Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

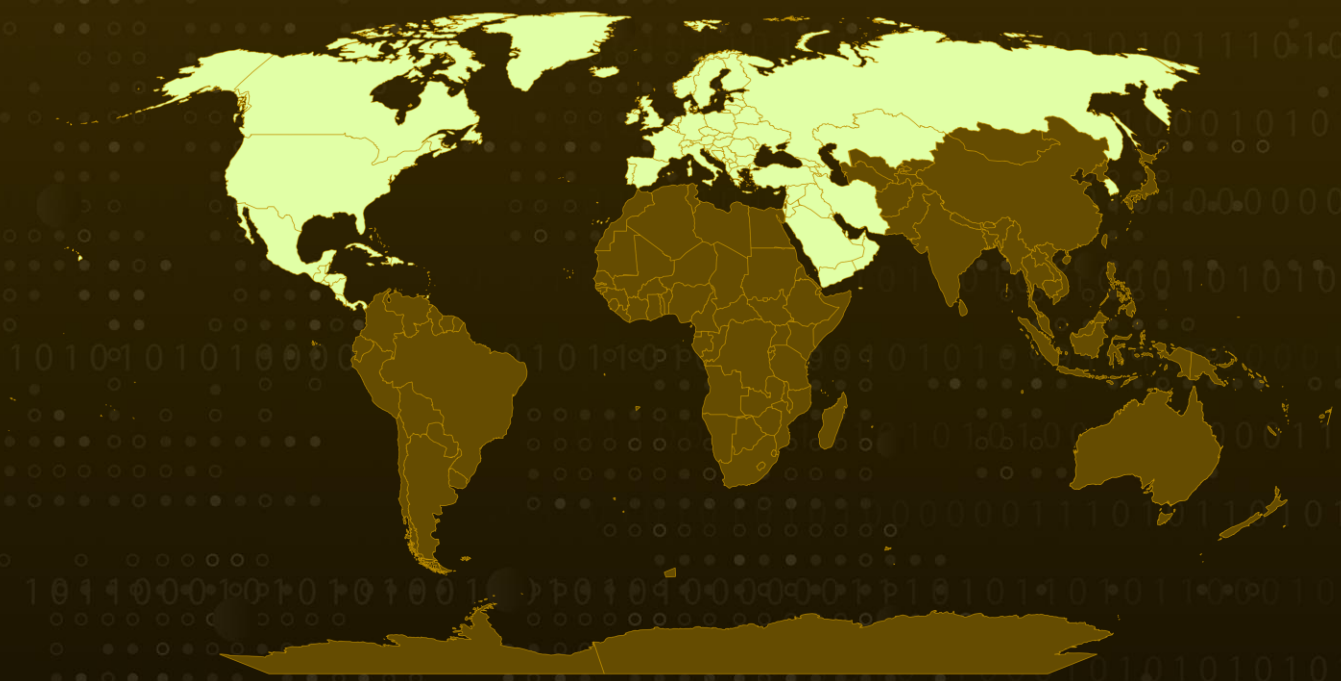
DEV#POPPER the North Korean Cyber Threat Hiding in Job Offers

Date of Publication	Admiralty Code	TA Number
August 2, 2024	A1	TA2024291

Summary

Campaign: DEV#POPPER
Malware: BeaverTail, InvisibleFerret Backdoor
Affected OS: Linux, Windows, and macOS
Targeted Regions: South Korea, North America, Europe, and the Middle East
Attack: The DEV#POPPER campaign, targeting software developers, has been identified with malware variants associated with North Korean threat actors. These actors employ advanced and covert malicious code execution techniques with significantly enhanced capabilities. The extent to which the threat actors go to execute their social engineering scheme in this attack is remarkably audacious.

Attack Regions



Attack Details

#1 An ongoing malware campaign targeting software developers, dubbed the DEV#POPPER campaign, has been identified with malware variants linked to North Korean threat actors. These actors employ stealthy malicious code execution tactics with significantly enhanced capabilities.

#2 The victims are primarily located in South Korea, North America, Europe, and the Middle East, demonstrating the widespread impact of the attack. The threat actors have expanded their target pool by incorporating support for Windows, Linux, and macOS.

#3 The threat actors disguise themselves as interviewers for developer positions and provide candidates with a ZIP file package containing an updated version of malware called BeaverTail, presented as part of a practical interview task. When the candidate extracts and executes the contents, a well-hidden line of JavaScript code is triggered, initiating the infection chain.

#4 The ZIP file contains numerous legitimate files, making it challenging to detect any foul play. The malicious code is concealed in a seemingly innocuous JavaScript file, heavily obfuscated, and utilizing multiple techniques to mask its true functionality, primarily designed for handling server connections. It starts by identifying the platform, constructing paths and variables, and then calling appropriate extraction functions based on the detected OS.

#5 Other functions manage sending stolen data to the command and control (C2) server, collecting system and geolocation information, and assigning unique identifiers to each compromised host. Additional functions handle downloading next-stage payloads and performing directory traversal, including filters to exclude specific files and directories from extraction. Post-exploitation scripts, such as a Python backdoor known as InvisibleFerret, are deployed to steal browser-stored passwords and credit card information, significantly enhancing the malware's data-harvesting capabilities.

Recommendations

Remain Alert During Job Interviews: Job interviews can be intense and stressful, but it is essential to maintain a vigilant, security-oriented mindset. Exercise caution with any requests or tasks that seem atypical or out of the ordinary. If something appears suspicious, it is prudent to err on the side of caution and decline to comply.

Implement Anti-Virus Solutions: Utilize Anti-Virus solutions to monitor and respond to suspicious activities on endpoints, providing real-time detection and automated responses to potential threats.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1560 Archive Collected Data	**T1132** Data Encoding	**T1027** Obfuscated Files or Information	**T1027.010** Command Obfuscation
T1070 Indicator Removal	**T1070.004** File Deletion	**T1033** System Owner/User Discovery	**T1082** System Information Discovery
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1059.006** Python
T1041 Exfiltration Over C2 Channel	**T1036** Masquerading	**T1056** Input Capture	**T1005** Data from Local System
T1555.003 Credentials from Web Browsers	**T1555** Credentials from Password Stores	**T1539** Steal Web Session Cookie	**T1059.007** JavaScript
T1056.001 Keylogging	**T1115** Clipboard Data		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	67[.]203[.]7[.]171, 77[.]37[.]37[.]81, 147[.]124[.]214[.]131, 173[.]211[.]106[.]101
URL	hxxp[:]//de[.]ztec[.]store[:]8000
File Name	onlinestoreforhirog.zip, printfulRoute.js
SHA256	6263b94884726751bf4de6f1a4dc309fb19f29b53cce0d5ec521a6c0f5119264, bc4a082e2b999d18ef2d7de1948b2bfd9758072f5945e08798f47827686621f2, 0639d8eaad9df842d6f358831b0d4c654ec4d9ebec037ab5defa240060956925, 63238b8d083553a8341bf6599d3d601fbf06708792642ad513b5e03d5e770e9b, eff2a9fca46425063dca080466427353dc52ac225d9df7c1ef0ec8ba49109b71, 2d10b48454537a8977affde99f6edcbb7cd6016d3683f9c28a4ec01b127f64d8, 7e5828382c9ef9cd7a643bc329154a37fe046346fd2cf4698da2b91050c9fe12, eff2a9fca46425063dca080466427353dc52ac225d9df7c1ef0ec8ba49109b71, B31f5bde1bdbc2dfd453b91bab2e9be0bececc555ee6edd70744c77f2ad15d18c, 33617f0ac01a0f7fa5f64bd8edef737f678c44e677e4a2fb23c6b8a3bcd39fa2, f9ca12321fb91157cce8513e935810d1c2005ab0739322b474f0cb4af2605d16, 977a9024962102b02128d391c0543c63328d3f26701eca1a5d282af4d493dc2e

References

https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering

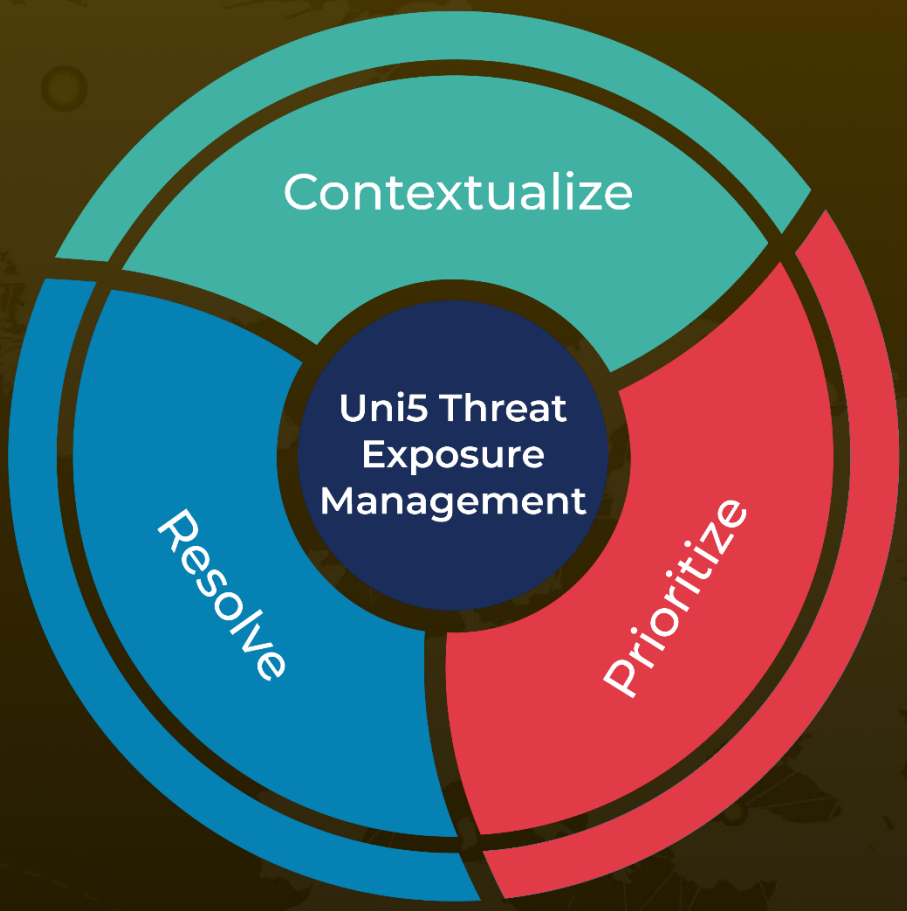
https://www.securonix.com/blog/analysis-of-devpopper-new-attack-campaign-targeting-software-developers-likely-associated-with-north-korean-threat-actors/

https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

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

August 2, 2024 • 7:00 AM

More at www.hivepro.com