Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

North Korean Hackers Unleash Flutter-Based Malware in New macOS Attack

Date of Publication	Admiralty Code	TA Number
November 13, 2024	A1	TA2024428

Summary

Attack Discovered: Late October 2024
Targeted Countries: Worldwide
Targeted Platform: macOS
Attack: North Korean threat actors have launched a novel approach to target macOS devices, using trojanized Notepad apps and Minesweeper games developed with Flutter and signed using a valid Apple developer ID. This marks the first time these adversaries have employed this method to compromise macOS systems. The distribution method for these malicious apps remains unknown, as does any evidence of specific targeting, suggesting the attackers may be testing a new delivery vector.

Attack Regions

Attack Details

#1 In late October, new malware samples were discovered, potentially linked to North Korean threat actors, exhibiting domain and tactic similarities with previous DPRK campaigns. Notably, the malware bypassed Apple's notarization process. The discovery involved three distinct variants: a Go-based malware, a Python variant built with Py2App, and a Flutter-based application, with the latter drawing particular attention due to its complexity in reverse engineering.

#2 The Flutter variant is camouflaged as a functional Minesweeper game, leveraging Google's cross-platform framework to maintain consistent behavior across macOS, iOS, and Android. Upon launch, it connects to a domain historically linked to DPRK threat activity, requesting further malicious payloads over HTTPS. The malware can execute complex AppleScript commands embedded in HTTP responses, even requiring specific coding formats like reversed scripts, signaling readiness for sophisticated macOS exploitation.

#3 Similarly, the Go variant mimics this behavior, initiating GET requests to the same command-and-control domain and employing AppleScript for arbitrary code execution. The Python-based variant is built with Py2App, appears as a simple Notepad application but contains malicious logic. Upon launch, it runs a Python script using tkinter for the GUI while fetching and executing commands from the C2 server.

#4 Together, these malware samples suggest pre-deployment testing, as the file names and application content seem misaligned with their true functions. This campaign represents the first known use of Flutter-built malware by DPRK-linked actors, possibly testing the ability to hide malicious code within dylib files to evade Apple's notarization process.

Recommendations

- **Restrict App Downloads to Trusted Sources:** Only download applications from the Mac App Store or official websites, minimizing the risk of installing trojanized apps.
- **Implement Network Monitoring for Unusual Traffic:** Set up alerts for suspicious network requests, particularly any outbound traffic to unfamiliar domains. Monitoring for unexpected use of AppleScript and other automation tools can help detect malicious activity early.
- **Deploy Endpoint Detection and Response (EDR):** Implement EDR solutions capable of detecting suspicious scripts, persistence mechanisms, and reverse shell activity on macOS endpoints.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
TA0011 Command and Control	**T1592** Gather Victim Host Information	**T1566** Phishing	**T1059** Command and Scripting Interpreter
T1059.002 AppleScript	**T1059.006** Python	**T1036** Masquerading	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1574** Hijack Execution Flow	**T1574.004** Dylib Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	6fa932f4eb5171affb7f82f88218cca13fb2bfdc, a12ad8d16da974e2c1e9cfe6011082baab2089a3, eadfafb35db1611350903c7a76689739d24b9e5c, 7cb8a9db65009f780d4384d5eaba7a7a5d7197c4, 0b9b61d0fffd52e6c37df37dfdffefc0e121acf7, ee22e7768e0f4673ab954b2dd542256749502e97, a2cd8cf70629b5bb0ea62278be627e21645466a3, 6664dfdbce1e6311ea02aa2827a866919a5659cc, dd38d7097a3359dc0d1c999225286a2f651b154e, 9598e286142af837ee252de720aa550b3bea79ea, 90e0e88e5b180eb1663c2b2cfe9f307ed03a301b, 710f84c42ba79de7eebb2021383105ae18c0c197, 5bf18435eb0dbb31e4056549f6ec880793f49a82, 2460c6ac4d55c34e3cc11c53f2e8c136682ac934, bc6b446bad7d76909d84e7948c369996b38966d1, 4476788a3178d53297caffca8ea21ab95352fc56, 3f51182029a2d4ed9c7cc886eb7666810904f9df, 6f280413a40d41b8dc828250bbb8940b219940c5
Domain	mbupdate[.]linkpc[.]net -&gt
IPv4	172[.]86[.]102[.]98
User Agents	dart-crx-update-request/1.0, CustomUpdateUserAgent/1.0, python-update-request/1.10.1
Team ID	BALTIMORE JEWISH COUNCIL, INC. (3AKYHFR584) FAIRBANKS CURLING CLUB INC. (6W69GC943U)

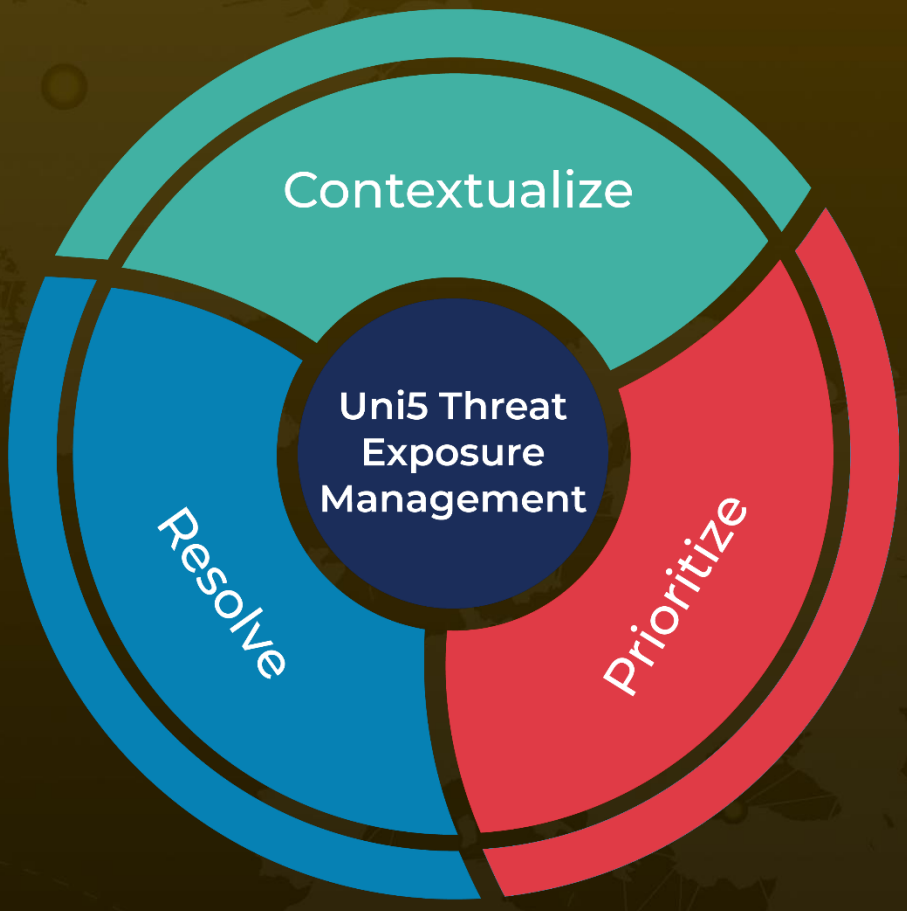
References

https://www.jamf.com/blog/jamf-threat-labs-apt-actors-embed-malware-within-macos-flutter-applications/

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 13, 2024 . 6:30 AM

More at www.hivepro.com