Analysis Report on Kimsuky Group’s APT Attacks (AppleSeed, PebbleDash) - ASEC

By ATCP

Published: 2021-11-15 · Archived: 2026-04-05 14:29:28 UTC

This document is an analysis report on types of malware recently utilized by the Kimsuky group. The Kimsuky group is mainly known for launching social engineering attacks such as spear phishing. Judging by the names of the attached files, the group seems to be targeting those working in the fields related to North Korea and foreign affairs. According to the scan logs of AhnLab’s ASD infrastructure, the threat group has been mainly targeting personal users rather than companies, but has also been continuously attacking public institutions and companies. Korean universities have been one of their major targets, but records exist of them attacking IT, information and communications, and construction institutions as well.

Normally, malware strains assumed to be attachments of spear phishing attack emails are disguised as document files. If a user runs the file, malware of this type runs the document that corresponds to the disguised file name and tricks the user into thinking that they have opened a normal file. It installs additional malware strains at the same time, mainly AppleSeed and PebbleDash. AppleSeed has been present since 2019 and when compared to other malware strains based on the IOCs organized by AhnLab, it takes up a significant portion due to being used in various other attacks. PebbleDash is one of the NukeSped variants, known for having been used by the Lazarus group since the past. Recently, it has been found that a new variant is being used for attacks along with AppleSeed.

They are both backdoors used by the Kimsuky group that can stay in the system and perform malicious behaviors by receiving commands from the attacker. The attacker can use backdoor to install another remote control malware such as Meterpreter and HVNC, or various other types of malware for privilege escalation and account credential theft.

This report will analyze the overall flow of attacks using AppleSeed and PebbleDash, starting from malware strains that are initially distributed. As both malware types are not confined to a single form, the report will compare each type and focus on similarities and differences, and also explain in detail other types of malware that the two malware additionally install.

——

Analysis Report on Kimsuky Group's APT Attacks (AppleSeed, PebbleDash)

Download

——

Contents

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/30532/