Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Vietnamese Actors Use Recruitment Lures for Espionage and Theft

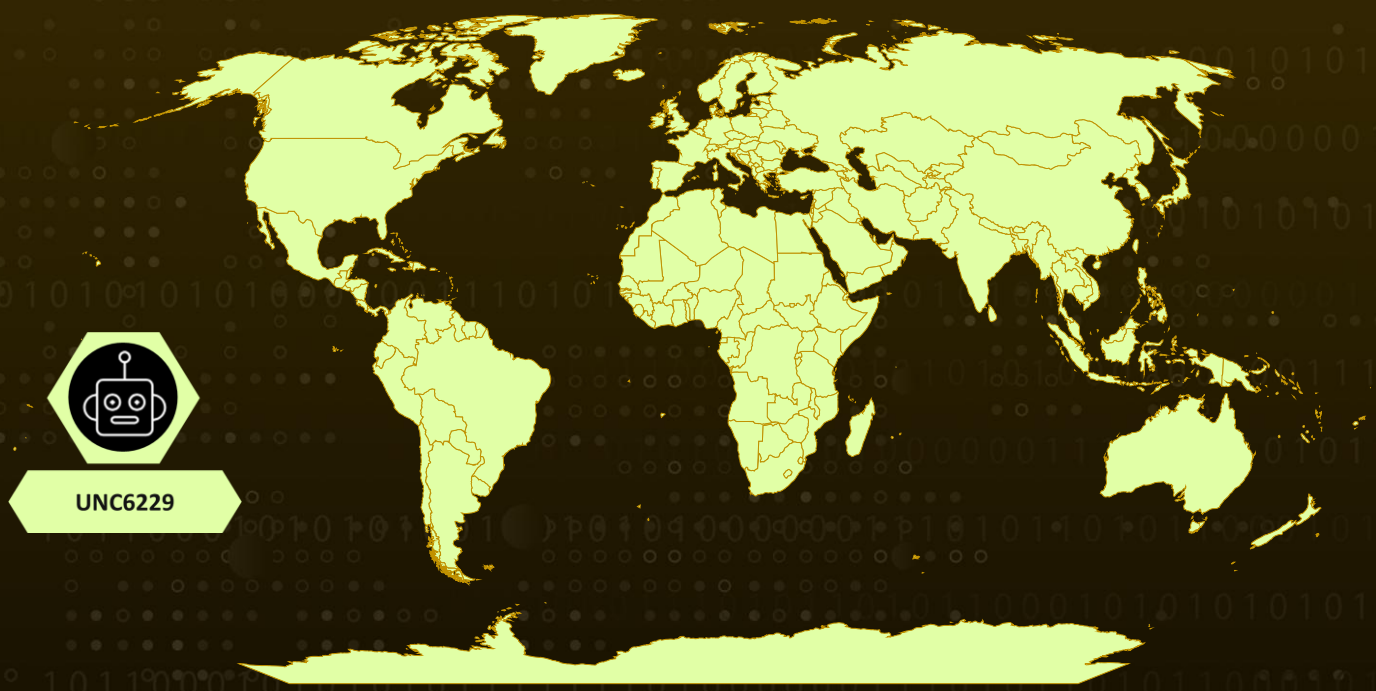
Date of Publication	Admiralty Code	TA Number
October 30, 2025	A1	TA2025332

Summary

Threat Actor: UNC6229
Targeted Region: Worldwide
Targeted Industries: Digital Advertising, Marketing

Attack: UNC6229, a financially motivated cybercrime group operating from Vietnam, targets professionals in digital advertising and marketing through fraudulent job postings on legitimate employment platforms and freelance marketplaces. Exploiting the trust of job seekers, the group executes advanced social engineering attacks to distribute malware and harvest credentials, enabling unauthorized access to corporate advertising and social media accounts.

Attack Regions



Attack Details

#1 UNC6229 is a financially motivated threat group operating from Vietnam, known for posting fraudulent job opportunities across major employment portals, freelance marketplaces, and attacker-controlled websites. The group conducts persistent and targeted social engineering campaigns aimed at compromising corporate advertising and social media accounts.

#2 The campaign begins when a target downloads and executes malware or submits credentials through a phishing site. If the victim is logged into a work computer with personal credentials or uses a personal device linked to company advertising accounts, the attackers can gain unauthorized access to corporate systems.

#3 Once access is achieved, the threat actors may sell advertising space, trade compromised accounts or monetize them through other illicit means. They may also retain victims' information to send future fraudulent job offers or sell curated lists of active job seekers to other malicious actors.

#4 The group initiates contact primarily through email, though direct messaging platforms and commercial CRM tools are also used to distribute bulk communications. Depending on the campaign, victims may receive an attachment containing malware, a link to a malicious website, or a phishing page disguised as an interview scheduler.

#5 In cases involving attachments, the file is often a password-protected ZIP archive presented as a skills test, application form, or preliminary hiring task. Victims are instructed to open the file as a required step in the recruitment process. These payloads frequently contain remote access trojans (RATs), granting full control over the victim's device and enabling account takeover.

#6 Alternatively, the attackers may send obfuscated links, commonly shortened URLs leading to phishing pages that mimic legitimate portals for interviews or assessments. The increasing abuse of trusted SaaS and CRM platforms for such malicious campaigns poses a significant challenge to conventional detection mechanisms.

Recommendations

Restrict Personal Account Access on Work Devices: Enforce strict separation between personal and corporate accounts. Prevent employees from logging into personal email or social media accounts from company systems to limit exposure pathways.

Monitor for Anomalous Access to Advertising Accounts: Establish continuous monitoring of corporate advertising and social media platforms for unusual login locations, behavioral anomalies, or unauthorized configuration changes.

Restrict File Execution Privileges: Limit execution of downloaded files from external sources. Use application allow-listing to prevent unapproved executables, particularly compressed or password-protected files, from being run.

Implement DNS and URL Filtering: Block access to malicious domains, shortened URLs, and known phishing infrastructure. Use threat intelligence-driven domain reputation services to update blocklists in real time.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0040 Impact	TA0043 Reconnaissance	TA0042 Resource Development	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File

T1212 Exploitation for Credential Access	T1078 Valid Accounts	T1219 Remote Access Software	T1036 Masquerading
T1608 Stage Capabilities	T1608.004 Drive-by Target	T1098 Account Manipulation	T1199 Trusted Relationship
T1586 Compromise Accounts	T1586.001 Social Media Accounts	T1657 Financial Theft	T1531 Account Access Removal
T1667 Email Bombing	T1589 Gather Victim Identity Information	T1589.001 Credentials	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	staffvirtual[.]website
SHA256	137a6e6f09cb38905ff5c4ffe4b8967a45313d93bf19e03f8abe8238d589fb42, 33fc67b0daaffd81493818df4d58112def65138143cec9bd385ef164bb4ac8ab, 35721350cf3810dd25e12b7ae2be3b11a4e079380bbbb8ca24689fb609929255, bc114aeaaa069e584da0a2b50c5ed6c36232a0058c9a4c2d7660e3c028359d81, e1ea0b557c3bda5c1332009628f37299766ac5886dda9aaf6bc902145c41fd10

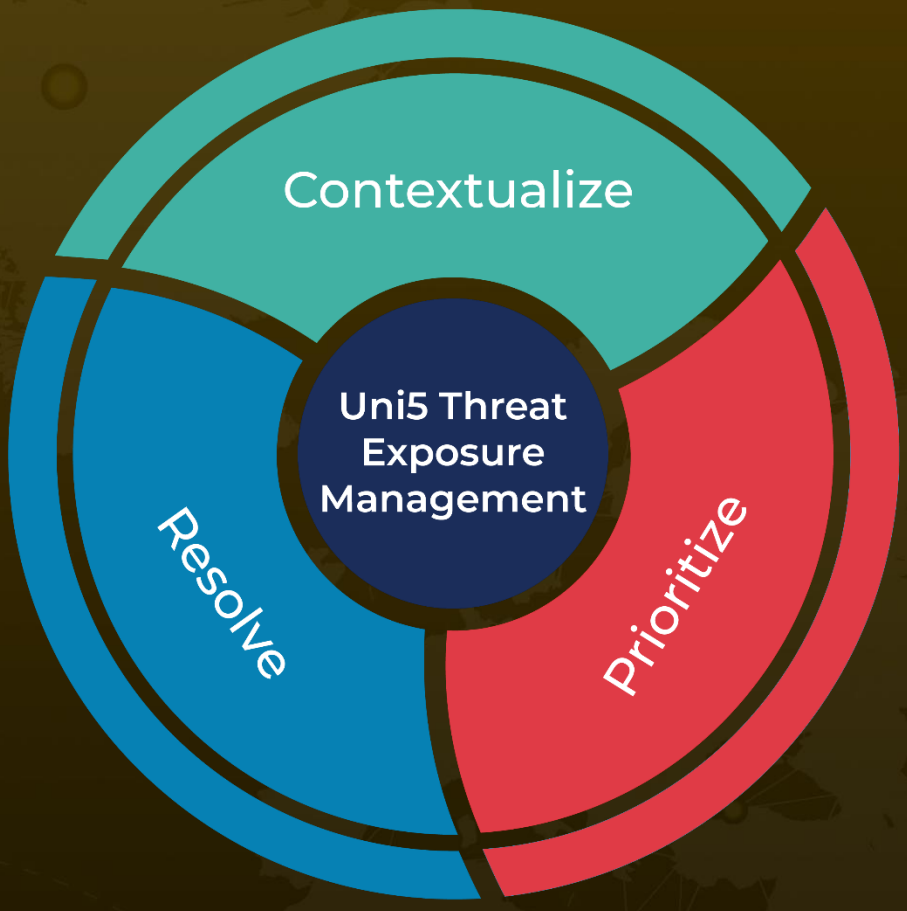
References

https://cloud.google.com/blog/topics/threat-intelligence/vietnamese-actors-fake-job-posting-campaigns

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 30, 2025 . 7:30 AM

More at www.hivepro.com