Kawasaki Heavy Industries, Ltd.

July 30 , 2021

Report on the Results of Investigation into Unauthorized Access to Kawasaki Group

Tokyo, July 30, 2021 - Kawasaki Heavy Industries, Ltd. has carried out a highly specialized investigation into unauthorized access by third parties (announced on December 28, 2020). The investigation has been conducted at all business sites in Japan and overseas, in a special project team formed with an external specialist organization.

In the investigation to date, we have confirmed the possibility that information may have leaked out from our group, and have identified the scope and type of unauthorized access. We have also implemented countermeasures, and reported the results of the investigation to the customers who may have been affected by the information leakage.

To date, we have not confirmed any specific damage related to our customers or business partners, but we would like to take this opportunity to once again express our deepest apologies for the inconvenience and concern we have caused to all the related parties.

The investigation report is as follows. However, from the viewpoint of ensuring information security, please note that we cannot disclose specific information about our customers or detailed information about our measures against unauthorized access.

1. Investigation Results

(1) Malware investigation[*1]

We conducted an investigation for malware on the PCs and servers (Approx. 29,000 units) at our major group bases in Japan and at the group bases overseas where infringement was confirmed. At the overseas bases, it was confirmed that the situation had been normalized through malware removal. In Japan, it was confirmed that there had been no malware intrusion.

(2) Forensic analysis[*2]

We identified the PCs and servers that had high traffic (Approx. 6,700 units) and investigated for evidence of infringement. As a result, we identified servers located in Japan and overseas that may have been subject to unauthorized access (Total 36 units). We conduced detailed forensic analysis on those servers and discovered that 15 of them contained suspicious encrypted files. We further narrowed down the information that could possibly be included in the encrypted files and reported the analysis results to the customers to whom that information may be related.

(3) Communication log investigation
As a result of investigating the communications logs, we confirmed that data was sent from bases in Thailand, Indonesia, and the United States to suspicious servers on the Internet.

As described above, the possibility of information leakage has been confirmed, but the leakage of personal information has not been confirmed as fact at this time.

2. Status of Countermeasures
We have tightened the management of communication between our overseas bases and bases in Japan, changed the data exchange process, and implemented measures to prevent unauthorized access to our authentication infrastructure. At the present time, there has been no confirmation of any new attacks or damage. In addition, we have continued the constant monitoring of communications and have strengthened the monitoring of terminals in our bases in Japan and overseas where the risk is considered to be particularly high, to expand and improve our system to detect unauthorized access.

3. Future Action
To prevent recurrence, we are further tightening the monitoring and access control for the communications networks between our bases in Japan and overseas and we are strengthening our processes to quickly detect any unauthorized access and to be able to rapidly identify the scope of damage and respond to it. We are also strengthening our organization by increasing the number of personnel involved and are expanding our in-house training to raise awareness of information security.
In addition, with the Cyber Security Group playing a central role, we will coordinate with the police, the relevant ministries and agencies, and specialist security companies and will strengthen the security measures throughout our group in response to the latest methods of unauthorized access.

*1. Generic term for malicious software and malicious code that is created with the intent to perform dishonest and harmful actions.
*2. Work to search for the cause of an accident or evidence of a crime from the detailed data left on a recording medium.

- End of document -