# Analysis of the North Korea-backed puNK-003’s Lilith RAT ported to AutoIt Script

Archived: 2026-04-05 12:39:41 UTC

- Research
- Threat Intelligence Reports

Analysis of the North Korea-backed puNK-003’s Lilith RAT ported to AutoIt Script

2024.08.22

S2W's Threat Intelligence Center, TALON, has published a detailed analysis report on the Lilith RAT malware distributed by the North Korean-backed attack group puNK-003. This report marks the first instance of publicly disclosing findings based on the threat group classification system (refer to Table 1 below) that S2W analysts have been managing separately.

✅ Report Title:

**Threat Tracking: Analysis of puNK-003’s Lilith RAT ported to AutoIt Script**

*puNK: partially unidentified North Korean threat actor

✅ Executive Summary:

**📌 Malware Disguised as a List of Supporting Documents Related to Tax Evasion Reports (LNK)**

On April 24, 2024, S2W's Threat Research and Intelligence Center, TALON, discovered and analyzed an LNK malware disguised as a document related to tax evasion reports.

When the LNK file is executed, it drops and displays a decoy document included within the file and downloads additional files from a hardcoded attacker server. The downloaded files consist of a malicious AutoIt script and a legitimate AutoIt3 executable used to run the script. Ultimately, the AutoIt script executes the Lilith RAT malware that has been reimplemented in AutoIt.

**📌 Inferring the Attack Group Through Malware Analysis (Comparison with KONNI Group)**

The recently discovered LNK malware exhibits characteristics of the North Korean-backed KONNI group, particularly in the composition of the PowerShell commands included in the execution parameters and the fact that the downloaded files are all reimplemented as AutoIt scripts.

However, there are differences in the execution purpose between this malware and the LNK malware used by the KONNI group. The former acts as a Downloader, while the latter functions as a Dropper. Additionally, in this

attack campaign, there is a notable absence of VBS and BAT script-based malware, which are commonly used by the KONNI group. Based on these differences, S2W TALON has distinguished between the two attack groups.

### 📌 Analysis of North Korean-backed Attack Group puNK

TALON separately manages unidentified threat groups, and among them, North Korean-backed attack groups are tracked under the name "puNK." The list of puNK groups tracked by TALON is shown in Table 1.

The entity responsible for distributing this malware has been designated as "puNK-003," and the LNK malware they use, which serves as a Downloader, has been named "CURKON."

👩‍💻 Report Author: S2W TALON (Jiho Kim)

👉 Learn more: https://bit.ly/3yKzuFn

List

---