Fake North Korean IT Worker Linked to BeaverTail Video Conference App Phishing Attack

By Unit 42

Published: 2024-11-14 · Archived: 2026-04-05 16:46:19 UTC

Executive Summary

Unit 42 researchers identified a North Korean IT worker activity cluster that we track as CL-STA-0237. This cluster was involved in recent phishing attacks using malware-infected video conference apps. It likely operates from Laos, using Lao IP addresses and identities.

CL-STA-0237 exploited a U.S.-based, small-and-medium-sized business (SMB) IT services company to apply for other jobs. In 2022, CL-STA-0237 secured a position at a major tech company.

We believe CL-STA-0237 is another cluster of a broader network of North Korean IT workers supporting the nation's illicit activities, including weapons of mass destruction (WMD) and ballistic missile programs. This article highlights the IT workers' shift from stable income-seeking activities to involvement in more aggressive malware campaigns. Additionally, the article illustrates the global reach of North Korean IT workers.

To address these risks, organizations should perform the following activities:

- Strengthening their hiring screening processes
- Implementing robust monitoring to identify insider threats
- Thoroughly evaluating outsourced services
- Ensuring that employees do not use corporate machines for personal activities

Palo Alto Networks customers receive better protection from malware discussed in this article through Cortex XDR and XSIAM and Prisma Cloud. Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with this activity as malicious.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Updated Contagious Interview Campaign Tactics

In a previous article, we covered the Contagious Interview campaign where North Korean threat actors posed as fake employers reaching out to IT developers with fictitious job offers and conducted technical interviews. During these interviews, attackers delivered npm (a package manager for the JavaScript programming language) projects with malicious content, which led to BeaverTail malware infections. Attackers then deployed InvisibleFerret malware, which includes additional remote access Trojan (RAT) features.

In addition to the recently published reports from The Object-See Foundation and GROUP-IB on the Contagious Interview campaign's updated TTPs, Unit 42 has released a new report that highlights the latest developments surrounding the BeaverTail malware. These reports delve into how threat actors set up fake video conferencing websites imitating MiroTalk and FreeConference. Attackers lured targets into downloading conference call installers embedded with BeaverTail malware.

This new approach differs from previous tactics in that malware delivery occurs at the start of the job interview, using installer packages. This method allows attackers to target a broader range of job seekers, rather than only those with npm JavaScript development expertise and specific machine configurations.

Our investigation into this updated campaign led to the identification of the fake North Korean IT worker cluster we are focusing on in this research. This is the second instance where we have observed connections between the Contagious Interview malware campaign and North Korean IT worker activities, also known as the Wagemole campaign. In the Wagemole campaign, North Korean IT workers pose as job seekers, often freelance developers, and they seek remote IT jobs using stolen identities.

Fake North Korean IT Worker CL-STA-0237 Linked to the Phishing Attack

Our internal telemetry identified newly registered domains resolving to a known IP address, 167.88.36[.]13, which is associated with the MiroTalk fake job campaign from July 2024 discussed above. Further investigation revealed that the CL-STA-0237 activity cluster, which registered these domains, used information from a U.S.-based SMB IT services company.

CL-STA-0237 not only exploited the company's information but also controlled multiple IT infrastructure and management accounts that belonged to the company. CL-STA-0237 listed the company as its employer, citing employment since 2019 in some of its fake resumes. It also managed email accounts that mimicked the company's owner, using them to apply for other jobs.

We could not fully verify the connections between CL-STA-0237 and the exploited company. Our hypothesis suggests two potential scenarios:

- CL-STA-0237 stole the company's access credentials and is now posing as the company to secure new IT jobs or target job seekers with malware infections.
- CL-STA-0237 was either hired by or had an outsourcing partnership with the IT services company, which allowed it to gain access to the company's infrastructure.

Fake Resumes Created by the Actor

In the Wagemole campaign, North Korean IT workers commonly managed multiple personas using fake or stolen identities from around the world. Figure 1 shows fake resumes created by CL-STA-0237.

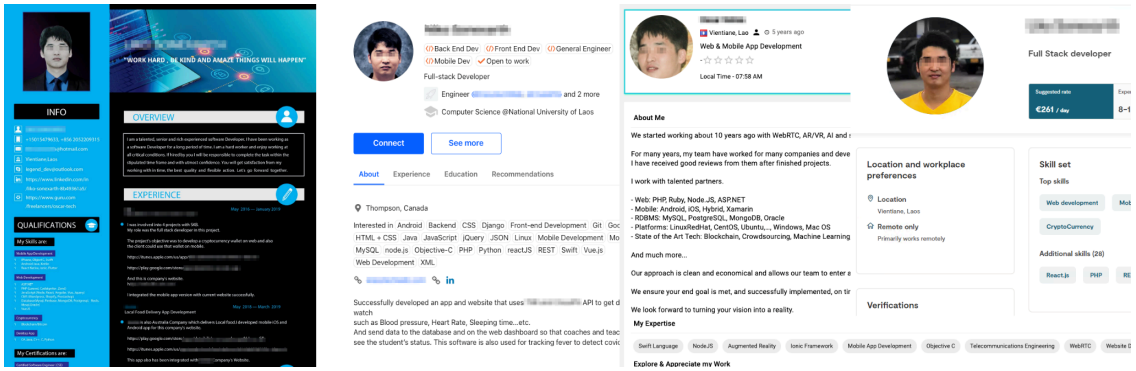

Figure 1. Fake resumes created by CL-STA-0237.

Although the headshot photos differ slightly, they appear to be different pictures of the same individual. With moderate confidence, we believe these headshots belong to a real member of CL-STA-0237, as they are likely required to show their face during video conference calls with employers or clients.

Possible Physical Presence in Laos

Tracing CL-STA-0237's activities revealed the use of multiple Lao residential IP addresses. Criminals commonly use residential proxy services, so the use of such IP addresses alone does not provide strong evidence of physical presence.

However, we were able to verify that one of the threat actor's headshot photos in Figure 2 was taken at a shopping mall in Vientiane, Laos, between late 2020 and mid-2021.

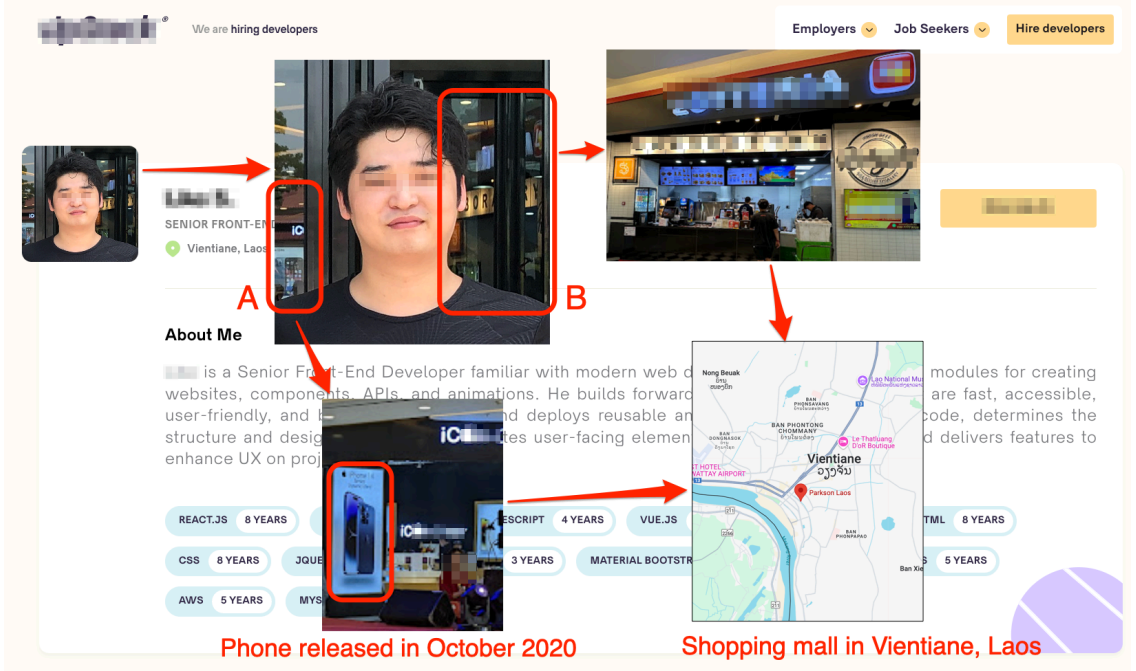

Figure 2. Tracing the geolocation and timeframe of CL-STA-0237.

The A and B sections of the background of the IT worker's headshot photo in Figure 2 strongly indicated that it was taken in a shopping mall. Additionally, an advertisement for a phone model released in late 2020 suggested the time frame in which the picture was taken.

Considering these factors, along with Laos being one of the countries where North Korean IT workers have been dispatched, it is plausible that CL-STA-0237 may have had a physical presence in Laos. In contrast, previous Wagemole campaign clusters were primarily linked to IP infrastructures based in China and Russia.

Securing a Job at a Major Tech Company

The intelligence we gathered on CL-STA-0237 suggests that it secured multiple short-term and long-term jobs from companies of various sizes. We believe, with moderate confidence, that CL-STA-0237 secured a position in at least one major tech company in 2022.

CL-STA-0237 had access to the company's single sign-on (SSO) system, with an account created under the company’s domain. We believe this account was created for the North Korean IT worker rather than stolen, as the username corresponds to one of the fake identities CL-STA-0237 has been using in its fake IT worker operation.

Attribution

Since our previous report on the two job-related campaigns, some researchers have begun attributing the Contagious Interview campaign to the well-known North Korean threat group, Lazarus. However, we are not certain whether the IT workers led the attacks or simply assisted other hacking groups. Despite this uncertainty, we continue to observe links between malware campaigns and North Korean IT workers, thus we track these activities under our temporary cluster names.

On the other hand, there have been new developments regarding the attribution of the Wagemole campaign. Ethereum wallets associated with one of the Wagemole clusters showed significant fund transfers to a wallet belonging to Sang Man Kim.

Kim is a North Korean individual sanctioned by the U.S. Treasury for his role in supporting North Korea's illicit activities, including its WMD and ballistic missile programs. Kim is specifically linked to managing the finances of overseas North Korean IT workers in Russia and Laos, providing a potential connection to the campaign's financial operations.

Conclusion

North Korean threat actors have been highly successful in generating revenue to fund their nation’s illicit activities. They began by posing as fake IT workers to secure consistent income streams, but they have begun transitioning into more aggressive roles, including participating in insider threats and malware attacks.

The continuous discovery of such operations highlights the vast scale of the threat. Despite numerous reports, media coverage and law enforcement efforts, these campaigns have not diminished. We anticipate that North Korean job-related campaigns will likely persist and even escalate.

To mitigate these risks, organizations must enhance their screening processes for new hires. This includes the following activities:

- Bolstering monitoring to detect insider threats
- Carefully vetting outsourced services

- Ensuring that employees do not use corporate machines for personal activities

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Cortex XDR and XSIAM customers, users of both cloud and on-premises agents, receive protections out-of-the-box. Cortex's XSIAM AI-assisted operations centralize data and SOC detection and response capabilities, providing protections from the advanced threats described in this article.
- Prisma Cloud customers are protected out-of-the-box should the infection chains discussed within this article expose cloud infrastructure. Prisma Cloud monitors CI/CD pipelines, Cloud Secret Managers, Infrastructure as Code (IaC) templates and Software Composition to ensure that malicious execution, creation, modification or deletion of cloud resources are detected and remediated.
- Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with this activity as malicious

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Domains

- effertz-carroll[.]com
- regioncheck[.]net
- freeconference[.]io
- ipcheck[.]cloud
- mirotalk[.]io
- mirotalk[.]net
- ftpserver0909[.]com

IP Address

- 167.88.36[.]13

Email Addresses

- adonis_eros@outlook[.]com

- brightstar1116@outlook[.]com
- buyerlao@outlook[.]com
- casey_qadir@outlook[.]com
- cescernand@outlook[.]com
- devstar1116@gmail[.]com
- ebcappservices@gmail[.]com
- hakajakin@outlook[.]com
- ideationbrand@gmail[.]com
- legend_dev@outlook[.]com
- liko.sonexarth@gmail[.]com
- liko.sonexarth@hotmail[.]com
- longines0924@gmail[.]com
- lujindane@outlook[.]com
- matthewhall14541@gmail[.]com
- niko.sonexarth@gmail[.]com
- niko.sonexarth@hotmail[.]com
- oscar.vetres127@europe[.]com
- oscar.vetres127@gmail[.]com
- pinefirst@outlook[.]com
- reply9998@gmail[.]com
- richard.stewart.1202@gmail[.]com
- richard.stewart.1202@outlook[.]com
- sniper_bruce@outlook[.]com
- stp.walsh33@gmail[.]com
- techcare127@gmail[.]com
- truepai415@gmail[.]com
- truestar222@outlook[.]com
- volodimir.work2020@gmail[.]com
- zhangming_k@yahoo[.]com
- zhuming1116@gmail[.]com
- lisettekolson8@gmail[.]com
- 312011217@qq[.]com
- alhinglovena3000@gmail[.]com
- jumphon2103@gmail[.]com
- mobilephetjum@gmail[.]com
- phetchamphone1998@gmail[.]com

Additional Resources

- Global Companies Are Unknowingly Paying North Koreans: Here's How to Catch Them – Unit 42, Palo Alto Networks
- Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors – Unit 42, Palo Alto Networks

- Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware – Unit 42, Palo Alto Networks
- This Meeting Should Have Been an Email - A DPRK stealer, dubbed BeaverTail, targets users via a trojanized meeting app – Objective-See Foundation
- APT Lazarus: Eager Crypto Beavers, Video calls and Games – GROUP-IB
- Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities – Press release, U.S. Department of the Treasury

---