Lazarus Group’s Operation Dream Magic - ASEC

By ATCP

Published: 2023-10-12 · Archived: 2026-04-05 19:38:47 UTC

The Lazarus group is a hacking group that is known to be state-sponsored and is actively conducting hacking activities worldwide for financial gain, data theft, and other purposes. A simplified overview of the Lazarus group’s watering hole attack that abused the INISAFE vulnerability is as follows: a malicious link was inserted within a specific article on a news website. Consequently, companies and institutions that clicked on this article were targeted for hacking. The hackers exploited vulnerable Korean websites with C2 to facilitate their attacks and implemented IP filtering for selective targeting. While the program vulnerability used in this watering hole attack has now shifted to MagicLine, the overall watering hole process remains unchanged from the earlier INISAFE case. AhnLab coordinated the efforts of multiple teams to respond to the Lazarus group’s exploitation of the MagicLine vulnerability in their watering hole attack. There were several teams involved in this collaboration. The analysis team was responsible for studying the conditions to detect the MagicLine vulnerability and updating the anti-malware. The technical support team was responsible for handling customer responses, including log and sample collection, in case the affected PC belonged to a customer. The response team was tasked with analyzing the gathered logs and liaising with national agencies. In addition, AhnLab, through the collaboration and information sharing with national agencies, tracked and analyzed the Lazarus group’s watering hole attacks exploiting the MagicLine vulnerability. Combining parts of the MagicLine manufacturer’s name and the name of MagicLine, AhnLab named this operation **“Operation Dream Magic”**. The following report includes content based on the malware analysis, detection status, and log analysis collected with the cooperation of several

companies, as well as the information sharing and collaboration done with national agencies. Furthermore, it provides an explanation for the basis upon which the recent operation was attributed to the Lazarus group. **[+] Download Report:** **20231013_Lazarus_OP.Dream_Magic** (This report supports Korean only.)

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/57736/