April 13, 2021

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

4th Update Regarding Data Security Incident Due to Unauthorized Access: Investigation Results

Capcom Co., Ltd. (Capcom) has previously issued statements from November 4, 2020 through January 12, 2021 ("previous announcements," below) announcing that it has been the victim of an attack due to unauthorized access to its network by a third party and that some personal information maintained by the Capcom Group has been compromised ("the incident," below).

The investigation into the incident, carried out with the cooperation of external specialist companies, has been completed and Capcom has received their findings. As such, Capcom can now make an announcement regarding the findings of that investigation as well as the measures it will take to prevent future incidents. At this point in time, the Capcom Group's internal systems are near to completely restored, and while coordinating with the newly established Information Technology Security Oversight Committee, the company will work toward continuously strengthening both security and the protection of personal information going forward.

Capcom offers its sincerest apologies for any complications and concerns its customers as well as its many stakeholders may have experienced, and further, would like to express its deepest gratitude for their ongoing support during this time.

1. Incident Response Timeline

November 2, 2020	Detected connectivity issues with internal network. Shut down systems and began examining.
November 2, 2020	Confirmed that these issues stemmed from a ransomware attack, which encrypted data on devices on the company's network. Discovered a threatening message from a group that calls itself Ragnar Locker on the affected devices and contacted the Osaka Prefectural Police. Requested support for system restoration from external companies.
November 3, 2020	Began contacting the relevant organizations in each country, including investigative authorities and those that oversee the protection of personal information.
November 4, 2020	Issued the press release: "Notice Regarding Network Issues due to Unauthorized Access."
November 12, 2020	Verified that nine items of personal information and some corporate information had been compromised.
November 13, 2020	Approached external IT security specialist company regarding investigating the root cause of this matter.
November 16, 2020	Issued the press release: "Update Regarding Data Security Incident Due to Unauthorized Access." Continued investigation into compromised and potentially compromised data.
December 21, 2020	Held preparatory meeting ahead of the launch of the Information Technology Security Oversight Committee, which functions as an advisory group for matters related to system security with external security experts.
January 12, 2021	Issued the press release: "3rd Update Regarding Data Security Incident Due to Unauthorized Access."
January 18, 2021	Held first Information Technology Security Oversight Committee meeting.
February 25, 2021	Held second Information Technology Security Oversight Committee meeting.
March 26, 2021	Held third Information Technology Security Oversight Committee meeting.
March 31, 2021	Received investigation findings from external IT security specialist company.
March 31, 2021	Received additional information from external software company.
April 13, 2021	Issued the press release: "4th Update Regarding Data Security Incident Due to Unauthorized Access: Investigation Results."

2. Root Cause and Scope

Capcom worked with multiple companies including major security vendors and IT specialist companies to carry out an investigation into the devices and transmission logs affected in the attack. As a result of carrying out this investigation, Capcom has found that the incident occurred as described in the following summary. Further, as stated in previous announcements, the Company has been coordinating both domestically and overseas with law enforcement and related organizations, while also continually reporting and corresponding on a timely basis with the authorities that oversee the protection of personal information in each country.

According to the IT specialists, unauthorized access to the Company's internal network was acquired in October 2020 through a cyberattack carried out on an older backup VPN (Virtual Private Network) device that had been maintained at its North American subsidiary (Capcom U.S.A., Inc.). At that time, the Capcom Group, including the North American subsidiary, had already introduced a different, new model of VPN devices; however, due to the growing burden on the Company's network stemming from the spread of COVID-19 in the State of California, where this North American subsidiary is located, one of the aforementioned older VPN devices remained solely at this North American subsidiary as an emergency backup in case of communication issues, and it became the target of the attack. The device in question has already been removed from the network at this time.

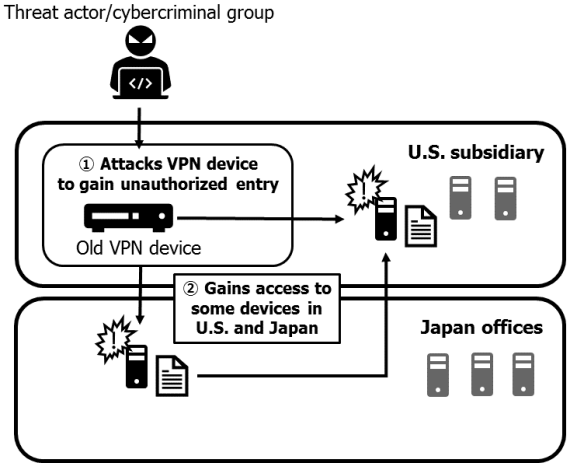
The IT specialists determined that following this, some devices were compromised at both the Company's U.S. and Japanese offices through the affected old VPN device at the Company's North American subsidiary, leading to the theft of information. While the Company had existing perimeter[*1] security measures in place and, as explained below, was in the processes of adopting defensive measures such as a SOC[*2] service and EDR[*3], the Company had been forced to prioritize infrastructure improvements necessitated by the spread of COVID-19. As a result, the use of these measures was still in the process of being verified (not yet implemented) at the time this matter took place.

Following the final stage of the attack, some devices at both the Company's U.S. and Japanese offices were infected with ransomware on November 1, 2020 beginning at approximately 11 PM (JST), resulting in the files on affected devices being encrypted. Beginning in the early morning hours of November 2, 2020 some of the Capcom Group networks experienced issues that affected access to certain systems, including email and file servers. While the Company halted certain operations, it worked to quickly restore them. The above is a broad explanation of the incident from the external specialist companies, who have provided Capcom with the conclusion that the incident was a malicious, multi-faceted attack that would be difficult to defend against.

*1: Security measures that include placing a firewall at the perimeter between external networks and internal networks.

*2: Acronym standing for Security Operation Center. A SOC service is a system that monitors systems and networks around the clock, and supports the detection, analysis and handling of attacks.

*3: Acronym standing for Endpoint Detection and Response. A system that introduces software to detect unusual activity on devices such as the PCs and servers utilized by end-users and supports quick responses to issues.



3. Security Measures to Prevent Reoccurrences

In addition to the Company's existing perimeter security measures, following the incident, Capcom has taken a variety of measures to strengthen existing security with the aim of preventing any reoccurrence. This includes the introduction of an SOC service, which continuously monitors external connections, and EDR, which allows for early detection of unusual activity on devices. Below are explanations of both the measures Capcom has taken to address the incident and those it plans to carry out, as of the time of this announcement.

i. Technical Measures

[Implementation complete] (list of major items only)

a. Leading software company carried out cleaning of all compromised devices
b. Reverified the safety of all VPN devices and that security measures are complete (further, old VPN device at North American subsidiary described above has been disposed of)
c. Introduced SOC (Security Operation Center) service in order to monitor external connections around the clock
d. Introduced the latest EDR (Endpoint Detection and Response) to provide early detection of unusual activity and computer virus infection on devices
e. Reviewed accounts used for business purposes
f. Further improved management methods for VPN and other devices, including those pertaining to long-term storage of logs to facilitate a quick response in the case that an incident occurs

[Implementation planned]

While Capcom has been informed by external specialist companies and the Information Technology Security Oversight Committee that items a.~f. above are in line with current best practices, it is possible that new threats and methods of attack could be created. Going forward, Capcom will continue to take various measures to address any such future developments with direction from the Information Technology Security Oversight Committee.

ii. Organizational Measures

[Implementation complete]

a. Launched the Information Technology Security Oversight Committee in the latter half of January 2021 in order to receive recommendations on a continuous basis from external experts based on the latest trends, with an aim to procure external checks and the swift accumulation of knowhow regarding strengthening cyber security (including data protection for securing personal information, etc.). Externally, there are four[*4] Committee members who consist of two university professors who are cyber security experts, one lawyer who is an expert on both cyber security and the Act on the Protection of Personal Information, and one certified public accountant that is an IT system audit specialist; internally, one director as well as three technicians who oversee security and networks participate. The Committee plans to continue to regularly hold meetings to strengthen protection standards.
b. Established the Information Technology Surveillance Section in December 2020, a new section directly under the Information Technology Security Oversight Committee, which gathers information regarding cyber security and builds knowledge of preventative measures to make recommendations, etc.
c. Strengthened the system for regular verification, including for the adoption of tools, in the management of accounts used for business purposes.
d. Constructed system to further raise awareness of security and the management of personal information at the Group overall.

[Implementation planned]

Build out and regulate a system for further strengthening security based on the PDCA cycle

*4: Prof. Tetsutaro Uehara of Ritsumeikan University; Hisamichi Okamura, attorney-at-law, of Cyber Law Japan Eichi Law Offices; Prof. Atsuo Inomata of Osaka University; Mitsuhiko Maruyama, Partner at PwC Consulting LLC.

4. Compromised and Potentially Compromised Information

i. Information verified to have been compromised
Since the January 12, 2021 announcement, the cumulative total for information verified to have been compromised since this investigation began decreased by 766 people, down to 15,649 people.

ii. Potentially compromised data
There have been no changes following the January 12, 2021 announcement.

As described in previous announcements, none of the at-risk data contains credit card information. All online transactions etc. are handled by a third-party service provider on a separate system (not involved in this attack), and as such Capcom does not maintain any such information internally.

Additionally, the areas that were impacted in the incident are unrelated to those systems used when connecting to the internet to play or purchase the company's games online, which utilized and continue to utilize either an external third-party server or an external server (not involved in this attack). As such, these systems were outside the scope of the incident, and it remains safe for Capcom customers or others to connect to the internet to play or purchase the company's games online.

Further, regarding the total number of people whose data was potentially compromised, because a portion cannot specifically be ascertained due to issues including logs having been lost as a result of the attack, Capcom has included the maximum number of individuals whose data was maintained on all potentially compromised servers. Additionally, the company has not been able to confirm any damages, etc. resulting from actual misuse of the compromised information at this point in time. (For information regarding ransom demands made to the company, see "6. Regarding Capcom's Awareness of Ransom Demands," below.)

5. Support for those whose personal information has been confirmed to have been compromised and those whose information has potentially been compromised

i. Capcom is notifying those whose personal information or corporate information has been confirmed to have been compromised to discuss the background of this incident and current situation.

ii. For individuals who wish to inquire about compromised personal information, as has been described in previous announcements, 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 – 8:00 PM

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

EMEA: Capcom Europe Customer Support
feedback@capcom.com

The number of inquiries the company has received in Japan has been declining: In the month prior to this announcement, the daily average was 0.2 inquiries per day; in the week prior to this announcement, the daily average was 0.1 inquires per day.

6. Regarding Capcom's Awareness of Ransom Demands

While it is true that the threat actor behind this attack left a message file on the devices that were infected with ransomware containing instructions to contact the threat actor to negotiate, there was no mention of a ransom amount in this file. As explained in previous announcements, Capcom consulted with law enforcement and determined to not engage the threat actor in negotiations; the Company in fact took no steps to make contact (see the company's November 16, 2020 announcement), and as such Capcom is not aware of any ransom demand amounts.

While there have been no changes to the most recent forecast for the Capcom Group's consolidated business results (for the fiscal year ended March 31, 2021), 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 the incident. As a company that handles digital content, it is treating this incident with the utmost seriousness, and will take the appropriate action to address any requests or directions provided by law enforcement and other relevant authorities in each country. At the same time, Capcom will endeavor to further strengthen its management structure while coordinating with the relevant organizations to pursue its legal options regarding criminal acts.

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