NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

2nd Quarter of 2021

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary

This report is the result of surveys and analysis by NTTDATA-CERT on quarterly global trends from its own perspective based on cybersecurity-related information collected during the period.

Cyberattack Trends Observed through the Tokyo 2020 Olympic and Paralympic Games

A number of cyberattacks were carried out during the Tokyo 2020 Olympic and Paralympic Games (hereinafter, “Tokyo Olympics and Paralympics”), which were held in Tokyo from July through September 2021, although none affected the operation of the Games. While sponsoring organizations such as The Tokyo Organizing Committee of the Olympic and Paralympic Games were targeted, cyberattacks were also carried out against their peripheral stakeholders such as supply chains and spectators at the Tokyo Olympics and Paralympics. Incidents such as personal information leaks were also reported. This document describes our theory that the spread of COVID-19 and the spread of cyberattacks around the world contributed to cyberattacks against the sponsoring organizations and their peripheral stakeholders.

Cost of Leaving Vulnerabilities of FortiGate Untreated

In May 2019, Fortinet released CVE-2018-13379, which is a venerability of FortiGate for SSL-VPN devices. Since many organizations have not yet taken appropriate countermeasures against CVE-2018-13379, damage has been reported caused by exploiting the vulnerability. CVE-2018-13379 is a vulnerability that exists in an SSL-VPN feature that provides access to the inside of an organization from an external environment. As its degree of danger is high due to the potential leakage of authentication information, Fortinet and both Japanese and overseas security organs continue to raise people’s awareness of this issue. This document examines why many organizations have not taken countermeasures yet, despite such awareness raising, and describes appropriate countermeasures against the vulnerability and actions that can be taken to accelerate the countermeasures.

Zero-click Attacks that Evade “BlastDoor” in iPhone

A zero-click attack targeting the iPhone, using “Pegasus,” was reported in August 2021. The attacker exploited a vulnerability contained in the iPhone to enable memory access to the outside of the processing area and installed Pegasus to tap the device to steal its information. It is confirmed that the attacker evaded “BlastDoor,” which is a security feature implemented in iOS 14, and the mechanisms for preventing the exploitation of the existing iOS vulnerabilities. A security update has already been released. Updating iPhone to iOS 14.8 or a later version can fix this vulnerability. The goal of the attacker is to continue to monitor a particular activist secretly, using Pegasus. If a wide range of targets are attacked,

someone may notice the attack, analyze the attack method and detect it. This defeats the attacker's intended purpose. As this type of attack does not target general users, the attack has already been discovered and countermeasures are also now available, damage will not spread to general users, as long as their device is updated.

Outlook

In July to September 2021, damage caused by web skimming continued to occur on EC sites using EC-CUBE. The situation suggests that there are still some websites where this vulnerability has been left untreated and falsification has not yet been noticed. It is predicted that incidents related to EC-CUBE on EC sites will continue to be made public.

As there is the possibility that the Omicron variant may spread again during the Beijing Olympics and Paralympics, while the spread of cyberattacks is expected to change very little, it is predicted that phishing attacks and supply chain attacks on peripheral stakeholders will be carried out again during the Beijing Games, just like when the Tokyo Olympics and Paralympics were held.

The advancement of AI technology and AI-based services are currently attracting people's attention and there is a concern that attackers could attempt AI-based "deepfakes" as an attack method in the future.

2. Featured Topics

2.1. Cyberattack Trends Observed through Tokyo 2020 Olympic and Paralympic Games

2.1.1. Examples of Cyberattacks during Tokyo 2020 Olympic and Paralympic Games

The Tokyo 2020 Olympic and Paralympic Games (hereinafter, “Tokyo Olympics and Paralympics”) were held in Tokyo from July to September 2021. They were unusual games, because they were postponed for one year and special measures such as no spectators were taken due to the impact of COVID-19.

As such large events attract global attention, they are also targeted by cyberattacks. The Tokyo Olympics and Paralympics were not exceptional, either. A total of more than 4 hundred million cyberattacks targeted operating systems of the Games and networks during the Games. However, it has been reported that all of the attacks were blocked by countermeasures and the operation of the Games was not affected [1].

Table1 shows examples of reported cyberattacks related to the Tokyo Olympics and Paralympics. While sponsoring organizations such as The Tokyo Organizing Committee of the Olympic and Paralympic Games (hereinafter, “the Organizing Committee”) and The Japanese Olympic Committee were targeted, cyberattacks were also carried out against their peripheral stakeholders such as the supply chains of system subcontractors and prospective spectators at the Tokyo Olympics and Paralympics. Incidents such as personal information leaks were also reported.

Why did these cyberattacks target not only the sponsoring organizations, but also their peripheral stakeholders? The following section describes our views on the causes of cyberattacks targeting peripheral stakeholders and the characteristics of such cyberattacks.

Table1: Examples of Cyberattacks Related to Tokyo Olympics and Paralympics

No.	Overview of Attack	Time of Occurrence	Attack Target	Description of Attack
1	Fake email calling for people’s support in response to the delay in the Games for one year	Late April 2020	Prospective spectators of Tokyo Olympics and Paralympics	There was a confirmed case of a fake email that called for support for damage caused by the postponement of the Games. Then, the attackers told the victims that they could purchase a ticket very cheaply in compensation for a donation and tricked the victims into sending their personal information by email after receiving the money. [2]

2	Ransomware infecting a server for the Secretariat of Japanese Olympic Committee	Late April 2020	Japanese Olympic Committee	The Japanese Olympic Committee was the victim of a cyberattack, which infected a server and PC in the secretariat and prevented access to internal data. However, there was neither an internal data breach nor a demand for money. All of the terminals in the secretariat were replaced and operation resumed [3].
3	Fake relay broadcasting website for Tokyo Olympics and Paralympics	After March 2021	Prospective spectators of Tokyo Olympics and Paralympics	A fake website for the live broadcast of the torch relay in Yamaguchi Prefecture was found and the Yamaguchi Prefectural Police put out an alert. When the user tried to play a video on the website, they were requested to enter personal information such as their ID, password, name and credit card number [4]. There were also other cases of attacks using a fake relay broadcasting website, including an attack that triggered browser notification spam, when a fake live sports broadcasting website was accessed [5].
4	Leakage of personal information of people involved in the Organizing Committee caused by unauthorized access to Fujitsu's ProjectWeb	May 2021	System subcontractor	Unauthorized access was made to ProjectWeb, Fujitsu's project management service, and there was leakage of information about projects related to the National Center of Incident Readiness and Strategy for Cybersecurity. The leaked information included personal information of those involved in the Organizing Committee [6].
5	Fake website pretending to refund purchased tickets	Unknown	Prospective spectators of Olympics and Paralympics	A phishing site for refunding purchased tickets was found [7].

2.1.2. Examination of Cyberattacks during the Tokyo 2020 Olympic and Paralympic Games

Although the operation of the Tokyo Olympics and Paralympics was not affected, cyberattacks were carried out targeting not only the Organizing Committee and other sponsoring organizations, but also peripheral stakeholders such as the supply chains of system subcontractors and prospective spectators of the Games. It is speculated that one of the causes of such attacks was the spread of COVID-19 during the Tokyo Olympics and Paralympics. Those cyberattacks might also have coincided with the ongoing spread of cyberattacks. This section describes the above two views in detail.

(1) View (1): Spread of COVID-19

COVID-19 was first discovered at the start of 2020 and spread quickly throughout the world.

It also affected the Tokyo Olympics and Paralympics significantly, which were postponed for one year and then held without spectators. How did the postponed opening of the Games and no spectators affect cyberattacks targeting the Tokyo Olympics and Paralympics?

As the Organizing Committee was originally planning to hold the Games in 2020, it secured the Games' sites, associated facilities, airline tickets and other resources. However, the postponement of the Games for one year required the Committee to make cancellations and changes, which might incur additional costs and compensation for damage. An attacker took advantage of such media reports and rumors and carried out a phishing email attack to an unspecified large number of people by sending the email described in "Fake email calling for people's support in response to the delay in the Games for one year" (No.1 in Table1).

Recently, more and more people are watching sports through relay broadcasting and collecting information on the Internet. As it was decided that the Games would be held without spectators, Internet relay broadcasting and transmission of information such as game results was enhanced. Some attackers undoubtedly predicted that more people would search for and view websites related to the Tokyo Olympics and Paralympics. There was an actual phishing attack using a fake relay broadcasting website for the Tokyo Olympics and Paralympics (No.3 in Table1). Also, the change to the Games being held without spectators caused the issue of refunding tickets. This inspired some attackers to carry out a phishing attack using a fake website pretending to refund purchased tickets (No.5 in Table1).

As described above, the spread of COVID-19 changed when the Tokyo Olympics and Paralympics were held and how the spectators could enjoy the Games. It is speculated that attackers also changed their attack method from cyberattacks on sponsoring organizations to phishing attacks accordingly.

(2) View (2): Spread of cyberattacks

This section analyzes the relationships between the items in *10 Major Security Threats* (hereinafter, "*10 Major Threats*"), which is issued by IPA, [8]and the cyberattacks targeting the Tokyo Olympics and Paralympics. The 10 major threats are selected through careful discussion and voting by experts in the information security field and they include security incidents, cyber attacks, vulnerabilities and other events that significantly affected society over the last year. Table2 lists the 10 major threats in the 2021 edition, which was created based on events that occurred in 2020.

The cyberattacks targeting the Tokyo Olympics and Paralympics include phishing attacks such as "Fake email calling for support in response to the delay in the Games for one year" (No.1 in Table1) and "Fake relay broadcasting website for Tokyo Olympics and Paralympics" (No.3 in Table1). Phishing attacks rank second in the 10 major threats to individuals. Supply chain attacks such as "Leakage of personal information of people involved in the Organizing Committee by unauthorized access to Fujitsu's ProjectWeb" (No.4 in Table1) rank fourth in the 10 major threats to organizations. As phishing attacks and supply chain attacks also ranked high in the 10 major threats in the 2020 edition, it is clear that these two types of attacks have been widespread for a long time.

Since the cyberattacks targeting the Tokyo Olympics and Paralympics resemble the cyberattacks that rank high in the 10 major threats in recent years, it can be said that the

cyberattacks targeting the Tokyo Olympics and Paralympics coincided with the ongoing spread of cyberattacks.

Table2: 10 Major Security Threats 2021 [8]

Ranking last year	Individuals	Ranking	Organizations	Ranking last year
1st	Fraudulent Use of Smartphone Payment	**1st**	Ransomware Attacks	5th
2nd	Phishing Fraud for Personal Information	**2nd**	Confidential Information Theft by APT	1st
7th	Cyberbullying and Fake News	**3rd**	Attacks on New Normal Work Styles such as Teleworking	NEW
5th	Extortion of Money by Blackmail or Fraudulent Methods with E-mail, SMS, etc.	**4th**	Attacks Exploiting Supply Chain Weaknesses	4th
3rd	Fraudulent Use of Leaked Credit Card Information	**5th**	Financial Loss caused by Business E-mail Compromise	3rd
4th	Unauthorized Use of Internet Banking Credentials	**6th**	Data breach by Internal Improprieties	2nd
10th	Personal Information Theft from Services on the Internet	**7th**	Suspension of Business due to Unexpected IT Infrastructure Failure	6th
9th	Internet Fraud caused by Fake Warnings	**8th**	Unauthorized Login to Services on the Internet	16th
6th	Malicious Smartphone Applications	**9th**	Unintentional/Accidental Data breach	7th
8th	Unauthorized Login to Services on the Internet	**10th**	Increase in Exploitations following the Release of Vulnerability Countermeasure Information	14th

2.1.3. Conclusion

This section described the possibility that due to the spread of COVID-19, cyberattacks targeting the Tokyo Olympics and Paralympics might have been carried out not only on the Organizing Committee and other sponsoring organizations, but also peripheral stakeholders, as well as the possibility that such attacks might have coincided with the ongoing spread of cyberattacks.

As the current trend in the spread of COVID-19 continues and the ongoing spread of cyberattacks since the Tokyo Olympics and Paralympics are taken into account, it is predicted that large global events in the future will also have to deal cyberattacks targeting not only the sponsors of the events, but also their peripheral stakeholders. Therefore, countermeasures should also be taken by the supply chains of system subcontractors and event participants

considering the risk of cyberattacks. During the Beijing 2022 Olympic and Paralympic Games, which will start in February 2022, there will be very little change in the current COVID situation and the ongoing spread of cyberattacks. It is predicted that the same trends observed during the Tokyo Olympics and Paralympics will continue in the Beijing Games.

3. Data Breach

3.1. Cost of Leaving Vulnerabilities of FortiGate Untreated

In May 2019, Fortinet disclosed the vulnerability CVE-2018-13379 [9]. CVE-2018-13379 is a vulnerability that exists in Fortinet's SSL-VPN device "FortiGate" and it was described as a serious vulnerability in the Quarterly Report on Global Security Trends in 2nd Quarter of 2019. Since this vulnerability could have a significant impact, Fortinet's Product Security Incident Response Team (PSIRT) and both Japanese and overseas security organs raised people's awareness of this issue repeatedly during that period [10]. However, many organizations haven't taken countermeasures against the vulnerability yet, despite the awareness raising efforts by the security organs. As a result, attacks exploiting the vulnerability continue to cause leakage of authentication information from Fortinet's FortiGate and intrusion into it.

In November 2020, someone exploited this vulnerability to collect FortiGate authentication information of about 50,000 units and released the information on the Internet, which drew significant attention [11]. FortiGate authentication information of 5,000 units used in Japan accounted for about 10% of the released information. The affected Japanese organizations included universities and other educational institutions, aviation organizations and independent administrative corporations. In September 2021, Fortinet revealed leakage of FortiGate authentication information of another 87,000 units [12]. This section examines why countermeasures against this vulnerability have not fully been implemented yet and describes appropriate countermeasures against the vulnerability and actions that can be taken to accelerate the countermeasures.

Table3 shows the events that occurred between May 2019 and September 2021 in chronological order.

Table3: Awareness Raising Events by Fortinet PSIRT and Security Organs

Date	Organization	Title
May 24, 2019	Fortinet PSIRT	Leakage of a FortiOS system file via SSL-VPN, using a specially modified HTTP resource request [13]
September 2, 2019	JPCERT/CC	Awareness raising regarding vulnerabilities of multiple SSL VPN products [14]
July 16, 2020	Fortinet PSIRT	ATP 29 targeting defects in SSL VPN [15]
November 27, 2020	JPCERT/CC	Release of information about the hosts affected by the vulnerability CVE-2018-13379 of the SSL-VPN feature in Fortinet's FortiOS [16]
November 30, 2020	Fortinet PSIRT	CVE-2018-13379-related update [17]

December 3, 2020	National center of Incident readiness and Strategy for Cybersecurity	Awareness raising concerning critical infrastructure operators, regarding CVE-2018-13379, a vulnerability of Fortinet VPN [18]
December 11, 2020	Fortinet PSIRT	Invasion of FireEye Red Team Tools [19]
April 2, 2021	CISA/FBI	CISA - FBI joint advisory regarding exploitation of Fortinet vulnerabilities [20]
April 3, 2021	Fortinet PSIRT	Patch and vulnerability management [21]
May 27, 2021	FBI	MI-000148-MW [22]
June 1, 2021	Fortinet PSIRT	Unable to prioritize patch application to ensure network integrity [23]
September 8, 2021	Fortinet PSIRT	Release of FortiGate SSL-VPN authentication information by a malicious actor [12]

3.1.1. Explanation of Vulnerability CVE-2018-13379

CVE-2018-13379 is a vulnerability that exists in FortiGate, Fortinet's SSL-VPN product. FortiGate provides SSL-VPN, which is suitable for accessing the company's internal network via the Internet during a business trip or when working from home [24]. There are different SSL-VPN access modes. Tunnel mode uses VPN client software provided by Fortinet, whereas web mode uses a web browser. The portal screen used to set these modes has a path traversal vulnerability [25]. The attacker may be able to exploit this vulnerability to specify and download any file on FortiGate without authentication. In particular, the attacker specifies the path to a sslvpn_websession file stored in FortiGate to try to download it. This file contains the user ID and plaintext password required for SSL-VPN connection. If the attacker succeeds in downloading the file, they can pretend to be a genuine user by using its authentication information and connect to FortiGate via SSL-VPN [26].

Once the attacker succeeds in SSL-VPN connection, they can access the organization's internal system in the same manner as a genuine user. As a result, damage is not limited to leakage of confidential information stored in FortiGate. They also escalate into secondary damage such as data breaches and falsification in other systems through the exploitation of the vulnerability of CVE-2018-13379.

Table4 below shows the firmware versions of FortiGate that have this vulnerability.

Table4: Firmware Versions with the Vulnerability

Patch System	Applicable Versions
5.4 system	5.4.6 ～ 5.4.12
5.6 system	5.6.3 ～ 5.6.7
6.0 system	6.0.0 ～ 6.0.4

3.1.2. Ransomware Attacks Exploiting CVE-2018-13379

(1) Example of attacks using the ransomware “Cring”

According to Trend Micro, attacks using the ransomware “Cring” accounted for about 70% of the ransomware attacks against which the company provided incident support between January and April 2021 [27]. Cring performs standard ransomware activities such as file encryption, generation of ransom notes, deletion of backup files and disabling of system recovery features. The attacker enters the target network and uses a tool inside the network to steal account authentication information and sends a batch file needed to establish continuous communications with the C&C server, and then executes the ransomware and infects the system. The company detected a number of cases in Japan, where the attacker exploited vulnerabilities of FortiGate to enter a system, especially the vulnerability of CVE-2018-13379. Another point to note is that some of the attacked organizations had already applied a security patch to their system before the attack, but still received Cring-based damage, because the password of an SSL-VPN user in FortiGate had not been changed.

(2) Exploitation by the cyberattack group “APT29”

The National Cyber Security Centre of the United Kingdom (NCSC), The Communications Security Establishment of Canada (CSE), and CISA and NSA in the U.S. reported that APT29, which is a cyberattack group that is also known as “Dukes” and “Cozy Bear,” was using vulnerabilities of Fortinet as the starting points of some of their attacks as follows [28].

“ATP29” uses various tools and techniques to mainly target governments, diplomatic channels, think tanks, medical institutions and energy facilities to obtain their information. Through 2020, ATP29 may steal information about the development of COVID-19 vaccines and intellectual properties of various organizations engaged in the development of COVID-19 vaccines in Canada, the U.S. and the U.K. In its recent attacks targeting the research and development of COVID-19 vaccines, the group has identified and exploited vulnerabilities through the vulnerability scan of a particular external IP address held by the organization as the initial vector of attack. In addition to the vulnerability of FortiGate CVE-2018-13379, the other reported vulnerabilities include vulnerabilities of Citrix, which were described in the Quarterly Report on Global Security Trends in the 4th Quarter of 2019, and vulnerabilities of Pulse Secure, which were described in Quarterly Report on Global Security Trends in the 1st Quarter of 2020 [29] [30].

3.1.3. Countermeasures against the vulnerability of CVE-2018-13379

The application of a security patch is required as part of countermeasures against the vulnerability of CVE-2018-13379. Since the vulnerability was revealed in May 2019, by October 2021 2 years and 6 months have already passed. Therefore, if the security patch has not been applied, it is highly likely that an attack has already been carried out and authentication information has leaked. When applying the security patch at this stage, therefore, it should be assumed that authentication information has already leaked and secondary damage is being caused. Such secondary damage should also be addressed in addition to taking countermeasures against the vulnerability. This section describes the

interim countermeasures that should be taken immediately, the permanent countermeasures that should be implemented in full scale, and the countermeasures for preventing secondary damage.

(1) Interim countermeasures against the vulnerability of CVE-2018-13379

① Stopping SSL-VPN connection

If SSL-VPN connection is not used, stop the SSL-VPN connection. Stopping the SSL-VPN connection prevents anyone from using the SSL-VPN connection. Attackers cannot exploit stolen authentication information to make unauthorized access via the SSL-VPN connection. As, however, this also prevents genuine users from using the SSL-VPN connection, it is not a convenient method.

(2) Permanent countermeasures against the vulnerability of CVE-2018-13379

① Application of a security patch

Apply a security patch that fixes the vulnerability of CVE-2018-13379. Table5 below shows the versions in which the vulnerability has already been fixed by the patch application [13].

Table5: FortiGate Versions in which CVE-2018-13379 has been Fixed

Version	Fixed Version	Support Status
5.4 system	5.4.13	Support ended
5.6 system	5.6.8 or later	Support ended
6.0 system	6.0.5 or later	Support ended
6.2 system	6.2.0 or later	Currently supported

When this report was written, 5.4 and 5.6 systems were no longer supported by the manufacturer. In principle, Fortinet does not provide a security patch for them. As the 6.0 system is also subject to the limited support that provides security patches only for critical vulnerabilities, there is a chance no security patch will be provided. Maintain the version 6.2 system in order to continue to receive Fortinet's support that provides security patches. In that case, note that if the latest security patch is applied to an old version to upgrade the version suddenly, the settings may not be inherited correctly. To inherit the settings correctly, therefore, apply patches, in stages, in the order recommended by the manufacturer to upgrade to the latest version [31] [32].

(3) Interim countermeasures against secondary damage (leakage of authentication information)

① Investigation on entry into ForigGate

Since the vulnerability of CVE-2018-13379 was revealed in May 2019, 2 and a half years have passed. If no countermeasures have been taken, it is highly likely that an attack has already been carried out. Therefore, if countermeasures are to be introduced long after the vulnerability of CVE-2018-13379 was first revealed, it should be fully expected that an attacker has already succeeded in attacking FortiGate, stolen authentication information for SSL-VPN connection and made unauthorized login by pretending to be a genuine user.

Therefore, whether FortiGate has been entered by attackers before or not must be investigated.

② Change of the password of an SSL-VPN user

If an attacker has already succeeded in unauthorized login to FortiGate, as shown in the example in 3.1.2, the attacker can enter FortiGate by exploiting its authentication information, even after a security patch is applied to FortiGate. Therefore, if an attacker has already entered FortiGate, the password must be changed after a security patch is applied.

(4) Strengthening countermeasures against secondary damage (leakage of authentication information)

Not limited to when authentication information is breached due to the vulnerability of CVE-2018-13379, IP address restrictions on the transmission source of SSL-VPN connection and the introduction of multi-factor authentication are strengthening countermeasures against leakage of authentication information.

① IP address restrictions on the transmission source of SSL-VPN connection

When the IP address of the transmission source of SSL-VPN connection can be fixed, restricting the IP address of the transmission source of the SSL-VPN connection can block unauthorized login from the IP address of an attacker. In that case, unauthorized login can be prevented, even if authentication information is breached.

② Introduction of multi-factor authentication

Multi-factor authentication, which combines multiple authentication methods, should be introduced by adding property authentication such as biometrics and a one-time password to intelligent authentication such as a user ID and password. Multi-factor authentication can prevent unauthorized login, even if one of its authentication methods is breached. For this reason, it is an effective countermeasure against data breach, not only when authentication information is stolen, but also when a vulnerable password is used and when a password is entered on a phishing website by accident. It is strongly recommended to use a multi-factor authentication method, when a service with login authentication is made available on the Internet, using a port that can be accessed by anyone.

3.2. Examining Why Vulnerability of CVE-2018-13379 was Left Untreated

This section examines why the vulnerability ofCVE-2018-13379 was left untreated for a long time without countermeasures against it.

Did an organization that did not take any countermeasure against the vulnerability of CVE-2018-13379 for two and a half years have any reason why it was unable to apply a security patch? For example, you might speculate that because the organization was in an industry or corporate scale where it could not afford a security countermeasure, it failed to apply a security patch. To determine whether such speculation is correct, we gathered and analyzed information about some organizations that had experienced leakage of FortiGate authentication information due to the exploitation of the vulnerability. Table6 shows results of reported information about the organizations that we summarized. Table6 indicates that damage was caused to organizations in a wide range of industries and no particular industry was targeted solely, including government and municipal offices, private businesses and

educational institutions. Each organizational scale also varied with neither different nor common features. Therefore, it is believed that the reason why these organizations did not take countermeasures against the vulnerability for such a long time had nothing to do with their industry or organizational scale.

Table6: List of Organizations that Experienced Leakage of Authentication Information

Classification	Name of Organization	Scale (e.g. No. of staff)
Government and municipal offices	National Police Agency [33]	No. of staff: 7,995 [34]
	Gifu Prefectural Office [35]	No. of staff: about 5,000 (excluding the public safety commission and the board of education) [36]
	Imari Municipal Office in Saga Prefecture [11]	No. of staff: 431 (excluding reappointed staff) [37]
	Togocho Town Office in Aichi Prefecture [38]	No. of staff: 308 [39]
	Japan National Tourism Organization [40]	No. of staff: 207 [41]
Private businesses	Recruit Co., Ltd. [35]	No. of staff: 15,807 (including casual staff and part-timers) [42]
	Nissin Sugar Co., Ltd. [43]	No. of staff: 259 [44]
	DeCurret Inc. [45]	No. of staff: 52 [46]
Educational institutions	Keio University [33]	No. of teaching staff: 2,791 (full-timers, including those under term contract) [47]
	Sapporo University [48]	No. of teaching staff: 76 [49]
	Fukui University of Technology [50]	No. of teaching staff: 99 [51]
Medical institutions	Ichinomiya Municipal Hospital [33]	No. of doctors: 180, No. of nurses: 664 [52]

Was each organization in Table6 performing an appropriate vulnerability countermeasure process? Figure1 shows the vulnerability countermeasure cycle that we devised and the following section describes each of the processes that form the vulnerability countermeasure cycle.

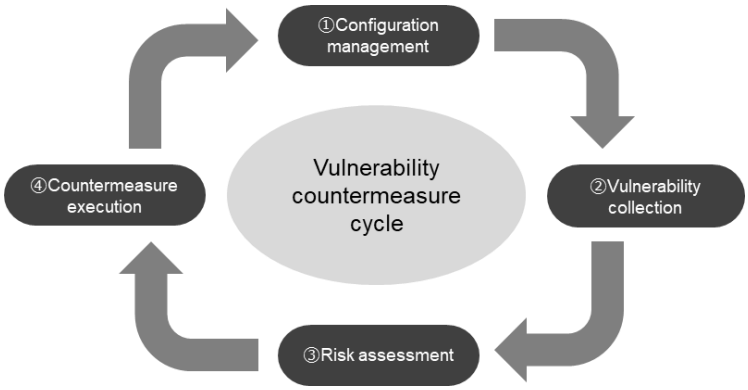


Figure1: Vulnerability Countermeasure Cycle

The first process of the vulnerability countermeasure cycle is “configuration management.”

The first step of configuration management is to understand information about the equipment used and its version information accurately. Unless the equipment information and version information is managed, the second process of “vulnerability collection” is not performed. Without this process, you cannot determine whether the equipment or software of your organization is subject to a certain vulnerability, even when the vulnerability is revealed or alerted. As a result, you might end up leaving the vulnerability untreated without considering its countermeasures.

The second process is “vulnerability collection.” In vulnerability collection, vulnerability information about the target equipment or software for which configuration management is performed is collected from their manufacturers and security information sites. Investigations and security diagnosis are also carried out to check whether there is any vulnerability in order to manage the equipment and software. It is essential to collect vulnerability information in order to detect vulnerabilities of the equipment and software. If the vulnerability information collection and the investigation process is missed, vulnerabilities may be left untreated, which will cause damage.

The third process is “risk assessment.” In risk assessment, the degree of danger of each vulnerability is assessed. More specifically, the necessity of countermeasures against each vulnerability and its severity are determined by assessing the probability of success in an attack on the target equipment or software that exploits the vulnerability, the degree of impact of the attack, if it is successful, etc. If you assess the severity of each vulnerability wrongly in risk assessment, the fourth process of “countermeasure execution” will be delayed and you may be attacked.

In the fourth process of “countermeasure execution,” countermeasures are implemented against each vulnerability. In this process, it is important not to make mistakes in countermeasures. Problems rarely occur in the task of applying a security patch. However, if you take a wrong step in interim countermeasures or strengthening countermeasures, you cannot achieve their effects. Some countermeasures are effective, only if particular conditions are met, such as certain system configurations and settings. You may also misunderstand interim countermeasures and strengthening countermeasures and implement them to a system that does not meet the conditions.

Presume that a certain vulnerability has been left untreated somewhere in the above four processes. First, if configuration management is not performed properly, you cannot identify the version of the equipment or software used in your organization. Therefore, even when vulnerability information is released, you will fail to perform risk assessment and countermeasure execution. Even if the vulnerability is alerted repeatedly, you will not notice that your equipment or software is subject to it and leave the vulnerability untreated for a long time.

Next, assume that vulnerability collection is not performed properly. If you don’t collect vulnerability information, even if you perform configuration management thoroughly, you will not notice that you have the vulnerabilities reported by manufacturers and security vendors. Also, if you only receive security-related news, but nothing else, you may not notice all vulnerability news. If you fail to collect vulnerability information or you don’t check your configuration information against such vulnerability information thoroughly, vulnerabilities will probably be left untreated for a long time.

If you fail to perform risk assessment, you may assess a certain risk as lower than it actually

is, by mistake, which will delay the countermeasure execution. However, as serious vulnerabilities are alerted repeatedly by manufacturers and security organs, it is hard to believe that organizations will continue to fail risk assessment and leave vulnerabilities untreated for a long time, as long as they perform configuration management and vulnerability collection properly.

If countermeasure execution is not in place, verification may take a long time before applying a security patch. However, the verification certainly should not take as long as 2 years and six months or so.

For this reason, it is speculated that vulnerabilities were left untreated for a long time, because a system administrator in the information systems department or information security department did not perform configuration management and vulnerability collection properly, and as a result, they failed to recognize the vulnerabilities. In news reports, some organizations revealed that they did not recognize the vulnerability situation, until an external source told them about it [33] [35]. If an organization does not perform configuration management and vulnerability collection properly, the succeeding processes of risk assessment and countermeasure execution cannot function. The vulnerability countermeasure cycle must be implemented fully to prevent vulnerability-based damage. However, it is not easy for organizations that have left vulnerabilities untreated for a long time to promote the vulnerability countermeasure cycle. Such organizations must determine their configuration management method and vulnerability collection method first, and then start collecting information about their management targets. They must also determine their risk assessment criteria. This is costly and also requires security skills. Also, it is probably a much larger task than something that can be handled by the system administrator alone. Some organizations may outsource the operation and maintenance of FortiGate and other network equipment to an external vendor. Many external vendors, however, only offer hardware maintenance and do not include security measures such as patch application and vulnerability countermeasures in the scope of their work. In that case, such organizations should be sure to include the vulnerability countermeasure cycle in the details of their outsourced operation.

As described above, the vulnerability countermeasure cycle must be implemented fully by involving not only the organization itself, but also its external outsourced vendors. To solve such problems, the organization faces issues such as a staff shortage, associated cost and the formation of internal rules. Therefore, the management should direct efforts in the implementation of the vulnerability countermeasure cycle across the entire organization from the top down. Leaving vulnerabilities untreated for a long time incurs a management risk, as it leads to the shutdown of operation and other damage caused by a cyberattack. Cybersecurity Management Guidelines Ver2.0, published by the Ministry of Economy, Trade and Industry, states that “The management must recognize cybersecurity risks and promote countermeasures through their leadership [53].” The management should clarify who is responsible for security countermeasures, along with their role, according to these guidelines, and then direct the person responsible to make efforts in the implementation of the vulnerability countermeasure cycle.

Vulnerabilities will not be left untreated for a long time if the introduction status of the vulnerability countermeasure cycle must be reported to the management periodically and the operation status of the vulnerability countermeasure cycle is also audited.

3.3. Conclusion

FortiGate is an SSL-VPN device that provides an environment where the internal system of an organization is accessed from outside the organization. If vulnerabilities of FortiGate are left untreated for a long time, a range of invasions by attackers are overlooked, from entry into the main unit of FortiGate to entry into an internal system that can be accessed via SSL-VPN, which may develop into secondary and further damage. Depending on the scale of damage, it may be unavoidable to suspend the business. If a ransomware attack forces the organization to pay a huge ransom or requires the affected system to take a long time to recover, the organization will suffer from deteriorating business conditions, and in the worst scenario, it will not survive.

For this reason, the management must recognize that leaving vulnerabilities untreated for a long time leads to management risks, therefore someone must be appointed who will be responsible for security countermeasures within the organization, clarify their role, and direct them to make efforts in the implementation of the vulnerability countermeasure cycle from the top down. The directed responsible member of the organization and its information systems department must establish and comply with the operation of the vulnerability countermeasure cycle. Vulnerabilities will be well-controlled if the management plays the main role in establishing an audit mechanism that checks to make sure that the operation of the vulnerability countermeasure cycle is executed appropriately.

4. Vulnerabilities

This chapter explains CVE-2021-30860, which is a vulnerability found in the iPhone, and provides examples of attacks that exploit the vulnerability.

4.1. Zero-click Attacks that Break through “BlastDoor” in iPhone

On August 24, 2021, Citizen Lab, a security research center in the University of Toronto, reported that the Bahraini government had attempted zero-click attacks on the iPhones of multiple human right activities by using the spyware “Pegasus,” which had been developed by an Israeli NSO group [54]. The Bahraini government seems to have tapped the activists’ phones using Pegasus in order to monitor their activities.

4.1.1. Description of Zero-click Attack

First found around 2016, the zero-click attack method causes malware or other infection without requiring the victim to operate their device. Since the malware infects the device without the victim actually using the device, the victim does not notice that they are falling victim to an attack.

On December 20, 2020, Citizen Lab revealed a zero-click attack that was carried out using “Kismet” to exploit a vulnerability contained in iMessage, a default iPhone application [55]. Although Citizen Lab was unable to identify the vulnerability exploited by the zero-click attack, it analyzed the victim’s iPhone in an attempt to understand the attack method. Immediately before the victim’s iPhone accessed the Pegasus installation server, it made abnormal connections to a number of iCloud partitions, as shown in “Highly unusual connections to Apple servers” in Figure 2 . Then, the phone connected to ”*.regularhours.net” and installed Pegasus from the Pegasus Installation Server. The analysis of the log recorded between those two processes suggests that the attack used the imagent process, which is an embedded application for processing iMessage and FaceTime, to execute it with a root privilege. For this reason, Citizen Lab suspects that the attack exploited a vulnerability contained in the imagent process.

4.1.2. Description of BlastDoor

Apple has implemented the “BlastDoor” feature in iOS 14 and later as a countermeasure against zero-click attacks exploiting vulnerabilities of iMessage. BlastDoor is a mechanism that processes messages within its original service process, which is separated from the imagent process (Figure 3). A message extracted in the identityservicesd process is stored in the MessagesBlastDoorService process, and then undergoes processes such as XML file formatting and data serialization. As no network operation occurs in this case, the MessagesBlastDoorService processes the data in a sandbox environment. The imagent process receives the data after the completion of the MessagesBlastDoorService process. Therefore, even if the message contains malicious code, the code is not executed directly on iOS. Since this feature was introduced, zero-click attacks based on Kismet have stopped

working.

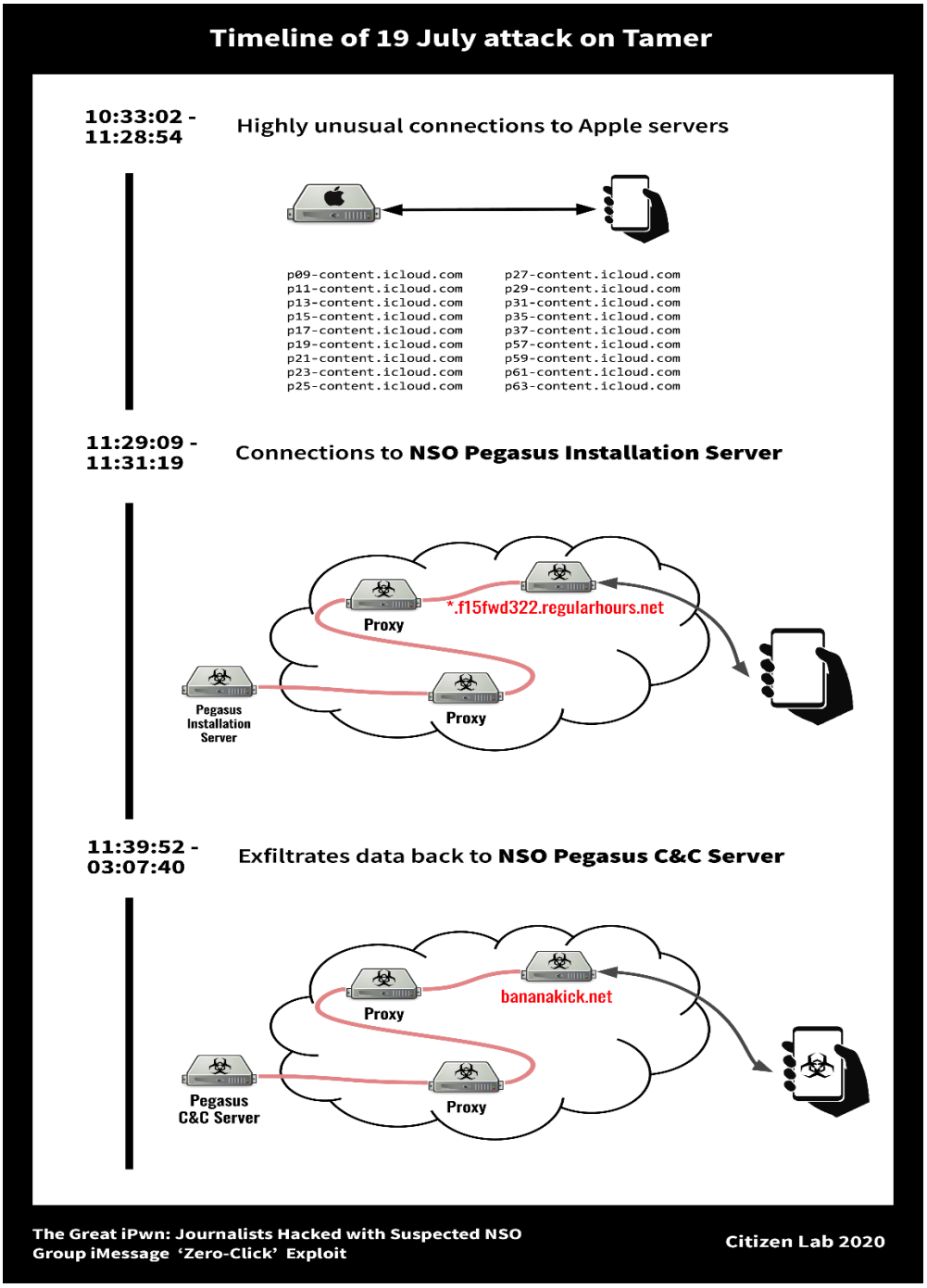


Figure 2: Timeline of Attack Exploiting Kismet [55]

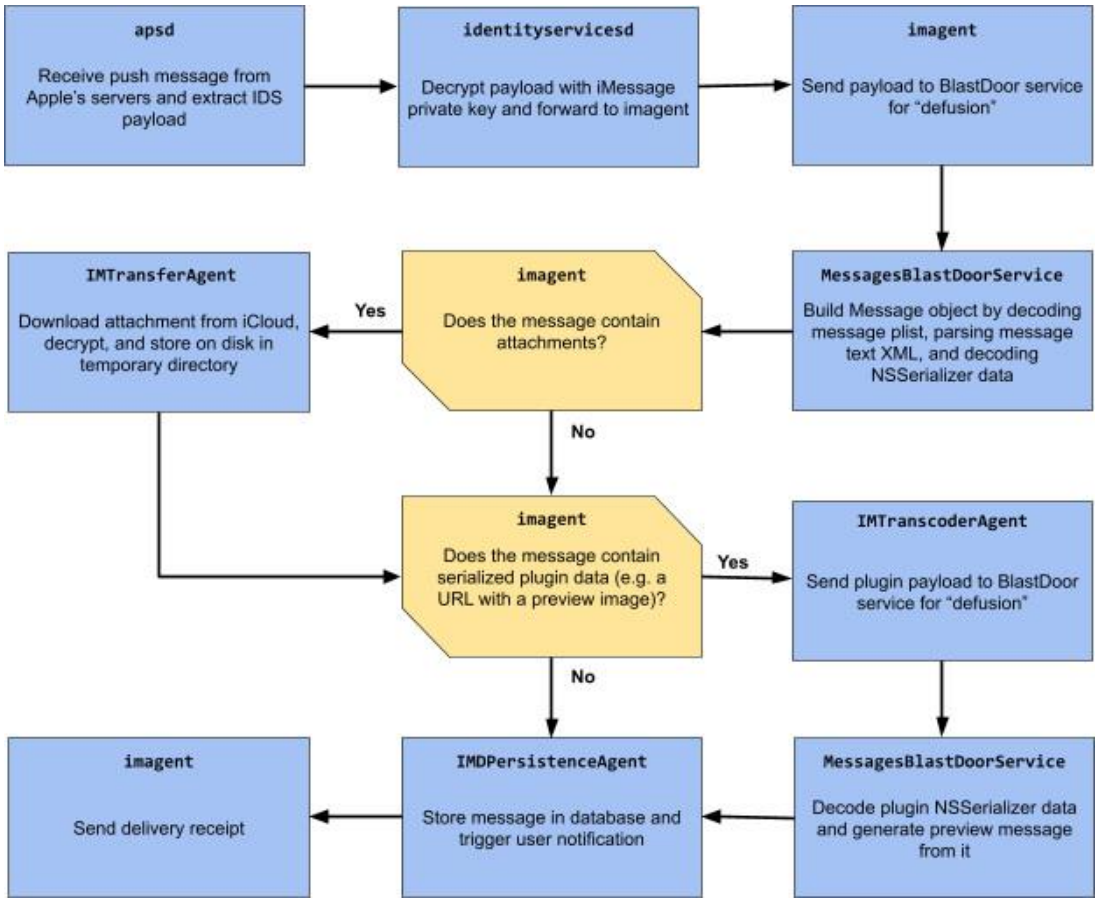


Figure 3: iMessage Process Pipeline with BlastDoor [56]

4.1.3. Zero-click Attacks that Evade "BlastDoor"

This section describes a type of attack that can achieve "Forced Entry" into the "Blast Door" of the iPhone. Such an attack uses "ForcedEntry," which exploits CVE-2021-30860, a vulnerability contained in iMessage [57]. This vulnerability exists in CoreGraphics, which is Apple's vector rendering framework in iMessage. If it processes a malicious file, an integer overflow occurs, allowing memory access to outside the processing range. In a concrete example, the above problem occurs when a PSD file for Adobe Photoshop that is disguised as a GIF. When a malicious file disguised as a PSD file is sent and processed, the above-mentioned BlastDoor is evaded to hack the iPhone. The analysis of the issue conducted by Trend Micro discovered that ForcedEntry evaded not only BlastDoor, but also the following two mechanisms that prevented the exploitation of iOS vulnerabilities [58].

(1) Disabling address space layout randomization (ASLR)

Address space layout randomization (ASLR) is a mechanism that suppresses the exploitation of vulnerabilities through memory corruption. When the OS executes a program, it randomly arranges the addresses of CPU memory areas that store data, such the data area, stack area and heap area. This mechanism makes it difficult for the attacker to send a malicious command to a particular memory address.
iOS also has an ASLR feature. According to Trend Micro, however, the ASLR feature was disabled before the exploitation of ForcedEntry. How the attacker managed to disable the ASLR feature has not yet been determined.

(2) Bypassing the pointer authentication code (PAC)

Pointer Authentication Code is a mechanism that suppresses the exploitation of vulnerabilities through memory corruption. When the OS executes a command, it affixes a signature (i.e. generates a pointer authentication code) to the pointer that will be used to call a process stored at another address in the CPU memory. The OS verifies the pointer authentication code before executing the called process. If the verification fails, it stops the process. This mechanism makes it difficult for the attacker to execute malicious code that is produced by falsifying a pointer. According to Trend Micro's analysis, however, the attacker successfully called a process by bypassing the security feature for the pointer authentication code [58].

As described above, the ForcedEntry attacker evaded the two defense mechanisms that were always in operation, when iOS executed a process. The method used to disable ASLR and bypass the pointer authentication code feature is yet to be determined. It is believed that the ForcedEntry attacker used a sophisticated attack method.

4.2. Conclusion

This section examined the vulnerability of CVE-2021-30860, which is contained in iMessage, as well as an example of an attack using "ForcedEntry," which exploits it. The attack in the example used a sophisticated, complex attack method that evaded multiple defense mechanisms of the iPhone and damaged the iPhone, which is said to be secure. This vulnerability can be fixed by updating the version of the iPhone to iOS 14.8 or later. The original purpose of the attacker is to continue to monitor a particular activist secretly, using Pegasus. If such an attack is carried out on a wide range of targets, its activity will be exposed more easily and defeat the purpose. For this reason, it is believed that the version update can prevent damage from expanding to general users.

5. Malware/Ransomware

5.1. Malware Attacks Using ProxyShell, Vulnerabilities of Microsoft Exchange Server

“ProxyShell” is a general term for three vulnerabilities of Microsoft Exchange Server, which were found in April 2021 [59]. As many servers haven’t had these vulnerabilities fixed yet [60], they may be attacked.

In April and May 2021, Microsoft released update programs to fix ProxyShell [61] [62] [63]. In early November 2021, seven months after the discovery of ProxyShell, about 27,000 servers have not had ProxyShell fixed yet [60]. As a result, there have been many cyberattacks targeting Microsoft Exchange Servers that haven’t had ProxyShell fixed yet [64]. More specifically, there has been damage caused by the ransomware “LockFile” in cyberattacks targeting the above-mentioned Microsoft Exchange Servers. This ransomware is rampant in various industries [65]. With the discovery of ProxyShell as the starting point, LockFile emerged as new ransomware, which was first found in the U.S. in July 2021. While this ransomware is rampant mainly in the U.S. and Asia, its damage is also expanding globally in a wide range of industries [65]. Although the names of affected organizations and the total amounts of their damages are unknown as of October 2021, the damage is in a broad range of industries from manufacturing and financial services to engineering, legal and tourism [65].

This chapter explains the general flow of an attack exploiting ProxyShell, characteristics of ProxyShell and recommended countermeasures against it.

5.1.1. Steps of Attack

This section explains the flow of the attack based on Figure4. The attacker takes a total of 10 steps to enter the target organization and execute malware. Steps up to ④ are related to ProxyShell and explained in detail below.

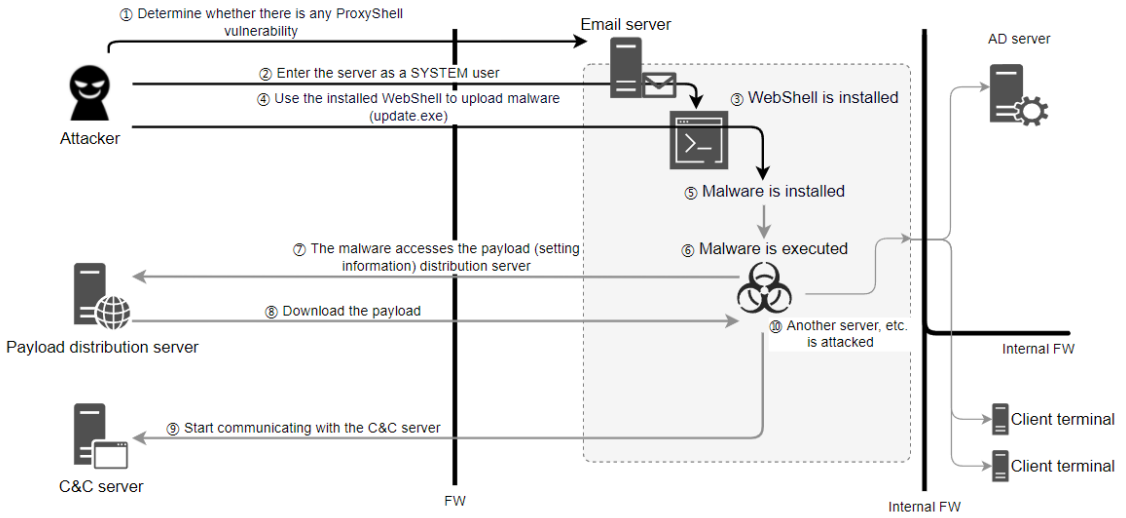


Figure4: Flow of Attack Exploiting ProxyShell

[Steps of Attack]

① Explore whether there is any ProxyShell vulnerability:
The attacker scans multiple Microsoft Exchange Servers on the Internet and identifies Microsoft Exchange Servers that have a ProxyShell vulnerability.

② Enter the backend server as a SYSTEM user:
The attacker exploits CVE-2021-34473 to attack the Microsoft Exchange Server with a vulnerability, which was identified in step ①. When the attacker requests the client access service (explained in the next section) for a modified URL, the client access service rewrites the URL for the backend service [66]. As a result, the attacker can access the backend service as a SYSTEM user [66].

③ Install WebShell:
After entering the backend service, the attacker attaches a WebShell file to an email and sends it to the mailbox of the target Microsoft Exchange Server from another server prepared by the attacker. WebShell refers to a backdoor program or its mechanism that the user uses to execute any command on a server [67]. Since a SYSTEM user does not have a mailbox, the attacker exploits CVE-2021-34523 to escalate their privilege from a SYSTEM user to the administrator of the Microsoft Exchange Server. This allows the attacker to use PowerShell with administrator privileges to retrieve the WebShell file from the mailbox of the administrator and save the file [66]. In this state, however, the WebShell file can only be saved in a folder that is prohibited from executing a program. Therefore, the attacker uses a special command for exporting PowerShell mail for Exchange Server management that has the vulnerability of CVE-2021-31207 that can write a file into any path to export the mailbox containing the WebShell file to the Webroot folder as a pst file [68]. The attacker extracts the WebShell file from the pst file and executes it in the Webroot

folder [68].

④ Use the installed WebShell to download malware:
The attacker downloads malware such as ransomware from the attacker's machine to execute the malware on the machine on which the Microsoft Exchange Server is operating. The attacker uses an arbitrary command on WebShell to upload the malware (update.exe).

In ⑤ and the subsequent steps, the attacker starts the malware and starts communicating with the C&C server to reproduce the malware or set ransomware in another server remotely.

5.1.2. Danger of ProxyShell Vulnerabilities

This section explains how dangerous ProxyShell vulnerabilities are, based on the high level of impact of ProxyShell and the ease of its attacks.

(1) Impact level: Theft of information assets and ransomware damage due to attacks exploiting the three vulnerabilities

As explained in Steps of Attack above, ProxyShell refers to three different vulnerabilities. When the three are executed in order, the attacker can execute commands easily and remotely without authentication [69]. As an attack is established when the three vulnerabilities operate in a coordinated manner, it is also called an "exploit chain [70]." "Exploit chain" is a new term that started being used around 2019. It refers to a series of multiple exploits (program that attacks security vulnerabilities contained in software or a system [71]). Table 7 shows the three vulnerabilities that make up the ProxyShell exploit chain [61] [62] [63] [68].

Table 7: Three ProxyShell Vulnerabilities Revealed by Microsoft

No.	CVE number	Characteristic of vulnerability
1	CVE-2021-34473	Vulnerability that can be exploited to execute a code remotely by avoiding authentication
2	CVE-2021-34523	Vulnerability exploited to escalate privileges
3	CVE-2021-31207	Vulnerability exploited to overwrite any file by bypassing a security feature

The section marked as "Client access services" in Figure5 is the frontend services in Microsoft Exchange Server client access services (hereinafter, "CAS") and the section marked as "Backend services" is its backend services. CAS provides authentication service and proxy service to client connection [72]. According to Microsoft, the vulnerability of CVE-2021-34473 exists in CAS frontend services. As the attacker can communicate with frontend services directly via the Internet, they can attack the vulnerability of CVE-2021-34473 easily. Backend services receive requests from various clients such as POP3/IMAP4/SMTP clients and Web clients (HTTP/HTTPS), which have been forwarded by CAS [72]. Since client software such as Outlook and a web browser normally accesses a mailbox and other features in backend services via CAS, it cannot access the backend services directly. However, if

CVE-2021-34473 exists, the attacker can exploit the vulnerability to access the backend services [59].

As the vulnerabilities of CVE-2021-34523 and CVE-2021-31207 cannot be exploited, unless the attacker enters the backend services [66]. Therefore, Microsoft explains that the probability that they can be exploited by an attacker is low [61] [63]. However, CVE-2021-34473 is a vulnerability that overlooks entry into backend services. Once the attacker achieves successful entry, they can also exploit CVE-2021-34523 and CVE-2021-31207, which have lower probability of exploitation. When these three vulnerabilities are linked in the end, any command can be executed [64].

When the attacker can execute any command, they may steal mail information from a mail database in a backend service, then download and execute ransomware. As such attacks may lead to data breaches and system suspension, the level of their impact on the attacked organization is believed to be high.

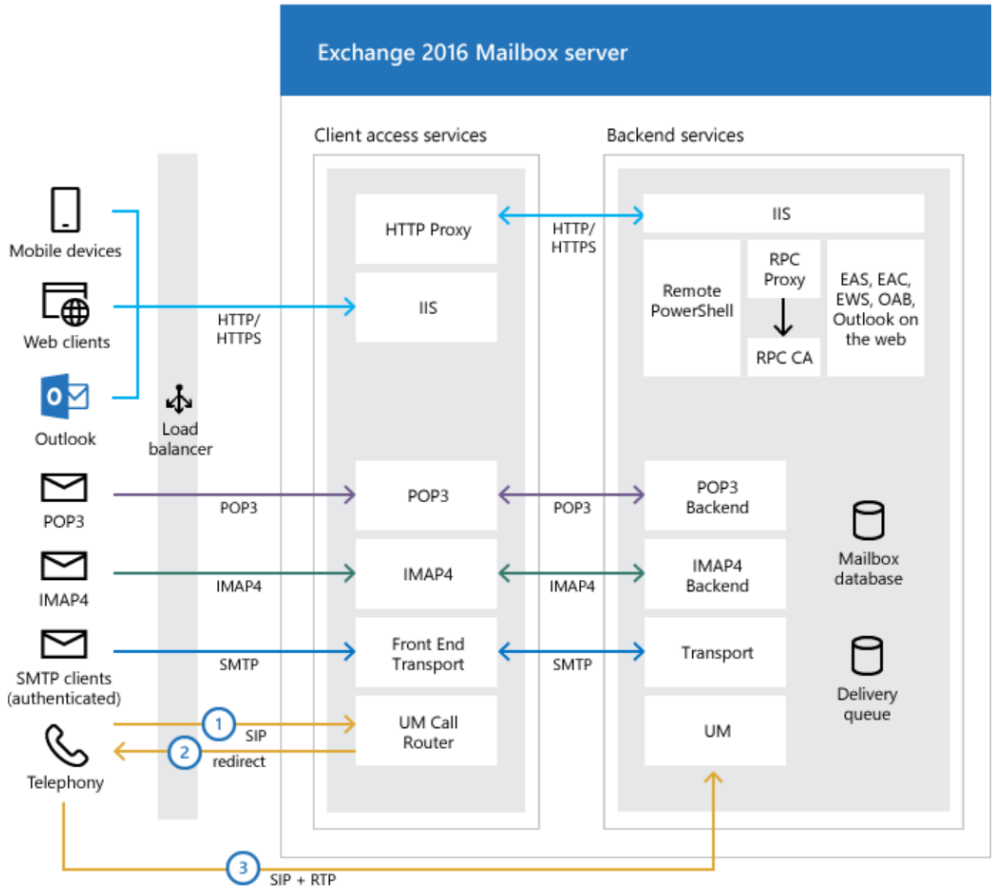


Figure5: Diagram of Network Configuration of Microsoft Exchange Server 2016, Presented by Microsoft

(2) Ease of attacks: Exposure of more than 400,000 Exchange Servers to the Internet

Microsoft Exchange Servers are exposed to the Internet, taking into account the convenience of their users so that they can access them from anywhere by using their smartphone, PC and other devices [73]. A total of about 400,000 Microsoft Exchange Servers are exposed to the Internet [59]. Attackers actively scan Microsoft Exchange Servers that have attackable vulnerabilities [64]. Under such conditions, more than 100 incident reports on ProxyShell were released in just two days in August 2021, which was four months after the discovery of the vulnerabilities [74]. This indicates that many attacks exploiting ProxyShell are still occurring, although it has been a long time since information about the vulnerabilities and their update programs were released.

5.1.3. Conclusion

As mentioned at the beginning of this chapter, about 27,000 servers have not had ProxyShell fixed as of early November 2021, seven months after the discovery of ProxyShell [60]. As examined in the article on data breaches in the Quarterly Report on Global Security Trends in the 2nd Quarter of 2021, the main reason is believed to be that a system

administrator in the information systems department or information security department does not perform configuration management and vulnerability collection properly, and as a result, they fail to recognize the vulnerabilities. However, even if the ProxyShell vulnerabilities are managed properly, it is still difficult to determine the degree of their response priority. Of the three vulnerabilities, CVE-2021-34473 alone cannot be exploited to install WebShell. The probability of exploitation of the second and third vulnerabilities is described as low [61] [63]. This may make the system administrator think that they don't need to be controlled. In addition to assessing risks of each vulnerability, the system administrator should also understand that an attack can be successful with the combination of the three vulnerabilities, based on information about the actual cyberattacks, as well as assessing the risks incurred when the attacker uses WebShell.

Since some cyberattacks become successful with a combination of multiple vulnerabilities, as in this case, risks of vulnerabilities should be assessed based on the information collected from analytical articles released by security-related companies and security experts. Then, updated programs should be applied immediately.

5.2. Examples of Ransomware Damage

Table8 shows some of the ransomware incidents that occurred in the 2nd quarter of 2021.

Table8: Examples of Ransomware Damage in 2nd Quarter of 2021

No.	Date of Occurrence	Victim	Overview of Incident
1	July 2, 2021*	Arthur J. Gallagher (AJG)	Arthur J. Gallagher (AJG), which is an international insurance intermediation and risk management company based in the U.S., received a ransomware attack and mailed infringement notices to individuals who might be affected. [75]
2	July 7, 2021	NIPPN CORPORATION	On the network operated by NIPPN BUSINESS SYSTEM, one of its subsidiaries, some servers and terminals were encrypted, causing damage to about 90% of its systems. The systems were unable to start up. [76]
3	July 9, 2021*	Kaseya	Since the U.S. IT company Kaseya's software fell victim to a ransomware (ransom virus) attack, the damage has been expanding worldwide. The company announced that up to 1500 businesses have been affected. [77]
4	August 1, 2021	The state of Lazio, Italy	The healthcare IT system of the Lazio state government in Italy fell victim to a cyberattack and was unable to book new appointments for COVID-19 vaccinations. [78]
5	August 11, 2021*	Accenture	Marketing information of Accenture was posted on a leak website for the ransomware "LockBit." [79]

6	August 13, 2021	Bewith, Inc	Bewith, Inc, which is a subsidiary of Pasona Group Inc., revealed that information of 15,421 past applicants for casual work and 9,375 employees had been encrypted due to unauthorized access. [80]
7	August 19, 2021	ORIENTAL CONSULTANTS	Since its business-related data was encrypted, some information may have leaked. The company calculated an extraordinary loss of about 750 million yen. [81]
8	August 30, 2021	Abecho Shoten Co., Ltd.	Abecho Shoten Co., Ltd. revealed that business-related data stored in its servers, terminals and other devices might have leaked due to unauthorized access to its internal network. [82]
9	September 10, 2021*	YAGAMI Co., LTD.	YAGAMI Co., LTD., which sells medical equipment and welfare products, fell victim to a ransomware attack on its internal network. The company announced that its internal network connections had been affected. [83]
10	September 19, 2021	Crystal Valley	Crystal Valley's computer system was infected by ransomware and the company's day-to-day operations were significantly interrupted. [84]

*: Date the article was published

6. Outlook

Continued Release of Information concerning EC Site Incidents Related to EC-CUBE

The Quarterly Report in the 1st quarter of 2021 covered cross-site scripting vulnerabilities of EC-CUBE [85]. The article alerted readers that vulnerabilities of EC-CUBE were easily targeted by attackers. In the 2nd quarter of 2021 (July to September 2021), web skimming continues to occur on EC sites using EC-CUBE, as shown in Table9. This trend matches the speculation made in the report in the 1st quarter. It is believed that some sites haven't recognized falsification yet, as the vulnerabilities have been left untreated. It is predicted that information concerning EC site incidents related to EC-CUBE will continue to be released.

In addition, new vulnerabilities of EC-CUBE may also be discovered in the future, as seven vulnerabilities were found in May and June 2021 [85]. Attention should be paid to vulnerability announcements by EC-CUBE CO.,LTD.

Table9: 2nd Quarter of 2021 -
Incident Examples of EC Sites Using EC-CUBE
[86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98]

#	Date Released	EC Site Name	EC Site Operating Company
1	2021/7/6	Hoick	SONGBOOKCafe Inc.
2	2021/7/12	COSMOS Online Store	COSMOS Pharmaceutical Corporation
3	2021/7/13	TRANSIC	TRANSIC
4	2021/7/14	Yomifa Net	Yomiuri Joho Kaihatsu Osaka Co.,Ltd.
5	2021/7/20	EC Site Pro Shop Takumi	CANDEAL DESIGN Co.,Ltd.
6	2021/7/21	MAINICHIGENKI Official Shopping Site	MAINICHIGENKI.CO.,LTD.
7	2021/7/26	KQLFT TOOLS	SONS-MARKET
8	2021/8/16	FUKUYAONLINE	Fukuya Co.,Ltd.
9	2021/8/18	THE HAIR BAR TOKYO Online Store	Gap International Inc.
10	2021/8/23	KOMAKI MUSIC website	KOMAKI MUSIC,INC.
11	2021/9/7	TACHIKICHI ONLINE SHOP	TACHIKICHI CORP.
12	2021/9/14	Ise Sekiya Online Shop	SEKIYA Co., Ltd.
13	2021/9/16	Omni EC System	GR Inc.

Cyberattacks Targeting Beijing 2022 Olympic and Paralympic Games

The cyberattacks that targeted the Tokyo 2020 Olympic and Paralympic Games (hereinafter, “Tokyo Olympics and Paralympics”) were carried out on not only the Organizing Committee of the Tokyo Olympics and Paralympics and other sponsoring organizations, but also peripheral stakeholders such as the supply chains of system subcontractors and prospective spectators of the Games. Section 2.1 described that there were relationships between the cyberattacks on peripheral stakeholders and the spread of COVID-19 and the ongoing spread of cyberattacks around the world.

The Beijing 2022 Olympic and Paralympic Games (hereinafter, “Beijing Olympics and Paralympics”) start in February 2022. Based on what was examined in section 2.1, it is predicted that phishing attacks and supply chain attacks on peripheral stakeholders will be carried out again during the Beijing Olympics and Paralympics, which are a large global event, just like when the Tokyo Olympics and Paralympics were held. As the infection status of COVID-19 in China is stabilizing [99], it seems that the Beijing Olympics and Paralympics will be held with spectators (who live in China, only) [100]. However, since the Omicron variant of COVID-19 has started to spread across the world, the number of infections in China may surge, which will force the Beijing Games to have no spectators. For this reason, it is predicted that phishing attacks using fake relay broadcasting sites will be carried out again in the Beijing Olympics and Paralympics. Moreover, as there is only a small time gap between the Tokyo and Beijing Olympics and Paralympics, there will be very little change in the ongoing spread of cyberattacks. Therefore, it can be speculated that cyberattacks will be carried out along with the current trends such as phishing attacks and supply chain attacks.

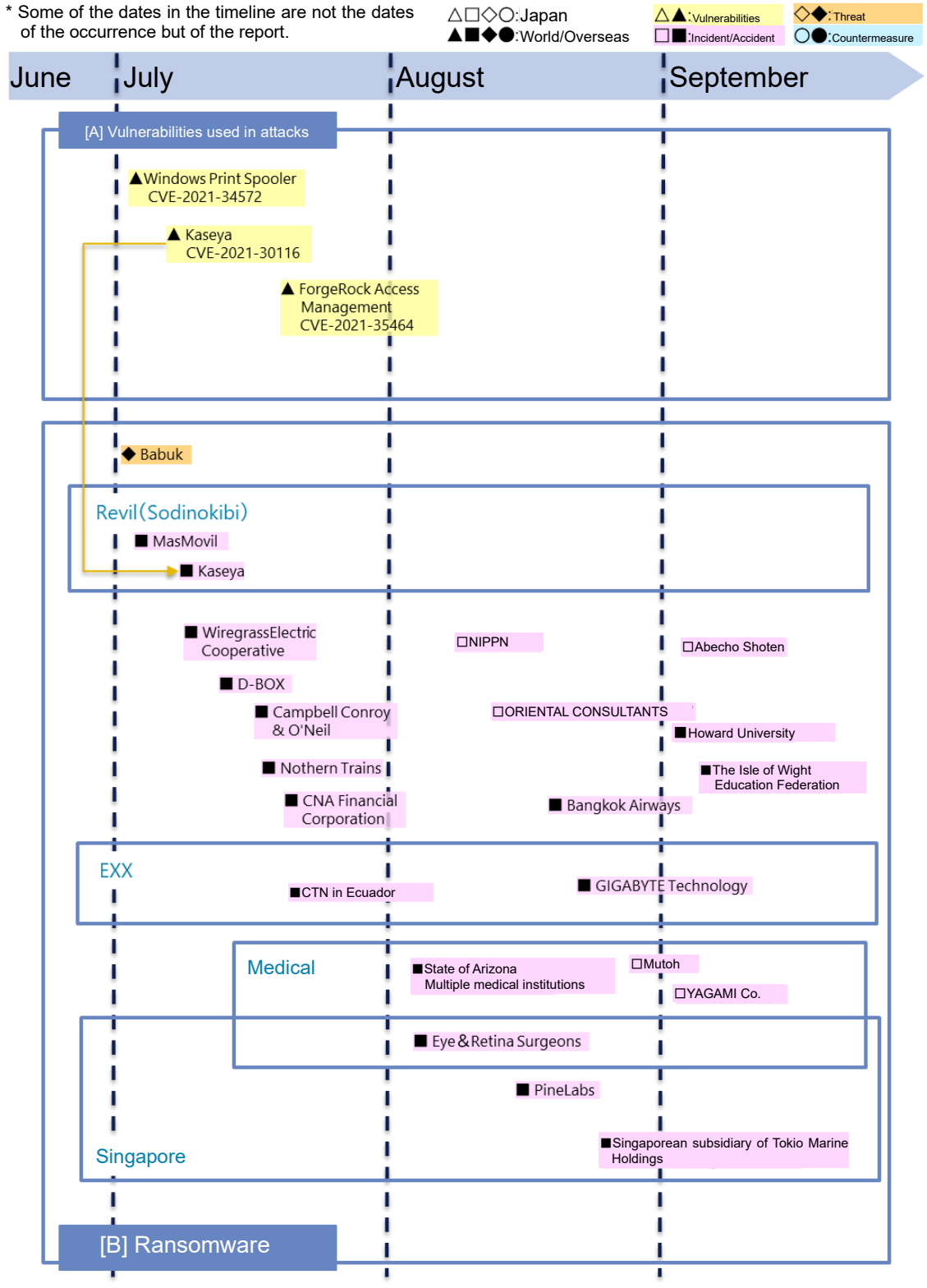
Attacks Exploiting Deepfakes

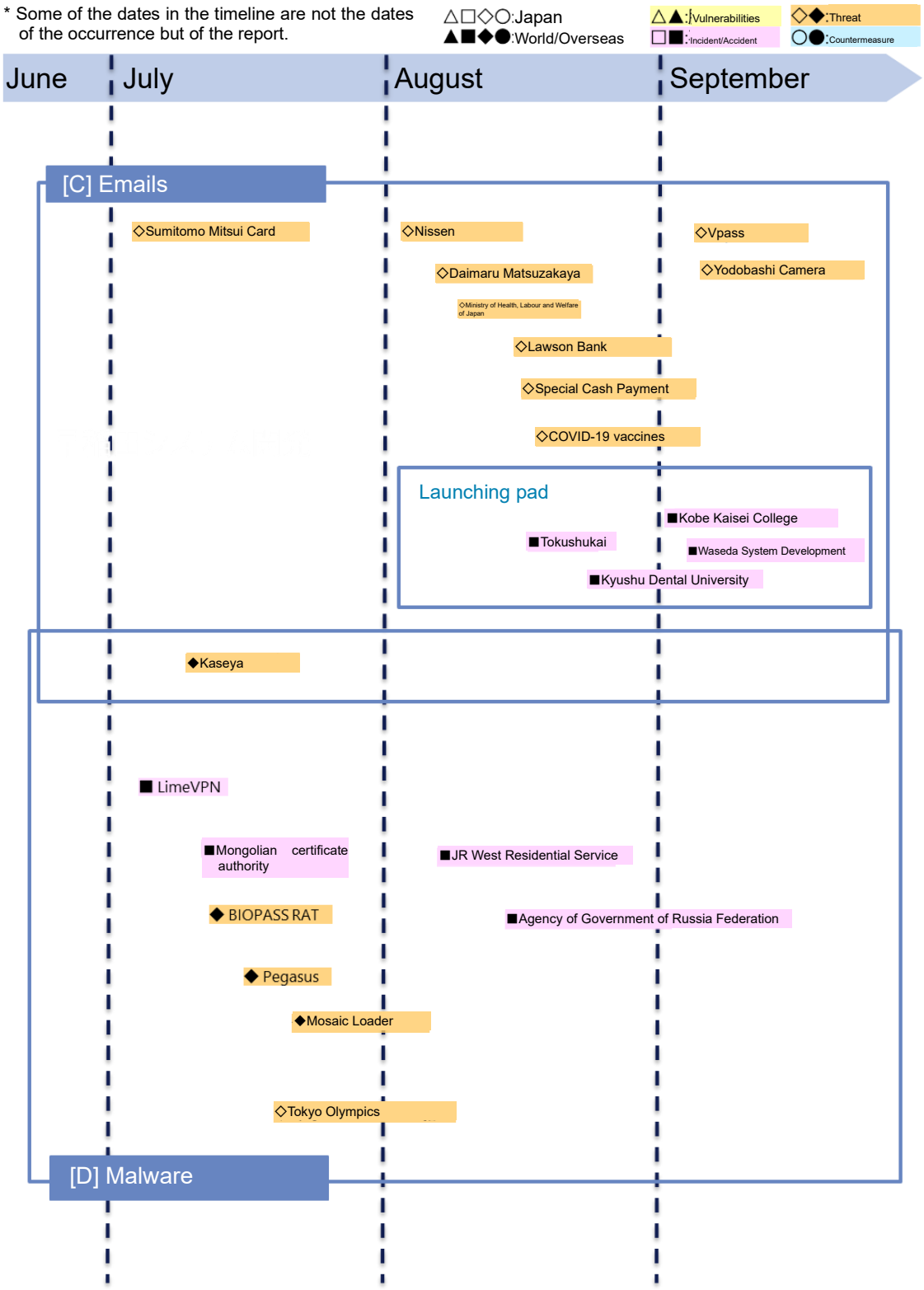
The advancement of AI technology and AI-based services are currently attracting people’s attention and there is a concern that attackers could attempt AI-based “deepfakes” as their attack methods in the future [101]. Deepfakes are fake videos and audio produced using AI deep learning. Since 2020, they have been seen as threats in the cybersecurity industry [102]. In 2019, there was an actual case of a deepfake attack on an energy company based in the U.K., which gave about 26 million yen to the attacker who exploited a deepfake. The CEO of the energy company received a phone call from his boss, who was the CEO of its parent company in Germany, requesting him to make a remittance. After fulfilling the request, he realized that the voice on the phone was actually produced using a deepfake [103].

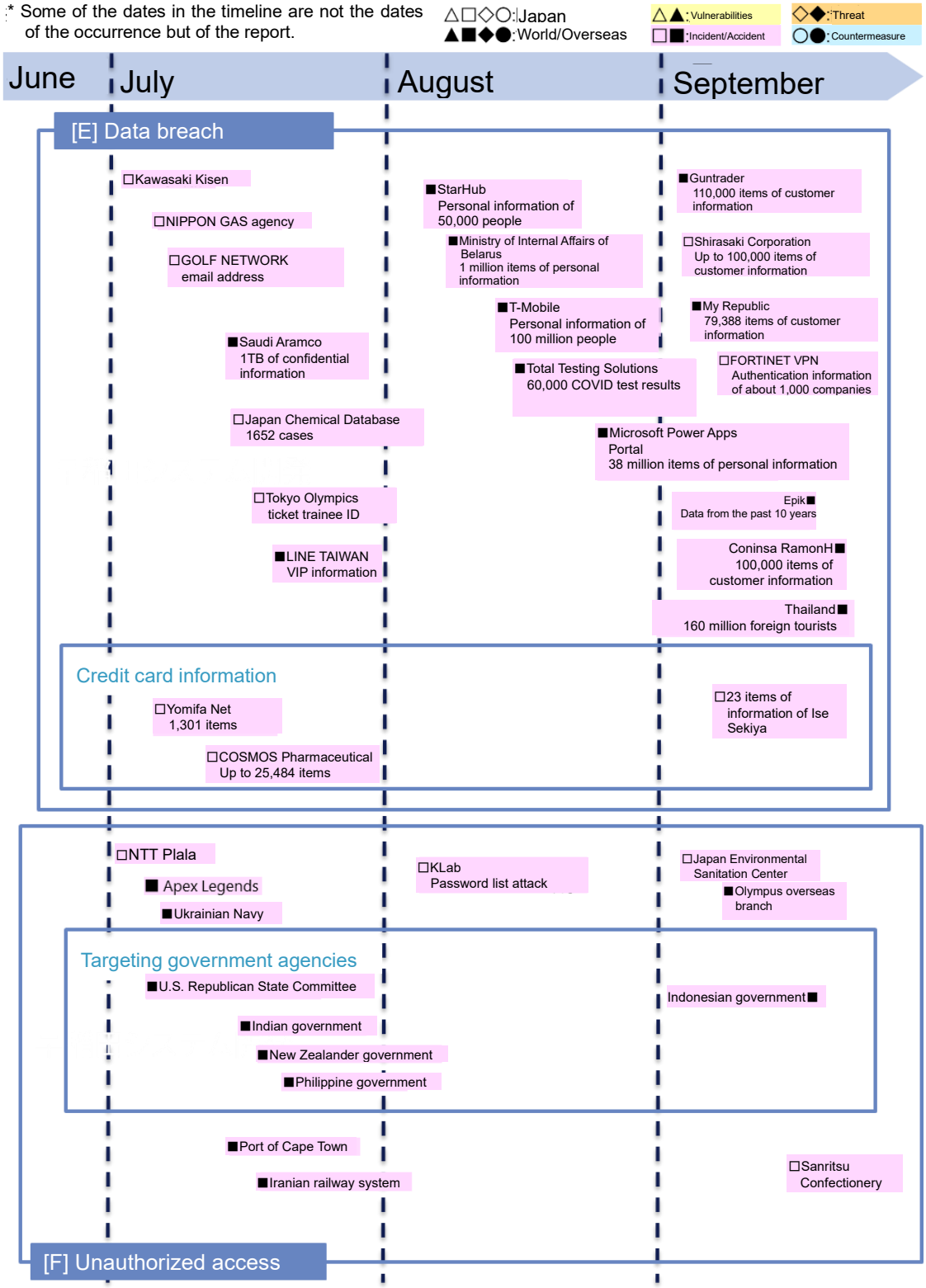
Considering this situation, some companies have already developed and released security countermeasure tools. Microsoft released “Microsoft Video Authenticator,” which can analyze videos and photos and indicate the probability of artificial production as well as their reliability by scoring them [104].

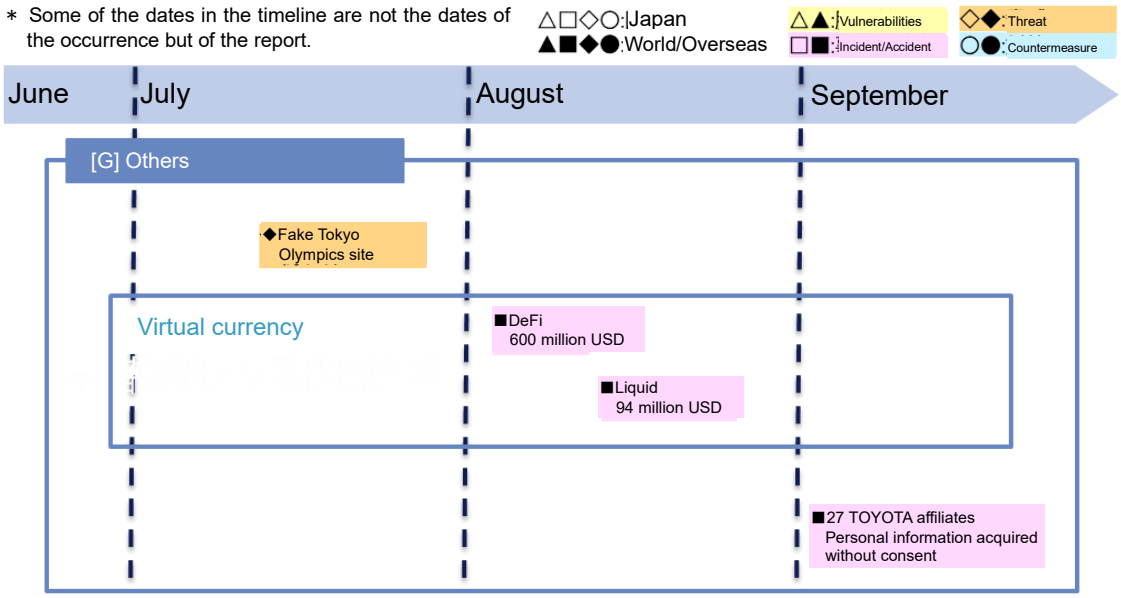
As deepfake technology is expected to improve further [104], it will be necessary not only to introduce such a tool, but also to acquire information literacy to identify fake information.

7. Timeline









References

[1] 日本放送協会, “東京オリ・パラ期間 サイバー攻撃 4億5000万回 運営に影響なし,” 21 10 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20211021/k10013316541000.html.

[2] トレンドマイクロ株式会社, “【注意喚起】東京オリンピックへの支援を呼びかける偽の寄付メールに注意,” 30 4 2020. [オンライン]. Available: https://www.is702.jp/news/3675/.

[3] 株式会社朝日新聞社, “JOCにサイバー攻撃、全PC交換　金銭要求「ない」,” 25 6 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP6S6V5TP6NULZU00B.html.

[4] 株式会社日本経済新聞社, “聖火リレーで偽サイト、警察が捜査　生中継うたう,” 15 5 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUE149WN0U1A510C2000000/.

[5] トレンドマイクロ株式会社, “東京オリンピック開会直前、偽のTV放送予定ページからブラウザ通知スパムへ誘導する攻撃を確認,” 19 7 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/28308.

[6] 株式会社日本経済新聞社, “五輪組織委の個人情報も流出　富士通の不正アクセス問題,” 4 6 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUE04A290U1A600C2000000/.

[7] 株式会社カスペルスキー, “オリンピックに乗じたオンライン詐欺：5つのパターン,” 28 7 2021. [オンライン]. Available: https://blog.kaspersky.co.jp/olympic-scams-top-5-schemes/31272/.

[8] 独立行政法人 情報処理推進機構, “情報セキュリティ10大脅威 2021,” 27 1 2021. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2021.html.

[9] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第2四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[10] Fortinet, Inc., “PSIRTと責任ある開示,” 20 8 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/psirt-and-the-responsible-disclosure.

[11] piyolog, “警察庁内端末不正アクセスと5万件の脆弱なVPNホストの公開についてまとめてみた,” 30 11 2020. [オンライン]. Available: https://piyolog.hatenadiary.jp/entry/2020/11/30/063636#f-6d9a455d.

[12] Fortinet, Inc., “悪意のあるアクターがFortiGate SSL-VPNの認証情報を公開,” 8 9 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials.

[13] Fortinet, Inc., “特別に細工されたHTTPリソースリクエストによるSSL-VPNを介したFortiOSシステムファイルの漏えい,” 24 5 2019. [オンライン]. Available: https://www.fortiguard.com/psirt/FG-IR-18-384.

[14] JPCERT/CC, “複数の SSL VPN 製品の脆弱性に関する注意喚起,” 2 9 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[15] Fortinet, Inc., “SSL VPNの欠陥を標的としたATP 29,” 16 7 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/atp-29-targets-ssl-vpn-flaws.

[16] JPCERT/CC, “Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について,” 27 11 2020. [オンライン]. Available: https://www.jpcert.or.jp/newsflash/2020112701.html.

[17] Fortinet, Inc., “CVE-2018-13379 に関するアップデート,” 30 11 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/update-regarding-cve-2018-13379.

[18] 内閣サイバーセキュリティセンター, “Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について,” 3 12 2020. [オンライン]. Available: https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf.

[19] Fortinet, Inc., “FireEye レッドチームツールの侵害,” 11 12 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/fireeye-red-team-tool-breach.

[20] CISA/FBI, “FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities,” 2 4 2021. [オンライン]. Available: https://us-cert.cisa.gov/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios.

[21] Fortinet, Inc., “パッチと脆弱性の管理,” 3 4 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/patch-vulnerability-management.

[22] FBI, “MI-000148-MW,” 27 5 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/210527.pdf.

[23] Fortinet, Inc., “ネットワークの整合性を確保するには、パッチ適用を優先することが不可,” 1 6 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/prioritizing-patching-is-essential-for-network-integrity.

[24] SB C&S株式会社, “FortiGateでリモートアクセス設定　SSL-VPN編（初級者向け）,” 13 8 2020. [オンライン]. Available: https://licensecounter.jp/engineer-voice/blog/articles/20200813_fortigatesslvpn.html.

[25] ラクラウド株式会社, “SSL-VPNポータルを設定する,” [オンライン]. Available: https://www.teracloud.co.jp/manual_remotevpn_operationaldesign_portal.html.

[26] Tenable, Inc., “CVE-2018-13379、CVE-2019-11510： FortiGateおよびPulse Connect Secureの脆弱性を突いた攻撃が確認される,” 2019. [オンライン]. Available: https://jp.tenable.com/blog/cve-2018-13379-cve-2019-11510-fortigate-and-pulse-connect-secure-vulnerabilities-exploited-in.

[27] トレンドマイクロ株式会社, “ランサムウェア「Cring」の被害が国内で拡大、VPN脆弱性を狙い侵入,” 20 5 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/27830.

[28] ncsc, “Advisory:APT29 targets COVID-19 vaccine development,” 2020. [オンライン]. Available: https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

[29] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第4四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_4q_securityreport.pdf.

[30] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2020年度第1四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf.

[31] レムシステム株式会社, “Fortigateのファームウェアをv4.0からv5.0へアップグレードする手順,” [オンライン]. Available: https://www.rem-system.com/fortigate-firm-versionup/.

[32] Fortinet, Inc., “Upgrade Path Tool Table,” [オンライン]. Available: https://docs.fortinet.com/upgrade-tool.

[33] 日本経済新聞, “サイバー攻撃、「関門」が入り口に放置される欠陥,” 10 12 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODG080Z40Y0A201C2000000/.

[34] 警察庁, “図表7-1　警察職員の定員（令和2年（2020年）度）,” [オンライン]. Available: https://www.npa.go.jp/hakusyo/r02/honbun/html/w7711000.html.

[35] 株式会社日経BP, “VPNのパスワードが外部流出　脆弱性の注意喚起に気づかず,” 5 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020600011/122400071/.

[36] 株式会社マイナビ, “岐阜県庁,” [オンライン]. Available: https://job.mynavi.jp/23/pc/search/corp93217/outline.html.

[37] 佐賀県伊万里市役所, “等級及び職制上の段階ごとの職員数（令和3年4月1日現在）について,” [オンライン]. Available: https://www.city.imari.saga.jp/18291.htm.

[38] 愛知県東郷町役場, “12月1日の中日新聞報道について（続報）,” [オンライン]. Available: https://www.town.aichi-togo.lg.jp/kikaku/joho/chousei/jouhouseisaku/20201201cyber.html.

[39] 愛知県東郷町役場, “等級及び職制上の段階ごとの職員数（令和３年４月１日現在）（その１）,” 1 4 2021. [オンライン]. Available: https://www.town.aichi-togo.lg.jp/jinji/jinji/chousei/jinji/jinjigyousei/documents/r3syokuinsuusono1.pdf.

[40] 一般社団法人共同通信社, “600超の組織にサイバー攻撃,” 1 12 2020. [オンライン]. Available: https://nordot.app/706248789438039137?c=39546741839462401.

[41] 日本政府観光局, “常勤職員は令和 2 年度末,” [オンライン]. Available: https://www.jnto.go.jp/jpn/about_us/reports/f_jigyou_r2.pdf.

[42] 株式会社リクルート, “会社概要,” [オンライン]. Available: https://www.recruit.co.jp/company/profile/.

[43] 日新製糖株式会社, “当社の社内システムに対しての不正アクセスについて（続報）,” 25 12 2020. [オンライン]. Available: https://www.nissin-sugar.co.jp/cms/wp-content/uploads/2020/12/201225.pdf.

[44] 日新製糖株式会社, “会社概要,” [オンライン]. Available: https://www.nissin-sugar.co.jp/company/outline/.

[45] 株式会社ディーカレット, 1 12 2020. [オンライン]. Available: https://news.decurret.com/hc/ja/articles/360060170213.

[46] パーソルキャリア株式会社, “株式会社ディーカレットの求人・中途採用・転職情報,” [オンライン]. Available: https://doda.jp/DodaFront/View/Company/j_id__10185053863/.

[47] 慶應義塾大学, “情報公開,” [オンライン]. Available: https://www.keio.ac.jp/ja/about/learn-more/data/.

[48] 札幌大学, “VPN(仮想私設網)へサイバー攻撃に関する報道について(第2報),” 4 12 2020. [オンライン]. Available: https://www.sapporo-u.ac.jp/news/su-news/2020/12043139.html.

[49] 札幌大学, “◆教員数/教員一人当たり学生数/年齢別教員数,” [オンライン]. Available: https://www.sapporo-u.ac.jp/img/2021_kyoinsuu.pdf.

[50] 福井工業大学, “VPN(仮想私設網)へのサイバー攻撃について,” 4 12 2020. [オンライン]. Available: http://www.fukui-ut.ac.jp/news/topics/entry-6566.html.

[51] 福井工業大学, “教職員情報,” [オンライン]. Available: http://www.fukui-ut.ac.jp/ut/introduction/public/teacher/.

[52] 株式会社ケアレビュー, “一宮市立市民病院,” [オンライン]. Available: https://hospia.jp/hosinfo/1232200369.

[53] 経済産業省, “サイバーセキュリティ経営ガイドライン Ver 2.0,” [オンライン]. Available: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf.

[54] The Citizen Lab - University of Toronto, “From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits,” 24 8 2021. [オンライン]. Available: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/.

[55] The Citizen Lab - University of Toronto, “The Great iPwn Journalists Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit,” 20 12 2020. [オンライン]. Available: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

[56] Project Zero, “A Look at iMessage in iOS 14,” 28 1 2021. [オンライン]. Available: https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html.

[57] The Citizen Lab - University of Toronto, “FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild,” 13 9 2021. [オンライン]. Available: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.

[58] トレンドマイクロ社, “スパイウェア「Pegasus」の攻撃で悪用されたiPhoneのゼロクリックエクスプロイト「ForcedEntry」を解説,” 27 9 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/28782.

[59] O. Tsai, “ProxyLogon is Just the Tip of the Iceberg. A New Attack Surface on Microsoft Exchange Server!,” 2021. [オンライン]. Available: https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf.

[60] SHODAN, “Shodan report,” 7 11 2021. [オンライン]. Available: https://www.shodan.io/search/report?query=http.title%3Aoutlook+exchange.

[61] Microsoft, “Microsoft Exchange Server のセキュリティ機能のバイパスの脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207.

[62] Microsoft, “Microsoft Exchange Server のリモートでコードが実行される脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473.

[63] Microsoft, “Microsoft Exchange Server の特権の昇格の脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523.

[64] Tenable, “ProxyShell: Attackers Actively Scanning for Vulnerable Microsoft Exchange Servers (CVE-2021-34473),” 9 8 2021. [オンライン]. Available: https://www.tenable.com/blog/proxyshell-attackers-actively-scanning-for-vulnerable-microsoft-exchange-servers-cve-2021-34473.

[65] BROADCOM SOFTWARE (Symatec Enterprise Blogs), “LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers,” 21 8 2021. [オンライン]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows.

[66] ZERO DAY INITIATIVE, “FROM PWN2OWN 2021: A NEW ATTACK SURFACE ON MICROSOFT EXCHANGE - PROXYSHELL!,” 18 8 2021. [オンライン]. Available: https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell.

[67] IT Media エンタープライズ, “Webシェル攻撃とはどんなものか　Microsoft 365 Defenderが月間14万件も検出する脅威,” 15 2 2021. [オンライン]. Available: https://www.itmedia.co.jp/enterprise/articles/2102/15/news130.html.

[68] 株式会社ソフテック, “Microsoft Exchange Server の脆弱性「ProxyShell」とは,” 6 9 2021. [オンライン]. Available: https://www.softek.co.jp/SID/blog/archive/entry/20210902.html.

[69] CertNZ, “Active scanning for Microsoft Exchange Proxyshell vulnerability,” 8 8 2021. [オンライン]. Available: https://www.cert.govt.nz/it-specialists/advisories/active-scanning-for-microsoft-exchange-proxyshell-vulnerability/.

[70] SecurityNext, “「Exchange」の脆弱性「ProxyShell」に要警戒 - 悪用発生で米政府が注意喚起,” 24 8 2021. [オンライン]. Available: https://www.security-next.com/129248/2.

[71] Canon, “エクスプロイトって何ですか？普通のマルウェア攻撃と何が違うのでしょうか？,” 10 9 2015. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/qa/detail/150910_1.html.

[72] Microsoft, “クライアント アクセス サービス,” 16 9 2021. [オンライン]. Available: https://docs.microsoft.com/ja-jp/exchange/architecture/client-access/client-access?view=exchserver-2019.

[73] 株式会社ソフィス, “ProxyShell vulnerabilities in Microsoft Exchange: What to do,” 23 8 2021. [オンライン]. Available: https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/.

[74] Huntress, “Microsoft Exchange Server Still Vulnerable to ProxyShell Exploit,” 19 8 2021. [オンライン]. Available: https://www.huntress.com/blog/rapid-response-microsoft-exchange-servers-still-vulnerable-to-proxyshell-exploit.

[75] BLEEPING COMPUTER, “US insurance giant AJG reports data breach after ransomware attack,” 2 7 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-insurance-giant-ajg-reports-data-breach-after-ransomware-attack/.

[76] ScanNetSecurity, “ニップンへのサイバー攻撃、グループ会社を含む基幹システムやデータサーバも暗号化被害に,” 19 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/08/19/46145.html.

[77] 朝日新聞 Digital, “米IT企業にサイバー攻撃　世界1500社に影響拡大か,” 9 7 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP785DG0P78UHBI00F.html.

[78] GIGAZINE, “ワクチン予約システムがランサムウェア攻撃でダウン、被害を受けたイタリアの州知事は「テロリスト」とハッカーを非難,” 1 8 2021. [オンライン]. Available: https://gigazine.net/news/20210803-italys-lazio-hacker-vaccine-booking-website/.

[79] ZD Net, “Accenture says Lockbit ransomware attack caused 'no impact',” 11 8 2021. [オンライン]. Available: https://www.zdnet.com/article/accenture-says-lockbit-ransomware-attack-caused-no-impact-on-operations-or-clients/#ftag=RSSbaffb68.

[80] Scan Net Security, “パソナグループの子会社にランサムウェア攻撃、求人情報や従業員情報が被害に,” 13 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/08/19/46146.html.

[81] IT Media NEWS, “ランサムウェア攻撃で7億円超の特別損失、建設コンサル大手のオリエンタルコンサルタンツが発表,” 17 9 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2109/17/news149.html.

[82] Scan Net Security, “阿部長商店へランサムウェア攻撃、業務関連データや個人情報が暗号化,” 30 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/09/08/46258.html.

[83] Security NEXT, “医療機器販売の八神製作所、サーバがランサム被害,” 10 9 2021. [オンライン]. Available: https://www.security-next.com/129574.

[84] DataBreaches.net, “Crystal Valley Computer Systems Infected By Ransomware Attack,” 19 9 2021. [オンライン]. Available: https://www.databreaches.net/mn-crystal-valley-computer-systems-infected-by-ransomware-attack/.

[85] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2021 年度 第 1 四半期,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[86] ニュースガイア株式会社, “保育関係者向けサイトに不正アクセス - クレカやアカウント情報が流出,” 6 7 2021. [オンライン]. Available: https://www.security-next.com/127865.

[87] 株式会社コスモス薬品, “弊社が運営する「コスモスオンラインストア」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ,” 12 7 2021. [オンライン]. Available: https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf.

[88] ニュースガイア株式会社, “革製品通販サイトに不正アクセス - クレカ情報流出の可能性,” 13 7 2021. [オンライン]. Available: https://www.security-next.com/128099.

[89] ニュースガイア株式会社, “読売関連会社のネットショップに不正アクセス - クレカ情報が被害,” ニュースガイア株式会社, 14 7 2021. [オンライン]. Available: https://www.security-next.com/128114.

[90] 株式会社キ ャ ン デ ィ ル, “当社子会社が運営するオンラインショップへの不正アクセスによる個人情報漏洩に関するお詫びとお知らせ,” 20 7 2021. [オンライン]. Available: http://fs.magicalir.net/tdnet/2021/1446/20210719469018.pdf.

[91] 有限会社毎日元気 , “弊社が運営する「毎日元気公式ショッピングサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 21 7 2021. [オンライン]. Available: https://www.mainichigenki.co.jp/210721.pdf.

[92] 株式会社 SONS-MARKET, “弊社が運営する「KQLFT TOOLS」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 26 7 2021. [オンライン]. Available: https://kqlft.com/card.pdf.

[93] 株式会社フクヤ, “弊社が運営するオンラインショップへの不正アクセスによる個人情報流出に関するお詫びとご報告,” 株式会社フクヤ, 16 8 2021. [オンライン]. Available: https://www.fancy-fukuya.co.jp/topics/news20210816/.

[94] ギャップインターナショナル株式会社, “クレジットカード情報流出に関するお詫びとお知らせ,” ギャップインターナショナル株式会社, 18 8 2021. [オンライン]. Available: https://thehairbar.jp/blogs/news/information001.

[95] 株式会社コマキ楽器, “弊社が運営する「コマキ楽器WEBサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 株式会社コマキ楽器, 23 8 2021. [オンライン]. Available: https://komakimusic.co.jp/pages/important-notices.

[96] 株式会社たち吉, “お詫びとお知らせ 「たち吉オンラインショップ」への不正アクセスによる個人情報漏えいについて,” 株式会社たち吉, 7 9 2021. [オンライン]. Available: https://www.tachikichi.co.jp/2021/09/07/%e3%81%8a%e8%a9%ab%e3%81%b3%e3%81%a8%e3%81%8a%e7%9f%a5%e3%82%89%e3%81%9b/.

[97] 株式会社関谷食品, “弊社が運営する「伊勢せきやオンラインショップ」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 株式会社関谷食品, 14 9 2021. [オンライン]. Available: https://www.sekiya.com/notice/.

[98] 東芝テック株式会社, “株式会社ジーアールが運営する「オムニＥＣ」への不正アクセスについて,” 東芝テック株式会社, 16 9 2021. [オンライン]. Available: https://www.toshibatec.co.jp/information/20210916_01.html.

[99] ヤフー株式会社, “中国国内、新型コロナ新規感染者「2人のみ」…感染状況落ち着きを見せる＝中国報道,” 25 11 2021. [オンライン]. Available: https://news.yahoo.co.jp/articles/980d2096cc9d2da53b075b994c26982605c7592c.

[100] 株式会社日刊スポーツ新聞社, “北京五輪、観客上限は未定　新型コロナの影響で,” 10 11 2021. [オンライン]. Available: https://www.nikkansports.com/sports/news/202111100000113.html.

[101] TREND MICRO, “「ディープフェイク」による詐欺やサプライチェーン攻撃に警戒：2020年の脅威動向を予測,” 10 12 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23044.

[102] NECソリューションイノベータ, “ディープフェイク　「機械学習の活用により今後懸念される攻撃手法の一つ」,” 不明. [オンライン]. Available: https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/33.html.

[103] ZDNet Japan, “CEOになりすましたディープフェイクの音声で約2600万円の詐欺被害か,” 5 9 2019. [オンライン]. Available: https://japan.zdnet.com/article/35142255/.

[104] Microsoft, “虚偽情報対策に向けた新たな取り組みについて,” 7 9 2020. [オンライン]. Available: https://news.microsoft.com/ja-jp/2020/09/07/200907-disinformation-deepfakes-newsguard-video-authenticator/.

NTT DATA
Trusted Global Innovator

Published on January 10, 2022

NTT DATA Corporation
Security Engineering Department
Hisamichi Ohtani / Chihiro Oyama / Daisuke Miyazaki / Kantaro Kudo / Yusuke Ota / Yuzuki Ezaki / Kenji Nagata
nttdata-cert@kits.nttdata.co.jp