

[NEWS RELEASE]

July 2, 2024

KADOKAWA CORPORATION

Further Criminal Declaration by the Perpetrators and the KADOKAWA Group's Response Concerning Information Leakage Caused by the Ransomware Attack

KADOKAWA CORPORATION (Headquarters: Chiyoda-ku, Tokyo; Chief Executive Officer: Takeshi Natsuno; hereinafter "KADOKAWA") expresses deep apologies for the significant inconvenience and trouble caused to its readers, users, writers, creators, business partners, shareholders, investors, and other stakeholders by the system failure currently affecting the KADOKAWA Group.

After the discovery of a significant cyberattack including ransomware on servers located in the data center targeting *Niconico* and the related services, the KADOKAWA Group promptly established a task force and commenced an ongoing investigation into the possibility of information leakage with assistance including external professional organizations

In the process, KADOKAWA announced on June 28 that the organization claiming to have carried out the ransomware attack had leaked some data held by the KADOKAWA Group, and following this announcement, on July 2, we confirmed that the organization claimed to have leaked more information held by the KADOKAWA Group.

We are currently investigating the authenticity of the claims the organization has made, but we expect that it will take considerable time to verify their accuracy. We will do our utmost to obtain accurate facts as soon as possible. Meanwhile, we expect to receive the results of investigations by external professional organizations by the end of July. As soon as the results of these investigations are known, we shall promptly report them to the public. We sincerely apologize for any concern this may cause, but we ask for your continued patience. As previously announced, KADOKAWA does not itself store credit card information on KADOKAWA Group customers, including customers of *Niconico* services. This structure prevents the leakage of this information from KADOKAWA.

Be aware that accessing or downloading data files from websites which the organization claims to have attacked comes with risks, such as malware infection. Although we are currently investigating what the organization claims as described above, we ask for your understanding and cooperation in refraining from sharing the leaked information on social media or elsewhere, as the spread of this personal information could have serious repercussions by infringing upon privacy.

The police have already begun an investigation into this case. In addition, KADOKAWA is providing the relevant authorities with necessary reports. As previously reported, the KADOKAWA Group's business activities have been affected to a certain extent, but we shall stand firm in our response rather than give in to such criminal acts.

Meanwhile, we take this situation very seriously. While proceeding with a more in-depth investigation of the cause, we will further strengthen our information security systems to prevent a recurrence.

KADOKAWA reiterates its deepest apologies to our customers and all those concerned for the considerable inconvenience and trouble this matter has caused.

<Dedicated Helpdesk for Information Leakage Inquiries*>

https://qa.nicovideo.jp/helpdesk?category_id=982&faq_id=22764&site_domain=default

*Japanese only

End of document

For media inquiries, please contact:

Investor and Public Relations Division, KADOKAWA CORPORATION

Email: pr-dept@kadokawa.jp