# North Korean Hackers Attacking MacOS Using Weaponized Documents

Date: 30th November 2023 | Severity: High

## Summary

Hackers often use weaponized documents to exploit vulnerabilities in software, which enables the execution of malicious code, Hackers Attacking MacOS.

## Attack Vectors

Hackers often use weaponized documents to exploit vulnerabilities in software, which enables the execution of malicious code.

North Korean threat actors focused on macOS in 2023 with two major campaigns, and here below, we have mentioned those major campaigns: -

1. **RustBucket:** Rust Bucket employed 'Swift Loader,' disguising itself as a PDF Viewer, to deliver a Rust-written second-stage malware.
2. **KandyKorn:** Kandy Korn campaign, Python scripts targeted blockchain engineers, delivering a C++ backdoor RAT named 'Kandy Korn' after hijacking the Discord app on hosts.

# Indicator of Compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | d28830d87fc71091f003818ef08ff0b723b3f358<br>43f987c15ae67b1183c4c442dc3b784faf2df090<br>26ec4630b4d1116e131c8e2002e9a3ec7494a5cf<br>46ac6dc34fc164525e6f7886c8ed5a79654f3fd3<br>62267b88fa6393bc1f1eeb778e4da6b564b7011e<br>8d5d214c490eae8f61325839fcc17277e514301e<br>8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18<br>9f97edbc1454ef66d6095f979502d17067215a9d<br>ac336c5082c2606ab8c3fb023949dfc0db2064d5<br>c45f514a252632cb3851fe45bed34b175370d594<br>ce3705baf097cd95f8f696f330372dd00996d29a<br>e244ff1d8e66558a443610200476f98f653b8519<br>e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f<br>e77270ac0ea05496dd5a2fbccba3e24eb9b863d9<br>79337ccda23c67f8cfd9f43a6d3cf05fd01d1588<br>a1a8a855f64a6b530f5116a3785a693d78ec09c0<br>e275deb68cdff336cb4175819a09dbaf0e1b68f6<br>09ade0cb777f4a4e0682309a4bc1d0f7d4d7a036<br>5c93052713f317431bf232a2894658a3a4ebfad9<br>884cebf1ad0e65f4da60c04bc31f62f796f90d79<br>be903ded39cbc8332cefd9ebbe7a66d95e9d6522<br>060a5d189ccf3fc32a758f1e218f814f6ce81744<br>3c887ece654ea46b1778d3c7a8a6a7c7c7cfa61c<br>c806c7006950dea6c20d3d2800fe46d9350266b6 |
| Domain | http [:]//docs-send. Online/get Balance/usdt/Ethereum.<br>https[:]//drive.google[.]com/file/d1KW5nQ8MZccug6Mp4QtKyWLT3HIZzHNIL2<br>http [:]//on-global[.]xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D<br>http [:]//tp-globa[.]xyz/OdhLca1mLUp/lZ5rZPxWsh/7yZKYQI43S/fP7savDX6c/bfC<br>http [:]//swissborg[.]blog/zxcv/bnm |
| IPs | 23.254.226[.]90<br>104.168.214[.]151<br>142.11.209[.]144<br>192.119.64[.]43 |

# Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the IPs to Network team to block in the firewall.

Block the Domain in the Proxy.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

https://gbhackers.com/korean-macos-weaponized-documents/