

# Forum:[Hack Forums](#)

Thread: [North Korean Hackers Spreading DocSwap Malware](#)

JoseMar - March 13, 2025, 5:12 am

## North Korean Hackers Spreading DocSwap Malware

### Disguised as a Security Document Viewer

A modern malware campaign focusing on portable clients in South Korea has been revealed, with clear joins to North Korean danger actors.

The pernicious application is disguised as a "Document Seeing Confirmation App."

This malevolent app was recognised through VirusTotal on January 21, 2025, and has effectively taken delicate data from compromised devices.

The S2W Danger Investigate and Insights Center analysts identified the malware, which they named "DocSwap", after finding a phishing page mimicking CoinSwap at the command and control infrastructure.

The analysts know that the pernicious app was malicious on December 13, 2024, and speaks to an already unidentified risk mainly planned to target South Korean users.

The advanced malware utilises a multi-stage disease preparation that starts with decoding a muddled record inside the package.

"The malicious app performs an XOR (0xCC) operation on the 'security.db' file in a subdirectory, which drops an APK file and loads the DEX file stored within it," clarified the report enumerating the threat.

The decryption of the security.db Record Upon execution, DocSwap forcefully demands various consents, including call logs, contacts, SMS messages, outside capacity, and phone capabilities.

It diligently creates notices inquiring clients to empower openness administrations with messages like "To guarantee legitimate usefulness, it would be ideal if you empower availability permissions."

The application guarantees determination by enrolling for boot-related bury counting BOOT\_COMPLETED, ACTION\_POWER\_CONNECTED, and ACTION\_POWER\_DISCONNECTED, permitting it to survive gadget restarts.

It employs the StartForeground API to keep a consistent nearness with notices expressing "Tap to see more points of interest or halt the app."

### Technical Capabilities and Command Structure

DocSwap communicates with a hardcoded command and control server at 204.12.253[.]10:6834, I would like to talk through an advanced command structure.

The malware supports 57 commands, enabling extensive surveillance and data exfiltration capabilities.

Key components of the decryption mechanism reveal the attackers techniques:

```
Code public static void dumpFile(String assetsPath, String destPath) {  
    File destFile = new File(destPath);  
    if(!new File(destFile.getParent()).exists())  
        new File(destFile.getParent()).mkdirs();  
    try {
```

```

if(!destFile.exists())
    destFile.createNewFile();
InputStream inputStream0 = MyApp.getInstance().getAssets().open(assetsPath);
FileOutputStream out = new FileOutputStream(destFile);
byte[] tmpbpt = new byte[0x400];
int v;
while((v = inputStream0.read(tmpbpt)) != -1) {
    for(int i = 0; i < 0x400; ++i) {
        tmpbpt[i] = (byte)(tmpbpt[i] ^ 0xFFFFFFFFC9);
    }
    out.write(tmpbpt, 0, readCount);
}

```

#### Malicious App Execution Process

This captured information is transmitted to a Command and Control (C2) server and moreover put away locally utilizing a organized path:

Code /data/data/com.security.library/Security/download\_{dd-mm-yyyy}.dat

Cybersecurity firm S2W has credited this campaign to a North Korean risk performing artist, puNK-004, citing foundation likenesses with past operations by the Kimsuky group.

Security analysts unequivocally exhort caution when introducing portable applications, particularly those asking availability authorizations or posturing as archive confirmation apparatuses from unsubstantiated sources.

Don't forget to update and stay safe!?

Additional sources to explore: You can also search directly by CVE on Google for more information:

<https://gbhackers.com/north-korean-hackers-deploy-docswap-malware/>

<https://cybersecuritynews.com/beware-of-north-korean-hackers-docswap-malware/>

**Pr0m3th3us** - March 17, 2025, 12:00 am

Thanks for another quality thread Jose

**DarkNovichu** - September 12, 2026, 11:59 am

gracias

**XtremeDiscount** - September 12, 2026, 1:03 pm

Wow it's scary thinking what a country like North Korea's intentions are when they're so closed off from the world