VB2019 paper: Kimsuky group: tracking the king of the spear phishing

Jaeik Kim, Kyoung-ja Park & Min-Young Jang

Date: 1 October 2019

Abstract

Kimsuky is a well-known APT group that has been active since at least 2013. This group has been mainly focusing on South Korean and Japanese targets and has been using various malicious documents and malicious macros to infect victims' PCs. In this paper, we will introduce the latest activities of the Kimsuky group, including their new malware, their new tactics and their new infrastructure.

1. Introduction

Kimsuky is a well-known APT group that has been active since at least 2013. This group has been mainly focusing on South Korean and Japanese targets and has been using various malicious documents and malicious macros to infect victims' PCs. In this paper, we will introduce the latest activities of the Kimsuky group, including their new malware, their new tactics and their new infrastructure.

2. Related cases

3. Tactical characteristics

Spear-phishing

Malware