Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

North Korean Hackers Go After Remote Job Openings

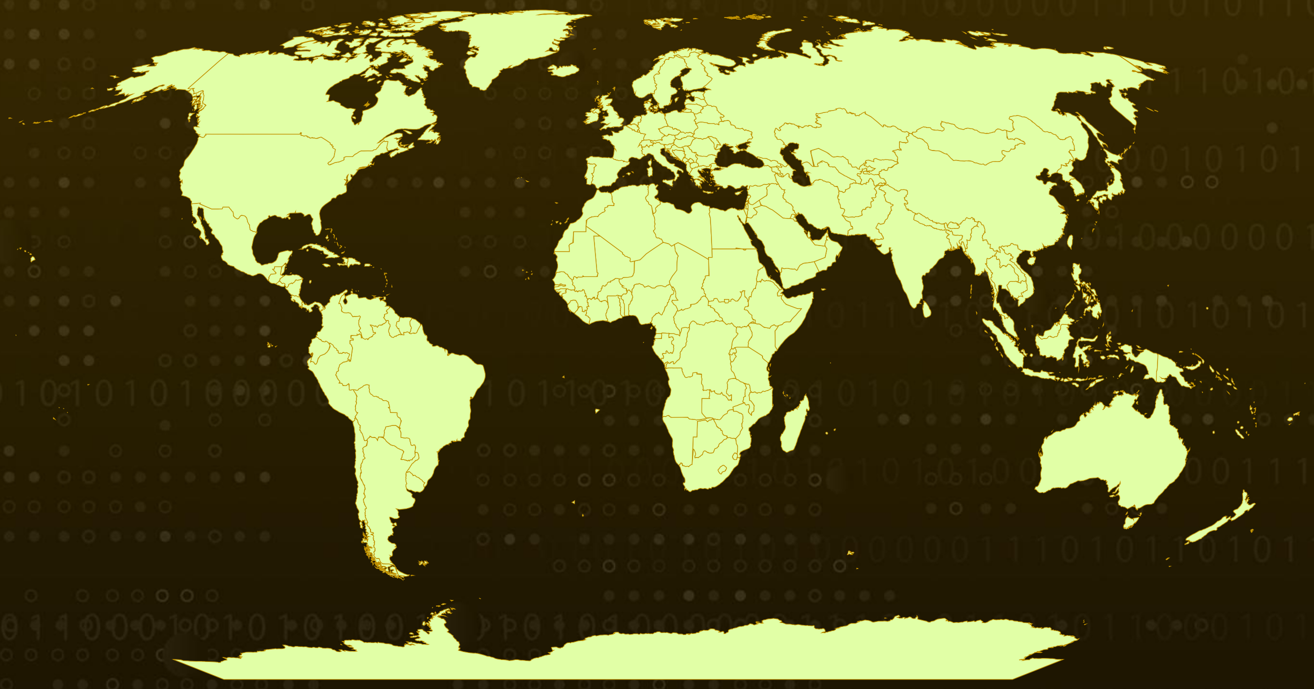
Date of Publication	Admiralty Code	TA Number
November 8, 2024	A1	TA2024423

Summary

Attack Commenced: November 2023
Campaigns: Contagious Interview and WageMole
Malware: BeaverTail, InvisibleFerret
Affected Platforms: Windows, macOS
Targeted Region: Worldwide

Attack: North Korean threat actors behind the Contagious Interview and WageMole campaigns have upgraded their techniques, using advanced obfuscation to avoid detection and targeting both Windows and macOS devices.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 North Korean threat actors behind the Contagious Interview and WageMole campaigns have upgraded their techniques, improving script obfuscation to evade detection and expanding support for both Windows and macOS application formats within their infection chains. These actors have compromised over 100 devices across multiple operating systems in a short timeframe.

#2 In the Contagious Interview campaign, unsuspecting applicants are drawn in by fraudulent job postings that require them to complete coding tasks on GitHub, where the attackers control the repository. This repository hosts malicious JavaScript code, known as 'BeaverTail,' which is used to establish fake identities and secure remote positions in the WageMole campaign.

#3 WageMole targets remote roles to infiltrate companies and potentially exfiltrate data, using automation to apply for positions like web developer or engineer on job platforms such as LinkedIn. These campaigns have led to the theft of source code, cryptocurrency data, and personal information.

#4 'BeaverTail' now incorporates advanced JavaScript obfuscation and is capable of downloading additional primary backdoor InvisibleFerret and a browser data-stealing script. The latest version of 'InvisibleFerret' features an upgraded remote monitoring and management (RMM) configuration, along with customized persistence mechanisms tailored to each operating system.

Recommendations

Harden Data Protection Policies: Enforce encryption on all files containing sensitive information, especially on shared drives or personal devices. Use role-based access control (RBAC) to limit folder access for personal data or credentials to authorized users only.

Strengthen Execution Controls: Implement Application Whitelisting and use application control software to allow only trusted and authorized applications to run on devices.

Ensuring Secure Onboarding by Verifying and Controlling Access: Verify the candidate's employment history by directly contacting previous employers to confirm roles, dates, and tenure. Conduct comprehensive background checks, including education, employment history, and certifications, to ensure integrity. Restrict new hires' access to sensitive information and systems until they complete their probationary period.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1041 Exfiltration Over C2 Channel	T1566 Phishing	T1566.003 Spearphishing via Service
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1059.006 Python	T1204 User Execution
T1204.002 Malicious File	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File	T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers	T1083 File and Directory Discovery	T1082 System Information Discovery	T1560 Archive Collected Data
T1560.001 Archive via Utility	T1005 Data from Local System	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1071.002 File Transfer Protocols	T1219 Remote Access Software		

Indicators of Compromise (IOCs)

TYPE	VALUE
Emails	MariuszKrol831[@]proton[.]me, Michael[.]dev314[@]gmail[.]com, MichaelAguilar[@]hotmail[.]com, adreabello[@]outlook[.]com, aguilarmichael314[@]proton[.]me, aktermorsheda469[@]gmail[.]com, bengrhimteh[@]gmail[.]com, blackstar9413[@]outlook[.]com, boye11251[@]gmail[.]com, codekings555[@]proton[.]me, cooldev626[@]gmail[.]com, devprince626[@]gmail[.]com, diachukoleksandr1[@]outlook[.]com, freelancermorshed123[@]gmail[.]com, goldenstar9393[@]gmail[.]com, goldenstar9393[@]outlook[.]com, greentree09288[@]gmail[.]com, greentree619[@]outlook[.]com, happystar555[@]outlook[.]com, marcog9912[@]outlook[.]com, prad[.]l936[@]proton[.]me, pradlash[@]outlook[.]com, pradlashodoski626[@]outlook[.]com, pradlashodoski[@]gmail[.]com, pradlashososki626[@]outlook[.]com, pradlashososki[@]outlook[.]com, praythelord0707[@]gmail[.]com , rakibvaihi538[.]com[@]gmail[.]com, rskvzw52056[.]com[@]gmail[.]com, smartcool319[@]gmail[.]com, smartkings626[@]gmail[.]com, soc888hailey[@]hotmail[.]com
URLs	hxxps[:]//github[.]com/goldenstar9393, hxxps[:]//github[.]com/TrustworthyDev, hxxps[:]//github[.]com/hermes1108, hxxps[:]//github[.]com/Stormer0528, hxxps[:]//github[.]com/CodeCraze25, hxxps[:]//github[.]com/gho555/, hxxps[:]//github[.]com/rot0505, hxxps[:]//github[.]com/CoffeeFam84, hxxps[:]//github[.]com/DevSCNinja, hxxps[:]//github[.]com/xbtasvs,

TYPE	VALUE
URLs	hxxps[:]//github[.]com/minatodev0421 hxxps[:]//www.linkedin[.]com/in/frank-schoneberg-a089832a4/, hxxps[:]//www.linkedin[.]com/in/logan-collins-374404306/, hxxps[:]//www.linkedin[.]com/in/adam-song05/
MD5	ae83d8531717a5c7696451166acc91f1, 3b7663f40ab4aa25a97bea17ad1b50eb, f5e89d2643a1e709f6f34f13b2501779, 47ebe86edb2a8305e48e142389ad5cd0, 4aea29dadcfd4fc75a27c9902cb4c623, 72841d2374648bc70dce53fbdcf69502, 1aaf8809b7ab4fa6848babe3f970afc0, 9cc9b773fe099d46eca556b610fd03cb, 0d4a9a974c4fc579d0699764c69cf0fd, 2ad64d0252b9778bdf3911e2924a3885, dee7ae804679b905b07953aa61136d2e, f713c6aa854c50854e4cac3e541be8cf, fdcc957f3b0050fcf351d99bcc4743b2, e23b3f3cea6e8c97ea67ad97b0dc2170, dee6eec3f11a3ba187a002eabfb7af3c, ab4138a74a42c8b83daf7c19587bb001, 61e07d69fbc48fb5c09503f926994636, 55cd5526fde209aea11bb41af0eb5c08, 2300548f253aea742d3b11925fa408d3, 41b0bb86e6409c08a298888dd7a91717, 30fbbceb33dbe40f50d3cb94714054fb, 8ed2ebb511e4436232b09991627790db, 43ae3120db22521a97e21b9c6ef13715, efed4ae29e74b01a11a746671fbd924d, d86f70735c7d53b315a35ddc29258476

References

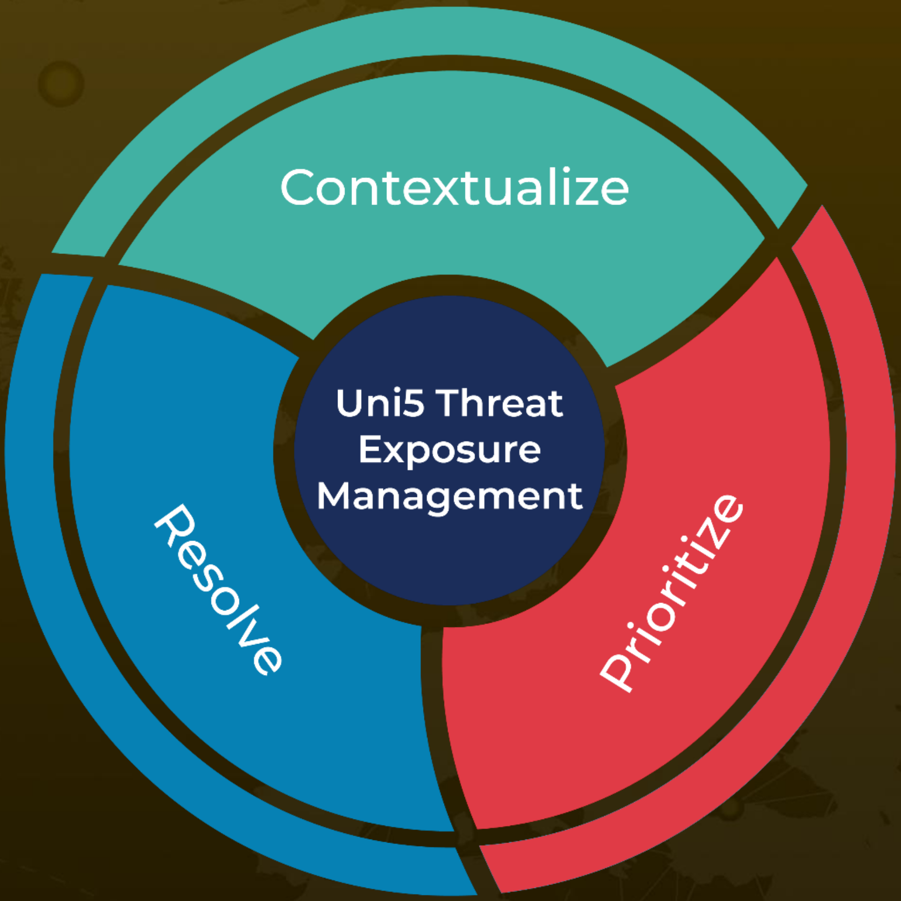
https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

https://hivepro.com/threat-advisory/devpopper-the-north-korean-cyber-threat-hiding-in-job-offers/

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

November 8, 2024 • 6:00 AM

More at www.hivepro.com