|  |
| --- |
| **Press Release** |
| **Release date: April 29, 2025** |
| **Public Relations Division, Ministry of Science and ICT**  **Contact Information: Songyi Han(+82-44-202-4034), Seonghwan Kim(+82-44-202-6461)** |
|  |

**MSIT Releases First Investigation Results on SKT Data Breach** — **No IMEI Leak Confirmed**

The Ministry of Science and ICT (Minister Yoo Sang-im) today, April 29, announced the preliminary results of its investigation into the recent security breach involving SK Telecom (SKT). The investigation was conducted over the past week by a Public-Private Joint Task Force established specifically for this incident.

The Task Force confirmed that no device unique identifiers (IMEI numbers) were leaked during the breach. It also verified that customers enrolled in SKT’s USIM Protection Service\* are safeguarded against illegal activities such as "SIM swapping" — the cloning of a user's SIM card to commit fraud using another device.

\*The USIM Protection Service blocks communication service access when a device other than the registered one attempts to connect under a customer's identity.

※ SKT has also been detecting and blocking unauthorized access attempts to its network through illegally cloned USIM cards by utilizing its Fraud Detection System (FDS).

The Task Force investigated on five servers across three categories that showed signs of compromise and is now expanding the investigation to additional servers containing sensitive information. To date, the compromised data confirmed to have been leaked from SKT includes four types of customer information which could be potentially used for USIM cloning, such as subscriber phone numbers and IMSI (International Mobile Subscriber Identity) numbers, as well as 21 types of SKT’s internal management data related to USIM information processing.

During the course of the investigation, the Task Force also identified four variants of BPFDoor malware used in the attack. BPFDoor is a stealth backdoor that exploits the Berkeley Packet Filter (BPF), a network monitoring and filtering tool built into Linux systems, making detection of hacker communications particularly difficult. On April 25, to help prevent further spread, the Task Force shared information about the malware with companies and relevant institutions.

To minimize public concern and prevent potential damage, the Ministry of Science and ICT is encouraging customers to either replace their USIM cards or subscribe to the USIM Protection Service, which offers comparable preventive effects. The Ministry has also urged SKT to expand service channels and implement a reservation system to allow more customers to subscribe the USIM Protection Service easily and promptly.

In addition, after discussions, the Ministry urged SKT to immediately ensure that customers are fully protected from the moment they complete a reservation for the USIM Protection Service — with SKT assuming 100% responsibility — even before the service is formally activated.

For further information, please contact the Public Relations Division (Phone: +82-44-202-4034, E-mail: [msitmedia@korea.kr](mailto:msitmedia@korea.kr)) of the Ministry of Science and ICT.