November 16, 2020

3-1-3, Uchihiranomachi, Chuo-ku, Osaka
Capcom Co., Ltd.
Haruhiro Tsujimoto, President and COO
(Code No. 9697 First Section of Tokyo Stock Exchange)

Update Regarding Data Security Incident Due to Unauthorized Access

Capcom Co., Ltd. (Capcom) announced that it has been the victim of a customized ransomware attack following unauthorized access to its network and has verified that some personal information maintained by the Capcom Group has been compromised.

Further, the company also stated that it has confirmed the possibility that additional personal and corporate information may have been compromised in this attack, which is listed in "2. Potentially compromised data" below. At present, its content development and business are operating without impediment.

Capcom offers its sincerest apologies for any complications and concerns that this may bring to its potentially impacted customers as well as to its many stakeholders.

As there is an ongoing investigation in place, it is possible that new facts may come to light going forward. Below is a general summary of what has been confirmed at this point in time (as of November 16, 2020).

1. Information verified to have been compromised
   i. Personal information: 9 items
      - Personal information of former employees: 5 items
        (Name & signature: 2 items; name & address: 1 item; passport information: 2 items)
      - Personal information of employees: 4 items
        (Name and HR information: 3 items; name & signature: 1 item)
   ii. Other information
      - Sales reports
      - Financial information

2. Potentially compromised data
   i. Personal information (customers, business partners, etc.): maximum of approx. 350,000 items
      - Japan: Customer service video game support help desk information (approx.134,000 items)
        Names, addresses, phone numbers, email addresses
      - North America: Capcom Store member information (approx. 14,000 items)
        Names, birthdates, email addresses
      - North America: Esports operations website members (approx. 4,000 items)
        Names, email addresses, gender information
      - List of shareholders (approx. 40,000 items)
        Names, addresses, shareholder numbers, amount of shareholdings
      - Former employees' (including family) information (approx. 28,000 people);
        applicants' information (approx. 125,000 people)
        Names, birthdates, addresses, phone numbers, email addresses, photos, etc.
   ii. Personal information (employees and related parties)
      - Human resources information (approx. 14,000 people)

iii. Confidential corporate information
- Sales data, business partner information, sales documents, development documents, etc.

None of the at-risk data contains credit card information. All online transactions etc. are handled by a third-party service provider, and as such Capcom does not maintain any such information internally.

Because the overall number of potentially compromised data cannot specifically be ascertained due to issues including some logs having been lost as a result of the attack, Capcom has listed the maximum number of items it has determined to potentially have been affected at the present time.

3. Support for individuals whose personal information has been confirmed to have been compromised and those whose information has potentially been compromised
   i. Action addressing personal or corporate information confirmed to have been compromised
   Capcom has begun contacting individuals whose information it has verified to have been compromised to explain the background of this incident and current situation.

   ii. Action addressing potentially compromised personal information
   Capcom is continuing the investigation into information that has potentially been taken or compromised.
   For individuals who wish to inquire about personal information that has potentially been compromised, please contact the following support desks in your country or region:

   Japan: Capcom Data Security Incident Support Line (Japanese only)
   Tel. (toll-free): Game customer inquiries 0120-400161
   General inquiries 0120-896680
   Hours: 10:00 AM – 08:00 PM

   North America: Capcom USA Customer Support Page
   www.capcom.com/support

   EMEA: Capcom Europe Customer Support
   feedback@capcom.com

4. Detection and action taken
   i.
   - In the early morning hours of November 2, 2020 after detecting connectivity issues with its internal network, Capcom shut down its systems and began investigating the situation.
   - Capcom confirmed that this was a targeted attack against the company using ransomware, which destroyed and encrypted data on its servers.
   - The company discovered a message from a criminal organization that calls itself Ragnar Locker, and after ascertaining that ransom money was being demanded, contacted the Osaka Prefectural Police.
   - On November 4, 2020 the company issued the following press release: “Notice Regarding Network Issues due to Unauthorized Access.”
   - On November 12, 2020, Capcom verified that nine items of personal information and some corporate information had been compromised.
   - In addition to these confirmed nine items, the company continued its investigation into the scope of potentially compromised information, making a public disclosure of this on November 16, 2020 (this release).

   Investigation and analysis, etc., of this incident took additional time due to issues such as the information saved on servers being encrypted and access logs being deleted in the attack.
   ii. At this point, Capcom has reported the occurrence of network issues to the supervisory authority under GDPR (ICO in the United Kingdom), and the Personal Information Protection Commission (Japan).
   iii. The company implemented protective software, shut down all suspicious transmissions, and carried out reconstruction of the servers. It is carrying out an ongoing investigation into the information that had been saved in each of its departments based on the servers it has recovered.

iv. The company has already commissioned a third-party security company to inspect system issues stemming from this incident. Capcom plans to announce the results of this inspection separately, when available.
v. Further, the company has arranged a structure of reporting and consultation with a major software company, a major security specialist vendor and law offices with extensive knowledge of system security.

Capcom will continue its investigation, beginning with contacting those individuals and other stakeholders whose information it has verified as having been compromised, while continuing to look into what other information was potentially taken.

Investigation and analysis of this incident took additional time due to the targeted nature of this attack, which was carried out using what could be called tailor-made ransomware, as was covered in some media reports, aimed specifically at the company to maliciously encrypt the information saved on its servers and delete its access logs. Capcom regrets that this report could not be made sooner than today. The company asks that everyone potentially affected by this incident practice an abundance of caution, looking out for any suspicious packages received by mail or messages that could potentially be received.

5. Measures going forward
   i. Capcom will continue coordinating with law enforcement authorities in Japan and the U.S., and also give timely reports to and receive advice from the institutions responsible for the protection of personal information in each country.
   ii. As stated above, the company is coordinating with parties such as a major IT security specialist company to work toward understanding the overall damage caused by the attack and preventing any reoccurrence.
   iii. Capcom is in discussions with external security experts. It plans to newly establish an advisory board regarding system security working towards preventing any reoccurrence.

Additionally, it is safe for Capcom customers or others to connect to play the company's games online and access its websites.

Presently, while the company believes that any effect from this incident on the Capcom Group's consolidated business results (for the fiscal year ending March 31, 2021) will be negligible, the company will swiftly make an announcement in the case that any further disclosure is necessary.

Capcom would once again like to reiterate its deepest apologies for any complications or concerns caused by this incident. As a company that handles digital content, it is regarding this incident with the utmost seriousness. In order to prevent the reoccurrence of such an event, it will endeavor to further strengthen its management structure while pursing legal options regarding criminal acts such as unauthorized access of its networks.

Inquiries regarding the above information may be directed to:

Press Contact
North & South America: https://press.capcom.com
Europe, Middle East & Africa: https://www.capcomeuro-press.com

Customer Support
North & South America: www.capcom.com/support
Europe, Middle East & Africa: feedback@capcom.com

Investors
Public Relations and Investor Relations Section
(Tel)+81-6-6920-3623 (Fax) +81-6-6920-5108

Business Partners
Please contact the representative department with which you work