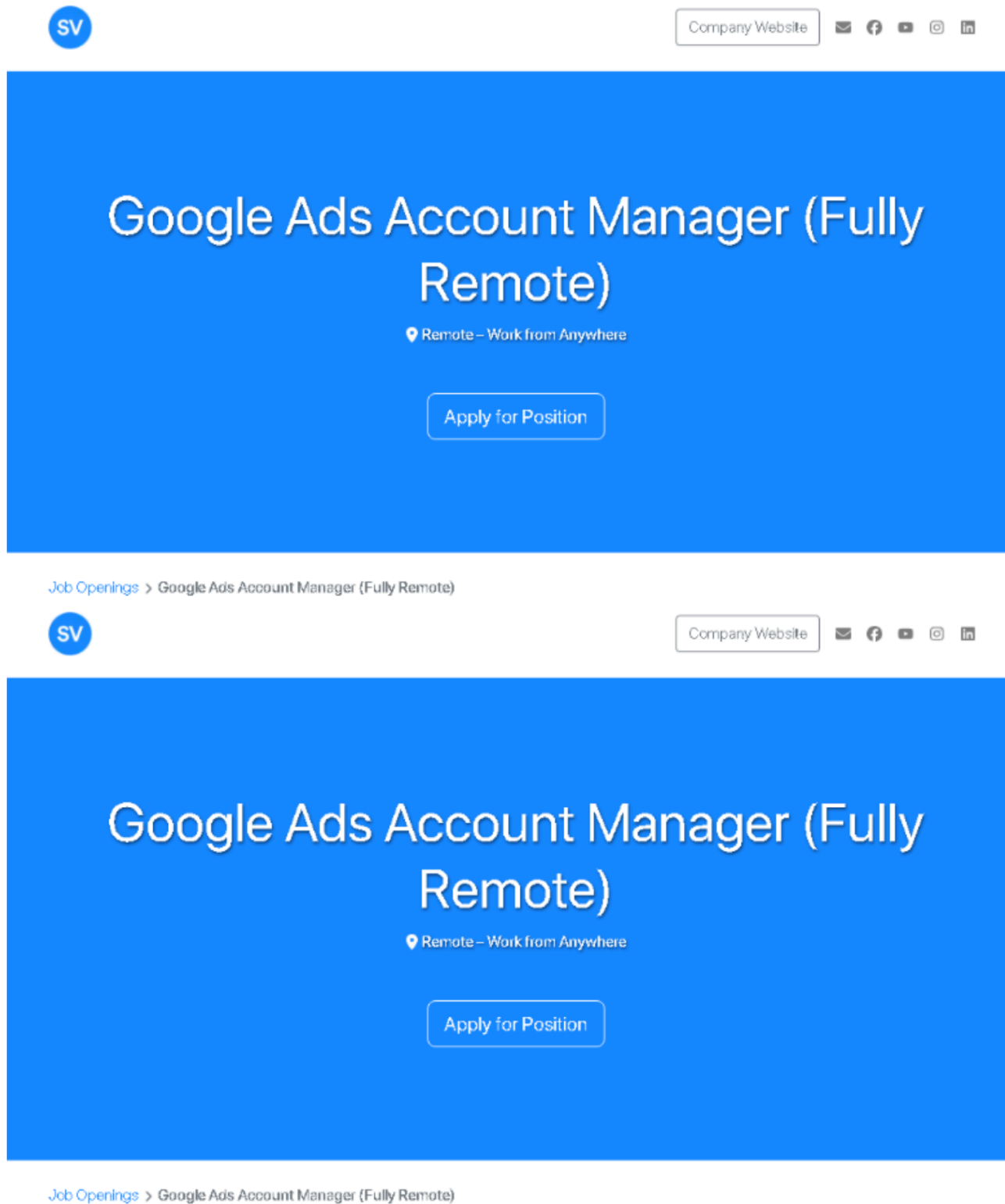


Figure 3: Attackers have set up their own fake job posting websites such as staffvirtual[.]website

## 2. Initial Contact and Infrastructure Abuse

Once a victim applies to a job posting, UNC6229 initiates contact, typically via email, but also through direct messaging platforms. The initial contact is often benign and personalized, referencing the job the victim

applied for and addressing the victim by name. This first contact typically does not contain any attachments or links, but is designed to elicit a response and further build rapport.

GTIG has observed UNC6229 and other threat actors abusing a wide range of legitimate business and customer relationship management (CRM) platforms to send these initial emails and manage their campaigns. By abusing these trusted services, the actor's emails are more likely to bypass security filters and appear legitimate to the victim. We've shared insights about these campaigns with CRMs UNC6229 has abused, including Salesforce, to better secure the ecosystem. We continue to disrupt these actors by blocking their use of Google products, including Google Groups and Google AppSheet.

### **3. Payload Delivery: Malware or Phishing**

After the victim responds, the actor proceeds to the payload delivery phase. Depending on the campaign the attacker may send the victim an attachment with malware or a link to a phishing page:

- **Malware Delivery:** The actor sends an attachment, often a password-protected ZIP file, claiming it is a skills test, an application form, or a required preliminary task. The victim is instructed that opening the file is a mandatory step in the hiring process. The payload often includes remote access trojans (RATs) that allow the actor to gain full control of the victim's device and subsequently take over their online accounts.
- **Phishing Link:** The actor sends a link, sometimes obfuscated with a URL shortener, directing the victim to a phishing page. This page is often presented as a portal to schedule an interview or complete an assessment.

The phishing pages are designed to be highly convincing, using the branding of major corporations. GTIG has analyzed multiple phishing kits associated with this threat activity and found that they are often configured to specifically target corporate email credentials and can handle various multi-factor authentication (MFA) schemes, including those from Okta and Microsoft.

### **Attribution**

GTIG assesses with high confidence that this activity is conducted by a cluster of financially motivated individuals located in Vietnam. The shared TTPs and infrastructure across multiple incidents suggest a collaborative environment where actors likely exchange tools and successful techniques on private forums.

### **Outlook**

The "fake career" social engineering tactic is a potent threat because it preys on fundamental human behaviors and the necessities of professional life. We expect UNC6229 and other actors to continue refining this approach, expanding their targeting to other industries where employees have access to valuable corporate assets. The abuse of legitimate SaaS and CRM platforms for malicious campaigns is a growing trend that challenges traditional detection methods.

### **Indicators of Compromise**

The following indicators of compromise are available to registered users in a [Google Threat Intelligence \(GTI\) collection](#).

staffvirtual[.]website
137a6e6f09cb38905ff5c4ffe4b8967a45313d93bf19e03f8abe8238d589fb42
33fc67b0daaffd81493818df4d58112def65138143cec9bd385ef164bb4ac8ab
35721350cf3810dd25e12b7ae2be3b11a4e079380bbbb8ca24689fb609929255
bc114aeaaa069e584da0a2b50c5ed6c36232a0058c9a4c2d7660e3c028359d81
e1ea0b557c3bda5c1332009628f37299766ac5886dda9aaf6bc902145c41fd10

Posted in

- [Threat Intelligence](#)